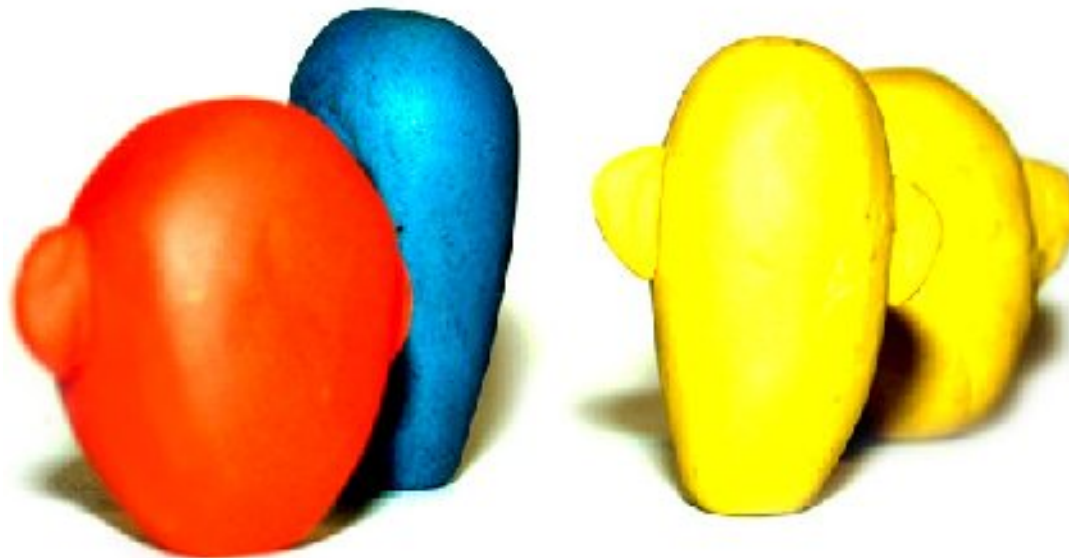


# eAuthentication in Estonia and beyond

Tarvi Martens  
SK





## E-stonia ?

- **Population: 1.35M**
- **Internet usage: 56%**
- **Internet banking: 88%**
- **Mobile penetration: >100%**
- **1000+ Free Internet Access points**
- **PKI penetration: >80%**
- **Biggest national eID card roll-out in Europe !**





# Agenda

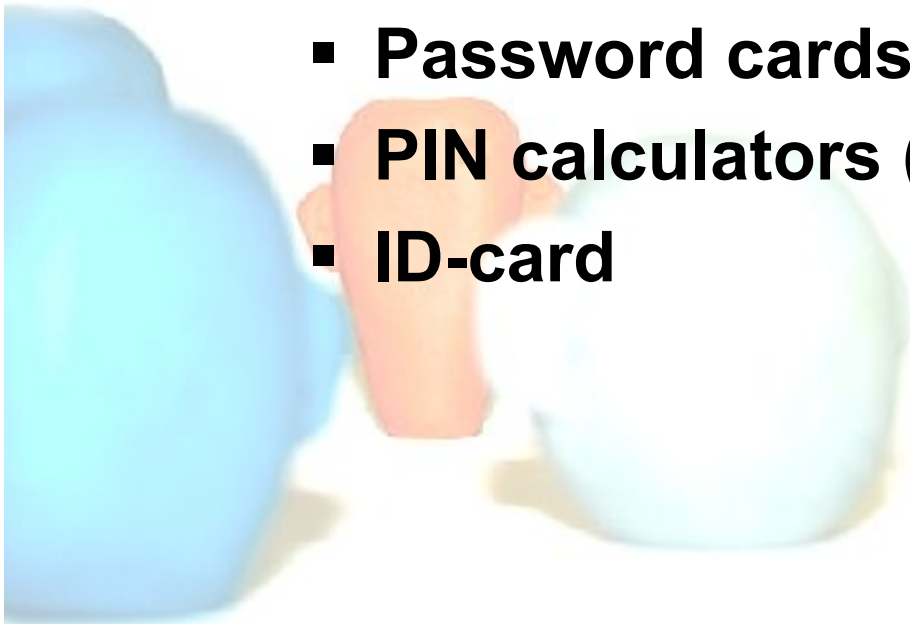
- **Bank eID**
- **The ID-card**
- **Mobile-ID**
- **Computer Security 2009**
- **On international eID interoperability**





