



REPUBLIC OF ESTONIA
INFORMATION SYSTEM AUTHORITY

ID-
card

CERT-EE

Digi
Doc

eID

eesti.ee

X-tee

The 2020
yearbook of the
**INFORMATION
SYSTEM
AUTHORITY**

RIHA

i-voting

INFORMATION SYSTEM AUTHORITY

Yearbook 2020



Issuer: **Information System Authority**,
Pärnu mnt 139a, 11317 Tallinn

Design: **Martin Mileiko** (Profimeedia OÜ)
Illustrations: **Linda Vainomäe** (Profimeedia OÜ)
Photos: **Nelli Pello, Rene Riisalu, Marek Metslaid**
Printed at: **Ecoprint**

Contents

INTRODUCTION

- 4 Column of the **Director General**
- 5 The Estonian E-state **in figures**
- 6 **Chronology of the Information System Authority**: how did we get here?



STATE INFORMATION SYSTEMS

- 8 **eID**: the key to e-services
- 12 **DigiDoc4 client**: the software that gives the ID-card wings
- 14 **X-tee**: the blood vessels of the e-state
- 16 **Eesti.ee**: our door to the e-state
- 18 **The state network**: fast and secure data communication for the public sector
- 20 **I-voting**: we are the pioneers
- 22 **State authentication service**: a secure gateway to e-services
- 24 **The signing service**: letting you focus on your main activity
- 26 **RIA's consent service** opens up the data economy
- 28 **RIHA**: the guide to the Estonian state information system

CYBERSECURITY

- 30 **CERT-EE**: the Estonian national cyber unit
- 32 **The situation in cyberspace**: 2019 was a year of phishing
- 35 Estonia will have a new **information security standard**
- 36 **Prevention campaigns** to combat cyber threats
- 38 **Hope for the best**, prepare for the worst



INTERNATIONAL RELATIONS

- 40 **International relations**: 150 delegations in a year
- 42 **International projects of RIA**



OUR PEOPLE

- 44 RIA **numbers** and **people**
- 45 **Structure of RIA**
- 46 **The employees of RIA** about RIA

We are creating the best **DIGITAL SOCIETY** in the world

The year 2019 was full of changes for the Information System Authority (RIA). A large part of our management changed, creating an essentially new mindset for the authority. New people mean new ideas and new directions to boost the e-state.

We can see that the digital and real worlds are so closely connected that it is no longer possible to keep them separate, and the Estonian people understand this more and more. E-services are becoming more and more important in everyday life, and now, even an hour-long interruption in the work of e-services significantly disrupts people's lives.

As e-services are becoming more popular, cybercriminals are becoming increasingly resourceful and finding new ways to exploit unsuspecting people. Therefore, more and more efforts are needed to make our services work at all times and in all situations. At the same time, we must not forget to educate people. The threats of the digital world are changing and our citizens and businesses are increasingly being targeted. It is up to the state to identify and mitigate these threats at an early stage.

International cooperation is becoming increasingly important because cybercrime knows no borders. According to the World Economic Forum's 2020 Global Risks Report, three of the ten main risks stem from technology and our inability to adequately protect it.

In addition, ordinary people are increasingly aware of the dangers of the cyber world and want the state to help them cope with those dangers. That is why we need to invest even more in cybersecurity – the Internet and cybercriminals are here to stay. The digital state largely depends on trust, and the role of the state is to build that trust.

Secure solutions require money and investments.

**The digital state
largely depends on
trust, and the role of
the state is to build
that trust.**



Margus Noormaa

Director General of the Information
System Authority

For years, we have depended on foreign aid to develop the key components of the e-state and other important solutions, but this is not sustainable. We are working to make funding more secure and consistent.

In addition to a common vision and money, it also requires competent and hard-working people. In fact, people are the key to success. As an employer, RIA wants to be attractive and dignified enough that the smartest people of the country want to work here and achieve something really great.

Results are born when people work for a common goal: the Estonian e-state is also built in close cooperation between the public and private sectors. At RIA, we work as a united team to create and protect the world's best digital society. Yes, money makes the world go round, but without skilled people, it is not enough. We have excellent people thinking about how to improve existing systems, services, and solutions. At the same time, we are working on innovative solutions to make life easier for digital citizens and eliminate excessive bureaucracy.

Per aspera ad astra! ●

The Estonian E-STATE IN FIGURES



We have
something to
protect and
develop.



1,354,000+

active ID-cards



234,000+

Mobile-ID accounts



501,000+

Smart-ID users



91.6%

of residents regularly
use the Internet



87%

of households
have a computer

20

MILLION

operations are performed
with ID-cards
each month



99.6%

of banking transactions
are performed
electronically



98%

of the people file
their tax return
electronically



99%

of prescriptions
are digital



3,000+

e-services are
available via
the X-tee



66,000+

e-residents



5,000+

e-services where you
can identify yourself
with an ID-card



46.8%

of voters cast
their ballots
electronically



10,000+

companies are owned
by e-residents

HOW DID WE

RIA has developed as a result of the reorganisation and merger of several institutions.

The Estonian Informatics Foundation (Eesti Informaatikafond), established in 1990 under the administration of the Government Office, has, over the years, become a government agency operating under the administration of the Ministry of Economic Affairs and Communications, employing approximately 150 people.

Directors of RIA

Margus Noormaa,

Director General
22 April 2019 – ...

Taimar Peterkop,

Director General
4 May 2015 –
9 December 2018

Jaan Priisalu, Director

General 1 June 2011 –
16 January 2015

Epp Joab, Director of the
State Information Systems
Development Centre

26. mai 2003 –

31. mai 2011

DIRECTORS OF PREVIOUS AUTHORITIES

Imre Siil, Director of the
Estonian Informatics Centre
... 1997 – 5 May 2003

Väino Sarnet,

Director of the Public
Procurement Centre
15 November 2001 –
2 September 2002

Ustus Agur, Executive
Director of the Estonian
Informatics Foundation
1991 – 1 January 1997



In November

1989, the Estonian Informatics Council was formed. In December 1990, the Estonian Informatics Foundation started working as its labour body in the administration of the Government Office.



In March

1993, the State Information Systems Department was formed within the Government Office, the most important partner of which was the EIF.



On 7 October

2002, the first digital signature was given, when the mayors of Tallinn and Tartu digitally signed a cooperation agreement.



On 28 January

2002, the first ID-card was issued.



On 12 March

2003, the citizen information portal <https://www.eesti.ee/en/> was launched, which provided people with information about their rights and obligations, as well as advice on practical dealings with public authorities.



In May

2003, the State Information Systems Development Centre was established by merging the Estonian Informatics Centre and the Public Procurement Centre.



As of 29 June

2015, the monitoring team of the Incident Response Department (CERT-EE) of the Cyber Security Branch is working 24 hours a day.



On 10 December

2013, the Prime Ministers of Estonia and Finland digitally signed a memorandum of cooperation in BDOC format.



From July

2016, digital signatures issued by Estonian citizens are accepted by public sector institutions of other European Union countries. Similarly, Estonian state and local government agencies recognise the e-signatures of other EU countries.



On 30 September

2016, the Information System Authority and the Finnish Population Register entered into an agreement to connect X-tee and its Finnish analogue (Palveluväylä).



In September

2019, RIA also introduced Smart-ID as an authentication tool in state services.

GET HERE?



In 1996, the Estonian Informatics Foundation was reorganised into a state authority managed by the Government Office, which became known as the Estonian Informatics Centre. The Estonian Informatics Council was transformed into an advisory commission to the government, the name of which remained the same as before, but which received new tasks.



In 1997, the Data Communication Department, which had previously operated at the Institute of Cybernetics, was added to the Estonian Informatics Centre.



In 2001, the State Information Systems Department launched two projects to transform the nationwide ICT infrastructure: the data exchange layer X-tee (then called X-Road in English) and eKodanik, which have now grown into a state portal uniting the country's e-services.



In 2000, the State Information Systems Department was established in the Ministry of Transport and Communications. **On 1 January 2001**, the Estonian Informatics Centre was also transferred to the administrative area of the Ministry of Transport and Communications as a state authority, where it continued its activities in the current main directions.



In 1998, the Data Communication Department became the administrator and developer of PeaTee, one of the most important data communication backbone networks in the country.



In August 2004, the ISKE system of security measures for state and local government information systems was introduced.



In 2006, the document exchange centre DVK was established, which connected the state-managed document management systems.



On 1 March 2006, the Information Security Incident Management Department was established, which performs the tasks of CERT Estonia at the state level.



On 1 June 2011, the State Information Systems Development Centre became the Information System Authority (RIA).



On 1 October 2009, the Critical Information Systems Protection Department was established.



On 29 May 2008, the administration system for the state information system (RIHA) was opened, the aim of which is to provide a comprehensive picture of the state's IT resources.



On 7 March 2017, the Estonian minister of entrepreneurship and information technology and the Finnish minister for foreign trade and development signed an Estonian–Finnish cooperation agreement, on the basis of which a joint non-profit association for the joint development of X-Road was formed.



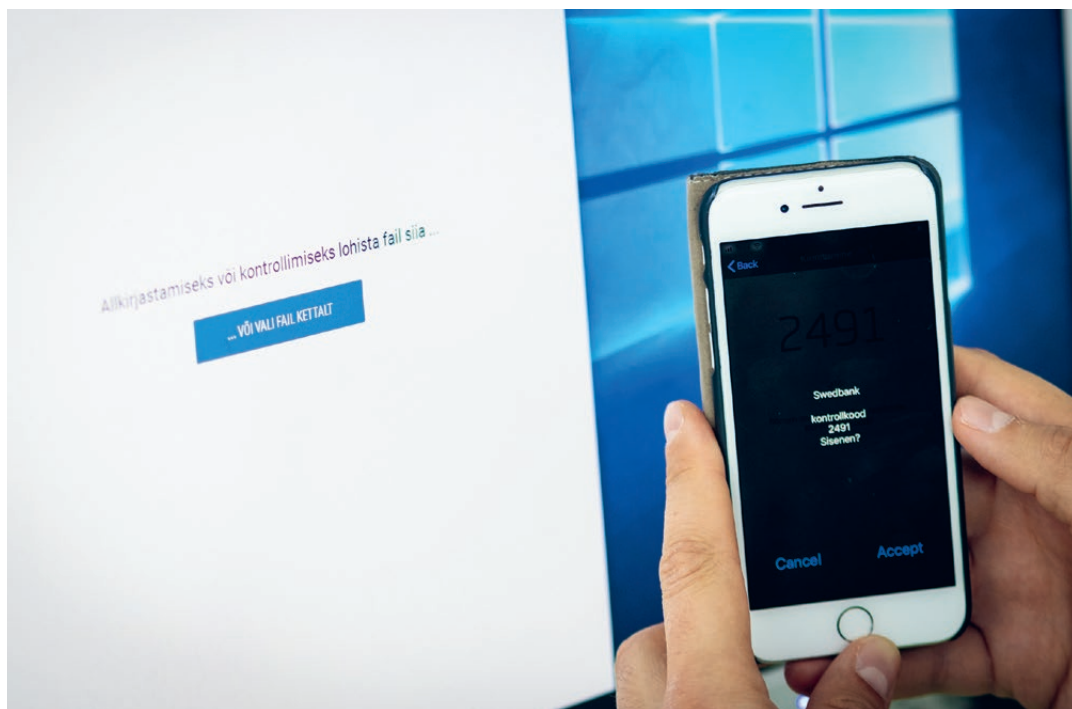
On 30 August 2017, an international team of researchers informed RIA that they had discovered a security risk affecting approximately 750,000 ID-cards. A security update for ID-cards was released in October.



In July 2019, the secretariat of EU CyberNet, a network of European Union cyber experts, was established at RIA, which will coordinate all cybersecurity projects carried out by the European Union in third countries.



In December 2018, a new generation of ID-cards with new security features and a contactless interface was introduced.



eID:

the key to e-services

Every person has a physical identity. In addition to that, almost all Estonian residents have an electronic identity (eID), which we can use to authenticate ourselves electronically, give digital signatures, and encrypt files.

The importance of eID cannot be overestimated: without it, we would not have our beloved e-services, digital signatures, or the opportunity to do business with public authorities over the Internet. Formal communication would be on paper and would take much more time.

WHAT IS IT?

An electronic identity is a set of data that links a person to their physical identity in an electronic environment. We all have only one national identity in both the physical and digital world, but one person can have several electronic identity carriers, i.e. places where their eID data are stored. There are three major eID carriers in Estonia: ID-card, Mobile-ID, and Smart-ID. In addition to these, electronic identity documents also include a residence card, a diplomatic ID, a digital ID, and an e-resident's digital ID, but



their share is small. Banks issue various authentication tools to their customers, but they can generally only be used in the bank's own services or in other services via a bank link.

HOW DOES IT WORK?

In Estonia, the basis of electronic identity is the public key infrastructure (PKI). The PKI model is based on two interrelated keys – the secret and the public key. As the name suggests, the secret key is protected and can only be used by the person to whom it was issued. The public key is available to everyone.

This model, containing both a secret and a public key, allows secure access to e-services, i.e. digital authentication and digital signing. It can also be used to transmit data securely or in encrypted form. All operations related to eID devices (authentication, signing, encryption, and decryption) are protected by PINs, i.e. you must enter the PIN1 or PIN2 to activate your secret key.

THE NEW ID-CARD HAS RECEIVED GOOD FEEDBACK

The ID-card is the most common eID carrier. It is obligatory for all Estonian citizens and permanent



There are three major eID carriers in Estonia: ID-card, Mobile-ID, and Smart-ID.

What does **RIA** do?

- We shape a vision and strategy for the development of the eID field. We are its spokesperson and influencer in Estonia.
- We are responsible for the security and compliance of the secret key carrier of the eID devices and the software on it.
- We are responsible for the operation, development, and management of the end-user ID software (the DigiDoc application).
- We are responsible for the development, operation, and management of eID software offered to e-service developers and providers.
- We are responsible for the interoperability of international electronic identities, i.e. the operation, development, and administration of the cross-border software solution.
- We participate in Estonian and international working groups and contribute to the development of the country's PKI field.
- We provide user support for the basic ID-card software.
- We provide support for developers.

residents from the age of 15.

There are more than 1.3 million valid ID-cards in circulation in Estonia. About 930,000 of them are used electronically to perform an average of about 20 million digital transactions each month (giving digital signatures and accessing e-services).

Although the Mobile-ID and Smart-ID solutions operating in smart devices are becoming more and more popular, they are currently used by only about half of the Estonian population. The ID-card is the primary eID carrier, without which neither Mobile-ID nor Smart-ID can be activated.

