

## Electronic identity management in Estonia between market and state governance

Tarvi Martens

Received: 22 October 2009 / Accepted: 4 February 2010 / Published online: 9 March 2010  
© The Author(s) 2010. This article is published with open access at Springerlink.com

**Abstract** The present paper summarizes the development of the national electronic Identity Management System (eIDMS) in Estonia according to a conceptual framework developed in an European comparative research project outlined in the first chapter of this special issue. Its main function is to amend the picture of the European eIDMS landscape by presenting a case with high involvement of the private sector and thereby checking the generalizations from the comparisons of Austria, Belgium, Germany and Spain, presented by Kubicek and Noack in the previous chapter of this special issue. Starting with a short introduction into the historical background of identity documents in Estonia the national population register, the passport as well as the bank ID are described as the main pillars of the Estonian eIDMS, on which the national ID card builds on, which has been introduced in 2002. The technical features of the eID and the ID card are described in Section two as well as the areas of application and the processes for production and distribution. Section three presents the actors constellation, Section four the time line of the development process, starting from 1997. Section five deals with the diffusion and promotion of the ID card and the eID authentication function. After a very low and slow take up during the first 5 years due to a cooperation agreement between major banks, telecom operators and the government usage has increased. But still the authentication by Internet banks, which provides authentication services to third parties, including government, is the biggest competitor for the eID function on the national eID card. Only recently the major banks have announced to slowly fade out the password cards and PIN calculators as alternative modes of bank authentication.

**Keywords** Estonia · Digital signature · Electronic identity

---

This report is based on official documents and the personal experience of the author. It has been compiled under contract with the Institute for information management Bremen, funded by Volkswagen Foundation, Germany

---

T. Martens (✉)  
Certification Centre, Pärnu Ave. 141, 11314 Tallinn, Estonia  
e-mail: tarvi@sk.ee

## Historical background of identity documents in Estonia

The present structure of the national identity management in Estonia has been established in 1992 after the full independence from the Soviet Union. Under the Soviet regime, Estonian SSR had the same identity document system as the rest of USSR had i.e. paper passports and other paper identity documents.

In the new system the central agency is the Citizenship and Migration Board (CMB<sup>1</sup>), a state authority under the Ministry of the Interior. It runs the national population register, administers the national Personal Identification Code and issues identity documents, since 1992 a passport and since 2002 an ID card, including an eID-function. However, the most popular method for online authentication for e-commerce and e-government was and still is via the Bank ID, which has been introduced in Estonia 1996 for Internet banking.

### The national population register and the personal identification code

The national Population Register is a central database for the performance of functions of the state and local governments established by the Population Register Act regulating the registration of the population, the maintenance of the records and the rights and obligations of citizens and public authorities.<sup>2</sup> It contains the personal data of the citizens, data of all identity documents and vital events certificates. The registry includes the following personal data: names, sex, date of birth, place of birth, citizenship, residence permit, place of residence and marital status and the Personal Identification Code (PIC).

PIC is the core element of the identity system in Estonia. It 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 (one digit for two attributes)
- date of birth digits (YY+MM+DD)
- three random digits
- one checksum digit

All certificates of widely accepted eID-s in Estonia (ID-card and Mobile-ID) contain the PIC. It is used as a primary key in the majority of databases containing personal information both in the public and private sector. Therefore service providers can easily link eID-authenticated users with their personal data. Moreover, digitally signed files contain a certificate of the signatory including the PIC and thereby allowing for a definite identification of the signatory.

The data entered in the Population Register is the basis for other databases of the state and local government authorities. The population registry is also issuing the PIC to other state authorities who have to document a person for

<sup>1</sup> As of 01.01.2010 CMB is a part of Police- and Border Guard Board, see <http://www.politse.ee/en/>.

<sup>2</sup> Population Register Act (2005), in English: <http://www.legaltext.ee/et/andmebaas/ava.asp?m=022>.

the first time (usually by birth or issuance of the residence permit or the right of the residence).<sup>3</sup> The data is collected and entered by different state and local government authorities, natural and legal persons. Persons and authorities can submit data to the population register online or by forwarding data through a data communication network.

### The passport

First passports in Estonia were issued in 1992 by the Citizenship and Migration Board (CMB). The CMB issues passports for Estonian citizens and aliens, temporary travel documents, seafarers' discharge books, certificates of record of service on ships and refugees' travel documents. For 10 years the passport was the only national ID document.

### Bank ID

In 1996 Estonian banks started Internet banking and introduced two methods for online authentication, which are still offered today:

- Password cards containing 24 one time passwords are issued personally to the customer in his bank,
- PIN calculators are off-line card readers with a keypad. At log in the customer receives a code number on his screen, enters his bank card and this number and the calculator generates a new one time PIN which the customer enters online. PIN calculators were introduced in the beginning of 90's.

Until 2002 the only and today still the most popular method for online authentication is to use the Bank ID authentication modes. In contrast to many other European countries Internet bank authentication is not only used for online banking but is a service, which the five major banks are providing to third parties. It started back in 1996 and today covers almost 100% of the people between 16 and 74. It is simple to use, as no special hardware or software is needed: the user logs into the Internet bank, using the appropriate method, selects "external e-service", user's PIC is securely communicated to the e-service and the user continues work with selected e-service.

Since 2002 the ID card based eID is offered as a third option. Considering the number of cards issued the password cards and ID cards are almost equal:

- around one million password cards (with 24 codes) have been issued,
- estimated 50,000 PIN-calculators are in use,
- since 2002 over one million ID-cards have been issued.

But looking at the use for online authentication, the password-based authentication with estimated 80% still is the mostly used method 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. Therefore it is not

---

<sup>3</sup> The use of the registry is regulated in the Personal Data Protection Act (English: <http://www.legaltext.ee/text/en/X70030.htm>).

surprising that several eGovernment services like eTaxation and Citizen Portal make use of the bank authentication.

### The eID and the ID-card

Considering that the first generation of passports had to be renewed in 2002, the Government had an historical chance to introduce a new type of identity document. It was obvious that lot of people will come for a new passport starting from 2002 as in 1992 people tried to get an Estonian passport as soon as possible.

