Estonian eID Infrastructure

ITAPA 2009 International Congress
November 3, 2009
Bratislava

Uuno Vallner, PhD
Head of eGovernment Division
Ministry of Economic Affairs and Communications, Estonia

Background

- 82 % householders have Internet connections (typically broadband)
- 52% of population - heavy users
- 100 % of public employees have computerized workplace with Internet connection
- All public sector institutions have web pages
- High level of Internet-banking (98% of transactions done by Internet)
- All citizens have ID-cards (smart cards)
- 88% tax declarations were filled and handled online
- Estonia - only binding Internet voting country
- (whole population – 1,356 mil.)

ID card: most important element of eID infrastructure

EESTI VABARIIK

MÄNNIK

MARI-LIIS

N/F

EST

20.02.1973

47302200234

A3051479

04.10.2011

- ID card is mandatory for Estonian citizens from age 15 and up and all aliens residing permanently
- ID card has three main functions: visual identification, authentication and digital signing.
- The card contains a chip holding personal data and two certificates: one for authentication purpose, and one for qualified digital signatures
- Validity period: five years

Deployment of ID card

- Deployment has commenced in January 2001
- The roll-out completed around October 2006
- Cards are issued by the Citizenship and Migration Board in cooperation with private sector
- The price of the card is for applicants approximately 10 EUR

- More information: http://www.pass.ee/2.html and http://id.ee

Content of ID card

- Physical card according to the ICAO specifications: signature, photo, name, PIC, birth time, sex, citizenship, card number, end of validity.
- On the chip same data except photo and signature, certificates for authentication and for qualified electronic signature, associated private keys protected with PIN codes
- The certificates contain only the holders name and PIC. Authentication certificate contains the holder's unique e-mail address.

Policy

- ID card contains minimal data for authentication. All other data can ask from registries.
- Authentication certificate should not be used for signature purposes
- Certificates are activated upon handover of the card- Before this process the ID card and certificates are not valid. Receiver may also opt to suspend the certificates.

Mobile-ID

- Mobile-ID was introduced in May 2007 by the largest mobile operator EMT with Certification Authority. Other main operators are preparing.
- Mobil-ID user needs to replace a SIM-card with the PKI-capable one.
- The user needs to “activate” his/her Mobile-ID with ID-card in the web. Functions, security and quality are on the same level as ID card.
- Advances: no need for smartcard reader, no need special software
- Active users about 20000.

Bank eID

- The quite popular method for authentication today is Internet bank authentication. 5 major banks (covering 99% of the banking customers) are providing authentication services to third parties.
- Most Government services for citizens are accessible in addition through bank authentication.
- Reasons behind popularity of bank authentication: early start of Internet banking in Estonia (1996); large number of Internet bank users (near 100%); simple use (no special hardware or software is needed)

eID related legislation (1)

- **Identity Documents Act (2000)**
  - ✓establish the national ID card as the primary personal identification document
  - ✓passport is voluntary
- Digital Signatures Act (2000)
  - ✓states that digital signature is equal to the handwritten one
  - ✓imposes an obligation on public sector institutions to accept digitally signed documents
  - ✓regulates the activities of Certification and Time-Stamping Service providers

eID related legislation (2)

- **Personal Data Protection Act** (1996)
  - ✓protects individuals fundamental rights and freedoms
  - ✓states that all citizens have a right to see the data that the public sector maintains about me
- **Public Information Act (2001)**
  - ✓ensures the opportunity for all to access information intended for public use
  - ✓imposes an obligation for public authorities to maintain a website and a document register
  - ✓states that everybody must have free access to the Internet at public libraries
  - ✓Sets out rules for the creation and maintenance of public sector registers

eID related legislation (3)

- The Population register act
  - ✓Generates and maintains the PIC
  - ✓Contains personal data, data related to the personal data (data of all identity documents and vital events certificates
- The government regulation of X-Road
  - ✓ citizen/resident shall be authenticated with ID-card, Mobile-ID or Internet bank
  - ✓Civil servant shall be authenticated with the ID card or via the information system of the authority
  - ✓Information system shall be authenticated on the basis of the certificate of the security server of X-Road

eID related legislation (4)

- The decree concerning database of identity documents
  - ✓Database contains the information on all issued identity documents issued by Estonian Citizenship and Migration Board
  - ✓Database contains all information that are necessary for the issuance identity documents to the eligible persons
  - ✓Contains also data of all valid and non-valid documents
- **Election act (2002)**
  - ✓Decision of Internet voting

Organisational interoperability (1)

- Ministry of Economic Affairs and Communication is responsible for general ICT coordination. More precisely the Department of State Information System.
- The Estonian Informatics Centre (subdivision of ministry) is responsible for implementation common infrastructure: X-Road, Citizen portal, eID infrastructure services, …
- The Estonian commercial Banks (Swedbank, SEB, Sampo Pank, Krediidipank, Norde) play important role: authentication, charges for services

Organisational interoperability (2)

- Citizenship and Migration Board (CMB) is responsible for the issuing of PKI enabled ID-cards and management of related matters
- The issuance process of ID cards and development of PKI infrastructure is managed through a tight cooperation with public and private agencies.
  - ✓ TRÜB AG – the production and personalization
  - ✓Subcontractors: SK and Trüb Baltic AS
  - ✓SK as sertification service provider is acting since 2001. SK has become de facto coordinator and excellence centre on PKI matters and eIDM systems in Estonia
  - ✓Mobile operator EMT (mobile-ID)

Organisational interoperability (3)

- Inter-institutional eID working group under the Ministry of Economic Affairs and Communication. Aims of group:
  - ✓to ensure coordinated development of applications related to eID and digidal signing as well as of solutions connected to PKI
  - ✓to solve respective technical, legal and organizational issues as well as making relevant propposals.
  - ✓ to bring together interested parties from various governmental agencies and from private sector (banks, telecom)
  - ✓ to draft legislation
  - ✓to discuss national PKI matters

Organisational interoperability (4)

- “Computer Protection 2009” – agreement signed between major banks, major telecom companies and the Government in May 2006. Objectives of the initiative include:
  - ✓promotion of ID-card
  - ✓increasing availability (and affordability)of smartcard readers
  - ✓introduction of alternative PKI-based authentication systems like Mobile-ID and alternative eID Cards
  - ✓10-fold increase of user base of PKI-based authentication systems in 3 years (from 40 000 to 400 000 by the end of 2009)