The Police and Border Guard Board started issuing ID-cards with a new design, security elements, and functionality at the end of 2018. The new card has a colour photo and several design elements typical of Estonia.

The chip of the new ID-card has a larger storage capacity, which will allow new applications to be

added to it in the future, such as an electronic ticket for public transportation or another certificate issued in electronic form. In addition to the usual contact interface, the new card also has a contactless version, which allows it to be used in the same way as contactless bank cards. For security reasons, digital signing and authentication are initially only possible with a contact chip.

In March 2019, our ID-card received high recognition when the awards for the best new documents and banknotes were presented at the High Security Printing conference in Malta. Estonia won in the ID-card category. The expert committee acknowledged the design of the card, the security elements, the chip, and the new solutions – QR code capabilities and the contactless option.

In 2020, we will develop the ability to remotely update ID-cards so that we could refresh the software and certificates on the chip if necessary. This is one of the solutions that we hope will never be needed, but, as the 2017 ID-card crisis showed, we must be prepared for the unexpected.

The ID-card chip that we will start issuing from July 2021 must have the cardholder's picture and fingerprints in addition to their personal data file. We are currently preparing for this.

We have been asked on several occasions when we will replace the PINs of ID-cards with fingerprints or face recognition. This would make personal identification and digital signing faster and more convenient. Unfortunately, this will have to wait because currently, no biometric authentication solution is secure enough to link it to our electronic identity. Both fingerprint readers and facial recognition systems have been deceived without much effort. The eID must first be secure and protected and only then convenient. Security and reliability cannot be compromised for the sake of convenience.

SMART-ID: CONVENIENCE AND SECURITY

In 2017, the new electronic identity solution Smart-ID arrived on the market, which works on smart devices

Active ID-cards:

OVER

1,354,000

Active Smart-ID accounts:

OVER

501,000

Active Mobile-ID accounts:

OVER

234,000

A digital signature saves every citizen

AN AVERAGE OF

5

WORKING DAYS A YEAR

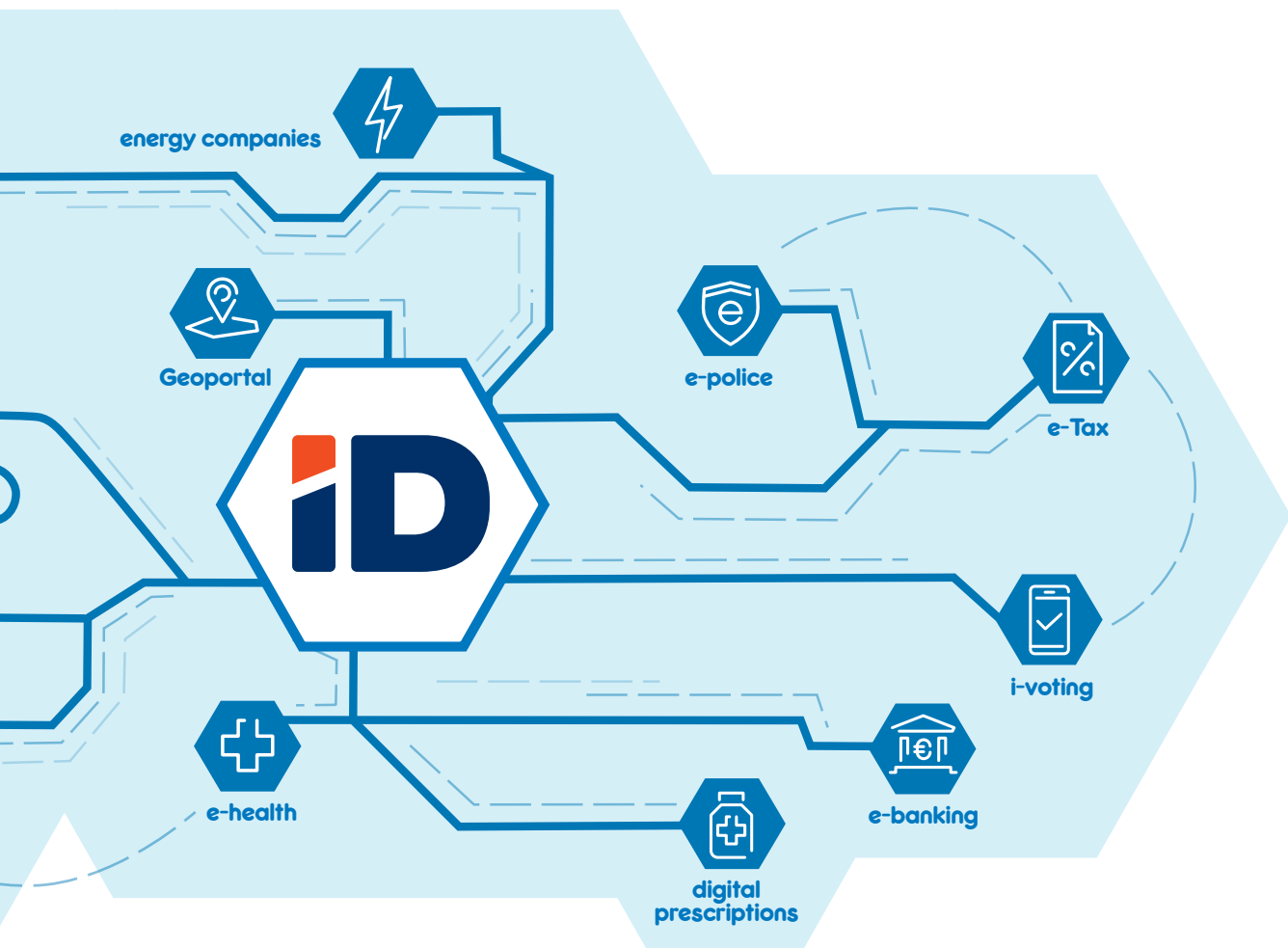


and, unlike mobile-ID, does not require a SIM card. Smart-ID is the second most popular eID carrier with more than 501,000 users in Estonia (as at March 2020).

From November 2018, Smart-ID can also be used for digital signatures.

Although the service has been warmly received, 2019 brought along some challenges for it. Fraudsters took over about twenty Estonian Smart-ID accounts, which has never happened with ID-cards or Mobile-ID. From 1 July 2019, activating your Smart-ID became a bit more complicated, but significantly more fraud-proof.

We all want access to e-services and giving digital signatures to be as easy and fast as possible. We wish that activating your eID carrier would be just as



convenient. However, we must think about security – if the activation is not secure, the users will lose trust in it, and this will mean that e-services will no longer be used.

We are convinced that convenience cannot be created at the expense of security. If asking the user for a few more taps on their screen or clicks with their mouse makes the eID carrier significantly more secure, we have to do so.

WHAT WILL HAPPEN TO MOBILE-ID?

The third most popular eID device is Mobile-ID. The service, which was launched in 2007 and operates on the basis of a SIM card, has more than 234,000 users. 22 per cent of the national authentication service's personal identifications are made with Mobile-ID. The procurement contract for Mobile-ID expires in 2021. What will happen after that?

If the activation is not secure, the users will lose trust in it, and this will mean that e-services will no longer be used.

We do not have a definite answer yet. We know that the state must issue two alternative eID tools to every citizen. For at least the next five years, the ID-card will be one of them. It is not clear at this time what the second state-issued electronic identity carrier will be. It may or may not be Mobile-ID.

HOW MANY eID CARRIERS DO WE NEED?

On the one hand, the more electronic identity carriers we have, the better. In this way, the risks are better spread: if one of them stops working, we can still use the rest of them, and our e-state will continue to operate. At the same time, the creation, development, and management of each eID tool creates additional costs for both eID tool providers and e-services. The three pillars – currently, the ID-card, Mobile-ID, and Smart-ID – are a sensible solution. The risks are sufficiently hedged and every tool has a sufficient number of users. ●

The DigiDoc4 client: the software that gives the ID-card wings

An ID-card without the software is an ordinary identity document. Its electronic capabilities are realised by the DigiDoc software, which is already installed on about 600,000 computers and used to give about half a million digital signatures every month. Previously, it was possible to use the DigiDoc software to perform operations with an ID-card and Mobile-ID. In January 2020, Smart-ID support was added.

WHAT IS IT?

DigiDoc is a piece of software that allows you to give digital signatures, open digitally signed documents, check the validity of signatures, encrypt files, and decrypt them – which means making classified data readable again.

In addition, you can set up an @eesti.ee e-mail address with DigiDoc, check the validity of your ID-card certificates, change PINs and PUKs and, if necessary, unblock certificates.

DigiDoc is available for Windows, macOS, Linux, iOS, and Android and can be downloaded from id.ee or from the Android and Apple app store.

THREE IN ONE

In July 2018, the DigiDoc4 Client was launched, which has a simpler and more modern user interface. Previously, it was necessary to install three separate applications on your computer for the basic functions – the ID-card management tool, the DigiDoc3 Client for signing, and DigiDoc Krüpto for encryption. However, with DigiDoc4, all operations can be performed in one user interface and only one

application needs to be installed on the computer.

During the installation of the ID software, the DigiDoc4 Client, add-ons, and drivers required for online authentication and signing are installed on your computer.

TERA ADDS TIMESTAMPS

Another useful application is installed on your computer: the stamping application TeRa. What does it do and why is it necessary?

As computing powers and the tools available to malicious people continue to evolve, our digital envelopes in DDOC format are no longer as secure as they were ten years ago. TeRa creates a new, time-stamped ASICS envelope that meets modern security requirements, in which the old original is placed.

The new time-stamped envelope helps to identify the opening and modification of the old envelope. If the parties have different versions of the same document, a timestamp can be used to prove which version is the original.

For those who have a lot of DDOC files on their computer that need to be checked and proven in the future, we recommend that you make them more tamper-proof with the TeRa stamping application. It is quick and easy: after

running it, TeRa retrieves expiring digital signatures (in DDOC format) from the computer and moves them into a new, cryptographically more tamper-proof container. All old files remain where they were originally, but new ASICS files are created that can be opened with DigiDoc4. It takes up to a few minutes to stamp a few hundred documents. ●

**It takes up to
a few minutes to
stamp a few
hundred
documents.**



The DigiDoc software is installed on approximately

600,000

computers.

What does RIA do?

- We **update our ID software** at least twice a year to keep pace with the development of operating systems, web browsers, and support programmes, and to provide new opportunities for our users.
- We **guarantee ID-card user support**: if you have problems using the ID-card, the DigiDoc4 Client application, or the TeRa software, you can find a solution at id.ee.
- We **develop and manage** the timestamping application TeRa.
- We **mediate the timestamping service** for public sector institutions.



Thanks to e-residents, the open-source DigiDoc software is used all over the world.

It is used to give around

500,000

digital signatures every month.

DigiDoc is a available for

Windows, MacOS, Linux, iOS, and Android.

From the beginning of 2020, DigiDoc also supports

Smart-ID in addition to ID-cards and Mobile-ID.

X-TEE: the blood vessels of the e-state

Many of us have seen illustrations of human blood circulation in a biology textbook or in a family physician's office. By looking at them, we get an idea of how a person survives and functions in life. The 'blood circulation' of the e-state can be visualised similarly to that of a human, but there is one important difference. The e-state does not have a heart without which a person would not survive. Our e-state is distributed.

LOTS OF EGGS, LOTS OF BASKETS

For each database, there is a risk that its contents will leak. If a state gathered all the information in its possession in one data warehouse, one attack or human error would be enough for all the data to be stolen. Not to mention that it would be costly and complicated to manage such a database centrally.

Estonia has mitigated this risk by ensuring that each agency and ministry takes care of its own data. The population register contains information about a person's place of residence, the commercial register contains information about a company, and the Road Administration has information about vehicles. If one database is 'hit', the others are not affected.

How do institutions perform their tasks if information about people, companies, vehicles, education, health data, plots of land, and tax receipts is spread all over Estonia?

X-TEE COMES TO THE RESCUE

The Estonian data exchange layer X-tee, completed in 2001, comes to the rescue. This is a

solution that, among other things, helps to buy medicines with a digital prescription in a pharmacy, check the data of the vehicle and its owner from the e-police device, and request information about new conscripts from the population register belonging to the Ministry of the Interior on the servers of the Ministry of Defence. There are thousands of examples that reduce bureaucracy and increase efficiency.

It is important to understand that X-tee is only a tool for secure data exchange by creating a unified protocol. If X-tee did not exist, each authority would have to deal with protocol and security issues on their own. Data integrity is not compromised because the data is not stored in the X-tee architecture. Without X-tee, keeping data up to date would be a constant challenge, because if each agency keeps copies on its own server, it is very time-consuming and difficult to find out which one is the most recent and correct.

DEVELOPMENTS KEEP THE E-STATE HEALTHY

X-tee is the main solution in Estonia that allows the public sector to exchange data with other parties in the public sector and with the private sector. We are pleased that the number of X-tee members, services, and inquiries is on the rise. To make it possible to become a member of X-tee with just a few clicks, we are developing a self-service environment. Companies and public authorities that do not yet use X-tee will be able to join it comfortably and with less effort in the future.

