

e-State

Monika Oit

Cybernetica Research Director,

Head of the Dept. of Information Security solutions

JRC Round Table 19.10.2007

Agenda

- ▶▶ Cybernetica ?
- ▶▶ e-State ?
- ▶▶ R&D
- ▶▶ Cooperation with JRC ?

Cybernetica?

1960 **Institute of Cybernetics
of the Academy of Sciences**

1997



BASIC RESEARCH:

▶▶ **Institute of
Cybernetics of
the Tallinn
University of
Technology**

▶▶ Public entity

APPLIED RESEARCH &
EXPERIMENTAL PART

▶▶ **Cybernetica**

▶▶ R&D company

▶▶ R&D personnell – 82

▶▶ Goal: 20% PhD

Research topics

- ▶ Cryptographic security attributes of electronic documents and their long-term maintenance
- ▶ Time stamping and digital notarisation
- ▶ Models of Threat Analysis and Their Applications in Practical Security Evaluation
- ▶ Methods of game theory and risk analysis in data security
- ▶ Cryptographic methods to achieve soundness of database queries
- ▶ Privacy-Preserving Data-Mining: Cryptographic Methods
- ▶ Software technology
- ▶ www.cyber.ee/english/rd/

Development:

- ▶▶ Communication security products (firewalls, VPN-s) – mainly for local market
- ▶▶ Digital Signature Technology
- ▶▶ Time Stamping service
- ▶▶ Integrated surveillance systems
- ▶▶ Intelligent marine navigation aids
- ▶▶ VHF VOIP solutions
- ▶▶ LED technology products (various signaling solutions)
- ▶▶ Large scale informations systems
- ▶▶ www.cyber.ee/english/products/

Governmental projects

(On contractual basis through public tenders only)

- ▶ **Electronic ID card**
 - ▶ **Digital signature and timestamping**
 - ▶ **Secure information exchange layer for the governmental databases (X-road)**
 - ▶ **E-voting**
-
- ▶ Included development of processes and organisation
 - ▶ Required changes in legal environment

e-State?

- ▶ Paperless governmental procedures?
- ▶ Internet-based public administration?
- ▶ 24/7 internet-based services for citizens
 - Issuing documents and certificates
 - Gathering applications
 - Gathering tax declarations
 - Providing information
- ▶ Government has 24/7 internet-based access to the information required for making decisions
- ▶ Governmental databases have to be on-line accessible for officials and for citizens

Security of the e-State

- ▶ e-Kingdom versus e-Democracy
- ▶ Security problems that arise when the governmental databases are opened for a widespread electronic access
- ▶ e-State architecture
- ▶ Electronic ID card as the solution for user authentication

(Headings from MSc thesis)

Test-site Estonia? E-stonia?

- ▶▶ Population: 1.35M
- ▶▶ Internet usage: 61%
 - In public service 99%
- ▶▶ Internet banking: 92%
- ▶▶ Mobile penetration: > 90%
- ▶▶ 1000+ Free Internet Access points

- ▶▶ PKI penetration: >75%
- ▶▶ Biggest national eID card roll-out in Europe !

ID card

▶ Compulsory for all residents

▶ Technical data:

- Infineon SLE66CX320P chip
- 32KB EEPROM
- Orga Micardo 2.1 operating system

▶ Contains:

- Personal data file (same data is printed on card)
- Key and certificate for authentication (along with e-mail address Forename.Surname@eesti.ee)
- Key and certificate for digital signature



Digital Signature Act

- ▶▶ Regulates only digital signatures used for evidentiary purposes (qualified signatures)
- ▶▶ In public relations, digital signatures are used as described in the DSA
- ▶▶ In private relations, digital signatures are used as agreed by the parties
- ▶▶ Several certification and time stamping service providers (CSP, TSP) allowed with different quality of service

X-Road project: goals

- ▶ To build an infrastructure that would allow effortless access to the data in state registries without compromising the security of the data
- ▶ Impact to the existing systems should be minimized
- ▶ Required security properties
 - Evidentiary value, authenticity, integrity
 - Availability
 - Confidentiality (restricted data, sensitive personal data)

Current state

- ▶▶ X-Road is secure message exchange system based on SOAP protocol
- ▶▶ X-Road is used for
 - interconnecting Estonian governmental agencies and databases
 - providing services for citizens
- ▶▶ X-road solution: scalable and efficient PKI for inter-organizational communication

E-voting

▶▶ Initial research 2001 stated:

- No perfect solutions for e-voting yet
- It could be done using some simplifications
- There are quite serious security risks

▶▶ But the project was started -

▶▶ Risk analysis 2003

- there are fundamental risks which are "out of control, out of scope" for e-voting and which need to be accepted

▶▶ Requirement specification 2003

Legal foundation

- 1) voter can use internet for voting;
- 2) voter is authenticated using **ID-card**;
- 3) voter confirms his selection with **digital signature**
- 4) e-voting takes place during absentee voting
i.e. days 6.-4. before the Election Day;
- 5) e-voting is not allowed before **2005.a.**

Voter registration

- ▶▶ Missing
- ▶▶ Population register is used to get voter lists
- ▶▶ All citizen (residents) should register their place of living in **central population register**
- ▶▶ Only voters with **registered addresses** are eligible

Main Principles

- ▶▶ All major principles of paper-voting are followed
- ▶▶ E-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

Simple process:

- ▶ Encrypt vote - sign - anonymise - decrypt
 - Fetch a candidate list
 - Pick a number, encrypt (RSA), sign (RSA), send it in
 - Check validity, remove signature, store the vote
 - Aggregate (decrypt + count) results, publish
- ▶ Encryption = single keypair, distributed with appl.
 - private key is secured by HSM, access control is N of M
 - private key is backed up into another HSM
- ▶ Signing = ID-card signature

Security?

- ▶▶ Too complex security measures are not understood, not deployed, not configured
- ▶▶ Security requirements in IT solutions:
 - minimal functionality
 - avoid unnecessary features
 - design goal – simplicity
- ▶▶ Develop also procedures and organisation
- ▶▶ Existing security infrastructure helps sufficiently
- ▶▶ More attention to cognitive and social sciences!

Cooperation with JRC ?

▶▶ The Institute for the Protection and the Security of the Citizen (IPSC)

Research Units:

- Support to external security (SES)
- Maritime Affairs (MARE), especially Maritime Surveillance (MASURE)
- Sensors, radar technologies and cybersecurity (SERAC), especially Border Security (BORSEC) and Security for Critical Networked Infrastructures (SCNI)

Cooperation with JRC ?

▶▶ The Institute for Prospective Technological Studies (IPTS)

Information Society Unit:

- Supporting the formulation and implementation of Information Society strategies, policies and regulations, with a view to contributing to a competitive, innovative and inclusive European Information Society.
- Foresighting and assessing the contribution of ICT to improve social inclusion, public services and the overall quality of life

Thank you for your attention!

Questions, comments...

monika.oit@cyber.ee

www.cyber.ee/english/