Electronic Identification
Focus on bank services and security

Bachelor’s thesis within informatics
Author: Oskar Eriksson, Kristian Marie, Hans Olsberg
Tutor: Mats Apelkrans
Jönköping January, 2005
Electronic Identification
Focus on bank services and security

Filosofie kandidatuppsats inom Informatik
Författare: Oskar Eriksson, Kristian Marie, Hans Olsberg
Handledare: Mats Apelkrans
Framläggningsdatum: Januari, 2005
Bachelor’s thesis in Informatics

Title: Electronic identification – Focus on bank services and security
Author: Oskar Eriksson, Kristian Maric, Hans Olsberg
Tutor: Mats Apelkrans
Date: 2005-01-27
Subject terms: Electronic identification, security, Internet bank, Bank ID, PKI

Abstract
Over the last years the typical way of handling your private economy has dramatically changed. Today millions of bank customers use Internet to pay their bills. This is of course a great advantage for the customer but it could also be a great risk since the security on the Internet can be of varying standard. The purpose of this thesis is to investigate the currently used techniques for identification of Swedish Internet bank customers and what is important for the banks when adopting a new technique. Furthermore we also want to give the reader a view of what can be expected in the near future.

We used a qualitative approach when studying the selected Swedish banks in this thesis. We gathered our empirical findings from interviews through telephone and e-mail. The banks included in this thesis are Danske bank, Föreningssparbanken, Handelsbanken, Nordea, SEB and Skandiabanken.

In the theoretical part we have collected information about the different technologies used today by the Swedish banks online. Our main source has been the library at Jönköping University. We have collected information from both literature and Internet web pages. Since information quickly gets old, we have tried to only use sources no older than 4-5 years.

From our empirical findings we have found out that: When the banks introduce a new technique they follow the same criterias as other companies but with a greater focus on security. All banks also monitor the development of new and upcoming techniques. When the banks are looking for a new security technique, the most important criterias are: cost effective, easy to use, mobility and ready to use. The reasons behind are mainly economical, but ofcourse they prioritize security. Today banks are combining several techniques, among these are techinques like BankID, digital signing, cryptography and electronic devices, such as the Active Card issued by for example Föreningssparbanken. There is a common view that the infrastructure for smart cards does not exist and that it is to expensive to develop. However the banks realize its potential. Our respondents further believe that the biggest concern about using biometric is that these techniques are not fully developed and therefore do not have sufficient security to be implemented in banks. All persons we interviewed agreed that the products they use today will not be replaced in the near future.
Sammanfattning


Från våra empiriska resultat har vi fått fram att:

## Contents

1 **Introduction** ............................................................................................................. 1  
1.1 Background ............................................................................................................. 1  
1.2 Problem .................................................................................................................... 1  
1.3 Purpose ....................................................................................................................... 1  
1.4 Interested parties ....................................................................................................... 2  
1.5 Delimitation ............................................................................................................... 2  

2 **Method** ..................................................................................................................... 3  
2.1 Knowledge characterisation ..................................................................................... 3  
2.2 Methodology approach ............................................................................................. 3  
2.3 Research approach .................................................................................................... 4  
2.3.1 Secondary data ..................................................................................................... 4  
2.3.2 Primary data ......................................................................................................... 4  
2.4 Criticism towards the selected method .................................................................... 5  

3 **Theoretical framework** ............................................................................................ 6  
3.1 Identification and the security behind it ................................................................... 6  
3.1.1 Cryptography ........................................................................................................ 6  
3.1.2 Digital Signatures ................................................................................................. 7  
3.1.3 Digital Certificate ................................................................................................. 10  
3.1.4 Certification Authority ........................................................................................ 10  
3.1.5 SSL .................................................................................................................... 11  
3.1.6 SET ................................................................................................................... 11  
3.1.7 3-D Secure ......................................................................................................... 12  
3.1.8 Public Key Infrastructure .................................................................................... 13  
3.2 Smart cards .............................................................................................................. 14  
3.3 Electronic Identification ............................................................................................ 15  
3.3.1 How does E-legitimation work? ............................................................................ 15  
3.3.2 BankID ............................................................................................................... 15  
3.3.3 E-legitimation ....................................................................................................... 16  
3.4 Biometrics .................................................................................................................. 16  
3.4.1 Finger scan .......................................................................................................... 17  
3.4.2 Hand scan ............................................................................................................ 17  
3.4.3 Retina scan .......................................................................................................... 17  
3.4.4 Iris scan ............................................................................................................... 17  
3.4.5 Facial scan .......................................................................................................... 18  
3.4.6 Handwriting and Signature Verification ............................................................. 18  
3.4.7 Voice scan .......................................................................................................... 18  

4 **Empirical findings** .................................................................................................. 19  
4.1 Information about the banks ..................................................................................... 19  
4.1.1 Danske Bank......................................................................................................... 19  
4.1.2 FöreningsSparbanken .......................................................................................... 19  
4.1.3 Handelsbanken .................................................................................................... 20  
4.1.4 Nordea ................................................................................................................ 20  
4.1.5 SEB .................................................................................................................... 20  
4.1.6 Skandiabanken ..................................................................................................... 20  
4.2 The Interviews ......................................................................................................... 21
4.2.1 Why did you choose the solution you have today and how does it differ from other banks? ............................................. 21
4.2.2 What do you think are the negative aspects or limitations in your current solution? ............................................. 21
4.2.3 Which were the steps behind the implementation of your current technique and what criterias must be fulfilled? .... 22
4.2.4 How does your bank acquire new techniques, technologies? What techniques did you choose between? ........ 23
4.2.5 What is the future for Smart Cards? ................................. 24
4.2.6 What technique does your bank think will replace the techniques of today? Is biometrics an alternative? ............ 25
4.2.7 What kind of role do you think the bank will play in the future when it comes to electronic purchases? (Third part, 3dsecure, SET, BankID) .............................................................. 26
4.2.8 Do you have any demands or pressures from the other market actors to introduce new solutions? .................. 27

5 Analysis .................................................................................. 28

6 Concluding discussions .......................................................... 31
   6.1 Reflections ............................................................................... 32
   6.2 Acquired experience ............................................................... 32
   6.3 Suggestions for further research ............................................. 32

7 References ............................................................................ 33

Figures
Figure 3.1 A model showing a brief overview over the process of signing... 9
Figure 3.2 A model showing the signing process .................................. 10
Figure 3.3 A model showing the information flow according to 3-D Secure. 14

Charts
Chart 2.1 A table showing an overview of our sources ....................... 5
Chart 3.1 A conclusive overview of signing messages and encrypting data 11
Chart 5.1 A chart briefly summarizing the criterias ............................. 31

Appendix
Appendix 1 - Questions to the banks ............................................. 39
Appendix 2 - Data dictionary .......................................................... 41
1 Introduction

In this chapter, we want to give the reader an introduction to the subject and an overview of our research. First comes the background that motivates why we find the subject important and then we line up the problems which acts as a base for our further research.

1.1 Background

Our society grows at a rapid pace and our lives are getting more electronically and “online”. More companies complement their business to also include the Internet as a marketplace. Today, you can order products from all over the globe and find everything from spare parts for old cars to managing bank affairs. This demands more reliable security as more people discover the possibilities of the Internet.

According to a survey conducted by the Cybercom group (2003), the Swedish banks had in May 2003 all together over 4.5 million customers connected to their Internet services and ½ million new Internet bank customers. This shows that the Internet services provided by the Swedish banks continue to attract new customers.

In recent years, banks have discovered the use of Internet and now let their customers handle their economy from home, decreasing the load on their local offices. As people make their money transfers online, the security aspect is of big concern both for the customers and for the banks.

Today, there are several different technical solutions that can be used to identify a person over the Internet. Many companies, and certainly banks demand a high level of security around their IT-solutions. Therefore we will focus on the different identification tools and the security behind them. We will also look at tomorrow’s techniques when it comes to identification, such as biometrics where individual and physical characteristics are used. Finally, we will summarize our findings and see what we can expect to see in a near future.

1.2 Problem

We want to answer these main questions:

- What techniques are used today for identifying a person electronically and to ensure a high security?
- What do responsible professionals at the selected Swedish banks think about biometrics?
- What criterias are considered as the most important ones when a new technique is introduced?

1.3 Purpose

The purpose of this thesis is to investigate the currently used techniques for identification of Swedish Internet bank customers, the technology and criterias behind it and what we can expect in the near future when it comes to identification.
1.4 Interested parties
This report can be read by anyone who has an interest in this subject. We have tried to keep the language simple and easy to read and understandable as this thesis holds a more general, not too detailed view. We include a glossary that describes terms mentioned in this report. We have noticed that a majority of the thesis within the subject at the University of Jönköping are written in Swedish. To broaden the range of interested parties we have written our thesis in English.

