University of Ljubljana
Faculty of Economics
And
International Center for Promotion of Enterprises
(ICPE), Ljubljana

MASTER'S DEGREE THESIS

# DIGITAL SIGNATURE AS A TOOL TO ACHIEVE COMPETITIVE ADVANTAGE OF ORGANIZATION

Ljubljana, March 2006 Andraž Zupan

## TABLE OF CONTENTS

## LIST OF FIGURES

## LIST OF TABLES

# 1.0 INTRODUCTION

In the last decade, organizations have been trying to move from a paper-intensive environment to a paper-free environment. Word processors have replaced the writing pad and pen, spreadsheet applications have replaced manual spreadsheets and emails have supplanted handwritten letters.

New business opportunities have emerged as paper-based transaction systems are being moved online. Yet the road to an economy where the vast majority of transactions are electronic is not without concerns. These include knowing whom you are dealing with (identification), who is authorized to access what information (entitlements), and how individuals will be held accountable for their online commitments (digital accountability). Digital signatures powered by public key infrastructure (PKI) technology, are widely recognized as the best practice for ensuring digital accountability for electronic transactions. Digital signatures are the most effective, secure, and easy-to-implement method of providing accountability while enabling electronic transactions.

Organizations are moving away from the traditional, time consuming paper processes and searching for new and innovative technology to improve efficiency. Digital signatures can significantly benefit organizations by eliminating the last of the paper in the business cycle. The ability to instantly sign and seal documents and transactions electronically results in much shorter process cycle times, accelerated customer service and drastic cost savings. Digital signatures provide enhanced convenience for both the customer and the organization, while significantly reducing application processing time.

## 1.1 Problem

Digital signatures are now as legally binding as hand-written ones, but it will not be long before it is commonplace to use this technology to substantially replace written signatures. Technology experts claim that it is more difficult to forge an electronic signature than a hand-written one.

A digital signature is superior to a traditional handwritten signature. A skilled forger can alter the contents of a document with a handwritten signature or move a signature from one document to another without being detected. With digital signature technology, however, any change in a signed document, such as content modification

or signature replacement, causes the digital signature verification process to fail (Tao, 1999).

The use of digital signatures in E-Business is not limited to certain types of businesses or technology related products and services. Organizations in every field are conducting business online. Networking through E-Business can be applied to any facet of an organization's operations, including marketing and sales; purchasing and logistics; production; design and engineering. A highly effective use of E-Business is the combining of several of these functions: information flows from sales to purchasing, to production. Management in companies is still not aware of all advantages that could be gained with use of digital signature.

Organizations could use digital signature for many functions, including as a means for a safe sales channel, for safely communicating with partners and clients, for safely connecting to back-end data systems, and for safely performing e-business transactions.

Digital signature provides solution for many improvements in business processes. For instance, in the Business-to-Business (B2B) sector there is a problem of decision-makers mobility. They must be able to initiate transactions all over the world so they can react quickly specially to extremely time critical business transactions. It has increasingly become difficult to find this group of people in the office. Important transactions are left incomplete because the person responsible has not authorized them. Implementation of digital signatures would benefit in mobility and taking care of this problem.

Another even more important organizational objective today is cost saving. Traditional transactions are managed using manually written, pre-printed, or electronic forms. This information is then manually transferred to other forms before the information is further processed and finally fed into the company’s general ledger. This transcription is expensive and error prone, and diverts limited resources from services to routine administration. Transcription is not necessary with paperless technology (Grupe, 2003).

Management is constantly striving to reduce costs with reengineering and reorganization of business processes but it is still not aware of all possibilities that implementation of digital Certificate could bring their organization in order to achieve competitive advantage. Some of authors like Matt Hicks say that in 10 years from now, we are all going to be there. It is a question of, are you going to do it in the first

couple years and take advantage of it and get the benefit of it, or are you going to do it in the last five and catch up to what the rest of the industry is doing (Hicks, 2001)?

## 1.2 Scope

The discussed problem is pertinent nowadays, when organizations strive for faster, more transparent and cost effective processes. Business processes supported with the use of digital signatures could be the way to get competitive advantage in organization today and a must-have to be competitive tomorrow.

My main goal is to present how organizations could benefit in various ways with the use of digital signatures and their implementation in their every day B2B, B2C processes. I would like to show that use of digital signature increases efficiency, improves decision time, eliminates paper work, improves transparency, increases safety and reduces costs of organization.

My sub goal is to present what digital signatures are and how they technically work in a way that middle and top management would understand. I will also briefly present current legislation in the EU and Slovenia. I will present the correlation between public key infrastructure and digital signatures, as well as considerations of them.

## 1.3 Method and organization of thesis

The organization of this thesis includes the following chapters.

Chapter I: Digital signature basics – This chapter explains basic characteristics of digital signatures and cryptography theories along with some description of their use. It also sketches the concept of a public key infrastructure (PKI) along with some of its implementation details.

Chapter II: Legislation – This chapter shortly presents the EU and Slovenian legislation on digital signatures.

Chapter III: PKI considerations – In this chapter some considerations related to PKI are presented from legal, technical, organisational and interoperability perspectives.

Chapter IV: Calculating financial returns on investment – This chapter is divided into two major sub-sections. The first sub-section presents an approach for computing

ROI on PKI, while in the second sub-section, a practical case of calculating ROI in PKI and digital signatures is presented.

Chapter V: Digital signature implementation steps – In this chapter some steps are outlined that reduce the risk of failure and cost overruns by digital signature implementation projects.

Information and data were collected from different articles, books and materials as specifications, which I used at my work when I was employed in the banking sector for four years – the field of electronic banking. I also used my own experiences, especially in the part of thesis where the business aspect is presented.

# 2.0 CHAPTER I – DIGITAL SIGNATURE BASICS

## 2.1 Paper signatures

Paper signatures are handwritten signatures on paper documents. Aside from legal and contractual issues, the primary characteristics of a paper signature are (Entrust, 2003):

1. A paper signature is intended to be associated with a particular individual

2. A paper signature generally denotes a commitment related to a particular document, with the exact meaning depending on context.

Though far from perfect, paper signatures serve surprisingly well in many parts of the world as the basis for business and legal transactions. This is due, not to the inherent features of paper signatures, but rather to accompanying processes, supplemental contracts, and the overall context surrounding acts of signing. Various customs of witnessing, public ceremony, and evidence have emerged over time, in large part aimed at increasing the chances of accurately reconstructing events should a dispute arise later.

Paper signatures themselves are generally not meaningful. In fact, in many cases a witnessed "X" serves equally well. If extracted through coercion, trickery or forgery, almost all societies will find a paper signature legally non-binding. The use and interpretation of a paper signature are typically defined by culture and context. State laws evolve to define reasonable default terms, both in the absence of explicit contracts and in the presence of contracts with ambiguous terms. Common conditions necessary for a party to be legally bound by a signature include the signature mark representing a desire to be bound to a well-defined commitment, the mark being made of free will, and the mark being an act of the party to be bound (or a duly authorized deputy of that party).

A popular myth is that a paper signature can easily be traced to a particular individual. In practice, this turns out to be difficult. Most office workers are unable to recognize the paper signature of a colleague, or of the company officers that sign their expense checks. Nonetheless, this is not a problem because in most cases paper signatures are effectively a formality; their subsequent verification is rare. The reason paper signatures seem to work so well is that over time, societies learn to discontinue their

use, or support them by additional means (witnesses, notaries, corporate letterhead, seals), in situations where it has been difficult to resolve disputes. The end result is that signatures are only rarely called into dispute, and there is confidence that the rare cases can be resolved through special procedures that rely on context, collective memory, and any and all available evidence beyond a physical signature itself.

In summary, societies have learned to use paper signatures in circumstances in which a physical marking on a paper document, augmented by sufficient controls and context, provides sufficient recallable evidence of a commitment related to that document by the marking party. The evidence is important in order to reconstruct circumstances, in the rare case of later disputes.

## 2.2 Digital signatures

A digital signature is the term used for marking or signing an electronic document, by a process meant to be analogous to paper signatures, but which makes use of a technology known as public-key cryptography. The analogy to paper signatures is helpful, though not precise. Clearly, paper signatures cannot be applied to documents that remain in electronic form. More significantly, additional security properties are required of signatures in the electronic world. This is because the probability of disputes rises dramatically for electronic transactions without face to face meetings, and in the presence of potentially undetectable modifications to electronic documents. Digital signatures address both of these concerns and offer far more inherent security than paper signatures. Compared to all other forms of signatures, digital signatures are by far the most easily verified and the most reliable with respect to providing document integrity.

This is not to say that digital signatures cannot be misused. If poorly implemented or not supported by appropriate procedures and processes, they are no more reliable than paper signatures or corporate seals under similar conditions. Digital signatures provide a far more secure basis for contracting and commitments than paper signatures, and offer the only viable solution to providing reliable evidence of commitments in an online world.

A given individual's paper signature is essentially identical regardless of the document being signed. For this reason, a threat related to paper signatures is a cut and- paste attack from one physical document to another. This risk is usually small because typically such an act would leave physical evidence of the misdeed. However, the point worth noting is that such an attack is not possible for digital signature, because

the digital signature of Mr. Janez Drnovšek differs significantly with each different document digitally signed by Mr. Drnovšek, even if the document varies by only a single character or bit. Yet the digital signature can be easily associated back to the correct individual. This is possible through the elegance of public-key cryptography.

The important summary points are that, when properly implemented and supported by the robust foundation of a PKI (Entrust, 2003):

1. Digital signatures are to electronic documents what paper signatures are to paper documents.
2. Digital signatures provide trustworthy evidence of the identity of the signing party (identification).
3. Digital signatures are not subject to being copied to (or forged from) other documents.
4. Digital signatures ensure that a signed document cannot later be modified to the advantage of one party - if the original is modified, the verification process detects this.
5. Digital signatures already have a legal footing equal with paper signatures in many countries.

In addition, the exact time of signing for a digital signature can be recorded more reliably than that for paper signatures, using a trusted time stamping server or service. With digital signatures, witnessing and notarization are naturally facilitated more efficiently and conveniently.

## 2.3 Electronic vs. Digital signature

An electronic signature is any form of marking that might be used to represent the equivalent of a paper signature, for the case of an electronic document. Digital signatures, based on public-key cryptography and supported by PKI, are one type of electronic signature. Other types of electronic signatures have been proposed. One example is digitized signature - scanned images of paper signature that are then simply attached as graphical representations (bit-map images) at the bottom of electronic documents. Another possibility is scripted font signatures – simply attaching the name of a signing party in a special scripted computer font, giving the likeness of a paper signature but including nothing characteristic of the signing party. Many other technologies, including smart cards, biometrics, and passwords, are confused as substitutes for digital signatures. The majority of these are in fact complementary to digital signatures, rather than substitutes.

It is clear that scripted font signature offers no security on their own (say in the absence of witnesses), as it would be very easy for anyone to enter the name Janez Drnovšek at the bottom of a message, in a particular computer font. Digitized signatures similarly offer little security - one could obtain a signature image from a copy of an electronic or paper document, and an electronic representation could be easily copied and transferred to any other document. Such cut-and-paste fraud is also possible with paper signatures, but in the paper world it leaves physical evidence and is therefore less of a risk.

Such attacks, which are possible with many weaker forms of electronic signatures, are not possible with digital signatures. The main reason is that a digital signature varies with each transaction. If a single message word or bit is altered after a document is digitally signed, the signature verification process will detect this. This is very important, because there is no point in verifying the identity of a signer if you cannot detect whether someone else has altered the document thereafter.

It is also important to note that simply obtaining the consent of a user, for example by having the user click on an "I accept" button, does not provide tangible evidence, at a later point in time, that such consent was actually obtained. An online brokerage would be hard pressed to prove to an arbiter, at a later point in time, that the button was located in an appropriate place, in an appropriate overall context, six months after a disputed customer transaction took place. Indeed, recreating the environment of a past user transaction is extremely challenging, as the design of Web sites and online forms changes frequently. This highlights the difference between obtaining user consent, and recording evidence, that such consent was obtained. While passwords are in common use for identification and entitling access to accounts, passwords alone are of little help in generating evidence generation such as easily verifiable digital receipts, that is, reliable electronic transaction records replacing paper receipts. Best practice for securing digital receipts is through digital signatures.

Digital signatures, when appropriately implemented in accordance with standard practice, provide more security than paper signatures or any form of electronic signatures. They are the only known means for reliably binding a signature to electronic data in a manner that is both secure and easily verifiable - a property that is fundamental to e-business. They also offer the ideal means for guaranteeing the integrity of audit trails and online storage. As a result, digital signature is equated with best practice for digital verification.

## 2.4 Symmetric cryptography

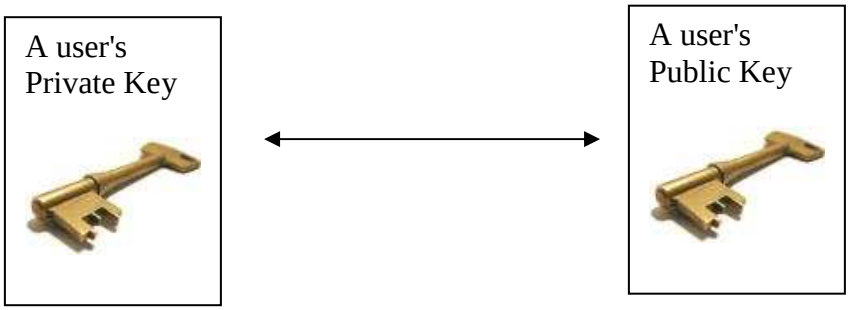
Symmetric key cryptography raises some problems related to its implementation. These problems are associated with the authenticity of information processed with a symmetric key, and with the secure distribution of the key among users. With simple implementations of symmetric key cryptography, a recipient will not know for sure who the originator of the encrypted message is because anyone in possession of the key could have been the sender.

A solution to these problems was provided with the introduction of asymmetric (public) key cryptography. Its basic principle is very different from the single encrypt/decrypt key of symmetric key cryptography, in that every user owns a key pair: one key called the public key and the other called the private key. Although implementing a system that uses asymmetric public key cryptography adds complexity, the benefits gained are very appealing.

## 2.5 Asymmetric cryptography

Asymmetric cryptography, also known as public key cryptography, in general, provides the same services as symmetric key cryptography, but it uses different keys for encryption and decryption. Public key technology is based on key pairs. A key pair in a public key cryptography scheme consists of a private key and a public key.