## Bank eID

- Internet banking started in 1996
- “Everyone” has a Internet bank account
- 5 (i-)banks covering 99% of the market
- Authentication options
  - Password cards (>1Mio, usage – 90%)
  - PIN calculators (~50 000 in use)
  - ID-card





## Bank eID for third parties

- **All banks are providing authentication services to 3rd parties:**
  - **Doing taxes – 86% online**
  - **Citizen portal providing access to 70 databases and over 700 services**
  - **E-school**
  - **Telecom, utilities**
  - **E-business**
- **Overwhelmingly used**





## 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: 1 000 000<sup>th</sup> card issued**



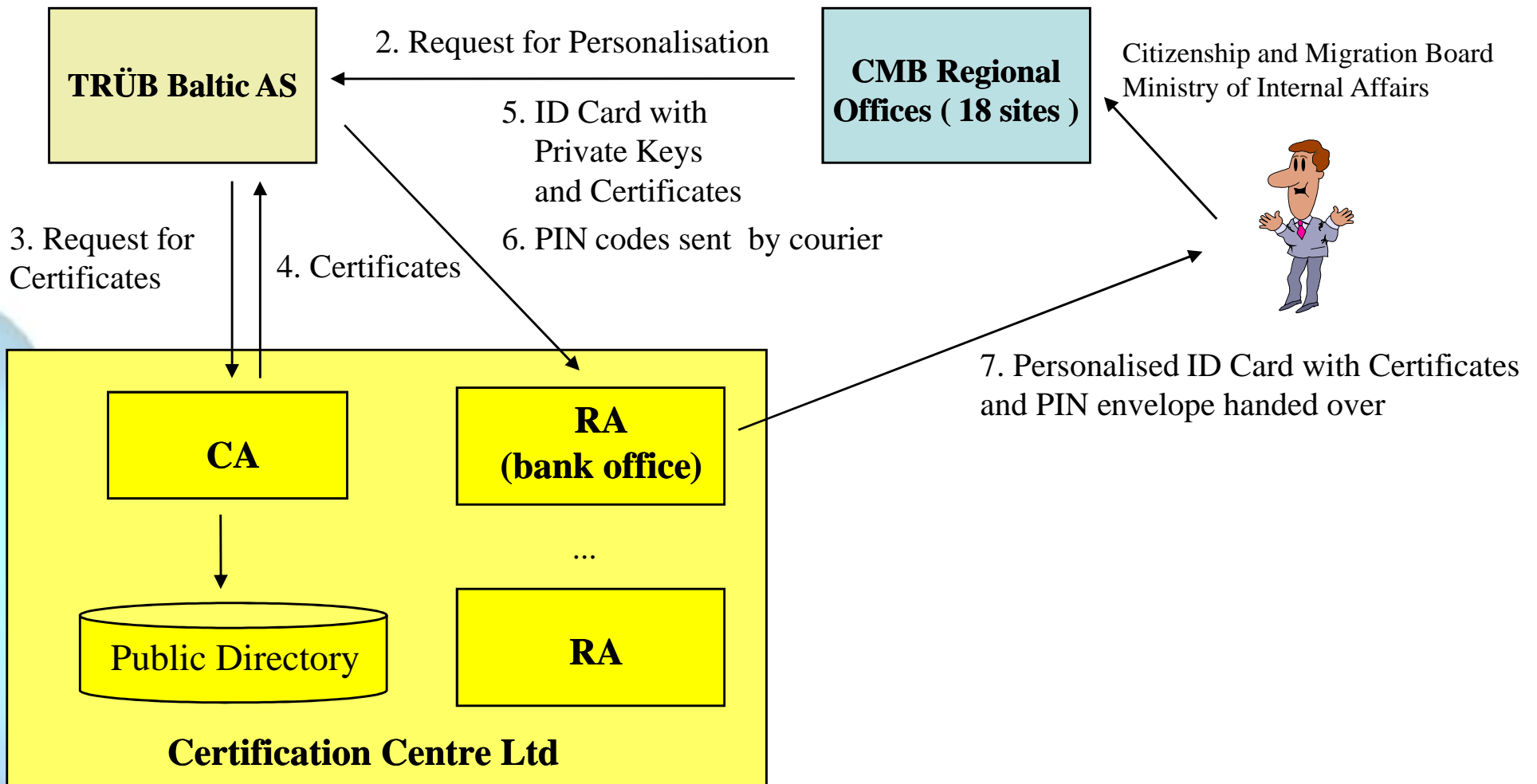
# The Card

- “Compulsory”  
for all residents
- Contains:
  - Personal data file
  - Certificate for authentication  
(along with e-mail address  
[Forename.Surname@eesti.ee](mailto:Forename.Surname@eesti.ee))
  - Certificate for digital signature





# Card issuance





## “ID-starter” packages

### Package 2003:

- card reader
- manual
- installation CD

Price ca 20 EUR



### Package 2007:

- card reader
- <https://installer.id.ee>

Price ca 6 EUR



# ID-card as a ticket for public transportation



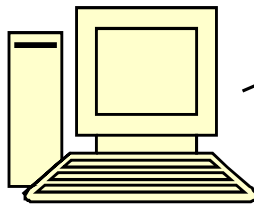
