Security aspects of e-ID and Digital Signing

Guarantee to Trusted Electronic Procedures

ega.ee

Raul Rikk
Head of National Cyber Security Domain

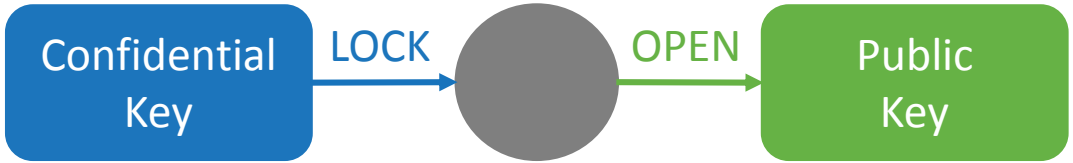
HOW SECURE IS MY PASSWORD?

ENTER PASSWORD

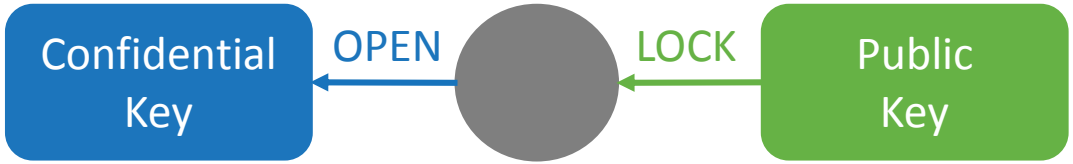
Public Key Cryptography

PRINCIPLE

One way calculation (**encryption**) is easy, other way calculation is time consuming (**decryption**)



Digital signature solution



Authentication solution

Encryption solution

Electronic Trust Services

ega.ee

1 WEBSITE AUTHENTI-CATION

2 USER e-ID

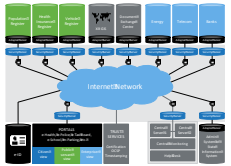
CREATION OF THE DOCUMENT

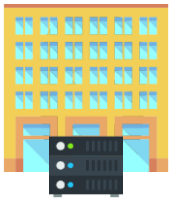
3 e-SIGNATURE / SEAL

4 e-TIME STAMP

5 SECURE DELIVERY

6 PRESER-VATION





Check if the website really belongs to the owner

Authenticate yourself using an e-ID

Signing or sealing the document

Proof of submission of the document in due time

Secure delivery with confirmation of receipt

Secure storage of the documen-tation

How hard is to break cryptosystem RSA 2048

Parameter	Classical computer	Quantum Computer
Working time	10 years	24 hours
Hardware size	Server farm 60% of Europe	1 room
Price	10^{17} … 10^{18}	10^{11}
Is the technology available?	Yes	Not yet

U.S. GDP in 2015 was ca $ 18 X 10^{12}

Source: Jeffrey Morris. Implications of Quantum Information Processing On Military Operations. www.cyberdefensereview.org/2015/05/29/quantum/

