International Journal of Computer Science and Informatics

Volume 2 | Issue 1 Article 9

July 2012

Choosing a Technique for Digital Signatures From the Customers' Perspective

Pushpendu Rakshit
Department of IT And Management, Navi Mumbai, India, pushpendu_rakshit@yahoo.com

Choosing a Technique for Digital Signatures From the Customers' Perspective

Pushpendu Rakshit

Department of IT And Management, Navi Mumbai, India
E-mail : pushpendu_rakshit@yahoo.com

Abstract – One way to secure identity over the Internet and other channels is to use digital signatures. Since this area is often used in contact with banks, we have during our work co-operated with Nordea IT. In order for customers to use a digital signature whenever they wish to, a way of making them mobile is required.

In our thesis we give an overall understanding of digital signatures and how they can be used. Our main goal is trying to find out what technique customers want to use for carrying their digital signature and if information positively affects customers' will to use the new service.

We have found theories about the customers from literature, articles and Nordea IT. The most important theories state the importance of listening to customers and the importance of creating a trust between bank and customer. The main method used for the investigation is a questionnaire. This questionnaire is used to find out public opinions regarding the use of digital signatures.

As seen from the result of our investigation most theories about the customers are confirmed. The answers from the questionnaire showed that it is important that the technique fulfils the customers' desire. Every other person could consider using digital signatures, if the number of uncertain can be convinced. From those who are negative or uncertain, one fifth are affected by information from the bank. The importance of information about security and bank policies is thus also confirmed. Both the choices of technique and the information positively affects customers' will to use digital signature. So we find through a study that how customer accepts such technological enhancement.

Keywords - *Digital signatures, carrying technique, information, customer-driven development.*

I. INTRODUCTION

1.1 Background

The Internet is growing rapidly. More and more people get connected every day and start to explore and use the simple solutions that Internet can provide. As a result of this, more people start using Internet for payments and transactions through banks and purchasing items on the Internet. In order for this to work properly and secure, some sort of reliable security solution must be used, to verify that the person using the services is authorised to do that.One of the security solutions used today is called "digital signatures", and is widely spread over the Internet. As more and more ways of communicating and performing business evolve, a way to make digital signatures mobile is desirable.In this thesis we have co-operated with Nordea IT, which is a service unit within the Nordea group. The Nordea group consists of a number of banks situated in the Nordic countries. The most known are Merita in Finland and Nordbanken in Sweden. The area of digital signatures is of greatest importance to banks in order to provide secure services.

1.2 Problem definition

The introduction of digital signatures with multipurpose (different services) means that a customer needs a way to carry his/her signature. In order for the customer to feel comfortable with this carrier, the carrier needs to suit the customers' demands. If the customer is not satisfied with the carrier, then he/she will not use it.

We also face the problem of customers hesitating to use digital signatures. Do they really want to use one? There are many factors that matter, not only the way the signature is carried by the customer, but several customers also need information regarding security from the bank. For example, who is to blame for potential loss of money? Can a rigorous campaign of information from the bank perhaps solve the problem of convincing hesitating customers?

1.3 Purpose

The purpose with this thesis is to investigate the area of digital signatures and different techniques that could be used to carry a digital signature. This subject is very important today and that is why it's very interesting for us. This area is also very important for companies that use or want to use digital signatures.

Another purpose is to investigate digital signatures from the customers' perspective. We want to find out what technique the customers prefer, which channels they want to use and what services the customers are interested in when using digital signatures. The purpose with our thesis could be summarised in three points:

- Examine the subject of digital signatures in order to give an introduction to our work.
- Examine the usage of digital signatures from the customers' perspective, including different carriers and channels, and the impact of information about different techniques to the customers.
- Present a result that can be used by a company.

1.4 Hypothesis

"If the bank offers a service for digital signing and identification with a technique that fulfils the customers' desire, and gives information about security and policies, then customers' will to use the service can increase."

1.4.1 Input variables

Technique: Different devices that the customer can use to "carry" his/her digital signature. Such devices are for example cards with a chip (credit card, regular ID-card, an additional card), or additional chip in a cellular phone.Information about security and policies: The customers can receive information about the security behind the technique and about policies decided by the bank regarding the technique. We assume that the information is detailed and sufficient.