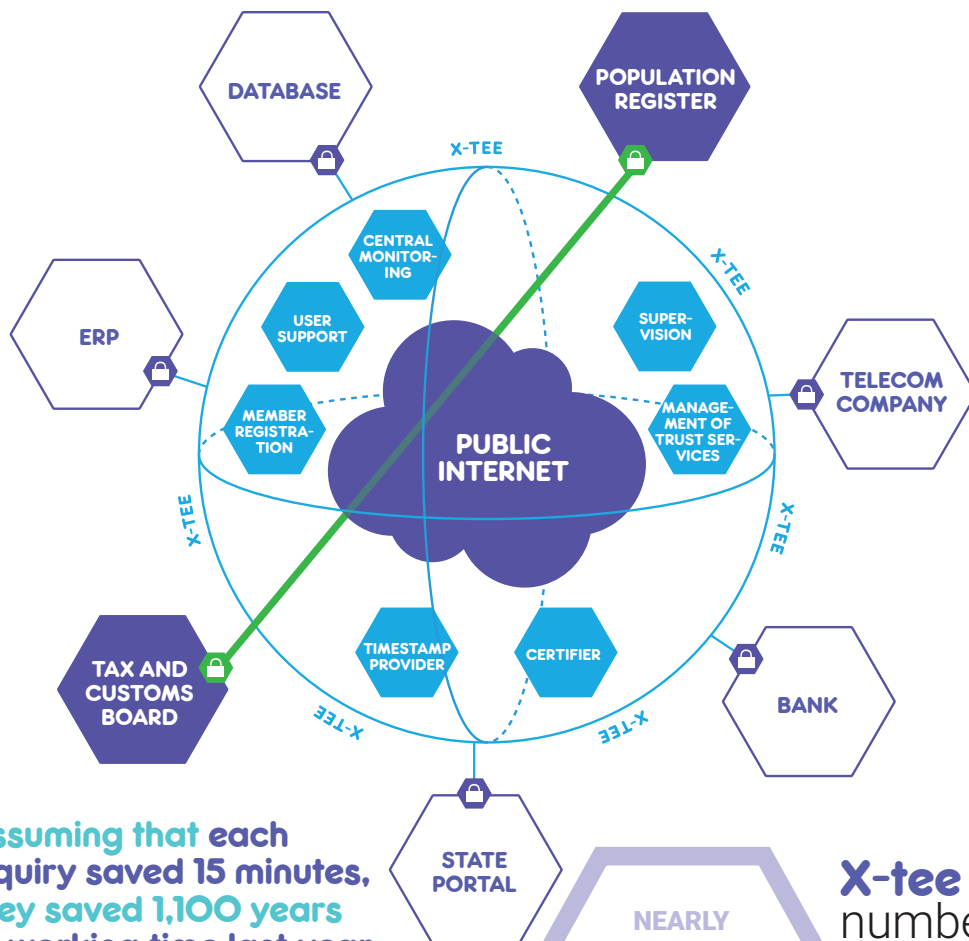
In 2019, we closed version 5 of X-tee, which had been in use since April 2011. In addition, we are internationally developing the next version – number 7 – of X-Road, which is the basis for X-tee.

AN ESTONIAN AND FINNISH JOINT PRO- JECT LED TO X-ROAD

X-tee used in Estonia is the term used for the Estonian state data exchange platform. However, when discussing the English version, X-Road, we mean the technology that Estonia and Finland have been developing together since 2015. In February 2020, an important milestone was reached – the Estonian and Finnish business registers shared data via X-Road for the first time.



X-ROAD



Assuming that each inquiry saved 15 minutes, they saved 1,100 years of working time last year.

What does **RIA** do?

- We **develop and manage** secure data exchange between agencies.
- We **work for a better customer experience**. The aim is to simplify and speed up the implementation of X-tee.
- We **share our experiences with X-tee to other countries**. Countries around the world use X-Road or its components, such as Finland, Canada, Mexico, Uruguay, Israel, Iceland, Norway, Scotland, Spain, Japan, and Vietnam. <https://x-road.global/xroad-world-map>

MAIN USERS OF X-TEE

In 19 years, almost six billion inquiries have been made in X-tee. Let us say three per cent of them were made by people. Assuming that clicks on the Internet save an average of 15 minutes per person (they do not have to go to the Road Administration, the Tax Board, or the hospital to book an appointment), these inquiries saved an estimated 1,100 years of working time last year alone. ●

X-tee in numbers

NEARLY
2,700
services can be used via X-tee.

In 19 years,
ALMOST
6bn
inquiries have been made in X-tee. An estimated 3% of them were made by people

Estonian X-tee has
MORE THAN
500
institutions and companies...

...and nearly
1,200
interfaced information systems.

EESTI.EE:

our door to the e-state

The state portal eesti.ee, launched in the spring of 2003, is a fast and practical contact point from which Estonian residents and entrepreneurs can obtain reliable information about the services offered by the state. In addition, it allows state authorities and local governments to communicate securely with people. The portal contains information about e-services and different events, and the state e-mail conveniently helps the state to inform people.

WE CLEANED UP THE BACK END

In 2019, the users of the state portal may not have noticed significant changes, as a large part of the developments was focused on the arrangement of the back end of eesti.ee. This project will largely be completed this year. Then, we will start updating the portal for entrepreneurs.

EESTI.EE MAILBOX

RIA is working to make the eesti.ee mailbox the main channel for exchanging information with the state in the coming years. The mailbox has been in operation for years, but there are currently discussions about possible changes that would allow the message to be considered delivered when it reaches the recipient's state

portal mailbox. The idea is still in its infancy and there is still no certainty about how it will work in the future.

Paper-based communication will not disappear, but it would no longer be the primary way to inform people, because digital information exchange is faster, more convenient, and cheaper. In the future, all notifications from the state or local governments will reach the eesti.ee mailbox and will always be available there.

Notices can also be sent to an external e-mail address, but the mailbox of the state portal is the place where all previous e-mails are stored. This way, you do not have to worry that the notice will not reach your inbox due to errors committed by yourself (deleting the message) or your service provider (service failure). The communication between the state and the citizen is preserved in the eesti.ee mailbox.

THERE WILL BE A CHATBOT

Currently, a quarter of a hundred state authorities use the eesti.ee mailbox to transmit important information. The aim is to get all institutions to join the service. There will also be a calendar which will inform the person about important events, and a chatbot that will help them to communicate with the state more easily. ●

The history of EESTI.EE

**The state portal
eesti.ee was
launched on 12
March 2003.**

The portal provides people with information about their rights and obligations in Estonia. It also provides advice on practical matters with public authorities.

In 2005, articles in English and Russian were added to the portal. The design of the site became more user-friendly and logical. Entrepreneurs could start using the @eesti.ee e-mail address.

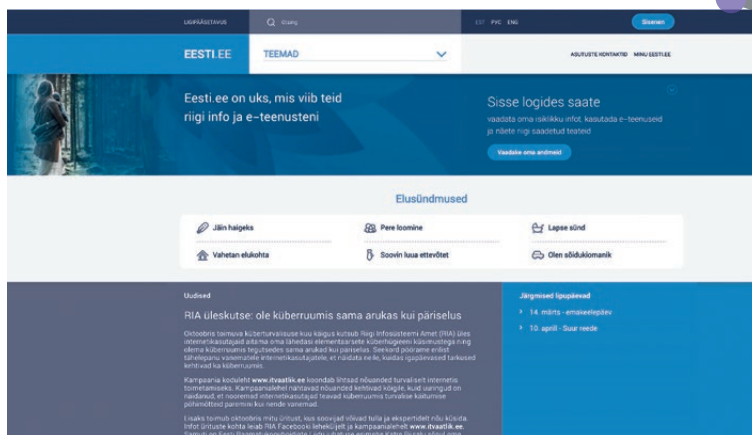
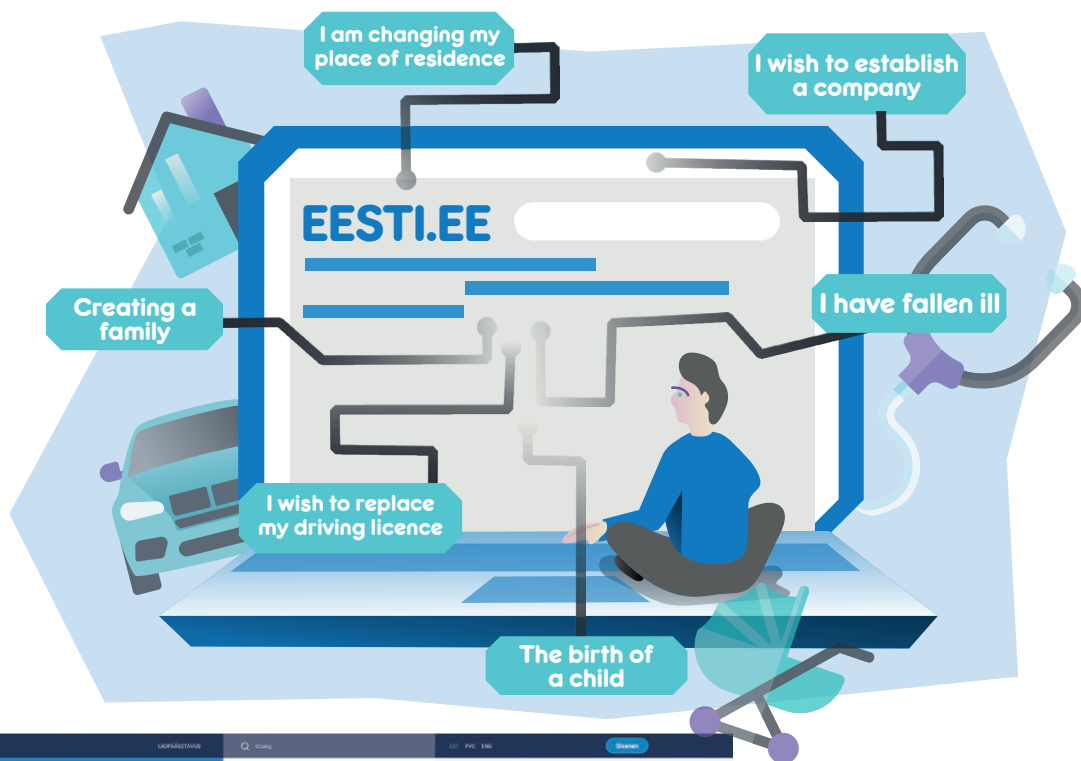
In 2007, the previous version of the current state portal was completed. The new state portal brought together the previous information portal and the citizen portal, and the information is divided into blocks for the citizen, entrepreneur, and official. Eesti.ee became the country's central portal, visited

by 110,000 people a month, including 8,000 foreigners. The @eesti.ee mailbox is used by 19,000 people and 17,000 companies.

From 2008, the portal could be accessed with Mobile-ID.

In 2009, eesti.ee received a new green logo that is still the best known one.

In 2011, the part for entrepreneurs became more comprehensive. The portal has 200 services, 400 articles, and 2,500 contacts.



What does RIA do?

- **We manage** the state portal eesti.ee
- **We consolidate** the e-services of state authorities there.
- **We mediate** the contact information of institutions and information about the services offered by the state through eesti.ee.
- **We guarantee** every person with an Estonian personal identification code on the state portal with the following e-mail address: personalidentificationcode@eesti.ee.
- **We offer** companies the following e-mail addresses: registrycode@eesti.ee and companyname@eesti.ee.

Since **2013**, the user can see their personal data and events on the home page if they are logged in.

In **2015**, eesti.ee had 815 e-services. In 2014, there were users from nearly 200 countries and 9,000 cities. People most often use it to view the menu item 'My things', log in to SAIS, update certificates of incapacity for work, and view their prescriptions.

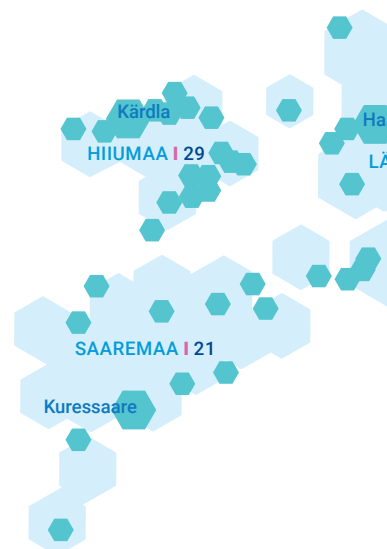
In **December 2015**, the terms of use of eesti.ee notices were changed. By forwarding

one's @eesti.ee address, the person consents to the state authorities sending them official documents and forwarding notices to this address.

In **2017**, eesti.ee had a total of 1,330 articles, 154 services, and 2,866 contacts in Estonian, Russian, and English.

At the end of **2018**, the current design of the eesti.ee portal was completed.

THE STATE NETWORK: fast and secure data communication for the public sector



The state network provides data communication and Internet services to state authorities and local governments in more than 1,400 locations all over Estonia. 97 per cent of public sector bodies are connected to the state network. In exceptional cases, legal entities providing public services on behalf of the state may also join.

THE STATE NETWORK IS FAST

The end-user is offered upload and download speeds of up to 1 Gbps, but we can offer connections that are up to ten times faster. The core of the state network is the backbone network which is expected to increase to 200 Gbps in the near future. At the same time, we keep at least 30 per cent of our resources in reserve to ensure the smooth operation of the backbone network, even in times of temporarily increasing load.

THE STATE NETWORK IS SECURE

Its work is monitored 24/7 by CERT-EE, which, in addition to detecting and resolving cyber incidents, works on their prevention. From spring 2019, external connections to the state network are protected against distributed denial-of-service attacks (DDoS). In case of attacks originating in Estonia, we quickly catch the attackers.

The state network manages the duplicate internet hub RTIX, which connects Estonian Internet networks and aims to ensure the network traffic even when the connection with foreign countries is disturbed.

HELP IS NEAR

We work with the IT and Development Centre of the Estonian Ministry of the Interior (SMIT) to resolve failures. If, for example, some network equipment in Valga or Kuressaare needs to be replaced as a matter of urgency, a technician of the Information System Authority (RIA) does not have to go there from Tallinn, but we can ask for help from the SMIT technicians who are usually closer. This is cheaper for the state, as we avoid duplication, and more convenient for the customer of the state network, because they receive help faster.

Technology is
evolving and
the state
network must
keep up with it.

WHAT WILL THE FUTURE BRING?

We continue to develop the state network on a daily basis and work to reduce the time it takes to establish a customer connection. We are expanding the backbone network and increasing its capacity – the goal is to increase the speed up to 200 Gbps.

