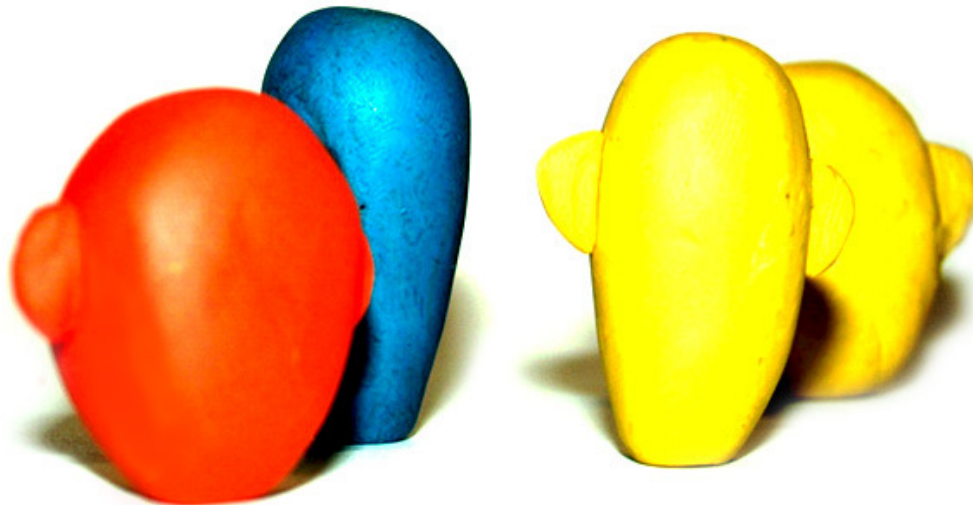


Estonia – The Country With Identification Infrastructure

Tarvi Martens
SK





E-stonia ?

- **Population: 1.35M**
- **Internet usage: 64%**
- **Internet banking: 88%**
- **Mobile penetration: >100%**
- **1000+ Free Internet Access points**
- **PKI penetration: >80%**





ID-card Project

- **Started in 1997**
- **Law on personal identification documents: Feb, 1999**
- **Digital Signature Act: March, 2000**
- **Government accepted plan for launching ID-card: May, 2000**
- **First card issued: Jan 28, 2002**
- **October 2006: 1 000 000th card issued**