Interoperability with other countries

- Company Registration Portal accepts users with Portuguese, Belgian and Finnish ID-card and Lithuanian Mobile-ID
- It is expected that during this year a project will be launched which would result in generalized system for accepting foreign qualified certificates both for authentication and for digital signing.
- DigiDoc, the common digital signature solution used in Estonia supports wide variety of PKI-based smartcards :Austrian, Belgium and Finnish ID-cards has been successfully demonstrated.

eHealth and eID

- The core system – Health Information System – is still under development but is expected to be the major e-service with support of ID-card authentication. As an exception the Health Information System does not support Bank ID authentication option because of the higher security level demands.

eJustice

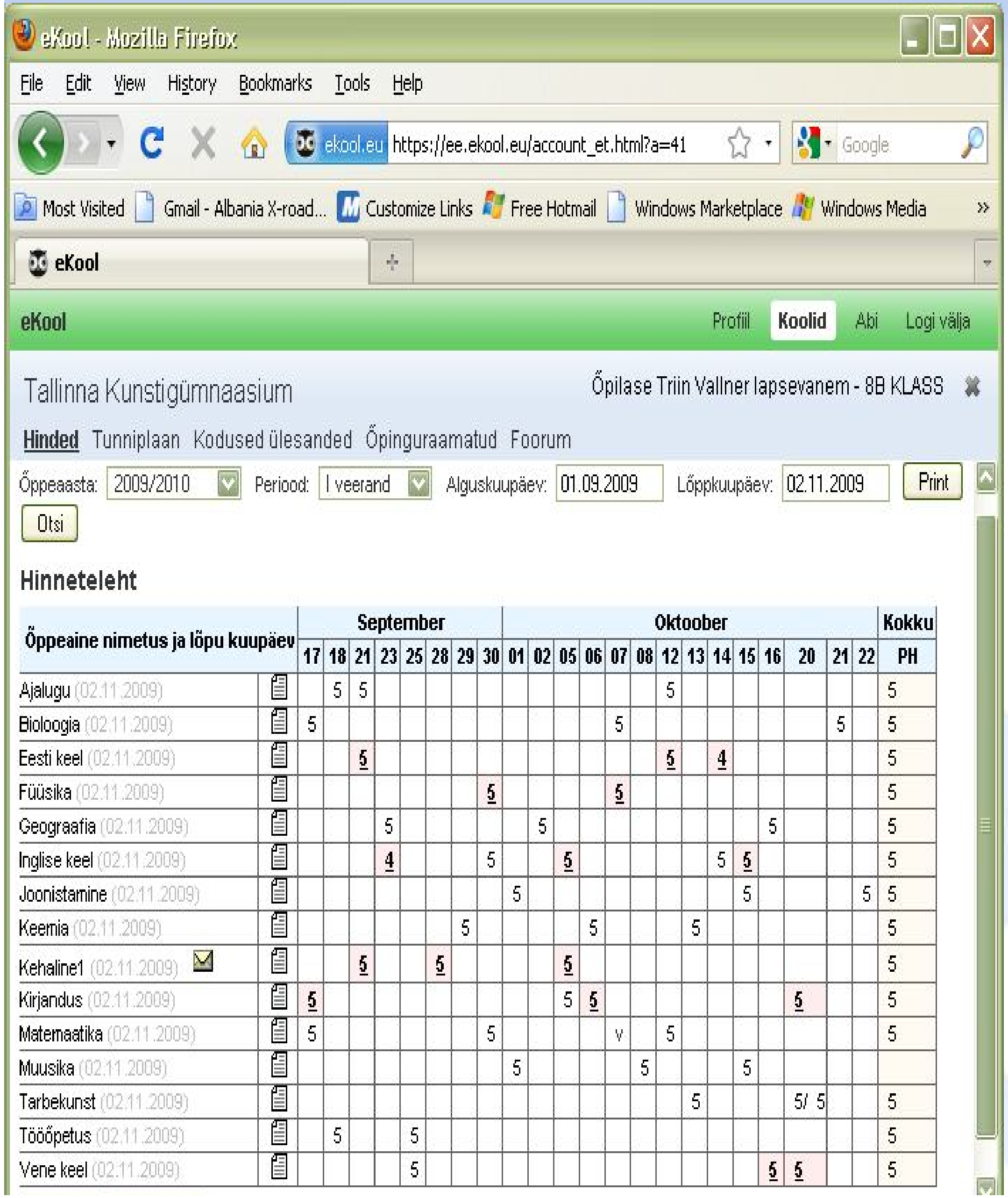
- Company Registration Portal (https://ettevotjaportaal.rik.ee/);
- Land register information system
- eNotary
- Court case system

Internet voting

- ID-card is considered as an enabler of Internet voting which was introduced in 2005. Internet voting in Estonia is an official method of voting and produces binding results.
- Internet Voters among total voters:

✓Local Elections 2005	1,85%
✓Parliamentary Elections 2007	5,4%
✓European Parliament Elections 2009	14,7%
✓Local Elections 2009	15,75%

E-school



Tallinna Kunstigümnaasium

Õpilase Triin Vallner lapsevanem - 8B KLASS

Õppeaasta: 2009/2010 Periood: I veerand Alguskuupäev: 01.09.2009 Lõppkuupäev: 02.11.2009

Hinneteleht

Õppeaine nimetus ja lõpu kuupäev	September								Oktoober														Kokku
	17	18	21	23	25	28	29	30	01	02	05	06	07	08	12	13	14	15	16	20	21	22	PH
Ajalugu (02.11.2009)		5	5												5								5
Bioloogia (02.11.2009)	5												5								5		5
Eesti keel (02.11.2009)			5												5		4						5
Füüsika (02.11.2009)								5					5										5
Geograafia (02.11.2009)				5						5									5				5
Inglise keel (02.11.2009)				4				5			5						5	5					5
Joonistamine (02.11.2009)									5									5				5	5
Keemia (02.11.2009)							5					5				5							5
Kehaline1 (02.11.2009)			5			5					5												5
Kirjandus (02.11.2009)	5										5	5								5			5
Matemaatika (02.11.2009)	5							5					v		5								5
Muusika (02.11.2009)									5					5				5					
Tarbekunst (02.11.2009)																5				5/ 5			5
Tööõpetus (02.11.2009)		5			5																		5
Vene keel (02.11.2009)					5														5	5			5

One of the most popular e-services accessible with ID-card is e-school. E-school is an easy-to-use student information system, connecting parents, students, teachers and school administrators over the Internet, making school information accessible from home and decreasing the work routine of teachers and school management.