1.5 Delimitation
We have only used major Swedish banks in our research, and the banks had to offer its customers some kind of Internet bank services. The banks included in our research are Danske Bank, Föreningssparbanken, Handelsbanken, Nordea, SEB, and Skandiabanken. We have decided to exclude the niche banks since they turn to specific customers like Ikanobanken to IKEA and ICAbanken to its ICA customers.
2 Method

The chapter discusses the approach of method, research approach selection of research method, criticism towards the selected method, and the design of the questionnaire.

2.1 Knowledge characterisation

To be able to measure how much our knowledge is worth, we must categorise the knowledge we attempt to produce. It is also important to know when you choose methodology. There are a few different categories of knowledge (Goldkuhl, 1998). We will only describe the categories that we intend to use in this thesis.

- **Categorisation knowledge** - To define and explain different terms used in our theoretical framework we need categorisation knowledge. This is the most basic form of knowledge and all the other forms are linked to it (Goldkuhl, 1998).

- **Predictive knowledge** - We also produced predicative knowledge, which is a type of knowledge that is used to describe a possible future scenario. The identification of future identification techniques can be categorized as predictive knowledge (Goldkuhl, 1998).

- **Descriptive knowledge** - Describes what something is, what different phenomenon means and how it should be understood. You do this by describing the attributes of a phenomenon and studying descriptions of it. Descriptive knowledge was produced in the process of reading the literature (Goldkuhl, 1998).

2.2 Methodology approach

Basically there are two different methods to be used when you are going to do an empirical study. You can either choose to use a qualitative or a quantitative method and there are some fundamental differences between the two, which can lead to various results in the end.

The qualitative approach is the most commonly used to get a deeper understanding of the subject and to get more details (Holme & Solvang, 1991). The techniques you use are most often interviews. The information you then get is not possible to present with figures and it is not possible to use some kind of statistical method. According to Repstad (1999), a qualitative study emphasises the close relationship between the researcher and the objects that are being studied. Another hallmark of the qualitative approach is the flexibility that is possible for the researcher. You have more space for changes in the research.

The quantitative approach produces figures and these figures can then be used to draw conclusions about a specific phenomenon. In other words: only investigating a few objects can lead to general knowledge. The most popular technique is question pools (Lundahl & Skärvad, 1999).

We have chosen the qualitative approach in our thesis. The different kinds of information we received from the banks were not the kind of information that was possible to measure with figures and graphs.
Method

2.3 Research approach
We mainly used two methods to base our research on:

- Interviews via telephone (and where it was not possible, via mail)
- Literature, secondary data

By interviewing certain key-persons in banks, we could gather facts and a close-to-reality-view that showed us the possibilities of these technologies. In this way, we were able to look into the banks opinion and their plans in the subject matter. We also looked into earlier research and draw conclusions from there.

2.3.1 Secondary data
Much of the information was collected from secondary data. This information was gathered from printed literature and websites. We have tried to only use newer information, meaning websites and books that are no older than 4-5 years, with some exceptions. This is a precaution to be up-to-date with new and current information. Behind a security technique it is commonly a company or an organisation, so the information found on their websites only reflects the positive sides and therefore we have complemented our secondary data with primary data.

2.3.2 Primary data
The primary data was collected by us through interviews with key-persons in the banks. However, in two cases it was not possible to do this due to the banks’ security policy. We quickly found out that the persons who answered our questions were well informed about the techniques mentioned in this thesis. They gave us feedback and also some negative aspects on the techniques.

According to Lundahl and Skärvid (1999), an interview can be divided into two subgroups, standardized and non-standardized interviews. The non-standardized interview can also be divided into structured and unstructured. In this thesis, we will not explain the techniques that we chose not to use, but briefly explain the reasons why we picked the one we did.

We wanted the interview more to be a conversation but with some main questions to start from. This because we felt that this way could give us more information. The questions have been numbered but sometimes the conversation has brought us away from our schedule. We later came back to those questions that were left out. This behaviour is more of the non-standardized way. We have been looking for information more than values and attitudes which points at the structured interview. The structured way is also to prefer when doing an interview via telephone (Lundahl & Skärvid, 1999).

The interviews were primary conducted via telephone due to the physical distances. Because it is hard to record telephone calls on a regular telephone, we decided to use a speaker telephone. This way, all in the group were able to participate and the telephone interview became more like a meeting. As one person were the “leader” of the interview and asked the main questions, the other two in the group made notes. As a complement to this, we also recorded the interview with a cassette recorder, which then could be used to clear out any misunderstandings we may have.
Method

We tried to get telephone interviews with all the contact persons on the different banks, but as we suspected, there were difficulties making contact with some of the persons. The next step was to e-mail the questions we had as a base for our telephone interviews to the contact persons we were not able to reach. As this would affect our empirical findings in a negative way, we discussed that it was better to get a little information than no information at all. A telephone interview is preferred as the information becomes more detailed and you are able to follow up with other relevant questions that emerge during the interview.

The positive side with e-mail-interview is that respondent does not have to answer the question at the same time as the questions are asked and that makes it more flexible. But the negative side is that an e-mail-interview lacks the spontaneity and discussion that enhances a personal meeting. We tried to make our questions as clear as possible to avoid misunderstandings and misinterpretations.

<table>
<thead>
<tr>
<th>Bank</th>
<th>Contact person</th>
<th>Form of interview</th>
</tr>
</thead>
<tbody>
<tr>
<td>Danske bank</td>
<td>Hans Petersson, security manager</td>
<td>Telephone</td>
</tr>
<tr>
<td>SEB</td>
<td>Stefan Söderberg, security manager</td>
<td>Telephone</td>
</tr>
<tr>
<td>Föreningssparbanken</td>
<td>Göran Zebhär, security manager</td>
<td>Telephone</td>
</tr>
<tr>
<td>Handelsbanken</td>
<td>Ralf Bjerström, product development</td>
<td>E-mail</td>
</tr>
<tr>
<td>Nordea</td>
<td>Rickard Lindell, product manager</td>
<td>Telephone</td>
</tr>
<tr>
<td>Skandiabanken</td>
<td>Stefan Johansson, security manager</td>
<td>E-mail</td>
</tr>
</tbody>
</table>

Chart 2-1 A chart showing an overview of our sources.

2.4 Criticism towards the selected method

We used interviews as our primary source of information. As there were some physical distances between us and the persons interviewed, we were forced to make interviews through a telephone and send out a questionnaire via e-mail. Doing interviews under these circumstances, we felt some limitations due to the interviewing method. A personal meeting would have enriched our interviews and given us more information and also could some misunderstandings have been cleared out. Further, some banks insisted on answering the questions by e-mail, making it hard for us to follow up the questions. We do not know how this would have affected our findings, but we think that we could have had more information and opinions from the banks. It should be pointed out that this has not lead to any critical errors in our empirical findings, but as mentioned, a personal meeting would have been more appreciated.
3 Theoretical framework

This chapter will describe the different techniques used today and also techniques that exist but have not been fully accepted. We will divide the techniques by first describing the most fundamental and used techniques, and then describe the newer techniques.

A part of the information was collected from interviews with certain key-persons in the banks. The more detailed and technical information was gathered from literature and from the respective manufacturers’ websites. We have also read and collected data from earlier reports that tangents our area of research. However, we have had in mind that some of the earlier essays are written around year 2000 and as the IT world is changing at a fast pace, especially the different techniques, we therefore believe that earlier literature is some what out-of-date.

3.1 Identification and the security behind it

3.1.1 Cryptography

The increased numbers of viruses, denial of service attacks, digital identity thefts, online theft of credit card numbers and penetration of online electronic banking will keep giving the public an insecure attitude towards the safety. The solution to this problem may lie in cryptography, which is the science of coding messages so that unauthorized persons cannot decipher them. The technique that from the beginning was used by the military has proved to be useful even for the civilians. As a result of this technology, credit card numbers, contracts, digital signatures and other vital information can flow on the Internet as an unreadable code instead of its original form. The modern cryptography use electronic keys, which allows the authorized to decipher the code and reconstruct the original message.

Cryptography is divided into two standards according to Guttman (2003):

- Symmetric
- Asymmetric

The first cryptography standard is the symmetric standard and it uses a single key for coding and decoding a message. This key has to be known to both parties. The disadvantage of the symmetric variant is that the key has to be secret. The key has to be exchanged in the transaction between the parties. If a party wants to communicate with 100 other parties then the key has to be transferred to all of them and in open networks such as the Internet, this can cause problems since an unauthorized third party can gain access of the key. This makes it hard to prove that the right person on the other end of the transaction is authorized. DES (data encryption standard) algorithm is the most commonly used symmetric cryptography (Zhang & Wang, 2003).

