e-Governance Academy

Global Information Society Initiative

eID
Estonian experience

This paper is developed in a framework of research conducted by Mrs Mari Pedak.

Tallinn
December, 2013

Content

Summary

During the first year after Estonia regained independence, the population accounting principles were established. Natural persons' identity management history begins in 1992, when the Personal Identity Code (PIC) - a unique number assigned to every Estonian citizen and resident - was introduced and first passports with lifetime of 10 years were issued in Estonia.

The relatively early start of Internet banking in Estonia in 1996 introduced the first electronic identity, usable in multiple applications – an Internet bank authentication. Banks also started to provide authentication services to third parties.

With the expiration of first passports issued there was a unique opportunity to renew the identification document system in Estonia by providing a new kind of document from 2002 – the ID card, on which the most important electronic identity management system in Estonia is based. Simultaneously, a Public Key Infrastructure (PKI) based electronic credentials framework, which includes the supervision of certificate service providers, and the data exchange layer X-Road to ensure interoperability of information systems, were developed.

The Estonian ID card is a mandatory electronic identity card that is intended to facilitate access to e-government services for all Estonian citizens and residents as well as offer access to a variety of other services.

After the roll-out of ID cards in 2006, both the supply and the consumption of e-services increased sharply. Currently almost half of the population (some 500,000 people) actively consumes thousands of e-services.

Increasing consumption of services led to the need for new means of authentication. Mobile ID was introduced in 2007 and the digital identity card in 2010.

PIC is in use unchanged to date. ID card certificates are linked to various registers through PIC, which functions as a unique identifier for Estonian citizens and residents in e-government services. PIC is included as a serial number on certificates of electronic ID cards and mobile ID.

The backbone of the e-government environment – X-Road – and the single entrance to the e-services portal – Eesti.ee – are accessible through authentication with ID card or mobile ID or through the use of authentication services provided by Estonian commercial banks.

The digital identity system in Estonia, established around PIC, ensures secure authentication and data exchange.

The present overview treats briefly the two main components of the e-government infrastructure: electronic identity and formalized exchange.

I (Digital) Identity Management as a Role of Government

Identity management processes already exist in the physical world, for example, when we want to open a bank account and are asked to show credentials to prove our identity or when we show an identity document to vote at national elections. Identity management in the physical world helps address risks associated with human interactions and increases confidence between the parties interacting. The same is true online, where the lack of a demonstrable link between a physical person and a digital identity can create additional uncertainties that do not exist offline.

Information is an asset today. IT security is the science of protecting information assets from threats. User identification and authentication play a vital role in security controls by providing user identity and assurance before user access to resources is granted to an individual. The user ID is a projection of an actual individual into the computer system.

A computer security system may allow for one or more types of credentials as proof of the user's identity: 1) "Something you know" (static password authentication schemes); 2) "Something you are" (authentication is based on biometric information); 3) "Something you have" (requires the possession of an authentication token like a smart card).

Over the past decade people's computer skills and awareness have significantly increased, which has led to a demand for both digital security and privacy.

While strong user authentication systems are significantly more expensive, more and more systems use multiple-factor authentication schemes, whereby the supplicant may be required to provide more than one type of evidence in order to be authenticated. For example, a supplicant may need to provide biometric evidence ("something you are") and a password ("something you know"), or even a password ("something you know"), biometric evidence ("something you are"), and a security token ("something you have").

Proof of identity or authentication is as strong as the credentials used for that purposes. Governments are the primary issuers of the most trustworthy credentials for individuals' identity attributes such as their name, citizenship, date of birth, civil status, etc. Governments have the ability to collect and securely store also other data necessary to prove personal (digital) identity. Only governments can create a clear framework providing a degree of harmonization for digital identity management at the national level.

In Estonia the identity management policy is closely related to identity documents policy. The Ministry of the Interior is responsible for policy in both areas.

At the heart of the Estonian identity management and identity documents policy are the following principles:

- state monopoly and responsibility to identify a person,
- centralized identity management,
- principle of "one person = one identity",
- unambiguous relationship of digital authentication and digital signing certificates with the user of the document,
- public verification of digital authentication and digital signing certificates via the personal identification code.

Digital identity management is essential to the security of the organization that grants access to resources in its information system. It is also essential to the security of the individual who accesses these resources, particularly when they belong or relate to him/her (e.g. money in a bank, or personal data such as a medical record). By offering security and privacy, digital identity management enables the establishment of a trusted relationship between remote parties.

II Legal Environment

The main legal acts concerning eID management systems are the Identity Documents Act[1] and the Digital Signatures Act[2] regarding general regulation and ID card certificates, as well as the Population Register Act[3] and the Personal Data Protection Act[4] regarding the PIC. The basis for the establishment and administration of databases is imposed by the Public Information Act[5].

The legal basis for identity management is the Identity Documents Act.

Initially, the law concerned only the issuance and usage of the certificates on ID cards and was very laconic. According to clause 9 sub-section 5, 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 documents (like ID cards, digital ID cards, PKI-capable SIM cards, etc).