Internet banking, telecom, ..

- Internet banking is the most popular e-service in the private sector, although logging in with an ID card is not the most popular option.
- In the financial sector, the Estonian Central Securities Register and Pension Register also make use of ID-card authentication.
- Telecom companies and utility companies (water, gas and electricity) make use of the ID-card authentication in their self-service environments.
- List of sites accepting ID-card authentication can be found in http://id.ee/?id=11457.

ID-card applications making use of the personal data file

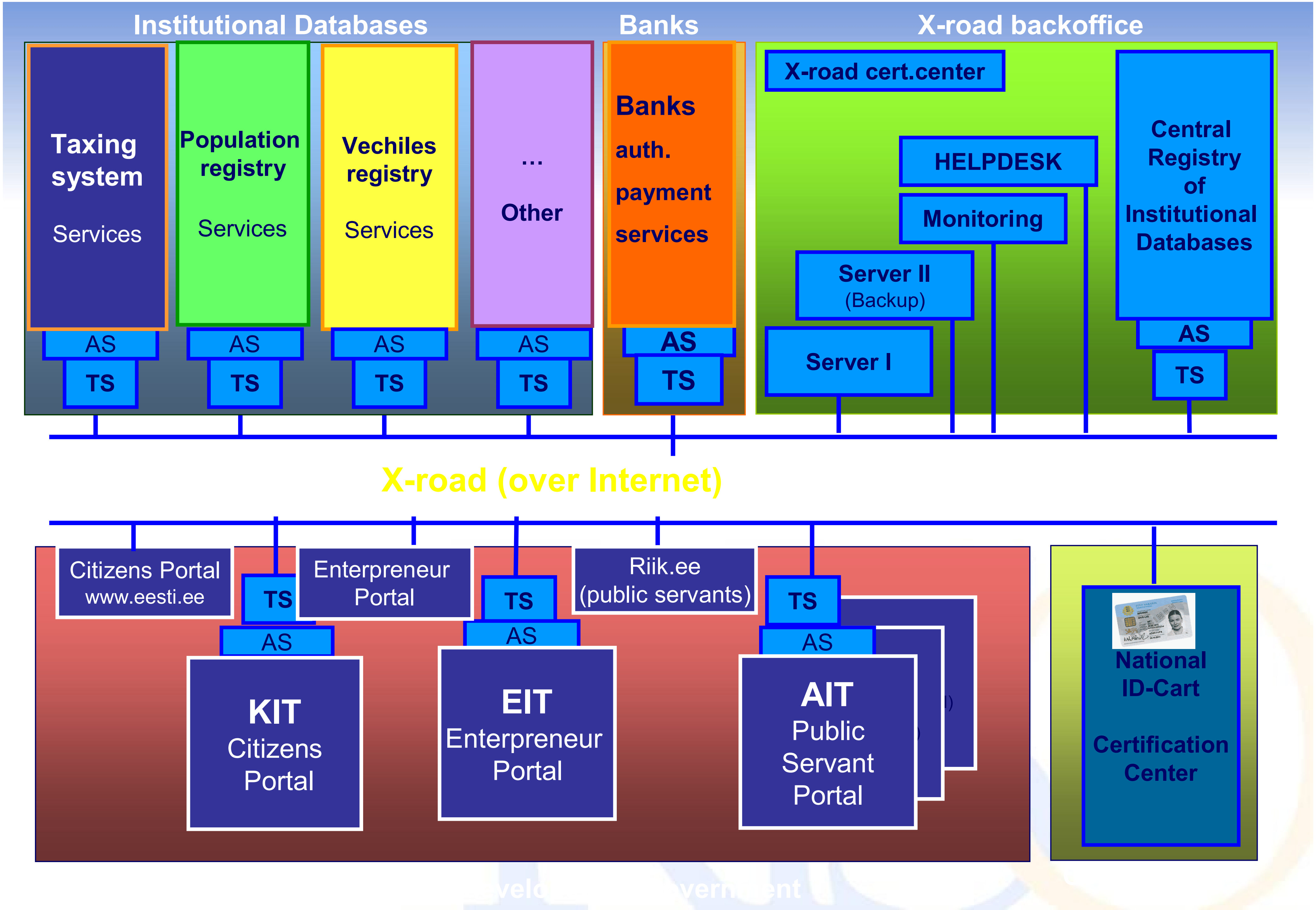
- The Estonian ID-card contains a data file in its electronic part which is unprotected. This allows for quick retrieval of personal data by application when the card is inserted into the reader. A number of applications take advantage of this, including:
  - ✓ID-card as a loyalty card
  - ✓ID-card as an entrance card to libraries, sport clubs etc.
  - ✓Quick registration to an event or for entering premises

ID-ticketing

- Over 120 000 active users are carrying just the ID-card every day to prove their entitlement to travel in public transportation in Tartu, Tallinn and surroundings (Harjumaa county). Period tickets – for 1-2 hours, or for 1, 3, 10, 30 or 90 days – can be obtained using the internet, mobile or landline phone, or paying cash in more than 80 sales points. Checking officers are carrying GPRS-enabled handheld terminals for quick and automatic entitlement checking.

