

The Estonian ID Card and Digital Signature Concept

Principles and Solutions

Whitepaper

Version: June 5, 2003

Contents

Contents	2
Status of the document	3
Introduction	3
Intended audience	3
Current project status	3
Principles.....	4
Digital signature regulation.....	4
Digital signature concept	4
Certification Service Providers (CSP-s)	4
Time-stamping Service Providers (TSP-s)	4
Supervision – Registry and Ministry	5
Foreign Certificates.....	5
Identity Document Regulation.....	5
Mandatory document	5
Card appearance and layout	5
Electronic data on card.....	6
Certificates	7
E-mail address.....	7
Data protection.....	8
Organizational structure, card issuing and operation.....	8
Solutions	10
Certificate profiles and e-mail addresses	10
Certificate validity verification methods	10
OCSP, time-stamping and evidentiary value of digital signatures	10
Document format and DigiDoc.....	11
Roles, authorizations and organizations' validations	12
Further development: replacement and alternative cards	13
International validity of digital signatures	14
The OpenXAdES project	15

Status of the document

This document is prepared by AS Sertifitseerimiskeskus (www.sk.ee). You may freely distribute it in original verbatim form (without making any changes). The Estonian ID card project information, including the newest version of this whitepaper, is available online at <http://www.id.ee>. You may contact us at info@id.ee.

Introduction

Estonia has implemented ID card as the primary document for identifying its citizens and alien residents living within the country. The card, besides being a physical identification document, has advanced electronic functions that facilitate secure authentication and legally binding digital signature, in connection with nationwide online services.

This whitepaper gives an overview of the principles behind the project and explains the choices and decisions made while carrying out the card project. It also presents an overview of how the associated services and applications are implemented.

Intended audience

The first part of the whitepaper, "Principles", is written for decision-makers and potential common users from a legal and economic perspective. The second part, "Solutions", is for implementers and assumes knowledge about basic PKI concepts.

Current project status

The first Estonian ID cards were issued in January 2002. In one year, more than 130 000 cards have been issued, and the total figure is expected to grow to more than 350 000 by the end of 2003 (about 25% of the whole population).

The card is meant to be universal and its functions are to be used in any form of business, governmental or private communications. It is already helping people to make everyday communications more convenient. You can find more details about the implementation and applications below.

Principles

Digital signature regulation

Estonian parliament (Riigikogu) passed the Digital Signature Act (hereinafter DSA) on March 8, 2000, and it entered into force on December 15, 2000. The law regulates issues that are essential for implementing a nationwide PKI and digital signature infrastructure. The law is available online at <http://www.legaltext.ee/text/en/X30081K3.htm>.

Digital signature concept

According to the Estonian DSA, digital signatures are equivalent to handwritten ones, provided that they are compliant with the requirements set forth in DSA and if other laws do not regulate otherwise. Thus as a rule, digital and handwritten signatures should be equivalent in document management in both public and private sectors. DSA also states that public sector organizations must accept digitally signed documents.

The requirements set forth in DSA to digital signatures state that digital signature must uniquely identify the signatory, be bound to the signed data in such a way that makes changing the data after signing impossible without invalidating the signature, and identify the time of signing (assuming the use of time-stamping or equivalent time establishment technology).

In the terms of EC directive 1999/93/EC, DSA only regulates advanced electronic signatures. Other types of electronic signatures can of course be used, but DSA does not give them legal power.

Certification Service Providers (CSP-s)

DSA regulates the work of CSP-s in Estonia, setting forth requirements to them and regulating their operation and supervision. CSP-s may only be legal entities with a regulated minimum share capital, they must be entered in the National Certificate Service Provider Registry (see below) and must carry out an annual audit to ensure organization and system reliability. CSP-s must also have liability insurance to safeguard against compensating faults made while providing the service.

It is important to note that according to DSA, CSP-s certify only real persons identifiable by name and ID code – issuing certificates to pseudonyms is not currently covered by DSA. It was discussed in the parliament during the law adoption process, but was considered to be an additional unnecessary risk and so far, no need for this has been seen.

Time-stamping Service Providers (TSP-s)

DSA also regulates the work of TSP-s and the comparison of time stamps between TSP-s. The requirements to service providers are generally the same as those to CSP-

s. According to DSA, a time stamp is simply a data unit that proves that certain data existed at a certain moment. DSA does not define time stamps in more detail, but states that they must be bound to the timestamped data and issued in such a way that it would be impossible to change the timestamped data without invalidating the timestamp.