The idea for a second ID-document emerged in 1997 in the form of a national ID card, which could carry an eID and certificates for electronic signatures. It has been launched in 2002 and roll out has been finished in 2006. It is obligatory. Every citizen older than 15 years has to hold such an ID card. Estonia has about 1.3 million inhabitants, and there are about 1 to 1.1 million cards active. The legal basis is the Identity Documents Act of 2004.<sup>4</sup> In addition to the eID on the national ID card in 2007 a mobile eID has been introduced.

#### The national ID card

Compared to the systems in Austria, Belgium, Germany and Spain as described by Kubicek and Noack in this special issue the Estonian ID card and eID is quite similar to the Belgian one (see Table 1).

The ID card contains the holder's surname, given names, sex, citizenship, date of birth, place of birth, personal identification code (PIC), a photo, a signature, the date of issue and date of expiry, and a document number. For resident aliens with valid papers, the ID card also contains residence and work permit or right of residence data. In addition to many security features, the card has a machine-readable code (Figs. 1 and 2).

The Estonian ID-card contains a data file, which is unprotected and includes the same personal data that is visibly printed on the card—most notably name and PIC of the cardholder. This allows for quick retrieval of personal data when the card is inserted into a terminal/smartcard reader, e.g. when using the ID card as a loyalty card, as an entrance card to libraries, sport clubs etc. or for quick registration to an event or for entering premises.

The ID1-shaped card is based on PKI technology and contains two certificates: one for authentication, and one for electronic signatures, both of them considered as qualified. Each private key is dependent on the use of a different PIN-code. The certificates contain name(s), surname(s), PIC (containing gender and date of birth) and a government-assigned e-mail address in the authentication certificate. There is no electronically usable biometric information on the card. The use of the certificates is regulated in the Digital Signature Act.<sup>5</sup>

Initially ID-cards were issued for a lifetime of 10 years with certificate validity of 3 years. Renewal of certificates is without charge for end users and the process can

<sup>4</sup> <http://www.legaltext.ee/text/en/X30039K10.htm>.

<sup>5</sup> <http://www.legaltext.ee/text/en/X30081K4.htm>.

**Table 1** The Estonian eID and eID card in comparison with other European systems

		AT	BE	GE	ES	EE
carrier card	identical with national ID-card	–	X	X	X	X
card character	obligatory / age	–	> 12	>16	>14	>15
card function	Authentication (online)	X	X*	X**	X	X*
	Authentication (visual)	X***	X	X	X	X
	e-signature	X	X*	X**	X	X*
Data on card and chip	contact/contactless chip	Contact	Contact	RFID	Contact	Contact
* opt out, ** opt in, *** depending of used Card	visual data:					
	• address	X***	–	X	X	–
	• owners photograph	X***	X	X	X	X
	national register number	–	X	–	X	X
	PIN-protected identity data	–	–	X	–	–
	PIN-protected authentication data	X	X	X	X	X
	Biometrics face fingerprints	–	–	X	X	–
		–	–	X**	X	–

be performed over the Internet. From January 2006 both certificates and the card have a lifetime of 5 years.

### Mobile-ID

In addition to the eID on the national ID card in May 2007 a Mobile-ID was introduced to Estonian market by the largest mobile operator EMT in co-operation with SK, the Estonian Certification Authority. In order to get a Mobile-ID, the user needs to replace his SIM-card by a PKI-capable one. As the registration process is performed by the mobile operator, it is not considered trustworthy enough. Therefore the user needs to “activate” his/her Mobile-ID with his ID-card. Thereby issuance of the Mobile-ID is bound to the security and quality of the ID-card. Mobile-ID certificates contain the same personal information on the subject.

Mobile-ID provides certain advantages for the end user compared to the ID-card: the user does not need a smartcard reader nor any specific software. Currently the Mobile-ID is available from one mobile operator only and the number of active users is below 100, 00. Two other main mobile operators (Elisa, Tele2) launched their Mobile-ID service in December 2009.

### Applications of the ID card

Besides many online services there are two remarkable applications to be mentioned separately:

- **ID-ticketing:** Over 120,000 users are carrying the ID-card every day to prove their entitlement to travel in public transportation in Tartu, Tallinn and



Fig. 1 Estonian ID card—front cover

surroundings (Harjumaa county). Tickets for one to two hours, or for one, three, ten, thirty or ninety 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.

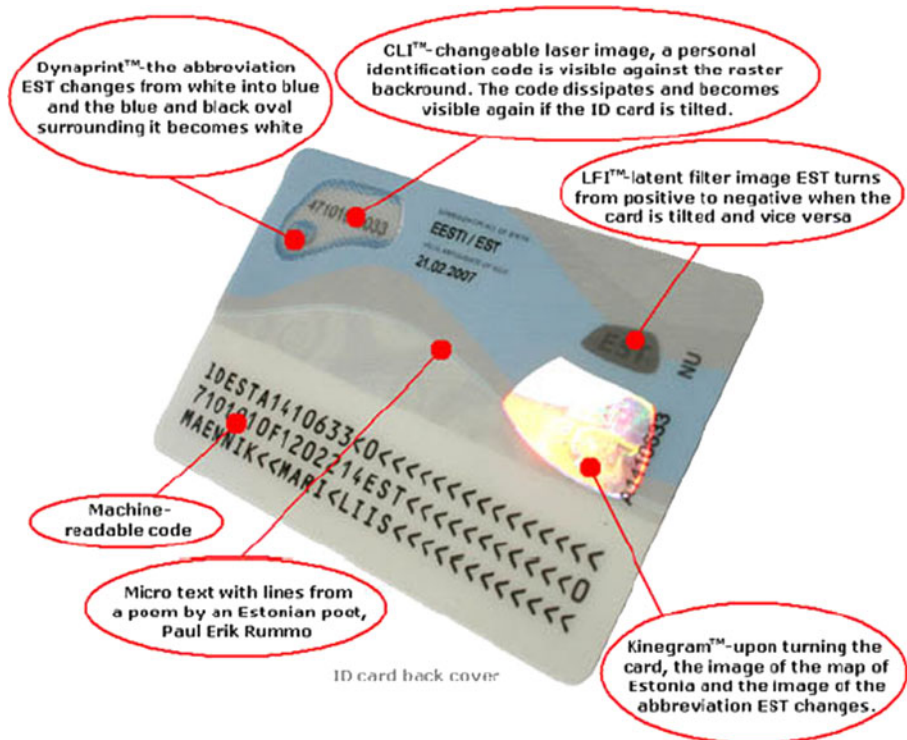
- **Partial replacement of driver's documents:** Almost all traffic police cars are equipped with devices for querying information from the drivers license database, car insurance and car registry. When a car driver has his ID-card with him, it would allow checking the identity and retrieving all other relevant information.