Fixed-line



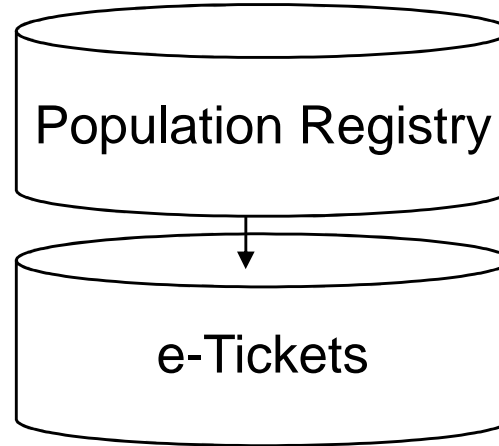
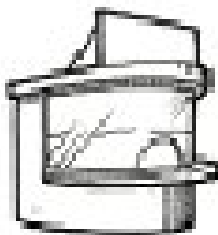
Mobile



Internet



Cash



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



# Authentication: e-Citizen portal log-in options

**Log-in with ID-card**

**Rahvastikuregister**

- Kodaniku pöring iseenda kohta rahvastiku registrist
- Kodaniku võimalus seavitada oma sotsiaalseid andmeid (rahvus, emakeel, haridus, tegevusala) muutmiseks
- Kodaniku võimalus seavitada oma andmetes vea leidmist registri vabivõtte 13812\_ale kodaniku portaali vahenditega

**Äriregister**

- Kodaniku pöring iseenda kohta

CELL ESTONIA

**Log-in via web-bank**

**Kodaniku portaali**

Kodaniku portaali kasutamine

Kasutades portaali saate teha järgmisi asju:

- Teha avaldusi ja taotlusi
- Teha avaldusi ja taotlusi
- Teha avaldusi ja taotlusi

Teie isiklikud andmed on kaitstud ja ei ole avalikud.

Teie isiklikud andmed on kaitstud ja ei ole avalikud.

Teie isiklikud andmed on kaitstud ja ei ole avalikud.

**Püringute portaali**

**Ambutimline**

- Teie isiklikud andmed on kaitstud ja ei ole avalikud.
- Teie isiklikud andmed on kaitstud ja ei ole avalikud.
- Teie isiklikud andmed on kaitstud ja ei ole avalikud.