1.4.2 Output variable

Customers will: The customers' will to use the new service. At the starting point all customers are uncertain whether to use the service or not. At the introduction of the service the customers' will can either increase or stay unchanged.

1.4.3 Relationship

The relationship between the variables is the increase of customers' will, which is dependant on how well the technique is suited to customers' desires and if they receive any information about the security and about policies. If the customers' will "can increase", that is equal to if they can consider to start using the new service.

1.5 Questions at issue

During our work we address a number of questions, related to the problem definition. Our thesis will answer these questions:

- Does the customer want to replace their ordinary signature with a digital alternative?
- Can information about digital signatures and company policy positively affect customers' attitude regarding the use of digital signing and identification?
- What technique for digital signatures do customers want to use to prove their identity and supply their digital signature?
- What channels for digital signing and identification are most requested by customers?

II. DIGITAL SIGNATURES

2.1 What is a digital signature?

A digital signature consists of several pieces, that combined create a way of encrypt messages, securing identification and prevent altering of messages. Ideally, this is all handled by applications, and the line of action is described below, in a simplified form.A checksum of the message is produced, that has the purpose of preventing altering of the message, since any change, even a minor one, would produce a non-valid checksum.

The message is encrypted with some kind of encryption technique, for example PGP (Pretty Good Privacy). PGP is an encryption alternative, based on the PKI-technique described below.

Now, we have an encrypted message, and an encrypted checksum. The only way to decrypt the message is using the correct key (the key that correspond to the key encrypting the information), and therefore the message can safely be sent over the Internet. When the message reaches the intended receiver, he decrypts the checksum and the message, and creates a new checksum for the decrypted message. If the new checksum is identical to the one included with the message, the receiver can be sure that the message been altered.[1]

But we are still facing major problems, the fact that we still don't know whom the owner of the key-pair is. In order to find out this, we introduce the concept of

[1] http://www.intranetica.com/intranetica/kds/signaturer.shtml

certificates, which bind a pair of keys to a physical person.

III. CUSTOMERS

Customers are the basis for any business. In order to get new and keep old customers in the digital signature business, several aspects must be considered. Today, developers tend to focus on whether it is technologically possible or not, and pay less attention to the willingness to use the new systems.[2] In this chapter we will discuss the importance of listening to customers, when developing and implementing a new system or process. We will also talk about various techniques from the customers' point of view.

3.1 Convenient and simple techniques

The consumers prefer simple and convenient techniques.[3] Today there already exist some techniques on the market. The important thing is to implement the technique that will be accepted and used by most customers. If the customers do not like a product or service, there will be a good chance of falling out of business.[4] The importance of listening to customers is shown when looking at the cash card, introduced in Sweden some years ago. Even though the bank benefits greatly from the cash card, the customers feel that they have no use for it in it's original form and therefore will not use it.[5] Julian Ashbourn express similar thoughts, when claiming the importance of getting users involved in the process of implementing any new system or process.[6]

The idealistic technique is one that can be implemented in something that customers already carry with them in their everyday lives. The problem is to find a solution that everyone can use. For example, not everyone possesses a cellular phone, so an alternative solution for those without it must be dealt with, if cellular phones are the main choice of technique.

[3] http://www.intranetica.com/intranetica/kcks/signaturer.shtml
[4] Jonas Hallberg Cambridge Technology Partners, "Taking Virtual Banking one step further: an introduction to WAP Nordic Banking", Nordic Mobile Banking conference (Copenhagen 7-8 November 2000)
[5] Ingemar Bureius MeritaNordbanken, "Establishing remote payment services through WAP Banking", Ibid.
[6] Patricia B. Seybold, "Customers.Com, how to create a profitable business strategy for the Internet and beyond" (Random House, 1999) p. 19-20
[7] Krister Adedal, "Cash-kortet dödfött (Computer Sweden, 1999-06-03)
[8] Julian Ashbourn "Biometrics: advanced identify verification: the complete guide" (Springer-Verlag 2000) p.83

3.2 Different channels

With different channels we mean various situations in which the digital signatures can be used. The underlying technique for the various channels and situations are the same, namely digital signatures (keys and certificates). The possibility to be able to use a digital signature at any time is vital. Therefore, the system must be designed to work over many channels. The more channels the customer can choose from, the more often he will be able to use his digital signature, and will hopefully do so when possible. Examples of such channels are:

- Internet
- Telephone net (cellular phone)
- Cash machines
- Service devices within stores, authorities, banks or other places.