Trust environment - X-road (2001)

- X-Road allows information systems to use the common data exchange environment as well as the common set of interfaces and **common authentication and authorisation system**.
- Joining an information system with X-Road saves money and considerably increases the efficiency of data exchange among state agencies and in communications between the local residents and the state.
- 6 million transactions per month, 300 service providers (all registers), 2000 services



Institutional Databases

Taxing system Services

Population registry Services

Vechiles registry Services

… Other

Banks

Banks auth. payment services

X-road backoffice

X-road cert.center

HELPDESK

Monitoring

Server II (Backup)

Server I

Central Registry of Institutional Databases

AS

TS

X-road (over Internet)

Citizens Portal www.eesti.ee

Enterpreneur Portal

Riik.ee (public servants)

KIT Citizens Portal

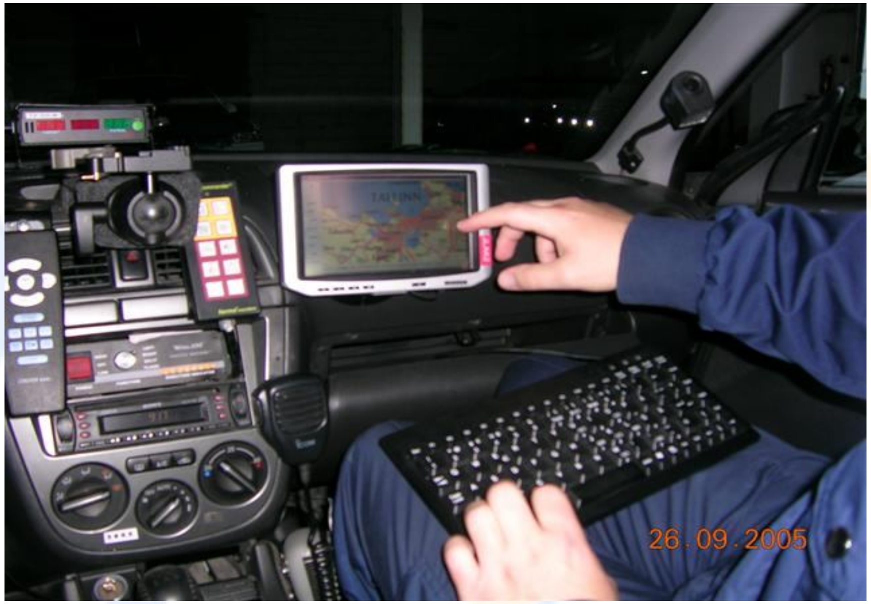
EIT Enterpreneur Portal

AIT Public Servant Portal

National ID-Cart Certification Center

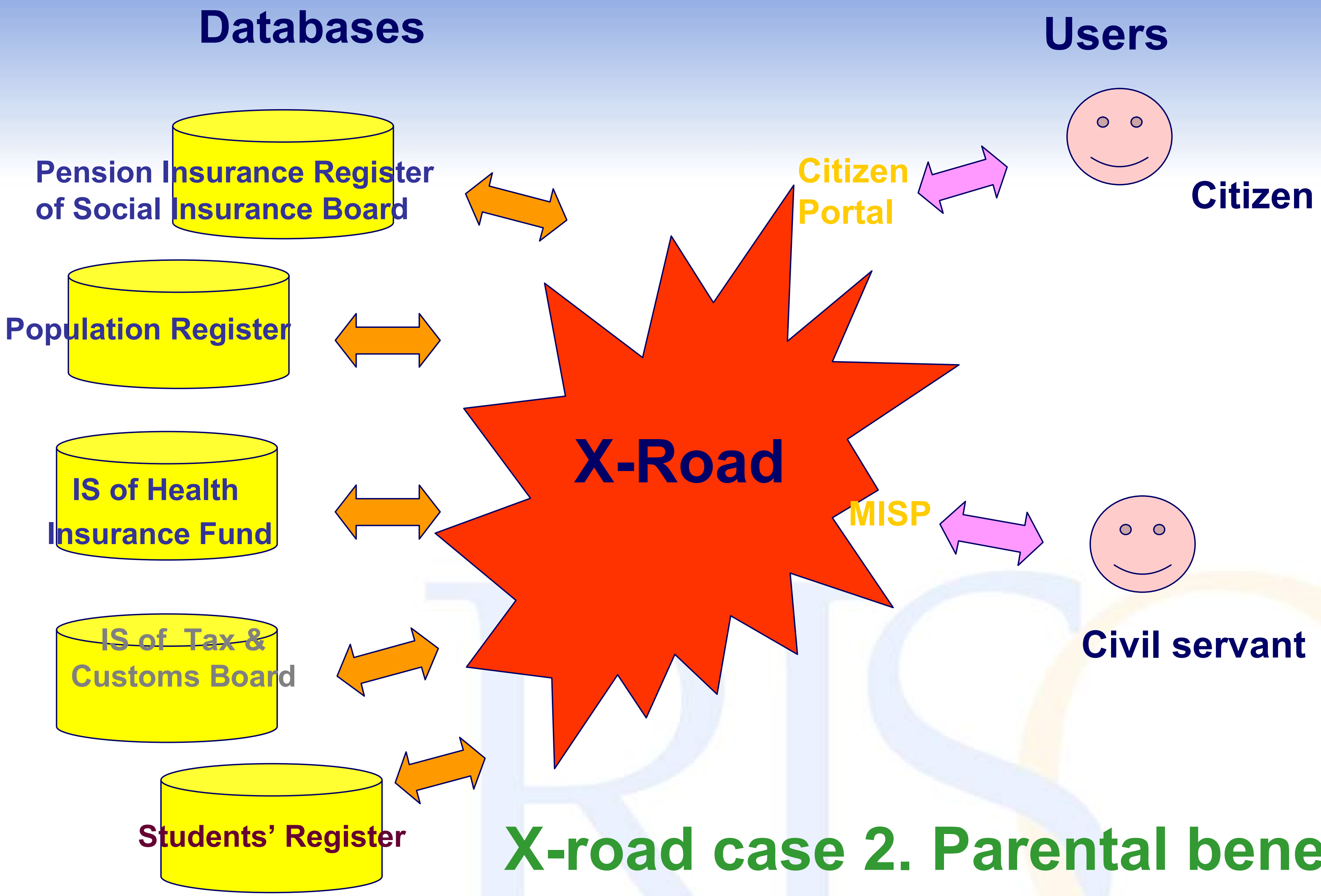
X-Road case 1 – police (traffic)(1)

- Computer in the luggage compartment
- Monitor
- Positioning device



X-road case – police (traffic)(2)

- All police vehicles have been equipped with positioning devices and with mobile workstations which enable aggregated queries in the databases of Police and:
  - Citizen and Migration Board
  - Estonian Motor Vehicle Registration Centre
  - Estonian Traffic Insurance Fund
- Control centre knows where is patrol car
- Patrolling police officer has computerized map
- Ca 20 000 queries per day
- Each query lasts ca 10 seconds



X-road case 2. Parental benefit & Family benefits in Internet

X-Road: What is differently in Estonia?