ega.ee

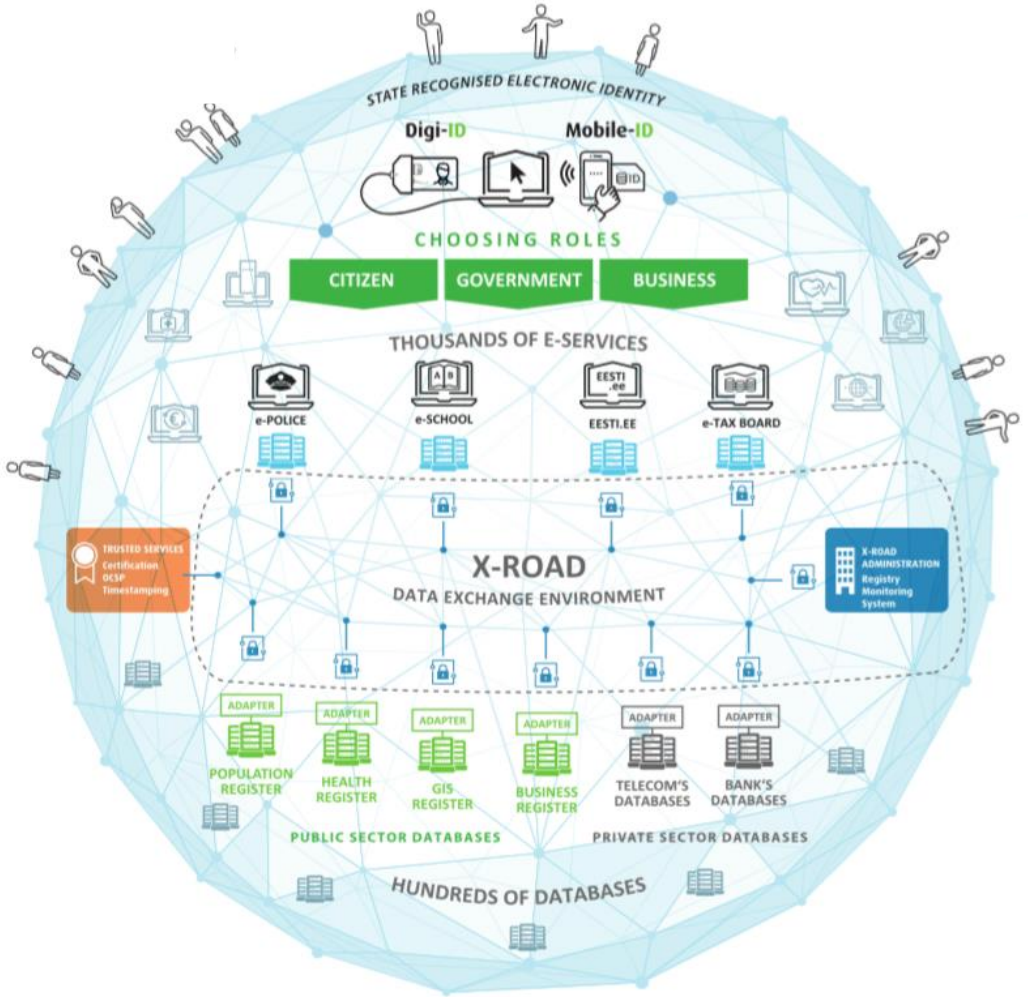
Digital ID and Signature since 2000

Active cards: 1 247 319
Authentications: 353 164 202
Signatures given: 221 400 892

ega.ee

Estonian Secure Internet Model

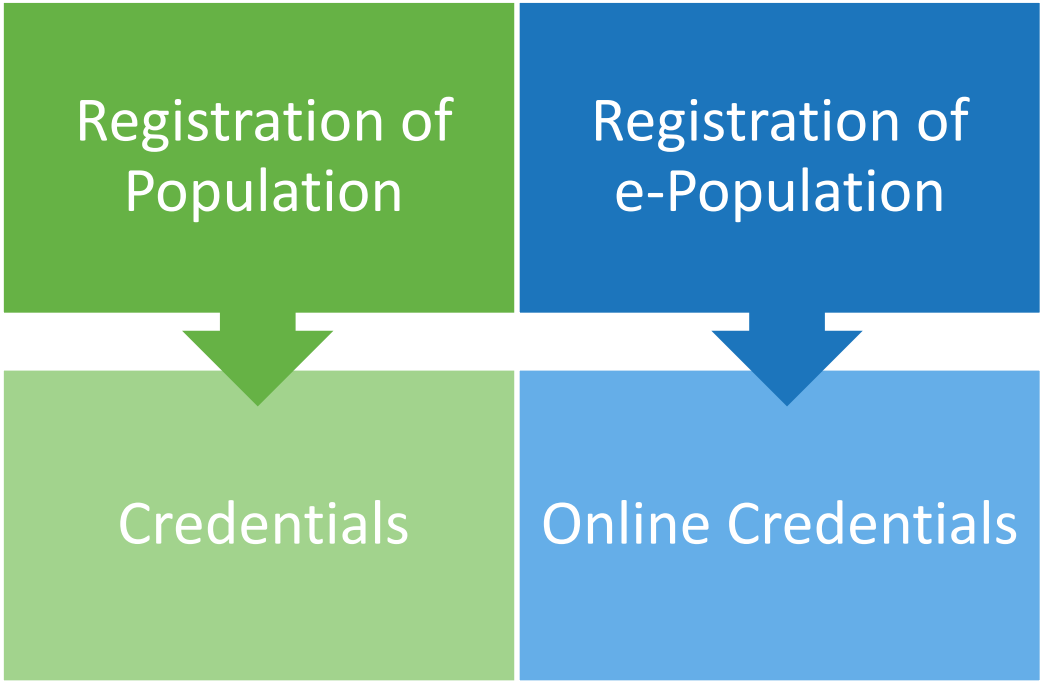
- Centralised electronic Identity
- Role-based access
- Decentralised architecture
- No duplicated databases
- Environment for secure data exchange