The solution to this problem is the asymmetric standard, which uses two different keys, one public and one private. This means that both keys can code the message but only one key can decode it. When communicating with 100 different parties a public key can be distributed to all of them and they can code a message but only one party can decode the message with the private key. The most commonly used cryptography in asymmetric cryptography is RSA. Figure 3.3 shows a table of keys used in asymmetric cryptography (Guttman, 2003).
3.1.1 Hash functions

A hash function is a calculating algorithm. Out of a document is a hash value created from a hash algorithm. This value is then stored in a secure place where it cannot be changed. To be certain that the document has not been changed, the value is calculated once more and is then compared with the original value. If the values are the same, you can be certain that the document has not been changed. If as much as one binary figure is changed then a different hash value is obtained. According to Zhang and Wang (2003), hash functions typically produce hash values of 128 or more bits. Hash functions could be used together with asymmetric cryptography to create a digital signature (Nakov, 2003).

3.1.2 Digital Signatures

The techniques used today within cryptography have developed far beyond the terms of just encryption and decryption. An important development within cryptography is the upcoming law of digital signatures, which were constituted by the US Congress in 2000. A digital signature binds a document to whoever has a certain key. The digital signature is much similar to the written signature but to the fact that its built up by encrypted data which is created with a private key and can only be verified by a public key. This release companies from the requirements of keeping paper records and the requirement of written signatures. It also enables companies to expand their range of activities online such as contracting where previously a written signature was required and issuing paper disclosures (Guttmann, 2003).

Digital signatures use the Public Key Cryptography. The Public Key Cryptography creates the digital signature through a two-step encryption and decryption process that encodes an electronic transmission by embedded algorithms in software or hardware. A digital signature allows a party to send a secure message over an open network (Bloemers, 2004).

Digital signatures can also be used as Certifying Authorities (CAs) for certifying that the keys belong to a certain person. A CA is a third part that has the task to control the involved parties’ identity and store the personal data. The CA then creates their public keys. A CA can, according to Halvarsson and Morin (2000), be a part in a company or an organization or an external organization. CA is discussed in section 3.1.4.

3.1.2.1 Public Key Cryptography

The Public key cryptography uses an asymmetric cryptography. This means that digital signatures involve the use of two encrypted keys. The private key is secret, and used only by the sender to sign documents. The private key is usually installed on the sender’s computer. The public key is available to anyone who wants to confirm the documents signed by the sender. The public key reads the digital signature created by the private key and verifies the validity of the documents created with it.

Digital signatures can be used by anyone by signing up with a certification authority (CA) and obtaining a digital signature certificate. This certificate is a computer-based record that identifies the subscriber and it contains the public key as well as a digital signature by the certification authority.

The private key is protected on the sender’s computer by an authorization code. If someone other than the authorized sender knows the authorization code and also has access to the sender’s computer, the private key is compromised and the certifying authority can be notified immediately to revoke the digital signature certificate (Bloemers, 2004).
3.1.2.2 The process of signing messages

According to Nakov (2003), the process of signing messages is:

1. Sender calculates message digest.

In the first step of the process, a hash-value (message digest) of the message is calculated by using a cryptography hashing algorithm (for example, some standards: MD2, MD4, MD5, SHA1).

2. Calculate the digital signature.

In the second step of digitally signing a message, the information obtained in the first hash-value is encrypted by using the private key of the person who signs the message as well as an encrypted hash-value, then a digital signature is obtained.

![Diagram of the process of signing messages]

Figure 3-1 A model showing a brief overview over the process of signing.

The process of digital signature verification is purposed to ascertain if the private key that corresponds to a public key has signed a given message. If we have to check whether a person has signed a message, we need to obtain the persons public key like from a floppy disk or by digital certificates through Public Key Infrastructure. If we don’t have a secure way to obtain the real public key from a person, it is not possible to check whether the given message is really signed by the right person.

The verification of a digital signature is performed in three steps:

1. Calculate the Current Hash-Value

In the first step, a hash-value of the signed message is calculated. In this calculation, the same hashing algorithm is used as in the signing process. The obtained hash-value is called the current hash-value since it is calculated from the current state of the message.

2. Calculate the Original Hash-Value

In the next step of the digital signature verification process, the digital signature is decrypted with the same encryption algorithm that was used during the signing process. The decryption is done by the public key that corresponds to the private key used during the signing of the message. As a result, we obtain the original hash-value that was calculated from the original message during the first step of the signing process.

3. Compare the Current and the Original Hash-Values

In the final step, the current hash-value obtained in the first step is compared with the original hash-value obtained in the second step. If the two values are identical, the verification is successful and the message has been signed with the private key that corresponds to
the public key used in the verification process. If the two values are unequal it means that the digital signature is invalid and the verification is unsuccessful (Nakov, 2003).

![Diagram](image)

Figure 3-2 A model showing the signing process.

<table>
<thead>
<tr>
<th>Key Function</th>
<th>Key type</th>
<th>Whose Key Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encrypt data for recipient</td>
<td>Public Key</td>
<td>Receiver</td>
</tr>
<tr>
<td>Sign data</td>
<td>Private Key</td>
<td>Sender</td>
</tr>
<tr>
<td>Decrypt data received</td>
<td>Private Key</td>
<td>Receiver</td>
</tr>
<tr>
<td>Verify a signature</td>
<td>Public key</td>
<td>Sender</td>
</tr>
</tbody>
</table>

Chart 3-1 A conclusive overview of signing messages and encrypting data.

**3.1.2.3 The Security**

The digital signature as well as the written signature is unique to the sender. The digital signature prevents unauthorized use of the document by the user code. Therefore, the recipient of a message can forward the message to a third party (CA) and be able to prove that the document was not changed or manipulated after it was sent.

A digital signature is according to Bloemers (2004), safer than a handwritten signature in two aspects.

- Digital signatures cannot be forged.
- Handwritten signatures can be changed without anyone knowing that changes in the text of a document have been made.
3.1.3 Digital Certificate

A digital certificate is an electronic document, which identifies people and resources over a network such as the Internet. The CA issues these certificates. The CA’s role is to validate the certificate holders’ identity and to sign the certificate so it cannot be tampered or forged. When the CA signs the certificate, the holder can present its identity securely to other people and networks.

A digital certificate typically includes the following information from the owner and the CA:

- Holders name and other information that uniquely identifies the holder such as the URL of the Web server using the certificate or the holders e-mail address.
- The holders’ public key. This key can be used to encrypt sensitive information for the certificate holder.
- Name of the Certification Authority.
- A serial number.
- Time of the certificates validity period.

When creating a certificate, the certificate is signed by the CA. This signature is similar to a tamper-detection seal on a bottle of pills and is therefore easy to detect whether it has been tampered with or not. Digital signatures use the Public Key Infrastructure.

- Web server certificates

This is a certificate that identifies the identity of a Web page to the visitor. When the visitor wants to send confidential information to a Web server it first has to access the digital certificate on the Web server. The digital certificate on the Web server contains the public key and is used to verify the identity of the Web server and encrypt the information. Since the Web server is the only one who can access its private key, only the server can decrypt the information. This is how the information can stay confidential on the Internet.

- CA certificates

CA certificates is a certificate that identifies a Certification Authority. The CA certificate is similar to other digital certificates except that it is self-signed. This means that the CA is used to authenticate the Web server certificate. When accessing a Web page the browser uses the CA certificate to determine whether to trust the Web server certificate. If the certificate is trusted a Secure Socket Layer (SSL) will be trusted. If not trusted no connection will be established. In the popular Web browsers like Firefox and Explorer, CA certificates are already installed (Robinsson, 2001).

3.1.4 Certification Authority

As mentioned in section 3.1.2, a certification authority (CA) is a third part that controls the involved parties in a transaction. The CA controls the parties’ identity and stores the personal data and creates their public keys. Further, similar to Halvarsson and Morin’s (2000) definition of a CA, Li and Wang (2003), defines a CA as an entity that validates identities and issue certificates. It can also be an independently third party as well as an organisation
like the Microsoft Certificate server which runs their own certificate-issuing server software.

A certificate that has been signed by a CA binds a particular public key to the name of the entity that the certificate identifies. Only the public key certified by the certificate will match with the private key possessed by the one who is identified by the certificate. In other words, only an authorized person who has been given the private key can complete a transaction (Li & Wang, 2003).

3.1.5 SSL

Secure Socket Layer is a connection-based protocol developed by RSA and is today embedded in all browsers. SSL is used to ensure a secure transaction between server and client by encrypting the information with a private key. To activate SSL, a digital certificate is needed, issued by a certification authority and approved by your browser from a list of trusted CAs which facilitates the public key exchange necessary for establishing an SSL connection. SSL also allows authentication of both server and client to confirm their identities.

The SSL also supports applications for more sophisticated transactions such as SET (Secure Electronic Transactions) were greater encryption technology is needed (Guttmann, 2003).