The Card

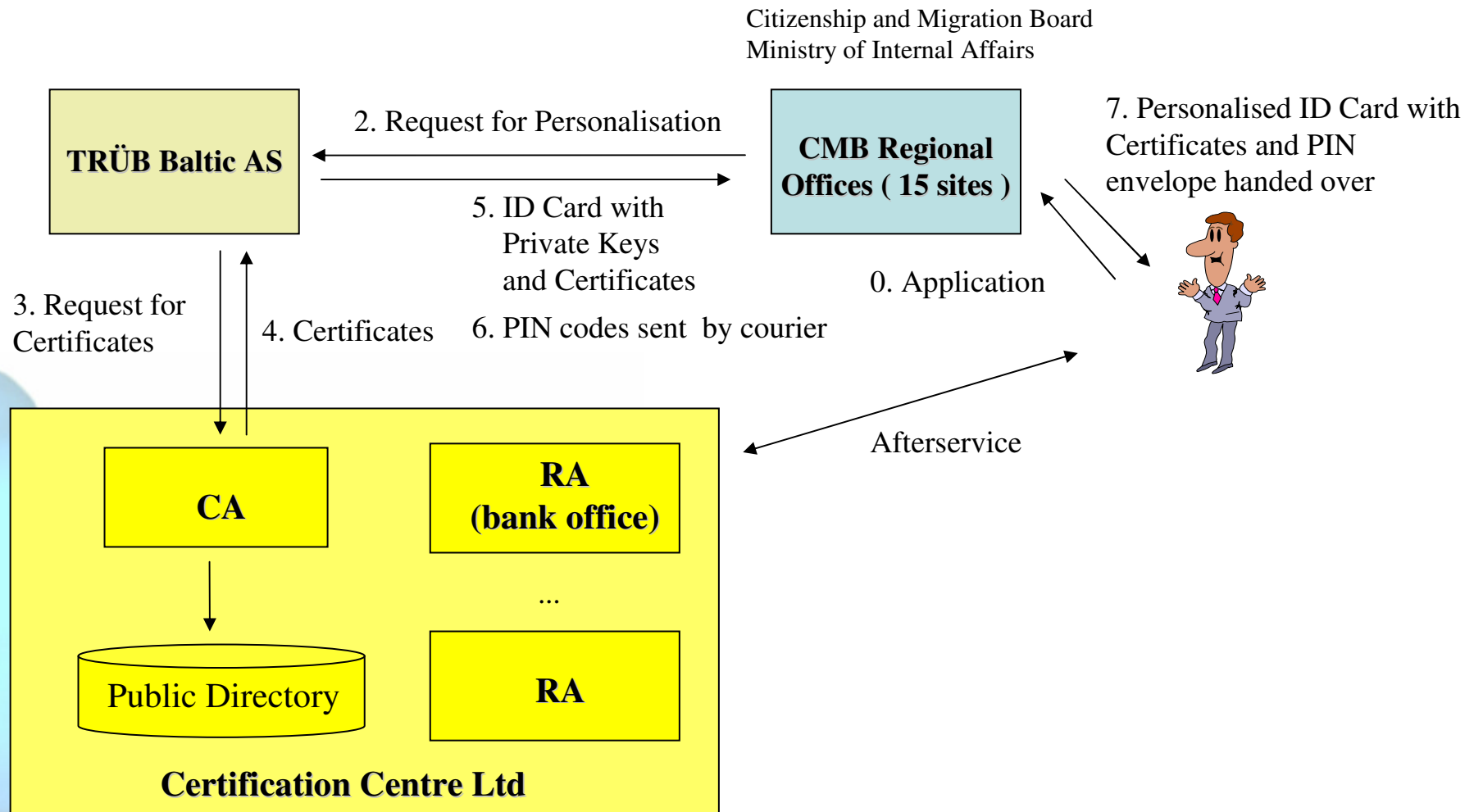
- “Compulsory”
for all residents



- Contains:
 - Personal data file
 - Certificate for authentication
(along with e-mail address
Forename.Surname@eesti.ee)
 - Certificate for digital signature



Card issuance



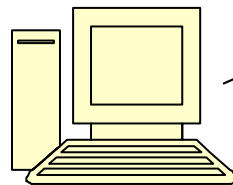


Fixed-line

Mobile

Internet

Cash



Population Registry

e-Tickets



ID-card as a ticket for public transportation

Person must possess and show an ID-card when buying or verifying a ticket



Authentication: e-Citizen portal log-in options

X-tee kodanikuportaal. Pääringud - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites Media

Links RadioExp

X-tee

Log-in with ID-card

Rahvastikuregister

- Kodaniku päring iseenda kohta rahvastikuregistrist
- Kodaniku võimalus teavitada oma statistiliste andmete (rahvus, emakeel, haridus, tegevusala) muutumisest
- Kodaniku võimalus teavitada oma andmetes vea leidmisest registri volitatud töötajale kodanikuportaalil vahendusel

Äriregister

- Kodaniku päring iseenda koh...

CELL NETWORK

Kodaniku võimalus teavitada oma andmetes vea leidmisest registri volitatud töötajale kodanikuportaalil vahendusel

Minu teenusteportaal - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites Media

Address: https://www.eesti.ee/

Kodanikuportaal

Kodanikuportaalile sisenemine

Sisenemisega aktsepteerite kodanikuportaalile üldtingimusi.

ID kaardiga sisenemiseks peab kasutajal olema ID kaart, arvuti küljes ID kaardi lugeja ja installeeritud vajalik tarkvara, mis ühendab omavahel eelnimetatud vahendid ja tagab ID kaardi kasutamise erinevates isiku tuvastamist vajavates internetikeskkondades.

ID kaardiga autentitud kasutaja saab kasutada kodanikuportaalil järgmisi teenuseid:

- Registrite teenused
- Lingimärkimise teenus
- @eesti.ee e-posti suunamise teenus

Kaudu sisenemiseks peab kodanik olema internetipanga klient. Internetipanga kasutajal pakuvad isiku tuvastamise teenust järgmised pangad: Ühispank, Krediidipank, Sampo Pank, Nordea Pank.