Figure 1: Public and private key pair




Source: edited after Jerman, 2004

The basic characteristics of the public and private keys are (Articsoft, 2003):

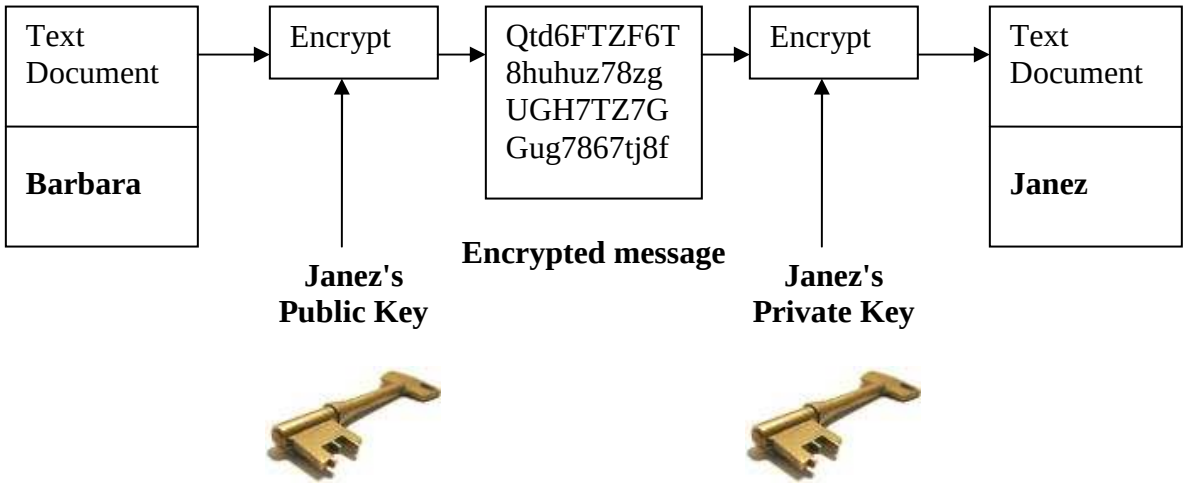
- A key is a binary string.
- Public and private keys are generated at the same time by a special software program.
- Public and private keys are not identical, but have a unique relationship so that they will only work with each other to encrypt and decrypt information. A process that ensures the keys are uniquely paired with one another and that neither key can be determined from an inspection of the other generates these key pairs.
- Information encrypted with one key can only be decrypted by the other, and vice-versa. In other words, a message encrypted using the public key, can only be decrypted by that key's corresponding private key.
- Each entity in a public key system will be assigned a mathematically related private and public key pair.
- The private key is :
    - Protected by the owner.
    - Used to digitally sign messages.
    - Used to decrypt messages.
    - Kept in the physical and/or cryptographic protection of the owner.
- The public key is :
    - Distributed freely and is accessible to anyone.
    - Used to verify digital signatures.
    - Used to encrypt messages.
    - Stored inside of "digital certificates" that provide for the integrity and authenticity of the user to public key value binding.

Public key cryptography is  used, for the encryption/decryption and signing/verification of information. Encrypting information ensures privacy by preventing unintended disclosure, signing messages, authenticates the sender of the message and ensures the message has not been modified since it was sent.

## 2.6 Function of encryption

When using public key cryptography, anyone that wants to send information to another, only has to obtain a copy of that other person's public key and encrypt the message to be sent using that key. Figure 2 presents the process of sending a message using a public key system.

Figure 2: Process of sending a message using a public public key system




Source: edited after Jerman, 2004

Barbara wants to send a message to Janez so that Janez is the only one who can read the message (confidentiality):

- Barbara obtains Janez's public key.
- Barbara encrypts the message with Janez's public key.
- Barbara sends the encrypted message to Janez.
- Janez uses his private key to decrypt the message.

The aforementioned information implies that Janez is the only one who will be able to decrypt this message since he is the only one who possesses his (Janez's) private key. If the message is intercepted during transmission, the interceptor will not be able to decrypt it.

In public key cryptography, the keys are used as follows (Articsoft, 2003):

- The public key is used for encryption

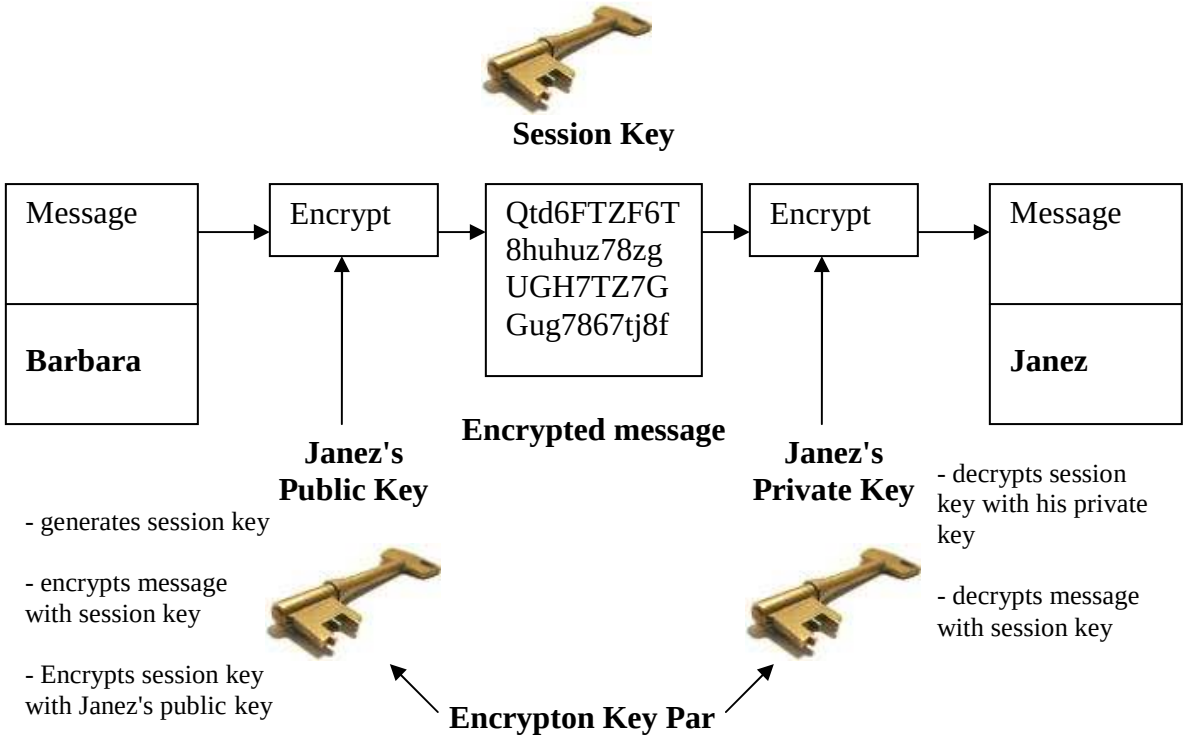
The sender uses the recipient's public key when desiring to send confidential information. The information to be sent is encrypted using the recipient's public key. The recipient can send the public key to the sender, or the sender can retrieve it from the directory in which it is published.

- The private key is used for decryption

A private key is used to decrypt information that has been encrypted using its corresponding public key. Both the sender and receiver of a message that has been encrypted with the receiver's public key, can be sure that only the receiver can decrypt the message. The receiver; however, cannot be sure of the message's sender, as it is possible for anyone to have the public key used to encrypt it.

In normal practice, both symmetric and asymmetric cryptographic mechanisms are used together in order to take advantage of the strengths of each. This specifically refers to the ability to distribute public keys without concerns of confidentiality (a strength of asymmetric key cryptography), and the faster encryption/decryption speed of secret keys (a strength of symmetric key cryptography relative to asymmetric). The general usage, therefore, is to use an asymmetric mechanism to deliver a secret key securely, then to have the actual information being sent encrypted using the secret key. This secret key can be any sufficiently long random number. Since the general usage is to generate at least one new secret key for each session of communication between two parties, the secret key is often also referred to as the session key. The public key is used to encrypt the session key and both the session key and the information encrypted with it are sent to the recipient. The recipient will use the private key to decrypt the session key, and then use the session key to decrypt the actual information. This is much faster than using the private key to decrypt all of the information.

Figure 3: Asymmetric encryption




Source: edited after Jerman, 2004

- Barbara encrypts the message with the session key
- Barbara encrypts the session key with Janez's public key.
- Barbara sends both the encrypted message and the encrypted session key to Janez.
- Janez uses his private key to decrypt the encrypted session key.
- Janez uses the session key to decrypt the encrypted message.

However, a problem still exists. Although confidentiality has been achieved because only the intended recipient of the message was able to decrypt it, there is no proof regarding from whom the message came, since anyone could have used the recipient's public key to encrypt the message.

It is under these circumstances that the concept/mechanism of a digital signature comes into good use.

## 2.7 Digital Signature detailed

A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and to ensure that the original content of the message or document that has been signed is unchanged (Jones, 2001).

A digital signature can be used on any binary string. Unlike a hand-written signature, which is slightly different every time it is signed, digital signatures are mathematically precise and reproducible. A further benefit of digital signatures is that timestamps can be included in the signed material thus establishing a means of recording the time that a signature was applied. Since digital signing is mathematically applied “over” the entire signed binary string, which comprises the document, the document cannot feasibly be changed without detection by the signature verification process. The ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later. Digital signatures provide for authentication, non-repudiation, and integrity of the information to which they are applied.

Digital signatures must not be confused with a digital certificate: which is a kind of electronic container for a user’s public key, which has been digitally signed by the certificate issuing authority to certify its validity.

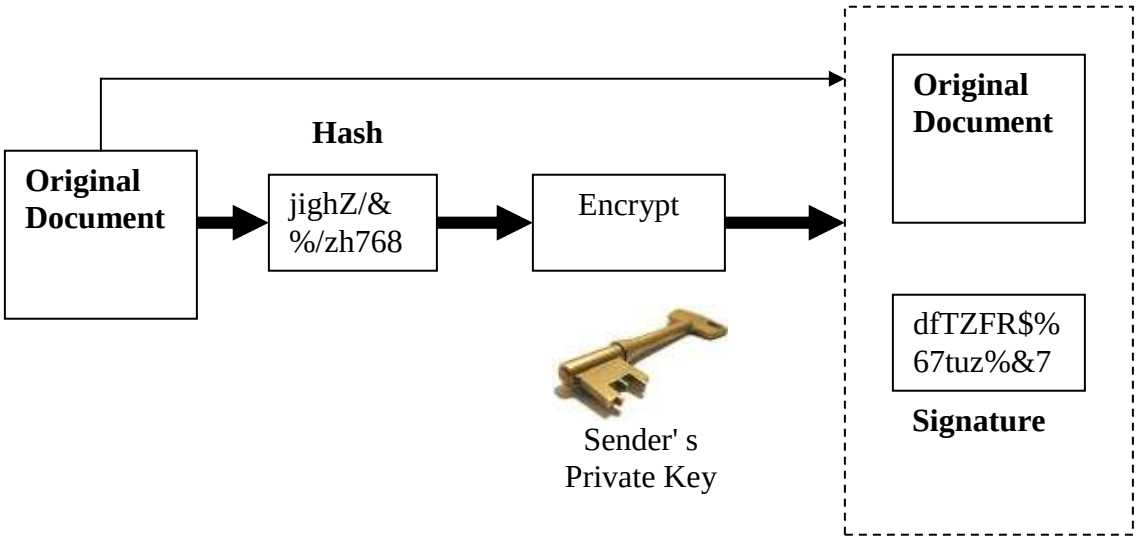
The recipient of a digitally signed message, having the public key of the signer, can determine (Articsoft, 2003):

- if the message was created with the signer’s private key
- if the message was altered since it was signed

When using a digital signature, the data itself is not encrypted, but a hash of the data is encrypted with a private key. A hash (also known as a digest) is a unique, fixed-length mathematical value that is determined by the content of the message and the ‘hashing’ algorithm used to create it. When some specific data is hashed, and the resultant hash value is encrypted with a user’s private key, the result is a digital signature for that specific data. The original data cannot be recovered from its hash, thereby resulting in the use of the term “one-way hash” (Jones, 2001).

The “signed” value either is attached to the end of the data or is sent as a separate file together with the data if the data is later transmitted to a remote location. The sender’s public key may also be sent with the message in the form of a certificate.

Figure 4: Digital signature creation



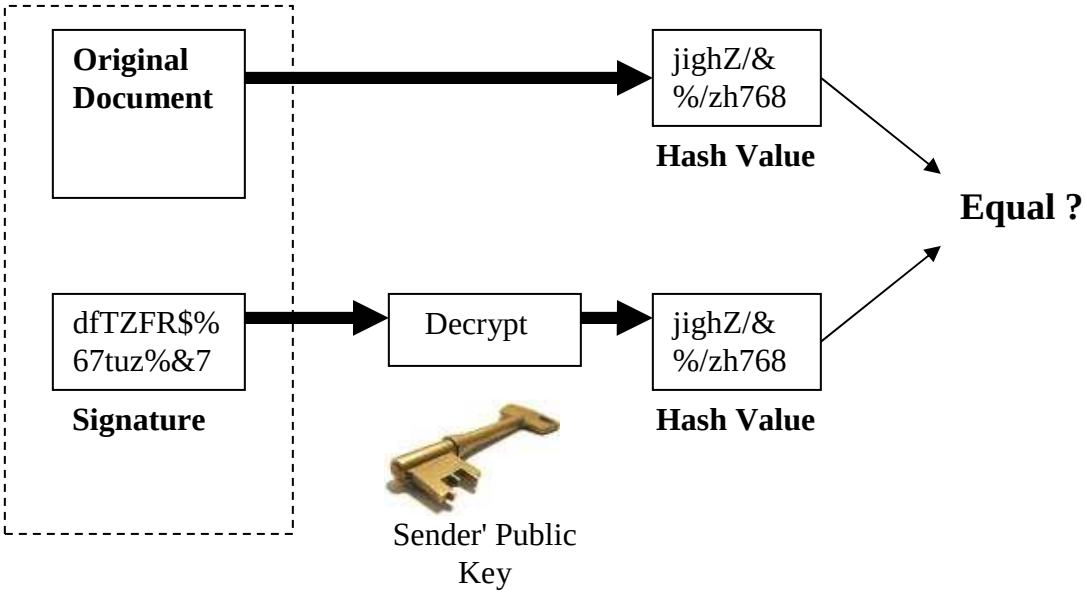

Source: edited after Jerman, 2004

In order to verify the received data, the recipient of a digitally signed message performs the following steps (Garnacho, 2004).

- Uses the public key of the sender to decrypt the latter’s digital signature and extract the encrypted hash value that the sender calculated for the information.
- Calculates the hash value for the received data using the same hashing algorithm that the sender used.
- Compares the two hash values, the newly calculated hash value is compared to the hash value that the sender originally calculated.
- If the values match, the receiver is certain that the person controlling the private key (corresponding to the public key) sent the data and knows that the data has not been altered since it was signed.
- If they do not match, the receiver knows that either the document has changed or the sender is not who he/she claims to be.

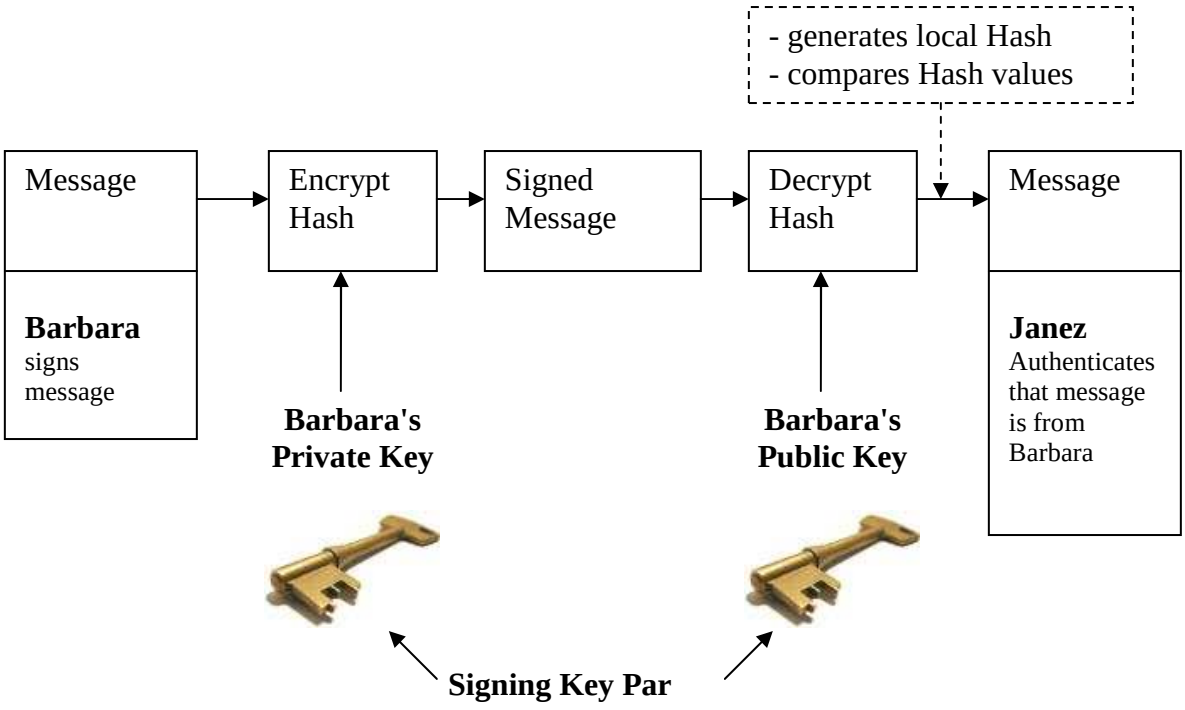
If no errors have been found, the receiver can be certain of the authenticity and integrity of the information that has been received.

