eID Interoperability for PEGS

NATIONAL PROFILE ESTONIA

November 2007

This report / paper was prepared for the IDABC programme by:

Author's name: Jos Dumortier - Hans Graux, time.lex

Company's name: Siemens - time.lex

Company's address (optional):

Company's logo (optional)

Contract No. 1, Framework contract ENTR/05/58-SECURITY, Specific contract N°3

Disclaimer

The views expressed in this document are purely those of the writer and may not, in any circumstances, be interpreted as stating an official position of the European Commission.

The European Commission does not guarantee the accuracy of the information included in this study, nor does it accept any responsibility for any use thereof.

Reference herein to any specific products, specifications, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favouring by the European Commission.

All care has been taken by the author to ensure that s/he has obtained, where necessary, permission to use any parts of manuscripts including illustrations, maps, and graphs, on which intellectual property rights already exist from the titular holder(s) of such rights or from her/his or their legal representative.

This paper can be downloaded from the IDABC website:

http://europa.eu.int/idabc/
http://ec.europa.eu/idabc/en/document/6484/5938

Executive summary

The project eID Interoperability for PEGS aims to propose a solution to the legal, technical and organisational issues related to the creation of an interoperable Pan-European identity management infrastructure. The EU Member States, Candidate Countries and EEA Countries are introducing more sophisticated ways to manage identities in the eGovernment area. Different member states are implementing different structures as their identity management solution. The main challenge for the eID Interoperability for PEGS project is to propose a general architecture that, while taking into account the existence of different models, is able to cope with them by obtaining the final goal of interoperability.

The project should conclude with several different proposals how to build interoperability without affecting member states' own existing infrastructures.

This document describes the current situation regarding the use of electronic authentication means in Estonian eGovernment applications.

Table of Contents

1 Documents

1.1 Applicable Documents

[AD1]	Framework Contract ENTR/05/58-SECURITY

1.2 Reference Documents

[RD1]	eGovernment in the Member States of the European Union – 5th Edition – May 2006 http://ec.europa.eu/idabc/servlets/Doc?id=24769
[RD2]	European Electronic Signatures Study http://www.law.kuleuven.ac.be/icri/itl/es_archive.php?where=itl
[RD3]	DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures http://europa.eu.int/information_society/eeurope/i2010/docs/esignatures/esignatures_en.pdf
[RD4]	Decision 2003/511/EC of 14 July 2003 on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council, OJ L 175, 15.7.2003, p.45 http://europa.eu.int/eur-lex/pri/en/oj/dat/2003/l_175/l_17520030715en00450046.pdf
[RD5]	DIRECTIVE 2004/18/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_134/l_13420040430en01140240.pdf
[RD6]	IDABC Work Programme Third Revision http://ec.europa.eu/idabc/servlets/Doc?id=25302
[RD7]	DIRECTIVE 2004/17/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 31 March 2004 coordinating the procurement procedures of entities operating in the water, energy, transport and postal services sectors http://europa.eu.int/eur-lex/pri/en/oj/dat/2004/l_134/l_13420040430en00010113.pdf

2 Glossary

2.1 Definitions

In the course of this report, a number of key notions are frequently referred to. To avoid any ambiguity, the following definitions apply to these notions and should also be used by the correspondents.

- *Entity:* anyone or anything that is characterised through the measurement of its attributes in an eIDM system. This includes natural persons, legal persons and associations without legal personality; it includes both nationals and non-nationals of any given country.

- *eIDM system*: the organisational and technical infrastructure used for the definition, designation and administration of identity attributes of entities. This Profile will only elaborate on eIDM systems that are considered a key part of the national eIDM strategy. Decentralised solutions (state/region/province/commune…) can be included in the scope of this Profile if they are considered a key part of the national eIDM strategy.

- *eIDM token (or 'token')*: any hardware or software or combination thereof that contains credentials, i.e. information attesting to the integrity of identity attributes. Examples include smart cards/USB sticks/cell phones containing PKI certificates, …

- *Authentication*[1]: the corroboration of the claimed identity of an entity and a set of its observed attributes. (i.e. the notion is used as a synonym of "entity authentication").

- *Authorisation*: the process of determining, by evaluation of applicable permissions, whether an authenticated entity is allowed to have access to a particular resource.

- *Unique identifiers*: an attribute or a set of attributes of an entity which uniquely identifies the entity within a certain context. Examples may include national numbers, certificate numbers, etc.

- *Official registers*: data collections held and maintained by public authorities, in which the identity attributes of a clearly defined subset of entities is managed, and to which a particular legal of factual trust is attached (i.e. which are generally assumed to be correct). This includes National Registers, tax registers, company registers, etc.

[1] For the purposes of this Profile, the notion of authentication is considered to be synonymous with 'entity authentication', as opposed to 'data authentication'. The notion of 'identification should be avoided to avoid confusion.

- *eGovernment application*: any interactive public service using electronic means which is offered entirely or partially by or on the authority of a public administration, for the mutual benefit of the end user (which may include citizens, legal persons and/or other administrations) and the public administration. Any form of electronic service (including stand-alone software, web applications, and proprietary interfaces offered locally (e.g. at a local office counter using an electronic device)) can be considered an eGovernment application, provided that a certain degree of interactivity is included. Interactivity requires that a transaction between the parties must be involved; one-way communication by a public administration (such as the publication of standardised forms on a website) does not suffice.

- *eSignature*: data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication with regard to this data. Note that this also includes non-PKI solutions.

- *Advanced electronic signature*: an electronic signature which meets the following requirements:

  (a) it is uniquely linked to the signatory;

  (b) it is capable of identifying the signatory;

  (c) it is created using means that the signatory can maintain under his sole control; and

  (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;

  Again, this definition may cover non-PKI solutions.

- *Qualified electronic signature*: advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device, as defined in the eSignatures Directive[2].

- *Validation*: the corroboration of whether an eSignature was valid at the time of signing.