ega.ee

Identity Management

Regular and Online



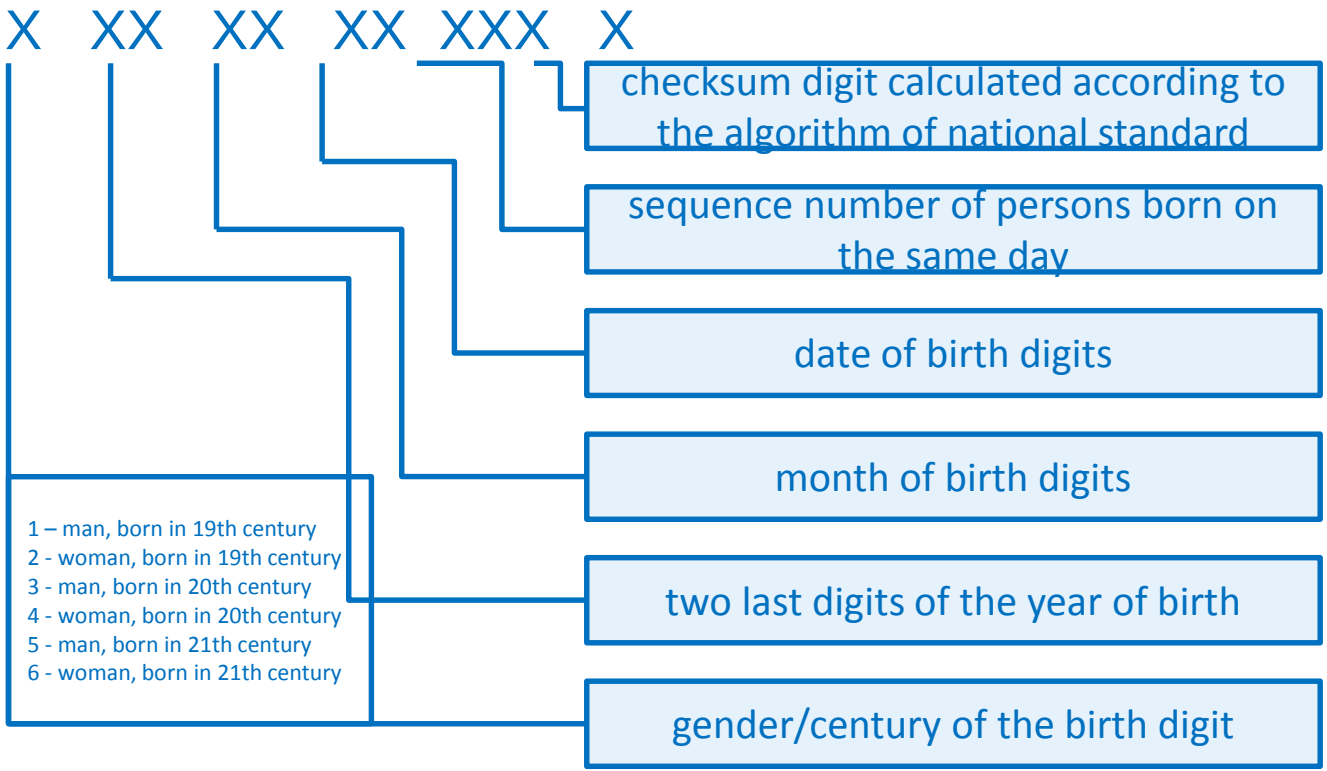
The Estonian identity system is established around the persistent life-long ID

