Managing Digital Identities & Signatures through Public/Private Partnership

CUSTOMER CASE STUDY

Company
AS Sertifitseerimiskeskus (SK)

Industry
Commerical/Government

Business Requirements
- Streamline a broad range of commercial and public services for companies and end-users within Estonia.
- Provide citizens and residents with dualpurpose identity cards – for physical and electronic authentication and transaction needs.

UniCERT Solution
- Assign a unique digital credential to each citizen and resident within the state.
- Enable users to electronically authenticate to resources and digitally sign pieces of information as required.
- Provide a flexible and scalable solution to manage today's needs and future requirements as they emerge.

"In conjunction with our public and private partners, we have provided a complete, end-to-end infrastructure for the provision and management of digital identities and digital signatures. To-date, over 200,000 citizens have been issued with dual-purpose identity cards and, by the end of 2003, we expect this figure to exceed 300,000 - or more than 20% of the entire population. This enables organizations and citizens within Estonia to confidently engage in electronic trade and communication – and thus streamline a range of processes for all concerned."

AIN JÄRV, CEO,
AS Sertifitseerimiskeskus

CONTENTS

Country Background	3
Project Background	3
ID Card Characteristics	4
The ‘Digital Certificate’ Role	5
e-Signature Legislation	5
Data Protection Measures	6
Document Signing Services	6
DigiDoc Use Case	7
Public Private Operational Structure	9
The Registration Process	9
UniCERT – providing core PKI security services	10
Certificate Validation and Verification System	11
Managing Users’ Role and Authorization Rights	12

Written and published by Cybertrust, Inc.

Country Background

The Republic of Estonia is a small, independent Baltic state with a population of just over 1.4 million people. While Estonia is a relatively small country (in terms of other European population sizes, land area, GDP levels etc.), the nation is an acknowledged 'innovator' when it comes to introducing and adopting new technology products and services. A study at the end of 2002 showed that 43% of the population, or 455,000 people, regularly use the web – the figure shows that Estonia has the highest Internet usage rate in Eastern Europe and has also surpassed countries such as Italy, the UK and France. Internet connectivity is also very high and well accessible at homes, offices and schools. A national 'free' basic Internet training program also aims to boost the usage to Scandinavian levels of more than 60%. Most companies and virtually all public sector agencies have a web presence. Mobile phone usage is also above average, with 64% of the population owning a mobile phone.

Project Background

Issued by the Estonian Government's 'citizen and migration board (CMB)', national ID cards represent the primary source of personal identification for people living within Estonia - and are mandatory for all citizens and resident aliens above the age of fifteen. The Estonian identification card carries two discreet functions:

Physical Identity – can be used as a regular ID in conventional 'real-world' situations – anywhere one would typically need to prove identity/age etc.

Electronic Identity – enables citizens to use the same card to electronically authenticate to websites, networks etc. and/or digitally sign communications and transactions as required.

There was no national ID card scheme in place in Estonia before the launch of the "new" ID card project. Conventional ID card schemes (e.g corporate cards) have been in operation for some time within Estonia, however the dual-purpose 'physical/electronic' ID cards were not so familiar. To fulfill the scheme's requirements, the CMB required a single, holistic system which could process and provision users with a dual purpose 'smart' identification card. The process had to be straightforward for citizens (to register and receive), easy to administer (for technology controllers) and above all, be secure and reliable. In conjunction with the 'ID Card' initiative, the CMB were also eager to drive the adoption of electronic signatures within the region – thus streamlining key 'public service' and commercial processes for residents and businesses.

The Estonian ID card scheme is the overall responsibility of the CMB, however the process itself is managed through a tight public/private partnership. Two key private organizations work with the government to support the ID card project:

1. AS Sertifitseerimiskeskus (hereinafter 'SK') - a joint venture formed in 2001 between two of Estonia's largest banks (Hansapank, Eesti Ühispank) and telecommunications organizations (Eesti Telefon and EMT).
2. TRÜB Baltic AS - a subsidiary of the TRÜB financial services organization – headquartered in Switzerland.

The following pages summarise some key aspects of this dual-purpose card scheme and highlight the relevant security aspects associated with its 'electronic authentication' and 'signing' requirements.