[2] See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML

2.2 Acronyms

A2A ..... Administration to Administration

A2B ..... Administration to Businesses

A2C ..... Administration to Citizens

CA ..... Certification Authority

CRL ..... Certificate Revocation Lists

CSP ..... Certificate Service Provider

eID ..... Electronic Identity

eIDM ..... Electronic Identity Management

IAM ..... Identity and Authentication Management

IDM ..... Identity Management

OCSP ..... Online Certificate Status Protocol

OTP ..... One-Time Password

PKCS ..... Public-Key Cryptography Standards

PKI ..... Public Key Infrastructure

SA ..... Supervision Authority

SOAP ..... Simple Object Access Protocol

SCVP ..... Server-based Certificate Validation Protocol

SSCD ..... Secure Signature Creation Device

USB ..... Universal Serial Bus

TTP ..... Trusted Third Party

XAdES ..... XML Advanced Electronic Signature

XML ..... eXtensible Markup Language

XML-DSIG ..... XML Digital Signature

3 Introduction

3.1 General status and most significant eIDM systems

The most important eIDM system in Estonia is based on the Estonian ID-card, a mandatory electronic identity card that is intended to facilitate access to eGovernment services for all Estonian citizens and residents as well as offering access to a variety of other services.

The ID-card is mandatory for Estonian citizens from age 15 and up (younger than 15 have an option to apply for an ID-card) and all aliens residing permanently in Estonia on the basis of a valid residence permit or right of residence irrespective of their age. The ID-card has three main functions: visual identification, authentication and digital signing. The card contains a chip holding a personal data file and two certificates: one for authentication purposes, and one for qualified digital signatures.

The ID-card certificates are linked to the various registers through the Personal Identification Code (hereinafter: PIC), which functions as a unique identifier for Estonian citizens and residents in eGovernment services. The PIC is included as a serial number on the certificates of the eID card. The PIC is provided by the Population register of Estonia.

Although the ID-card is an important eIDM system, it is not the most used system today. Estonia has relatively long tradition of Internet banking and nearly everyone has access to it. The main method to access Internet banks is using password cards with 24 codes on it (usage of ID-card and PIN-calculators is estimated below 15% today). Banks are providing authentication services to 3rd parties (~30 systems), including eGovernment systems. It is estimated that over 90% of eGovernment transactions requiring authentication is performed only thanks to the authentication service from Internet banks. The PIC has also here the function of unique identifier in the authorisation process.

This situation is going to change in a few years – banks are going to drop authentication service to 3rd parties and reduce usage of password cards by gradually lowering transaction limits. More information on this expectation can be found in section G – Future Trends.

Identification information with regard to legal persons is provided through the Centre of Registers and Infosystems (http://www.eer.ee/index_eng.phtml). Although companies and organisations have a unique register code, there is no such thing as “eID of the company”. All transactions with regard to legal persons are performed by physical persons using their personal eID; corresponding access rights are maintained separately.

These systems will be discussed in greater detail below.

From a practical perspective, usage and uptake can be summarised as follows:

eIDM system	Potential user base	Actual penetration	Actual use
National ID-card	Estimated at 1.1 million (around 80% of the population)	1072849 cards issued, 935786 active (13.05.2007)	2847071 authentications (checked with OCSP), 2305290 signatures (13.05.2007)
Bank Eid	Estimated at 1.1 million	Estimated at 1.1 million	No public statistics are available

3.2 Background and traditional identity resources

3.2.1 General ICT coordination in public administration and e-Government infrastructure

In Estonia the Ministry of Economic Affairs and Communications is responsible for the general ICT coordination – more precisely the Department of State Information Systems. The tasks of the department include the coordination of state IT-policy actions and development plans in the field of state administrative information systems (IS): state IT budgets, IT legislation, coordination of IT projects, IT audits, standardization, IT procurement procedures, and international cooperation in the field of state IS.

The Estonian Informatics Centre, which is a subdivision of the ministry, is responsible for the coordination and implementation of the development of state registers, computer networks and data communication, standardization, IT public procurement, monitoring Estonian IT situation, etc. The Estonian Informatics Centre is also responsible for the development of the environment for eGoverment services (including X-Road, the Citizen portal etc).

There are also IT councils of ministries and IT councils of counties. In addition, there is the Estonian Informatics Council, which is a government committee of experts and the implementing body in the general coordination of state information policy.

The backbone of the eGoverment environment is the X-Road network of distributed and central servers. X-Road is a platform-independent secure standard interface between databases and information systems (to connect databases and information systems) of the public sector, which has a common user interface and a standard authentication system. The X-Road enables secure access to nearly all Estonian national databases; ensures the necessary availability, integrity and confidentiality of electronic document exchange over the Internet servicing Estonian residents, the state and local government authorities. In this environment, information systems provide and also consume different e-services. In 2006, nearly 163 736 people (i.e. more than 12% of the Estonian population) used X-

Road services. The number of different enterprises and public bodies among X-Road users during the same time was 25 752. There were 65 databases offering their services over the X-Road in 2006.[3]

Direct communication between the citizens/residents and the eGovernment environment is established over a set of communication portals: the Citizen Portal (www.eesti.ee), the Entrepreneur Portal (www.eer.ee) and the Civil Servant Portal for central and local government agencies. The Citizen Portal serves as the main channel for mediating eGovernment services between citizens/residents and the government. In Citizen Portal a person can check his or her data in the various national databases and fill out application forms (for example health insurance card), digitally sign and send documents, and receive for example information about planned electrical supply interruptions in the specific area. As already stated above the citizen/resident has via the Citizen Portal access to his/her personal data in the Estonian databases. According to the Estonian personal data protection law every Estonian citizen has the right to know what kind of data the government has collected about him or her. For example it is possible to check the data in Commercial register etc.

X-road and portals are accessible for citizens/residents through authentication with the ID-card or by use of authentication services provided by the Estonian commercial banks. Please find more information about the ID-card and related PKI infrastructure in section D.

The Estonian commercial banks (Hansapank, SEB Eesti Ühispank, Sampo Pank, Krediidipank and Nordea pank) play an important role in the development of eGovernment. As already mentioned they provide portals connected to the eGovernment environment with the authentication service for these persons who do not possess an ID-card yet or find this way more familiar. Some services are charged for and a solution has been developed for paying these charges through the banks.

The further information: www.mkm.ee (Ministry of Economic Affairs and Communications), www.riso.ee (Department of State Information Systems), www.ria.ee (Estonian Informatics Centre).