Personal Identification Code (PIC)

Formation of PIC is based on the Estonian Standard EVS 585:2007 „Personal Code. Structure“ and the Population Register Act

Personal Identification Code

The 11-digit PIC consists of:



Digital Identity Management Principles

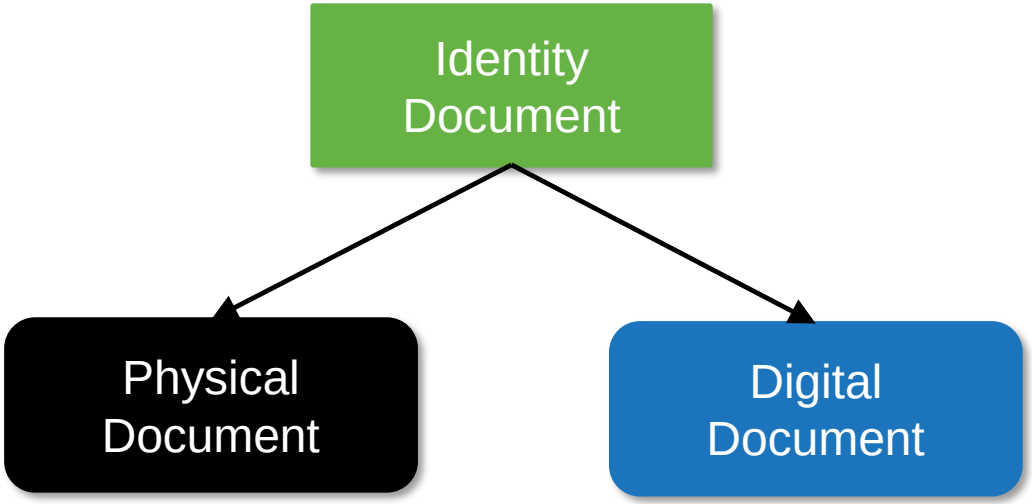
State monopoly and responsibility to identify a person, confirm the identity and issue certificates on identity documents

Principle of "one person = one identity”

Public verification of certificates via the personal identification code

Electronic Identity Documents and Related Services

ega.ee



- Passport
- ID card
- Residence permit card

- ID card
- Digi ID / e-resident’s card
- Residence permit card
- Mobile ID

Digital Document

- Identity Documents Act §3:

A document which is prescribed for digital identification of a person (hereinafter a digital document) is a document prescribed for identification of a person and verification of identity in an electronic environment.