Amendment of the law that entered into force on 30th of July, 2009 established the concept of digital documents and created a clear basis for digital identification policy. According to clause 3 sub-section 3, a digital document is a document which is prescribed for the digital identification of a person and the verification of identity in an electronic environment. In addition to the earlier regulation of the identity card, the legal basis for the digital identity card was created. The passport was also acknowledged as a document that is prescribed for digital identification of a person in an electronic environment and the basis was created for processing biometric data.

The Estonian legislation distinguishes between authentication and digital signing, leaving authentication out of scope of the law. There are no general regulations on authentication or legal acts that 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. For example, the authentication and authorization in the X-Road environment is regulated by a Government regulation.

The Digital Signatures 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 Signatures Act is harmonized with the European Council Directive on a Community framework for electronic signatures (1999/93/EC).

According to clause 49 of the Population Register Act, the Personal Identification Code is a number formed on the basis of the sex and date of birth of a person that allows the specific identification of the person. The procedure for the formation and grant of personal identification codes is established by the regulation of the Minister of Regional Affairs[6].

There have been no significant privacy concerns with the introduction of the eID in Estonia with one remarkable exception. Initially all active certificates were published in the freely accessible LDAP directory. This made it possible to find out the PIC (and therefore the birthday and gender) of any cardholder. After several years and a couple of scandals in the media, the set-up was changed so that certificates can be queried from the LDAP directory by PIC only.

[1] https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/504112013003/consolide

[2] https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/530102013080/consolide

[3] https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/525112013008/consolide

[4] https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/512112013011/consolide

[5] https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/514112013001/consolide

[6] Minister of Regional Affairs Regulation No 4 from 7th January, 2005 “The formation and grant of personal identification codes“.

III Personal Identification Code

An e-identity management framework is based on persistent life-long electronic identity, which links all online identities together, declaring them as belonging to the same person.

In Estonia the identity of a person is based on a persistent life-long ID called the Personal Identification Code (PIC), which was introduced in 1992.

Formation of PIC is based on the Estonian Standard EVS 585:2007 „Personal Code. Structure", the Population Register Act[7] and a regulation of the Minister of Regional Affairs[8]. The PIC is considered to have been issued to a person after the entry into the Population Register.

According to clause 49 of the Population Register Act, the personal identification code is a number formed on the basis of the sex and date of birth of a person that allows the specific identification of the person. The meaning of numbers forming the Personal Identification Code is described in Figure 1.

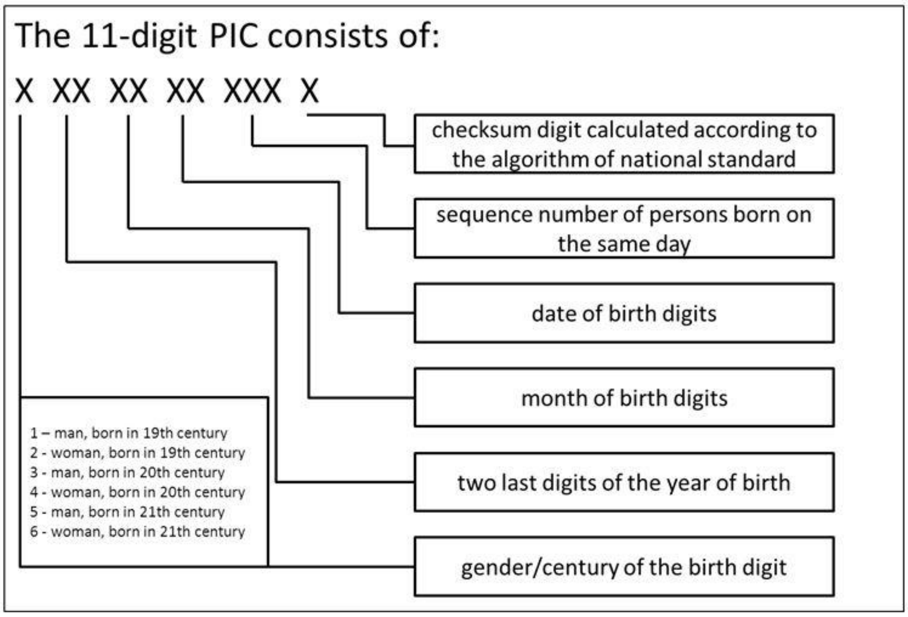

The 11-digit PIC consists of:
X XX XX XX XXX X
checksum digit calculated according to the algorithm of national standard
sequence number of persons born on the same day
date of birth digits
month of birth digits
two last digits of the year of birth
gender/century of the birth digit
1 – man, born in 19th century
2 - woman, born in 19th century
3 - man, born in 20th century
4 - woman, born in 20th century
5 - man, born in 21th century
6 - woman, born in 21th century

Figure 1. Formation of PIC

The PIC contains some privacy-related data – gender and date of birth. However, it is ordinary, non-sensitive personal data as has been emphasized by the Estonian Data Protection Inspectorate (DPI). The Personal Identification Code may be disclosed if it is necessary to identify specific person[9]. At the same time, the DPI emphasizes in its guidelines, issued in 2009, that the use of the Personal Identification Code, as all other personal data, must be guided by the principle of minimization[10].