In doing all of this, we realise that the state network is like Tallinn, which will never be complete. Technology is evolving and the state network must keep up with it. ●

The data rate
offered to the
customer is
usually up to

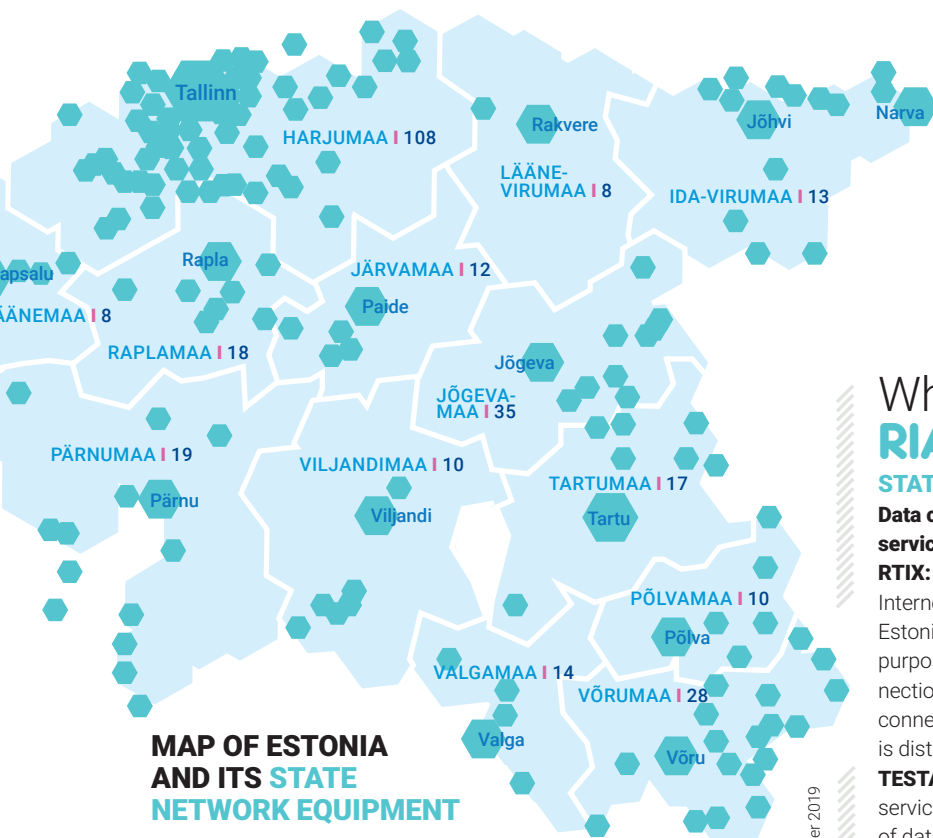
1 Gbit/s

but we
can also
offer

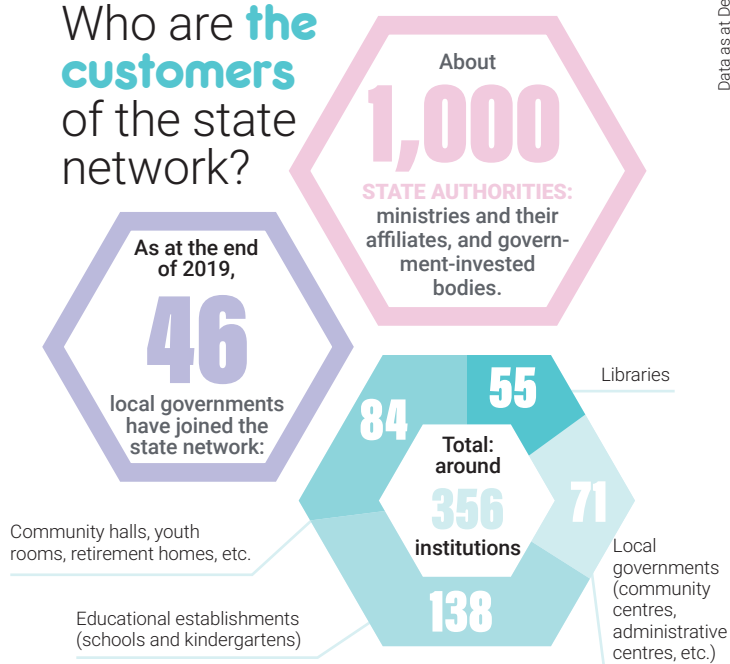
10 Gbit/s

The aim is to
increase the
backbone network
speed up to

200 Gbit/s



Who are the customers of the state network?



Data as at December 2019

What does RIA do?

STATE NETWORK SERVICES

Data communications and Internet services for the public sector.

RTIX: a state-managed duplicate Internet hub that interconnects Estonian Internet networks. Its purpose is to ensure the interconnection of networks even when the connection with foreign countries is disturbed.

TESTA-NG: a data communication service used for the secure exchange of data between the institutions of the European Union and the Member States. The aim is to bring all secure data exchange solutions between EU Member States into the TESTA network.

DNS: a name server service that allows us to type the domain name instead of an IP address, or a combination of numbers, into the address line of the web browser to reach the desired web page.

DNSSEC: security extensions for the domain name system that ensure that the user is redirected to the specific web page whose address they entered in the web browser, not a phishing page.

NTP: accurate time service. For this, you have to set the ASO time server (ntp.aso.ee) as your primary time source. We use GPS-based STRATUM 1 class NTP servers, which are duplicated and located in physically different locations, to provide the service.

CACHE: the state network customers can use proxy servers to help deliver the data you requested faster.

97%

of public sector bodies are connected to the state network.

In 2019, we invested

1 million euros

in upgrading the state network equipment.

I-VOTING:

we are the pioneers

The local elections held in October 2005 were special: Estonia became the first country in the world to introduce i-voting in nationwide elections.

At the time, there were only 9,317 i-voters, accounting for 1.9% of the voters. At the 2019 Estonian Parliament (Riigikogu) elections, 247,232 people voted electronically, making up 43.8% of those who voted.

WHAT DOES I-VOTING MEAN?

Electronic voting means voting via electronic means using the Internet. I-voting allows you to cast your vote from anywhere as long as you have an Internet-connected computer and an ID-card, mobile-ID, or digi-ID with valid certificates. You can i-vote throughout the pre-voting period, but not on election day.

The purpose of i-voting is to make elections easy and convenient for voters and organisers alike.

HOW DOES IT WORK?

You need to download the voter application to your computer to i-vote. Once you have been identified, the application checks if you have the right to vote and, if you do, displays the list of candidates.

Once you have selected your favourite candidate and confirmed your vote with a digital signature, the voter application will send the vote to the vote collection servers. The registration service adds a timestamp to each vote, allowing to check later that all votes have been forwarded to the collector. You can check if the vote you gave went to the candidate you chose with a phone app especially created for that.

All of the votes are encrypted. This is done using a cryptographic algorithm, the specification of which is determined by the State Electoral Office before each election. The vote is encrypted with two keys. The voter application uses a public key to encrypt your vote. A secret key, accessible only to members of the State Electoral Committee, is required to decrypt the vote.

WHAT DOES IT HAVE TO DO WITH THE INFORMATION SYSTEM AUTHORITY (RIA)?

I-voting is organised by the State Electoral Office in cooperation with RIA. Collaboration began years ago when we hosted the i-voting system, and has been expanding ever since. It is the wish of both the State Electoral Office and RIA that in the future, RIA will be responsible for the development and management of all electoral information systems.

In 2019, responsibility for electoral information security shifted from the State Electoral Office to RIA. We purchased additional servers, strengthened the firewall, provided distributed denial-of-service (DDoS) safeguards for the state network, and tested the election information systems. In addition, we conducted cyber hygiene training for candidates and campaign teams, tested campaign and party websites, and created an interdepartmental security manager position.

WHAT WILL THE FUTURE BRING?

Since 2019, RIA is also responsible for developing the electoral information system. We are working on the new version, VIS3. This will bring

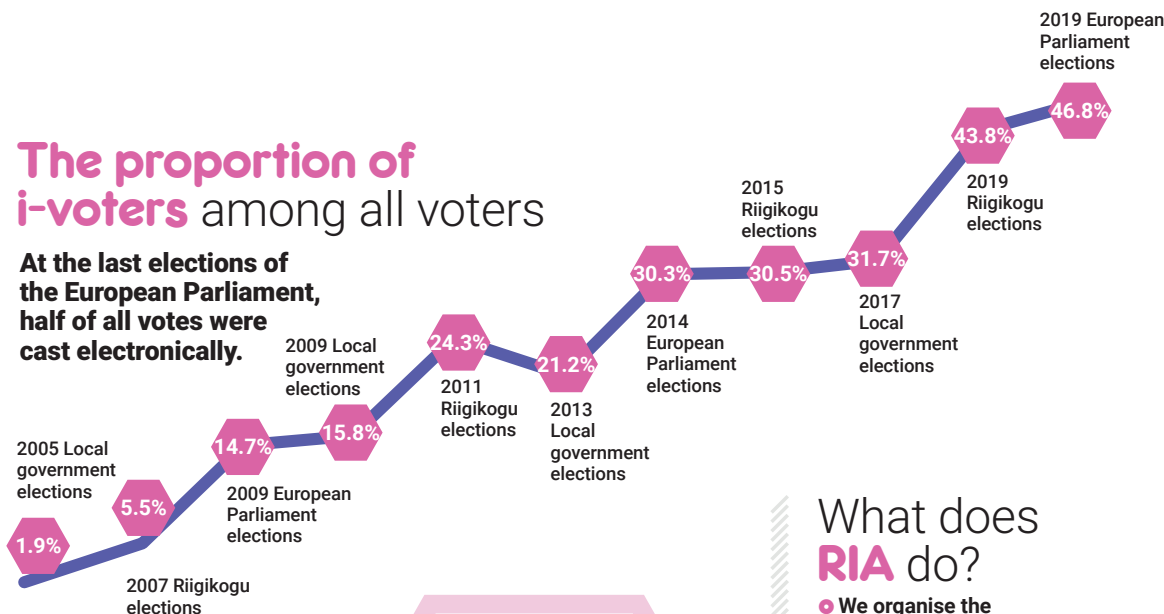
When will it
be possible
to vote with
my **mobile**?

We also want to make the elections available on smartphones, which we use more and more every day.

We hope that the possibility of m-voting will be added to local elections in 2021, but we must first be convinced of their security.

The proportion of i-voters among all voters

At the last elections of the European Parliament, half of all votes were cast electronically.



I-voting in numbers

The time it takes to cast an i-vote:

3
MINUTES

In the 2019 parliamentary elections,

247,232
PEOPLE VOTED ELECTRONICALLY,...

...which accounts

43.8%
of those who voted

What does RIA do?

- **We organise the conducting of i-voting:** we provide the necessary hardware and software.
- **We develop and maintain the election information system (VIS):** it allows to register candidates, identify election results and turnout, and share this information with the public.
- **We are responsible for the information security of the elections:** we test election information systems, protect against potential attacks, and train candidates and campaign teams.

about a number of changes that will mean less hours of work for election organisers and candidates and increase transparency.

Until now, the list of voters was printed on paper and the polling station member manually checked if the person entering the polling station was included there, while VIS3 makes the voter lists electronic. This and the amendment of the legislation on elections are pre-requisites for allowing i-voting to take place until the end of the advance voting and for letting the voter change their i-vote by voting on paper at the polling station on election day.

Up until now, information on turnout has been

With the new election information system, we will save thousands of hours of work.

communicated once a day during the pre-election period and three times on election day. The new electoral information system, however, will release it more frequently.

The new information system can also be used by candidates and political parties, who do not have to go to the State Electoral Office to submit the list of candidates but can also do so via the

election information system and also pay the necessary state fees there. With the new election information system, we will save thousands of hours of work otherwise spent on organising and conducting elections.

When VIS3 is completed, we will release the code so that anyone interested can see how it is done. ●

STATE AUTHENTICATION SERVICE

a secure gateway to e-services

If you want to access any of the state e-services, you must first authenticate yourself to prove that you are who you are claiming to be. The authentication must be reliable and secure because no one wants their data to be accessed by strangers or deals to be made on their behalf by a criminal.

Therefore, public authorities and those who perform public functions can use the state authentication service, which may use ID-card, mobile-ID, Smart-ID, and/or cross-border authentication. They can be combined or used separately.

WHAT IS IT USED FOR?

There are hundreds of e-services in the public sector in Estonia that require user authentication. Although most of them already supported ID-card and mobile-ID authentication, it was foreseen that there will be more eID tools available and that, in addition to Estonians, they would have to be able to identify citizens of other EU countries.

Because new developments and requirements mean extra costs to each service provider, a centralised authentication service was created that can be used by all public authorities and is developed and maintained by RIA. This way, the service providers can focus on their core business.

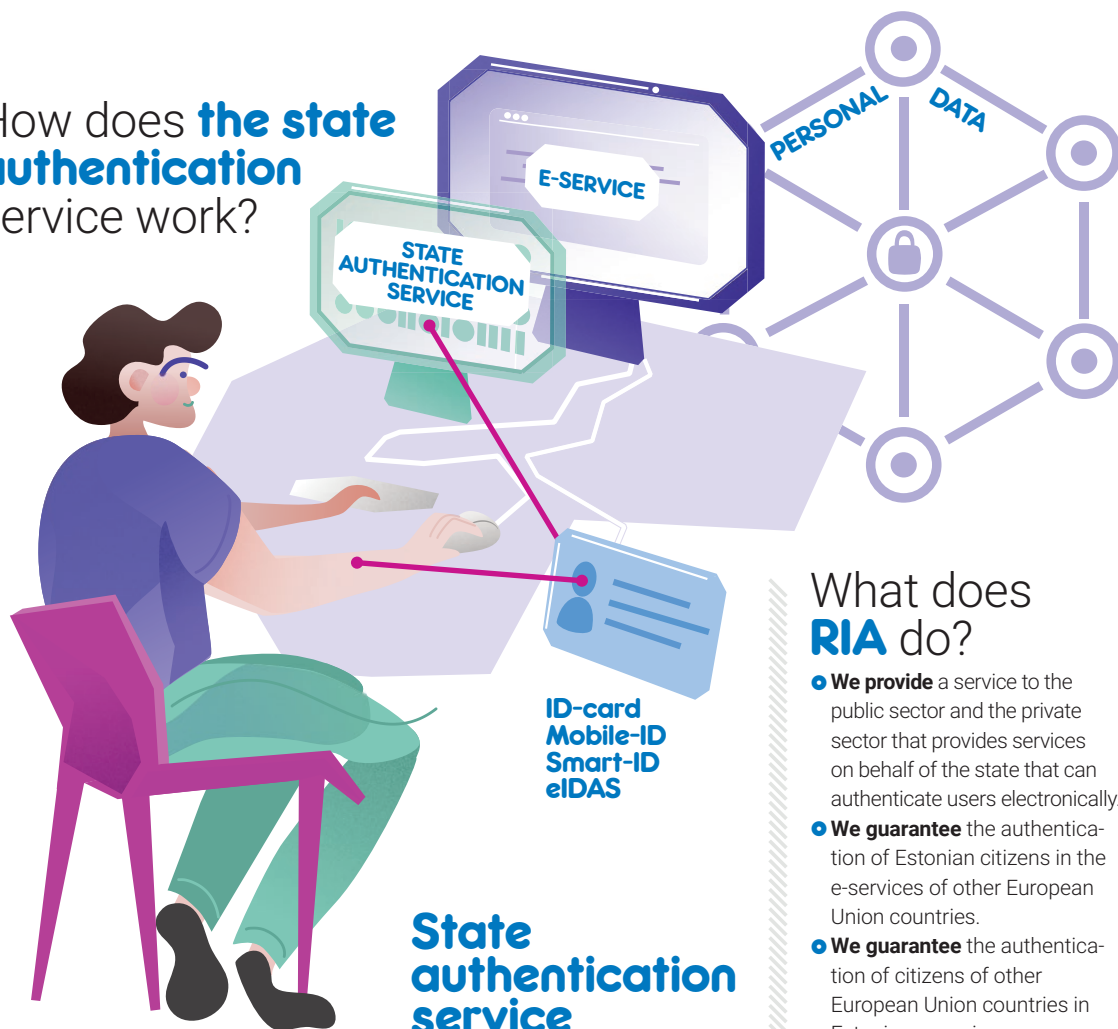
**The authentication
must be reliable
and secure.**

WHAT WILL THE FUTURE BRING?