All main web-based applications requiring strong user authentication make use of the ID-card both in public and private sector. Most sites supporting ID-card login also support Mobile-ID. Authentication is using standard TLS/SSL protocol. This implies that the service provider receives the complete certificate of the user including the PIC.

In public sector the most notable service is the Citizen Portal,<sup>6</sup> which links the majority of public services via a single point of entrance. Another important service is provided by the Estonian Tax and Customs Board<sup>7</sup> allowing tax declarations online for natural persons as well as for companies. While most government applications offer Bank ID authentication option as well, this is not the case in the

<sup>6</sup> <http://www.eesti.ee/>.

<sup>7</sup> <http://www.emta.ee/>.



**Fig. 2** Estonian ID card—back cover

eHealth field. The Health Information System<sup>8</sup> does not accept Bank ID authentication because of the higher security level demands, instead authentication is only possible by the national eID.

The ID-card is also an enabler of Internet voting (I-voting), which in Estonia is an official method of voting and produces binding results.<sup>9</sup> It was introduced in 2005 for elections of local governments and repeated in 2007 for elections of the national Parliament. I-voting is a major application for engaging new ID-card users: up to 40% of I-voters in 2007 were first-time users of the eID function. In 2009, I-voting was enabled in two elections (European Parliament and Local Elections) and the number of I-voters finally broke barrier of 100,000 which makes I-voting share more than 15% of all voters. For full statistics please refer to National Electoral Committee.<sup>10</sup>

One of the most popular e-services accessible with the eID is e-school,<sup>11</sup> 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.

<sup>8</sup> <http://www.digilugu.ee>.

<sup>9</sup> <http://www.valimised.ee/>.

<sup>10</sup> <http://www.vvk.ee/index.php?id=11178>.

<sup>11</sup> <http://www.ekool.ee/>.

Internet banking<sup>12</sup> 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<sup>13</sup> and Pension Register<sup>14</sup> 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 on <http://id.ee/?id=10953>.

### Digital signatures with eID

One of the main reasons for introducing the ID-card was to implement the Digital Signature Act and provide means for digital signing for Estonian residents. Free tools for end-users and system integrators were released back in 2002 and are still evolving. As a result, Estonians are sharing a common understanding of digitally signed documents in file form, fully standardized and widely accepted by everyone, including courts. A piece of software called “DigiDoc Client”, allowing for digital signature creation and verification, comes with a package of the ID-card software and therefore can be installed on every computer with a smartcard reader attached.

This development has resulted in massive use of digital signing as digital signatures created with those tools are legally equivalent to a hand-written signature. There are cases in the law where digital signatures are considered even to be stronger than handwritten ones—e.g. in the establishment of companies.<sup>15</sup> Digital signatures are massively pushed by Internet banks as all transactions are required to be signed digitally (in case the user logged in with his ID-card or Mobile-ID).

### Authority to access the eID

The personal data on the ID card—data file and certificates—are available to every card terminal as they are not PIN-protected. The authentication certificate is available to Service Providers after successful ID-card login. The digital signature certificate is available in the digitally signed document to everyone who sees the document. As a result, the citizens’ PIC in the data file or in certificates is made available with every electronic use of the ID-card. Furthermore, the PIC is used as a key in almost every database—both in the private and public sector. The question of cross-use of different registries and databases is a legal matter covered by the Personal Data Protection Act<sup>16</sup> and controlled by Data Protection Agency.<sup>17</sup> Cross-use of databases is generally allowed only if granted on application.

<sup>12</sup> <http://www.hansa.ee>, <http://www.seb.ee>, <http://www.sampo.ee>, <http://www.krediidipank.ee>, <http://www.smbank.ee>, <http://www.rahanet.ee>.

<sup>13</sup> <https://www.e-register.ee/>.

<sup>14</sup> <https://register.pensionikeskus.ee/public/authorization.jsp>.

<sup>15</sup> <https://ettevotjaportaal.rik.ee/index.py?chlang=eng>.

<sup>16</sup> <http://www.legaltext.ee/text/en/X70030.htm>.

<sup>17</sup> <http://www.aki.ee/eng/>.



Production and distribution of the ID card and the eID

The eID card is issued by the Citizenship and Migration Bureau (CMB). The Database of the CMB is communicating heavily with the Population Register (see above) so that the integrity of identity management is ensured. All changes in the Population Register (i.e. death of a person, change of name etc.) are communicated to CMB through the Population Register. In those cases CMB invalidates the ID-card and issues a request for certificate revocation which is carried out automatically.

CMB cooperates with private sector suppliers in the issuance process of the ID-card. CMB receives an application from the resident (by post or in person) and decides upon issuance and data on the card. Personalization and certification services are outsourced to private companies as illustrated in the following Fig. 3.

Personalization of the ID card is carried out by TRÜB Baltic AS, which requests certificates from AS Sertifitseerimiskeskus (Certification Centre, SK). The latter also provides after-service (PIN renewal, certificate renewal etc) through the bank offices (Swedbank and SEB) operating as Registration Authorities. There is currently just one CA in Estonia (SK).