Supervision – Registry and Ministry

The National Registry of Certification Service Providers contains data about all Estonian CSP-s and TSP-s. Although it confirms the public keys of CSP-s, it is technically not a root CA in Estonia. Instead, it functions as a supervisory authority, confirming the results of service providers' annual audits among other things. The Ministry of Economy and Communications, in whose administration area the registry works, has the right to verify audit results and inspect the service providers' premises and relevant information.

Foreign Certificates

DSA regulates the recognition of foreign certificates, stating that in order for them to be recognized equivalent to those issued by Estonian CSP-s, they must be either confirmed by a registered CSP, be explicitly compliant with DSA requirements or covered by an international agreement.

Identity Document Regulation

Identity documents in Estonia are regulated by the Identity Documents Act. The law is available online at <http://www.legaltext.ee/text/en/X30039K7.htm>.

Mandatory document

According to the Act, possessing an ID card is mandatory for all Estonian residents and also for all aliens who reside permanently in Estonia on the basis of a valid residence permit with a period of validity of at least one year. There are no sanctions for not having a card, but it is expected that as the first Estonian passports were issued in 1992 with validity period of 10 years and they are expiring, most people will apply for either only ID card, or ID card together with passport when renewing their documents in the period 2002-2006. By the end of 2006, one million cards will have been issued.

There is only one version of the document: there are no different optional features that users can opt out of or choose to (not) have. All documents are equipped with a chip containing electronic data and certificates (see below). It is understood that some users may have doubts or fears about electronic use of the card, but remedies are provided for that: if users do not wish to use the electronic functions of their cards, they can suspend the validity of their certificates, thus making it impossible to use the card electronically. Certificate suspending or revoking also removes user's data from public certificate directory.

Card appearance and layout

The card looks as follows.

certificate contains the holder's unique e-mail address. Read more about certificates and e-mail address below.

Certificates

Each issued ID card contains two certificates: one for authentication and one for digital signing. There are also two associated private keys, protected by two separate PIN codes, on the card. The certificates contain no restrictions of use: they are by nature universal and meant to be used in any form of communications, whether between private persons, organizations or the card holder and government. They contain no roles or authorizations: those where required must be managed using some out-of-band method (also see below, "Roles, authorizations and organizations' validations").

The certificates contain the card holder's name and national ID code. It is agreed in Estonia that this data is public by nature. The certificates identify the card holder uniquely because even though there may be name overlaps, the national ID code is unique. In addition, the authentication certificate contains the card holder's e-mail address.

In terms of the European Council and Parliament digital signature directive 1999/93/EC, all the certificates on Estonian ID card are qualified certificates.

E-mail address

The authentication certificate on each ID card contains the card holder's government-assigned e-mail address in the format [firstname.lastname_NNNN@eesti.ee](#), where NNNN are four random numbers. The random numbers are necessary to provide unique e-mail addresses even to persons with the same name. The address does not change with subsequent certificate or card issuing – it is guaranteed to be a person's "lifetime" address.

There is no real e-mail service associated with the address. It is a merely a relay address which forwards e-mails to users' "real" addresses (e-mail accounts). Each user must configure the forwarding addresses using an online service made available for this purpose, and may reconfigure the addresses as often as he or she pleases. Up to five forwarding addresses can be specified.

The address is supposed to be used in communications from government to the person, but it can also be used in communications between persons and companies and private persons themselves. The addresses are available online to anyone through CSP-s certificate directory.

The address can be used as a simple e-mail address, but using the address and the authentication certificate on the card, users can also digitally sign and encrypt their e-mail. The digital e-mail signature is not legally binding and not covered by DSA, but it provides receivers additional confirmation of sender authenticity. E-mail encryption and signing using certificates on smart card is a standard function of various e-mail applications.

Anti-spam measures are implemented in the forwarding server. In addition, spamming is illegal in Estonia and spammers will be prosecuted accordingly.