If you use Google's services, you are aware that one sign-in is enough to access your e-mails, documents, and photos. However, every time you use Estonian public sector e-services, you have to be re-authenticated.

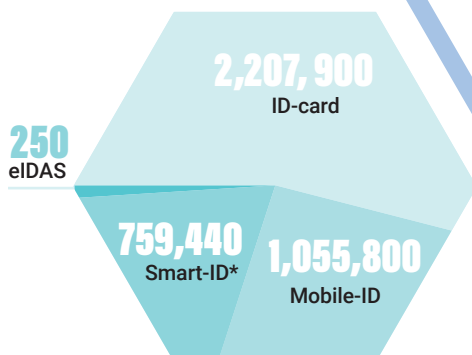
We would like to change this and are testing whether a single sign-on service (SSO) can be used for the state authentication service. As the name implies, such a solution requires only one authentication: once a user has logged into an e-service through the state authentication service, they can use the other e-services without having to re-authenticate themselves in all of them. ●

How does **the state authentication** service work?

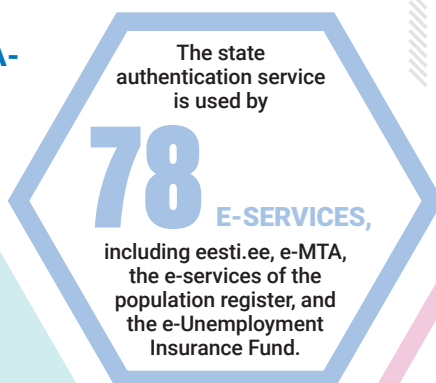


State authentication service in numbers

THE RELATIVE IMPORTANCE OF AUTHENTICATION METHODS in the state authentication service, 29 March–31 December 2019



* Smart-ID was added in October 2019.



What does **RIA** do?

- **We provide** a service to the public sector and the private sector that provides services on behalf of the state that can authenticate users electronically.
- **We guarantee** the authentication of Estonian citizens in the e-services of other European Union countries.
- **We guarantee** the authentication of citizens of other European Union countries in Estonian e-services.
- **We guarantee** the reliability and security of the state authentication service.
- **If necessary, we add** new secure authentication methods to the state authentication service (Smart-ID was added in October 2019).



THE SIGNING SERVICE:

letting you focus on your main activity

Signatures have existed for centuries. By signing a document, we agree with its content or confirm that we have taken note of it. A digital signature is a modern analogue of a standard signature. This enables us to do activities electronically which previously required paper and pencil.

A digital signature is considered by law to be equivalent to a handwritten signature and all Estonian authorities must accept digitally signed documents. This saves time, money, and nature. You do not need to go to an authority or a contract partner to sign the documents and you can make an infinite number of legally equivalent (backup) copies of a signed file. A copy of each paper document should be signed separately.

RIA provides to all those who perform public functions a central signing service so that they do not have to develop and manage it themselves and can focus on their core business.

WHAT IS IT?

The state signing service provides the service of creating signed envelopes. In addition to providing signatures, the service can be used to add a timestamp to the envelope, confirming that the signature has been given at that moment, and verify the validity of the signatures.

Otherwise, those who perform public functions would have to sign separate contracts for Mobile-ID signing, validity confirmation service, and timestamp service. With the service provided by RIA, however,

there is only one contract and one interface needed to provide all these options.

HOW DOES IT WORK?

The state signing service operates within other e-services. If you enter the state portal eesti.ee or any other e-service, you may use the signing service without even noticing it.

When you upload a document to an e-service and press the 'Sign' button, it creates a hash of the document, or a digital fingerprint, and asks for a PIN-protected signature from the ID-card or another eID carrier.

This information is sent to the signing service, which forms a digital envelope, or ASICE container, and sends it back to the e-service. The e-service then checks whether the file

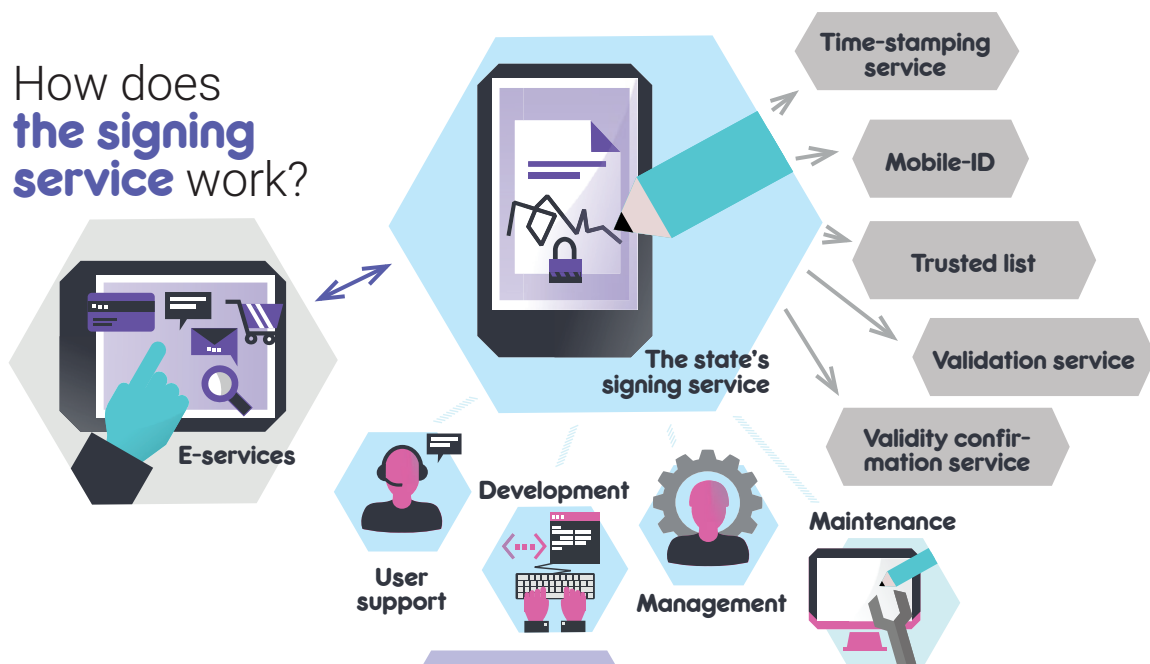
and signature you sent match the one received from the signing service and, if so, puts the document to be signed in the ASICE container. Then, it is checked whether the signatures are valid. When everything is fine, your computer screen will display you a message that the document has been signed.

In the background, there is a lot of things happening, but the whole process is completed before you can say 'Information System Authority'.

The signing service offered by RIA is free of charge for those who perform public functions. The underlying software is available to anyone interested at GitHub and allows anyone to provide a similar service. ●

**A digital signature
is considered
by law to be
equivalent to a
handwritten
signature.**

How does the signing service work?



What does RIA do?

- **We provide** a central signing service for all those who perform public functions via ID-card and mobile-ID.
- **We guarantee** the security, reliability, development, and support of the signing service.
- In addition to providing signatures and verifying their validity, we also provide a timestamping service through the signing service.
- **We keep** the technical components required for signing up to date.

RIA's CONSENT SERVICE

opens up the data economy

A state needs data to exist as a state. The state needs to know who its citizens are, where they live, how much they are paid, how many children they have, and whether they own a plot of land or a vehicle. This determines how much someone pays in taxes or how much benefits they receive from the state.

WHY IS THE CONSENT SERVICE NEEDED?

The state also has a lot of health data which is located in various national databases, but which is also of interest to others. For example, if a person agrees to share their health information with an insurance company, they may receive a more favourable life insurance policy.

We are also entering an era of personal medicine where our genetic data and medical history are used to determine the best treatment. To move the necessary data between different participants with the person's permission, the consent service is needed. It is important to know that the consent to what data is shared and with whom is given by the person themselves. In the same way, they can withdraw their consent at any time and stop sharing the information.

The creation of the consent service was motivated

by the healthcare sector, but it is also facilitated by the European Union's General Data Protection Regulation (GDPR), which extends people's control over their data.

AN IMPORTANT MILESTONE

In December 2019, we showed a prototype of the consent service to public and private partners and asked them for feedback. We were assured that the service is highly welcome – even outside the health sector. We will continue to develop the service with the knowl-

edge that it will become a universal solution that belongs to the state's IT infrastructure and is widely used.

In parallel with the developments, the Ministry of Social Affairs is assessing the impacts of sharing health data. The innovative approach to the sharing of personal data

also involves certain risks, which must be clearly described and, of course, mitigated.

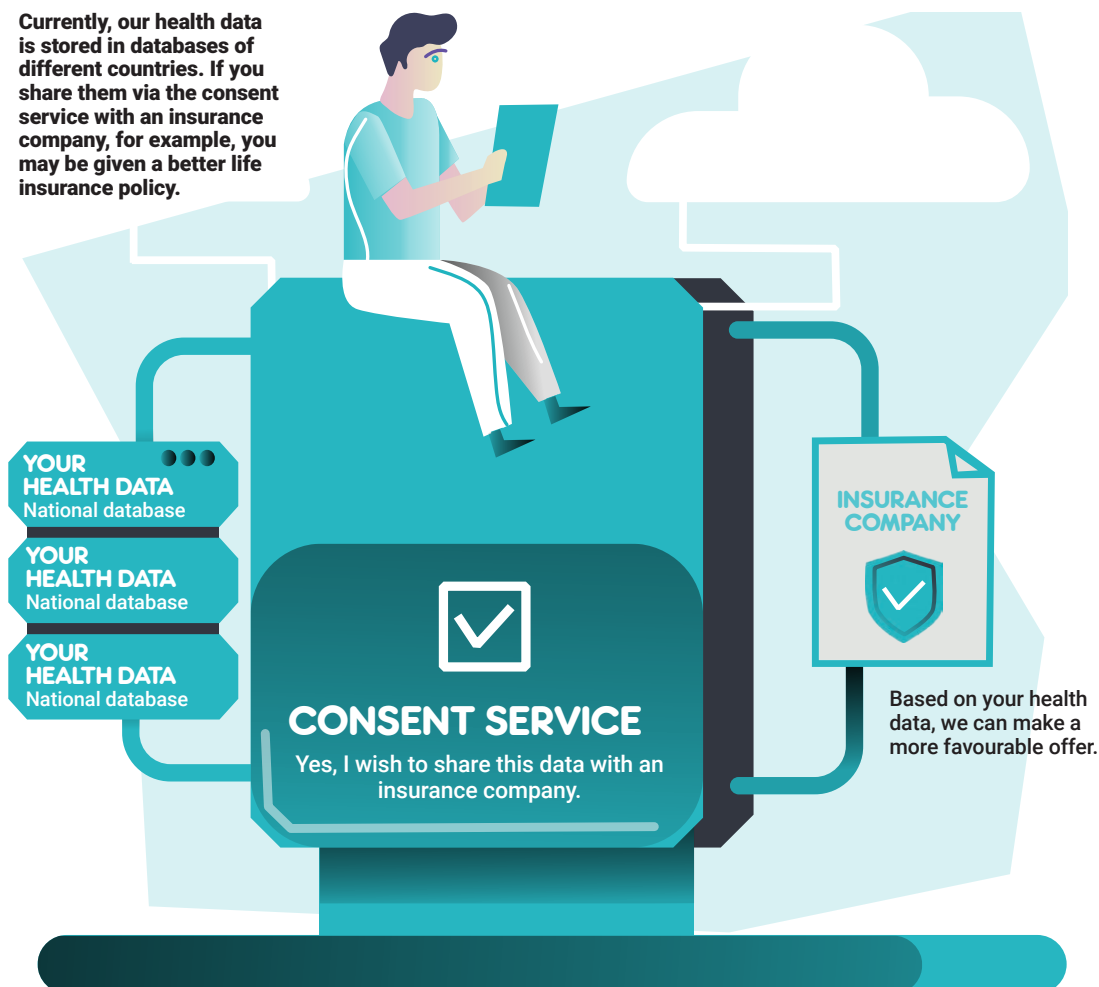
LET US START WITH HEALTHCARE

In addition to the Ministry of Social Affairs, the Information System Authority's partners in creating the consent service are the Health and Welfare Infor-

**We will continue
to develop the service
with the knowledge that it
will become a universal
solution that belongs to
the state's IT infrastructure
and is widely used.**

How does **the consent service** work?

Currently, our health data is stored in databases of different countries. If you share them via the consent service with an insurance company, for example, you may be given a better life insurance policy.



mation Systems Centre and the Health Insurance Fund, both of which manage large databases containing health data. The project also involves a number of private service providers, many of whom could also be future users of the consent service.

The consent service should be completed in the first quarter of 2021. A few months before that, selected users, service providers, and databases will be able to start testing the solution.

Once the impacts have been thoroughly analysed, the risks mitigated, and the difficulties overcome, the Estonian consent service will become unique in the world, because our e-state has very good preconditions for sharing data from the public to the private sector. This, in turn, creates fertile ground for new and unique services. ●

What does **RIA** do?

- **We are developing** a consent service that allows people to share information about themselves found in national databases with third parties.
- In December 2019, **we showed** a prototype of the consent service to public and private partners. The feedback was positive.
- **The consent service** will be completed in the first quarter of 2021.

RIHA:

the guide to the Estonian state information system

RIHA is the administration system for the state information system. It is like a guide, thanks to which we know what is happening in our state's information system and on what basis. Without RIHA, it would be very difficult to get an overview of what kinds of data institutions collect. In addition, RIHA helps to reuse existing data and services and thereby reduce duplication.

THE RENEWED RIHA HELPS TO DISCOVER THE E-STATE

In Estonia, data is stored in distributed form, i.e. there is no single central database. This method has many advantages, but it also presents challenges as data is scattered across the country. RIHA currently provides an overview of the information systems of the Estonian state, but the overall picture could be more up to date and of higher quality.