All certificates of widely accepted eIDs in Estonia (ID card, digiID and mobile ID) contain PIC. The PIC is used as a primary key in the majority of databases containing personal information,

[7] https://www.riigiteataja.ee/en/eli/ee/525112013008/consolide

[8] The Minister's of Regional Affairs Regulation no 4 from 7th of January, 2005 "The formation and grant of personal identification codes".

[9] Initially all active certificates were published in the freely accessible LDAP directory. This made possible to find out PIC (and therefore 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.

[10] The Data Protection Inspectorate Guide "use of personal identification code" from 27th of April, 2009 (changed in 1st of March, 2013).

both in 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 (which in turn contains PIC), which allows for a definite identification of the signatory.

Data on the card – data file and certificates – are available to every card terminal as they are not read-protected. The authentication certificate is available to the service provider upon a successful ID card login. The digital signature certificate is available in the digitally signed document to everyone who sees the document. As a result, PIC in the data file or in the certificate is made available with every electronic use of the ID card. Furthermore, PIC is used as a key in almost every database. The question of cross-use of different registries and databases is a legal matter covered by the Personal Data Protection Act[11] and controlled by the Data Protection Agency[12].

The PIC is generated and maintained by the Population Register, which 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 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 Register issues the PIC also to other state authorities who have to document the person for the first time: usually upon birth or issuance of the residence permit or the right of residence. Thus, as a rule, people get the personal identification code from health care institutions (newborns), as well as from the vital statistics offices, or during Police and Border Guard Board procedure.

IV Digital Documents

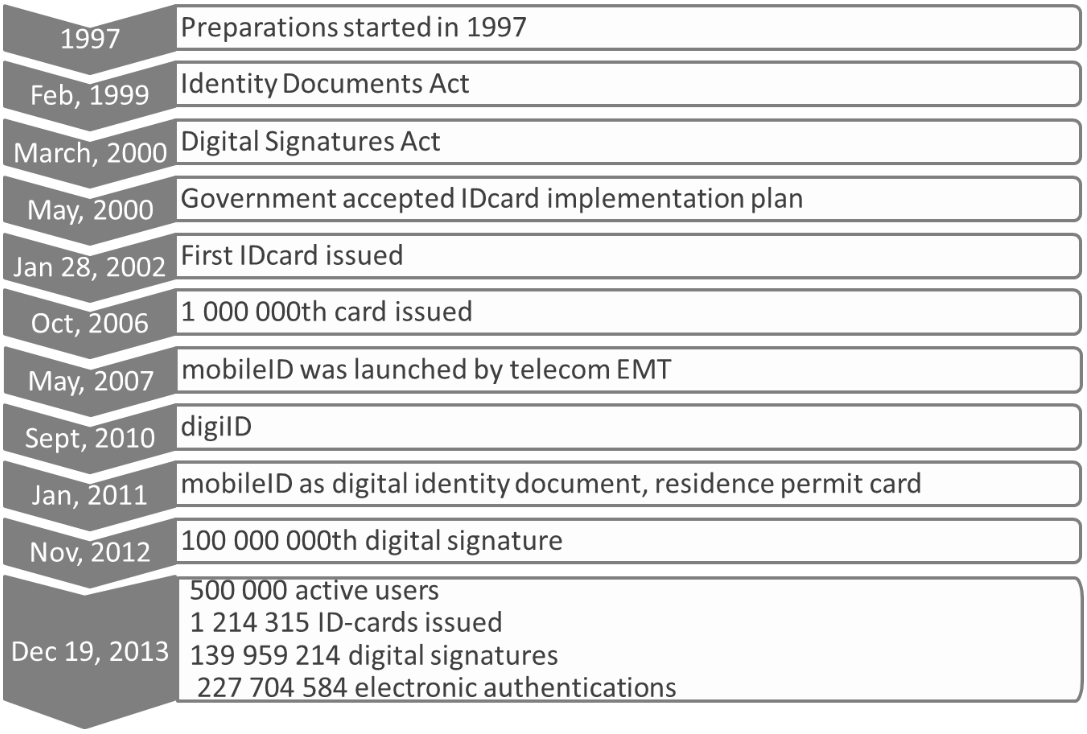
The first digital document – ID card – was issued on 28th of January, 2002. In October 2006 the 1,000,000th ID card was issued, so 90% of the population of Estonia between 15 and 74 years of age held the card. That was a breakpoint, beyond which both the supply and the consumption of e-services started to increase.

The increasing consumption of services led to the need for new means of authentication. Mobile ID was introduced in 2007 and digital identity card in 2010.

The history of digital documents is reflected in Figure 2.

[11] https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/512112013011/consolide

[12] http://www.aki.ee/en



1997	Preparations started in 1997
Feb, 1999	Identity Documents Act
March, 2000	Digital Signatures Act
May, 2000	Government accepted IDcard implementation plan
Jan 28, 2002	First IDcard issued
Oct, 2006	1 000 000th card issued
May, 2007	mobileID was launched by telecom EMT
Sept, 2010	digiID
Jan, 2011	mobileID as digital identity document, residence permit card
Nov, 2012	100 000 000th digital signature
Dec 19, 2013	500 000 active users 1 214 315 ID-cards issued 139 959 214 digital signatures 227 704 584 electronic authentications

Figure 2. History of digital documents

The concept of the digital document was provided by law only in 2009. An amendment of the law that entered into force on 30th of July, 2009 established the concept of digital documents and created a clear basis for digital identification policy. According to clause 3 sub-section 3, a digital document is a document that is prescribed for the digital identification of a person and the verification of identity in an electronic environment.