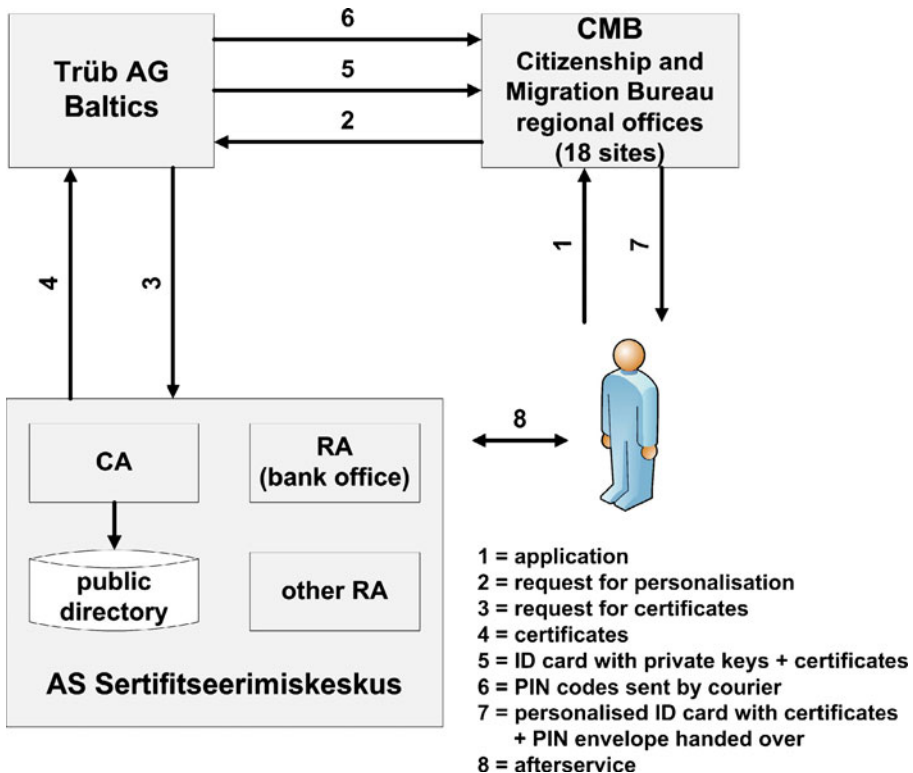


Fig. 3 Production and distribution of the Estonian eID

## Actor constellation

### Main actors

On the political level there are two major ministries in Estonia involved in the eID development:

- The Ministry of the Interior (MoI) is supervising the Citizenship and Migration Bureau<sup>18</sup> (CMB), directly responsible for issuance and maintenance of identification documents and for maintaining (electronic) identities of residents at large.
- The Ministry of Economic Affairs and Communications (MEAC) includes the Department of State Information Systems (RISO) which is responsible for the general ICT coordination in the public sector. The tasks of the department include the coordination of state IT-policy actions and development plans in the field of state administrative information systems. Furthermore the Estonian Informatics Centre (EIC), a subdivision of the MEAC, is responsible for implementation of the policies set by RISO.

*State register of certificates* functioning under MEAC is a supervision body for certification and time-stamping service providers. As the number of this kind of service providers is very low (one CSP and 2 TSP-s) the Register has been quite inactive functioning as a mere registrar just receiving compulsory yearly audit reports from service providers and filing them.

An eIdentity Working Group had been established under the auspices of MEAC consisting of different stakeholders from the public and private sector. The group held meetings on-demand basis addressing actual issues around the eID topics. The group is supposed to advise the Minister but in reality functions as a roundtable for exchanging information and ideas.

Private sector is playing a significant role in the Estonian eIDMS. ID-card manufacturing and personalization is outsourced to TRÜB Baltic AG and certification and validation services are provided by privately held AS Sertifitseerimiskeskus (SK). The latter functions also as an excellence centre for electronic usage of the ID-card providing software, including a digital signature software framework, end-user support as well as support and services to Service Providers making use of the ID-card.

SK is owned by the “big four” of Estonian economy—two of the biggest banks (Swedbank and SEB bank) and the two big telecom operators (Elion and EMT). This set-up allows SK to act as a unique roundtable bringing together public sector, telecom and banking sector. This is definitely one reason for having established the ID-card as a preferred eID token across all sectors and a reason for the absence of alternative strong eID tokens (besides Mobile-ID which is seen more like a tool complementary to the ID-card). This set-up has also facilitated the broad-bottomed introduction of digital signatures.

By definition the Department of State Information Systems and its executive branch EIC are responsible for the implementation of the Digital Signature Act, including software for digital signing. Lack of activities from these parties forced SK and its

<sup>18</sup> <http://www.mig.ee/index.php/mg/eng>.

owners to take over this role. As a result, SK has been filling the gap for 7 years now in this area. With money from the European structural funds EIC finally announced a tender for ID-card software in 2008, which shall be available late in beginning of 2010.

Actors and relations around eID in Estonia are illustrated in Fig. 4:

### Importance of policy fields

Although the main reason for introducing the ID card with an eID was the provision of electronic signatures, the design of the system included authentication functionality. CMB under the authority of the Ministry of the Interior played the main role throughout the introduction phase of the ID-card and made most of the decisions regarding the ID-card functionality (sometimes with help of the established working groups). The card is and will always be “CMB-issued” i.e. coming from Ministry of Interior. Although the card contains a certificate for a digital signature, CMB is not supporting this field by any software or any other initiative.

With regard to the importance and the influence of different policy fields according to the categories applied by Kubicek and Noack in their comparison of Austria, Belgium, Germany and Spain we may conclude that the Estonian picture is quite similar to the German and Spanish one, although the outcome is quite different and more like the Belgian system (Table 2).

### Timeline of the development process

As mentioned above, preparations for a “new generation identity document” started at CMB in 1997. Several working groups were formed with representatives from the

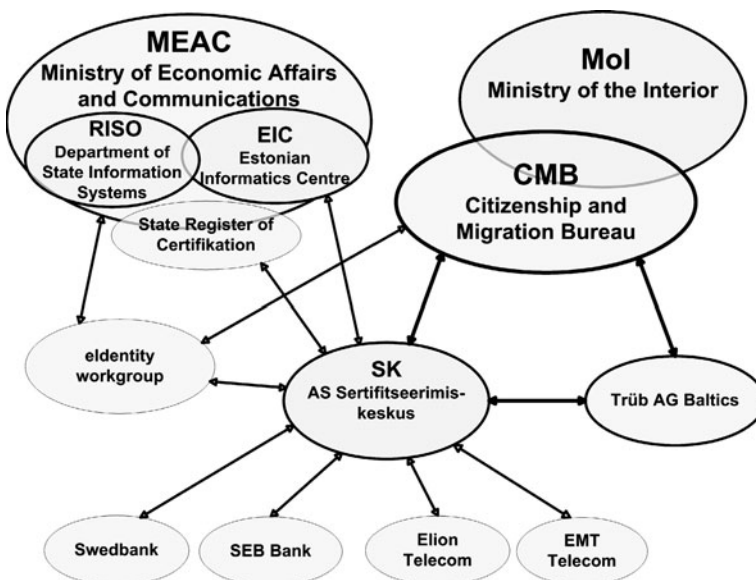


Fig. 4 Actors in the Estonian eID development

**Table 2** Actors and their importance and influence in the eID development process

Actors and their importance and influence in the process (1=low, 3=high)					
Actors / Policy Fields	GER	AUT	ESP	BEL	EE
Interior/Police	3	1	3	1	3
Public Administration	2	3	2	3	2
Industry/Commerce	1	1	2	1	2
Finance	1	1	1	1	1
Social/Health	1	2	1	2	1
Chancellery/Cabinet	1	3	2	1	1..2 <sup>a</sup>