Vahendusel autentitud kasutaja saab kasutada kodanikuportaalil järgmisi teenuseid:

- Registrite teenused

ID - kaart

Sisesta PIN-kood isikutuvastuseks (PIN 1)

OK Käesista

Kasutamistingimused | Abiks sisenemisel

X-tee päringute portaal. Autentimine - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites Media

Address: https://portal.vik.ee/5633/kodanik/index.php?m=aktak/itak/legacy1.v1

X-tee

Pääringute portaal

Autentimine

Hansapank	
Ühispank	
Krediidipank	
Sampo pank	
Nordea Pank	

CELL NETWORK

Log-in via web-bank



ID-card for secure e-mail

- The authentication certificate contains an e-mail address
Surname.Lastname[.X]@eesti.ee
- All S/MIME mailers are usable
- The eesti.ee server runs a forwarding service
- Usable for secure C2C, B2C and G2C communication

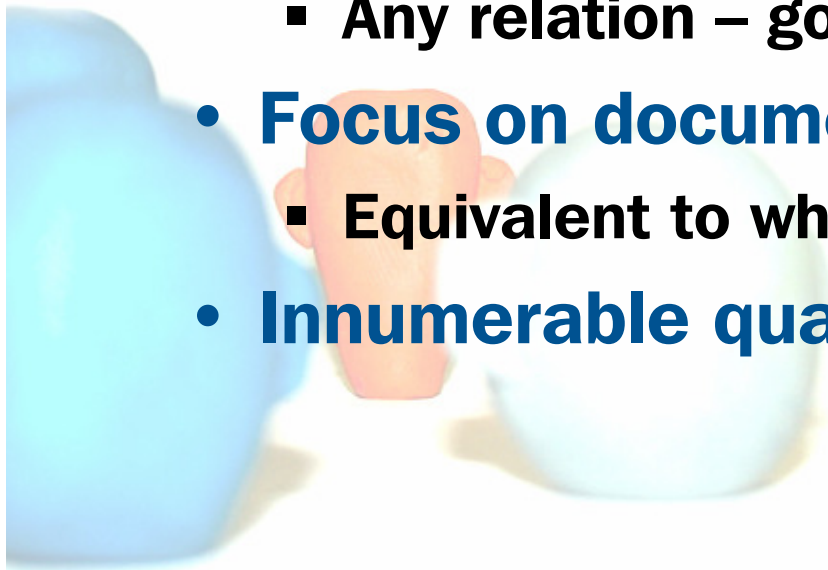




Digital Signature - concepts



- **Public sector is obliged to accept digitally signed documents**
- **Digital signature is universal**
 - Open user group
 - Any relation – government, business, private
- **Focus on document concept**
 - Equivalent to what we are doing on paper
- **Innumerable quantity of “applications”**

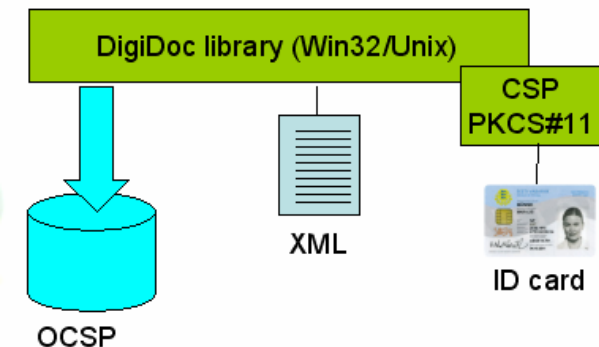




Uniform platform - DigiDoc

- **Full-scale architecture for digital signatures and documents**

- Document format
- Program libraries (C, Java, COM)
- End-user client – DigiDoc Client
- End-user portal – DigiDoc Portal
- Webservice