3.2.2 Coordination regarding eIDM

The issuing of PKI enabled ID-cards and management of related matters is the responsibility of the Citizenship and Migration Board (hereinafter: CMB). The CMB is a state authority acting under the Ministry of the Interior. The main task of the CMB includes the determination of persons living in Estonia either as Estonian citizens or aliens and the issuing of identity documents. The CMB issues the following identity documents: identity cards (hereafter: ID-cards), Estonian citizens' passports, aliens' passports, temporary travel documents, seafarers' discharge books, certificates of record of service on ships and refugees' travel documents. On the basis of data collected during documentation and issuance of identity documents the CMB maintains the Database of identity documents issued by the CMB.

The issuance process of ID-cards and the development of PKI infrastructure is managed through a tight cooperation with public and private agencies. The production and personalization of ID-cards, as

[3] Information Technology in Public Administration of Estonia. Yearbook 2006. http://www.riso.ee/en/pub/2006it/index.php?mn=10&prnt=6

well as certification services are outsourced by service contracts to TRÜB AG. TRÜB AG has two sub-contractors: AS Sertifitseerimiskeskus (hereinafter: SK) and Trüb Baltic AS. TRÜB AG as main contractor is producing ID-cards, which are then personalized by Trüb Baltic AS. SK, founded by two major Estonian banks Hansapank and SEB Eesti Ühispank and two telecom companies Elion and EMT, functions as a certificate service provider and validation authority, and maintains the electronic infrastructure necessary for issuing and using the card, and develops the associated services and software.

SK has acted as a certificate service provider for ID-cards since 2001. Since then, SK has become *de facto* coordinator and excellence centre on PKI matters and eIDM in Estonia. Public sector has even delegated some responsibilities of international representation of Estonia in eID/eSign matters to SK. SK is a nationally accredited provider of certification and time stamp services in Estonia. Its spheres of activity include development of software relation to the certification and time stamp services as well as the development and administration of e-ticketing and e-transaction systems.

In March 2006, an inter-institutional working group was established under the Ministry of Economic Affairs and Communications with an aim to ensure co-ordinated development of applications related to ID-card based electronic identity and digital signing as well as of solutions connected to PKI. The working group has been assigned the task of solving respective technical, legal and organizational issues as well as making relevant proposals. The Working Group consists of interested parties from various governmental agencies and from private sector (banks, telecoms). A group of this kind was formed for drafting the Digital Signature Act in 1997-2000 and was a useful forum for discussing national PKI matters.

See for more information: www.id.ee, www.sk.ee (AS Sertifitseerimiskeskus), www.mig.ee (Citizenship and Migration Board), www.trueb.ch (TRÜB AG), www.trueb.ee (Trüb Baltic AS).

3.2.3 Traditional identity resources

The main IDM systems traditionally used are ID-cards, the database of identity documents issued by CMB and the population registry regarding the PIC.

ID-cards

The detailed information about ID-cards and certificates is available in sections C.2 and D.

The database of identity documents issued by the CMB

The reliability of ID-card is based on the chain of documentation (application processing, personalization etc), where the actual physical document is one of the most important links. The important role in the issuance process of ID-cards and related identity management is playing the database of identity documents issued by the CMB (See the list of documents issued by CMB in

section C.2). The legal base is the decree of the general director of Estonian Citizenship and Migration Board from 19th March of 2003 no 72.

This database contains the information on all issued identity documents (including the ID-card) and relevant data of document users and document applicants that are necessary for the issuance of identity documents to the eligible persons. The main purpose is to ensure that the eligible person has the appropriate document (included by identification of the person and check of the right to the identity document). The database also contains the data of all valid and non-valid documents and document applications the person has submitted. Since 2001 the face images of document users are entered into the database. Most of the population is documented, therefore it is possible to verify the information submitted by applicants against the entries of the database and check his/her identity. If the applicant has not yet had a document issued by the CMB, he/she needs to provide additional source documents proving the applicant has the right for the identity document (citizenship).

The identity documents for aliens are issued on the basis of his/her residence permit or the right of residence in Estonia. So the database has a connection with national Aliens' registry (CMB is the responsible authority).

The database consists of a central online database and a paper database (source documents etc). The issuance process (including logistics etc.) and personalization process of ID-card is based on and monitored by the online database.

The following persons have the right to access the data:

1) an adult has the right to access data entered to the database on him or her and his or her minor children and persons under his or her guardianship;
2) state agencies and local government agencies and legal or natural persons for the performance of public duties;
3) natural and legal persons with legitimate interest;
4) agencies and persons of foreign state in accordance with the Vienna Convention.

The access to data and data processing shall follow the personal data protection act.

Many state authorities (the Police Board, the Tax and Customs Board etc), notaries etc identify persons or check the validity of the identity documents on the basis of information included in the databases. The identification queries are made electronically via X-road. Also citizens have access to data entered on them via X-road from the Citizens Portal.

Population Register

The Population Register generates and maintains the PIC. The Population register is the central national register containing the main information about natural persons (Estonian citizens and aliens who have obtained a residence permit or the right of residence). The Chief processor of the population register is the Ministry of the Interior. The main aim of the Population Register is to ensure the collection of the main personal data of Estonian citizens and aliens who have obtained residence permits in Estonia in a single database for the performance of functions of the state and local

governments provided by law upon the exercise of the rights, freedoms and obligations of persons, and the maintenance of records on the registration of population.

The Population register contains the personal data of the subject, data that are related to the personal data (data of all identity documents and vital events certificates), and also data preparing the status of the subject of population registry. The registry includes the following personal data: names, sex, date of birth, place of birth, PIC, citizenship, residence permit, place of residence and marital status. The data entered in the population register is the basis for other databases of the state and local government authorities which contain data on the subjects of the population register. Also the use of data on the subject of the population register upon performance of public duties shall be based on the data entered in the population register. The authorities, who collect these data for their services, receive and check these data from the population registry via X-Road (cross-usage of data).

The population registry is also issuing the PIC to other state authorities who have to document the person for the first time (usually by birth or issuance of the residence permit or the right of the residence). More detailed information about the PIC can be found in the section D.1.1 and D.2.3.