In addition to the earlier regulation of the identity card, the legal basis for the digital identity card was established. The passport was also acknowledged as a document that is prescribed for the digital identification of a person in an electronic environment.

The law does not restrict what kind of token may bear a digital document. Technical requirements for the token, which can carry a digital document are established by the Regulation of the Minister of the Interior.[13] Compliance with the requirements established for the token of the digital document is evaluated by the competent authority issuing the digital document.

At the present time, the digital documents bearing the identity of Estonian residents are plastic cards (ID card, digiID, residence permit card) and mobile phone (mobile-ID).

ID card, digiID and Residence Permit Card

The ID card allows to consume the following services: physical identification (when traveling within the European Union it serves as a travel document), digital identification, authentication, digital signatures, encryption/decryption (see Figure 3).

[13] Regulation of the Minister of the Interior No 36 from 12th of August, 2010 “Technical requirements for the token of the document to prove digital identity”

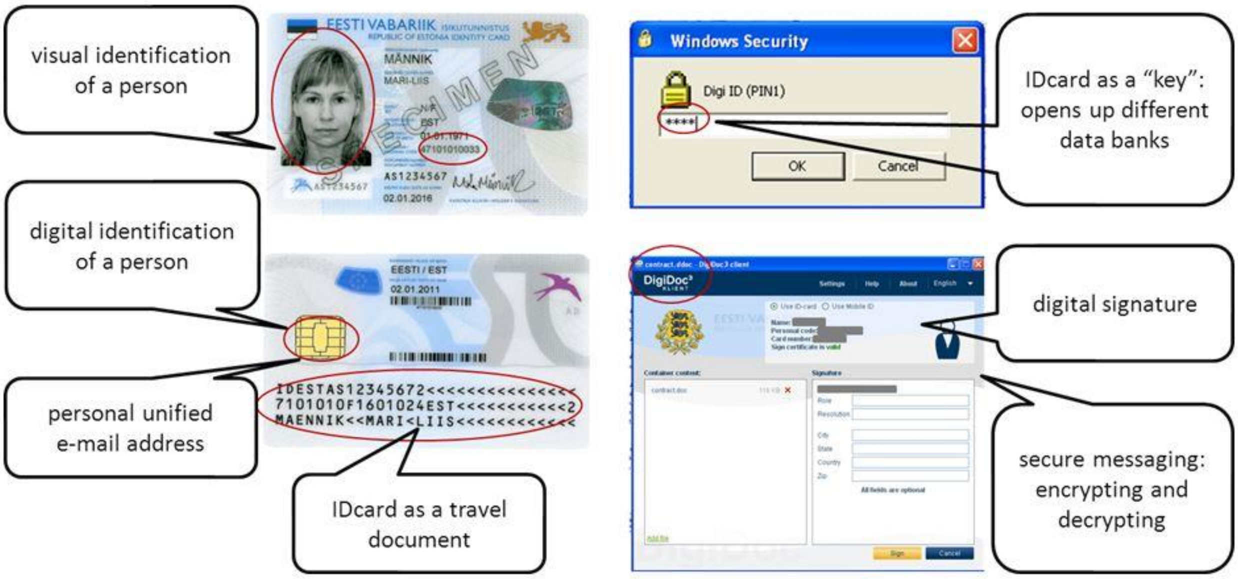

visual identification of a person
digital identification of a person
personal unified e-mail address
IDcard as a travel document
IDcard as a "key": opens up different data banks
digital signature
secure messaging: encrypting and decrypting
EESTI VABARIIK
MÄNNIK
MARI-LIIS
SPECIMEN
47101010033
AS1234567
02.01.2016
EESTI / EST
02.01.2011
IDESTAS12345672<<<<<<<<<<<<<<<
7101010F1601024EST<<<<<<<<<<<2
MAENNIK<<MARI<LIIS<<<<<<<<<<<<
Windows Security
Digi ID (PIN1)
****
OK
Cancel
DigiDoc3 CLIENT
Settings
Help
About
English
Sign
Cancel

Figure 3. ID card and related services

The digital ID card (digiID) (see Figure 4), which is issued from 1st of October, 2010, allows to consume the following services: digital identification, authentication, digital signatures, encryption/decryption. DigiID cannot be used for the physical identification of a person.