According to Robinsson (2001), certificates are used in an SSL transaction in the following way:

- When a person visits a web page secured with SSL, the browser sends a message to the Web server saying that a secure session is needed.
- The Web server responds by sending a certificate to the person that contains the public key.
- The persons browser will now verify that the certificate is valid, signed by a CA whose certificate is in the browsers database and also that the CA certificate has not expired.
- If the certificates are valid the person’s browser will generate a one-time, unique “session” key and encrypt it with the public key. The browser will then send the encrypted key to the server so that both client and server have a copy.
- The server will decrypt the message by using the private key and recover the “session” key.

Now the person communicating with the web page can be sure of that the web page is the one it claims to be and that only the persons browser and the web server has a copy of the session key (Robinsson, 2001).

3.1.6 SET

SET (Secure Electronic Transaction) is a standard that describes how to encrypt financial data. The founders behind this standard are MasterCard, VISA, Microsoft and Netscape. The technology is embedded in Microsoft’s web browsers and is not visible for the user.
This technology is today obsolete and is replaced by 3D-secure. Therefore, we will only briefly show a typical SET-scenario.

The scenario involves a bank, a third party and a customer. If the customer has a VISA bank account, the customer receives a digital certificate from the bank that includes a public key. This public key has been validated by the bank to assure that it is genuine.

The third party (an online store) also receives a certificate from the bank with a public key, included is the online store’s public key and the banks. When the customer then places an order from the online store, the customer's web browser automatically check if the online store’s certificate is valid. The browser then sends the order information to the online store, encrypted with the online store’s public key and the payment information encrypted with the bank’s public key (the payment information can therefore not be read by the online store). After that, the online store is checking the validity of the customer by looking at the customer's certificate. If everything is valid, the online store forwards the order along with the online store’s certificate. The bank makes a final verification on the order and the online store’s certificate. The bank then digitally signs and sends an authorization to the online store, which can proceed with the order (Whatis, 2004).

3.1.7 3-D Secure

3-D Secure is a protocol similar to SET. 3-D Secure is developed by VISA. The major difference between 3-D Secure and SET is that the actors in 3-D Secure have different roles when it comes to identifying the cardholder and the merchant. In 3-D Secure, it is up to VISA to identify and guarantee that the user claiming to be the owner of the card really is the owner (Comtrust, 2004).

The protocol is easier to use and can be used on different platforms such as a PC and a mobile phone (Comtrust, 2004).
3.1.8 **Public Key Infrastructure**

Public Key Infrastructure is according to Li and Wang (2003), the combination of software, encryption technologies and services that enables enterprises to protect the security of their communication and business transactions on the Internet. PKI integrates certification authorities, public key cryptography and digital certificates into a security architecture. The public key infrastructure provides several security services such as user authentication, confidentiality and integrity.

A PKI infrastructure is expected to offer the following benefits to its users: (ArticSoft, 2004).

- Certainty of the quality of information sent and received electronically
- Certainty of the source and destination of that information
- Assurance of the time and timing of that information
- Certainty of the privacy
- Assurance that the information may be used as evidence in a court

PKI uses the public key cryptography, which is mentioned in section 3.1.2.1 where a pair of cryptography keys is used to verify the identity of the sender and to ensure encryption (ArticSoft, 2004).

Further Li and Wang (2003), offer these following benefits for securing information by using PKI:

- Authenticate identity

Digital certificates are issued in order to allow users such as organisation, individuals or web site operators to communicate and to ensure the identity of each participant in a transaction.

- Verify integrity

The digital certificate ensures that the document has not been changed during the transaction by “signing it”.

- Ensure privacy

The digital certificate protects the information (document) from interception.

- Authorize access

The digital certificate ensures secure access.

- Authorize transactions
With the use of PKI the enterprise or organisation can control the access privileges for certain online transactions.

- Support for non-repudiation

The digital certificate validates the users’ identity and makes it practically impossible to repudiate the digitally “signed” transaction.

To explain it in its most simple way PKI is a system for publishing the public key values used in the public key cryptography (Li & Wang, 2003).

### 3.2 Smart cards

Smart cards are made of plastic and include an integrated circuit. A smart card is visually like a normal credit card. Instead of storing information on a traditional magnetic stripe, the information is programmed on the internal microchip. It also includes a random access memory, read only memory and electronically erasable programmable read-only memory. In this way, a smart card can contain far more information than a card with a traditional magnetic stripe. There are two ways of communication with smart cards; the most common way is a contact-based communication where a reader is connected to a computer. In the second case a wireless communication is used via, for example, a radio transmission (Knorr, Kou & Poon, 2003).

Today smart cards are used for prepaid phone cards, mobile communication and for banking purposes. In the area of identification, smart cards have potential: governments in Malaysia, Hong Kong and Singapore are interested in using smart cards in a national ID solution. A smart card can be used to store personal information, healthcare information and almost every kind of information. The key is the encryption. If someone loses his or her smart card, no one else can use the information (Knorr, Kou & Poon, 2003).

However the breakthrough of smart cards has not reached its expected peak and according to Weisman (2004), there are four important reasons why:

- The consumers do not need it. There are plenty of well-understood payment options such as cash, checks, debit cards, and credit cards.
- The infrastructure does not exist. The retailers has already spent lots of money on outfitting checkout lanes with credit card readers and pin pads and these readers do not support smart cards.
- The security does not require it. With the advanced telecommunications infrastructure in the U.S. and Europe almost all transactions can be quickly and cheaply made online.
- The business case remains a mystery. Who will pay the extra freight of the chip on the card? And how will banks make money issuing and routing transactions? MasterCard and Visa have a history of duelling over interchange for debit and credit cards.
3.3 Electronic Identification

E-legitimation is an electronic identification tool that is much similar to a normal or physical ID. E-legitimation can be used for electronic identification towards governments, corporations and organisations. The authenticity of the E-legitimation is controlled by the issuer who makes sure that the E-legitimation is valid and not blocked.

Different names have been used for the functionality of establishing secure e-services. The Swedish Tax Agency (Skatteverket) and other governments have decided to use the term e-legitimation for this functionality instead of the previous term Electronic ID Identification, or certificates.

When an E-legitimation has been acquired it can be used as identification for various things on the Internet and both governments and corporations are continuously creating more services where E-legitimation can be used. The e-legitimation can for example be used for identification and signing company matters to the Tax agency (Skatteverket) or The Swedish Companies Registration Office (Bolagsverket) or various bank services (Skatteverket, 2004).

The Samset-project is an effort from the Swedish government and has been commissioned to lead the development of electronic legitimation (E-legitimation) and electronic signatures within the central government administration. The project also handles the economical, technical and legal aspects such as how people, companies and organisations should obtain the legitimation as well as how it should be financed. The commission has been performed in collaboration with Skatteverket, Riksförsäkringsverket, Patent- och Registreringsverket and Statskontoret. At the moment there are three different types of E-legitimation: BankID, E-legitimation used by SEB and E-legitimation used by Nordea and Posten (Skatteverket, 2004).

3.3.1 How does E-legitimation work?

When you have an E-legitimation/BankID you can go to a company’s website and identify yourself by using the corresponding password. The company now knows who you are. When this is done the requested data can be delivered. During the process of identifying yourself, the company will require a confirmation that your identity is valid. This is done by the bank, which checks the validity and sends back a confirmation to the company and by doing that, the bank will confirm the validity.

If a signature is required on the matter the E-legitimation can be used again with the corresponding password. Then the agreement is binding (BankID, 2004).

3.3.2 BankID

BankID is a standard, which is accepted by most big Swedish banks. It makes it possible for companies and authorities to identify customers and signing documents. BankID is a third party solution, but it is based on the banks customer identification, which is then linked to the Internet banks.

The banks issue the certificates that companies and authorities need. They follow a specific template when they approve a certificate. The client software is called Crypto Based Transactions or CBT and it is developed by IBM. CBT is a JAVA application and therefore it is not necessary to install it, which makes it much faster and easier to use.
To reach as high security level as possible, every company and authority using BankID is forced to use the service BankID Control Server. This software checks that the certificate is valid. The following Swedish banks use BankID:

- Handelsbanken
- Föreningssparbanken
- Ikanobanken
- Skandiabanken
- Danske Bank
- Lånsförsäkringar Bank
- Sparbanken Finn
- Sparbanken Gripens

(BankID, 2004).

### 3.3.3 E-legitimation

E-legitimation as well as BankID makes it possible for companies and authorities to identify customers and to make it possible to sign documents. E-legitimation is a personal ID and is used for identification on the Internet. Skandinaviska Enskilda Banken (SEB) is the only bank that uses this E-legitimation and it was developed in cooperation with Telia. Nordea and The Swedish Post however uses the same term for their E-legitimation but to be able to use the Nordea and The Swedish Post E-legitimation you will need to install a security program called Smart Trust Personal (Försäkringskassan, 2004).