Data protection

The data protection question is not very relevant in the context of Estonian ID card because there is very little private data involved in the card issuing and further utilization process. There is a broad Personal Data Protection Act in effect in Estonia which regulates the use of personal data and databases containing personal data by public authorities and private entities, and Estonian Data Protection Inspection is the government body overseeing that the requirements of the act are met and enforcing compliance if necessary.

The certificates on the card are available publicly in a directory service and contain only the card holder's name and personal ID code, which are considered public data by nature in Estonia. In addition, e-mail addresses in authentication certificates are also available in the directory. The directory contains only valid (active) certificates: if a person suspends or revokes his certificate, it is also removed from the directory and the data are no longer available.

The public data file is not published anywhere online. The personal data on the card in visual and electronic format are accessible only to those persons to whom the card holder physically presents the card.

The general stance to ID card and data protection in Estonia is that the card should contain as little private data as possible. Instead, the data should be kept in databases at relevant authorities, and a person can use the card as key (authorization method) to access his or her data in the database.

Organizational structure, card issuing and operation

The card issuing as well as its further operation is done in close public private partnership. There are three main organizations that are associated with issuing and operating the ID card and the associated infrastructure.

Estonian Citizenship and Migration Board (hereinafter CMB) is the government organization responsible for issuing identification documents to Estonian citizens and alien residents, as required in the Identity Documents Act. CMB is in the supervision area of Estonian Ministry of the Interior. CMB receives the card application from citizens.

AS Sertifitseerimiskeskus ("certificate centre", hereinafter SK), founded by two major Estonian banks Hansapank and Eesti Ühispank and two telecom companies Eesti Telefon and EMT, functions as CA, maintains the electronic infrastructure necessary for issuing and using the card, and develops the associated services and software. SK also takes care of delivering the card to its holder through Hansapank and Eesti Ühispank bank offices.

TRÜB Baltic AS, subsidiary of Swiss TRÜB AG, is the company that personalizes the card.

The card issuing process starts when a person submits card application to CMB. He can do this either in person or by regular post. At CMB-s request, TRÜB personalizes the card and SK issues the certificates to the card. SK also issues the card and its PIN

codes to card holder at a bank office specified by the card holder at time of application.

The secret keys are generated on the card at the time of personalization – the keys will never leave the card. Also, for security reasons, there is no key escrow mechanism in place for either key. The authentication key/certificate can be used for encryption purposes, but this is mainly seen as a tool for secure transport, e.g. encrypted e-mail – the ID card is not supposed to be used for long-term document encryption, since the certificates are only valid for three years.

For further operation of the card, SK maintains the associated electronic services including an LDAP directory service, OCSP validation service and other necessary services for online validity and digital signature confirmations. 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 (see below, "Document format and DigiDoc"). In addition, SK maintains a 24-hour telephone hotline that can be used for immediately suspending the validity of certificates in case of card loss or theft.

Solutions

Following are a number of issues and questions that have been solved when implementing the Estonian ID card and digital signature infrastructure.

Certificate profiles and e-mail addresses

The certificates on Estonian ID cards are standard X509v3 certificates. The authentication certificate contains the card holder's e-mail address. The certificate profile is available in a separate document.

Certificate validity verification methods

According to Estonian DSA, CSP-s must provide "a method of verifying certificate validity online". SK as the issuer of certificates to ID cards provides users three ways of checking certificate validity.

CRL-s are provided, containing the list of suspended and revoked certificates. CRL-s are standard but outdated method, because as of January 2003, CRL size has grown to over 1 MB in one year and it is not very convenient to use. CRL-s are mainly provided for backwards compatibility and standards compliance. SK updates its CRL twice a day. Delta CRL-s are not provided.

The second method is an LDAP directory, containing all valid certificates. The directory is updated in real time – if a certificate is activated, it is uploaded to the directory, and if it is suspended or revoked, it is removed from there. Among other things, this provides everyone a chance of finding the e-mail address of any ID card holder. Restrictions are in effect as to the maximum number of responses returned to one LDAP query to protect against server overload.

The most convenient method of verifying certificate validity is SK's OCSP service. It can be used for simple certificate validity confirmations, but also for validity confirmations ("notary confirmations") to digital signatures. SK provides a standard OCSP service compliant with RFC 2560. An important detail is that according to the RFC, OCSP responses are supposed to be based on CRL-s and therefore may not necessarily reflect the actual certificate status. In contrast, SK has implemented its OCSP service in such a way that it operates directly off its master CA certificate database and does not use CRL-s. Thus, SK's OCSP responses reflect actual (real-time) certificate status.