Entry into force 30.07.2009

Estonian Identity Card

- Valid max 5 years
- Compulsory ID document from 15 years age

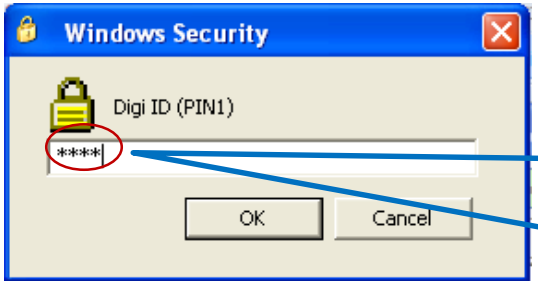
IDcard = Medium of Digital Identity

visual identification of a person

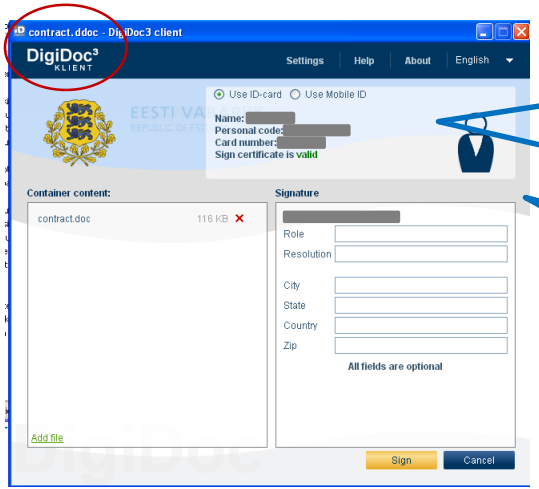
digital identification of a person

personal unified e-mail address

IDcard as a travel document



IDcard as a “key”: to e-services



digital signature

secure messaging: encrypting and decrypting

ega.ee

What Is Inside the Chip?

- Cryptoprocessor
- Personal data file
- Certificate for authentification along with e-mail address Forename.Surname@eesti.ee
- Certificate for digital signature

Digital Signature - Concept

- Legally binding
- Equivalent to what we are doing on paper
- Public sector is obliged to accept digitally signed documents
- All relations: G2G, G2B, G2C, B2C

Trust services in Estonia

until 1 July 2016

In Estonia trust services were regulated with the

Digital Signature Act

Since 2000

(amended 11 times)

2 services were defined:

1. Certification service
2. Timestamp service

EU e-IDAS Regulation from July1, 2016 + Estonian e-ID and Trust Services Law from Oct 26, 2016

EU electronic trust services:

1. Electronic signatures
2. Electronic seals
3. Time Stamping
4. Electronic registered delivery service
5. Website Authentication

Trust Services Providers in Estonia

1. **Certification Centre** – certification service and time stamping service

2. **Guardtime** – time stamping service

Trust services Management in Estonia

1.

Register for trust service providers – an entity in the register can provide electronic trust services

Responsible processor - The Ministry for Economic Affairs and Communications

Authorized processor – The Technical Regulatory Authority

Trust services Management in Estonia

2.

In order to become a trust service provider, an audit of the entity must be carried out.

Regulation “**Procedure for Auditing Certification Service Provider’s Information Systems**”

- Auditor could be a physical person with an appropriate certificate (ISACA – CISA).
- Audit is ordered by the Service Provider
- Auditor must get all relevant

Trust services Management in Estonia

3.

The Technical Regulatory Authority creates the root certificate and signes the service certificates of the trust service providers

Trust services Management in Estonia

4.

Trust service providers:

- Issue personal or organisations' certificates for authentication, e-signatures, and e-seals.
- Provide validity confirmation service
- Publish certificate revocation lists

Trust services Management in Estonia

5.

Trust service providers must order an audit once per year and provide the result to the authorised processor of the register

Audit

1. **Professional care** in order to ensure high quality and safe service
2. The **compliance of information system** with Digital Signatures Act, the Personal Data Protection Act and other legislation
3. The **compliance of information system, including the organization and arrangement of work** with documented requirements for certification or timestamping principles
4. **Fulfilment of obligations** in accordance with the Digital Signatures Act

Audit

5. The **compliance of the certification principles and security measures** with the standards EN 319 401, EN 319411-2 and EN 319411-3 or other equivalent
6. The **compliance of time-stamping service provider and its information system** with the ETSI TS 102 023, or other equivalent
7. The **compliance of the information system's security** with the ISO / IEC 27001 or other equivalent
8. The **compliance of information system** with other relevant legal acts.

Thank You

e-Governance Academy
Tõnismägi 2, Tallinn, Estonia
www.ega.ee

Raul Rikk
Head of National Cyber Security Domain
raul.rikk@ega.ee