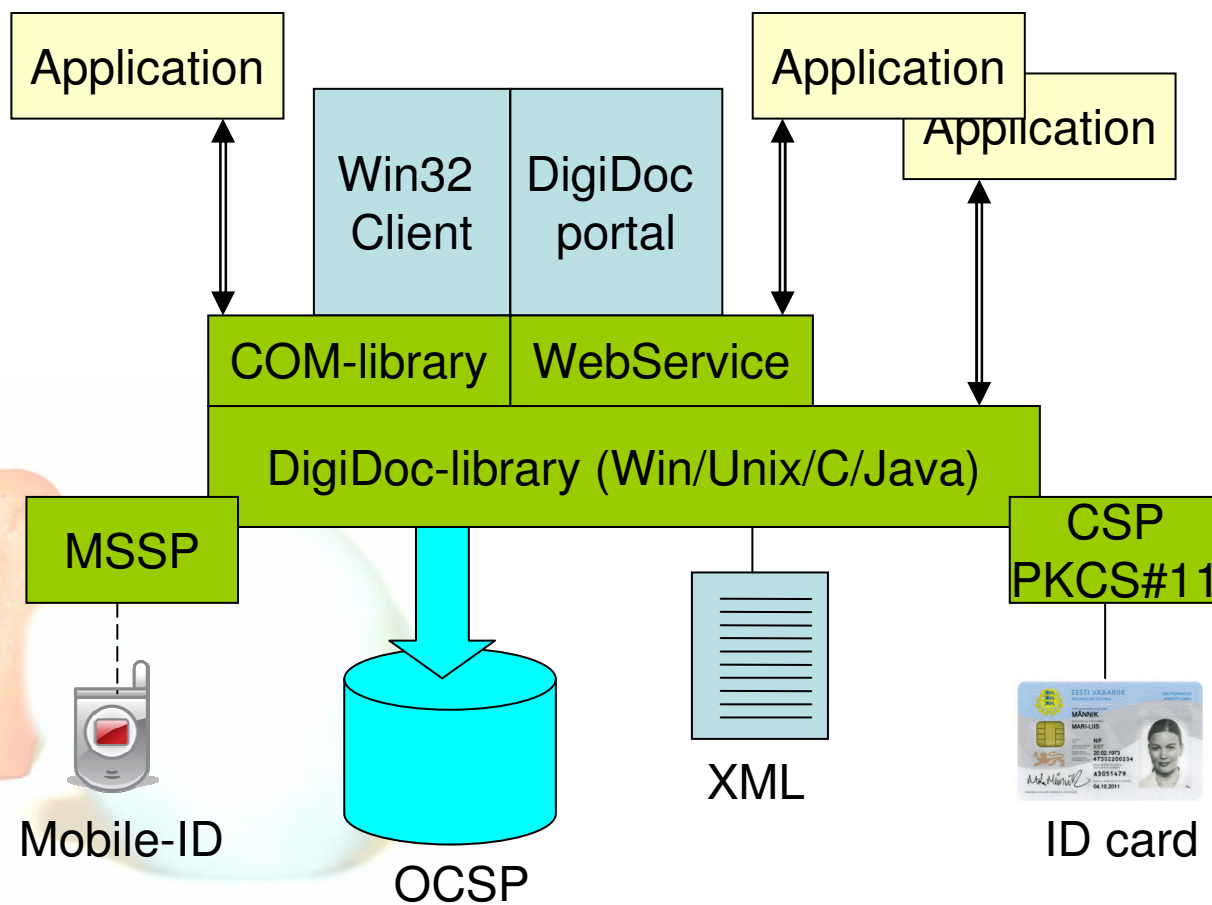
- **Based on international technical standards**

- ETSI TS 101 903 – XML Advanced Electronic Signatures aka “XAdES”

- **Includes real-time validity confirmation of a certificate (OCSP)**
- **Long-term validity of a documents is ensured**



DigiDoc architecture





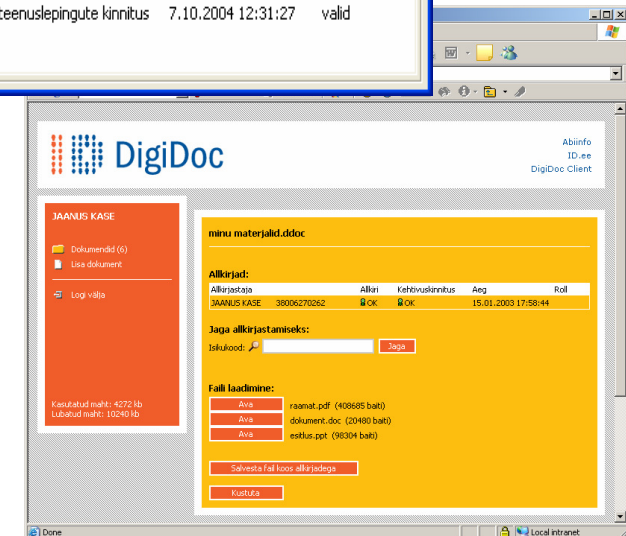
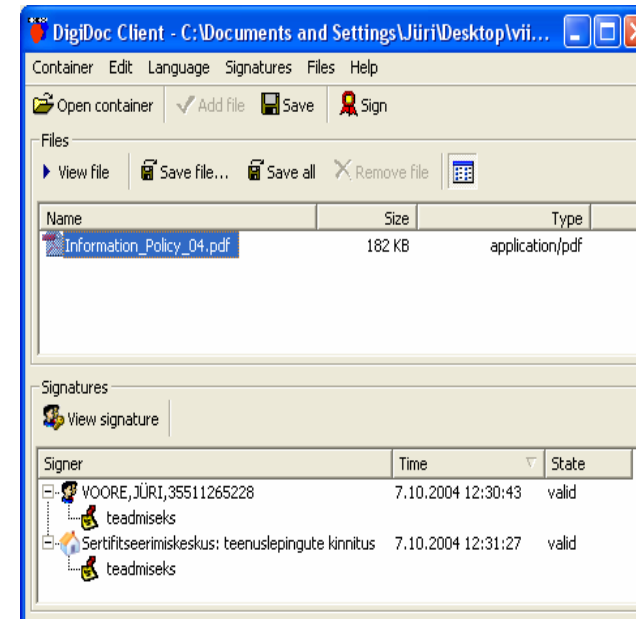
DigiDoc for end-user