OCSP, time-stamping and evidentiary value of digital signatures

For legally binding digital signatures, time is an extremely important factor. According to the Estonian DSA as well as common sense, only signatures given using a valid certificate are to be considered valid. On the other hand, to provide remedy to the risk that the signing device (ID card) may be stolen together with PIN-s and digital signatures could be given on behalf of the user by someone else, users have the chance of suspending their certificate validity using a 24-hour telephone hotline operated by SK. With these two concepts combined, users must be able to clearly differentiate the signatures given using a valid certificate from those given using a

suspended or revoked certificate. Thus, there is a need for a time-stamping and validity confirmation service that binds the signature, time and certificate validity.

Another important concept concerning signature validity is that the signature must be valid also when the certificate has already expired or been revoked. If a certificate is suspended by the card holder or anyone else, the card holder can reactivate it at a bank office.

SK chose to base its time-stamping implementation on standard OCSP. This enables the service provider to conveniently deliver certificate validity and time information in one convenient query response. The OCSP protocol query format contains a Nonce field, which protects against replay attacks. Instead of cryptographically random data, the Nonce field is set to contain the hash of the data to be signed, because it can also be interpreted as just a random number. According to the RFC, the OCSP responder signs its response which in SK's case, contains the original Nonce (document hash), response providing/signing time and ID of the certificate used to give the signature, binding the three pieces of data together and providing the validity confirmation for the digital signature. SK stores the signed response in its log as evidence material.

The main features of the above concept are:

- it guarantees long-time digital signature and document validity
- it is based on standard protocols and standards
- verification process is lightweight and the document is self-contained – no additional verification services are needed

SK has implemented all of the above, including both client and server parts, in its DigiDoc digital signature architecture.

Document format and DigiDoc

In order to bring digital signatures into everyday life, common understanding and signature handling practices are required. In addition, software and technology must be available for anyone interested, in order to create compatible applications. After all, the key to unleashing potential digital signature benefits lies in communication between organizations, not within one organization. Therefore, it is vital that all organizations in a given community interpret and understand digital signatures the same way. In case of Estonia, the community is the whole country.

A number of digital signature implementations and applications are available on the market, all claiming to be suitable for specific purposes. However, no known application or implementation of the latest standards was found which would suit the needs of the Estonian project, and reliance on foreign software providers guaranteeing the functioning of a country's everyday life relying on digital signatures can also be seen as a strategic risk. Therefore, a whole new approach – and a whole new software architecture – was needed.

In 2002, SK together with its partners created an all-around digital signature architecture called DigiDoc. As the name suggests, DigiDoc aims to meet all the needs users might have about digital signature creation, handling and verification.

On the server side, DigiDoc provides an RFC2560-compliant OCSP server, operating directly off the CA master certificate database and providing validity confirmations to certificates and signatures. On the client side, it provides a number of components.

The most important component is digital document format, which is key to common digital signature implementation and practice. As of 2002, a number of standards have been adopted or are in preparation. SK based the DigiDoc document format on XML-DSIG standard. In February 2002, ETSI published its extensions to XML-DSIG as ETSI TS 101 903, also known as XAdES. DigiDoc document format is a profile of XAdES, containing a subset of its proposed extensions. The DigiDoc format is described in a specification document.

Based on the document format, a library was developed in C language that binds together the following:

- DigiDoc document format
- SK's OCSP validation service
- Interfacing with the user's ID card using Windows' native CSP interface or cross-platform PKCS#11

The DigiDoc library provides easy-to-use interfaces to all of the above and there is no need for application developers to know OCSP protocol specifics or DigiDoc (XAdES, XML-DSIG) format internals. It can be embedded in any application and on top of it, a COM interface has been implemented, making it easy to add DigiDoc support to any Windows application supporting COM technology. A Java implementation is also provided.

However, providing the libraries and formats was not enough because these do not add value to end users without real applications. Although it is expected that DigiDoc support will eventually be present in most Estonian document management systems, web sites dealing with documents etc, a number of example or "reference" applications are also provided. DigiDoc Client is a Windows application that lets users simply sign and verify documents, and DigiDoc portal is an application that lets users do the same online without the need to install any stand-alone software. Naturally, both are based on the same DigiDoc library and thus fully compatible – signatures given in Client can be verified in portal and vice versa.