### 3.4 Biometrics

Biometrics is the term used to describe the automatic identification based on a person's physiological or behavioural characteristics. The advance in technology is according to Zhang and Yu (2003), always inspired by the practical applications and the emergence of automatic biometrics technology and is rooted in the requirements for real-world security applications. Even though biometric technology is still at the development stage it has been implemented in various applications. The most used method of today to access computers and data are passwords and PIN numbers and since they are easy to use they provide according to Zhang and Yu (2003), a weak proof of identity. The major biometric technologies used today all share the same four-step process: sample capture, feature extraction, template comparison and matching. The major biometric techniques used today are:

- Finger scan
- Hand scan
- Retina scan
- Iris scan
Biometric is the most secure and convenient identification tool since it cannot be borrowed, stolen or forgotten and any kind of forge is practically impossible. In this chapter we will briefly cover these different biometric techniques (Zhang & Yu, 2003).

3.4.1 Finger scan

Finger scan technology is based on the distinctive characteristics of a human's fingerprint. When the fingerprint is scanned the features are extracted from the image and a template is created. Finger scan can be divided into two categories: Minutiae and Correlation technique. Fingerprint verification can be used for in-house systems in a controlled environment as well as secure online banking transactions. By implementing fingerprint authentication in combination with passwords and pin numbers it would make it more secure accessing corporate information. However the benefits of using the finger scan includes fraud protection, customer confidence and retention (Zhang & Yu, 2003). However there are some obstacles with finger scan and that is the inability to enrol some users. Certain ethnic and demographic groups have lower quality fingerprints and are thereby harder to enrol than others. Elderly populations, manual labours and some populations in Asia have an insufficient fingerprint (Nanavati, Thieme & Nanavati, 2002).

3.4.2 Hand scan

Hand scan uses the geometric shape of a person’s hand. Hand scan is relatively accurate but is not as accurate as finger, face or iris scans since the features of the hand are not very descriptive. The ergonomic design limits the usage by certain populations (Nanavati, Thieme & Nanavati, 2002). However, according to Zhang and Yu (2003), this technique can be combined with other techniques to identify a person.

3.4.3 Retina scan

Retina scan is said to be the most accurate and reliable technique along with Iris-scan. This technique is however hard to use since it requires a cooperative and patient and well trained user. When a person is being scanned it is required to situate the eye ½ inch from the device since rays go thorough the pupil into the retina and is then scanned were over 400 points on the retina are registered. Compared to fingerprint scan with 20-30 points registered the retina scan is far more accurate (Zhang & Yu, 2003). Another negative factor is that a special acquisition device is needed and population with weak sight may be unable to effectively use this scan (Nanavati, Thieme & Nanavati, 2002).

3.4.4 Iris scan

Iris technique uses the unique features of the human iris. When the iris is scanned the features are found in the coloured ring of tissue that surrounds the pupil. This technique does not require the user to situate the eye up close to the device such as in the case with retina scan and is thereby said to be less intrusive and challenging than the retina scan. The iris scan uses a camera lens to identify a user and is together with retina scan the most reliable
3.4.5 Facial scan

The facial scan technique uses as well as finger scan the unique form of the person. When using a facial scan, sections of the face are scanned such as the upper outlines of the eye sockets, the areas surrounding the cheekbones as well as the sides of the mouth. No images are stored but instead the templates that consist of numerical codes are stored and are usually not bigger then 1 kilobyte of data. This technique has recently gained a lot of interest from the casino industry were it enables a casino to store these templates in a database and then identify scam players (Zhang & Yu, 2003). However when using facial scans the user’s face must be lit evenly and not acquired from sharp horizontal or vertical angles. Further it is a problem when users are enrolled at one location and verified in another (Nanavati, Thieme & Nanavati, 2002).

3.4.6 Handwriting and Signature Verification

This technique identifies a person by analysing the way a signature is written. When the signature is written, the velocity, speed, pressure as well as the actual finished shape is analysed. The benefit of this technique is the fact that people are used to signatures as a mean to sign bank transactions and most people would se nothing unusual by extending this method into biometrics. Electronic signatures are gaining ground for retail and e-commerce. This technique includes installing electronic signature software (Zhang & Yu, 2003). People who do not sign their names in a consistent fashion may have difficulties with this technique due to the fact that it is a difference with signing onto an electronic board instead a signing on paper (Nanavati, Thieme & Nanavati, 2002).

3.4.7 Voice scan

A speaker recognition system can be divided into two groups: text-dependent and text-independent systems. In the text-dependent system a user has to use the same text during a training and recognition session. The text independent system however does not require a training session when recognizing. Both text-dependent and independent include feature extraction, similarity analysis and selection. Voice scan technique use coefficients in a predictive system and compare a voice sample by computing the regression between the coefficients. This technique can be used in ATMs or anti-theft systems for automobiles (Zhang & Yu, 2003). The ability of the voice scan is however reduced when using PC microphones in noisy offices or mobile phones with a low reception and further the template size (occupied memory) are larger then those of the other typical biometrics (Nanavati, Thieme & Nanavati, 2002).
4 Empirical findings

The empirical findings include presentations of the Banks, results from the mail questionnaire and the interviews with the selected Swedish banks. They are presented in alphabetic order.

4.1 Information about the banks

4.1.1 Danske Bank

Danske Bank is one of the leading banks in Scandinavia and has over 3 million customers in Denmark, Norway and Sweden as well as international and domestic corporations and institutions. Danske bank consists since 1997 of Bohushanken, Hallands Provincbank, Närkes Provincbank, Skånes Provincbank, Smålandsbanken, Sundsvallsbanken, Sörlmands Provincbank, Upplandsbanken, Värmlands Provincbank, Västmanlands Provincbank, Ålvsborgs Provincbank, Östgöta Enskilda Bank and Fokus Bank (Norway). Danske Bank has 46 offices and about 1200 employees.

Hembanken is the name of Danske Bank Internet service and offers the following solutions:

- Kodbox
- E-Safekey

Kodbox is an electronic device which creates a different pin number each time when logging on to Hembanken. Kodbox can also be used for identification when using the telephone service, Telebank Direkt.

E-Safekey is a software which installs a certificate on the computer the first time someone logs on to Hembanken. When communicating with the bank, a password in combination with the certificate is needed to ensure the identity of the user and communicate with the bank.

Hembanken uses 128 bit SSL (Danske bank, 2004).

4.1.2 FöreningsSparbanken

Föreningssparbanken was established in 1997 when Föreningsbanken and Sparbanken merged. Their common history reaches back from 1820 and Föreningssparbanken today is one of the biggest banks in the Nordic countries. They have somewhat over 15,000 employees and 9,000 of these are in Sweden.

According to their website, Föreningssparbanken has a total, with all the banks in the group, around six million private customers and about 2.6 million Internet customers in the Nordic countries.

Föreningssparbanken uses an Active Card solution similar to Danske bank’s Kodbox which generates codes when logging on to the Internet bank. Föreningssparbanken also uses soft certificates over 128 bit SSL (Föreningssparbanken, 2004).
4.1.3 Handelsbanken

Handelsbanken was founded in 1871. Today the bank has about 540 offices in the Nordic region and almost 9,000 employees. The Internet bank that has been in use since 1996 is serving approximately 500,000 customers.

Handelsbanken uses security software called Smart trust Personal. This software has a stronger version of the SSL than the standard version in your web browser. The use of personal certificates makes it possible to do digital signatures. The encryption used is a 128-bits encryption. A one-off password is received in your ordinary mail (Handelsbanken, 2004).

4.1.4 Nordea

Nordea is one of the leading financial corporations in Scandinavia and the Baltic region as well as a leading Internet bank with 3,7 million customers. Nordea has significant market shares on the Scandinavian market: 40 percent in Finland, 25 percent in Denmark, 20 percent in Sweden and 15 percent in Norway.

Nordea's Internet service is called Solo and makes it possible to log on to the bank by using a card or a code.

- Card

Only one code is necessary when using the card. However hardware with a smart card (e-legitimation) has to be connected to the computer and a software program has to be installed.

- Code

The customer gets a personal code and a card with one off codes. The personal code is always used when using the Internet or the telephone service. The “one time” codes are used as an extra identification (Nordea, 2004).

4.1.5 SEB

SEB is a north European bank group intended for companies, private customers and institutions. With four million customers, approximately 1,5 million are e-banking customers. The SEB Internet bank started up in 1996 and today customers can make all their bank businesses at the Internet bank office.

SEB uses a hard certificate in the login process. The “Digipass” is a security box, which gives you a code. This code is used when you login or to verify a transaction. Each code is unique and only used one time. All information is encrypted with SSL, 128bit (SEB, 2004).