- **DigiDoc Client**

- **Windows application**
 - 5 languages
- Lets users sign, verify signatures etc
- ID Card not needed for document verification
- Available at www.id.ee

- **DigiDoc portal**

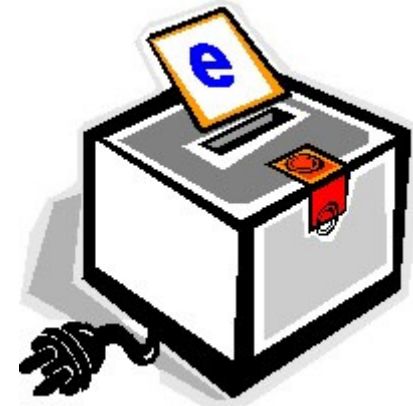
- <https://digidoc.sk.ee>
- Signing, verification, co-signing by multiple persons





Internet voting

- **Happened first in October 2005**
- **First pan-national binding occasion (municipal government elections)**
- **Parliament elections is 2007**
- **ID-card as an enabling tool**
- **Normal behaviour vs. Rocket Science**



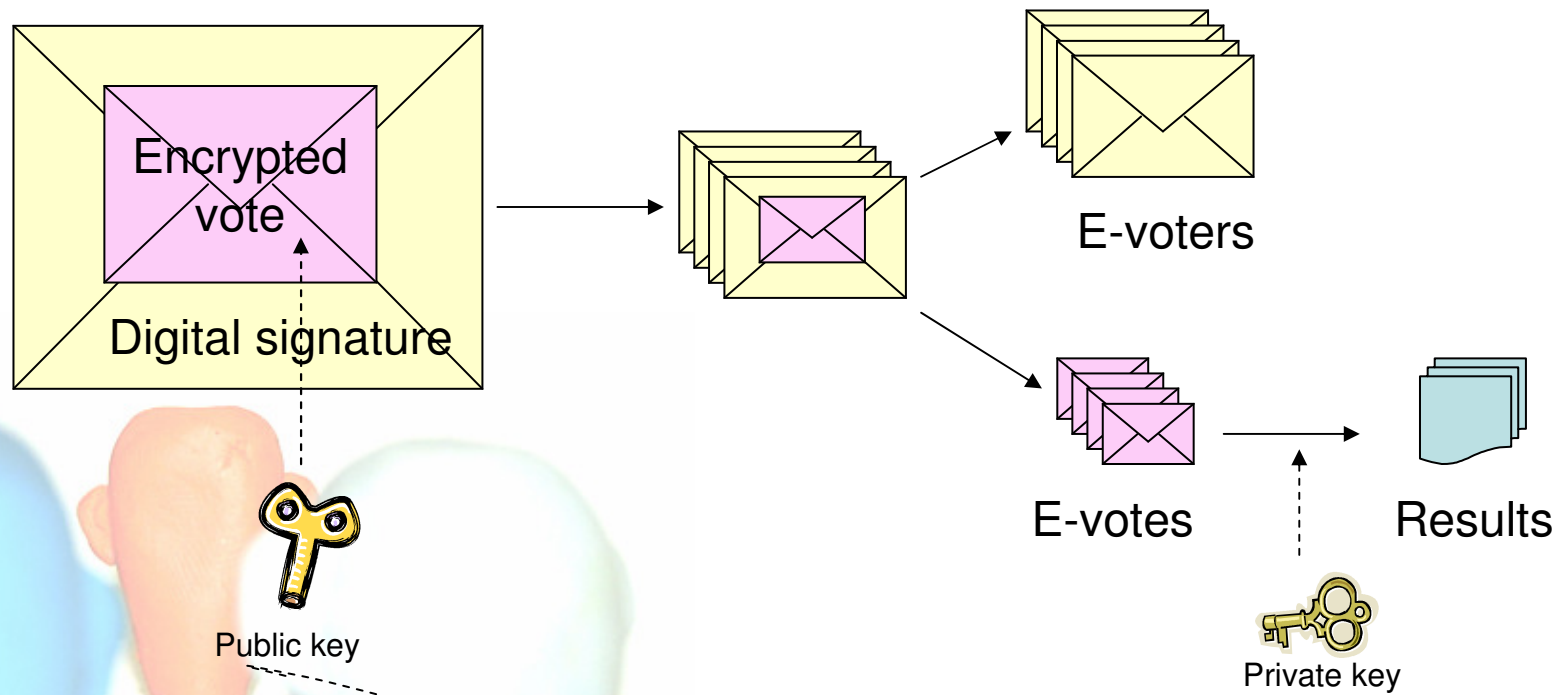


I-voting: Main Principles

- All major principles of paper-voting are followed
- I-voting is allowed during period before Voting Day
- The user uses ID-card
 - System authenticates the user
 - Voter confirms his choice with digital signature
- Repeated e-voting is allowed
 - Only last e-ballot is counted
- Manual re-voting is allowed
 - If vote is casted in paper during absentee voting days, e-vote(s) will be revoked



I-voting: The Envelope Scheme





Morale (1)

- PKI stands for Public Key **Infrastructure**
- There are no services nor applications before **The Infrastructure** is built
 - Roads generate no benefit, transportation does
 - People do not buy cars unless there are roads
- **Infrastructure first**





Flip side of the coin

- **1,000,000 ID-cards**



- **30,000 electronic users
(2006)**





Why won't they go e?

- **Habits**

- Strong tradition of banks-provided authentication service

- **Barriers**

- Need for smart-card reader and software

- **No awareness promotion**

- ID-cards are perceived as merely physical documents
- Unawareness about security benefits

1. 12345678	15. 12345678	28. 12345678