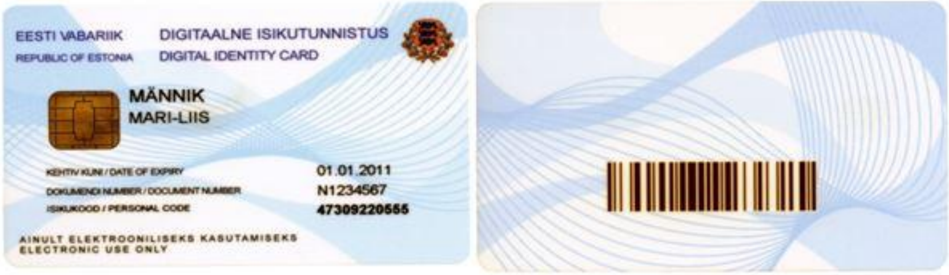

EESTI VABARIIK
REPUBLIC OF ESTONIA
DIGITAALNE ISIKUTUNNISTUS
DIGITAL IDENTITY CARD
MÄNNIK
MARI-LIIS
KEHTIV KUNI / DATE OF EXPIRY
01.01.2011
DOKUMENDI NUMBER / DOCUMENT NUMBER
N1234567
ISIKUKOOD / PERSONAL CODE
47309220555
AINULT ELEKTROONILISEKS KASUTAMISEKS
ELECTRONIC USE ONLY

Figure 4. Digital ID card

Residence permit card (see: figure 5), issued to foreigners from 1st of January, 2011, allows the consumption of the following services: physical identification, digital identification, authentication, digital signatures, encryption/decryption.

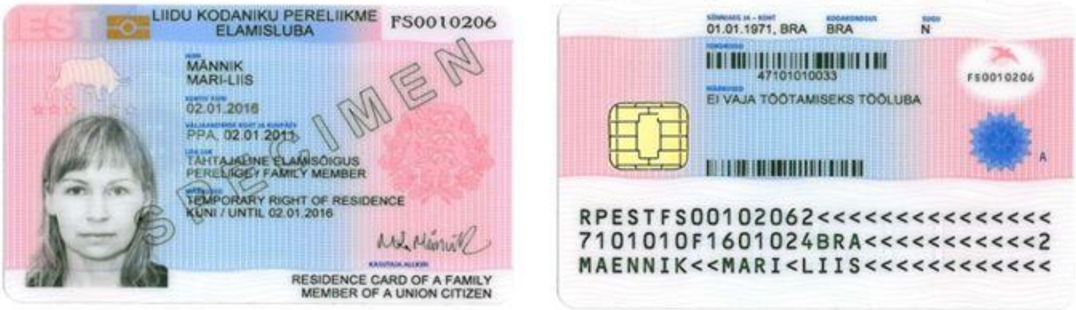

EST
LIIDU KODANIKU PERELIIKME ELAMISLUBA
FS0010206
MÄNNIK
MARI-LIIS
02.01.2016
PPA, 02.01.2011
TÄHTAJALINE ELAMISÕIGUS
PERELIIGEY FAMILY MEMBER
TEMPORARY RIGHT OF RESIDENCE
KUNI / UNTIL 02.01.2016
SPECIMEN
RESIDENCE CARD OF A FAMILY MEMBER OF A UNION CITIZEN
01.01.1971, BRA
BRA
N
47101010033
EI VAJA TÖÖTAMISEKS TÖÖLUBA
FS0010206
RPESTFS00102062<<<<<<<<<<<<<<<
7101010F1601024BRA<<<<<<<<<<<2
MAENNIK<<MARI<LIIS<<<<<<<<<<<<

Figure 5. Residence permit card

The ID1-shaped documents - defined by ISO/IEC 7810 standard[14] - are based on PKI technology, and incorporate two certificates: one for authentication, and the other for electronic signatures[15]. 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. There is no electronically usable biometric information on the card.

Certificates on the ID card contain the following data on the subject:

- name(s), surname(s);
- PIC (containing gender and date of birth);
- Government-assigned e-mail address in the authentication certificate. In order to make use of this e-mail address (e.g. for secure S/MIME e-mail exchange) the user must configure his/her actual e-mail address(es) in the Eesti.ee portal[16]).

The data file contains no more personal data on the subject, apart from some additional technical information like the number of the ID card, card validity dates, etc.

Initially ID cards were issued for a lifetime of 10 years with certificate validity of 3 years. Renewal of certificates is without charge for the end user and the process can be performed over the Internet. In January, 2006 the scheme changed: both certificates and the card have a lifetime of five years.

The roll-out of the ID card was assumed finished in October, 2006 when the threshold of 1,000,000 cards issued was surpassed. Since then, the number of active ID cards has been in the range of 1.0 and 1.2 million.

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 plastic ID card. Obviously, in this case the card offers no digital identity management functionality to the holder. Generally, this option is not widely used.[17]

Mobile ID

Mobile ID can be used for digital identification, authentication and digital signatures.

Mobile ID was introduced to the Estonian market in May, 2007 by the largest mobile operaator EMT in co-operation with Certification Centre (SK). Certification Centre (SK) provides mobile authentication and mobile signing services to service providers.

In order to get mobile ID, the user needs **to replace a SIM card with the PKI-capable one**. Although the registration process is performed by the mobile operator, it is not considered trustworthy enough.

[14] ISO/IEC 7810. Identification cards. ID1 format card size is 85.60 x 53.98 mm. Most banking and ID cards are of this size.