<sup>a</sup> the one-time remarkable role of the Cabinet was the very first decision to introduce ID-card with full eID functionality to everyone

public sector and private sector. Preliminary studies concluded that eID technologies had developed far enough to allow application on a nationwide scale and that there is a demand in society for electronic ID-cards, particularly in connection with digital signatures. The following process can be divided in four additional phases: legal provisions, organizational and technical preparations, roll-out and up-take (see bottom line, Fig. 5).

The “legal phase” took longer than anticipated as topics of electronic identity and digital signatures were uncommon at the time: The working group preparing a draft of the Digital Signature Act started working in 1997 and took almost 3 years to finish the job.

The “preparation phase” saw the formation of two new companies in 2001, primarily for the sake of participating in the ID-card project: the establishment of AS Sertifitseerimiskeskus (by the two largest banks and two large telecom companies) and the creation of a Baltic subsidiary of Swiss-based company TRÜB AG. The decision for delivering chip- and certificate-equipped ID-card to everyone, however, was made in the last minute by the falling government under Prime Minister Mart Laar in October 2001. That decision, initiated by Mr. Linnar Viik, advisory to Prime Minister on ICT matters played a crucial role in the success story of Estonian ID-card.

The first card was issued January 28th, 2002 to the President of Republic of Estonia. The milestone of 1 million cards was surpassed in October 2006 and from this time on the number of active cards has remained between 1.0 and 1.1 million. During the roll-out phase several software releases have been issued in order to make usage of the ID-card easy and comprehensive, including wide distribution of digital signing software. Relatively low uptake of electronic usage of the ID-card became an issue in 2006, resulting in a new program “Computer Security 2009” (CS 2009) addressed in the next section.

Compared to Austria, Belgium, Germany and Spain the development process took 5 years until the first card was issued and thus is rather short as in Austria and Belgium, without the delays that occurred in Germany and Spain (see Kubicek and Noack in this issue. Considering the generalizations derived from the four other countries, we may confirm for Estonia that the rather straight development process was due to a smooth cooperation of the two ministries via the working groups and

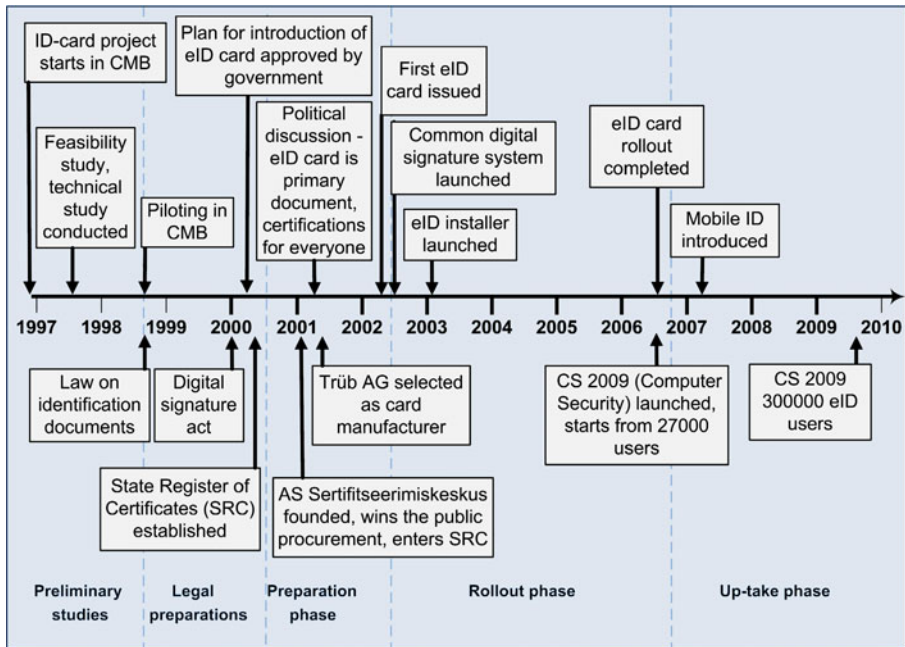


Fig. 5 Time line and most important events in the development process

that with regard to important decisions the Prime Minister and his advisor formed a successful couple of a power and an expert promoter.

Although these decision had been taken by a fallen government, change in governments did not hinder steady introduction of the ID-card in the way it was agreed at first. Thus the generalisation also applies also to Estonia: Changes in government offices due to elections during the development process did not influence the design and dissemination of the eID function.

With regard to the influence of industry we have to consider that there is no Estonian chip industry that might have tried to be involved. However the telecom and banking branches successfully have offered their services and influenced the eIDMS. This is quite different from the four countries compared by Kubicek and Noack in this issue, and much more like the Swedish case described by Aklund in the following paper. Banks were involved from the beginning and became part of the eIDMS via their shareholder role with SK. On one side the eID is in competition with their previous authentication by password cards. But on the other hand they have an interest in an additional system with qualified certificates and stronger authentication as well. Thus it was better for them to join and gain some control over the competitor.

**Diffusion and promotion**

Although the public perception was not positive after the launch of ID-card, it has been rapidly changing into more positive direction. The lack of applications,

unawareness and news about outrageous investment of 20 million EURO into the project raised a lot of criticism in the public. No one seemed to take care of ID-card-enabled applications and usage in 2002. Although the MEAC was in charge of that by the book, they did not take this role at the time.