2. 12345678	16. 12345678	29. 12345678
3. 12345678	17. 12345678	30. 12345678
4. 12345678	18. 12345678	31. 12345678
5. 12345678	19. 12345678	32. 12345678
6. 12345678	20. 12345678	33. 12345678
7. 12345678	21. 12345678	34. 12345678
8. 12345678	22. 12345678	35. 12345678
9. 12345678	23. 12345678	36. 12345678
10. 12345678	24. 12345678	37. 12345678
11. 12345678	25. 12345678	38. 12345678
12. 12345678	26. 12345678	39. 12345678
13. 12345678	27. 12345678	40. 12345678





Who is driving ?

Public sector service

Tax
Declarations



Once in a **year**

Private sector service

Online banking



Once in a **week**



“Computer Security 2009”

- Co-operation program between private and public sector
- Aims for safe information society in general

arvutikaitse



- Special target: **ten-fold** increase of eID users (300,000 by the end of 2009)





Measures for CS09

- **Availability**
 - Alternative PKI-based tokens/methods
 - Redundant service network
- **Wide support and usability**
 - Support for alternative platforms (Mac, Linux, ..)
- **Awareness and training**
- **Pressure by banks**
 - Termination of authentication service to 3rd parties
 - Reduction of transaction limits with passwords



Reader distribution

- card reader
- <https://installer.id.ee>
- Price ca 6 EUR



- Available at retail stores
- Sold by banks
- Giveaways in campaigns





Installer.id.ee

 ID-kaardi paigaldustarkvara





Sellelt leheküljelt saab paigaldada enda arvutisse kõik vajaliku ID-kaardi kasutamiseks.

С этой страницы вы можете загрузить на ваш компьютер всё необходимое для пользования идентификационной картой.

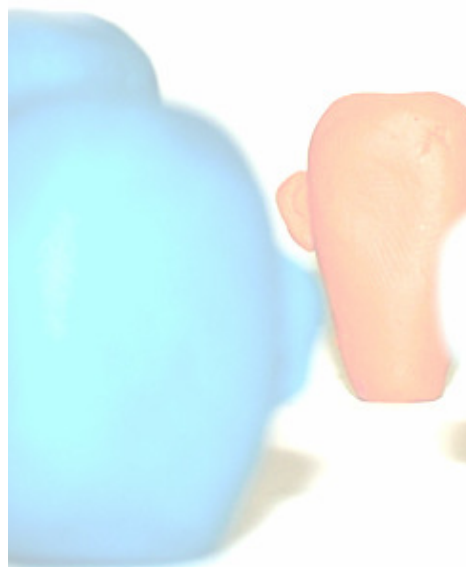
Here you can install the software necessary for electronic use of the ID-card.