CELL ESTONIA



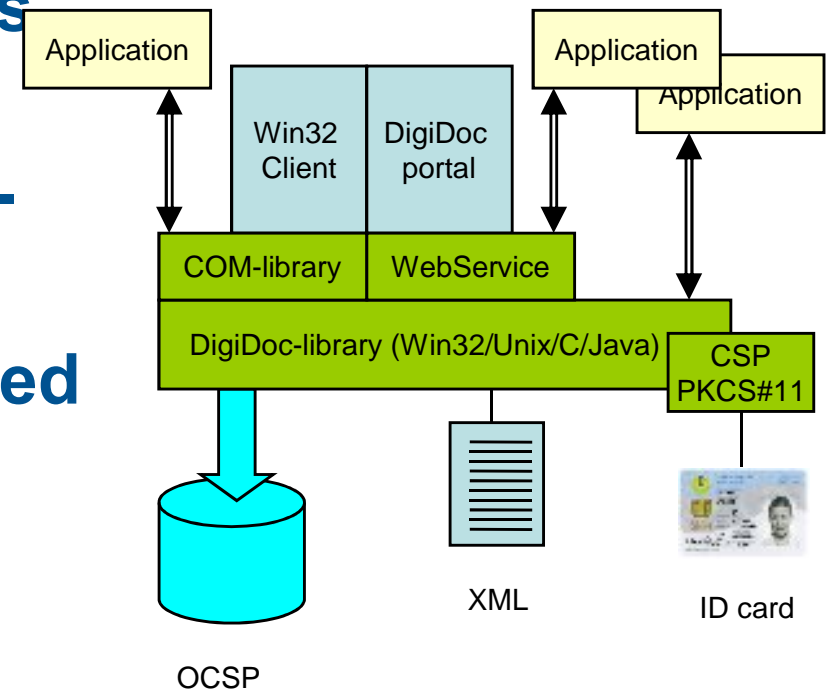
## ID-card for secure e-mail

- 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 with ID-card

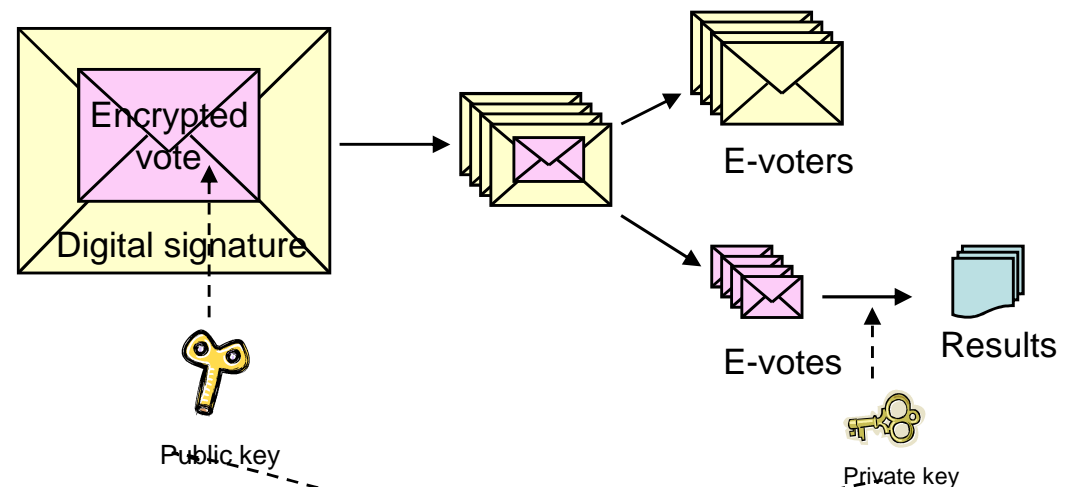
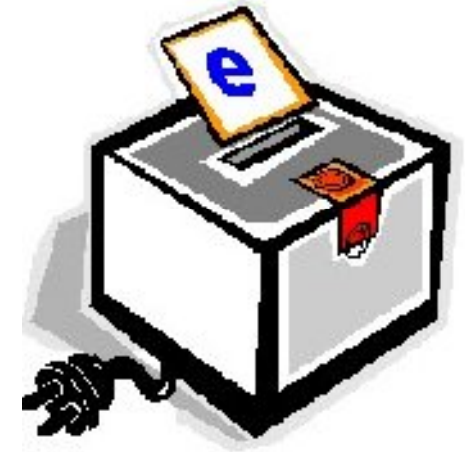
- Public sector is obliged to accept digitally signed documents
- Common Digital Signature System “DigiDoc” is used cross-sector, no alternatives around
- Highest security level (long-time validity) is provided
- Over 2 Mio signatures created in 4+ years





# Internet voting

- Happened first in October 2005
  - First pan-national binding occasion (municipal government elections)
- Parliament elections is 2007 (3x increase on i-voters turnout)
- ID-card as an enabling tool