Figure 5: Digital signature verification




Source: edited after Jerman, 2004

Figure 6: Digital signing (Authentication, Integrity, Non-Repudiation)




Source: edited after Jerman, 2004

In this scheme the use of keys is:

- The Private Key for Signature

If the sender wishes to prove to a recipient that he or she is the source of the information, the sender uses his or her private key to digitally sign a message (a digital signature).

- The Public Key for Signature

The receiver of a digitally signed message uses the sender's public key to verify the signature so that the receiver knows that the person controlling the private key corresponding to the public key sent the information, and that the received information has not been altered since it was signed.

Table 1: Public and private keys usage in asymmetric cryptography

| **Key Function** | **Key Type** | **Whose Key Used** |
|---|---|---|
| Encrypt data for a recipient | Public key | Receiver |
| Sign data | Private key | Sender |
| Decrypt data received | Private key | Receiver |
| Verify a signature | Public key | Sender |

Currently, Public Key encryption and digital signatures are used in order to provide the following services: confidentiality, authenticity, integrity, and non-repudiation. It therefore ensures that:

- the data has not been altered
- the data actually came from the stated sender
- only the intended recipient will be able to read the message

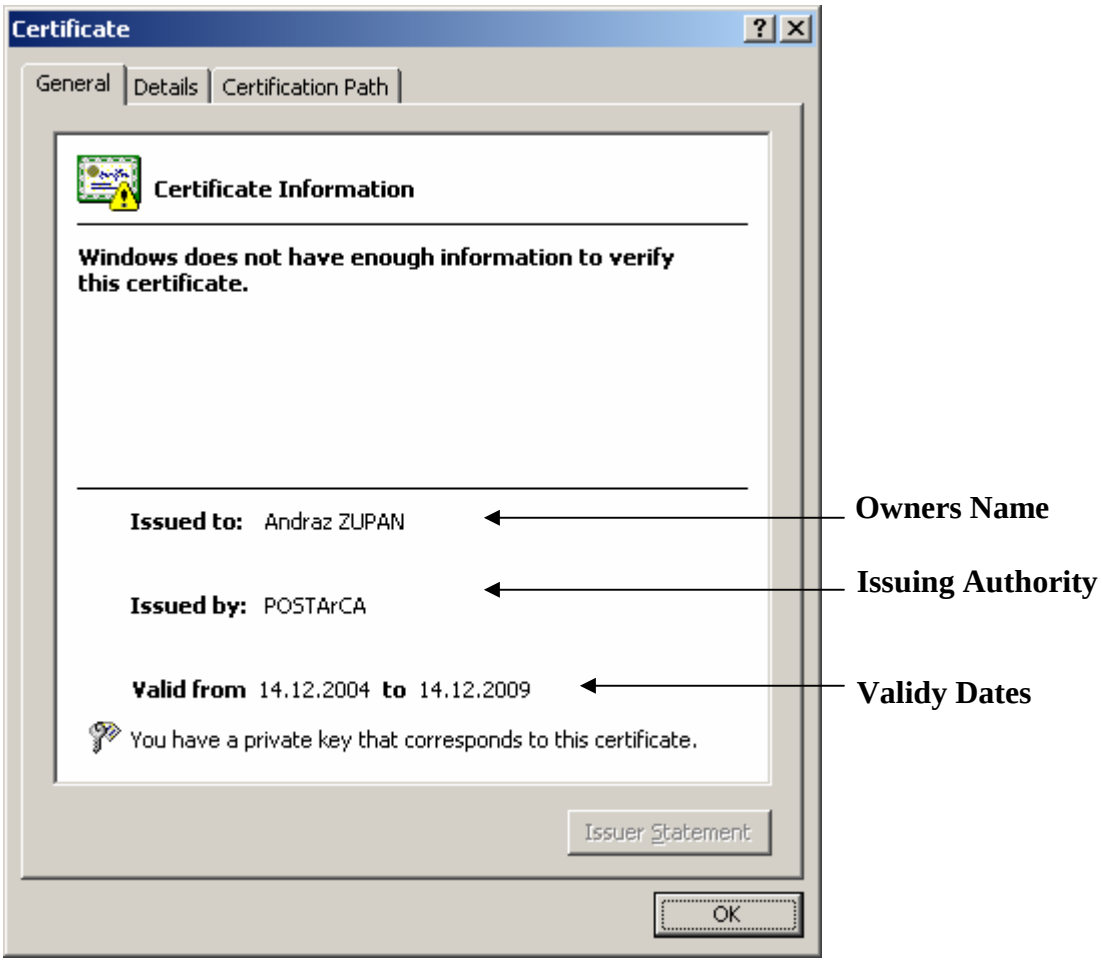
Although use of the techniques described above have solved many problems regarding data integrity and authentication, a big question still remains unanswered: how can the recipient of a digitally signed message be assured of the validity of the certificate that is used to verify the signature? There must be a level of trust within the system in order for public key encryption to be legitimate. A cryptographic binding between a user's identity (and possibly other credentials) and his/her public key(s)

must take place. This binding and required level of trust can be achieved through digital certificates and Certification Authorities within a public key infrastructure.

A digital certificate is an electronic “document” or computer generated record that officially links together the subscriber’s identification with the corresponding public key. The certificate is digitally signed by the issuing Certification Authority (CA) to ensure the certificate’s authenticity so that anyone in possession of the CA’s public key can verify the legitimacy of the certificate (Verisign, 2003).

Certificate authorities (CA’s) will provide a requestor with someone’s public key contained in a certificate. Information in the certificate will identify the public key’s owner, and provide the name of the CA who validated the identity and signed the identity to public key binding. In this way it is possible to see that a certificate serves as a kind of protective “container” for the public key, protecting the integrity of its binding to an owner and authenticating both the binding and identity via the reputation (and trust) of the signing CA. In addition to the user’s identity and public key, digital certificates also hold other relevant information. A user’s company affiliation information, expiration date, usage, the issuer of the certificate, and the degree to which an identity check was conducted on the users, and so forth. The exact contents of any certificate are flexible, and determined by the policy of the organization that enlists a CA to provide the necessary fields and values to support their infrastructure. This information is found in the organization’s Certificate Policy (CP).

Figure 7: Digital certificate




A digital certificate can be used by other users to verify that a public key belongs to a specific individual, as long as the issuer of the certificate is trusted. Therefore, if a user wants to send an encrypted message to another person, the recipient's name is looked up in the directory of a Certificate Authority and then downloaded to her workstation so she can use the enclosed public key to encrypt the message.

## 2.8 Public Key Infrastructure fundamentals

### 2.8.1 Public Key Infrastructure (PKI)

Living in the Internet era has increased the importance of, and requirements for, information security, especially within large information intensive organizations. In order to meet these requirements, organizations are deciding to develop and

implement a public key infrastructure (PKI) as a way of securing information that is exchanged either through their own networks or through the public Internet.
The term PKI can be very confusing because it is used to mean several different things. On the one hand, PKI may mean the methods, technology and techniques that utilize public key encryption to provide a secure infrastructure (a “macro-level” interpretation). On the other hand, it may mean the use of a public and private key pair for authentication and proof of content (a “micro-level” interpretation).

PKI is a security architecture that was introduced to provide an increased level of confidence in exchanging information over an insecure internet. In this sub-section, a basic overview of the public key (PKI) infrastructure and the key terms and concepts used in a PKI are presented.

Public Key Infrastructure refers to the framework and services that provide for the generation, production, distribution, control, and accounting of public key certificates, and provides that critically needed support to applications providing confidentiality and authentication of network transactions as well as data integrity and non-repudiation. The PKI encompasses certificate management and registration functions.

Essentially, a PKI includes all the components required to establish and maintain the trust relationship and the binding of a public key to its owner within a system providing public key based applications

### 2.8.2 Characteristics of PKI

A public key infrastructure lets an organization take advantage of the speed and immediacy of the Internet while protecting critical information from interception, tampering, and unauthorized access. A PKI provides the following capabilities (Fhield, 2004):

- Communicate securely with an organization’s employees around the world. A PKI offers remote users with secure channels to their home intranets.
- Exchange confidential data with an organization’s business partners. A PKI supports the creation of secure extranets that give select partners easy access to business-critical information stored on an organization’s internal network.
- Take advantage of secure e-commerce. PKI offer a world of customers the confidence to purchase goods and services on the Web.

In more analytical terms, a PKI is expected to offer its users the following benefits (Fhield, 2004):

1. Authentication - proof that the sender is whom he claims to be
    - Digital certificates issued as part of an organization's PKI allow individual users, organizations, and website operators to confidently validate the identity of each party in an Internet transaction.

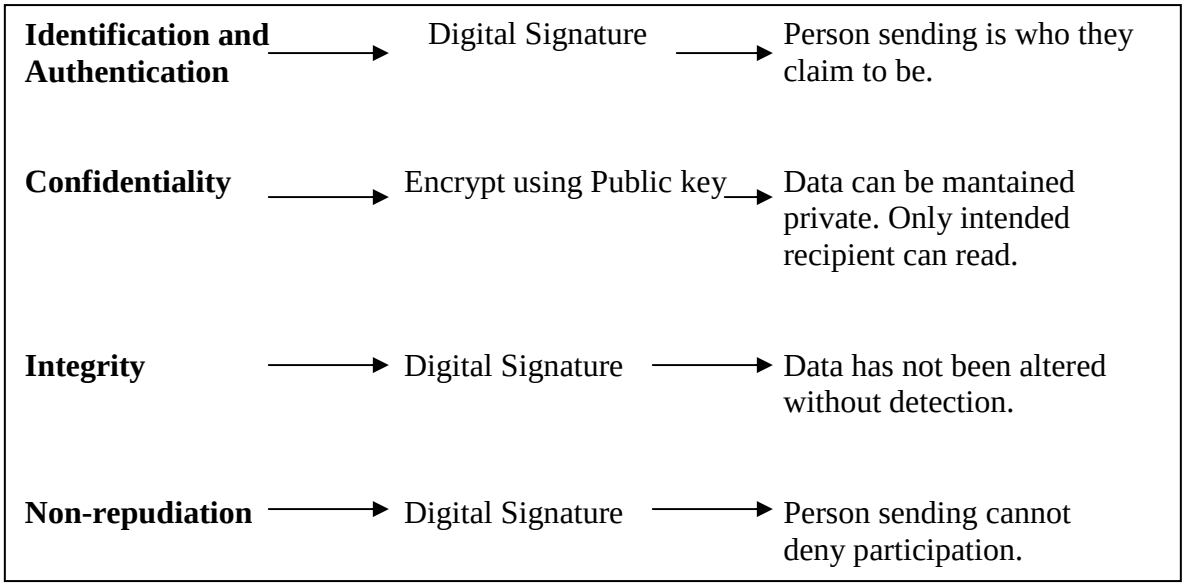
2. Privacy (Confidentiality) - assurance that only the intended recipient is able to decrypt the sent message
    - Public key encryption protects information from inspection during transmission.

3. Authorization - protection against unauthorized use
    - PKI digital certificates replace easily guessed and frequently lost user IDs and passwords to streamline intranet login security (access authorization).
    - With PKI solutions, an organization can control access privileges for specified online transactions (transaction authorization).

4. Integrity - verification that no undetectable modification of data has taken place during storage or transmission across the network.
    - A digital certificate ensures that the message or document the certificate owner "signs" has not been changed or corrupted.

5. Non-Repudiation - assurance for the legal community that the person sending cannot deny participation.
    - Digital certificates validate their users' identities, making it nearly impossible to repudiate a digitally "signed" transaction later.

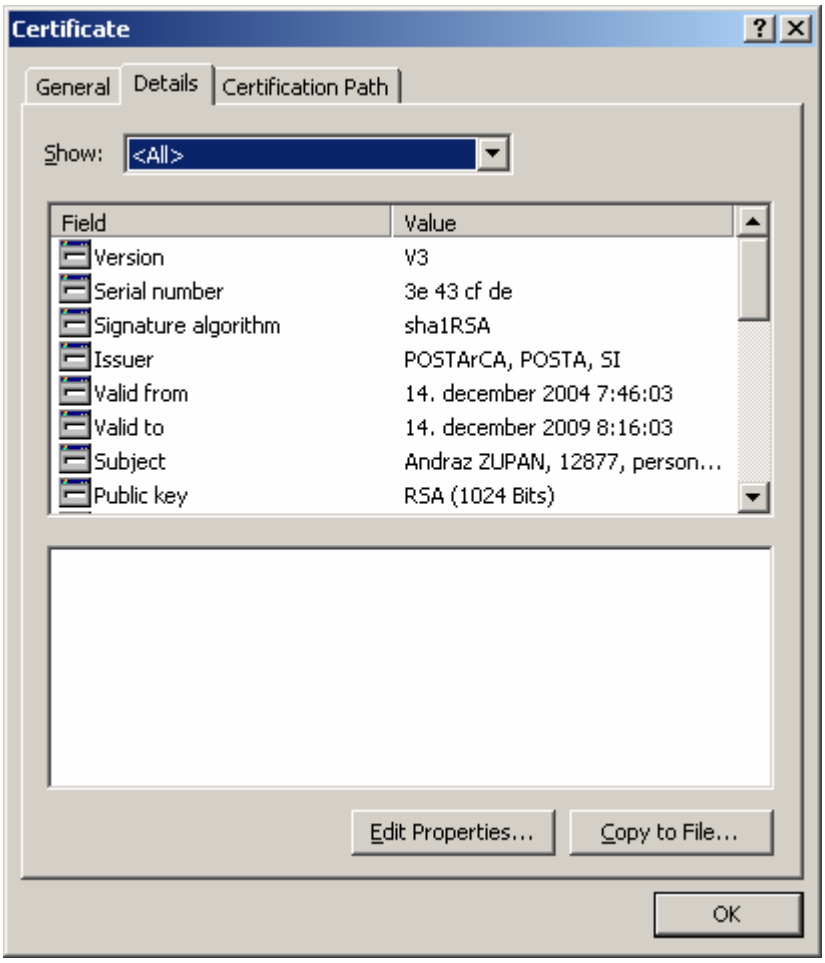
Figure 8: PKI basic security services




### 2.8.3 Certificates

There are some problems regarding public key usage. For example, how can users "carry" and manage many, and how they can be sure that, each key truly belongs to its claimed owner. Certificates and certification authorities are used to answer these questions and build confidence into a public key infrastructure.

Figure 9: Certificate fields




1. Identity

This certificate is used to digitally sign documents or electronic forms and to authenticate (prove a claimed identity) the user to applications. Each individual will have, at a minimum, an Identity certificate.

2. E-Mail Signature

This certificate is used to digitally sign e-mail messages. This is only required if the user's organization is using a PKI-enabled E-mail application.

3. E-Mail Encryption

This certificate is used to digitally encrypt e-mail messages. This is only required if the user's organization is using a PKI-enabled E-mail application.