Jätka

Продолжить

Continue







ID card software

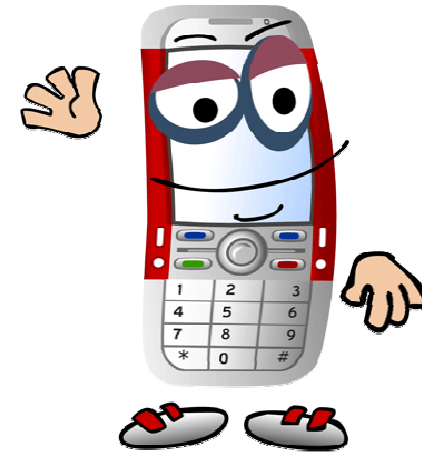
- **Complete rewrite underway**
- **Multi-platform**
 - **Card drivers (CSP/PKCS#11)**
 - **Card maintenance tool**
 - **Digital signing**
 - Libraries
 - Webservice
 - Desktop client
- **Expected to launch by the end of 2009 by LGPL terms.**





Alternative eID - MobileID

- **PKI-capable SIM cards**
 - Requires replacement of SIM
- **Instantly ready to use**
 - No specific software required
- **Equal legal power and security with ID-card**
- **Launched: May 2007**
- **Available from the major GSM operator (EMT – 40%)**





id.ee

Windows Internet Explorer window showing the ID.ee website.

Address bar: <http://id.ee/>

Navigation bar: Google, powerpoint clipart, Mine, RS, Järjehoidjad, 15 blokeeritud, Kontrolli, Saada, powerpoint, clipart, Seaded

Search bar: ID.ee

Header: ID-kaart - uue ajastu isikutunnistus

Navigation menu: [Avaleht](#) | [ID-kaart](#) | [Kasutusosalad](#) | [Tarkvara](#) | [Arendajale](#) | [ID-projekt](#) | [ID-koolitus](#) | [Abi](#)

Three main content blocks:

- Saa e-kodanikuks!**
 - ▶ Hangi ID-kaart
 - ▶ Hangi ID-kaardi lugeja
 - ▶ Paigalda tarkvara
 - ▶ Kontrolli sertifikaate
 - ▶ Vaata veebikoolitust
- Vajad abi?**
 - ▶ ID-kaardi abikeskus
 - ▶ Probleemileidja
 - ▶ Teadmistebaas
 - ▶ Küsi abi
- Teenused!**
 - ▶ Isikutuvastus internetis
 - ▶ Digiallkirjastamine
 - ▶ ID-Pilet
 - ▶ ID-blogis teenuste kohta

idBlog | Kõik ID-kaardiga seonduv

Arhiiv: - Vali periood -

Teemad blogis

- ▶ Üldine (1)
- ▶ Blogroll (0)
- ▶ Tarkvara (1)
- ▶ E-hääletamine (1)
- ▶ Teenused (2)