## Flip side of the coin

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



- **55,000 electronic users**





## Why won't they go E?

- **Habits**

- Strong tradition of banks-provided authentication service (based on passwords)

- **Barriers**

- Need for smart-card reader and software

- **No awareness promotion**

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





# 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
- Special target: **ten-fold** increase of eID users (400,000 in 2009)

arvutikaitse





## 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**



id.ee

Windows Internet Explorer window showing the ID.ee website. The address bar contains "id.ee". The page title is "ID-kaart - uue ajastu isikutunnistus". The main navigation bar includes: [Avalaht](#), [ID-kaart](#), [Kasutusala](#), [Tarkvara](#), [Arandajale](#), [ID-projekt](#), [ID-koolitus](#), and [Abi](#).

The page features three main sections:

- Saa e-kodanikuks!**
  - Hangi ID-kaart
  - Hangi ID-kaardi lugaja
  - Paigalda tarkvara
  - Kontrolli sertifikaate
  - Vaata veebikoolitust
- Vajad abi?**
  - ID-kaardi abikeskus
  - Probleemileidja
  - Teadmistehaas
  - Kusi abi
- Teenused!**
  - Isikuvastus internetis
  - Digitaalkirjastamine
  - ID-Pilet
  - ID-blogis teenuste kohta

The **idBlog** section is titled "Kõik ID-kaardiga seonduv" and features a post titled "ID.ee veebist uus versioon" by [Maar Parve](#), dated 29.03.2007. The post text reads: "Nagu ehk isegi lähele paned, oleme üllitanud uue versiooni ID-kaardi veebileheküljelt. Lilled ja pasunakooriga me seda välja kuulutanud veel ei ole, sest tööd on veebiga veel küll ja küll. Kuid sel nädalal..."

The right sidebar shows "Teemad blogis" with a list of topics: Üldine (1), Blogid (11), Tarkvara (1), E-hääletamine (1), and Teenused (2).



# Mobile-ID

- **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%)**



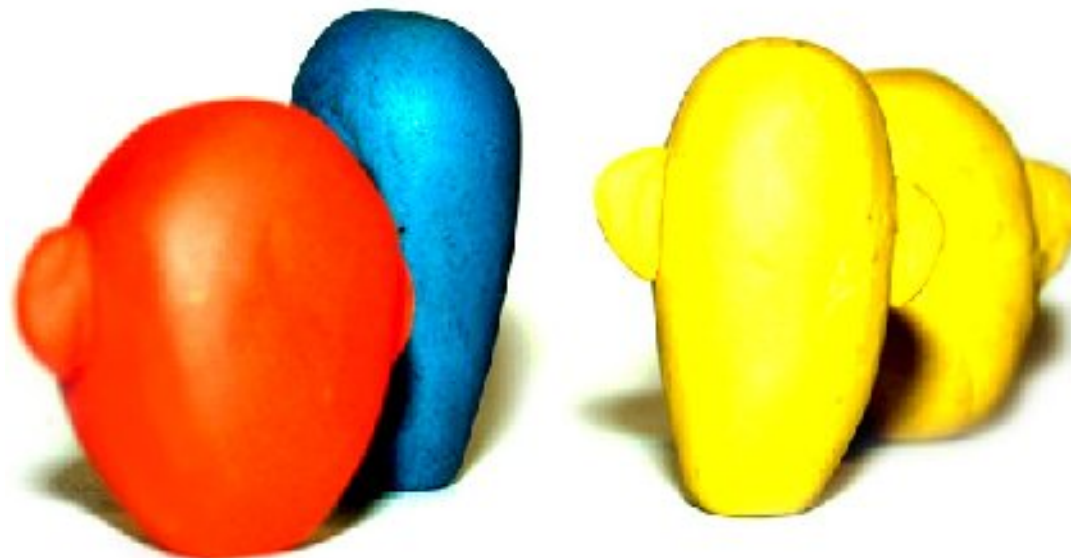


## Estonia: conclusions

- **Banks were not ready to go for full PKI before end of the ID-card roll-out**
- **PPP is crucial for pan-national cross-sector happiness**
- **C2G & G2C happens 1.4x/year !**
  - **This is not driver to e**
- **“People from street” seldom sign something**
  - **Not a e-driver either**
- **Start from major e-service providers!**