4. Server

Certain servers, such as private web servers, will be required to have their own identity certificates to properly identify the server on the network and to provide secure, encrypted communications.

Table 2: Certificates usage

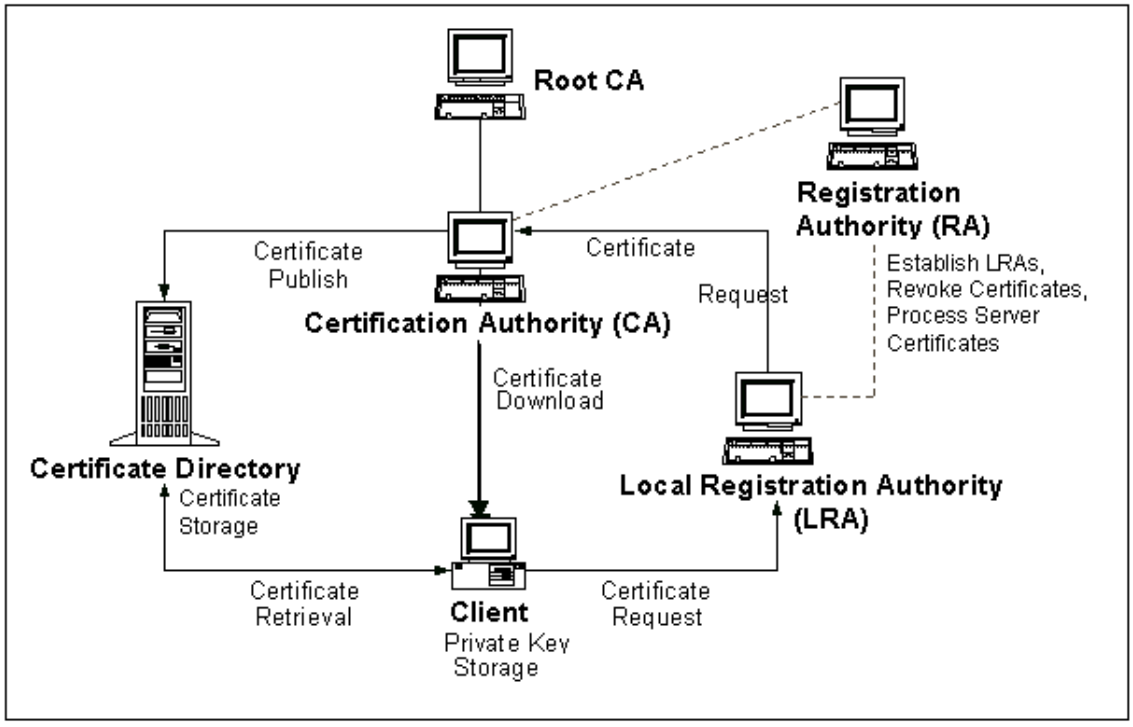
| **Type** | **Facilitates** |
|---|---|
| Identity | Authentication, Non-repudiation, and non-e-mail digital signature |
| E-mail Signature | Authentication, Non-repudiation, and e-mail digital signature |
| E-mail Encryption | Encryption of electronic transmissions for greater security and confidentiality |
| Server | Enables SSL Encryption of Web Server Content |

Source: Verisign, 2003

## 2.9 Major components of PKI

A PKI is created by combining a number of services and technologies.

Figure 10: Services basic relationship




Source: edited after Zero-Knowledge Systems, 2000

### 2.9.1 Certificate Authority (CA)

The CA is an essential component of a PKI. The CA issues certificates after the prospective certificate owners' identities have been confirmed. "Issuing" a certificate, means that the CA signs the hash of the identity and public key value; thus protecting the integrity of the binding and authenticating the identity of the certificate owners. As a result, the issued certificate can be made publicly available and used by other individuals doing business with the certificate owner.

The CA can be a unit within an organization or by an independent entity, for example PoštaCA. The CAs issue certificates to RAs, LRAs, and users. They are also responsible for revoking certificates, creating, maintaining, and publishing certificate revocation lists (CRLs), renewing certificates, maintaining archives of expired and

revoked certificates, and possibly retaining a copy of the user's data encryption private key for purposes of data recovery in the event the user loses this key.

A CA may also state the quality of the checks conducted before the certificate was issued. Different classes of certificates can be purchased that correspond to the level of checks made. There are four general classes of certificates:

- Class 1 certificates can be easily acquired by supplying an email address.
- Class 2 certificates require additional personal information to be supplied.
- Class 3 certificates can only be obtained after more thorough checks have been made of the requestor's identity.
- Class 4 certificates may be used by governments and organizations needing very high levels of identification verification.

The revocation information provided by the CAs about revoked certificates lets users know when certificates are no longer valid. This can be done in one of two ways:

1) Certificates can be deleted from the directory or database in which they should be found. As a result, any attempt to find them to check that they still exist will fail and anyone looking for them would know that they have been revoked.

2) A system of revocation lists (CRLs) has been developed that exists outside the directory. This is a list of certificates that are no longer valid (no matter the reason).

### 2.9.2 Registration Authority (RA)

A CA typically employs one or more separate facilities, called Registration Authorities (RA) to perform the necessary identity checks on certificate applicants. A RA authorizes the creation of a certificate and provides identity validation information to the CA. Depending upon the specific infrastructure; it may also be the RA (or LRA) that also sends the applicant's public key to the CA to have it certified and place in a certificate. RAs are also responsible for administering any Local Registration Authorities that are deemed necessary, and serve as reporting point for the notification of revocation requests.

### 2.9.3 Local Registration Authority (LRA)

Like RAs, LRAs are responsible for registering applicants. They authorize the creation of a certificate and provide the requisite information to the CA.

Users are required to prove their identity using their ID cards. Once the identity is verified, the LRA then registers the users. Afterwards the users are taught how to generate their key pair and obtain their certificate from the CA. LRAs are established only in larger PKIs where users are expected to be spread over a wide geographical area, and would therefore benefit from the accessibility of a local office that handles the registration and user level administration of the infrastructure on behalf of the superior RA.

### 2.9.4 Directory (or Repository)

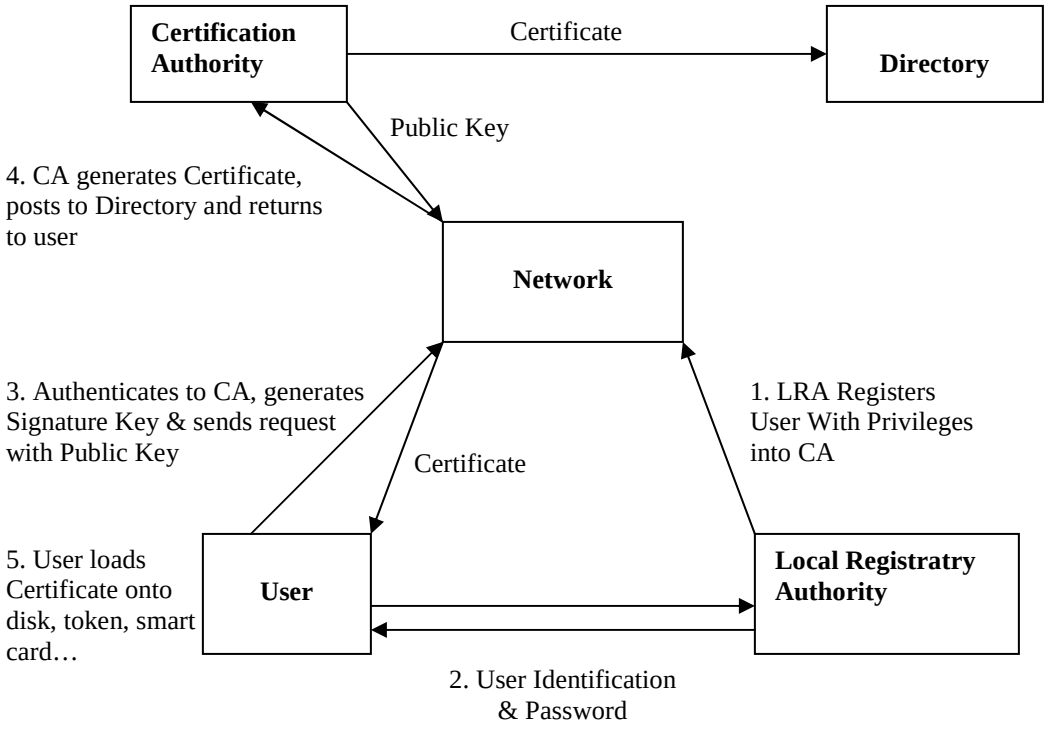
Directories are one of the vital elements of any PKI. The CAs publish certificates and CRLs to these directories. In this manner, a user can retrieve the certificate of any other user who has been issued a certificate by the directory owning CA. These directories store all current certificates and current certificate revocation lists.

Directories are databases that contain certificates. They may be made publicly available or may be access limited to a specific organization. For example, an organization may have its own directory where it holds certificates for the exclusive use of only its users.

### 2.9.5 Users

Users are all people, devices or applications, that will be issued certificates (certificate owners), or will utilize the certificates of others (relying parties). All users who are issued certificates are expected to keep the associated private key confidential.

Figure 11: PKI components relationship




Source: Zero-Knowledge Systems, 2000

### 2.9.6 Certificate Revocation Lists

Each certificate contains an expiration date. In addition, a certificate may become invalid before the expiration date occurs. Since the entire infrastructure relies upon certificates validity, a system has to exist which allows participants to know when certificates have been invalidated prior to their normal expiration date. Consequently, CAs need a mechanism to provide a status update for the certificates they have issued and published.

One approach to solving this issue could be to delete certificates from the directory or database in which they should be found. As a result, any attempt to find them to check that they still exist will fail and anyone looking for them would know that they have been revoked. There are three problems with this approach (Cisco, 2004):

- A denial of service attack on the directory or database might create the false appearance of a failed certificate.

- Deleting the record does not tell the person asking for the information why it is not there, which may be important depending upon local policy regarding the reason for revocation.
- Many implementations of the PKI will result in certificates being cached (copied) in multiple locations; thus complicating the simple solution of simply deleting certificates only from the CAs directory.

As a result, a system of managing revocation lists has been developed that exists outside of the certificate directory/database.

A Certificate Revocation List (CRL) is a computer generated list of certificates that have been revoked by the issuer prior to their original expiration dates for some reason. Revocation lists are periodically issued by each certificate authority and published to the directory. Accessibility to the revocation lists is of paramount importance to the trust required of the infrastructure, as relying parties must ensure that the certificates they use have not been revoked. Thus, these lists should be available at all times, even when their corresponding certificate directory may not be available. In other words, the inability to obtain a certificate is deemed less problematic than the inability to verify the status of a certificate.

Certificates may be revoked for a variety of reasons, including (Cisco, 2004):

- Key Compromise – there is reason to believe the token on which a user or other end-entity private key resides or an unauthorized individual has obtained a copy of the private key, in the case of software tokens.
- CA Compromise – there is reason to believe an unauthorized individual has obtained the token on which the CA private key resides.
- Affiliation Changed – the user has terminated the association with an organization listed in the Distinguished Name field in the certificate. Position changes within an organization do not require revocation of a certificate.
- Superseded – a replacement certificate has been issued to a user, other end-entity, or CA and none of the above reasons are applicable. Examples include that the token has failed, the user has forgotten the password to unlock the token, there is a change in legal name or a change in unique identifier.
- Cessation Of Operation – applies to CA certificates. The operation of the CA has been terminated. Note that if a CA no longer issues certificates, but remains capable of issuing CRLs, its certificate need not be revoked and certificates issued by the CA may continue to be used.

## 2.10 Smart card

Smart cards were conceived as an alternative that could help securely manage both private and public key (certificate) management, providing both convenience and security while minimizing the users need to expose personal and private information. Since the smart card is an active device (it is capable of processing data via an onboard processor), it is able to restrict the information it provides to only that is required for the specific services for which it is intended to interface with. In addition to information security, smart cards achieve greater physical security of services and equipment, because the credentials on the card provide a relatively strong authentication mechanism (PIN code) for access to physical facilities.

A smart card is a type of plastic card embedded with a computer chip that stores and processes data on behalf of the card's owner and computer system with which he interacts. Pertinent external data (the hash of a document to be signed) is transferred to the card and processed within the card's microprocessor chip. User or application-specific data or programs stored on the card are accessed via a peripheral card reader device that acts as a conduit between the functionalities provided by the card and various network applications. The cards greatly improve the convenience and security of cryptographic transactions and they provide somewhat tamper resistant storage of the owner's cryptographic credentials. Smart cards also provide vital components of system security for the exchange of data throughout virtually any type of network. They protect against a full range of security threats, from careless storage of user passwords to sophisticated system hacks. Smart cards can also serve as a means for network system access, and can store other personal data such as medical, security clearances, authorizations, biometric information, payroll information, etc.

Smart card enhanced systems are in use today, and to varying degrees, all applications can benefit from the added features and security that smart cards provide. People worldwide are now using smart cards for a wide variety of daily tasks. Most of these tasks revolve around some implementation of securing information and/or physical assets (Boshell, 2004).

# 3.0 CHAPTER II - LEGISLATION

A lack of electronic signature legal regulation could in the first place represent, a significant obstacle within the development of electronic commerce in the business sector and thus within the development of the specific country in general.

New business possibilities are available, thus creating new ways for increasing of productiveness and decreasing of costs and new ways to approach the customers. The act of electronic commerce offers Slovenia an opportunity for a faster economic development and an equal competition with much bigger countries to its economy. Namely, it is precisely in the electronic world, where size is losing its significance.

## 3.1 EU Directive on electronic signatures

On 19 January 2000, the directive on a EU community framework for electronic signatures (1999/93/EC) entered into force. The member states had to implement the directive in national legislation by 19 July 2001 (Diedrich, 2000).

The rationale for this directive stems from the fact that divergent rules with respect to legal recognition of electronic signatures in the member states may create significant barriers to the use of electronic communications and e-commerce. A clear community framework regarding the conditions applying to electronic signatures could strengthen confidence in and general acceptance of the new technologies. The main objectives of the Directive are (Diedrich, 2000):
-To make sure that all member states accept the legal validity of an electronic signature.
-To make sure that all services relating to electronic signatures can be provided on the EU market without national obstacles.

According to the directive, every kind of electronic authentication attached to or logically associated with the data to be signed obtains legal validity. The directive calls such a general authentication method an “electronic signature”. An “advanced electronic signature” is an electronic signature that meets some specific requirements set in the directive. An advanced electronic signature that is based on a qualified certificate and created by a secure signature creation device has, according to the directive, the same legal value as a handwritten signature. About thirty requirements need to be fulfilled in order to have this kind of signature.

Practically, this means that, for electronic signatures, every type of electronic authentication will be regarded as an electronic signature, as long as it is attached to or associated in a logical way with other electronic data. Signatures created using public key infrastructure (PKI) fall under electronic signatures as well. The definition of an electronic signature in the directive does not even exclude the typed name at the bottom of an e-mail or the attachment of a scanned signature to a document.

Furthermore, the member states shall ensure that advanced electronic signatures based on a qualified certificate and created by a secure signature creation device satisfy the legal requirements of a signature and are admissible as evidence in legal proceedings. A judge can only decline giving legal value to an electronic signature if he or she assumes the security was not sufficient to ensure trustworthiness.

The Directive is technologically neutral and is not limited, for example, to PKI. PKI is one technology available to implement some certification services.

According to Article 3 of the directive (on market access), member states shall ensure that certification services (the issuance of certificates or the provision of other services related to electronic signatures) can be provided in the EU market without being confronted with national legal barriers, such as a national licensing system. Hence, a provider of certification services is not subject to prior authorisation.