ID Card Characteristics

The legal framework associated with the issuance and government of ID cards was established through the 'Identity Documents Act' which was passed in 1999 and took effect on January 1, 2000. The specific legislation associated with 'digital signatures' was passed separately in late 2000. While there is no direct sanction for not holding an ID card, it is expected that as the first Estonian passports were issued in 1992 (following independence from the Soviet Union) with a ten-year validity period, most people will apply for a card when renewing their passport – if not already done so independently. By 2007, the government expects over 1 million cards to be issued (almost the entire registered and qualified population).

There is only one version of the national ID card – no 'optional features' or variations exist. All cards are equipped with a chip containing electronic data and a unique digital certificate relating to each individual. It is understood that some residents will have doubts or fears about using the electronic functions of the card. For this reason, certificates can be suspended if required – disabling the ability to use the card for electronic authentication/ transactions. Certificate suspending or revoking also removes the user's data from the public certificate directory.

The card itself looks as follows:

Front of Card:

- Cardholder's signature and photo
- Name, Sex, Birth date, and citizenship
- Personal code, card number and validity

Back of Card:

- Card holder birthplace & residence permit details (if applicable)
- Card issuing date
- Card and holder information in machine readable format (ICAO)

All of the data outlined above (except for the handwritten signature and photo) is stored in electronic format on the ID card – in a special publicly-readable format.

The 'Digital Certificate' Role

Each national ID card contains two discreet PKIbased digital certificates – one for authentication; one for digital signing. These certificates are standard 'X509 v3' certificates and have two associated private keys on the card – each protected by a unique user PIN code. While policies are normally set to designate the usage and authorization rights associated with any given 'Digital Certificate', the certificates associated with this scheme do not contain any such 'role' or 'authorization' information. The certificates do not contain any 'use restriction' – they are universal in nature and are designed to be used in the widest range of scenarios e.g. between private individuals, companies, card holders and the central government etc.

The authentication certificate on each ID card contains a unique government-assigned email address – in the format 'firstname.lastname_NNNN@eesti.ee' where NNNN are four random numbers. The random 'N' numbers are necessary to assign a unique email for each individual (even to persons with the same name). This unique address is for life (does not change when card is reissued or renewed). There is no pre-determined email service associated with these email addresses, they are merely a relay address which forwards email messages to users' day-to-day email account. Each individual goes to a designated online website to configure their forwarding email address as appropriate.

While these email addresses were introduced to facilitate government-citizen communications, the address can be used by the individual for any other 'standard' email requirement. Individuals can use their 'authentication' certificate to sign and encrypt mail messages if required, however, this email signature (using the authentication certificate) is not legally binding and is not covered by the digital signature act.

e-Signature Legislation

The Estonian parliament (Riigikogu) passed the national Digital Signature Act (hereinafter DSA) on March 8, 2000 and came into force on December 15, 2000. This law regulates the framework and rules required to effectively govern a national PKI and digital signature infrastructure.

The primary aim of the DSA was to give electronic signatures the same level of trust and assurance as hand-written ones. As a rule, digital and handwritten signatures should be equivalent in both the public and private sector. The DSA also states that public service departments must accept digitally signed documents. The DSA requires that each digital signature can:

- Uniquely identify the signatory
- Bind the individual to the signed data
- Ensure that signed data cannot be tampered with retrospectively – without invalidating the signature itself

In terms of EU status, all certificates issued in association with the ID card scheme are 'qualified certificates' as per the European digital signature directive 1999/93/EC. The Estonian DSA only regulates 'advanced electronic signatures'

with regard to the EU directive. Naturally, other types of electronic signatures can also be regulated, but the DSA does not give them legal power or stature.

One of the core components of the DSA was the establishment of rules and regulations with regard to Certificate Service Providers (CSPs) – which issue digital certificates to users and manage related security services. The Estonian DSA mandated a number of stringent requirements (financial and procedural) to ensure that CSPs are set-up and managed properly - to perform their function to the highest possible standard.