- PKI infrastructure everywhere;
- Evidentiary value of data;
- High availability;
- Confidentiality;
- Transparent usage of web services;
- We protect data not channels;

X-Road: Authentication

- We have two type of authentication: that of information systems and that of users.
- Every information system is authenticated by the certificate issued by certification authority of X-road
- Persons are authenticated by:
  - ID card
  - MobileID
  - Internet banking (citizens only): Roll of Banks: authentication and e-payment

X-Road: Authorization

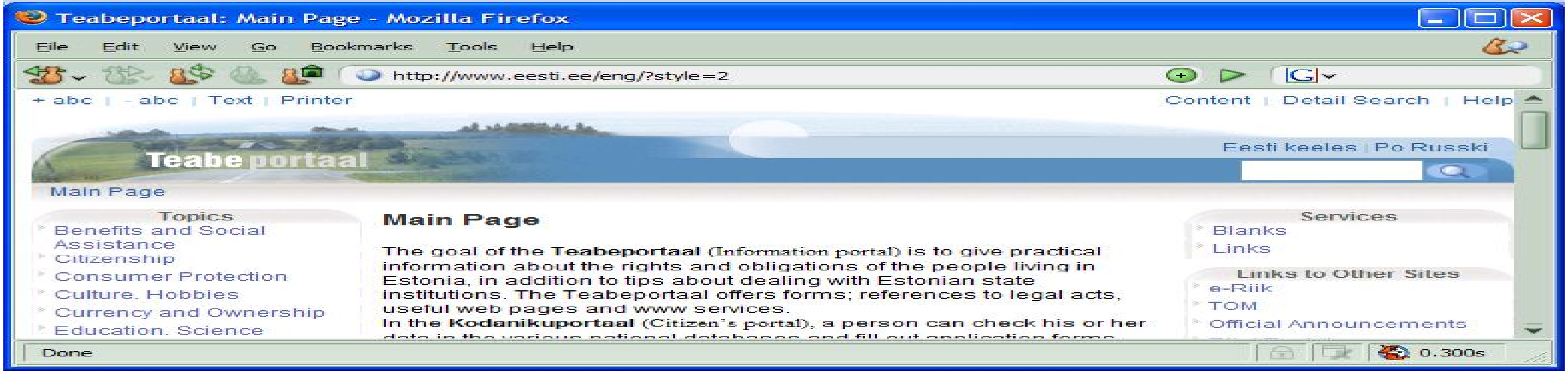
- Two levels of authorization: information systems and users
- Groups of consumers
- Every institution (as user) is responsible for the authorization of its own users (before: service provider was responsible for the authorisation of users. It is similar to situation where alcohol factories are responsible for results of alcohol misuse)
- Service providers must open a new service in case any public institution should need (customers are owners of state registers)

X-Road: What we protect: data or channels?

- The old problem: What we need to protect the king (person) or route (where king is moving)?
- We choose the king (data)
- Most attacks (over 80%) comes from inside, “secure” channels can not resolve the problems
- We use public Internet, but data is crypted, signed.
- Additional channels can increase availibility

- PKI infrastructure protects our data

Citizen portal www.eesti.ee(2003)



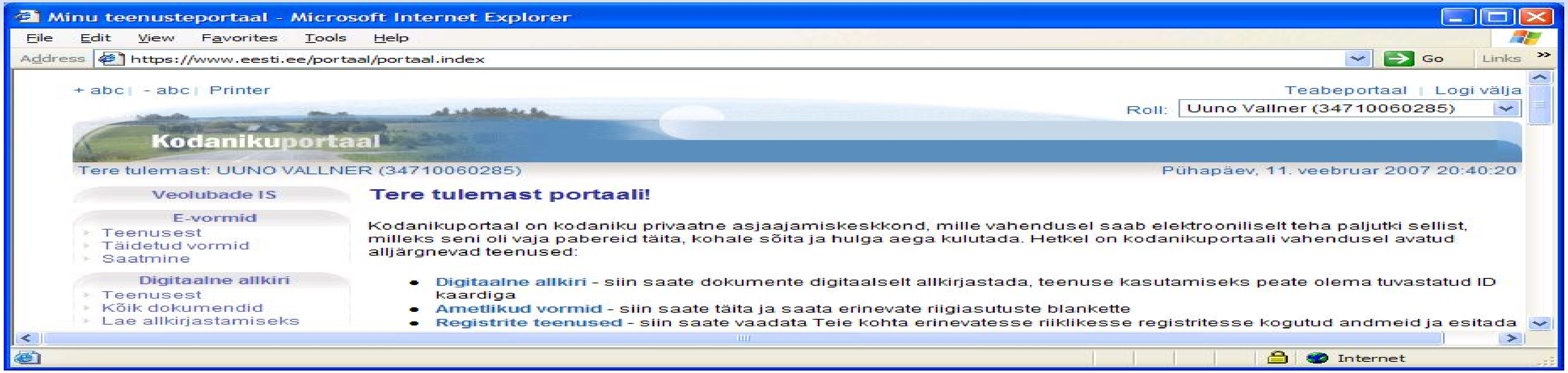
Main Page

The goal of the **Teabeportaal** (Information portal) is to give practical information about the rights and obligations of the people living in Estonia, in addition to tips about dealing with Estonian state institutions. The Teabeportaal offers forms; references to legal acts, useful web pages and www services.

In the **Kodanikuportaal** (Citizen's portal), a person can check his or her data in the various national databases and fill out application forms.