Member States are allowed to introduce “voluntary accreditation schemes” to enhance the level of certification service provision. This means that if a member state wants to introduce a new electronic signature system, which is more secure than the EU electronic signatures (as defined in the directive), it is allowed to do so. According to Article 3 of the directive, the conditions related to such schemes must be objective, transparent, proportionate and non-discriminatory. Participation in the accreditation scheme must be voluntary (Diedrich, 2003).

Member States shall establish a supervisory system to control the Certification Service Providers (CSPs) issuing qualified certificates and established on their territory. CSPs wishing to issue qualified certificates have to meet certain conditions. The directive does not exclude the establishment of private bodies designated by member states for this purpose (Dumortier, 2004).

## 3.2 Slovenian e-signature act

The act provides clear and predictable rules for the exchange of the electronic messages, and rules for the use of the electronic signature and operation of the certification service providers of the electronic signatures. The act insured also that the Slovenian legal framework of the electronic commerce and electronic signature is adjusted with the relevant foreign, mostly European and international legal framework, and thus to ensure an international recognition of the electronic signatures (Silič, 2000).

The adoption of the act gives to the Slovenian economy and state administration an important competitive advantage, because Slovenia with a modern legal framework was placed among the first ten European countries, which had, accordingly to the new rules of the EU, regulated the electronic commerce and opened with the relevant legislation a way into a new, technologically supported millennium.

***Brief explanation of the act***

The electronic signature act regulates certain legal questions, imposed by fast technological development and accelerated introduction of the electronic commerce into the business and public sector. The essential purpose of the legislator was legally equalize, where it is possible and reasonable, the electronic form of operation with the earlier classical paper operation, and, under special conditions recognize to the electronic signature the same validity as the autographic signature has in the paper world.

The act has been entirely adapted under the provisions United Nations Commission or the International Trade Laws (UNCITRAL) model law of the electronic commerce and with the provisions of the primary European legislation. It assumes also all the provisions of the Directive 1999/93/EC of the European parliament and EU Council from 13 December 1999 concerning common framework of the community framework for electronic signatures (Perenič, 2000).

The act of the electronic signature is based on modern principles (Perenič, 2000):
- The principle of non-discrimination of the electronic form.
- The principle of openness.
- The principle of the contractual freedom of the parties,.
- The principle of duality.
- The principle of protection of personal data and protection of the consumers.

- The principle of international recognition.

The principle of non-discrimination of the electronic form means, that the paper form and the electronic form are reasonably equalized, thus the courts and state organs within the evaluation of the evidence cannot refuse evidence solely on the grounds of its electronic form.

The principle of openness or technological neutrality ensures, that the act does not refer only to one kind of technology or just to current solutions, but remains general and thus useful for a longer time term and new technologies. Along with the fast and various technological developments is also the principle of duality, which allows the use of different technological solutions with different reliability and thus different legal consequences of the use of such solutions.

The principle of the contractual freedom of the parties enables the parties to agree and regulate their relationships differently. Therefore, the act explicitly provides that it is not valid for the closed systems, where the parties regulate in advance with a contract all the essential characteristics of the operation of the system. Thus, contractual parties within electronic commerce in closed systems are not bound only by the solutions, foreseen by law.

Because of the technological complexity of the solutions for electronic commerce, the principle of the protection of personal data and protection of the consumers are also important. The principle of the protection of personal data follows the rules, enforced in Slovenia and the European Union concerning the protection of personal data, which are even more exposed in the electronic world. The principle of the protection of consumers protects an average consumer, for whom, without a lot of technological knowledge, is more difficult to implement his rights in the complicated electronic commerce, and imposes to the service providers special care for the consumer.

The principle of international recognition enables a simple mutual recognition of electronic documents and signatures and thus enables a simple integration of the Slovenian economy into the international economy. International recognition of the legal effect of data and signatures in electronic form is very important, because electronic commerce does not take into account state borders or borders between individual legal systems.

In the third chapter, the act regulates more extensively the electronic signature and the operation of certification service providers, who represent an inevitable condition

for the use of the electronic signatures. The act entirely relies on European and world orientations and uses a so-called dual approach. It allows the operation of the certification service providers without previous permission and does not imply special conditions for their operation, but it enables the operation of certification service providers to provide different verification services under very varid conditions, which gives them different legal effect regarding their reliability. A part of these rules is also a provision of obligatory and voluntary supervision.

The act provides only general conditions for operation of certification service providers and electronic signature creation. The more detailed requirements are on an explicit legal authorization with a special provision provided by the Government of Slovenia. The act in itself in its fourth chapter incriminates certain conducts as criminal offences and thereof provides sanctions.

# 4.0 CHAPTER III – PKI CONSIDERATIONS

In the following sub-sections, some considerations related to PKI are presented from legal, technical, organisational and interoperability perspectives.

## 4.1 Legal considerations in EU

Different national laws could have implications for certificate authorities and their liabilities and for the deployment of PKI technology in general. In addition, the dispute resolution framework (for when problems occur with the use of the certificates) could differ across national legal systems. The E-signature directive defines qualified electronic signatures in a functional, non-technical way. Due to the technology neutral approach of the directive, work needs to be carried out on setting standards for fulfilling the requirements. The European standardisation bodies are working on technical standards, which comply with the directive and can easily be implemented in technical solutions. Furthermore, the E-signature directive does not specify how it should be ensured that the CSPs act in a prudent manner and leaves this aspect to the member states. In addition, the effectiveness of the electronic signature process depends upon the reliable association of a public-private key pair with an identified person. In the absence of clear requirements and procedures for these requirements to be met, an RA might refrain from prudently verifying the identities of persons to whom they issue certificates for e-payments (EUCB, 2002).

## 4.2 Technical and organisational considerations

A PKI model requires good implementation and prudent operation, which are essential to guarantee the proper use of certificates and proper verification of a certificate's validity. Some considerations that need to be addressed are (EUCB, 2002):

- How is the trustworthiness of the institution that provides the public key certificates (the CA), or of the institution that authorises other certification authorities, ensured?

- How carefully does the CA verify the identity of the applicant?

- How are the private signing keys protected from misuse? These keys may be stored on PCs that are subject to attacks. Under some jurisdictions, responsibility for the

private key remains with its rightful owner, even in the event that it is stolen and misused.
- How is the security of the directory services ensured? Attackers could add their own public key (under an imaginary name) to the directory or a public key in the name of somebody else (organization).

- How is tampering with keys detected? Are they then revoked? Can the revocation be retroactive? (Can a certificate holder deny having made some signature in the past?)

- How can the robustness of an e-signature certification scheme be measured? Not all applications require the same degree of security. Some solutions however, may be unsuitable for payment and financial applications.

## 4.3 Interoperability considerations

The development of PKI is now focusing on building proprietary solutions that, by involving a large number of participants, could later become standards in specific environments. These private PKI solutions reflect organization business needs and will implement different PKI architectures, security policies and cryptographic tools to meet specific needs.

It can be expected that in the future efforts will move to address the need for interoperability among different proprietary solutions developed by competitors in the same organization business (as already observed for smart card technology). Large organizations may have a competitive advantage, as they will be able to impose a “proprietary PKI application” simply because they have a large number of customers and hence possible counterparts. In the banking sector, large banks could be the leading force and might impose solutions on smaller players and their customers (like NLB bank in Slovenia).

A wider interoperability of e-payment PKI schemes would facilitate consumer adoption because of increased scope. Such increased interoperability would mean that the critical mass needed for successful implementation of an e-payment PKI would be likely to be achieved sooner. Interoperability would also increase efficiency by limiting the need for investment by both users and merchants.

## 4.4 Summary

The main obstacles to any security infrastructure are related to establishing the appropriate organisational framework needed to complement the technical implementation. This is true for both symmetric and asymmetric encryption technologies. It is also obvious that when secure communication needs to be established between several parties, symmetric encryption might not be efficient, as the distribution of bilaterally shared secret keys can become a very burdensome and risky task. However, although asymmetric encryption simplifies key distribution, it does not solve the problem completely. One of the most relevant challenges with asymmetric encryption is the establishment of the infrastructure needed to provide trust and to manage the keys. The infrastructure that combines cryptographic tools with the organisational framework is known as PKI. PKI initiatives are being implemented throughout the EU to ensure security of all types of electronic transactions over the internet. At the same time, different implementations of PKI and different regulatory frameworks can be observed across Europe. From a European perspective, two questions are important. Firstly, will PKI become or stay a dominant method for securing e-payment? Secondly, if so, how could interoperability of the different schemes be ensured without compromising the desired level of security (EUCB, 2002)? In addition to user acceptance, legal, technical and organisational considerations are important to answer the first question. PKI does require a relatively complex infrastructure with relatively high costs. If simpler and cheaper solutions are available, those may come to dominate the market.

# 5.0 CHAPTER IV – CALCULATING FINANCIAL RETURNS ON INVESTMENTS

This chapter focuses on quantifying the value of public key infrastructure (PKI) to organization. This information is most useful for organization business executives who want to understand how PKI applications improve their organization's bottom line and IT managers who want to show financial justification for their IT spending on PKI.

Obviously, to have positive ROI, a PKI application must either increase organizations revenues or reduce organizations costs. This chapter provides a methodology and an actual quantitative financial analysis of the decision to purchase PKI applications. This approach attaches a euro value to the benefits of applying PKI to organization. In second sub-section of this chapter a practical case of calculating ROI in PKI and digital signature is presented.

## 5.1 What is ROI (Returns on Investments)

For a given use of money in organization, the ROI (return on investment) is how much profit or cost saving is realized. An ROI calculation is sometimes used along with other approaches to develop a business case for a given proposal. The overall ROI is sometimes used as a way to grade how well an organization is managed (Adelman, 2003).

If organization has immediate objectives of getting market revenue share, building infrastructure, positioning itself for sale, or other objectives, a return on investment might be measured in terms of meeting one or more of these objectives rather than in immediate profit or cost saving.

Decision makers make IT project selection decisions based upon the perceived value of the investment. IT's value is determined by the relationship between what the organization will pay (costs) and what it will get back (benefits). The larger the amount of benefit in relation to cost, the greater the value of the IT project (Adelman, 2003).

## 5.2 Approach for computing ROI on PKI

PKI is not uniquely complex or difficult to analyze with appropriate approach. This subsection defines approach for computing financial returns for PKI enabled applications, which is the same one used for virtually any other significant investment.

***1 step: Focusing on the business process.***

PKI is an e-security infrastructure, and infrastructure in the absence of a specific business process returns nothing. For example, investment in telephones is made but calls never placed, there would not be any gain in this. Moreover, returns from e-security infrastructures are generally difficult to separate from the returns from the business processes themselves. The primary focus, once it has been determined that authentication, data privacy, data integrity, digital signatures, or other e-security capabilities provided by PKI are important business requirements, should therefore be on the financial returns from the successful implementation of a particular (security-enabled) business process. This approach also accommodates the reality that financial returns are typically application-specific, company-specific, industry-specific, and so on (RSA, 2002).

***2 step: Establishing Appropriate Metrics.***

With a proper focus on security-enabled business process, the next step is to establish the appropriate metrics for determining potential financial returns. The metrics chosen will logically be a function of not only the particular business process under analysis (is it an internal process, a customer-facing process or a partner-facing process?), but also the specific business objectives (is it aimed to increase revenues, lower costs or improve efficiency?) (RSA, 2002).

***3 step: Establishing a Baseline for the Current State.***

Having established an appropriate set of metrics, the next step is to use them to establish a baseline for the business process under analysis, based on the way things are today. This is the “business as usual” scenario (RSA, 2002).

***4 step: Comparing to the Desired Future State.***

The same metrics can then be used to compute the financial impact of implementing a new or improved business process that meets the specific business objectives. This is the “business as a result of ” scenario (the desired future state that will result from the successful implementation of a new or improved PKI enabled business process).

All that is needed is a general framework to help organize the approach and a detailed discussion of potential financial returns can start.(RSA, 2002).

The first, critical step is to frame the ROI discussion in the context of the key e-security enablers for a particular e-business process or application. The next step is to establish an appropriate set of metrics for determining potential financial returns.

### 5.2.1 Metrics

The most appropriate metrics are a function of both the business process under analysis and one or more specific business objectives. Tables 3,4 and 5 list a number of potential metrics for certain example business objectives, and provides examples of “impact statements” in the form of questions that set up a comparison of the current state with the desired future state in terms of one or more specific metrics. Quantifying the answers to these questions is the key to unlocking the financial returns made possible by PKI enabled applications.

Quantifiable financial returns made possible by PKI enabled applications tend to fall into one of the following four high-level categories: Revenues, Costs, Compliance, and Risks.

Table 3: Potential metrics 1

| Business Process | Example Business Objectives | Potential Metrics | Example Impact Statements (The Key to Unlocking Financial Returns) |
|---|---|---|---|
| Customer-Facing | Maximize online revenues from existing customers | • % of revenue generated online<br>• % of existing customers doing business online<br>• % of customer wallet spent online<br>• % drop-off rate<br>• Repeat business rates<br>• % of up-sell, crosssell conversions<br>• Lifetime revenue per customer | 50% of our online customers don't complete transactions that require them to print, sign and mail paper documents. What is the financial impact in case of reduction of this drop-off rate to 25% by using digital signatures to complete the entire transaction online, as well as eliminate the cost of paper, printing, postage, and processing? |
| | Minimize costs of finding and acquiring new customers | • % of new customers acquired online<br>• Cost of new customer acquisition<br>• Brand perception, brand awareness | What is the financial impact in case of leveraging 50% of all established online account relationships with Line of Business #1 to create an online account relationship with Line of Business #2? |
| | Maximize customer satisfaction; reduce help desk and support costs | • Number of incorrect order incidents<br>• Service levels used<br>• Number of service / help desk requests<br>• % of service / help desk requests resolved online | What is the financial impact if authorized customers could resolve 80% of help desk calls directly, online, rather than by live agents over a toll-free number? |

Source: CCE Journal, 2002

Table 4: Potential metrics 2

| Business Process | Example Business Objectives | Potential Metrics | Example Impact Statements (The Key to Unlocking Financial Returns) |
|---|---|---|---|
| Internal | Increase responsiveness to changing market conditions | • Order cycle / delivery time<br>• Product time-to market<br>• Product time-to change | What is the financial impact if the process cycle time is reduced from X days to Y hours, while preserving the integrity and authenticity of documents and transactions? |
| | Reduce costs, improve productivity | • Cost of materials<br>• Cost of services<br>• Productivity per employee<br>• Number of service / help desk requests<br>• % of service / help desk requests resolved online | What is the financial impact if employee productivity is increased and help desk calls, caused by password resets, reduced, by using PKI-based authentication with Virtual Private Network or with Reduced Sign-On initiative? |

Source: CCE Journal, 2002

Table 5: Potential metrics 3

| Business Process | Example Business Objectives | Potential Metrics | Example Impact Statements (The Key to Unlocking Financial Returns) |
|---|---|---|---|
| Partner-Facing | Tighten degree of system integration with strategic Partners | • % of production goods procured online<br>• % of maintenance / repairs / operating supplies procured online | What is the financial impact if delivery times are shorten and inventory reduced, by enabling authorized users to procure 80% of all maintenance, repairs and operating supplies through a Web browser, mobile phone, or wireless personal digital assistant? |
| | Reduce Partnership costs, improve Partner reliability | • Comparative prices<br>• Cost / Uptime of partner connections<br>• Cost / Rate of partner repairs, replacements, returns<br>• Cost, time commitment scorecard | What is the financial impact if authorized strategic partners are provided with increased access to sensitive information, without compromising security or giving up control? |

Source: CCE Journal, 2002

### 5.2.2 Revenues

Business processes that generate new or increased revenue streams create the most compelling justifications for investments in enabling infrastructure such as PKI. Because revenue enhancements are generally more strategic than tactical in nature, they can also be somewhat more difficult to quantify.