The data is collected and entered by different state and local government authorities, natural and legal persons. According to the Population register act[4] the persons submitting data to the population register are agencies and persons who issue documents defined in the population register act, and agencies and persons who perform data acquisition from documents issued prior to the introduction of the population register with regard to data which are entered in such documents and which are subject to entry in the population register. Data are required to be entered in the population register or to be transferred to the authorized processor to be processed upon the issuing, amendment and revocation of documents, if such data creates, amends or specifies personal data or data related to personal data subjects for entry in the population register.

The Population registry is a centralized single-level electronic database. Persons and authorities (for example: persons regarding their own data, local authorities, CMB, courts etc) can submit data by entering data in the population register online or by forwarding data through a data communication network.

The following persons have the right to access the data of Population register:

1) an adult has the right to access data entered in the population register on him or her and his or her minor children and persons under his or her guardianship;
2) state agencies and local government agencies and legal or natural persons for the performance of public duties;
3) natural and legal persons with legitimate interest;
4) agencies and persons of foreign state if such right is provided for in an international agreement or ensured in the specific cases by an order of the chief processor.

The chief processor has an obligation to issue only such data which the applicant has the right to receive or notify the data recipient of the restrictions on access to the data issued. The Population

[4] Population Register Act (2005), in English: http://www.legaltext.ee/et/andmebaas/ava.asp?m=022

register act contains more detailed requirements for the access to the abovementioned persons. Please see more detailed information in the Population register act.[5]

3.3 eIDM framework

3.3.1 Main eGovernment policies with regard to eIDM

Unique Personal Identification Code

The Personal Identification Code (hereinafter PIC) is a unique number assigned to every Estonian citizen and resident. The legal basis for assigning and using the PIC was established in 1992.

The 11-digit PIN consists of:

- gender/century of the birth digit (1)
- date of birth digits (2+2+2)
- three random digits (3)
- one checksum digit (1)

As we see, the PIC contains some privacy-related data – gender and date of birth.

The ID-card

A ministerial decision to introduce an ID-card was made in May 2000. First passports in Estonia were issued in 1992 with a lifetime of 10 years – it was a unique opportunity to renew the identification document system in Estonia by providing a new kind of document.

The decision was that the ID-card will be the mandatory (or: primary) identification document compulsory for Estonian citizens from age 15 and up (younger than 15 have an option to apply for an ID-card) and for all aliens residing permanently in Estonia on the basis of a valid residence permit or right of residence irrespective of their age. An alien receives an ID-card with the data of residence permit or right of residence. There are no separate residence permit cards. There are no sanctions for not having an ID-card, but the ID-card is provided as the "primary" identification document with the passport being optional.

It was decided that the ID-card will contain a contact chip with a personal data file (all data personalised to the visual card) and two certificates (subject to suspension on handover) – one for the

[5] Population Register Act (2005), in English: http://www.legaltext.ee/et/andmebaas/ava.asp?m=022

secure electronic authentication of persons and the second for creating a digital signature. More detailed information about certificates and their technical profile is in section D.3.

Until 2006, the maximum validity period of ID cards was 10 years, while the duration of certificates accounted for three years. ID-card users had to renew the certificates of the card several times during its validity period. As result of a change in the legislation introduced in 2006, ID-cards are issued since 1st of January 2007 with a maximum validity period of five years[6] with the duration of certificates covering the same period. The period of validity of certificates shall not exceed the period of validity of an identity card. The expiry of the period of validity of certificates shall not be the basis for the expiry of an identity card.

Deployment of this card has commenced in January 2001, and presently over 1 million cards have been issued (including ID-cards issued to aliens). The number of valid ID-cards by 1 January 2007 accounted for 910 207. Taking into account the population of Estonia (near 1,4 million) and the "addressable market" (people over 15 of age – roughly 1,1 million) one may say that the roll-out is completed.

Cards are issued by the Citizenship and Migration Board in cooperation with private sector. See information in section C.2 and D.4. The price of the card is for applicants approximately 10 EUR.

The physical card has the dimensions of ID-1 according to the ICAO specifications. The card contains:

1) on the front side of the card the card holder's signature and photo, and also name, PIC, birth time, sex, citizenship, card number, end of the date of card validity;
2) on the back side card holder birth place, card issuing date, residence permit details and other information (if applicable), card and holder data in machine readable zone (according to the ICAO standards).

All the above mentioned data except photo and handwritten signature are also present on the chip in electronic form, in a special publicly readable data file. The chip also contains two certificates, allowing the authentication of the citizen and the use of a qualified electronic signature and their associated private keys protected with PIN codes. The certificates contain only the holder's name and PIC. In addition, the authentication certificate contains the holder's unique e-mail address. Read more about certificates and their profiles in section D.3.

One specific goal to implement the eID was to improve government efficiency, since electronic authentication would allow the government to automatically retrieve the electronic information about the holder that it already has, thus reducing data redundancy and unnecessary form filling (the so called "authentic source" principle: there should be only one authentic source for each piece of information, to be reused by all applications).

[6] The period of validity of an identity card held by an alien shall not exceed the period of validity of his or her residence permit or the period of his or her right of residence.

It should be noted that, while the signature certificate is considered to be qualified, the authentication certificate has emphatically not been given this label. This choice was justified by concerns of legal certainty: the authentication certificate should not be used for signature purposes, and for this reason only the signature certificate is considered qualified. This way, parties are expected to take adequate precautions to ensure that the authentication certificate is not misused.

Certificates on the ID-card are activated upon handover of the card. The ID-card itself is also activated at issuance. Before this process the ID-card and certificates are not valid. When the card is issued, the receiver may also opt to suspend the certificates, so that the card can only be used as a traditional paper ID-card. Obviously, in this case the card offers no eIDM functionality to the holder. Generally, this option is not widely used.

More information can be obtained from http://www.pass.ee/2.html and http://www.id.ee.

Bank eID

The most popular method for authentication today is to use Internet bank authentication. Virtually all banks (5 major ones covering 99% of the banking customers) are providing authentication service to 3rd parties.