Significant breakthrough came with a decision of SK to enter the ID-card usage business. SK developed and launched the digital signing system DigiDoc at the end of 2002 and started systematical work in areas of public promotion and support for application developers and service providers. The reason for entering this business was quite straightforward: SK was in charge of selling certificates; in case no one would use them SK would have to go out of business. In addition SK was backed by powerful industry players, including banks which are No.1 e-service providers making use of ID-card authentication and digital signing. This unique setup of private and public cooperation with strong players enabled to build a uniform platform. But it was extremely hard to achieve this status as there were attempts challenge it. In 2002 AS Cybernetica ([www.cyber.ee](http://www.cyber.ee)) launched an alternative digital signing tool/system and tried to compete with DigiDoc via local Estonian standardization. This attempt was not successful and named standards were replaced by a DigiDoc-style standard in 2008.

Strong commitment from the private sector has definitely been the key for the successful uptake of the ID-card. E-services by private sector (e.g. Internet banking) are massively more heavily used than public sector e-services. It is obvious that without private sector involvement there will be no incentive to make ID-card holders overcome the barrier of smartcard reader acquirement and usage learning curve. Lately, MEAC and EIC have woken up and are making significant contributions to the ID-card uptake by procurement of a new generation software for the ID-card and supporting the Computer Security 2009 initiative by a number of promotional and educational programs.

Computer Security 2009 is an initiative by major banks, telecom companies and the Government, who signed a co-operation agreement on May 2006.<sup>19</sup> This initiative addresses general IT-security topics for end-users (firewalls, anti-virus etc.) but with high emphasis on a transition to PKI-based authentication methods, including

- promotion and widened support of the ID-card and Mobile-ID,
- increasing availability and affordability of smartcard readers,
- introduction of alternative PKI-based authentication systems like Mobile-ID and alternative eID cards,
- significant increase of the user base of PKI-based authentication systems in 3 years (from 27,000 to 300,000 by the end of 2009 (Fig. 6)).

The Computer Security 2009 initiative has notably accelerated growth of ID-card users. An “ID-card user” in these figures is defined as a cardholder making use of certificates, for e-authentication or digital signatures. As every electronic usage of the ID-card involves a certificate validation from SK’s OCSP responder, the numbers are drawn from the statistics of the OCSP responder usage. Number of ID-card eID functionality users reached almost 300,000 by the end of 2009.

<sup>19</sup> <http://www.sk.ee/pages.php/02030201,1107>.

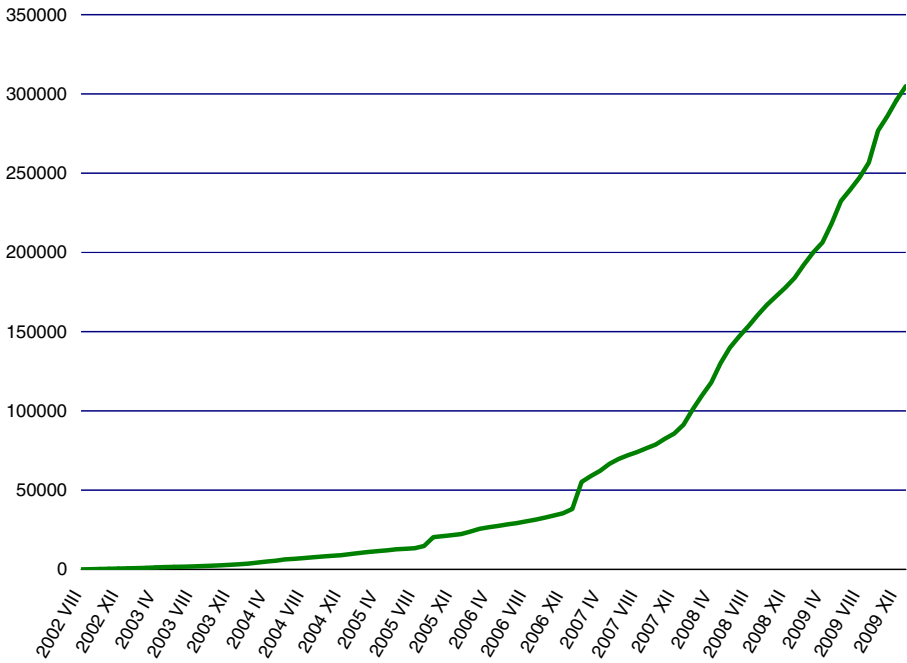


Fig. 6 Development of eID card users

The authentication by Internet banks is another significant factor to be considered when assessing usage of the ID-card as banks providing authentication services to third parties. The following graphs illustrate the growth of ID-card usage during 1 year with the two largest Internet banks (Figs. 7 and 8):

The most popular e-government service is tax declaration. In addition to ID-card and Mobile-ID authentication, the e-tax board allows login via Internet banks and

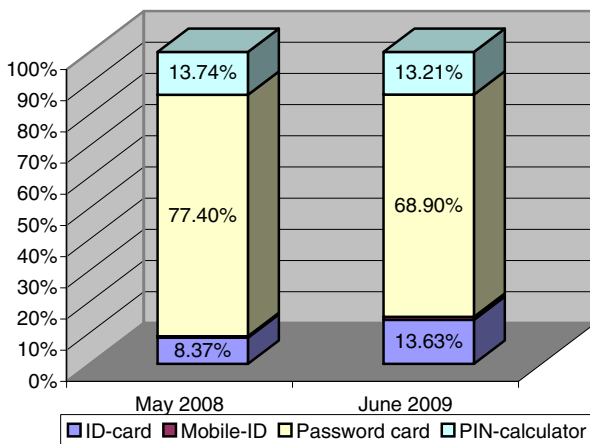


Fig. 7 Online authentication at SEB Bank

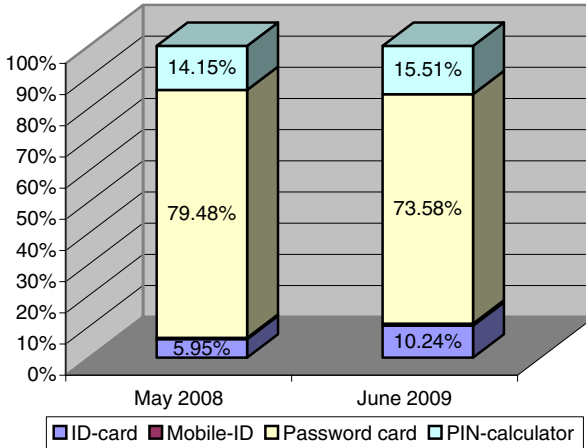


Fig. 8 Online authentication at Swedbank

also delivers its own password cards. Usage of PKI-based authentication methods, however, has been increased almost five-fold over past 2 years:

The most popular e-government service is tax declaration. In addition to ID-card and Mobile-ID authentication, the e-tax board allows login via Internet banks and also delivers its own password cards. Usage of PKI-based authentication methods, however, has been increased almost five-fold over past 2 years (Fig. 9).