[15] The issuance process for both certificates is the same and Estonian experts opinion is that both of them need to be considered as qualified. Both certificates include the label of qualified certificate. Part of the European Union experts, however, are of the opinion that only the signature certificate is considered to be qualified and the authentication certificate has emphatically not been given this label. The reason is that the European Council Directive on a Community framework for electronic signatures (1999/93/EC) does not address the authentication certificates as such. At the same time, the European Union uses the term qualified certificates described precisely in this Directive.

[16] See https://www.eesti.ee/eng

[17] More information can be obtained from http://www.id.ee/?lang=en&id= and http://www.politsei.ee/en/teenused/isikut-toendavad-dokumendid/

Therefore, the user needs to "activate" his/her mobile-ID with an ID card in the web environment. In this manner the issuance of the mobile ID is bound to the security and quality of the ID card.

Mobile ID provides certain advantages for the end user over the ID card: the user does not need a smartcard reader attached to the computer and does not need to install any specific software to use it.

Currently mobile-ID is available from three mobile operators and the number of active users is approximately 45,000.

Mobile ID certificates contain the same personal information on the subject as certificates on ID cards.

V Digital Signatures

One of the main reasons for introducing the ID card was to actually implement the Digital Signatures Act[18] and provide Estonian residents with means for digital signing. Free tools for end users and system integrators were released back in 2002 and are still evolving. As a result, Estonians share a common understanding of a digitally signed document, which is in file form, fully standardized and widely accepted by everyone, even courts of law.

A piece of software called "DigiDoc Client" comes with the package of the base ID card software. The DigiDoc Client allows for digital signature creation and verification. In addition to that, the online DigiDoc Portal provides the same functionality (but requires to upload your sensitive document to the service provider). Finally, there are web-service and multiplatform program libraries available for system integrators, allowing all of them to share the same file format.

There are basically two scenarios for creating digital signatures:

- in the Service Provider's environment: a user is requested to sign within the web application (by entering PIN2 of the ID card). The result of the signing must be available for download in file form for independent verification and archiving;
- As a stand-alone process using the desktop application (DigiDoc Client). The resulting file can be uploaded or sent to any party.

This development has resulted in massive use of digital signing, as digital signatures created with those tools are completely legal and replacing universally hand-written signatures. There are legal cases where digital signatures are considered "better" than handwritten ones – e.g. in establishment of companies. Digital signatures are massively produced by Internet banks, as all transactions are required to be signed digitally (in case the user logged in with an ID card or mobile ID).

VI Stakeholders and Issuance Process

The Citizenship and Migration Bureau (CMB) under the Police and Border Guard Board (PBGB) is the body issuing ID cards, digiID and residence permit cards. CMB/PBGB cooperates with private sector suppliers – TRÜB AG Baltic and Certification Centre (SK) in the issuance process of the ID card. There is currently just one certification authority (CA) in Estonia - SK.

[18] https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/530102013080/consolide

The personalisation of digital IDs takes place in Service Offices and the waiting time is ca 30 minutes. The card is made of PVC and there are no security features, visual data is printed by thermoprinter.

The issuance procedure of mobile-ID is different. In 2011, in cooperation with the Ministry of Internal Affairs, EMT and Certification Centre (SK) the opportunity to apply for government-guaranteed mobile ID certificates was created. Persons who already had a mobile ID, if desired to have government-guaranteed certificates, had to apply for new certificates. The state added digital identity management to the technological solution. A prerequisite for the government-guaranteed mobile ID certificates is the existence of a valid ID card. Government-guaranteed mobile ID certificates can be requested only electronically.

Government-certified mobile ID application process is as follows. At first, a mobile ID contract with a mobile network operator has to be concluded to get a PKI-capable SIM card, with the person identified with ID card. Then a holder applies digitally for (government- guaranteed) mobile ID certificates on the website of PBGB. Application is processed and decision is made automatically: certificates activation order is sent to Certification Centre (SK), certificates are activated and holder is informed about the new document status.

This bounds the issuance security of the mobile ID to the security of the national ID card.
Actors and relations around eID co-ordination in Estonia are illustrated in Figure 6.