This works in practice as follows:

- the user logs into the Internet bank (using the appropriate method)
- the user selects “external e-service”
- user’s PIC is securely communicated to the e-service
- user continues work with selected e-service

There are basically 3 methods for logging into Internet bank:

- password cards (with 24 codes) – around one million cards issued
- PIN-calculators – estimated 50 000 in use
- ID-card – over one million issued

Password-based authentication is the most (estimated – 90%) used method for Internet bank logging today. It is considered relatively secure as these password cards are issued personally in the bank office. Trustworthiness of banks is generally considered as good. Considering this, it is not surprising that number of eGovernment services make use of the bank authentication.

Services like eTaxation and Citizen Portal are accessible through bank authentication. As a result, most (~86%) of the people declare their taxes via Internet. Citizen Portal represents a single point of access to ~70 governmental databases with more than 700 services.

Reasons behind popularity of bank authentication include:

- relatively early start of Internet banking in Estonia (1995) with early provisioning of authentication service to 3rd parties;

- large number of Internet bank users (nears to 100% for people between 16 and 74);
- simple to use – no special hardware (e.g. smartcard reader) or software (e.g. drivers) is needed.

Usage and trends of eIDM systems

It is obvious to everyone that ID-card-based authentication is more secure than using bank authentication, but the number of ID-card users is still low at the time being. It is up to every eGovernment service provider to decide about the security level of authentication and most of them support both (ID-card and bank eID) methods. Regional/local government authorities use the same eIDM resources as national ones.

As noted before, bank authentication is the most used authentication method today with password cards being overly popular. After "completion" of roll-out of the ID-card and with the rise of cyber-theft, banks have been starting to change their thinking and policies towards provisioning of the authentication services and use of password cards in general.

As a result, a co-operation agreement was signed between major banks, major telecom companies and the Government in May 2006 with code-name "Computer Protection 2009" (http://www.sk.ee/pages.php/02030201,1107). This initiative addresses general IT-security topics for end-users but with large emphasis on transition to PKI-based authentication methods.

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 2009)

It is expected that banks will cease provisioning of authentication service to 3rd parties by the 2nd half of 2008 and will gradually phase out password cards by lowering transaction limits in Internet banking.

3.3.2 Legal framework

The main legal acts concerning e-IDM systems are the Identity documents act[7], the Digital signature act[8] regarding ID-card certificates, the Population register act[9] and the Personal data protection act[10] regarding the PIC.

General regulations

There are no general regulations about authentication or legal acts which would define the hierarchy of the different authentication systems. Existing regulations are usually application specific or define the approved authentication systems in the specific area, but also these regulations are very laconic. For example, the government act which regulates the X-road environment[11] states that the access shall be enabled only to the authenticated user, which shall be authenticated: 1) in the case of the citizen/resident with the ID-card or via internet banking authentication service; 2) in the case of civil servant with the ID-card or via the information system of the authority; 3) in case of the information system, on the basis of the certificate of the security server of X-Road.

Certificates on the ID-card

The legal basis for the issuance and usage of certificates on ID-cards is the Identity documents act. Also the regulation in Identity document act is very laconic about the certificates and authentication with the ID-cards. According to clause 9 sub-section 5 of the Identity document act information which enables identification and signing and other digital data, the list of which shall be established by regulation of the Government of the Republic, may be entered in a document (including ID-cards). The Government regulation no 260 from 14th December 2006[12] defines the data entered on ID-cards. According to this government act ID-card shall contain the certificates that enable digital

---

[7] Identity documents act

Estonian (2006): https://www.riigiteataja.ee/ert/act.jsp?id=1042877

English: (2004) http://www.legaltext.ee/text/en/X30039K10.htm

[8] Digital signature act

Estonian: http://www.legaltext.ee/text/et/X30081K4.htm

English: http://www.legaltext.ee/text/en/X30081K4.htm

[9] Population register act (2005), in English: http://www.legaltext.ee/et/andmebaas/ava.asp?m=022

[10] Personal data protection act

Estonian: http://www.legaltext.ee/text/et/X70030.htm

English: http://www.legaltext.ee/text/en/X70030. htm

[11] The goverment regulation no 331 from 19th December 2003, only in Estonian: https://www.riigiteataja.ee/ert/act.jsp?id=688079

[12] The goverment regulation no 260 from 14th December 2006, only in Estonian: https://www.riigiteataja.ee/ert/act.jsp?id=12763871

authentication and digital signing, also personal keys that are corresponding to public keys that are generated into these certificates. The government regulation defines also the data set of each certificate and the validity of the certificates, also the obligation of the issuing authority to inform the document/certificates user about the validity of certificates. The obligation to inform about the nature of certificates, the related data processing (the citizen has to give his/her consent) and requirements for the secure usage for the user is not explicitly regulated in those legal acts, but the procedures are followed to fulfil the general requirements (for example about informing etc) stated in the Personal data protection act. For more information about the terms of use for ID-card certificates, see http://www.pass.ee/160.html. The terms of use for the ID-card shall be communicated to the ID-card applicant. The terms of use for the ID-card contain also references and requirements of the certification policy that shall be followed in certification and certification servicing procedures. See the certification policy of Estonian ID-card in more detail: http://www.sk.ee/pages.php/0203040504 (look for ESTEID-SK policy).

The Estonian legislation distinguishes between the authentication and digital signing. The general regulation (not application based) about digital signatures exists in the Digital signature act. The Digital signature act provides the necessary conditions for using digital signatures and the procedure for exercising supervision over the provision of certification services and time-stamping services. The Digital signature act was drafted in accordance with the European Councils regulation in EC 1999/93.

Regulations about the PIC

According to the Population register act, the population register is responsible for generating the PIC. There is no detailed regulation about generation, the regulation about generation and related data processing etc. is regulated in the government act (not available in English).

Use of the PIC is regulated with the Personal Data Protection Act which states in §16 that:

> *"Processing of a personal identification code is permitted without the consent of the data subject if processing of the personal identification code is prescribed in an international agreement, an Act or Regulation."*

As a result, almost all databases in all sectors (including private sector) would ask for permission to process the PIC and use PIC as a primary key in database records to identify persons. This makes cross-usage of the databases technically possible.