4.1.6 Skandiabanken

Skandiabanken opened in 1994 and was at that time one of the first banks to only offer their services over the phone. Since then the bank has developed into a full service Internet bank and has been awarded best Internet bank in Privata affärer (2003) and best bank in Cybercomes during 2003. Skandiabanken has 500 employees in Sweden, Norway and Denmark.
The security when using the Internet service is built up by the four-digit pin number and the “one time” number that is sent to the costumer by sms or mail when logging on to the bank. A digital certificate with a key pair is used to ensure that the customer is communicating with the bank and vice versa. All data is encrypted by using SSL128 bit (Skandiabanken, 2004).

4.2 The Interviews

The interviews were originally conducted in Swedish and then translated to English.

4.2.1 Why did you choose the solution you have today and how does it differ from other banks.

Hans Petersson, security manager at Danske bank:

We did a “quick and dirty”, we went from a production model to a practical, functioning environment in just six weeks. We found that the Kodbox was the most suited for the task.

Göran Zebühr, security manager at Föreningsparbanken:

We went live in March 1997 and we found the Active Card as the best suited. We wanted to have a stand alone, mobile solution that does not tie you to a certain computer and it was the solution that needed least support and installation to work properly.

Ralf Bjerström, product development, Handelsbanken:

It was decided that we should use a PKI-based solution which among it abilities could sign and verify data from the user.

Rickard Lindell, product manager at Nordea:

We followed directions from EU and those later became adjusted to Swedish demands. Our solution is a good solution, it is mobile, easy administered, and demands low support.

Stefan Söderberg, security manager at SEB:

The product Digipass was out early, around 1997. It was the technique that was the most developed. This solution does not need any kind of installation which makes it mobile to use.

Stefan Johansson, security manager at Skandiabanken:

We think the technique we use is the most customer friendly, cost effective and it is a good technological solution and is therefore secure enough.

4.2.2 What do you think are the negative aspects or limitations in your current solution?

Hans Petersson, security manager at Danske bank:

The Kodbox has one advantage – it is insensitive to viruses and manipulation. Soft key on the other hand can be manipulated through trojans and other kinds of viruses.

Göran Zebühr, security manager at Föreningsparbanken:
We do not see any disadvantages right now, as we are using our solution both for identifying and signing. One point we could improve is that it only use eight digits, it would be easier and more pedagogical if it were able to show more digits, but we are satisfied at the moment.

**Ralf Bjerström, product development, Handelsbanken:**

The weaknesses that exist are more dependent on the software used on the workplace, like operating system and web-browser.

**Rickard Lindell, product manager at Nordea:**

We can not see any bad sides with our solution.

**Stefan Söderberg, security manager at SEB:**

The negative part is that the actual cost for the Digipass and the fact that we can not use it for digital signatures.

**Stefan Johansson, security manager at Skandiabanken:**

We are very pleased with our solution and we feel that other banks want do use the same solution as our bank do.

**4.2.3 Which were the steps behind the implementation of your current technique and what criterias must be fulfilled?**

**Hans Peterson, security manager at Danske bank:**

Many factors must be considered. You usually think much in an analogue way, but everything must be converted into a digital thinking. Also, costs are a big factor.

**Göran Zebhür, security manager at Föreningssparbanken:**

There are some bank politics and some questions for the management before a technique could be introduced.

**Ralf Bjerström, product development, Handelsbanken:**

The introduction of different security solutions is preceded by different processes like risk analysis and so on.

**Rickard Lindell, product manager at Nordea:**

Demands from authorities, these could be different between different countries. They could be demands, specifications. We also have some criterias like mobility, high security, low investments, low support and customer friendly.

**Stefan Söderberg, security manager at SEB:**

At our bank, we have a group called “Group Security” which lies on a concern level that must approve new proposals before they get implemented.

**Stefan Johansson, security manager at Skandiabanken:**

The most important is the security. Also factors like customer friendly and cost effectiveness are important.
4.2.4 How does your bank acquire new techniques, technologies?
What techniques did you choose between?

Hans Petersson, security manager at Danske bank:

This mission was given to Kryptomatic (IT consultant partner to Danske bank) in the beginning and at the moment there is no need to change anything since there is any direct threat. During the last couple of years, hard-key solutions have emerged but they are too expensive. Danske bank keep themselves informed about new alternatives and techniques and are involved in the BankID cooperation for instance in order to have a commonly used standard. The hard part is that everyone has to see their value and the meaning in cooperation. Many banks has been involved in the development of BankID but later dropped out, even though they will probably get back on when they realize the importance. BankID has not yet been a success.

Göran Zebhür, security manager at Föreningssparbanken:

Scandinavia is well known for their security awareness compared to the US where they for instance use more pin code related techniques. Most of the technologies come from the US and Föreningssparbanken keeps an eye at the development in this field and tries to grasp information about new techniques from conventions and corporation visits. BankID is a nation wide standard, compared to Handelsbanken's first certificate, which was “home made” and now we try to make a standard for certificates so that soft certificates are compatible to hard certificates and vice versa. Today there are no standards for card readers that match the required security.

Ralf Bjerström, product development, Handelsbanken:

Information about new techniques is acquired from different distributors, seminars and media etcetera.

BankID is a form of e-legitimation. Several banks are involved in BankID and Handelsbanken is one of them.

Rickard Lindell, product manager at Nordea:

Nordea is Nordea and we do not really need to search for information about new techniques since we get information from others and since we participate in a lot of groups that develops and search for information and news in this field. Consultants come to Nordea frequently to inform about new things.

Stefan Söderberg, security manager at SEB:

SEB gets a lot of information from different companies and we also have a group that study trends all around the world. SEB has a BankID through Telia but puts more effort into their E-legitimation.

Stefan Johansson, security manager at Skandiabanken:

Skandiabanken keeps an eye on the market and are fully aware of the alternatives that are available. The choices that were made at Skandiabanken were made before I was working here.
4.2.5 What is the future for Smart Cards?

Hans Petersson, security manager at Danske bank:

Smart cards exist in many different forms. ID-Cards and credit cards (EMV-Card) has chip and they contain certificates and keys, however there are no services for using these. The card in the mobile phone could also be used in the same way as a smart card. There are two ways, the mobile way and the wallet way and both these ways will probably have a commonly used standard in the future (services, codes and signatures in the smart card or applications on computer).

Smart card is a way to transport information, and you can get far with ID and a password and you will get even further with a soft key. The “harder” keys can be more secure since it is less vulnerable to viruses. It depends on what kind of service you want.

Göran Zebrur, security manager at Föreningssparbanken:

This is a very interesting area, since we are all different and we all want different solutions. Some people want different cards for different purposes and some people want one card for everything. Important is that the card should not be magnetic but have a chip like EMV chip and be able to have certificates. Föreningssparbanken tries to make it possible for people to individually make a "personal smart card" that can contain whatever a person wants and to be used for both identification and for other services. Föreningssparbanken are looking into this now.

Ralf Bjerström, product development, Handelsbanken:

The future for smart cards lays probably in the EMV. Smart cards have been around for a long time but have never really broken through. Smart cards are too advanced for sole actors to establish. That is why the increased use of EMV cards for all bank customers will result in an increased use of smart cards in various areas, both commerce and as identification. The development of software applications also makes it easier for users to use card readers for the smart cards.

Rickard Lindell, product manager at Nordea:

We have smart cards in the mobile phone, in the credit card; there are a lot of places where a smart card can fit in. Smart cards have a very good possibility to carry security solutions.

Nordea will start implementing smart cards when it is clear that it is of great value for both costumers and for themselves. We do not really know when this will break trough. We try most solutions, and try its value to the customers. The Estonians has invested heavily on national ID cards with smart cards and they are used over the whole country.

Stefan Söderberg, security manager at SEB:

Smart cards will be implemented in the bankcard within a 10-year period.

Stefan Johansson, security manager at Skandiabanken:

The market has been waiting for 10 years to be able to put a certificate in the smart card but the problem has always been the lack of an infrastructure (card readers). Since the possibilities have increased over the last years for hard certificates, banks including Skandiabanken plans to put hard certificates on the chip in the new EMV cards. The card reader has also become cheaper so it will definitely be more commonly used in the future.
4.2.6 What technique does your bank think will replace the techniques of today? Is biometrics an alternative?

Hans Petersson, security manager at Danske bank:

Some countries are already using biometric techniques, and many countries are experimenting. Biometrics can be used in combination with PKI, but it can not entirely replace it. However, some biometric techniques are not safe, for instance if someone unauthorized lays hand on biometric data it could be misused forever. There are other techniques, for instance Belgium where some banks use voice scan when clients are logging in to their bank. High security will be reached with a combination of different techniques, for instance some kind of biometry in combination with cryptography and a pin number. There have been discussions to implement new techniques but there is not yet a sufficient need or gaps big enough in the present techniques.