Until today we find a similar pattern as reported by Kubicek and Noack in this issue for Belgium, Austria, and Spain: As long as other modes of authentication are accepted by the tax office, the share of the eID is rather low (Table 3). But as in Belgium it is growing.

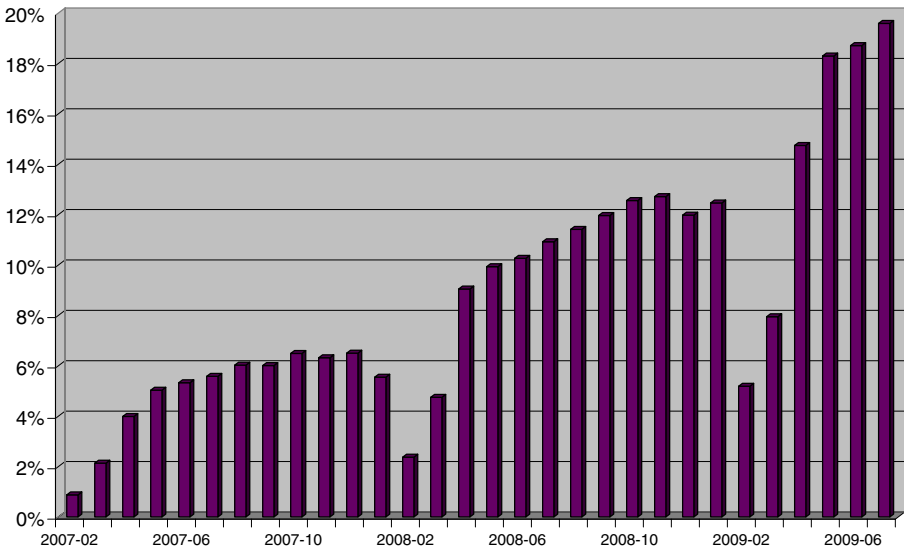


Fig. 9 Usage of ID-Card and Mobile-ID in the E-tax Board



**Table 3** The share of eID authentication in online tax services

	BE	ES	AT	EE
State of rollout early in 2009	9.3 million, 90% of the Belgians entitled to an ID card	3 million, 10% of the Spaniards entitled to ID card	8.4 million e-Cards, 100% of all citizens	1.1 million active cards, roll-out complete
eID function activated	7.5 million (80%)	not necessary	approx. 74000, 0.9% thereof approx. 20000 office ID cards	Around 50%, the rest have expired certificates.
Use rate for electronic income tax	2008: 24% 2009: 56%	21%	25.7%	87%
eID use rate for income tax (% of the electronic applications)	2008: 3.6% 2009: 14.2% (half of them with the help of civil servants in the tax office)	2008: 0.1%	2008: 0.7%	6% (yearly average)

The authentication by banks was and still is the biggest enemy of the eID based authentication. But in Estonia, several measures are employed to make users favouring the eID-based authentication:

- All banks have continuously lowered the maximum money transfer sum when authenticating with password cards. This sum is currently € 200/day.
- A number of e-services advertise ID-card and Mobile-ID based authentication over “bank authentication” by displaying informational banners and requiring users to make an extra step for bank authentication.<sup>20</sup>
- Few services like e-health, Internet voting and digital signing can be used exclusively with the ID-card or Mobile-ID only.

### Promotion and stimulation of applications

SK has been the center of eID support, promotion and excellence from the very launch of the ID-card. SK operates a 24/4 phone support (short number: 1777) initially designated for certificate suspension only but providing full end-user support nowadays. A website [www.id.ee](http://www.id.ee) contains comprehensive information for end-users and developers on a wide range of eID topics. This includes self-training application, problem solver, massive amount of well-structure information etc.

The ID-card software is available as of 2003 from <https://installer.id.ee>. The Installer is an intelligent application which analyses configuration of the computer (including attached smart-card reader if any) and installs all essential software with one-click button. The user can enjoy animation on topics of ID-card usage whilst the software is being installed. Essential software covers smart-card reader drivers for

<sup>20</sup> See for example e-tax board <http://www.emta.ee/?Id=12223>.

more than twenty readers, middleware for the ID-card, web plug-ins for web-based signing, service certificates, card management utility and DigiDoc Client for digital signing and digital signature verification in the desktop environment. The latter has a self-update functionality in order to drive people to update the software when important updates are available.

Smartcard reader distribution problems were first tackled in 2003 after launching the Installer mentioned before. At that time a €20 package was made available in Elion stores (a fixed-line telecom giant) containing smartcard reader, manual and CD with installation software which contained the same software as was available from the website. This package was not entirely successful as the software in the printed CD tended to outdate rapidly and the price margin was above expectations of the average consumer (Figs. 10 and 11).

The second wave of smartcard reader distribution was started in 2007 after a bulk deal with smartcard reader vendor Omnikey. This allowed bringing USB smartcard readers at a price around €6 in the retail market. According to the deal, selected alternative models like one with PIN-pad and one PCMCIA reader are also available with above-the-average price mark. These readers are available from a number of competing retail channels. This low price has inspired a number of campaigns such as banks giving out free readers for selected customers, political party distributing readers for free in order to promote Internet voting etc.