Based on metrics such as those found in Table 3,4 and 5 it can be reasonably quantified any number of incremental revenue streams for PKI enabled applications. For example, suppose 50% of organization online customers currently end up abandoning transactions that require them to print, sign and mail paper documents rather than allow them to complete the entire transaction online. What would it mean with respect to incremental revenue if this drop-off rate could be substantially

reduced, say to only 25%, by using digital signatures to complete the transaction immediately while simultaneously minimizing the risk of subsequent repudiation? For many document-intensive industries (including financial services, insurance, healthcare…) this would have an enormous impact on revenues – not to mention the potential for reducing the related costs associated with paper, printing, postage, and processing of traditional paper forms.

Other possibilities for quantifiable revenue-based financial returns include cross-selling or up-selling opportunities with established customers, an increased number of transactions per customer, higher rates of repeat business, etc. Important but less quantifiable examples in this category might include competitive advantage, strategic positioning, corporate brand and image.

***Revenue Example with online brokerage transactions***
Organization is online brokerage firm servicing self-directed individual investors. Application enables instant account opening online, therefore paperless process to open an online brokerage account and fund the account electronically.

Business benefits are (Brink, 2002):
- Time to open a new account is reduced from 3-10 days to less than 15 minutes. This is an important factor in accelerating revenues from new account growth and from converting prospects more quickly to active traders.
- Cost avoidance compared to manual account processing and helpdesk calls related to new account openings.
- Cost reductions from reduced mailing and storage costs.

Benefits of PK are (Brink, 2002):
- Account activity acknowledged and authorized by digital signature.
- Reduced risk through use of stronger authentication.
- Higher integrity of stored customer data.

### 5.2.3 Costs

Reductions in cost are perhaps the most reliable drivers of financial returns for PKI enabled applications. Although cost reductions are generally more tactical than strategic in nature, they are also generally the easiest returns to quantify. Cost based financial returns are typically expressed as some combination of the following:

• Cost Savings: the new or improved business process is less expensive.

• Cost Avoidance: the new or improved business process reduces new costs. Spending as many additional euro in support of new capabilities or expanded scale can be avoided.

• Efficiency: the new or improved business process saves time. The velocity at which e-business is conducted can be increased.

• Effectiveness: the new or improved business process increases productivity. More or different things with existing resources can be done.

While it is impossible to generalize about the best sources for cost-based financial returns, at present there are three areas that seem to be particularly effective: help desk costs, telecommunications costs, and costs associated with the processing of electronic forms.

The table 6 illustrates why so many organizations target the help desk as a rich and easy source of cost-based financial returns. End-users can usually experience faster, more convenient service at a reduced cost of up to two-fold. Common PKI enabled applications that can result in substantial reductions in help desk costs include corporate intranets, reduced Sign-On initiatives, virtual private networks, and one-to-many extranets.

Table 6: Transaction costs

| Type of customer service average cost | Transaction |
|---|---|
| Agent (Phone-based) | aprox. 4.00 euro |
| Agent (Web chat) | aprox. 2.00 euro |
| Agent (E-mail) | aprox. 1.75 euro |
| E-mail (Auto reply) | aprox. 0.50 euro |
| Web (Self-service) | aprox. 0.05 euro |

Source: edited after CCE Jurnal, 2002

***Cost example with secure extranet***

Organization is an investment services company that sells mutual funds. Application enables secure extranet for 1,000 independent financial advisors and 7 x 24 self-service access to high-value financial and client information.

Business Benefits are (Brink, 2002):
- Annual cost savings of approximately 40% compared to phone-based, agent based system.
- Largest driver for cost savings is estimated reduction in toll calls and direct agent assistance for three times.

Benefits of PKI are (Brink, 2002):
- Privacy compared to previous process, and integrity of data.
- Authentication of users.
- User accountability for data.
- Customized content.
- Reduced risk of data loss or theft.
- Centralized control of trust properties.

Telecommunications costs also represent great opportunity for cost-based financial returns, and are often used in particular to justify investments in virtual private networks. Many organizations implementing virtual private network technology overlook authentication as a critical e-security requirement, however, on the mistaken assumption that an encrypted communications channel has fully addressed the problem of secure remote communications. Replacing a virtual private network's weak password-based authentication with stronger authentication technology such as PKI improves overall security by more strongly establishing who is on the other end of our virtual private network. This allows sensitive deal making information to be available to remotely located individuals when it is critically needed without the fear of compromise while leveraging the cost advantages of extranet delivery.

A third area of opportunity for cost-based financial returns has to do with the cost of processing paper forms, documents and business records. This is most relevant in document intensive industries such as financial services, insurance, and healthcare, where enormous financial returns are possible from cost reductions in paper, printing, postage, and processing.

The cost of manual document processing is very high: the average paper document is copied 9 to 11 times at a cost of approximately 15 euros and filed at a cost of approximately 18 euros. In addition, there is also the cost of storage, electronic media, physical plant, postage and other distribution.

Mistakes are also expensive: the cost of finding and retrieving misfiled paper documents is approximately 50 euro.

Of course, there are other business benefits to electronic forms processing in addition to lower cost: wider and easier access, better quality, higher data integrity, lower growth in personnel requirements and other.

As an illustration of the magnitude of financial returns of this type, Table 7 compares the average distribution cost through Internet based channels with those through traditional channels for term life insurance, bill payment, and banking, respectively.

Table 7: Distribution costs

| | Traditional Distribution | Internet based Distribution |
|---|---|---|
| Term Life Insurance | 4.00 euro | 1.75 euro |
| Bill Payment | 1.75 euro | 0.50 euro |
| Banking | 0,70 euro | 0,10 euro |

Source: edited after CCE Jurnal, 2002

***Cost Example with electronic mortgage transaction***

Organization is offering home mortgage services. Application enables online mortgage transaction.

Business Benefits (Brink, 2002):
- 15-30 day cycle time reduced to couple of hours.
- Reduced risk of mishandled documents, errors and omissions.
- Reduction in administrative staff, training costs.
- Improved customer service.
- Savings of approximately 20% in total loan lifecycle costs compared to previous process.

Benefits of PKI (Brink, 2002):
- Provable chain of evidence as to the authenticity of documents.
- Authorization to access documents based on user authentication.

### 5.2.4 Compliance

Compliance refers to certain business processes that are required to be implemented, or some e-security requirements that are obligated to be met. Compliance generally refers to things about which there is little choice. These are things that have to be done in order to stay in business. In some cases, compliance

may be related to cost avoidance (avoiding a fine). In others, it may be related to protecting an existing revenue stream. In any event, compliance based business cases tend to be binary: above a certain threshold, they are just done. As it relates to e-security infrastructure, compliance based arguments tend to come from one of the following four categories: Regulatory, Partner, Customer, and Competitive (Brink, 2002).

• Regulatory compliance: where failure to implement could mean fines, loss of revenues or jail terms.

• Partner compliance: where failure to implement could mean losing the ability to participate with a key partner or group of partners.

• Customer compliance: where failure to implement could mean the loss of a business relationship with a key account,.

• Competitive compliance: where failure to implement could mean the loss of competitive advantage and likely revenue loss.

Compliance based business cases tend to be made not so much on the basis of precisely quantified financial returns, but on the basis of “the cost of doing business” In some cases compliance brings with it huge financial and efficiency benefits associated with paper reduction and the enablement of e-business strategies.

### 5.2.5 Risks

Until only recently, risk based arguments were probably the most frequently used approach to justify investments in e-security infrastructure. Marketing campaigns and business cases alike were commonly based on arguments of fear, uncertainty and doubt. Selling security through fear can be reasonably effective, up to a point but it also tends to marginalize e-security as an operating expense, subject to being trimmed at the first round of budget cuts. Today there is significantly more emphasis on the systematic management of risk.

Risk is an inescapable fact of e-business. Investments in e-security infrastructure that are made with prevention in mind are usually not highly visible, unless there is a problem, which tends to make risk based justifications the least glamorous of the four categories in this model.

It seems obvious, but risk mitigation investments should be focused on things that are worth protecting, such as high value information or high volume transactions. For examples of “high value” information, the following is considered (RSA, 2002):

• Information that generates revenue, either directly or indirectly: information, programs, services.

• Information essential to the smooth running of the organization: operational information, administrative information.

• Information pertaining to future revenue streams: research, new product plans, marketing plans, and customer databases.

• Information that must be protected by law: personnel records, student records, patient records.

Once high-value information has been identified, a reasonable attempt to quantify the impact of various security related risk scenarios, using the “impact statement” approach can be then made. For example (RSA, 2002):

• Productivity loss: what would the financial impact be if a security breach caused a sustained disruption of internal processes and communications or if the ability to communicate with customers is lost?

• Monetary loss: what would the financial impact be if there were a security related corruption of accounting system, which led to delays in shipping and billing or if there were a diversion of funds? What would be the expense of recovery and emergency response?

• Indirect loss: what would the financial impact be if a security breach caused the loss of potential sales, the loss of competitive advantage, negative publicity or the loss of goodwill and trust? Indirect losses are among the most difficult to account for, but also among the most compelling in the risk mitigation category, especially for businesses built on the fundamental foundation of trust.

• Legal exposure: what would be the financial impact of failure to meet contractual milestones, failure to meet statutory regulations for the privacy of data or illegal user

or intruder activity on company systems? Organization counsel can potentially be an excellent source of justification for PKI enabled business process.
The answers to these risk oriented impact statements can be difficult to quantify, but the financial implications can be extraordinary. Moreover, the risks themselves are very real. Unauthorized access by insiders is twice as frequent as unauthorized access by outsiders, and growing. The Internet has rapidly replaced internal systems and remote dial-up as the most frequent point of attack.

***Risk Example with E-Government***
A government introduces application that enables logical access to information and other system services.

Business Benefits (Brink, 2002):
- Reduced cost resulting from combined management of personnel identity, physical, and logical access for a geographically diverse population.
- The efficiency of converting paper processes to electronic processes while improving the information assurance posture for sensitive information.

PKI Benefits (Brink, 2002):
- Common infrastructure to support geographically dispersed mobile population.
- Flexible but consistent registration processes.
- Adaptable to multiple levels of assurance.
- Full flexibility in providing confidentiality and authentication of communications and network transactions as well as verification of data integrity and non-repudiation of these transactions.

### 5.2.6 Summary

The most important points for developing meaningful financial returns for PKI enabled applications are to focus on the business process, establish appropriate metrics, and look for all relevant returns in the following high-level categories: Revenues, Costs, Compliance, and Risks.

By properly framing the ROI discussion in the context of the key e-security enablers for a particular e-business process, a beginning to quantify financial returns using a straightforward, widely accepted approach can be very quick. In general, the benefits from PKI enabled applications significantly outweigh the costs of PKI implementation.

The total cost of ownership for implementing and enabling e-security infrastructure such as PKI is significantly less than the financial returns made possible by PKI enabled applications, when revenues, costs, compliance and risks are understood an quantified.

## 5.3. Practical case of calculating ROI in PKI and Digital Signature

Most analyses of PKI focus on its value in ensuring the security of organizations data and communications. From a broader business standpoint, however, this is a very limited view of the value of a Public Key Infrastructure. PKI is central to two major transitions every Organization either has begun to make or will make in the next years:

1. The transition from paper-based to electronic business processes such as electronic mail, electronic file storage, and electronic contracting with digital signatures.

2. The transition from physical separation to Internet integration, allowing remote employees, customers, and vendors to exchange data with the internal corporate network.

These two transitions provide enormous cost savings, productivity benefits, and a competitive market advantage to organizations. It is not a question of whether an organization will complete each transition but when. This sub-section will analyze four PKI applications that facilitate these transitions successfully and calculate the ROI in them.

### 5.3.1 Eliminating Paper-Based Business Processes

Long predicted, the elimination of paper based business processes is finally happening. Three of the PKI applications analyzed in this sub-section include a component of value based on eliminating paper communications.

• Although electronic mail has replaced many paper-based communications, documents that are more sensitive are still sent the old-fashioned way for greater security. PKI based trusted messaging allows sensitive documents to be sent by e-mail, eliminating the processing costs, mailing costs, and time delays associated with traditional regular or overnight mail.

• Trusted online account activation for financial accounts, which have traditionally required the sending of physical contract signatures and transfer authorizations by paper mail to get started, uses digital signatures and electronic authentication records checking to dramatically speed-up activation.

• Trusted forms with PKI based digital signature eliminates processing time, storage costs, and labour associated with manual procedures.

### 5.3.2 Enabling Internet integration

PKI based authentication procedures are central to Internet integration. As the data exchanged with remote employees, customers, and vendors becomes increasingly sensitive, and as these people are increasingly allowed to access internal corporate data and the internal network, making sure they are who they say they are, has become a crucial precondition for many applications. One application that analyze the financial value of PKI for Internet integration is :

• Trusted Access – evaluates the security value of PKI-based authentication to access corporate web based applications.

Trusted messaging and trusted online account activation also could be said to “enable Internet integration,” even though they do not allow access to sensitive organizations data. They are included in the first category, however, because their primary economic value is in replacing paper-based processes (paper mail and paper contracting) with electronic ones.

### 5.3.3 Methodology

Before beginning the quantitative analysis, the ROI value metric should be defined.

The selected ROI value metric is “Average Euros Per User Per Year”. There are also many other possible value metrics for an ROI analysis such as (Infoworld, 2006):

• Year-by-year cash flows
• Time to payback
• Internal rate of return
• Net present value

One disadvantage of some of these metrics is that computing them requires knowledge of the size of the organization (or the number of users in the PKI installation) and the time horizon over which the organization evaluates its technology investments. Because these variables cannot be known in advance, the selected metric is “Average Euros Per User Per Year” which can be multiplied by the variables once they are know.

For example, suppose a PKI installation will have 1000 users, and the organization wants to know the value of the application over three years. Then he average euros per user per year for the application should only be multiplied by 1000 to get the actual euros per year. The result is then multiplied by three to get the total nominal euro value of the application for the three year time horizon.

### 5.3.4 Value of Secure Applications

***Application trusted messaging***

One of the principal benefits of trusted messaging technology is the added security it provides. Secure messages that are intercepted on the way to their destinations cannot be read because they are encrypted. What is more, if they are digitally signed, hackers cannot spoof the sender’s identity.

Quantifying the value of this added security is difficult in the case of trusted messaging because no or only few statistics are kept on the number of messages that are intercepted.

Therefore, the statistical approach will not be used in the case of trusted messaging. For trusted messaging, instead of measuring and valuing statistical risk reduction, more appropriate are measures and values of the improved business processes that result when electronic communication replaces paper-based communications.

**Value Drivers**

Many types of messages that are currently sent on paper could be sent securely using PKI for Trusted Messaging:

• Sensitive contract drafts.
• Sensitive pricing information.
• Any organization’s data that is being shared with a customer or competitor that the sender does not want forwarded or intercepted.

To maintain simplicity the following variables are used in the trusted messaging value model. For the average employee on the system, next variables are examined:

• The number of paper based messages (traditional mail) per year that can be replaced with secure e-mail.

• The cost of the paper based messages (both in labour time for printing, mailing, addressing and in actual printing and mailing costs).

• The number of days of cycle time that are eliminated when a formerly paper based communication goes out to and returns from its recipient. In business, reducing this turnaround time for key communications directly affects the bottom line.

• The value per day of cycle time reduction.

**Input Assumptions**

Highly conservative assumptions for trusted messaging are used. It is assumed that the average employee will replace only 10 paper-based communications per year with secure e-mail. The average cost to print and mail a traditional piece, including employee labour, is estimated at 2 euros.