PIC is also included in certificates on the ID-card. From the beginning of issuance of ID-cards in January 2002, all active certificates are published in an LDAP directory. This has made possible for everyone to find out everyone's PIC by querying the public LDAP directory. This has caused lot of discussion in public resulting in amendment to the Identity Documents Act in June 2006 which now states that:

> *"…certificates can by publicly queried through the use of PIC"*

As a result, people are now required to know the PIC of the person in order to query his/her certificate from LDAP directory. This requirement was put in practice in December 2006 – almost five years after the PICs have been public through the use of LDAP. Till then, people still were able to collect information on PICs…

To further complicate the situation, there is a new amendment to the Data Protection Act in works in governmental level which would remove all restrictions from processing the PIC.

3.3.3 Technical aspects

As stated above, the ID1-shaped ID-card is based on PKI technology, and incorporates two certificates: one for authentication, and one for electronic signatures, with only the latter being considered as qualified. Each private key is dependent on the use of a different PIN-code. In addition, a single user-readable data file is on the card replicating data from the visual layer.

The physical card is a polycarbonate card containing a chip from ORGA having Micardo COS with a crypto-processor. As ORGA is not an active smartcard producer anymore the current supplies are about to exhaust in 2008. For that, preparations for the new card platform have been started. There has been developed a prototype on the current ESTEID card application on MultOS-compatible cards, so in all likelihood MultOS will be the next platform for Estonian ID-cards. It also means that card-specific software (middleware and card utility, see below) does not have to be (significantly) altered with the new platform.

There are no specific requirements for smartcard readers to be used with Estonian ID-card. Smartcard readers following PC/SC or CT-API standard are supported although CT-API (smartcard readers with pinpads) would require special attention in some cases.

Middleware for supporting standard interfaces to applications like MS Crypto API (CAPI) and PKCS#11 (aka Cryptoki) have been developed domestically. Support and responsibility for CAPI-supporting CSP (Cryptographic Service Provider) has been voluntarily taken by SK. Support for multi-platform PKCS#11 driver is integrated in the OpenSC (www.opensc.org) framework and is “officially” unsupported although working almost perfectly so far.

An ID-card utility has been developed and released to the public from the beginning. The utility has the ability to display contents of the electronic part of the ID-card, changing PIN and PUK codes and providing all other card management functions.

Qualified certificates for the ID-card are issued by SK. The certificates follow the X509v3 standard. However it has to be taken into account that the PIC is used as the subject serial number. More details on the certificates, certificate profiles, certification policies and practice statements can be obtained from SK’s repository http://www.sk.ee/pages.php/0203040503.

The Estonian ID-card uses a single CA model. However, CA certificates for ID-card certification tend to change, so there are currently two CA certificates (ESTEID-SK and ESTEID-SK 2007) in use, both

certified by root certificate of SK (JUUR-SK). The SK's root certificate is further certified by National Register of Certification Service Providers (register.srr.ee) but this certificate is not considered as a "root" one but rather as evidence that SK is an officially registered service provider.

The JUUR-SK certificate is distributed through the Microsoft Root Certificate Program and with a widely-promoted and used web-based ID-card software installation package available from https://installer.id.ee.

The basic source of ID-card-related information is a website www.id.ee which often refers to www.sk.ee as a source of services and technology. www.sk.ee also contains all information about certification matters.

Validation services are provided by SK by various means. The primary and most heavily promoted way to obtain certificate validity information is through the OCSP service from ocsp.sk.ee. Access to the OCSP service is controlled. Service provider must have a contract with SK and access the service from a specific IP address(es).

SK also provides CRLs, although it does not encourage its use. The CRL is way too large and is updated only every 12 hours. Given the possibility of certificate suspension/end of suspension, CRL can be used only in low-security applications.

Finally, SK's LDAP directory has certificate validation properties – only active certificates are present in the directory.

3.3.4 Organisational aspects

As mentioned in previous sections the ID-card issuing as well as its further operations is done in close public-private partnership. CMB is the government organization responsible for issuing identification documents to Estonian citizens and alien residents, as required in the Identity Documents Act. SK functions as CSP and Validation Authority, maintains the electronic infrastructure necessary for issuing and using the certificates on the card, and develops the associated services and software. TRÜB Baltic AS, subsidiary of Swiss TRÜB AG, is the company that personalizes the card.

The card issuing process consists of the following steps:

1) the person fills in and submits application for the card to CMB indicating the office where he or she would like to receive the card. Applications for issuance of ID cards can be submitted to CMB:
- in person (80 %)
- by mail
- digitally through a website (requires ID card with valid certificates);

2) CMB enters the data into the information system (The database of identity documents issued by the CMB);

3) CMB decides to issue the document (As referred in section C.3.2, since the most of the submitted applications are recurrent applications, the information submitted by applicants is verified against the entries of the database. If the applicant has not yet had a document issued by the CMB, he/she needs to provide additional source documents proving the applicant has the right for the identity document;

4) the personalization order is then pieced out based on the scanned and alphanumeric data presented in the application and entered into the information system;

5) CMB forwards the personalization order to TRÜB Baltic AS;

6) The procedure of the personalization of the card are carried out in the following steps:

- TRÜB Baltic AS personalizes the physical card layout;
- TRÜB Baltic AS gives the card the order of generating private keys (internal function of the card, the keys will never leave the card) and prepares the secure PIN envelopes;
- TRÜB AS formulates certificate requests (2 per card) and forwards them to SK;
- SK issues the certificates, stores them in its directory and returns the certificates to TRÜB Baltic AS;
- TRÜB Baltic AS stores the certificates and personal data file on the card chip;
- TRÜB Baltic AS prepares the final delivery envelope, enclosing the card, secure PIN envelope and an introductory brochure;