The DSA also regulates 'time stamping' services which are provided by dedicated 'Time Stamp Providers'. These 'TSP' service providers have to adhere to similar laws and regulations as CSPs. The time stamp is simply a piece of data which attests to the occurrence of an event at a specific time. The DSA does not define time stamps in great detail, but ensures that time stamped data cannot be tampered with or amended without invalidating the time stamp itself.

A national registry of service providers contains all the relevant information associated with registered CSPs and TSPs.

Data Protection Measures

The data protection issue is not significant with regard to the Estonian ID card scheme as there is very little private data present in the card issuing and further utilization process. A broad 'Personal Data Protection Act' regulates the use of personal data and databases by public authorities and private entities. A dedicated government body ensures that these rules are met and enforced.

Basic certificate information is publicly available through a directory service. This directory outlines 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. The directory contains only valid (active) certificates. If a person suspends or revokes his certificate, it is also removed from the directory.

Personal data which is published on the card (in visual and electronic format) is only accessible to the cardholder. The general stance on ID cards 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.

Document Signing Services

In order to drive the adoption of digital signatures within the region, software and technology had to be available for parties looking to incorporate compatible applications. When technical experts looked for a generic application or implementation which would fulfill this requirement, no ideal solution was found. It was also not optimal to rely on a foreign software/technology vendor to provide and guarantee support for a critical piece of national infrastructure – could have detrimental impact on the country's day-to-day functioning going forward. Because of these considerations, a bespoke software model was developed specifically to cater for Estonia and its digital signature constituents.

SK, together with its partners, delivered a comprehensive digital signature architecture called 'DigiDoc'. DigiDoc is a universal system for giving, processing and verifying digital signatures created by AS Sertifitseerimiskeskus. It can be connected to any new or existing piece of software, but its components are a standalone client program and a web portal. The core components of DigiDoc are:

- **Client program**. DigiDoc Client is available to anybody to download for free. Anyone can use it to verify digital signatures or, if you have an Estonian ID card and smart card reader, generate digital signatures.

- **Web portal**. The portal is located at http://digidoc.sk.ee and is available to all ID card holders free of charge. Its functions are similar to the client program - you can use it to generate and verify digital signatures. In addition, you can use it to have a document signed by a number of people. With a few clicks of the mouse, you designate the people whose signatures you need on the document, and they can all sign it in the same portal. Every user has a directory of his or her documents which no one else sees but where anyone can send documents to be signed by you.

- **File format**. DigiDoc specifies the file format for storing a digital signature and other technical data in a container file, together with the original file that was signed. All DigiDoc-enabled programs must support this format, and it must be possible to export files from all the programs into standalone files, to be verified with the standalone DigiDoc Client.

- **Software library**. The DigiDoc librar y is available to all developers as a program library in C and as a Windows COM component. It can be connected to any existing or new software. For example, you could add DigiDoc support to accounting software, document management system, web/intranet applications etc.

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 being the digital document format which is key to common digital signature implementation and practice.

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.

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 or on top of it. A COM interface has been implemented, making it easy to add DigiDoc support to any Windows based application supporting COM technology. A Java implementation is also provided.

Despite these strengths, 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 and web sites dealing with documents, a number of sample or 'reference' applications were 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. Both are based on the same DigiDoc library and thus fully compatible e-signatures given in Client can be verified in portal and vice versa. The libraries, specifications and applications are provided to the 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 through 2003- 2008. The first official digital signatures in Estonia were given using DigiDoc Client on October 7, 2002.

DigiDoc Use Case

The Estonian office of Hedman Osborne Clarke Alliance law firm uses digital signatures and ID cards in business communications with its partners and customers.

Background
Established in 1975, Hedman Osborne Clarke Alliance is based in the centre of Helsinki. Hedman Osborne Clarke Alliance is a member of Osborne Clarke Alliance, a pan-European grouping which offer access to 500 lawyers in 14 European commercial centres, as well as in Silicon Valley, USA. The Tallinn office of HOCA (hereinafter Hedman) was founded in 1992.