- This portal is freely accessible and contains information about the rights and obligations of Estonian citizens, as well as about services which are provided to them by public sector institutions. The information is relevant both for permanent residents and foreign residents who are interested in having a better understanding of the Estonian way of life.
- The information portal ensures access to information provided by state institutions throughout the citizen's life cycle and by thematic fields

Personal portal https://www.eesti.ee(2003)


Minu teenusteportaal - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Address
https://www.eesti.ee/portaal/portaal.index
Go
Links
Internet

+ abc | - abc | Printer

Teabeportaal | Logi välja

Roll: Uuno Vallner (34710060285)

Kodanikuportaal

Tere tulemast: UUNO VALLNER (34710060285)

Pühapäev, 11. veebruar 2007 20:40:20

Veolubade IS

E-vormid
- Teenusest
- Täidetud vormid
- Saatmine

Digitaalne allkiri
- Teenusest
- Kõik dokumendid
- Lae allkirjastamiseks

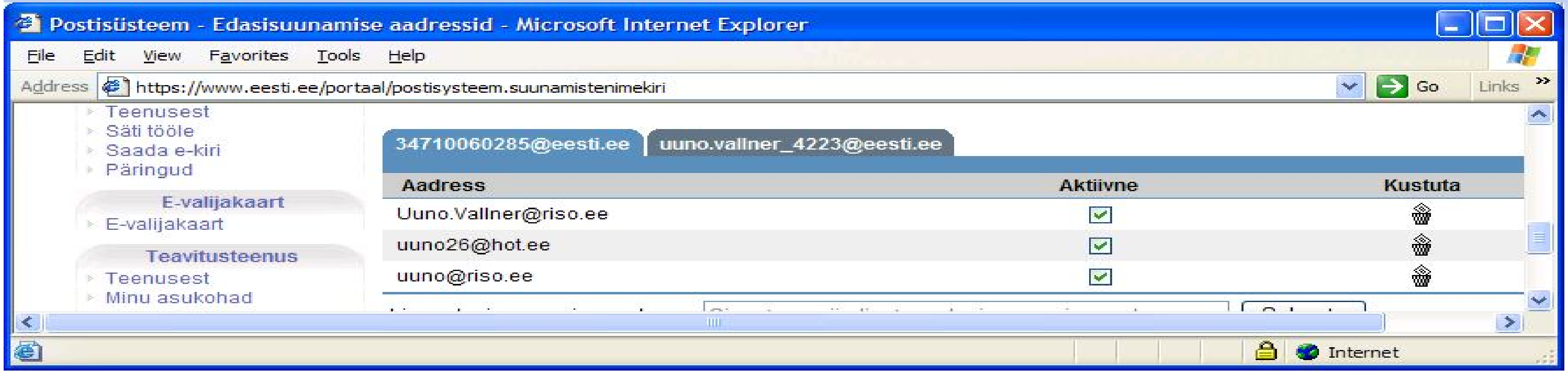
Tere tulemast portaali!

Kodanikuportaal on kodaniku privaatne asjaajamiskeskkond, mille vahendusel saab elektrooniliselt teha paljutki sellist, milleks seni oli vaja pabereid täita, kohale sõita ja hulga aega kulutada. Hetkel on kodanikuportaali vahendusel avatud alljärgnevad teenused:

- Digitaalne allkiri - siin saate dokumente digitaalselt allkirjastada, teenuse kasutamiseks peate olema tuvastatud ID kaardiga
- Ametlikud vormid - siin saate täita ja saata erinevate riigiasutuste blankette
- Registrite teenused - siin saate vaadata Teie kohta erinevatesse riiklikesse registritesse kogutud andmeid ja esitada

- Having passed authentication, the citizen portal allows citizens to use personal secure environment
- Public sector institutions are obliged to provide e-services that require authentication and are targeted at citizens and the private sector (express services, notification services etc.) via the citizen portal. Besides, respective links to the citizen portal should additionally be published on their own websites.

Personal portal. Secure mail @eesti.ee


Postisüsteem - Edasisuunamise aadressid - Microsoft Internet Explorer

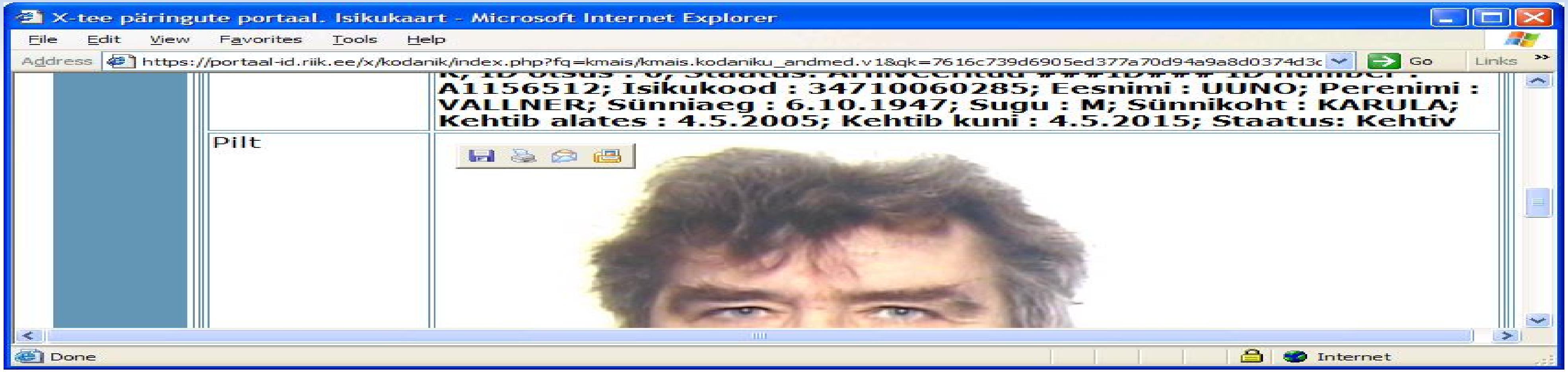
Address: https://www.eesti.ee/portaal/postisysteem.suunamistenimekiri

34710060285@eesti.ee | uuno.vallner_4223@eesti.ee

Aadress	Aktiivne	Kustuta
Uuno.Vallner@riso.ee	☑	🗑
uuno26@hot.ee	☑	🗑
uuno@riso.ee	☑	🗑

- The secure E-mail area. Each local resident has his or her own E-mail address, which is recorded on the citizens ID card and can be used to send signed and encrypted E-mail. The system does not, however, support E-mailboxes for users. Each resident must declare an E-mail address to which mail is to be forwarded so as to redirect the E-mail address that has been provided trough the national ID card