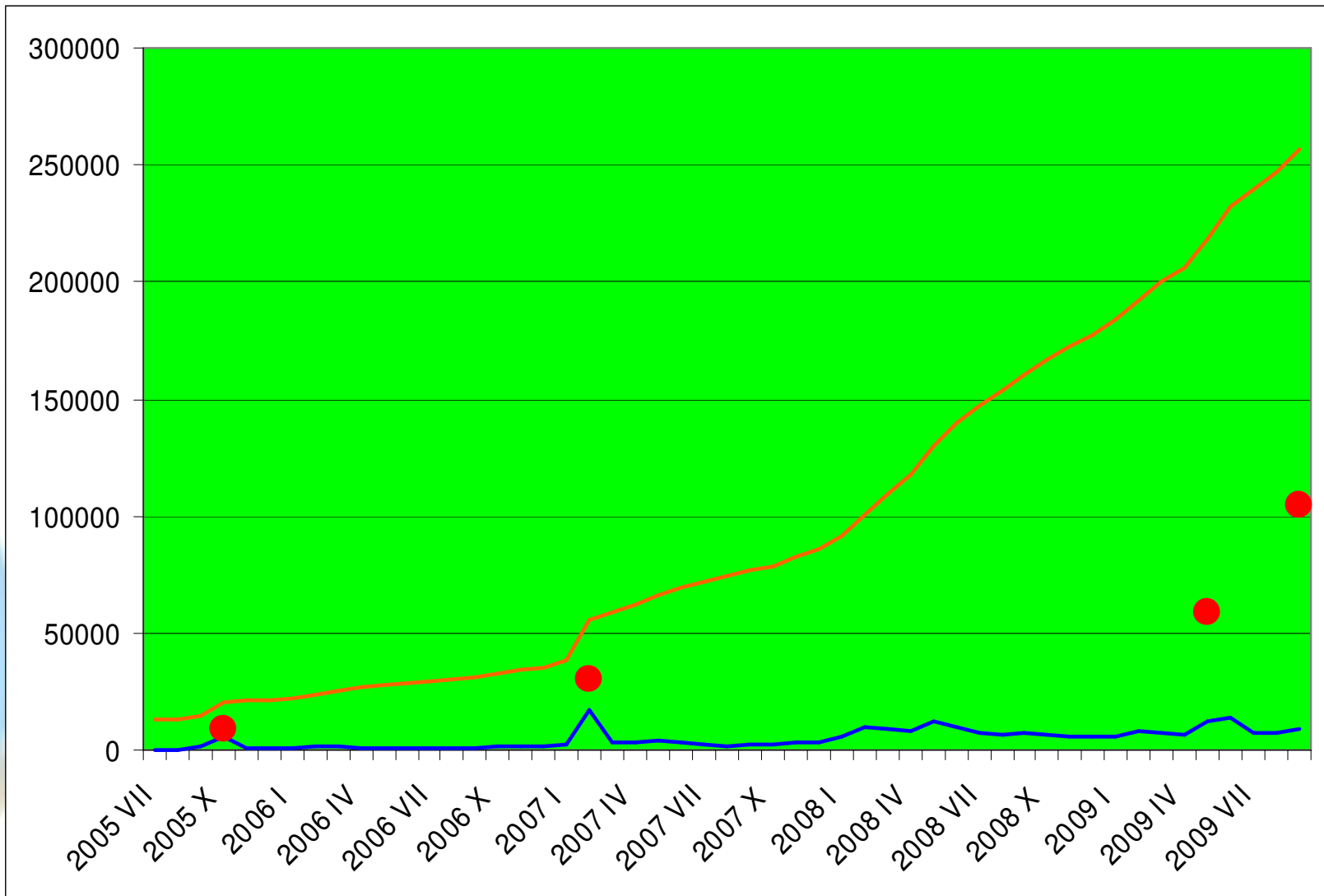
ID.ee veebist uus versioon

Autor: [Mart Parve](#) Sisestatud: Neljapäev, 29.03.2007 Teemad: [Üldine](#)

Nagu ehk isegi tähele paned, oleme üllitanud uue versiooni ID-kaardi veebileheküljest. Lilled ja pasunakooriga me seda välja kuulutanud veel ei ole, sest tööd on veebiga veel küll ja küll. Kuid sel nädalal



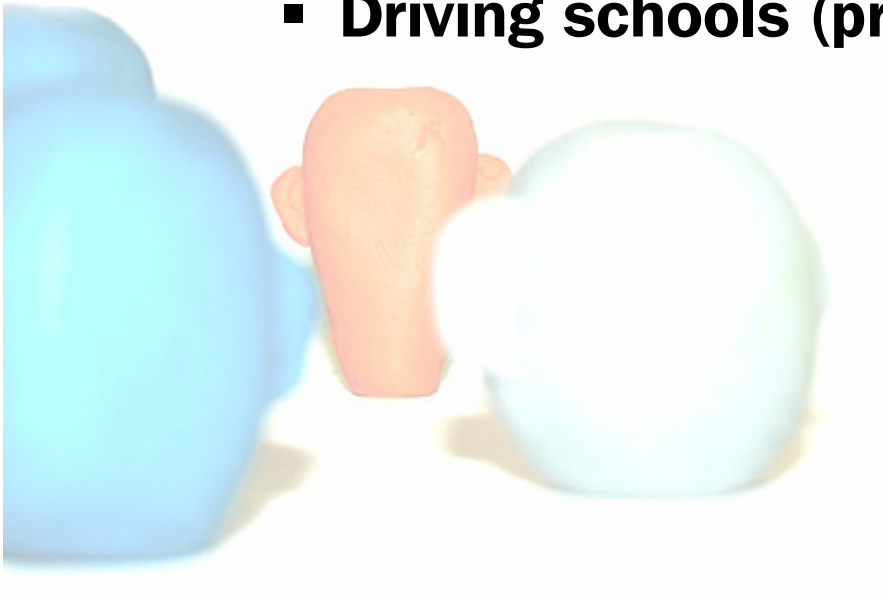
CS2009: So far so good...





Morale (2)

- Roads are ready
- Now we have to teach people about the wonders of transportation
 - Car manufacturing (services)
 - Driving schools (promotion & awareness)





Additional Information

- ID-card issuance www.pass.ee
- PKI & CA www.sk.ee
- ID-card practices www.id.ee
- Digital signature software www.openxades.org



Contact point:
tarvi@sk.ee