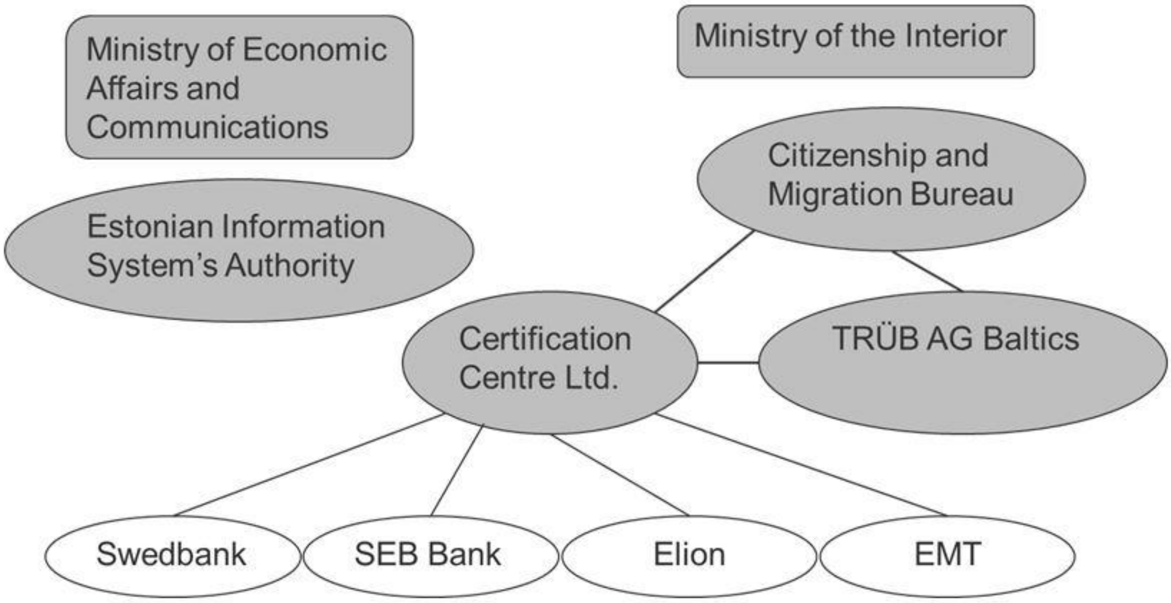

Ministry of Economic Affairs and Communications
Ministry of the Interior
Citizenship and Migration Bureau
Estonian Information System's Authority
Certification Centre Ltd.
TRÜB AG Baltics
Swedbank
SEB Bank
Elion
EMT

Figure 6. Actors and relations around eID co-ordination in Estonia.

There are two major ministries in Estonia involved with eID matters:

- Ministry of the Interior (MoI). Citizenship and Migration Bureau (CMB) is one of subordinated institutions of this ministry directly responsible for the issuance and maintenance of identification documents and maintaining (electronic) identities of residents at large.
- Ministry of Economic Affairs and Communications (MEAC). The Department of State Information Systems (RISO) of this ministry is directly responsible for the general ICT coordination in 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 Information System's Authority (EISA), which is a subdivision of the MEAC, is responsible for the 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.

Private sector plays a significant role in the Estonian eID ecosystem. ID card manufacturing and personalization is outsourced to TRÜB Baltic AG; certification and validation services are provided by the privately held Certification Centre (SK). The latter functions also as an excellence centre for electronic usage of the ID card, providing:

- software for ID card electronic use, including digital signature software framework;
- end-user support;
- support and services to Service Providers making use of the ID card.

VII BankID: Password Cards and PIN Calculators

The most popular method for authentication has been to use Internet bank authentication. Virtually all banks (5 major ones covering 99% of the banking customers) provide authentication service to third 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 working with the selected e-service.

There are basically 3 methods for logging into an 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.

Reasons behind the popularity of bank authentication include:

- relatively early start of Internet banking in Estonia (1996) with provisioning of authentication service to third parties;
- large number of Internet bank users (nearly 100% for people between 16 and 74);
- simple to use – no special hardware (e.g. smartcard reader) or software (e.g. drivers) is needed.

VIII Data Exchange Layer X-Road

The data exchange layer X-Road is a technical and organizational environment that enables secure Internet-based data exchange between the state's information systems. The X-Road environment was launched in Estonia in 2001. The Estonian information system is shown on Figure 7.

According to the Public Information Act[19] clause 43^9 sub-section 5, exchange of data with the databases belonging to the state information system and between the databases belonging to the

[19] https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/514112013001/consolide

state information system shall be carried out through the data exchange layer of the state information system.

The X-Road allows institutions/people to securely exchange data as well as ensures people’s access to the data maintained and processed in the state databases. All public and private sector enterprises and institutions can connect their information systems with the X-Road. This enables them to use X-Road services in their own electronic environment or offer their e-services via the X-Road. Joining the X-Road enables institutions to save resources, since the data exchange layer already exists. This makes data exchange more effective both inside the state institutions as well as in the communication between a citizen and the state.

The X-Road also facilitates public enquiries, for example the forwarding of insurance data to the Estonian Health Insurance Fund. In order to use the services, the end users must first authenticate themselves with an ID card or an Internet bank account, while business people can do this based on their listing in the Commercial Register.

In case of citizens, the X-Road enables them to use its services through different portals, allowing citizens to use state databases for their purposes and to control the information related to themselves on these databases.

Officials can use the services intended for them (for example the document exchange centre) in the information systems of their own institutions. This facilitates the officials’ work, since it avoids the labour-consuming task of processing paper documents, large-scale data entry and data verification. This means that communication with other officials, businesspeople and citizens is faster and much more accurate.

An overview of X-Road is available online[20].