Most of the measures for helping the uptake have been carried out under the “Computer Security 2009” program described above. Currently a number of educational programs are running in order to bring more (especially elderly) people to Internet and use of ID-card such as a moving ID-bus, stands in shopping malls, courses for beginners, advanced courses and courses for “mentors” in local



**Fig. 10** €20 ID-card Starter Kit from 2003



**Fig. 11** €6 Omnikey smart card reader

communities. The program is expecting to bring some 100,000 more Internet and ID-card users during 1 year by summer 2010.

### **The Estonian case in comparison**

#### Path dependency

Comparing the Estonian case with the developments in Austria, Belgium, Germany and Spain and considering the main hypothesis related to the threefold path dependency formulated by Kubicek and Noack in this issue, for the Estonian eID we may state a only a medium degree of path dependency and some significant path creations.

With regard to the definition of the eID there was no change. The eID has been defined according to the ID registered in the national Population Register. But new organizational paths have been created for production, issuing and personalization as well as running the infrastructure. While in the other countries existing organizations have taken over additional eID related functions in Estonia the founding of CMB is a unique approach.

With regard to technical features there is a high degree of path dependency similar to the other countries: The decisions taken for most of the technical components of the Estonian eIDMS follow established paths of smart card and authentication technologies. However the introduction of an additional mobile eID solution is a case path creation which offers an alternative to the necessity for smartcard readers.

The regulatory pattern was kept quite stable. Existing legislation only was adopted to legalize the technical and organizational changes.

#### Privacy issues

Kubicek and Noack report that in Austria, Belgium and Germany there was no doubt that, because the eIDMS concerns basic privacy rights, precise legal regulation is required. In Spain the Ministry of the Interior took the view that no additional data

will be collected compared to the previous ID card and the filing of fingerprints in a central database and therefore no parliamentary consent is required.

In Estonia, although the certificate reveals personal data such as the date of birth and as these personal data on the card are not PIN-protected, there was no privacy debate in the process of legislation or in the media. There is only one remarkable exception. Initially all active certificates were published in the freely accessible LDAP<sup>21</sup> directory. This made it possible to find out the birthday and gender of any cardholder. After several years and couple of scandals in the media the set-up was changed so that certificates can be queried from the LDAP directory by PIC only.

As the PIC is used as a key in most databases, both in the public and the private sector, technically different personal information can be correlated. However, the Data Protection Agency is taking care of personal privacy. Cross-relating personal data between different databases is possible only with official permit from the Data Protection Agency. The citizen can find out via Citizen Portal<sup>22</sup> what data is recorded about him/her in different databases of public administration and in some cases also who has accessed the data.

Estonia seems to be culturally close to Scandinavian countries where safety of personal data handed over to the government is considered “safe enough” and privacy concerns are not that acute.

### Staatsverständnis

A remarkable difference to the development in Austria and Spain as described in previous papers in this issue, but somehow in line with the Belgium development is the recent intense promotion. Compared to these countries Estonia since 2006 is offering much more support. However, it has to be noted that this support does not come from government and therefore is not caused by an corresponding Staatsverständnis according to the Welfare State model. Rather Estonian politics is called sometimes “ultra-liberal” meaning that government tries to outsource what they can and therefore building so-called “thin state”. This happened to the eID development as well.

ID-card is issued by the government and was subsidized (around 50%) during 2002–2007. Now the fee for the ID-card is raised to almost covering the costs of the issuance. But government did nothing during this period about client software or smartcard readers. Rather the privately owned company SK did this so far. But this is expected to change from this year as government is in the middle of contracting for developing new wave of ID-card software.

Both these changes have very little to do with political changes. In case of subsidizing the ID-card it was just a matter of calculation and judgment of “people have now enough money to pay the full prize”. Software procurement was a result of 5 year long lobbying and opening of EU structural funds. Therefore we can not fully confirm the generalisation by Kubicek and Noack that differences with regard to the “Staatsverständnis” did influence the opening for e-commerce, the provision for electronic signatures and the supporting provisions for components, hotlines etc.

<sup>21</sup> Light Weight Directory Access Protocoll.

<sup>22</sup> <http://www.eesti.ee>.

## Future perspectives

There will be no major changes in the eID arena in Estonia, except for a possible upgrade of the ID-card chip. A next-generation ID-card is envisaged to be launched during 2011, which will contain an RFID chip with biometric information such as in the electronic passports. This, however, will not change anything with regard to the definition of the eID and the electronic functionalities and applications for the ID-card. Two other major mobile operators launched Mobile-IDs in December 2009. This could result in more attention and usage in Mobile-ID field in the future. Thus, in contrast to Belgium and Spain, we can not confirm, that once a technical choice has been made and a new path has been created, this establishes path dependency for the future.

**Open Access** This article is distributed under the terms of the Creative Commons Attribution Noncommercial License which permits any noncommercial use, distribution, and reproduction in any medium, provided the original author(s) and source are credited.

## Background reading

- Cimander R. eID in Estonia. Good Practice Case. MODINIS Studÿ on Interoperability at Local and Regional Level. Prepared in Cooperation with Andreas Aarma and Ain Jary, AS Sertifitseerimiskeskus, Estonia. Download from [http://www.ifib.de/projekte-detail.html?detail=Study%20on%20Interoperability%20at%20Local%20and%20Regional%20Level&id\\_projekt=194](http://www.ifib.de/projekte-detail.html?detail=Study%20on%20Interoperability%20at%20Local%20and%20Regional%20Level&id_projekt=194) (last visited December 28th 2009).
- European Commission, eGovernment in Estonia. eGovernment Factsheets, Edition 11.0, May 2009. Download from <http://www.eptactice.eu/en/factsheets>. Last visited December 28 2009.
- IDABC (Ed.), National Profile Estonia. eID Interoperability for PEGS. Brussels, November 2007.
- Kubicek H, Noack T. The path dependency of national electronic identities. A comparison of innovation processes in four European countries. Identity In The Information Society, Special Issue, 2010.
- Tepandi J. A population wide ID Card (Estonia). Case description on <http://www.eptactice.eu/cases/eIDEstonia>, last updated 10 December 2009. last vistied December 28 2009.
- Smith A, Pickles J. Theorising transition: the political economy of post-communist transformation: political economy of post-communist transformations London. Routledge Chapman & Hall; 1998.
- Subrena J-J (Ed). Estonia: identity and Independence: Amsterdam–New York; 2004.