Regarding cycle time reduction, with trusted messaging a response can be received the same day or the same hour. By contrast, it takes a minimum of two days to receive a response to a sent piece of print mail because it takes at least one day for the piece to arrive and at least one day for the response to return. Therefore, two days of reduced cycle time are assumed.

The value per day of cycle time reduction can be very high. It might be thousands of euros for a major sale or highly sensitive transaction. To be extremely conservative, a cycle time reduction value of only 10 euros per day is used. (A day of cycle time should be worth more than 10 euros by the following reasoning: when a letter is sent using a next day delivery service to save a day versus using regular mail, typically it will cost 5-10 euro). Therefore, 10 euros is used as the minimum value.

The following table summarizes these assumptions.

Table 8: Trusted messaging inputs

| **Mailing costs impact with PKI** | |
|---|---|
| Number of additional e-mails replacing traditional mail per user per year due to reduced security e-mail risks | 10 |
| Cost per piece to print and send traditional mail, including user labour | 2 euro |
| **Cycle time reduction impact with PKI** | |
| Days of cycle time (days spent waiting for mail delivery and then waiting for a response) saved per mailing | 2 |
| Euros saved per day of cycle time (the value of faster business processes) | 10 euro |

**Results**

The value of trusted messaging is estimated at 220 euro per user per year. Interestingly, the majority of that value is in the cycle time reduction associated with faster business processes. Twenty days of cycle time on key communications is worth 200 euro based on a conservative estimate of 10 euro per day cycle time reduction value.

The elimination of mailing costs is the second biggest factor at 20 euros per employee per year for ten avoided print mailings. Again, the security value of trusted messaging is excluded from this analysis due only to the lack of available statistical data. Otherwise the results would be even higher.

***Application trusted access***

PKI provides a powerful security benefit by protecting access to web applications. While passwords might be easily guessed or sniffed, intercepted on route to the application, or revealed by a brute force attack, PKI based authentication is very difficult to break.

Assessing the value of PKI based authentication for web access is more complex than the trusted messaging analysis. The reason is that the primary value of trusted access is the additional security protection it provides for usernames and passwords.
A secondary value of trusted access is in potential savings of help desk call costs for password resets. Only the second value is used in to assess the value in the case of trusted access calculation, since it is more appropriate.

**Value Drivers**

The two key sets of value drivers for trusted access in this analysis are:

• Reduced risk and damages from security breaches. (Obviously, these kinds of impacts can be quite large. However, they are not explicitly quantified here because specific numbers must be customized to the individual company involved.)

• Reduced help desk calls.

**Input assumptions**

Help desk call reduction

As mentioned, a second benefit of using PKI for authentication to web applications is the reduction in help desk calls. Based on experiences in the bank sector, a typical organization will experience three help desk calls for password resets per user per year. The cost of a help desk call is estimated to 20 euros.

It is estimated that half the password reset calls will be saved as password resets are eliminated, but there are some PKI related calls. Therefore, PKI reduces the cost of help desk calls by 30 euro per user per year. The table 9 summarizes these assumptions.

Table 9: Help desk call reduction assumptions

| **Before PKI:** | |
|---|---|
| Number of username and password related help desk calls per year | 3 |
| Reduction in help desk calls and password resets with PKI 50% | 50% |
| **After PKI:** | |
| Number of username and password related help desk calls | 1.5 |
| Net number of help desk calls eliminated per year | 1.5 |
| Cost per instance to service username or password request | 20 euro |
| Savings from reduced help desk calls per user per year | 30 euro |

**Results**

On a euro per user per year basis, the reduction in help desk calls is worth 30 euro per user per year. In addition, two unknown factors must be estimated. The first is the

risk reduction due to reduced breaches. The second is the reduction in potential consequential damages.

### 5.3.5 Value of digital signature

The trend towards replacing paper contracts and forms with digital signature is still in its earliest stages but as already said, it is no longer a question of whether contracts and forms will become electronic but how fast the transition will occur.

Digital signatures can be divided into:

- contract signatures, in which a legal transaction for the exchange of money, goods, or services between two parties takes place.

- form signatures, in which one party asserts the validity of information provided to another party. Also included in forms signatures are internal company forms that authorize various actions but by themselves, do not create a transaction.

Signatures happen all the time in business. Whether the applications are in the B2B, B2C, C2C, or even G2B and G2C spaces, regular signatures are generally required and digital signature is eventually replacing them.

In general, it has been found that there are three key benefits from digital signatures:

1. Cycle time reduction. Digital signature speeds up the process of contracting. This is a major benefit in the financial account sign-up model.

2. Elimination of printing, mailing, faxing, and storage costs for paper forms. Digital signature eliminates the need to move paper forms around.

3. Reduction in form handling labour and data entry time. Paper forms actually impose significant costs on an organization in terms of time spent by staff entering data from the forms into computers, and copying forms.

Analysis is focused on the following applications:
• Trusted online account activation
• Trusted forms

***Application trusted online account activation***

Consumers are rapidly adopting online financial services, such as Internet banking, online trading, and online loan origination.

However, organizations still utilize paper forms and contracts as part of their online processes. They rely on paper because it provides two assurances: authentication and a legally binding signature. The electronic process that replaces paper forms has slowly begun to catch the attention of organizations.

What took 7 to 14 days to complete can now be completed in as little as 15 minutes. The next step is to assess its value to for online brokerage or banking application example.

**Value Drivers**

Although consumers will certainly place a value on immediate trading and on avoiding paper forms, the focus here is on the value to the online brokerage or bank application and their revenues and costs. The most important source of value to the online brokerage is signing up more new customers. Customer acquisition costs in the financial services industry are roughly 150 euro per customer. This high cost represents an enormous marketing expense for online services. Every newly signed-up customer that does not require additional marketing saves 150 euros in marketing expenses on the online brokerage.

Drop-off rates for prospects hitting an online site range as high as 80 percent. By eliminating the requirement of printing, filling out, and mailing in a paper form the online brokerage can dramatically reduce its drop-off rate. A reduction in the drop-off rate from 80 percent to 50 percent, for example, would increase the number of new signups by 150 percent because the percentage of site visitors signing up would increase from 20 percent to 50 percent.

Other benefits that a brokerage or bank can realize from automated signup include:

• The value of increased trading. The new customer has 7 to 14 more trading days in which to generate commissions and fees for the brokerage.
• Eliminated labour costs for paper form processing.
• Eliminated printing and mailing costs for paper forms.
• The increased security value of having customers continue to authenticate using the PKI based authentication system rather than just using usernames and passwords.

**Input Assumptions**

The value drivers have been numerically estimated in the following table.

Table 10: Input assumptions (Trusted online account activation)

| | |
|---|---|
| Customer acquisition cost | 150 euro |
| **Value of increased trading** | |
| Average euro value of a customer per year? | 100 euro |
| By how many days will this application improve your processing time? | 13 |
| Based on the above inputs, here is the implied value of 13 more days of customer trading to the brokerage. | 3,56 euro |
| **Labour Cost** | |
| How many hours are required to process customer paper forms per signup? | 0.5 |
| What is the average annual salary of processing employees? | 20.000 euro |
| What are the productive hours per year of a processing employee? | 1440 |
| Based on the above inputs, what is the implied labour cost per new employee due<br>to the usage of paper forms (calculated). | 6,94 euro |
| What is the printing and mailing cost per form? | 2 euro |

The 150-euro customer acquisition cost already has been explained. To evaluate the value of the extra trading days (an average of 13 in the estimation), the euro value per year of a customer must be known, which here is estimated at 100 euro. This gives an implied value of 3.56 euro per customer in added trading time.

Making reasonable assumptions regarding labour time required to receive, open, process, and mail forms, a savings to the brokerage of 6,94 euro in labour time is identified. A 2-euro savings per form is also assessed for printing and mailing costs to the brokerage.

**Results**

In assessing the value per signup of this digital signature application, by far the dominant factor is whether faster signup causes more people to join the online brokerage. Labour cost savings, printing and mailing cost savings, and trading time are relatively small (less than 15 euro) compared with the 150 euro customer acquisition cost that is saved when someone new signs up. While faster signup for a customer who would have signed up anyway is only worth 12,5 euro per customer, faster signup that drives a new customer is worth 162,5 euro per customer. If the fast signup process were to double the number of signups, then the average value per signup due to fast signup would be 87,5 euro (halfway between 12,5 and 162,5 euro). For a brokerage that then signs up 1000 new users in a year, the value of this digital signature application would be 87500 euro per year.

***Application trusted forms***

Human resource (HR) forms permeate the modern workplace. Employees spend time filling out, signing HR forms, and getting additional signatures if needed from managers. HR staff spends time processing paper forms and calling around to correct errors or incomplete forms.

Many forms are one-time forms associated with new employee orientation. Other forms must be completed on a sporadic or annual basis. Some forms apply to all employees, others apply to part time employees only.

The estimated value of completely automating HR forms would be: completing them online, signing them with digital signature, automating error checking, and storing the form data electronically in corporate databases.

The analysis is focused on estimating the cost savings associated with automating 10 forms that each employee has to fill out and sign.

**Value Drivers**

It was identified that the following savings would result from automating new employee HR forms:

• Labour time for HR people to process the forms, including all mailing time, photocopying time, filing time, time spent creating offer letters, time spent receiving and processing the forms.

• Employee labour time filling out and processing the forms.

• Printing costs.

A final potential cost savings that could be considered but is not included is cycle time reduction is reducing the number of days from submission of a form to the response by HR.

**Input Assumptions**

The value drivers are numerically estimated in a question and answer format:

Table 11: Input assumptions (Trusted forms)

| **HR labour time saved** | |
|---|---|
| The number of processing hours per new employee by HR for existing paper forms, including all mailing time, photocopying time, filing time, time spent creating an offer letter, time spent receiving and processing the forms. | 3 |
| If the whole process were completely electronic, how many hours would it take an HR person to process each new employee's forms? (Copying, mailing, filing, and processing time are all eliminated, and the new form data is automatically entered into the appropriate databases.) | 0.5 |
| Fully loaded HR labor cost per hour? | 10 euro |
| HR labor time saved per new employee | 25 euro |
| **Employee labour time saved** | |
| Processing hours per employee (paper version) by employee. | 0.5 |
| Processing hours per form (electronic version) by employee. | 0.25 |
| What is the fully loaded employee labour cost per hour? | 10 euro |
| Employee labour time saved per new employee | 2,5 euro |
| Estimating the benefit of shifting from paper to electronic forms | |
| **Printing costs** | |
| What is the total number of pages of HR documents per employee? | 50 |
| What is the printing cost per page? | 0,1 euro |
| Total printing costs per new hire | 5 euro |

Reviewing the input assumptions, it has been found that the total HR time required to create, process, mail, receive, and store forms is three hours under the current system. Using complete electronic forms automation with digital signatures, only 30

minutes would be required. Thus, 2.5 hours of HR labour time would be saved per new employee. The total savings would be 25 euro per new employee.

Employees who might spend half an hour filling out the paper versions of the employee forms could potentially reduce that time to 15 minutes, in part by not having to talk to HR about needed corrections. The total savings would be 2,5 euro per employee.

Finally, printing costs would be eliminated. The cost savings would be 5 euro.

Also storage costs would be virtually eliminated, replacing paper based storage with nearly zero cost electronic storage. But because storage costs are not the significant part of HR forms costs they are not analyzed.

**Results**

Adding all savings, the total savings per employee of automating employee forms would be 32,5 euro per year.

This is a fairly high savings. However, it is important to note, once again, that digital signature is only one part of the technology contributing to the savings. The other part is the HR forms automation technology that integrates with a company's existing corporate databases.

### 5.3.6 Summary

Once a public key infrastructure is in place in an organization for one application, the variable cost of integrating additional applications is quite low. Each new application can take advantage of the same underlying PKI. The benefit of each new application is just as high as if it were the only application being used by the organization. The table 12 provides a summary of the analyzed application values determined in this chapter's calculation.

Table 12: Application value

| **Application value** | **(euro per user per year)** |
|---|---|
| Trusted messaging | 220 |
| Trusted access | 30 |
| Trusted online account activation | 87,5 per customer |
| Trusted forms | 32,5 |

Several themes emerge from this table:

• More applications mean more value.
• More users mean more value.
• More time is more value. The longer the applications are used, the greater the value because value accrues on a per use per year basis.

The incremental cost of PKI enabling additional applications is very low once a PKI infrastructure is in place in an organization. Therefore, dramatic increases in ROI can be achieved.

For example, for an organization such as SKB bank with around 1000 employees and 3500 corporate customers the ROI would be 588.750 euro per year. This estimated ROI is as said, just for applications analyzed in this chapter. It could be much higher if would be implemented also in other bank processes. In addition, the value of added security and risk reduction, which are not included in this calculation, should not be forgotten.

# 6.0 CHAPTER V – DIGITAL SIGNATURE IMPLEMENTATION STEPS

Implementing digital signature in database applications can be a difficult task if the project team is not prepared. In this chapter, some steps are outlined that reduce the risk of failure and cost overruns. This scenario assumes that a public key infrastructure (PKI) environment already exists and the users are in possession of their digital certificates.

**Step 1: Planning the Effort**

All well managed and successful projects begin with well-planned effort. First, the selection of competent project leader has to be made. This project will probably be the first of its kind for an organization and it uses new technology that the project team will probably have little or no experience with. Putting a strong project leader at the helm is crucial. The project leader needs to be technically competent to anticipate and provide leadership in resolving technical issues as they arise and, because there are likely to be many different groups involved, the leader needs to be a good communicator who fosters good working relationships with other teams.

Then a qualified team has to be assembled. The project team should consist of business analysts that have extensive knowledge of the business processes and approval points in the processes. Project team should consist of software engineers that are experienced with the design and development of the application software. Further a team should consist of data modellers or data architects that are familiar with the physical database architecture. Also software engineers that are familiar with organization public key infrastructure, cryptographic toolkits, and middle-ware products that will be used should be found. If this is the first implementation of digital signature technology, finding personnel experienced with the cryptographic toolkits and middleware products is very hard. In this case hiring an outside consultant who has experience is a good choice. The consultant can help train the staff to be self-sufficient also for future implementations.

Then a comprehensive project plan should be developed. A project that clearly defines the scope, anticipated schedule, cost, and resources required for each detail task will reduce the risk of cost overruns and unexpected schedule delays. Project manager should be realistic when defining the schedule. If a digital signature is added to an existing application, ample time to make modifications to each software module that affects data values of any data items used to verify or create digital signature, should be allowed. To ensure ample time is allocated, every software configuration

item requiring any type of coding change should be identified on the project schedule. It should be known in advance how the progress report will be tracked. Digital signature implementation does not come without costs and since there is new technology involved it is reasonable to expect that this project will have its fair share of visibility from all of the stakeholders. To minimize the impact of this visibility, it should be planned in advance how the project will be tracked and reported. Reporting times, methods and thresholds for deviations have to be established and then requests for information other than what is regularly reported managed.

**Step 2: Analyzing the application to identify where digital signature is needed**
A complete list of the business transactions the application processes has to be developed. A complete list of the business transactions will help facilitate the identification of all the digital signature that will be needed for the application. A process flow of the transaction lifecycle is also useful.

A list of significant data items for each business transaction should be identified. For each of the business transactions the significant data items should be identified. These data items will become the basis for selecting what fields to be used in each of the digital signatures.

Then a list of approval points for each transaction should be developed. Approval points are the points in each business transaction's lifecycle where someone approves the data before the next step in the lifecycle occurs. Approval points are used to identify the places in the application that will have to be modified to do a digital signature verification and/or creation.

The physical data schema for each of the significant data items in each business transaction should be analyzed. Once the approval points have been identified in the business transaction lifecycle, they need to be identified in the physical data schema. Then the approval points where digital signatures are needed should be identified. After all the approval points have been identified in the business transaction lifecycle and the physical data schema, the points at which the signatures will actually be created and the data elements for each signature need to be identified. The appropriate level for the signature should be identified. By creating the signature at the higher level, fewer signatures have to be created and maintained.