Personal portal: Direct services



X-tee päringute portaal. Isikukaart - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Address
Go
Links
Done
Internet

https://portaal-id.riik.ee/x/kodanik/index.php?fq=kmais/kmais.kodaniku_andmed.v1&qk=7616c739d6905ed377a70d94a9a8d0374d3c

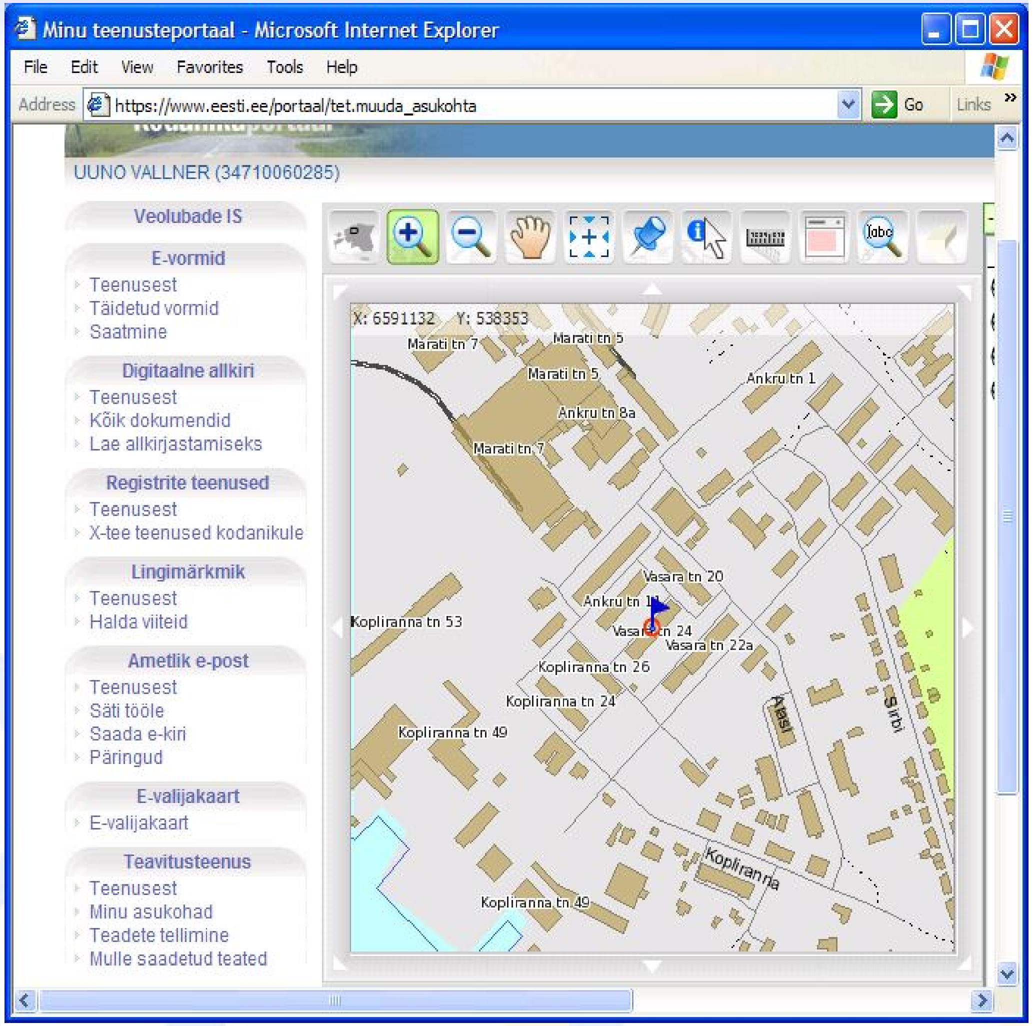
A1156512; Isikukood : 34710060285; Eesnimi : UUNO; Perenimi : VALLNER; Sünniaeg : 6.10.1947; Sugu : M; Sünnikoht : KARULA; Kehtib alates : 4.5.2005; Kehtib kuni : 4.5.2015; Staatus: Kehtiv

Pilt

- The direct services area allows people to view the data which the government has collected about them. They can also receive e-services which do not involve specific institutions. Direct services are produced through the X-road.

Personal portal: Notification services

- There is an area for notification services: breaks in electricity or water deliveries; expiration of a period of validity etc.