Starting Point Hedman decided to start using digital signatures for a number of reasons:

- Digital signature is not a magic wand, but it enables to do business more efficiently and securely
- A law firm's most valuable resource is time and digital signature helps to save it
- Customer demand was strong – desire to use digital signatures if possible

Solution
Prior to full-scale usage, Hedman initiated the planning phase where the hardware and software necessary for using the digital signature was analyzed. As the cost of card readers was not particularly high and software was available for free, Hedman decided to equip all the company's PC's with card readers and make it mandatory for employees to have an ID card.

The initial concept was followed by a testing and training phase. Digital signatures on documents were tested out throughout the office and all the employees were trained to use it. Also, Hedman held seminars where everyone discussed how to make the most of ID card and digital signatures.

Hedman has drawn the following observations from its experience:

- Employees accept the ID card readily if the can see both business and personal benefit from it (logging in to Internet bank, transmitting personal digitally signed documents etc)
- The notions "copy" and "original" lose their meaning in the digital world - all documents are original
- Printing out digital signatures is not possible, document storage and archiving must be done digitally
- Digital document management presents new requirements to corporate IT environment: reliability, backups, security need to be ensured
- Fax machines became almost redundant
- Digital documents are much easier to handle than those on paper
- Document processing becomes quicker
- The readiness of government agencies to accept digital signature varies greatly - some can do it right away, others need more time. Eventually, they all have to do it as it is required by law
- If you send digitally signed document to someone for the first time, also add short info about how to verify the document and where to get the software (DigiDoc) from

In the future, Hedman plans to use the ID card also as an access token in place of door locks, and as primary user identification tool for logging on to computers.

Public Private Operational Structure

The card issuing and administration infrastructure is managed through a close public/private partnership. The three main organizations involved are:

The Estonian CMB – responsible for the issuance of identity documents to citizens and alien residents as required by the government's National Identity Act. The CMB is the institution that physically receives card application forms from residents.

AS Sertifitseerimiskeskus (SK) – functions as the certificate authority for the Estonian ID card project and manages a complete range of associated electronic services – including the LDAP directory service, OCSP validation service, and other certificate related services. SK also manages the end-user distribution channel (through its parents' retail bank outlets)

TRÜB Baltic AS – is the company that personalizes the card itself – both physically and electronically. TRÜB receives the card application from CMB and manufactures the card, printing and engraving the personal data on the card, generating keys on the chip and embedding the certificates on the card.

The Registration Process

Steps Involved in Registration (Start to Received)

Citizen or resident submits an ID card application to CMB – face-to-face or via post. CMB verifies that the person is indeed entitled to receive the card – he must be either Estonian citizen or have a valid residence permit. At the time of application, the person must prove his entitlement – this is not necessary if the person is a citizen and has already been issued a previous document such as Estonian passport, but in other cases (e.g. ID card is the first document that is issued by Estonia to the person), additional documentation, e.g. birth certificate, archive record copies or foreign certificates may be necessary to prove the entitlement.

Once approved, CMB sends a request to TRÜB to personalize the card. TRÜB starts manufacturing and simultaneously sends a certificate request to SK to issue the PKI-based digital certificates. SK issues the certificates, returns them to TRÜB and also publishes them to the central database.

During the manufacturing process, TRÜB gives the card a command to generate the private keys – they never leave the card. TRÜB also ties the keys to PIN and PUK codes which are printed in a secure envelope, similar to the technology used in bank cards, mobile SIM cards etc. Finally, TRÜB embeds the certificates issued by SK in the card.

After personalization, the card and PIN's are delivered in separate envelopes to a bank office using secure courier delivery. At the time of application for the card, the person indicated at which bank office he would like to receive the card and PIN's – he can now go to that office and receive the card and PIN's over the counter.

UniCERT – providing core PKI security services

In order to issue and manage their PKI-based digital credentials, SK chose UniCERT for a number of key reasons:

- Proven PKI product - range of successful deployments in similar environments
- Proven scalability and flexibility – the product's modular architecture was a significant advantage here as it allowed security professionals within SK to build and architecture their security system exactly as they needed.
- Standards-based technology structure was also significant. The PKI had to interoperate with a broad range of complementary technologies, so SK needed a solution that was built with this 'reality' in mind.
- Internationalization aspects were a major consideration. The Estonian language is rich in non-ASCII characters and these need to be correctly processed and embedded in the certificates.
- Auditable security and the possibility to construct reliable processes. Technology is just one aspect of security, equally important are the organizational and physical security measures. Estonian legislation requires annual external infosystem audits from SK and UniCERT improves the auditability of SK's systems with its international certification and proven track record.