To achieve this, we want to introduce common protocols and standards in RIHA and automate the transfer of database metadata to RIHA. This would help us find out more precisely and easily from the 'guide' on what data and services the state has and how they can be reused.

However, this requires that all

database owners use agreed standards to describe the data collected, the services provided, and other components. This way, it will be possible to reuse data more efficiently in the future, reduce duplication, and thus cut the red tape. This reduces the need for the state to repeatedly ask people and organisations for the same information.

The potential and value of RIHA is obvious. If we know as precisely as possible what data, services, and reusable code lines exist in the state, both the public and the private sector can offer completely new services. The updated RIHA creates the preconditions for our e-state to make the next leap in development.

RIHA provides information on:

- which information systems constitute the state information system
- what kinds of data and in which information systems are collected and processed
- who are the owners, users, and contact persons of the information systems
- what legal bases are information systems maintained and data processed on
- what are the reusable components of information systems that ensure interoperability (XML assets, classifiers).

WHAT DOES RIA DO TO UPDATE RIHA?

The first RIHA was practically a notebook with information about the information systems of Estonia at the time, but now, it has developed into an administrative system that provides an overview of the information system of the Estonian state. Work with RIHA continues, and in the new version of RIHA, we will introduce a data description standard, the development of which is led by Statistics Estonia.

We are working more and more with customers to make RIHA more useful and meet their expectations with the help of their feedback. Analysis and prototyping of a distributed RIHA is also underway. ●

HEALTH BOARD:
document management
software Delta

**MINISTRY OF THE
INTERIOR:**
e-service environment of
the population register

**LÄÄNE COUNTY
HOSPITAL:**
X-tee subsystem

RESCUE BOARD:
OIS service interface
for the rescue
information system

GOVERNMENT OFFICE:
subsystem of the draft act
information system

RIHA

**CHANCELLERY
OF THE
RIIGIKOGU:**
VIS subsystem

**DEFENCE
FORCES:**
Defence Forces portal

**RIHA in
numbers**

RIHA has
more than
2,600
registered informa-
tion systems and
databases.

RIHA has
900
ACTIVE
INSTITUTIONS
AND
COMPANIES

5
COORDINATING
AUTHORITIES

In 2019,

24

coordination processes
of databases and
information systems
were initiated.

What does
RIA do?

- **We manage** the administration system for the state information system (RIHA).
- **We keep records** of the state information system.
- **We provide** an overview of the state information system (data, parties, requirements).
- **We concentrate** the requirements of the state information system and make it possible to assess compliance with them.
- **Through RIHA**, we ensure convenient communication between information system owners and evaluators.

CERT-EE:

the Estonian national cyber unit

Unless there is a major crisis, the offices of RIA are empty at night. But there is one room where the lights never go out and the computers are always turned on. That is RIA's Cybersecurity Incident Response Department, or CERT-EE, which monitors the Estonian cyberspace 24 hours a day and resolves cyber incidents in the middle of the night, if needed.

CERT-EE is the national contact point for Estonia for similar authorities in other countries when it comes to reporting incidents in the Estonian cyberspace. CERT-EE also sends notifications to cyber incident teams in other countries, but also to web hosts and other service providers if some phishing pages seen in Estonia are still operating.

WHAT IS A CYBER INCIDENT?

Pursuant to the Cybersecurity Act, a cyber incident is any event in the system compromising or having an adverse effect on the security of the system. The most common cyber incidents are phishing, disruption of service, malware distribution, and interception of user accounts. Cyber incidents also include ransomware attacks, financial fraud, and data leakage.

Some agencies and companies have a duty to report incidents to us (such as state authorities, critical service providers, or local governments), but the notices are also often submitted by companies and individuals who do it out of good will or to get help.

The number of cases registered is growing rapidly. In

2017, we recorded 10,649 cases and in 2018, 17,440 cases. In 2019, however, there were as many as 24,369 cases. This averages 67 notices per day and three notices per hour.

The more we are informed, the better our overview will be and the more effectively we can protect Estonia's cyberspace and warn our people of the threats.

HOW DOES IT WORK?

Most public sector bodies are connected to the state network. CERT-EE's role is to ensure that this network is clean, secure, and protected. To do this, we monitor the state network 24 hours a day to detect signs of malicious activity. If we find them, we will intervene.

However, our activities are not limited to the state network: we also monitor some of the vital service providers' networks. To this end, we have developed an automated network monitoring solution, Suricata4All (S4A). This system helps to detect attacks and malware, and in some cases, vulnerabilities and configuration issues.

The S4A consists of a central system managed by CERT-EE and sensors that network owners can install on their devices. The central system provides the sensors with rules to detect attacks. In accordance with the changed threats, we update these rules regularly. The sensors, in turn, send alerts to the central system when they detect malicious traffic. S4A allows its users to record, index, and analyse network traffic. ●

The number of cases registered is growing rapidly.

CERT-EE's services

File transfer environment:

paste.cert.ee

A tool to send suspicious files to CERT-EE for analysis. Suitable for larger logs, phishing e-mails and attachments, malware samples, etc.

CERT-EE's 'sandbox':

cuckoo.cert.ee

A file analysis tool for IT professionals. Allows the professionals to monitor, in a secure environment, how operating systems on different virtual and physical platforms behave when opening a suspicious file.

CERT-EE's warnings and notifications:

twitter.com/cert_ee

The fastest way to stay informed about CERT-EE's notifications and warnings.

Automated monitoring solution

Suricata4All (S4A)

A solution consisting of a central system and sensors which helps to detect attacks and malware, and in some cases, vulnerabilities and configuration issues.

Cyberspace newsletter

CERT-EE produces a daily cyberspace newsletter that summarises cyber and IT news from public sources. To subscribe to the newsletter, send an e-mail with the subject 'Subscribe' to certnews@cert.ee.

What does RIA do?

- **We monitor the information security situation in Estonia.** To do this, we use the reports we receive and collect information on cyber incidents ourselves.
- **We help prevent cyber incidents and reduce security risks,** in particular by raising security awareness and informing the public.
- **We assist authorities on cyber incidents** and advise them if they want law enforcement to investigate an incident.
- **We organise emergency response.** If necessary, we involve partners.

CERT-EE in numbers

Since 2015, CERT-EE has been monitoring the Estonian cyberspace

24 h
A DAY

In 2019, CERT-EE was notified of

24,369
CASES

in Estonian computer and data communication networks.

This averages

64 NOTICES PER DAY

3 NOTICES PER HOUR

The situation in cyberspace: **2019 WAS A YEAR OF PHISHING**

Based on the notices received by RIA's Incident Response Department CERT-EE, 2019 can be called the year of phishing. Although the highest recorded number of notices was related to infections with robotic networks, the number of infections known to us decreased, while the number of phishing sites and phishing attacks almost doubled.

BAD GUYS IN THE BANK

Until 2019, cybercriminals whose main crime is stealing money from banks had largely not attacked Estonians. This was probably due to the fact that the local banks use relatively secure authentication methods: ID-card, Mobile-ID, and Smart-ID.

In April, however, they found a way to create new Smart-ID accounts on behalf of their victims using phishing messages and sites. The criminals sent a message to the user's mobile phone on behalf of the bank which seemed to direct the user to the bank's login page. There, the victim was instructed to log in with their Mobile-ID. When they entered their username, personal identification code, and PIN1 on the phishing site, the criminals started creating a new Smart-ID account at the same time. Once they had created the account, the criminals logged in to the bank on behalf of the victim and transferred the money out.

**Proper management
of logs is essential if
the authority is to
understand what type
of information has
been stolen.**

STOLEN ACCOUNT DATA

In addition to phishing letters and sites created to steal money, phishing campaigns that stole account data also did a lot of damage. A simple e-mail that warns you that your mailbox is full or asks you to change your password can, at first glance, give criminals easy access to your personal messages and the ability to spread their phishing e-mails further. However, there is often a long-term plan behind such account data breaches – to look up the agency's business partners in the e-mails, to intervene in e-mail conversations, and to send an e-mail at the right time stating that the bank account for payment has changed.

Last year, we repeatedly saw phishing scams that could be prevented with multi-level authentication. Employees from local governments, at least three of Estonia's largest universities, hospitals, as well as smaller institutions such as a fuel company and a road maintenance company have fallen victim to such phishing.

Eliminating the consequences of incidents and determining the extent of information leaks is often complicated by the fact that information security teams (if there are any) or service providers do not have enough logs to determine which e-mail accounts were compromised and to what extent. Proper management of logs is essential if the authority is to understand what type of information has been stolen.



Analysing the trends in cyberspace

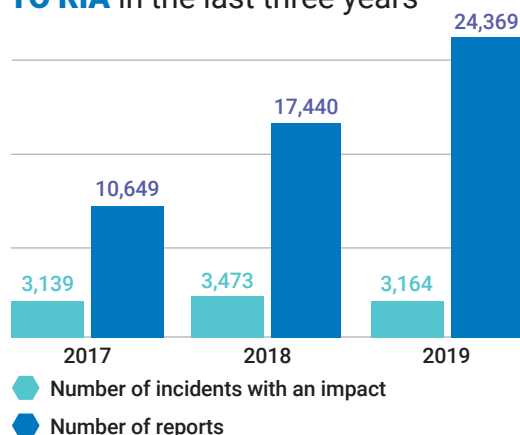
The Analysis and Prevention Department of RIA's Cyber Security Branch analyses the trends in Estonian cyberspace largely on the basis of incidents registered by CERT-EE. The department prepares weekly, monthly, and quarterly reviews based on the information received. RIA's analysts also delve into different individual cases or deal with some of the larger research issues facing RIA, if necessary. The department has also recently taken over curating national research and development of cybersecurity.

BEC SCHEMES ARE WAITING FOR NEW DATA

The biggest impact in 2018 was caused by financial fraud initiated through compromised e-mail accounts (business e-mail compromise or BEC schemes), which caused at least 600,000 euros in damage to Estonian companies. In 2019, we also paid attention to these incidents, but fortunately we learned about significantly less damage. As far as we know, the largest amount transferred to the wrong bank account due to fraud was 112,000 euros. That time, the company recovered the amount lost due to cooperation between banks.

It is important to note that BEC schemes can affect anyone and any Estonian company cooperating with a foreign partner may lose data (and then money) as a result of phishing account data. In most cases, the victims were importers of certain products (tools, tyre products, industrial equipment, medical equipment, etc.) and the amounts lost ranged from 1,000 euros to 70,000 euros.

NUMBER OF REPORTS SUBMITTED TO RIA in the last three years



- Number of incidents with an impact
- Number of reports

We consider incidents with an impact to be those that caused disruptions in the confidentiality, integrity, or availability of information or systems.

Reports are all notices of incidents with and without an impact, interruptions of services, notifications of spam, questions to CERT-EE, summary reports of partner institutions, etc.

However, we have also heard of several cases that were discovered by attentive accountants or managers and where no damage was suffered. We were also informed of situations where foreign business partners of Estonian companies suffered losses due to similar schemes. Therefore, it is important that Estonian companies that have managed to avoid the account data leakage incident also inform their foreign partners, who may become the next target of fraudsters.

SIGNIFICANT SERVICE INTERRUPTIONS

In 2019, we wrote in the Cybersecurity Yearbook: 'Maintaining cybersecurity in Estonia requires constant effort and vigilance from business and government leaders. Updates and security standards are important and it is also vital to invest time and money in updates and standards. To be able to avoid cyber incidents with a major impact in the future in Estonia, this work must be done.'

In 2019, we saw significant service interruptions that could have had a far-reaching impact on the people of Estonia: a software error left the Emergency Response Centre's phones silent for 20 minutes in September; due to the unnoticed breakage of the state network cables, the digital prescription and the state portal were inaccessible for hours in November; then, the digital prescription was again inaccessible in December due to the maintenance of aging systems. The transfer of Mobile-ID to new systems cut off this method of authentication and signing for 24 hours in May; the population register, the national authentication service, the new version of X-tee, etc. also failed.

The Estonian people are so used to digital services that it is necessary to invest in their availability, check the continuity of operations, test systems, improve procedures, and test again.

Service interruptions in 2019 were mostly caused by human error, administrative errors, or natural causes, but vulnerable systems can also fail due to malicious people and threats with public connections who do not care about our safety or health.

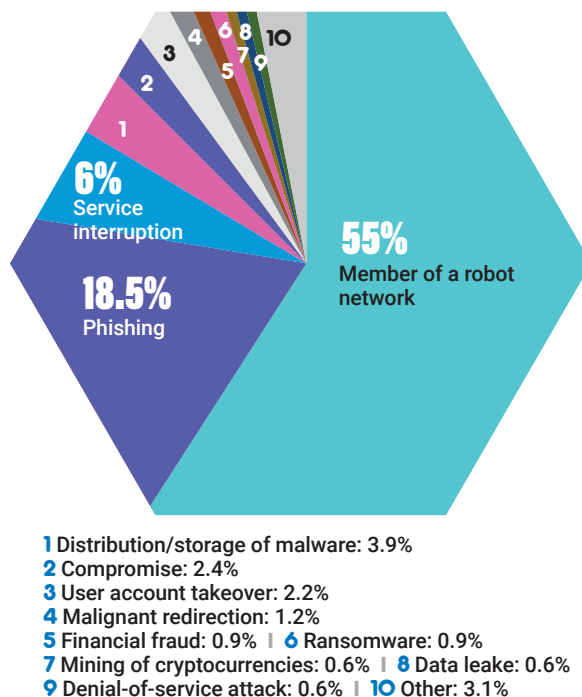
ROBOT NETWORKS – AGAIN

We have written about robot networks (botnets) in previous years as well. A large number of malware incidents reported last year, for example, was caused by the Avalanche robot network. It was shut down as a result of an international police operation in December 2016, but the malware does not automatically disappear from the devices and they must be cleaned separately to prevent the same infrastructure from being taken over again later.

The year of **phishing**

Incidents registered by CERT-EE. Infections with robot networks accounted for the largest share. Alongside them, however, the number of phishing incidents doubled compared to last year.

Percentage of incidents registered in 2019 by type



The other majority of infected devices have joined the Necurs botnet, which was used for years to carry out, among others, denial-of-service attacks, malware distribution (e.g. stealing bank data), sending spam, and so on. In March 2020, Microsoft announced that it had taken control of the network. Nevertheless, many devices in Estonia are still infected, even though they may no longer be as dangerous to others.