Göran Zehbür, security manager at Föreningenssparbanken:

The objective view on Biometry is that it is not 100 percent safe. For instance can a father and a son have similar voices and it can be hard for a program the separate them. Further 5-7 percent of the fingerprints cannot be used for identification because of insufficient fingerprint. However it might be useful in combination with other techniques in that sense that we take the best from biometrics and the best from another technique.

Ralf Bjerström, product development, Handelsbanken:

The next step will probably be some kind of infrastructure based on EMV cards. Biometry solutions are today very expensive, complex and weak. They could be used as a complement to other solutions.

Rickard Lindell, product manager at Nordea:

Biometrics has a lot of problems. The technique is available to for instance put fingerprints scanner on cards or keyboards, but this is however very expensive and very complex. The functionality has to be very high (it is harder to change a thumb) and at the moment they do not reach Nordea’s standards but they are frequently looking into it.

Stefan Söderberg, security manager at SEB:

There are currently no plans to implement biometry in SEB it might be possible in the future but when “logging in” PKI will always be behind

Stefan Johansson, security manager at Skandiabanken:

Soft and hard certificates will dominate the used techniques in the future.
4.2.7 What kind of role do you think the bank will play in the future when it comes to electronic purchases? (Third part, 3-Dsecure, SET, BankID)

Hans Petersson, security manager at Danske bank:

Hans Peterson from Danske Bank predicts almost the same things as his colleague at SEB does. Hans Pettersson talks about three basic services that banks always have and always will offer their customers. Number one is to move money from one place to another. This could be within the same bank or to another bank in a different country. Number two refers to loans and investments, or as Hans Pettersson calls it, “moving money through time”. The third service is to convert different values. For example from dollars to shares to bonds.

These three services are so associated with banks that in the future, it will be no change. However, with the tough competition today we will see many extra services offered to the customers.

Göran Zebhür, security manager at Förentingssparbanken:

The environment changes quickly and the bank has to look over its role. Förentingssparbanken has a part in the overall cash flow and needs to be alert to changes. This includes looking over new technical inventions on a regular basis. But the basic role will not change.

Ralf Bjerström, product development, Handelsbanken:

Handelsbanken is involved in the BankID project. He believes that in the future, banks will play an important role as inventors of new general standards and infrastructures for e-business. A standard system for e-business payments would probably increase the usage of e-business.

Rickard Lindell, product manager at Nordea:

The bank has a big group of people who is already identified and that is a great advantage. This makes it much easier for us to issue some kind of electronic identification and that might be a role for the bank in the future.

The authorities affect the bank different in different countries and therefore it is hard to be general. In Estonia for example the authorities issue identification and the only thing the bank can do is to accept that. But the bank will play a central role in some way.

Stefan Söderberg, security manager at SEB:

Banks have always been those who transfer money from one place to another. Stefan Söderberg does not think that it will change in future. SEB is of course involved in many projects, among them the 3-D secure cooperation, which includes actors such as VISA and MasterCard.

Stefan Johansson, security manager at Skandiabanken:

Stefan Johansson at Skandiabanken assumes that banks will be responsible for electronic identification in the same way they do today. However, it will never be the core business but a compliment that is possible just because of the unique position banks hold.
Even though more and more transactions will be made electronically, the bank’s role never really changes, says Stefan Johansson. As long as both customers and companies have their accounts in banks, the banks will do what they do today.

4.2.8 Do you have any demands or pressures from the other market actors to introduce new solutions?

Hans Petersson, security manager at Danske Bank:

Sometimes the credit card companies demands that the banks have to introduce new standards of security. Most often they have a schedule for this and when some actor is not keeping up with the schedule they will put pressure on the bank in question. It is the same thing with other security issues that appears. We have to come up with a solution, says Hans Petersson.

Göran Zebhür, security manager at Föreningssparbanken:

Göran Zebhür's opinion is that the EMV project is a clear example of when the global credit card companies have demands on the banks. If they still want to be issue their credit cards they have to implement the new standards involved in EMV.

Ralf Bjerström, product development, Handelsbanken:

No.

Rickard Lindell, product manager at Nordea:

It is more a question of requests from different actors on the market. It is mainly different authorities, which put pressure on us when it comes to different standards and security issues.

Stefan Söderberg, security manager at SEB:

The introduction of “e-legitimation” was to some extent a result of pressure put on SEB from the authorities. The authorities could force SEB with new laws. Companies also come to SEB and want their product or service sold. However, this is maybe more convincing selling methods.

Stefan Johansson, security manager at Skandiabanken:

No.
5 Analysis

In this chapter we will analyse the results from our empirical study by using the theoretical framework as base and complement with our empirical findings.

A common opinion from the different banks is that they choose the technique that needed least development. As for the banks that used the Active Card solution, they said that it was fully developed and could be used. Most of the banks started as early as 1996 with their Internet solution. As Hans Peterson, security manager at Danske bank said: “In 1996, we went from a function model to practical implementation in sec weeks and the Kodbox solution was the only product that was ready for production at that time”.

As for other aspects, we can see that the banks value a technique that is easy to use and therefore cost less in support. Göran Zebehur, security manager at Föreningssparbanken said that they looked at other solutions; among these were a technique that required a card and also a card reader for the computer. They evaluated it and concluded that it would require more support to make the technical environment for the customer to work properly. The solution they choose was the Active Card, which does not require any additional software or hardware to work. This also leads us to the third aspect: mobility. As for the Active card, you can log on to your bank from an Internet connected computer anywhere.

As for the last aspect, the solution had to be cost effective, not only in support but also administration and maintenance as Rickard Lindell at Nordea underlined.

Therefore, we can summarize four criterias:

<table>
<thead>
<tr>
<th>Ready to use</th>
<th>The technique should be fully tested and developed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Easy to use</td>
<td>The easier it is to use, the less it scares customers and puts demand on support.</td>
</tr>
<tr>
<td>Mobility</td>
<td>The mobility is an advantage for customers that often need to log on to their Internet bank.</td>
</tr>
<tr>
<td>Cost effective</td>
<td>This is an overall term and includes costs like support, start-up, administration and maintenance.</td>
</tr>
</tbody>
</table>

Chart 5-1 A table briefly summarizing the criterias.

The majority of the banks mean that their solution did not have any negative sides, but eventually some weaknesses turned up. Hans Petterson at Danskebank means that a negative aspect is that the soft key can be manipulated through trojans and other kind of viruses. Stefan Söderberg, security manager at SEB pointed out that the cost for the Digipass was a negative aspect and that their solution could not be used for digital signatures. As for Handelsbanken, they admit that their solution is somewhat dependant to the workplace as many threats are using the weaknesses in the computers software, for example Microsoft Windows operating systems and Microsoft Internet Explorer.

As we suspected was “cost effectiveness” and “high security” the key words all the banks had in common. We realize that this is of high importance as an Internet bank is a large investment for the banks. Hans Petersson underlined an important thing, to make it more natural and pedagogical to use an electronic service, it is important that the thinking from
an analogue world to an electronic environment is taken seriously. As Föreningssparbanken
and Nordea mentioned, bank politics and authorities has a part in the development as well
in forms of demand and specifications.

The banks all have some kind of relationship with the surrounding environment when it
comes to finding new technologies. The banks are always keeping and eye on develop-
ments in the area such as attending conventions studying development in other countries,
studying media and having frequent visits from organisations with new products. Hans Pet-
tersson, security manager at Danske bank pointed out that they had the ambition to make
everything electronically. In order to be up to date it is important that banks follow emerg-
ing trends and are quick to implement easy and safe solutions. Göran Zebhür, security
manager at Föreningssparbanken meant that when it comes to snapping up new techniques
Scandinavia are well known for their security awareness compared to for example the U.S
where they use more pin code related techniques.

It is clear that the attitude towards smart cards among the banks is that the market has
been waiting for the breakthrough of smart cards but it has not yet emerged. The reasons
why this has not happened is according to the banks that the infrastructure does not exist
and that it has been to expensive and complicated to implement this technique since in
most cases a card reader is necessary. Weisman (2004) shares this argument in his article
Smart cards still irrelevant for U.S. retailers, were he also states that other payment options, the
security aspect and the lack of infrastructure has an effect on the outcome of smart cards.
It is important to mention that smart cards exists in many forms such as in ID cards and
credit cards (EMV) and could also be used as the sim card in a mobile phone. There are a
lot of places where a smart card can be used and it has a great potential of holding security
solutions. Since people are different, people require different solutions, smart cards can be
multifunctional in the sense that one card can contain both identification information and a
credit card as well as other services. In other words instead of having lots of different
cards, only one card can have all the functions if preferred. If the smart card will break
trough it is because of a common interest and that all parts such as banks customers and so
on can value from it.

A common factor when discussing future techniques such as biometrics is that so far it is
not totally reliable. It is also expensive and complex to implement. Furthermore biometric
technology, as Zhang and Yu (2003) points out, is still at the development stage. Biometric
could be used in combination with other techniques such as PKI and pin codes and the
general opinion of the banks shares this view.