Business transaction process flows identifying where all signature verification and signature creations will occur should be developed. If business transaction process flows exist already, they should be updated to reflect the points in the process where

the digital signatures will be verified and/or created. If the process flows do not exist, this is a great opportunity to add these needed documents to the organization system documentation repertoire. All stakeholders need to agree on these flows, as they will become the basis for building the digital signature templates and making the application modifications.

**Step 3: Creating the digital signature templates**

A signature template identifies the location (table and columns) of the data in the database. It also identifies the data types, primary keys, and relationships of the data being signed and verified. If organization middleware product supports using digital signature templates, there will be tools available to create these. If organization middleware does not support these, we may need to contract out or develop some API's in-house to support the templates. If it is decided to develop these templates in house, project manager has to be sure that he has experienced cryptographic software engineers on his staff.

A template name and description has to be made. Each digital signature template is identified with a name and a description. Then the columns, tables and data format for the data elements in the digital signature template have to be specified.

The template needs to identify each significant data item to be used in creating and verifying signatures. In addition, the data format needs to be specified. This is very important because the format of the data must be the same when it is signed and verified.

Then the primary keys and the relationships between the tables have to be designated. Usually, the API's that perform the actual signature creations and verifications are independent of the application but must operate on the application with some application knowledge because the data items that are used in the digital signature will often times come from multiple tables. When the data for a signature comes from multiple tables, the relationships between the tables and the primary key values to retrieve specific rows from the tables must be defined.

Then a version number to the template has to be assigned. When signatures are created, the version of the template is included in the signature so the correct template can be used for future digital signature verifications. This is important because signature templates need to be revised when business requirements change that affect the data items used in the signatures. If there is not this capability, every time a database change is made that affects the data items used in the signatures, all

the records affected by the signatures must be resigned. When they are resigned a risk losing the non-repudiation of the data emerge. The signature has the attribute of non-repudiation if it is protected against a successful dispute of its origin, submission, delivery, or content. In other words, the origin of the data and that it has not been tampered with, can be proven.

A security level to the template has to be assigned. Security levels are associated with smartcard or software certificates. Associating a minimum security level with a digital signature template allows users with a certificate that meets or exceeds the minimum security level to sign data using the template. Users attempting to sign data with a certificate that does not meet the minimum security level will not be successful.

These levels correspond to the amount of protection the software or the smartcard provides to the users certificate. It easier to steal a user's software certificate from a computer than the microprocessor based certificate on a smartcard.

**Step 4: Modifying the application**

All code modules that update or insert data into significant data item fields have to be identified. Every code module that affects the values of any of the significant data items to be used in the digital signature needs to be identified. Every time a value is changed a new signature will need to be created, and most of the time a signature verification will need to be done before the new signature is created. Specifics of how the code needs to be modified will be dependent on the used middleware product.

Then a decision upon a standard error handling routine for signature verification and creation failures should be made. When a signature fails to verify or a signature fails to create, the processing of business transaction should halt until the discrepancy is resolved. Handling digital signature errors are really no different than handling general application abort errors and if standard error handling routine is not used, this is an opportune time to introduce one. Using a standard method for handling errors will help ensure that all errors are handled the same way and the users are presented with the same error message.

Reusable code modules should be created where possible. Once all the code modules that must be modified are identified and the team members have a thorough understanding of the middleware API's and how they must be implemented and executed within the code, the impact to the application software should be minimized by creating reusable code modules for each of the signature verifications and

creations. Depending on the middleware product used, the API's might already facilitate reusability with little or no extension.

**Step 5: Testing strategies**

Thorough testing of the application software and its operation within the specific PKI environment is critical to the successful implementation of digital signatures. Support for the application becomes infinitely more difficult if software, hardware or communication errors are allowed into the production environment.

A comprehensive test plan has to be developed. There are many components to the PKI and interaction of the application software within that environment. When testing the application, all aspects of the environment must be considered. Participation from all involved teams (public key infrastructure, networking, communications, database administration, and others.) in the development of the test plan will help ensure that all aspects of the application within its operating environment will be tested.

Written test events that test the entire lifecycle of each business transaction have to be created. The complete lifecycle of each business transaction needs to be tested both positively and negatively. In other words, test for success, then test for failure. To test for failure, a tamper with the data is needed after it has been signed to create a verification failure. To test for a creation failure, scenarios need to be created where data is missing or is in valid for the signature.

**Step 6: Implementation**

Project manager has to be sure that the infrastructure environment is in place before going live. A public key infrastructure supports the broad use of public key based digital signatures and encryption and requires that certification authority services be in place and operational. Often times, PKI requires that multiple certification authorities cooperate to satisfy the requirements of the user environment. It is critical to the success that the certificate services are operational and available to the user community. Integrating digital signatures in organization applications will require that some of user base be issued certificates in order to process business transactions. If their certificates cannot be obtained or problems with them exist, they are unable to transact business. This can be detrimental to the underlying business that the application supports.

**Step 7: Providing Support**

Processes to resolve signature verification failures have to be in place. Digital signatures will fail for a number of reasons other than malicious tampering of the data. Failures other than those the digital signature is designed to detect are usually a result of software bugs in the application software. If digital signatures are implemented correctly, the business transaction will stop processing if a signature fails to verify but, if the data has not been tampered with, the team must be prepared to quickly remedy the situation in order to allow the process to continue. Because it must be ensured that the data has not been tampered with, defining the process for resolving signature failures requires careful consideration.

Non-repudiation of the data and data integrity is the backbone of digital signature. It is important to understand that when a digital signature is resigned in order to allow the business transaction to continue following a signature verification failure, non-repudiation is lost. However, data integrity will be maintained if a thorough investigation is conducted to determine the reason for the failure and a conscious decision is made by authorized agents of the data to resign the transaction. The ability to resign data has to be restricted. The ability to resign data should be limited to a single data security officer and his backup. Users should not have the ability to resign data following a signature verification failure.

## 6.1 Summary

Digital signature implementation in existing or new database applications requires careful consideration of all the elements involved from the underlying public Key infrastructure to the physical data schema of the application's database to the application software and cryptographic modules used to create and verify the digital signatures. Integrating all of the elements can be a difficult task, but with the proper planning, tools and controls in place, it is achievable.

# 7.0 CONCLUSION

The major goal of this thesis was to present how organizations could benefit in various ways with use of the digital signature and its implementation in their every day business processes.

From all the facts put out in the fourth chapter of this thesis, I can conclude that digital signature is in fact a tool, which helps organizations to achieve competitive advantage. This is achieved with increased efficiency, improved decision time, eliminated paper work, improved transparency and increased safety. All those improvements lead the way to substantial cost reduction.

Research in this thesis showed that there are justifications for investing in public key infrastructure and digital signature implementation. Those justifications are supported by a practical case, which is calculated with before well presented methodology and quantitative financial analysis. In general, the benefits from public key infrastructure and digital signature enabled applications significantly outweigh the costs of its implementation.

Research in this paper showed that for an organization such as SKB bank with around 1000 employees and 3500 corporate customers the return on investment would be 588, 750 euros per year. However, this return on investment was calculated just for applications analyzed in this thesis. It could be much higher if implemented also in other bank processes. Moreover, the value of added security and risk reduction were not included in this calculation.

It is important to emphasize that use of digital signatures is not limited to certain types of businesses or just technology related products and services. Digital signatures can be applied to any facet of an organization's operations, including marketing, sales, purchasing, logistics, production, design and engineering. Organizations can use digital signatures for many functions, including as a means of a safe sales channel, for safely communicating with partners and clients, for safely connecting to back-end data systems, and for safely performing all other e-business transactions. Digital signatures provide the solution for many improvements in the business processes.

Digital signatures were first conceived of in 1976. Now 30 years later, wide-scale acceptance of public key infrastructure based enhanced security solutions includes

legislative support, with essentially all modern economies having existing legislation giving digital signatures legal recognition.

Organizations should move away from traditional, time-consuming paper processes to new and more innovative technologies to improve efficiency. Digital signatures can significantly benefit organizations by eliminating the last paper in the business cycle. They provide enhanced convenience for both the customer and the organization.

Transitions from paper-based to completely electronic business processes and from physical separation to Internet integration provides enormous cost savings, productivity benefits, and a competitive market advantage to organizations. Therefore, it is not a question of whether an organization will complete those transitions, but when.

## 8.0 BIBLIOGRAPHY


1. Adelman Sid: Measuring Data Warehouse – Return on Investment. Whitepaper, 2003.

2. Berčič Boštjan: Pravni akti e-poslovanja. Glas gospodarstva, August 2004.

3. Boshell Patrick: Smart cards could prove effective for electrical utilities. Electricity Today, Issue 8, 2004.

4. Bračun Franc: Varovanje elektronskih dokumentov. Sistemi za upravljanje z dokumenti, 1996.

5. Brazell Lorna: Electronic Signatures Law and Regulations. s.l. Thomson, Sweet & Maxwell, 2004.

6. Brink Derek: A Guide to Determining Return on Investment for E-Security. CCE Journal, Issue 6, March 2002.

7. Clen Stephen: Strategic Management of e-Business. s.l. John Wiley & Sons, 2004.

8. Deise V. Martin, Nowikow Conrad, King Patrick, Wright Amy, PricewaterhouseCoopers: Executive's Guide to E-Business: From Tactics to Strategy. s.l. Wiley, 2000.

9. Deitel M. Harvey, Deitel J. Paul: e-Business & e-Commerce for Managers. s.l. Prentice Hall, 2000.

10. Dumortier Jos, Kelm Stefan: The Legal and Market aspects of Electronic Signature . Study for the European Commision.

11. El Sawy A. Omar: Redesigning Enterprise Processes for E-Business. s.l. McGraw-Hill, 2000.

12. European Central Bank (EUCB): E-Payments in Europe – The Eurosystem’s perspective.Whitepaper, September 2002.

13. Feghhi Jalal, Williams Peter: Digital certificates: Applied Internet Security. s.l. Addison-Wesley Professional, 1998.

14. Fhield Christina: Gap Assessment of the Top Web Service Specifications. DePaul University, June 2004.

15. Fingar Peter, Kumar Harsha, Sharma Tarun: Enterprise E-Commerce. s.l. Meghan-Kiffer Press, 2004.

16. Ford Warwick, Baum S. Michael: Secure Electronic Commerce : Building the Infrastructure for Digital Signatures and Encryption. s.l. Prentice Hall, 1997.

17. Diedrich Frank: A law of the internet ? Attempts to Regulate Electronic Commerce. Journal of Information, Law & technology, 2000.

18. Garnacho R. Arturo: Electronic Signature at the Heart of Information Security Development. Upgrade, June 2004.

19. Grant L. Gail: Understanding Digital Signatures: Establishing Trust Over the Internet and Other Networks (CommerceNet). s.l. Computing Mcgraw-Hill, 1997.

20. Grantham Charles: The Future of Work: The Promise of the New Digital Work Society. s.l. McGraw-Hill Trade, 1999.

21. Hammond Ben: Digital Signatures. s.l. Osborne/McGraw-Hill, 2002.

22. Hoque Faisal, Orchard David: e-Enterprise: Business Models, Architecture, and Components (Breakthroughs in Application Development). s.l. Cambridge University Press, 2000.

23. Jakhel Žiga: Tudi e-dokumenti potrebujejo podpis : kako zagotovimo verodostojnost elektronskih dokumentov. Finance, Issue 61, 2002.

24. Jerman Blažič Aljoša: Informacijska varnost. Monitor, May 2004.

25. Jones A. Virginia: Sign On The Botted Cyber-Line - electronic signatures and the Electronic Signatures in Global and National Commerce Act. OfficeSolutions, September 2001.

26. King M. Christopher: Public key infrastructure : end-to-end Security. Business communications review, Issue 11, 1997.

27. Klasinc Peter Pavel: Elektronsko poslovanje, elektronski podpis in slovenska arhivska teorija in praksa. Sodobni arhivi, Issue 23, 2001.

28. Lientz P. Bennet, P. Rea Kathryn: Dynamic E-Business Implementation Management: How to Effectively Manage E-Business Implementation (E-Business Solutions). s.l. Academic Press, 2000.

29. Mauth Rainer: Digital signatures to power E-commerce. Byte, Issue 1, 1998.

30. McCormack P. Kevin, William C. Johnson: Business Process Orientatation: Gaining the E-Business Competitive Advantage. s.l. Saint Lucie Press, 2001.

31. McGovern Gerry, Norton Rob: Content Critical: Gaining Competitive Advantage through High-Quality Web Content. s.l. Financial Times Prentice Hall, 2001.

32. Melkote Gita, Y. Jayachandra: Future Prospect: Envisioning EBusiness in 2020. s.l. Tata Mcgraw Hill India, 2003.

33. Motty Alon: Digital Signatures in a Document Intensive Organization. White paper , July 2003.

34. Parag Shiralkar, Bindiganavale S. Vijayaraman: Digital Signature Application Development Trends in E-business. Journal of Electronic Commerce Research, 2003.

35. Patel Ahmed, Munoz L. Javier, Martinez Nadal: Electronic Signature as the Key to Security in the Information Society. Upgrade, June 2004.

36. Piper Fred, Blake-Wilson Simon, Nitchell John: Digital Signatures Security and Controls. s.l. Information Systems Audit and Control Foundation, 2000.

37. Ramon Ray: Technology Solutions for Growing Businesses. s.l. American Management Association, 2003.

38. Robinson Marcia, Tapscott Don, Kalakota Ravi: e-Business 2.0: Roadmap for Success. s.l. Addison-Wesley Professional, 2000.

39. RSA Security: VPN Security and return on Investment. Whitepaper, 2002.

40. Rundgren Anders: Usage of PKI in and between Organizations. January 2003.

41. Silič Marin, Perenič Gorazd: Electronic Commerce and Electronic Signature Act. Whitepaper, June 2000.

42. Stoklosa Janusz: Cryptography and electronic payment systems. Informatica, Issue 1, 1998.

43. Toplišek Janez: Elektronski podpis - usklajevanje tehnoloških in pravnih rešitev pri elektronskem poslovanju. Organizacija, Issue 5, 1996.

44. Toplišek Janez: Elektronski podpis: Dnevi slovenskih pravnikov, od 17. do 19.oktobra 1996 v Portorožu. Gospodarski vestnik, Issue 5/6, 1996.

45. Vrbica Senka: Elektronsko poslovanje in elektronski podpis. Delo + varnost, Issue 49, 2004.

46. Žužek Alenka, Dobnikar Aleš: Novosti na področju arhiviranja elektronsko podpisanih dokumentov. Tehnični in vsebinski problemi klasičnega in elektronskega arhiviranja, Issue 2, 2003.

## 9.0 SOURCES


1. American Bar Association: Digital Signature Guidelines – Tutorial
   [www.abanet.org/scitech/ec/isc/dsg-tutorial.html]

2. ArticSoft Web Site
   [www.articsoft.com/whitepapers/pki_intro.pdf]

3. Business 2.0 : Business News, Technology News, Innovation
   [www.business2.com/b2/]

4. Cysco Systems Inc.
   [www.cisco.com/application/pdf/en/us/guest/products/ps6664/c1650/cdccont_0900aecd80313df4.pdf]

5. Digital Futures Conference
   [www.digitalfutures.org.uk]

6. e-Business Watch
   [www.ebusiness-watch.org]

7. Ecommerce Guide
   [e-comm.webopedia.com]

8. Entrust Web Site
   [www.entrust.com]

9. InfoWorld Web Site
   [www.infoworld.com]

10. Zero-Knowledge Systems
    [www.freedom.net/]