There are still a number of devices in Estonia that have joined another robot network, but whose control servers are not under the control of law enforcement agencies and about which we do not receive regular information. All so-called Internet of Things (IoT) devices, the software of which has not been updated or the default administrator password of which has not been changed, can become members of such networks and send out the same phishing or malware messages that caused so much trouble last year without the owner's knowledge. ●

Estonia will have a new INFORMATION SECURITY STANDARD

We all want the water we drink, the food we eat, and the buildings we live in to meet safety and quality standards. From the point of view of the functioning of the e-state, information systems and the data in them are equally important, and therefore, we must make sure that they are designed and protected in a way that ensures the reliability of the systems and the security of the data.

The information and network security of state authorities and local governments must be built in accordance with the established requirements. The RIA is responsible for verifying compliance with these requirements. In addition, we monitor vital service providers, i.e. energy companies, water companies, banks, telecom companies, etc.

WHAT IS ISKE?

Specific requirements and instructions are presented in the **IT Baseline Security System (ISKE)**. It sets out three levels of security: low (L), medium (M), and high (H). ISKE must be implemented by all state authorities and local governments, which are the data controllers of some databases.

RIA advises and assists implementers: we distribute instructional materials, organise trainings, and answer questions. We have created the ISKE portal (iske.ria.ee), where

all the necessary information is available. However, it must be remembered that RIA does not implement information security measures on behalf of other institutions.

At present, the state of implementation of ISKE in state authorities is generally good. Most of them have already been audited several times and there are no significant deficiencies. Local governments are not obliged to carry out audits. In 2019, the main focus of RIA's Standards and Supervision Department was on local governments.

What does RIA do?

- We **assist and advise** on the implementation of the three-level baseline security system ISKE.
- We **control the implementation of security measures** in the information systems of state and local government agencies, as well as essential and vital services, communication services, trust services, and digital service providers.
- We **update and supplement** the applicable requirements in accordance with the changed hazards and the environment

WHAT DOES THE FUTURE HOLD?

ISKE is currently the only acceptable set of requirements established on the basis of the Public Information Act under the so-called ISKE Regulation. The internationally recognised and widespread information security standard ISO 27001 will be added to it in the near future. Several institutions have expressed an interest in its implementation.

In parallel, the new Estonian information security standard is being developed. The new standard includes a more risk-based approach and will replace ISKE in the future. The new standard is not so voluminous, it is simpler and more flexible for the implementer, and takes into account the size, characteristics, and possibilities of different institutions. ●

PREVENTION CAMPAIGNS

to combat cyber threats

One of the most important tasks of the analysis and prevention department of the Cyber Security Branch of the RIA is prevention activities. The most prominent of these are public information campaigns aimed at raising awareness of cyber threats and providing solutions to deal with them.

Through advertising and PR activities, the messages of the campaign reached at least 80% of the target audience.

basic knowledge of cyber hygiene, the main target group of which was the population aged 55+. Our media partner Havas created the memorable message 'Ole IT-vaatlik' and organised TV, radio, outdoor, and online advertisements that stood out in the autumn of 2019 with their blue

and white contrast and retro design.

PROBLEMS OF THE ELDERLY

RIA has been organising information campaigns for years. For example, in 2016, the Nuti-Mati campaign with the Vaata Maailma foundation drew attention to the security of smart devices, and in 2013, we tried to reduce the number of users of the outdated Windows XP.

However, now is the time to review our information activities more systematically. Using the results of surveys from Statistics Estonia, Eurostat, and others, we tried to better define the target groups of information campaigns. The research clearly highlighted a group with poor cyber hygiene, but to whom little attention has been paid to when it comes to cybersecurity – the elderly.

For example, the Estonian Union for Child Welfare, the Police and Border Guard Board, and several ministries have paid quite a lot of attention to younger Internet users over the years. However, older people have had to learn and manage on their own in the changing cyberspace.

Therefore, in the second half of 2019, we organised an extensive information campaign about the

LIBRARIES CAN HELP

During the campaign, we also cooperated with the Estonian Librarians Association. At the information day in November, people from all over Estonia had the opportunity to go to their local library for advice on cybersecurity issues. More than one hundred libraries took part in the information day, one of the aims of which was to emphasise the message that the local library could be a place where people can get help with issues related to the security of their smart devices.

Through advertising and PR activities, the messages of the campaign reached at least 80 per cent of the target audience. The follow-up survey also showed that more than a quarter of the people who saw the ads in our campaign additionally researched cybersecurity or took at least one step to increase their own or their loved ones' safety/privacy online.

On the one hand, we wanted to use the campaign to emphasise to the elderly that cybersecurity is important, and on the other hand, we urged the public to help their older friends and relatives to behave more safely in cyberspace.

APPLES and TREES

48% of 15–24-year-olds use different passwords in different places

11% of people aged 55+ use different passwords in different places

Source: Eurobarometer 2017



LIBRARIES CAN HELP: at the information day in November, people had the opportunity to go to a local library for advice on cybersecurity issues.

What does RIA do?

- **We increase** the level of cyber hygiene in Estonia.
- **We carry out** information and prevention campaigns. Last year, we focused on the elderly; this year, our priority are entrepreneurs.
- **We offer** public sector employees and family physicians a cyber hygiene test and the learning environment DigiTest.

Ole IT-vaatlik :) 123456 ei ole hea parool_

Ole IT-vaatlik :) Tark ei torma petukirjale vastama

Ole IT-vaatlik :) Aita lähedasel küberruumis arukam olla_

Ole IT-vaatlik :) Ära topi oma PIN2 võõrastesse kohtadesse_

THE NEXT CAMPAIGN WILL BE FOR ENTREPRENEURS

In 2020, we will move forward with information activities first towards small and medium-sized enterprises. They are the ones most affected by service interruptions, ransom attacks, and financial fraud through compromised e-mail accounts. The more entrepreneurs know about potential cyber threats, the better they will be able to out-source IT services and protect their business from cyber risks.

At the same time, we will continue to measure cyber hygiene practices to better target future campaigns. After the 'IT-vaatlik' campaign in 2019, we asked the Estonian people what cybersecurity practices they follow, and in 2020, we will survey entrepreneurs.

All of this gives a better picture of how we can prevent high-impact cyber incidents in Estonia. ●

'IT-vaatlik' campaign in numbers

On 20 November 2019,

16

LIBRARIES

invited seniors to seek advice on cybersecurity.

The 'IT-vaatlik' video clip was shown

400,000

TIMES

on Facebook and YouTube.

The 'IT-vaatlik' banner was shown on Internet platforms

6 mln

TIMES

HOPE FOR THE BEST, prepare for the worst

Before Christmas 2015, 230,000 people in the Ivano-Frankivsk Oblast in western Ukraine were left without electricity. This time, the interruption was not caused by some of the usual suspects – it was the first known successful cyber attack against electrical systems.

In May 2017, the UK's National Health Service had to cancel 19,000 appointments with patients. The reason: due to ransomware called WannaCry, a number of hospital computers were hit.

WE ARE INCREASINGLY DEPENDENT ON IT

Our well-being, security, and vital services are increasingly dependent on information technology, which is why its reliability and protection are particularly important. As the events in Ukraine and the United Kingdom showed, an attack on IT systems can quickly and painfully affect the physical world.

The Critical Information Infrastructure Protection Department works at RIA to make it as difficult as possible to attack the information systems of Estonian vital and important service providers, to make sure we know how to behave in the event of an attack, and to minimise the effects of possible incidents.

WHAT IS WHAT?

Critical infrastructure is an asset, system, or a part of either of them that is essential for the functioning of vital societal functions. For example, for the functioning of health, safety, security, human economic, and social well-being.

Critical information infrastructure is made up of network and information systems whose operation, reliability, and security are essential for the operation of critical infrastructure. If such systems are damaged or destroyed, the country as a whole will be severely affected.

RIA organises the protection of critical information infrastructure, including the preparation of risk assessments of emergencies caused by cyber incidents, the development of necessary security measures, the organisation of security testing, and the provision of advice for vital and essential service providers in crisis prevention and resolution.

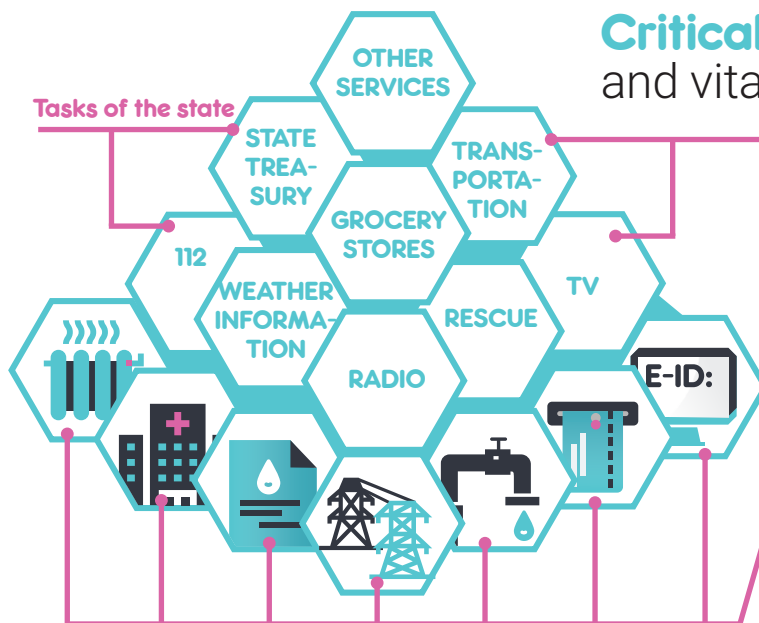
Emergency risk assessments of major cyber incidents are regularly prepared under RIA's leadership. It assesses the likelihood and consequences of an emergency and sets out the measures to prevent an emergency or, if that fails, to mitigate the consequences.

In 2020, our focus is on the energy and medical sectors. We will start with training for

family physicians, whose IT systems must meet the requirements established in the Cybersecurity Act from 2022. We will organise a training session for those responsible for cybersecurity in energy companies so that they can practice resolving a high-impact cyber incident.

**This time,
the interruption was
not caused by some of
the usual suspects –
it was the first known
successful cyber
attack against
electrical systems.**

IN **2019,** we organised or helped organise **10** exercises



Critical infrastructure and vital services

Services of general interest

Vital services that form the basis for other services

What does RIA do?

- We collect and manage information about critical information infrastructure.
- We prepare reviews of critical information infrastructure risks.
- We develop security measures, instructions, and sample materials.
- We advise vital service providers on crisis prevention and resolution.
- We organise local and international exercises.
- We raise awareness of cybersecurity.

A HARD DRILL MAKES AN EASY BATTLE

Organising exercises is one of our everyday tasks. Here are some examples:

In March last year, together with our Finnish colleagues, we practised how to solve a ransom attack on energy companies. In April, we coordinated Estonia's participation in the world's largest international cyber defence exercise Locked Shields. We helped prepare and participated in the NATO Crisis Management Exercise CMX2019 in May, which included cyber attacks. We participated in the organisation of NATO's Cyber Coalition 2019 cyber defence exercise in Tartu in December.

In addition, we organise the annual Kübertorm exercise during the Spring Storm exercise of the Defence Forces, in which we practice the cooperation of civil and military forces in resolving a cyber incident. In 2019, we played through incidents in the energy sector; in 2020, we will focus on the field of telecommunications.

There are
128
vital service providers in Estonia.

In addition, the pan-European cyber exercise Cyber Europe will take place in 2020. In Estonia, RIA is responsible for its organisation. While the previous Cyber Europe exercise in 2018 focused on cyber incidents in aviation, this time, the focus is on healthcare facilities.

The more complex the exercises, the easier it will be to manage a real crisis situation. Although we hope that we will never need to apply what we have learned from the exercises, we must be prepared for possible emergencies. In an emergency, we do not have time to learn. ●

AND **14** trainings were conducted.

40 information security awareness trainings are planned for

2020

and we will focus on **ENERGY** and **HEALTH**

INTERNATIONAL RELATIONS: 150 delegations in a year

In addition to collecting and sharing information within Estonia, RIA is also very active internationally. On the one hand, we are interested in cooperation with likeminded partner countries, and on the other hand, delegations from a number of countries are keen to visit RIA for inspiration and information on how e-Estonia works. The guests want to see first hand how to build a country where people never have to visit state institutions in person or wait in queues while there. This is not yet the case in most countries.

2019 WAS A RECORD YEAR

In 2019, a record number of 150 foreign delegations visited RIA. The most distant ones were Brunei, Cambodia, Aruba, Sri Lanka, Australia, Thailand, Rwanda, Eswatini, and others. Numbers-wise, Japan, Germany, and the United States had the highest number of guests.

The hosting of such a large number of guests also demonstrated RIA's multi-year commitment to support Estonia's successful campaign for the non-permanent seat in the UN Security Council 2020-2021. In parallel to expert-level delegations RIA is also frequently visited by prime ministers, ICT ministers, and deputy ministers as well as head of states from many countries. The guests' prime interest concerns the structure and daily management of the Estonian e-state. At RIA they gain an overview of the basic elements of the state information system as well as how to protect the e-state from cyber threats.

The majority of visitors come from government agencies of other countries. Many of them are in Estonia for the second or third time. The first time they came here, they visited the e-Estonia Briefing Centre, but on subsequent visits, they want to know more. For this reason, they come to RIA and meet

with companies that have participated in the construction of the digital environment as partners of the state.

We also host students and the private sector.

WHAT DO THE GUESTS WANT TO KNOW?

The guests are mainly interested in the Estonian solutions for secure data exchange. Most countries in the world seem to be looking for a solution that would allow secure data exchange between authorities (and the private sector). The Estonian X-tee has been in operation for 18 years and remains an inspiration to other countries in coming up with their solution.

Other popular topics include electronic identity and digital signatures, as well as cybersecurity, which is becoming more and more relevant.

WHICH PLACES DO WE VISIT?

In addition to hosting guests, experts of RIA often go abroad. We negotiate, we present, and we learn.

RIA annually conducts five-to-six bilateral meetings with key partner countries to discuss issues of mutual interest. At such meetings, we clarify and, if possible, reconcile our positions on issues that are the subject of working groups in the European Union. RIA also works closely together with the European Union Agency for Cybersecurity (ENISA).

International destinations where RIA's experts presented in 2019 included Australia (on several occasions), Singapore, the Americas, Middle Eastern countries, and several European countries. It provides an opportunity to introduce Estonia and helps to facilitate cooperation with the regions and the private sector. In developing and defending the Estonian e-state, it is necessary to be aware of new solutions, and the widest possible network of contacts will be useful in doing so. ●

**The first time they
came here, they
visited the e-Estonia
Briefing Centre,
but on subsequent
visits, they want to
know more.**



VISITORS FROM FAR-OFF LANDS:

In September 2019, RIA was visited by Dr Rauda Al-Saadi, Head of Abu Dhabi's Digital Authority, who was welcomed by Piret Urb, Head of International Relations of RIA.