The most used method of today to access computers and data are still passwords and PIN
codes and since they are easy to use, they provide, according to Zhang and Yu (2003), a
weak proof of identity and should be used in combination with other techniques.

When it comes to electronic transactions the banks see no difference of the way they work
today and a few years forward. It is still the role in the cash flow that will be the core busi-
ness. Every bank employee we have asked agreed upon this.

It is clearly that the security around transactions over the Internet will play an important
role in the future. It is crucial that we can trust the identification of the different actors and
it is as an issuer of electronic identification the banks will act. It is, according to Stefan Jo-
hansson at Skandiabanken, because of the unique position the banks hold. They already
have all of their customers identified as customers of the standard bank.
Analysis

Though all of the respondents are convinced that the identification part is just a minor part of the bank business, it is an important one for the banks. A high security is necessary and the work with security never ends. Ralf Bjerström at Föreningssparbanken believes that the bank will play an important role as inventor of new technologies and standards. This is not hard to believe since many of today’s standards are developed by banks. BankID and E-legitimation are just two recent examples.

A few major actors can really put pressure on the banks. Those are mainly the credit card companies and authorities. The credit card companies can threaten the banks with a withdrawn card-issue permit. The authorities have the possibility to change the regulation and therefore they are an important actor as well. But it seems that no real pressure is really put on the banks, two banks does not experience any demands at all.
6 Concluding discussions

In this chapter we summarize the analysis and take out the most important parts, further we will answer the questions to the main problems in chapter 1.2. We also reflect upon the study, discuss experiences and makes suggestions for further research.

The purpose with this thesis was to examine what different techniques that existed behind the Internet banks and how new techniques, like biometrics, could be used. We think that we fulfil our purpose, but we also think that the technology behind, which is described in our theoretical framework, could be more contextual, but due to the banks security regulations, they were not able to reveal much of their security solutions.

We will pick out some important points from the thesis and summarize these:

Most of the banks introduced their Internet bank solution in the later part of the 90’s and they chose the technique that was the most developed on the market. Some adjustments were made and then implemented. The banks still use the same technique today with minor upgrades.

When the banks introduce a new technique, they go after the same criterias as other companies, but with a higher focus on security. The four criterias we identified were ready to use, easy to use, cost effectiveness and mobility.

When it comes to snapping up new technologies it is important for the banks to be up to date and monitor the environment in order to follow the development. This is something that all banks engage in and considers important.

The attitude towards smart cards are shared in the sense that the infrastructure does not exist and that it is to expensive and complex to implement today. However the banks realize its potential in the future.

The usage of biometrics among the banks does not exist today and they all share the same view that it is still at the development stage and so far not totally reliable. The conclusion drawn is that it can be used in combination with other known techniques in order to produce a secure solution, but this is something that is not planed in the near future. Biometrics has potential and may play a big part in the future when it comes to identification.

The banks role in the future should be mainly the same as today, but more as an issuer of electronic identifications. This thanks to their already existing database with identified persons.

One question we asked was if the banks were somewhat forced to implement new techniques or standards, this is not the case. It is often up to the banks and the development is often conducted in close relationship with banks and other companies. There are some legally and standardisation issues given by the authorities the banks must adapt to, but this was by us seen as expected.

It seems like the banks have a high level of security. We noticed that it is prioritized and not taken for granted. The banks are highly aware of the changes made on the market and new threats that could weaken the tight security around the Internet banks. As one could image, it is much at stake for the banks. A serious error or a weakness in the security could not only make customers lose money, the bank could also get a bad reputation.
6.1 Reflections

We have had both wonderful moments, but also some difficulties during our work. The first thing we discovered was to find a somewhat unique approach within this subject. Many thesis were already written and therefore it was hard to find a unique approach.

After settling with the approach, the second major thing was the hard time planning the interviews with the banks. Tight schedules and geographical distances made it nearly possible, so going from a personal interview, we were concentrating on interviews via telephone, and for some of the banks via e-mail. This was a minor setback as the empirical information acquired became somewhat limited and therefore harder to draw conclusions from.

As a consequence, our seminars with our tutor were not as rewarding as it could have been because of the late answers from the banks.

Also, with one of our questions, we wanted to found out if the banks noticed any negative aspects with their techniques. As you may think, this was a question that was a bit sensitive and therefore, none of the banks could admit that they had weaknesses in their solution. A few weeks later, we read in Aftonbladet that a teenager “hacked” into Skandiabanken Internet bank by just guessing PIN-codes by random (Carnhede, 2004).

6.2 Acquired experience

We now see the importance of scheduling the interviews ahead, and to be persistent by calling back and e-mailing back and forth to really confirm an interview.

Also, it gave us a reminder of making back-ups and sorting of our work, sometimes we could write in three parallel documents and merging these was quite a difficult task.

6.3 Suggestions for further research

As the banks see potential in Smart Cards, we draw the conclusion that it will be a common used technique in just a few years. Therefore, more research on this area could be made to enlighten the weaknesses, but also the positive sides and potential of this card. You can read in the newspaper now and then about the smart cards and right now, it seems like there are some ethical limitations of how much information you should have on your smart card. Saving fingerprints and medical history could be too dangerous if it falls into wrong hands.
References

7 References

Literature


Internet Sources


References

Organisation for smartcard, retrieved April 13, (2004) from www.smartcard.co.uk,

Interview Sources

Bjerström, R. product development, Handelsbanken: June 16, (2004). E-mail
Questions to the banks

1. Varför valde ni den teknik ni använder idag för er Internetbank och hur skiljer den från andra bankers?

1. Why did you choose the solution you have today and how does it differ from other banks.

2. Ser ni några nackdelar eller begränsningar med den teknik ni använder idag?

2. What do you think are the negative aspects or limitations in your current solution?

3. Vilka var stegen bakom implementeringen av er nuvarande teknik och vilka kriterier skulle den uppfylla?

3. Which were the steps behind the implementation of your current technique and what criterias must be fulfilled?

4. Hur får ni information om nya tekniker, teknologier? Vilka tekniker fick ni välja mellan?

4. How does your bank acquire new techniques, technologies? What techniques did you choose between?

5. Hur ser framtiden ur för så kallade Smart Cards?

5. What is the future for Smart Cards?

6. Vilken teknik tror Ni kommer ersätta den ni använder idag? Är biometrik ett alternativ?

6. What technique does your bank think will replace the techniques of today? Is biometrics an alternative?

7. Vilken roll tror du banken kommer ha i framtiden när det gäller elektroniska köp?

7. What kind of role do you think the bank will play in the future when it comes to electronic purchases? (Third part, 3-D secure, SET, BankID)

8. Får ni krav eller påställningar från andra aktörer på marknaden om att implementera en ny lösning?

8. Do you have any demands or pressures from the other market actors to introduce new solutions?
# Data dictionary

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3-d secure</td>
<td>A newer, more modern technique than SET for safe transactions over the Internet.</td>
</tr>
<tr>
<td>BankID</td>
<td>It is a kind of identification standard, the same as E-legitimation.</td>
</tr>
<tr>
<td>Biometric identification</td>
<td>Identification based on the characteristics on a human body, for example eyes, fingerprints and facial construction.</td>
</tr>
<tr>
<td>CA</td>
<td>Certificate Authority, a third party that authorizes certificates.</td>
</tr>
<tr>
<td>CBT</td>
<td>Crypto Based Transaction, a transaction that is ciphered.</td>
</tr>
<tr>
<td>DES</td>
<td>Data Encryption Standard, a standard technique for symmetrical cryptography.</td>
</tr>
<tr>
<td>E-legitimation</td>
<td>It is a kind of identification standard, the same as BankID.</td>
</tr>
<tr>
<td>EMV</td>
<td>Europay MasterCard and Visa, a cooperation that insures that Smart Cards and other terminals to interoperate with each other.</td>
</tr>
<tr>
<td>JAVA</td>
<td>A platform-independent language for computers</td>
</tr>
<tr>
<td>Active Card/ Digipass</td>
<td>A small electronic device, like a calculator, which generates codes for logging on to Internet banks.</td>
</tr>
<tr>
<td>PKI</td>
<td>Public key infrastructure, a kind of standard that ensures the security for the involved parties. This is based on combining cryptography, digital signing and certificate authorities.</td>
</tr>
<tr>
<td>RSA</td>
<td>A technique for asymmetric encryption is among the most common techniques today.</td>
</tr>
<tr>
<td>SET</td>
<td>An older technique for safe transactions over the Internet.</td>
</tr>
<tr>
<td>Smart Card</td>
<td>A card that looks like a typical credit card, but has an integrated chip that enables several smart functions, like for example electronic identification.</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
</tr>
</tbody>
</table>