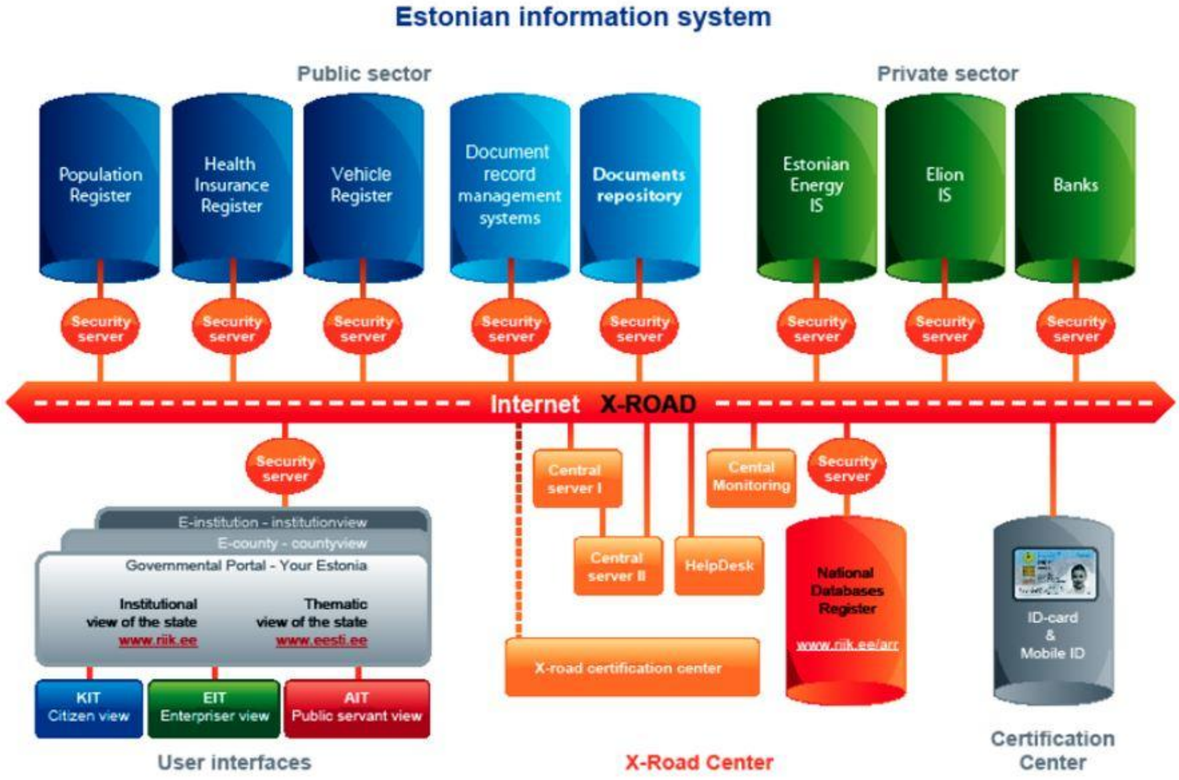


Figure 7. Estonian Information System.
Source: https://www.ria.ee/public/x_tee/xRoadOverview.pdf

[20] https://www.ria.ee/public/x_tee/xRoadOverview.pdf

In addition to it being an excellent and secure technical solution, it is necessary to point out two other characteristics that hasten the development of e-government:

- The X-Road does not have to be used by all the authorities at the same time, which permits a more gradual transition. The more innovative authorities can do it more quickly and more skeptical ones can wait to see what happens. This means that there is no need to put pressure on anyone – they will have the chance to see the advantages of this solution during its development;
- Employing the X-Road does not require a large-scale alteration of the already established databases and information systems, which will reduce the potential resistance to these mergers, which is a major advantage.

VIII Authentication Policies

Estonia does not have an official policy defining the hierarchy of different e-authentication methods. However, PKI-based authentication methods are preferred by the public sector policy.

In practice all above-mentioned authentication methods (ID card, mobile ID and Bank ID) are widely used in services requiring true identity both in public and private sector. Most of sites supporting ID card login also support mobile ID.

Authentication to web environment is carried out using standard TLS/SSL protocol with Client Authentication, supported by most of the browsers used (IE, Mozilla, Safari, Chrome). The protocol implies that the Service Provider will receive full certificate of the user with PIC within.

A few services like e-health, Internet voting and digital signing are usable with ID card (or mobile-ID) only.

Electronic personal identification with an ID card (digiID) or mobile ID is better and more secure than identification with a user name and password in several ways.

- Electronic authentication provides assurance regarding the fact that correct data is received from the ID card, thereby decreasing the risk of users submitting false data to service providers.
- All service providers are able to directly and securely provide their services to all ID card holders without prior registration.
- This is also convenient for the users as they need not remember various user names and passwords – the same card and PIN are valid for all services.

For checking the validity information of certificates in real time, the validity verification service of the Certification Centre (SK) should be used. The service ensures secure electronic personal identification and gives digital signatures their legal effect.

Sources

Digital Identity Management. Enabling Innovation and Trust in the Internet Economy. – OECD 2011.

Dobromir Todorov. Mechanics of User Identification and Authentication: Fundamentals of Identity Management. June 18, 2007 by Auerbach Publications.

eID Interoperability for PEGS: Update of Country Profiles study. Estonian country profile. IDABC. July 2009.

Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL) Profile.

ISO/IEC 7810. Identification cards.

Machine Readable Travel Documents Third Edition — 2008-Doc 9303. Part 3. Machine Readable Official Travel Documents. Volume 1.

European Council Directive on a Community framework for electronic signatures (1999/93/EC).

Websites:

https://www.riigiteataja.ee/en/

https://www.eesti.ee/eng

https://www.ria.ee/en/

http://www.sk.ee/en

http://www.politsei.ee/en/

http://www.aki.ee/en