The libraries, specifications and applications are provided to Estonian public free of charge, and it is expected that digital signature usage in common life and everyday business and government practices will grow significantly already in 2003. The first official digital signatures in Estonia were given using DigiDoc Client on October 7, 2002, and implementing digital signature on a national scale naturally takes a while.

Roles, authorizations and organizations' validations

In connection with implementing PKI and digital signatures, the question of roles and authorizations has arisen in various projects. It is assumed that certificates for digital signing may be issued for specific purposes only, and that a person's roles can be embedded in role certificates that are then used for authenticating the certificate holder into different systems and giving digital signatures in different roles. Thus, a person needs additional role and signature certificates for each different role he or she

has, and the number of certificates grows, creating substantial interoperability and scalability issues.

The Estonian approach states (as also said in the Estonian DSA) that a digital signature given using a digital signing certificate is no different than a handwritten one. A person's handwritten signature does not contain his or her role – the role and authorization are established using some out-of-band method (out-of-band in the context of certificates). The same approach also goes for authorization while authenticating – a person's certificate should not contain his or her authorization credentials. Instead, everyone has a similar universal key (authentication certificate), and the person's role and authorization can be determined using some other method (e.g. an online database) based on that key.

A practical example illustrating the above concept is signing documents in organization using power of attorney. In traditional PKI environments, this has been done using some form of attribute certificates where issues described above arise. In Estonian and PKI context, we could ask how is power of attorney given in real life, and use the same principles in electronic document management. Traditionally, power of attorney is granted in the form of a document signed by the person giving the authorization. The document is then given to the person who receives the authorization and who can then present the document to relevant parties if necessary. The same can be done electronically: the person giving the power of attorney can sign the document using his own universal personal certificate, and forward the document to the person who is given authorization. The person can then enclose the digital power of attorney with any further documents he signs. The person receiving the document can then verify both the original signed document and the enclosed power of attorney that confirms that the person indeed had the right to sign such a document.

Attribute certificates can of course be used in connection with the universal certificates and documents outlined above, but the Estonian concept is geared more towards universal certificates.

An exception to the above is organization's validation. Digital documents sometimes need to be validated by organizations, so that other organizations can be sure of the identity of the organization where the document originated. This is useful for e.g. signing pieces of databases (e.g. bank statements) online, to be presented to other organizations. For this, SK issues certificates to organizations that can be used to sign documents digitally. Technically, they are equivalent to personal signing certificates on everyone's ID card, but legally, they are not viewed as signatures and need not be covered by law, because according to the Estonian law, only real persons can give signatures. The "organizations' signatures" must therefore be viewed simply as additional tools for proving information authenticity (that it really originated from a specific organization) which may or may not be accompanied by a digital signature of a real person working in that organization. Still, the PKI complexity stops here, and besides personal and organizational signature certificates, there is no need for personal role certificates or anything else more complex.

Further development: replacement and alternative cards

As of the beginning of 2003, a number of ideas are being discussed for improving the availability and usability of digital signatures in Estonia. One of them is the

"replacement ID card", or backup card. The main concern here is that the card issuing process described above is quite complex and according to current regulations, it may take up to 30 days for a person from the moment of presenting the application to receiving the card. If a card is lost or damaged and a person needs to get a new one, this may mean that he or she may not be able to give digital signatures for 30 days which may not be acceptable in some high-stake business environments. Therefore, a possibility could be established that current ID card holders might get a "backup card" to minimize the extent of the above problem. However, this is currently not implemented, and another remedy for the problem is that the above organizations will just implement an "express service" which would be more expensive but quicker method of getting an ID card in the "normal" way.

Another upcoming service is "alternative card". National ID card need not be the only carrier of digital signing certificates. Also, SK can issue certificates to people who do not have Estonian residency and wouldn't need an Estonian ID card. This is also required by large companies who are already using smart cards for their internal services in a multinational operation, and would like to have digital signing certificates issued by SK to be added to their internal cards and create a common infrastructure across different countries. The company itself would act as Registration Authority, and SK would be responsible for issuing certificates in response to certificate requests, as is also the case with regular ID cards. Still, this "alternative card" will remain a niche solution and for the general public, the Estonian national ID card is the universal signing tool for whatever role a person may be acting in.