UniCERT is primarily used as the certification component in SK's "PKI factory" in fully automatic processing mode – it receives the certificate request and issues the corresponding certificate without human intervention. UniCERT is fully integrated in SK's other PKI and CA/RA components, some of which have been custom developed for the project and interfaced with UniCERT.

UniCERT meets SK's needs for close-to perfect security and traceable, auditable processes. Security aspects like root key generation and protection and system integrity in daily operations are given great consideration in SK, and UniCERT could be relied upon to provide these trusted PKI systems and processes.

Certificate Validation and Verification System

The Estonian Signature legislation was very clear that authorized certificate providers must provide 'a method of verifying certificate validity online'. As the issuer of certificates to ID cards, SK provides users three ways of checking certificate validity - CRLs, LDAP checking, and real-time OCSP checks.

CRLs are provided containing the list of suspended and revoked certificates. Although a commonly used method of validating certificates, CRLS are not the optimal validation method. As of January 2003, the CRL size had grown to over 1 MB in one year and is therefore not very convenient to use. CRLs are mainly provided for backwards compatibility and standards compliance. SK updates its CRL twice a day. Delta CRLs are not provided.

SK also holds an LDAP directory containing all valid certificates. This 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. Among other things, this provides everyone with a way of finding e-mail addresses of any ID card holder. Query restrictions are deliberately imposed (limits the maximum number of responses returned to one LDAP query) to protect against server overload.

'OCSP' checks are the most convenient option/method of verifying certificate validity. It can be used for simple certificate validity confirmations, but also for signature validation confirmations ("notary confirmations"). 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 CRLs 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 CRLs. In this way, SK ensures that OCSP responses reflect actual (real-time) certificate status.

OCSP and Time Stamping

For legally binding digital signatures, time is an extremely important factor. According to the Estonian DSA, only signatures generated using a valid certificate are 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 are able to clearly differentiate between signatures generated using a valid vs. invalid or suspended 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 retrospectively valid - even if the certificate has already expired or been revoked at a later date. If a certificate is suspended by the card holder or anyone else, the card holder can reactivate it at a local 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, as part of its DigiDoc digital signature architecture.

Managing Users' Role and Authorization Rights

While the Estonian ID cards are deliberately 'universal' in nature, the question of roles and authorizations still arises. It is sometimes assumed that certificates for digital signing may be issued for specific purposes only, and that a person's role can be profiled within the certificate. 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 DSA states that a digital signature (produced through a PKI-based digital certificate) is no different than a handwritten one. A person's handwritten signature does not contain his or her role, therefore neither does the digital equivalent.

If needed, 'roles' and 'authorization rights' are established using some out-of-band method (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 an 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 the Estonian context, it simply mirrors the real-world model/procedure.

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 then encloses the digital power of attorney with any further documents he signs. The person receiving the document can, upon receipt, verify both the original signed document and the enclosed power of attorney - that confirms that the person did have 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 organizations' 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.

For example, this is useful when signing pieces of databases (e.g. bank statements) online for presentation 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 are not covered by law (because according to the Estonian law, only real people can generate signatures). The 'organization's signature must therefore be viewed simply as an additional tool proving data 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. This is the only exception - no other personal role certificates or other such exist.

About Cybertrust

Cybertrust is a global provider of information security, providing a unique mix of processes, products, and people to enable enterprises and government agencies to secure and manage their IT infrastructure. With over 15 years of proven experience, Cybertrust is the first company to comprehensively address the entire security lifecycle by providing offerings for each of the four critical security domains of identity, threat, vulnerability, and compliance management. These offerings leverage Cybertrust's unmatched security knowledge and intelligence gathering resources, which includes ICSA Labs®, the global leader in information security product certification. Headquartered in Herndon, VA with more than 30 offices around the globe, Cybertrust is the trusted advisor for information security to over 4,000 customers worldwide.