# How to Achieve International Interoperability in eAuthentication

*few thoughts*





## On eID Interop

- **Widely discussed topic**
  - One of main targets of EC i2010 program
- **Technically repeatedly proven**
  - IDABC Bridge/Gateway
  - European Bridge-CA (TeleTrust, Germany)
  - Euro-PKI, GUIDE, ...
  - [openvalidation.org](http://openvalidation.org)
- **We have organizational and legal issues!**



## Organizational issues

- **Paper-ID interoperability works!**
  - Miracles happen in border points
- **Organizational set-up of Paper-ID interop:**
  - ICAO sets standards
  - Continuous information exchange by network of MoIA-s to the borderguards etc.
- **Organizational set-up of eID interop ???**
  - Standards are not strict and not imposed
  - Continuous information exchange is missing completely



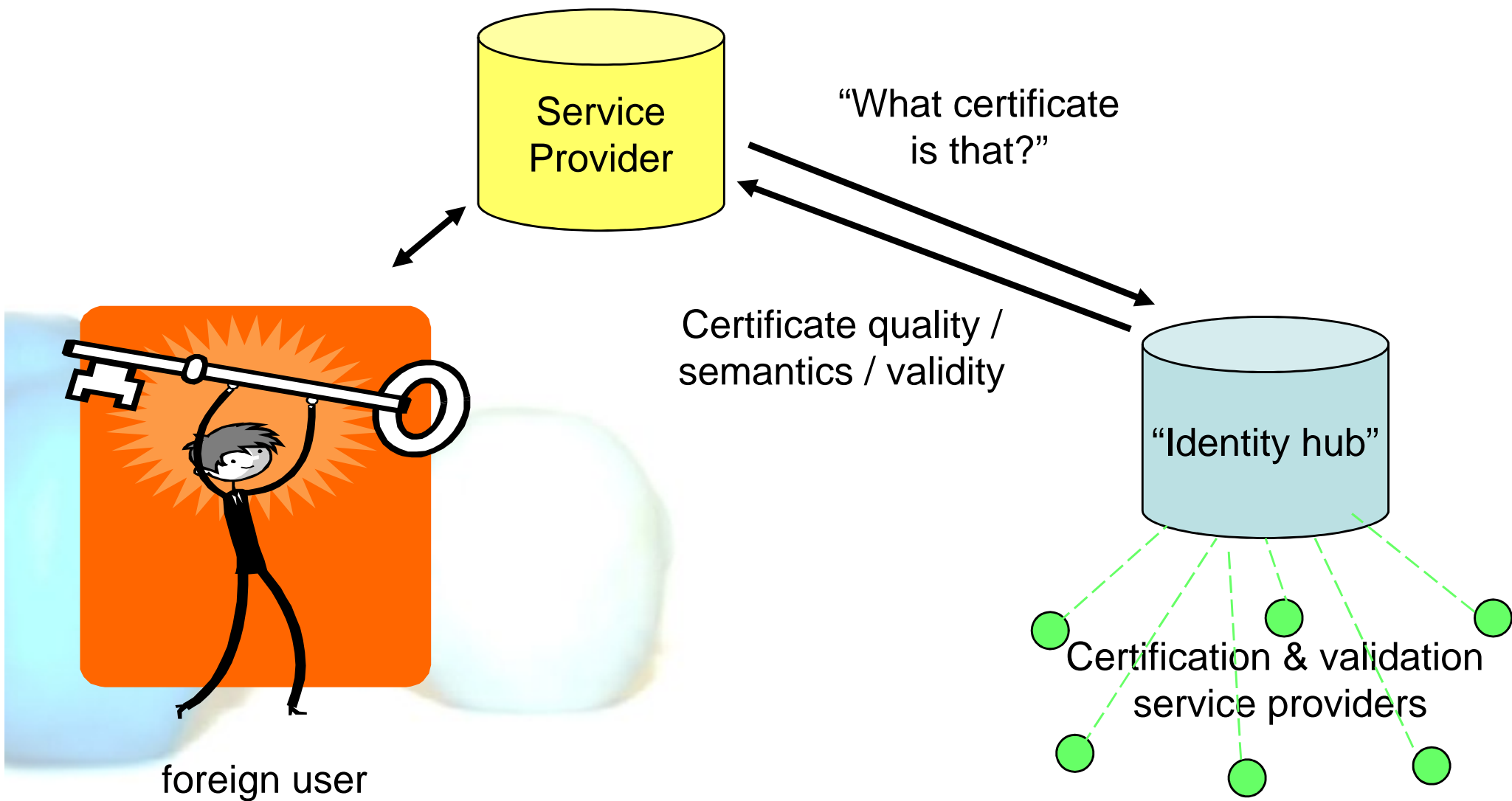
## Need for (foreign) eID info

- **Collecting and managing eID/service info is a daily job, not project-based**
- **What info is needed ?**
  - **Certificate validity (reference)**
  - **Certificate semantics**
  - **Certificate quality (!!!)**
    - Hardware token vs. software certificate
    - Quality of service provider & certificate
    - Context of certificate issuance
    - .....





# Desirable situation





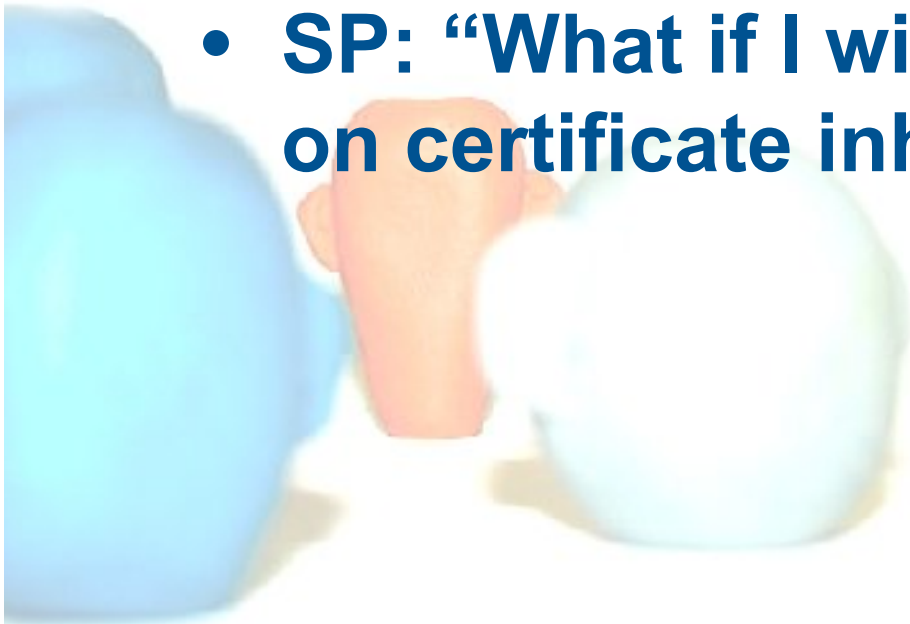