Employees of RIA
gave presentations almost

25 TIMES

in Australia (on several occasions), Singapore, America, Arab countries, and many parts of Europe.

In 2019,

150

foreign delegations
visited RIA

96

in 2018.

What does **RIA** do?

- In our foreign relations, **we shape the reputation** of the Estonian digital state.
- **We gain new knowledge** and contacts that could be useful in developing and defending our e-state.
- **We hold bilateral meetings** with key partner countries.



JAPAN, GERMANY, and the **US** had the highest number of guests. The guests are most interested in data exchange, electronic identity, and cybersecurity.

The most exotic and distant ones were **Brunei, Cambodia, Aruba, Sri Lanka, the Caribbean, Australia, Thailand, Rwanda, and Eswatini.**

INTERNATIONAL PROJECTS of RIA

International projects are very important for RIA, as they help maintain Estonia's positive image and raise the cybersecurity capacity worldwide. They also provide a good opportunity for our staff to put their training skills to the test, establish work-related contacts across the globe, and share their best knowledge and experience with other countries.

RIA is currently conducting three international projects: EU CyberNet, Cyber4Dev, and Interreg Europe CYBER

WHAT IS EU CYBERNET?

EU CyberNet is a new cyber capacity building initiative of the European Union. As the greatest provider of development cooperation in the world, the European Union (EU) has set the objective of providing more support to third countries in the fields of digitisation and cyber resilience as well as developing the cooperation between cyber experts of Member States and their professional skills.

The objective of the project is to set up a EU-wide network of cybersecurity experts that the Member

States and the EU institutions can use to implement projects related to cybersecurity in third countries.

Why is the success of such projects important for the EU? Because figuratively, European cybersecurity starts with the awareness of all Europeans and our ability to cooperate with cybersecurity experts outside of Europe.

In order to set up the network, the European Commission published an international call for tenders in the spring of 2019. The winner was the tender by RIA, supported by an international consortium (Estonia, Germany, Luxembourg, and Finland). The EU CyberNet team is hosted by RIA and would in perspective coordinate the different all EU cybersecurity projects in third countries and mediate experts for them.

The EU CyberNet project is also remarkable for RIA and Estonia in general because we are managing its implementation. As the contractual partner of the European Commission's Directorate-General for International Cooperation and Development (DG DEVCO), RIA is responsible for implementing the project involving the entire European cybersecurity community.

The expectations of the EU institutions and Member States are high, as the area requires improved coordination and a more harmonised approach than before. Making it work will be a great challenge, which we are sure to rise to.



By the end of the project, the network must include more than 500 experts and 150 partner institutions, from national cyber centres to universities and think tanks. We have developed a communication strategy and a website centralising the experts is being created. The first trainings of the EU CyberNet have taken place and one expert has already been dispatched on a mission.

DURATION OF THE PROJECT: 1 September 2019 – 31 August 2023

TOTAL BUDGET OF THE PROJECT: 4 million euros

WHAT IS CYBER4DEV?

The European Union project Cyber Resilience for Development, or Cyber4Dev, is aimed at developing cyber skills and knowledge in third countries to support economic and social development. The project is led by a multinational consortium consisting of Estonia, the Netherlands, and the United Kingdom. Estonian experts are key contributors to the project, sharing Estonia's unique knowledge and experiences. Cyber4Dev supports improving cyber resilience in African, Asian, Latin American, and the Caribbean



In 2019, the Cyber4Dev project hosted 48 events with a total of 28 Cyber4Dev experts and over 400 trainees in the target countries. In addition, the participation of experts from 25 target countries in international professional forums in Europe was supported.

DURATION OF THE PROJECT: 1 January 2018–30 June 2021

TOTAL BUDGET OF THE PROJECT: 11 million euros

WEBSITE OF THE PROJECT: cyber4dev.eu

countries through a wide range of training programmes. The project assists participants in the design and implementation of cybersecurity strategies, enhances the capability of Computer Emergency Response Teams (CERTs), and supports regional and international cooperation.

In 2019, Cyber4Dev organised training sessions and study visits in the target countries for different groups, from politicians to technicians. The project has supported the creation of a CERT in Botswana and the development of Sri Lanka's CERT's incident management capacity, assisted Rwanda in drafting its first national cyber strategy, advised Sri Lankan cybersecurity law makers and eID developers, organised training sessions for CERTs of several African countries on incident management, and organised the first national cybersecurity exercise in Mauritius.

Last year, the geographical scope of the project was expanded to include Latin America and the Caribbean in addition to African and Asian countries. RIA has many years of experience working with this region thanks to the Organisation of American States (OAS), which has often involved Estonian experts in its training. Estonia's experience in building a secure digital state is well-known and valued around the world.

WHAT IS INTERREG EUROPE CYBER?

Interreg Europe CYBER is a project funded by the European Regional Development Fund (ERDF), aimed at supporting the competitiveness of small and medium-sized enterprises in the field of cybersecurity. Seven countries are participating in the project: France (leading partner), Estonia, Italy, Spain, Belgium, Slovakia, and Slovenia.

In Estonia, this project is developing entrepreneurship and innovation in the field of cybersecurity. This involves developing policy instruments, national coop-

Liina Areng

**Cyber4Dev
project manager**



At Cyber4Dev, I most enjoy the commitment of the participants of our training sessions. They are full of willingness to learn, ask questions, and take on new challenges. We mainly share Estonian knowledge and EU experiences during the project, and I believe that we will learn a lot as well. The target countries of our project are undergoing an ultra-fast digital transition. Developing countries are making advancements in a number of areas, using innovative digital platforms, experimenting with financial and mobile technologies, using offline renewable energy solutions, and supporting the emergence of domestic businesses. Cyber4Dev aims to raise awareness both in the society and among policymakers who are eager to reap the benefits of the 'digital revolution'. We help them understand the importance of investing in the security of digital solutions so that they can withstand potential cyber attacks and that the country can respond to cyber incidents in a coordinated manner and recover quickly.

eration, and organising international consultations with project partners. Estonian companies will have the opportunity to build relationships with partner countries and their companies, and RIA will have a better understanding of how to support innovation. The aim of the project is to look at the Estonian cybersecurity ecosystem, define the existing partners, and detect and systematically address the ecosystem's concerns.

The project will result in analyses for the international expansion and co-operation of small and medium-sized enterprises, as well as consultations on the same subject. ●



DURATION OF THE PROJECT: 1 June 2018–31 May 2023

TOTAL BUDGET OF THE PROJECT: 1,864,242 euros

WEBSITE OF THE PROJECT: www.interregeurope.eu/cyber

RIA: NUMBERS & PEOPLE

RIA designs and fortifies the pillars of the Estonian information society: we develop and manage infrastructure services centred around the e-state and ensure the cybersecurity of the country. Together, we create and defend the world's best digital society.

We have agreed on common values that we consider important and follow in our work and decisions:

- **responsibility:** we build the best digital state, which creates new opportunities for the people and the society, we acknowledge our role in the organisation, and we know how we influence the end result with our contribution;
- **learning and sharing:** in a constantly evolving digital society, we must be able to develop and be open, both as an organisation and as employees;
- **cooperation:** to achieve results, we need unity, mutual understanding and support, and commitment to a common goal.

RIA in numbers

61%

of the employees of RIA are **MEN...**

The ages of the employees of RIA fall within the range of

18–68
YEARS

...and

39%
WOMEN

72%
of them have higher education

In 2019, the employees of RIA completed a total of

6,426 HOURS OF TRAINING

The average employee of RIA is a **37-YEAR-OLD MAN** who has worked at RIA for **3.6 YEARS.**

In 2019, the average number of RIA employees was

141

Total staff turnover was

22%

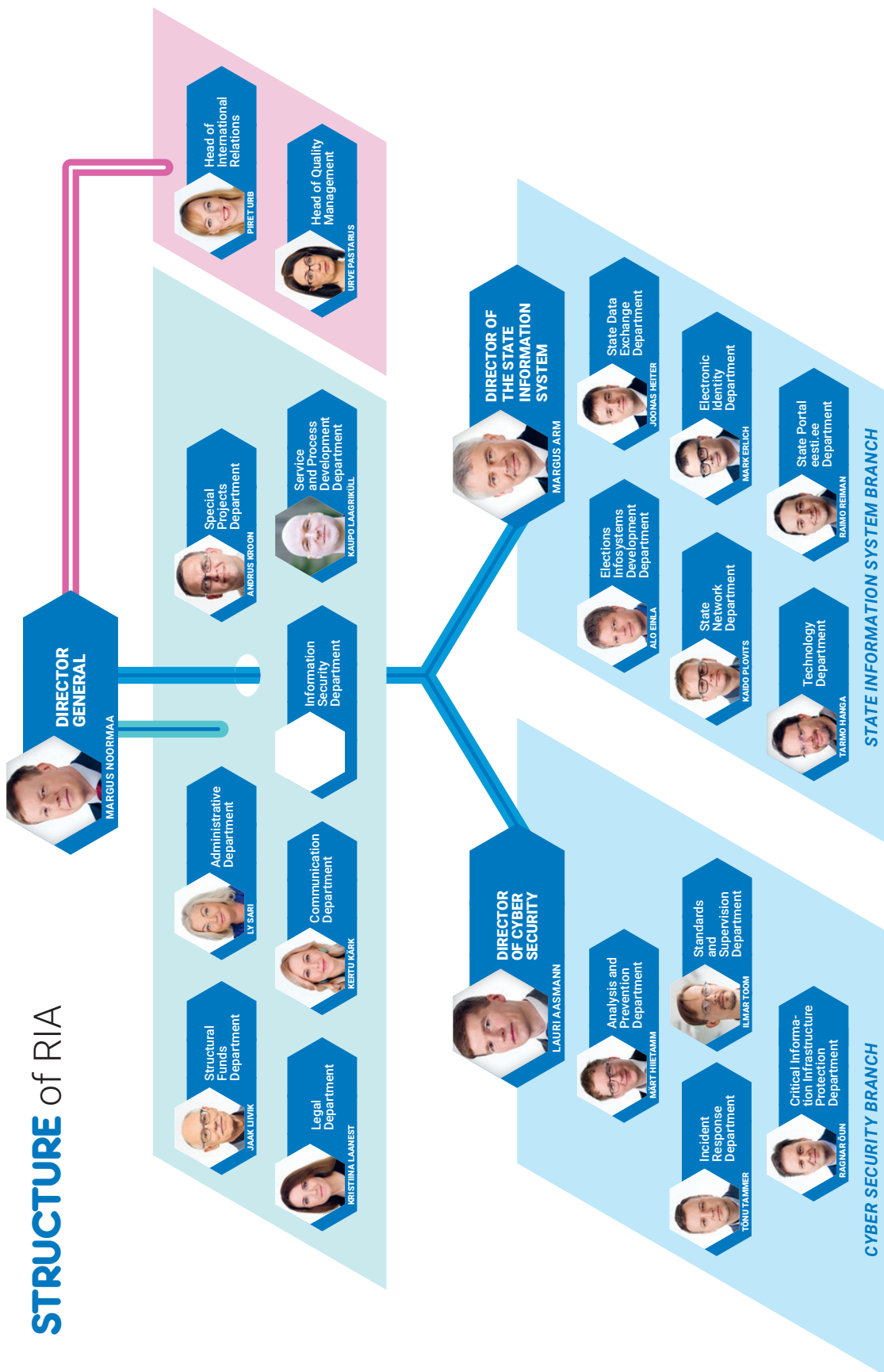
As at 16 March 2020, the average gross salary of RIA was **2,539 euros.**

In 2019, RIA made investments for

4.1 million euros

The management expenses of RIA amounted to **5.2 million euros.**

STRUCTURE of RIA



The employees of RIA about RIA

TARMO HANGA

Head of the Technology Department

Has worked at RIA for more than ten years

At RIA, I have learned the art of compromises and maintaining a healthy attitude. People working in the IT industry have fairly stressful jobs, so I have learned how to deal with stress so that my job could still be fun. You should be able to come to work happily and enthusiastically, not reluctantly. Is it still interesting to work at RIA after ten years? For me, a position is worthwhile if it does not get boring and is challenging enough. You must feel that you have done something important for Estonia and the IT world. RIA can offer me all of that.



MARGUS ARM

Director of the State Information System

Has worked at RIA for three and half years

I joined RIA in September 2016 from the private sector to work as the head of the electronic identity (eID) field. Based on my time at RIA so far, I can say that it is very nice here. However, with all due respect to my previous employers, I dare say that none of my previous jobs have been so exciting, interesting, and busy. We have new and exciting tasks here every day that affect the operation of almost the entire e-Estonia. The daily contact with very pleasant, willing, and responsible co-workers from RIA and other institutions gives us motivation and strength to strive every day to make things better for everyone in Estonia so that we could continue to be the leading e-state.



SEIKO KUIK

Press officer

Has worked at RIA for one year

The work at RIA is interesting and we have interesting people. Before, I was not even aware of the crucial importance of RIA in maintaining and developing the digital state. I have the opportunity here to contribute to taking e-governance to a whole new level. All employees contribute to this.



ANNIKA KLUGE

Project manager at the Electronic Identity Department

Has worked at RIA for four years

I appreciate that at RIA, I can choose the location and time of work myself – within reasonable limits, of course, so that meetings could still be held! I feel that I am trusted and that I am able to have a say in making decisions. People are cooperative and nice, and the work is diverse. I feel useful here.



KÄTLIN PIRK

Office management chief specialist

Has worked at RIA for two years

I have never felt bored during my time at RIA. Every day brings different tasks and challenges, new acquaintances, and knowledge. RIA has given me a great deal of experience. I have gained the confidence and courage here to work on things that are new to me. With the support of co-workers and managers, I can constantly develop personally and make my own small contribution to creating an even better e-state.



LIINA ARENG

Cyber4Dev project manager

Has worked at RIA for more than five years

In my opinion, RIA is the most wonderful institution in Estonia to work in. The different units of RIA cooperate a lot with each other and have a common goal. I like that RIA always finds ways to support the implementation of all ideas, rather than looking for bureaucratic justifications to prevent it from happening.



Together, we create and protect the best digital society in the world. If you want to join RIA, send your description and CV to personal@ria.ee.



Read more at www.ria.ee/en