International validity of digital signatures

Legally binding digital signatures in international communications are an emerging area. As most countries have not yet implemented their domestic practices and legislation to such extent that digital signatures would be widely used in daily communication, the harmonization of such practices remains a question of the coming years.

The widening of standards has led to diversity, not interoperability. Current standards and to some extent also legislation tries to cover all possible PKI- and certificate-related transactions and give them different amounts of legal power. This has again led to great complexity and confusion.

The position of Estonian ID implementers is that in this respect, digital world is analogous to traditional document management and there are two basic sorts of documents and communications.

- 1) legally binding signed documents, whether signed digitally or by hand
- 2) any other form of communication which need not be regulated so strictly

Notarized documents (in the traditional sense, associated with the institution of notary public) are a special case of 1).

For example, the Estonian public administration regulation states that in all cases where signing a document or management act is not necessary, the case can be resolved by any other communication means which is convenient to both parties, e.g. signed and/or encrypted e-mail, faxing, phone call, oral conversation. Officials just have to make appropriate notices in their document management systems about how

the case was resolved, and include appropriate contact and other details. But whenever signing a document is required, it must be signed either digitally or by hand.

For internationally interoperable digital signatures, both parties (countries) must recognize the signatures issued by the rules of the other party. There are three main technical aspects to consider.

- **what is the quality of issued certificates.** In the terms of 1999/93/EC, the certificates used to give legally binding digital signatures should be qualified certificates, clearly indicating the signing person.
- **what format is used for the signature and document itself.** The DigiDoc system described above is certainly a valid option, as it is based on the XAdES standard which, to date, is probably the most advanced standard for digital signatures and the associated technical information. An important aspect is that the format and software must be available, preferably open source, for public audit, review and scrutiny. Both the XAdES standard and DigiDoc source code are available to any interested party.
- **what infrastructure services are associated with the signing and certification to ensure system reliability and signature validity.** This assumes a certain quality of certificate-related services, such as signing device delivery to end users and the available of emergency helpdesk for certificate suspension, as well as the service that the CA provides for certificate and digital signature validity confirmations. One option is to use standard OCSP-based services for all online validity confirmations, as described above in association with DigiDoc.

Another important question is, under whose jurisdiction are disputes solved. This is no different from general international agreements jurisdiction. In the contract, it is usually set forth under whose jurisdiction it is concluded and where are the disputes solved. The contract itself could therefore also indicate which legislation's requirements are considered for the certificates and signatures in case of dispute. Of course, digital signatures are not used in case of contracts only, and more generic approach is probably necessary.

The OpenXAdES project

When the Estonian ID card project started at the beginning of 2002, we started looking for solutions that are readily available for giving digital signatures. As it was described above, we found no solutions that would suit all the Estonian needs. So, it was decided that there is a need for such a system, and DigiDoc was born.

The Estonian ID card project has received and is continuously receiving international attention. We decided that in order to promote the "universal digital signature/document" concept beyond Estonian borders, there is a need for a project with the codename OpenXAdES. The name indicates our commitment to open communication and following international standards. The technology is now available to other countries and communities at www.openxades.org. The site describes our motivations behind the project and offers documentation and software

libraries for download. In the summer of 2003, the site will feature a number of test services that are freely available to anyone possessing a smart card with digital signing certificates and allow them to sign and verify documents.

Our goal is to make OpenXAdES compliant with different legislations and technology standards, yet maintain the focus on legally binding digital signatures and documents. OpenXAdES can work with smart cards and other signing tokens issued in different legislations and under different rules. The ultimate goal of the project is to bring legally binding digital signatures and paperless document management into everyday life, business and communications – this is already happening in Estonia where relations are transforming using this technology, and we would like to help other countries achieve the same benefits that we are experiencing here.

OpenXAdES is, as the name indicates, an open initiative where anyone is welcome to join. In May 2003, AS Sertifitseerimiskeskus and Finnish Väestörekisterikeskus (Population Register Centre, PRC) signed an agreement for improving digital signature interoperability between the countries, with the goal of making digital documents a reality within and between Finland and Estonia. We invite other parties from other communities to join the project and thus expand the network of "digital countries".