## Who will run the Indentity Hub ?

- **EC does not have mandate (yet)**
- **Single MS cannot afford it (to cover all Europe/World)**
  - **To tell the truth – there is no actual demand (read: need covered with money) for this**
  - **99% of transactions occur domestically**
  - **Uptake of national eID-s is still underway**
- **We need clear political agreement to create such a service in EU level**
- **In future we can envisage situation where every MS runs its own “e-borderguard”**



## Legal problems

- **There is no eAuthentication Directive**
- **National legislations hardly touch the subject**
- **SP: “What if I will make wrong assessment on certificate inheritance/validity ?”**





## Bottom Line

- **We need to create and distribute eID-s first**
  - Preferably PKI-based quality certs
- **Then teach holders of eID-s to use them**
  - Estonian case: penetration ≠ usage
- **But interop shall be addressed NOW**
  - Without vision, political wisdom and hard work there would never been such thing as EU



## Additional Information

- ID-card issuance [www.pass.ee](http://www.pass.ee)
- PKI & CA [www.sk.ee](http://www.sk.ee)
- ID-card & Mobile-ID [www.id.ee](http://www.id.ee)
- Digital signature software [www.openxades.org](http://www.openxades.org)



Contact point:

[\*\*tarvi@sk.ee\*\*](mailto:tarvi@sk.ee)