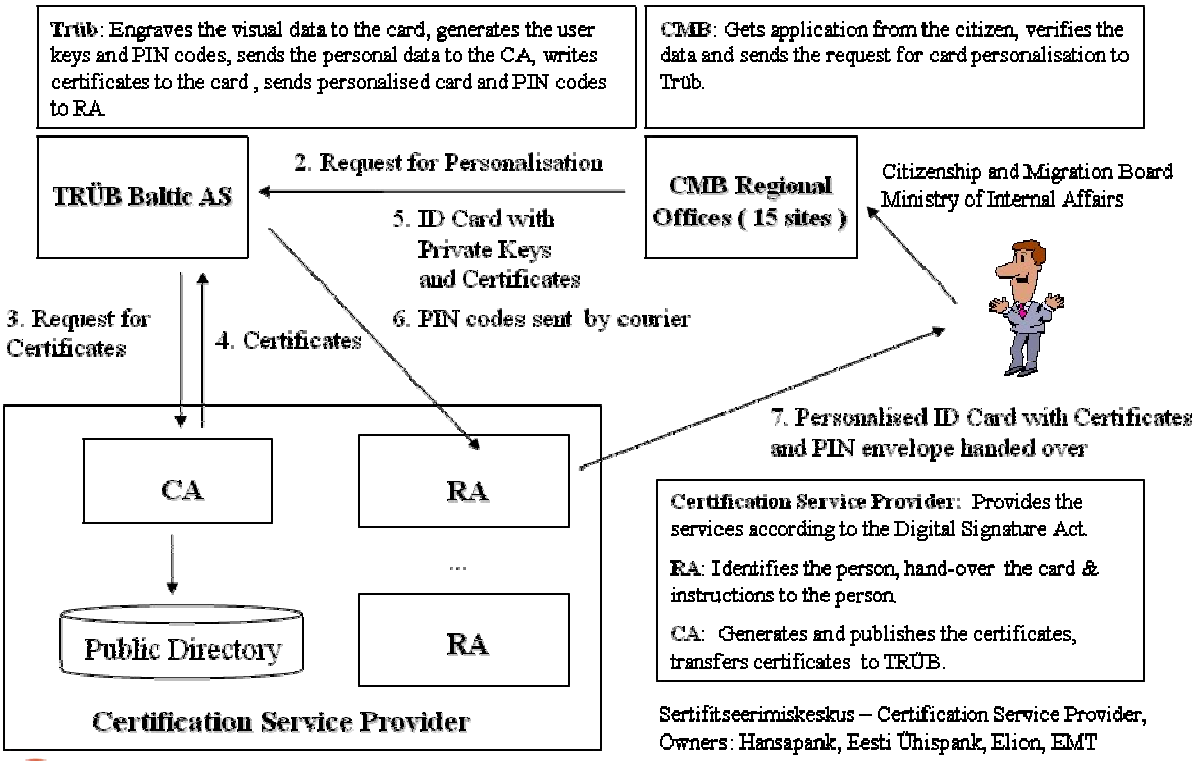
7) TRÜB Baltic AS hands the final delivery envelope over to CMB;

8) CMB sends delivery envelope to the local office specified in the original application (done using security couriers);

9) person receives the delivery envelope (containing card and PIN codes) from the local office of CMB;

10) upon receipt of the card, the card and certificates are activated.

The process is illustrated below:



For further operation of the card concerning certificates, SK maintains the associated validation services including an LDAP directory service, OCSP validation service and CRL publishing. Use or the CRL is not encouraged as it is published only once every 12 hours.

The renewal of certificates is free of charge and is provided as an online service. An alternative renewal option is over-the-counter in Hansapank and SEB Ühispank or in CMB offices.

Procedures have been put in place to suspend or revoke certificates when the ID-card is lost or destroyed or there is suspicion of loss of PIN codes. ID-card certificates can be suspended over the phone operating on 24/7 basis, SK maintains the telephone hotline. In order to end suspension or revoke certificates, an ID-card holder shall physically appear to bank branch office or CMB office and fill in an application form.

SK also provides the software to anyone interested in creating applications to the card and digital signature, and provides a readymade client and web portal for giving and verifying digital signatures.

From a card-issuance point of view, all the responsibility lies on CMB. CMB has contractual agreement with TRÜB detailing the relevant outsourcing of responsibilities (sub-suppliers are Trüb Baltic AS and SK). From a certificate issuance point of view – all the responsibility of certification procedure relies on SK (TRÜB has the contract for supply the certification service). CMB, TRÜB Baltic AS, banks and also hotline for certificate suspension act as Registration Authorities of SK. SK has an insurance policy (required by the DAS) in excess of 5 million kroon (around €32,000) for

covering possible damages caused by misbehaviour of SK or its contractual partners in certificate issuance or validation information provision process.

The information of issued ID-cards is stored and maintained centrally in the database of identity documents issued by the CMB. See more about the information management in this database in section C.3.2. The information of certificates on ID-cards is maintained by SK in the database of certificates and published and accessible to the third parties by OCSP validation service, CRL and LDAP directory service.

SK has also voluntarily taken the role of software and user support for the ID-card usage and applications. From the other hand, the Ministry of Economics and Communications (MEC) have the role of overall governmental IT-coordination and fulfilling requirements for the Digital Signature Act in particular. Negotiations are on the way to find a suitable scheme for involving MEC to play (financing) role in supporting of end-user software and services for digital signing and verification currently available for free for public use.

3.4 Interoperability

The Estonian ID-card is issued only to citizens and residents of Estonia. Due to ID-card's universality – it is usable in every sector and provides a security level sufficient to every service provider – no alternative PKI tokens have been issued to a significant extent. Only from today, Mobile-ID is being deployed as an alternative eID tool.

This has resulted in many e-services strictly oriented and configured to accept Estonian ID-card only (with Mobile-ID support evolving) – as long as we are talking about PKI-based authentication mechanism.

Any intent to accept foreign eID-s in governmental e-services is virtually inexistent. Business processes in public sector are mostly built in the way that it would not make sense for foreigner to use governmental e-services – they are meant for Estonian citizens and residents.

There is some interest in banking sector for accepting foreign eID-s in Internet banking applications. This interest is limited to neighbouring countries (Finland, Sweden).

From the other hand, interest to achieve international eSignature interoperability is relatively high. Some governmental agencies have admitted that they would like to accept some digitally signed applications. DigiDoc, the common digital signature solution used in Estonia, is designed to support wide variety of PKI-based smartcards. Compatibility with Belgium and Finnish ID-cards has been successfully demonstrated.

3.5 eIDM Applications

This section will provide a short overview of key applications for the eIDM systems.

3.5.1 ID-card applications making use of PKI functionality

All main web-based applications requiring strong user authentication make use of the ID-card both in public and private sector.