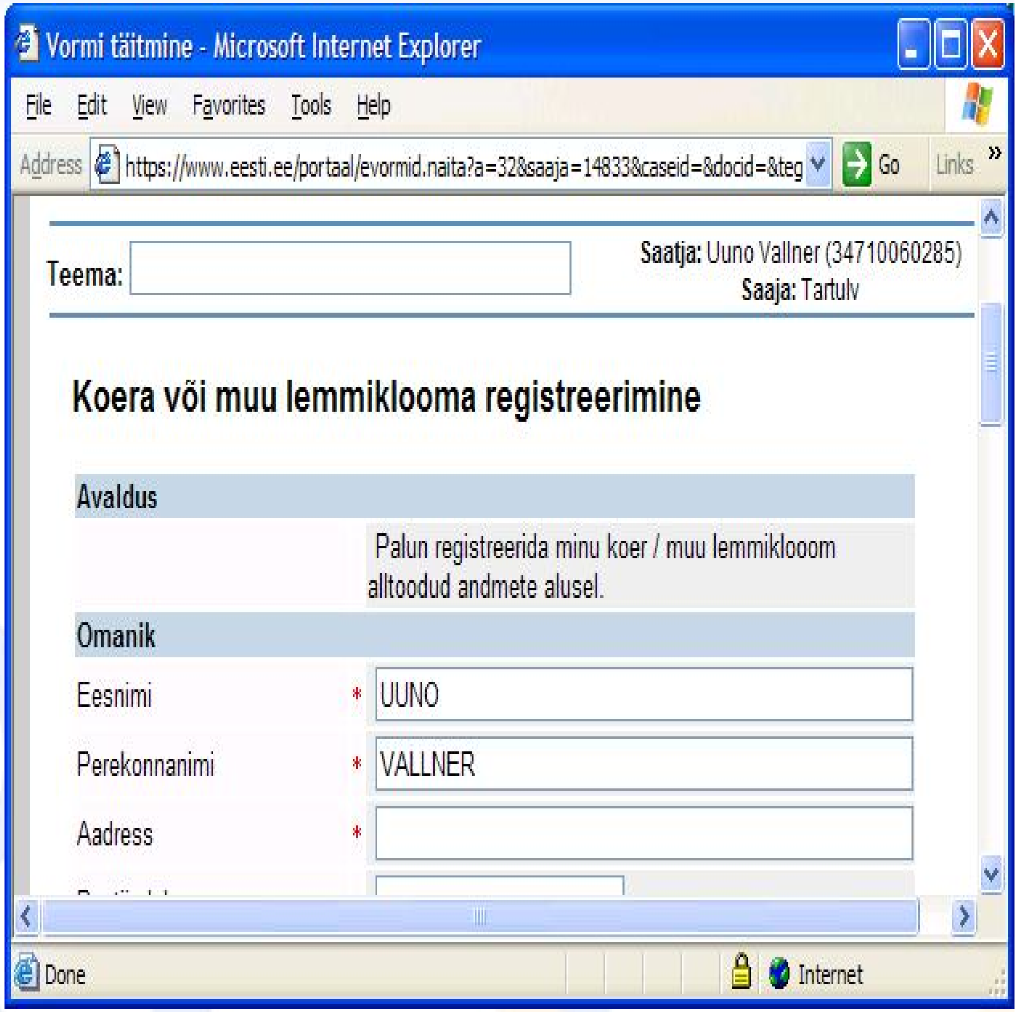


Address https://www.eesti.ee/portaal/tet.muuda_asukohta

UUNO VALLNER (34710060285)

Personal document management system

- The personal document management system allows people to fill in forms and then forward them to the relevant institutions. The institutions process the forms and report the results to the personal document management system from which the form has been submitted. People can trace the proceeding of their case through various institutions. No user is allowed to monitor someone else's case.



https://www.eesti.ee/portaal/evormid.naita?a=32&saaja=14833&caseid=&docid=&teg

Teema:

Saatja: Uuno Vallner (34710060285)
Saaja: Tartulv

Koera või muu lemmiklooma registreerimine

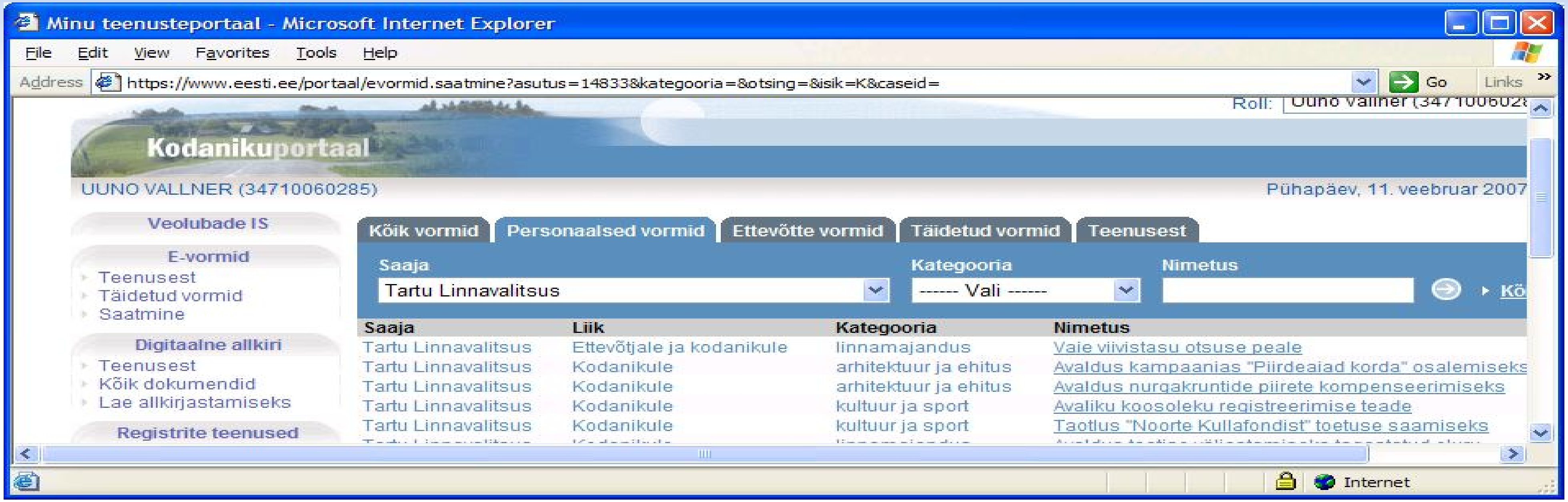
Avaldus

Palun registreerida minu koer / muu lemmiklooom alltoodud andmete alusel.

Omanik

Eesnimi	*	UUNO
Perekonnanimi	*	VALLNER
Aadress	*	

Personal area for signing



Minu teenusteportaal - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address
Go
Links

https://www.eesti.ee/portaal/evormid.saatmine?asutus=14833&kategooria=&otsing=&isik=K&caseid=

Roll: Uuno Vallner (347100602

Kodanikuportaal

UUNO VALLNER (34710060285)

Pühapäev, 11. veebruar 2007

Saaja: Tartu Linnavalitsus

Kategooria: ------ Vali ------

Nimetus:

Saaja	Liik	Kategooria	Nimetus
Tartu Linnavalitsus	Ettevõtjale ja kodanikule	linnamajandus	Vaie viivistasu otsuse peale
Tartu Linnavalitsus	Kodanikule	arhitektuur ja ehitus	Avaldus kampaanias "Piirdeaiad korda" osalemiseks
Tartu Linnavalitsus	Kodanikule	arhitektuur ja ehitus	Avaldus nurgakruntide piirete kompenseerimiseks
Tartu Linnavalitsus	Kodanikule	kultuur ja sport	Avaliku koosoleku registreerimise teade
Tartu Linnavalitsus	Kodanikule	kultuur ja sport	Taotlus "Noorte Kullafondist" toetuse saamiseks

- The secure documents area allows the user to sign documents and then send them. These facilities are based on free DigiDoc software

Thank you for your attention!

Uuno.Vallner@eesti.ee