In public sector the most notable service is the Citizen Portal[13] which links together the vast majority of public services and thus serves as a single point of entrance. Another important service is provided by the Estonian Tax and Customs Board[14] allowing doing taxes online for physical persons as well for companies.

The Ministry of Justice[15] provides access to several registers using the ID-card. This ministry also hosts the Business Register and provides an e-environment for data exchange for companies.

One of the most popular e-services accessible with ID-card is e-school[16]. 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[17] 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[18] and Pension Register[19] also make use of ID-card authentication.

Telecom companies (for example: Elion, EMT, Tele2) and utility companies (water, gas and electricity) make use of the ID-card authentication in their self-service environments.

A list of sites accepting ID-card authentication can be found in http://id.ee/?id=10953.

[13] http://www.eesti.ee/

[14] http://www.emta.ee/

[15] http://www.eer.ee/index_eng.phtml

[16] http://www.ekool.ee/

[17] http://www.hansa.ee, http://www.seb.ee, http://www.sampo.ee, http://www.krediidipank.ee, http://www.sbmbank.ee; http://www.rahanet.ee

[18] https://www.e-register.ee/

[19] https://register.pensionikeskus.ee/public/authorization.jsp

3.5.2 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 terminal/smartcard reader. The personal data file contains the same information that is visibly printed on the card – most notably name and PIC of the cardholder.

The facial image on the ID-card further helps to make sure that cardholder is an authentic person.

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

There are two remarkable applications to be mentioned separately:

3.5.3 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.

3.5.4 “Replacement” of driver’s documents.

Almost all traffic police cars are equipped with IT and communication systems for querying information from the drivers licence database, car insurance and car registry. When a car driver has ID-card with him, it would enable to check identity and retrieve all other relevant information from live databases.

3.5.5 Bank eID applications

Every service supporting ID-card authentication usually provides an option to log in via Bank eID as well. In addition to the e-services mentioned in the previous paragraph there are few services accepting Bank eID authentication only.

Most notably Bank eID authentication is used in e-commerce sites in conjunction with payment schemes.

As mentioned before, banks will cease providing authentication services to 3rd parties. This is expected to happen in second half of 2008. This means that all e-service providers relying on Bank eID authentication shall turn their users to use of PKI-based solutions – ID-card and Mobile-ID.

3.6 Future trends/expectations

The roll-out of the ID-card is completed in practical terms in Estonia. The next phase – getting people to use it electronically – has started with the initiative "Computer Protection 2009" described in section D.1.4. The objective of a ten-fold increase of ID-card users in three years constitutes a tremendous challenge requiring all stakeholders to play an active role in it.

Ideas about next-generation ID-cards are quietly circulating with no decisions made yet. Plans include transformation from Orga/Micardo platform to MultOS and including RFID capability (with separate chip) for biometrics. Compliance with the European Citizen Card standard is also considered.

There are high expectations in the field of Mobile-ID. It is expected that ease of use (no software installation required) and mobility (no smartcard reader required) will drive the use of this PKI-based authentication and digital signing mechanism. Market leader EMT will issue PKI-capable SIM cards only after they exhaust their current stock of "old-fashioned" SIMs. Other mobile operators (Elisa, Tele2) have been showing interest to follow Mobile-ID issuance.

A new dimension in the PKI world in the Baltic area is the formation of a "Baltic WPKI Forum"[20] with the aim to harmonize technical standards in Mobile-ID/WPKI service provision.

3.7 Assessment

Estonian ID-card scheme is described as successful in general. The following success factors deserve mentioning:

- Positioning ID-card as a primary/compulsory identification document with activated certificates served as a way for building the Infrastructure (I in the PKI). This has led to the situation where almost the whole population is electronically identifiable – although they not necessarily making use of it;
- The issuance scheme is designed in a secure two-level way which has resulted in near-zero false eID problems in five years of existence of ID-card thus increasing trust of the private sector in ID-card security;

[20] http://www.wpki.eu

- A successful combination of Private-Public-Partnership has led to the provisioning of eID-enabled services both in private and public sector. Unique ownership of SK ("big four" from private sector) and SK's tight relationships with the Government provide for ground for common cross-sector development;
- The enrolment scheme of ID-card where a citizen can apply by post and get his ID-card from a favourite bank branch office has proven user-friendly and a good solution for massive roll-out (until 2007 ID-cards were issued mainly from bank branches of the two main banks of Estonia, as large-scale roll-out is completed by now, only regional offices of CMB are issuing ID-cards);
- All major e-services were eID-enabled for authentication relatively fast after launch; the common digital signature system was launched less than a year after roll-out – there was no major delay in providing applications for ID-card;
- Although "low-tech", e-ticketing and "substitute for driver licence" gave ID-card mass market popularity;
- Successful deployment of common digital signature system and Internet voting system serve for 1st-grade examples of electronic ID-card use;
- "Computer Protection 2009" represents a new era in the history of deployment of PKI and ID-cards in particular. The fact that major stakeholders are in favour of PKI-based technology and will replace other authentication mechanisms represents a triumph of ID-card and related techniques;
- The introduction of alternative PKI-based methods like Mobile-ID will allow for using PKI in business-critical applications where redundancy is unavoidable.

At the same time there have been certain pitfalls in the process, mentioning of which could benefit builders of national eID schemes tomorrow, especially:

- Weak launch campaign – because of inexistent market education and unawareness of eID-enabled services the ID-card was regarded as "unusable" for the first few years;
- The coordination on the state level in supporting the development of end-user software and services was weak;
- Ideas for creating a common digital signature system or packaging user-friendly "ID-card starter kit" (bundle of smart-card reader and supporting software) came too late. Probably a number of early adopters got disappointed with first experiences and hardly got back to the electronic ID-card usage;
- Major e-service providers – banks – did not focus on ID-card before the roll-out was nearly completed. Bank eID and provisioning of authentication services to 3rd parties constituted major restraining factors to the uptake of ID-card usage;
- It is not entirely clear whether pure legal and organisational means are enough for preserving privacy in the situation where there is a common PIC which is used in all databases. Introduction of a PIC-neutral identity code in certificates (like in Finland) would maybe have been a good idea.