IV. CASE STUDY

In this case study the bank Nordea IT is focused and the reader gets an insight into the company and its services and techniques. The goal of the case study is to give an understanding of the problems that the bank is facing, in order to know what the customers want.

4.1 Background

A goal for us was to find a company to co-operate with, who could use something that we wanted to investigate. We thought that a bank could be very interesting and appropriate, since the security is of vital importance for them and they often use digital signatures. We got in contact with Nordea IT and decided to co-operate with them. Our philosophy is that you do a better work if you have something to reach up to and if you know that a company is interested in what you do. Together with Nordea IT we decided the direction of our work. The bank wanted to find out if the customers wanted to use a digital signature and in what way the customers possibly want to use it. An example of the reason is that there are many ways of how the digital signature can be used or carried. In a card with a chip is one possibility, but do the customers really want another card? This issue is of great importance for the company since it is meaningless to develop something that the customers do not want to use. This mistake was done when the so-called cash cards came a few years ago. The customers didn't use this product as much as desired. With this background we formed our thesis with focus on the customers' perspective. Beside a brief introduction to the area of digital signatures we focused on the customers and what solutions the bank should provide to them.

4.1.1 Nordea IT

In our thesis we have co-operated with the bank Nordea and especially Nordea IT, which is a service unit within the bank. The company is one of the world's largest banks on the Internet. It has a leading position in the market, and many resources are used to keep that position. It's very important for the company to keep its customers. One of many factors is of course to have good security solutions that the customers can trust.

Nordea IT has about 2700 employees and about 620 of those works in Sweden.[7] Besides Stockholm there are offices in Göteborg and Sundsvall but also in the rest of the Nordic countries. Nordea IT works in many areas and has for example units for system development and card management.

4.1.2 The customers

The company has a total of 2.2 million customers on the Internet from the Nordic countries and over 800.000 agreements in Sweden.[8] In order for customers to use the SOLO services provided by the bank (described in chapter 4.2), the customer need a personal account for transactions. To open and maintain an account of this kind, the demand is a well kept personal economy, with some sort of income (wages, student support, pension). This means that several target groups can use the services.

4.1.3 Competitive edge

For any company, it is of vital importance to have a market and to have products with which they can compete with their competitors. The companies endeavour to always have a selling product that is competitive in the market. When the selling rate for a product decreases, another, new product should take over. Like this the companies will not lose money, but it is very hard to reach up to this goal. Difficult decisions that have to be made are for example when the time is right to start the development of a new product and how long time it is going to take. It's also a big issue to estimate which product the company should develop, since it is a prediction of the future and what the customers want to buy at that moment in time. Another aspect is use and development of new techniques. Whenever new products and techniques are introduced on the market, a company should be well prepared, and ideally lead the progress. If they do that, they will hopefully not fall behind its competitors in the use of new services and products. These theories are very important to Nordea IT and they endeavour to have a competitive edge like this.[9] They want to investigate what the customers want in order to know which services they should provide and what technique they should work with. This is just one stage of the process but perhaps the most important. The underlying research forms the basis of the development and gives a hint of the prospective use.

4.2 Nordea IT and its services

Nordea IT is one of the companies in Sweden that can be called a CA, Certificate Authority, which means that they issue certificates with digital signatures. Another company provides the certificates so the bank does not have their own certificates and the bank only issues certificates to its own customers. Nordea was the first company in Sweden that started to use a digital ID card within the company. Since 1992 every person that works in the banks branch offices has a card. When using these cards, all financial transactions are encrypted and sealed.[10] The company has developed many services for their customers for several years. The main concept today is called SOLO. In that concept the customers can use the services on the Internet provided by the bank. They can also use an ordinary phone or a WAP-phone[11] in order to use the banking service. The customers have two options when they choose a security solution. The first solution is managed with a card-reader, a smart card, an application for the security, and a personal code. With this solution the customers consequently use a card in order to log in. The other option is to use ID numbers, a personal code, and codes that are only used once and which are provided by the bank. With this solution the customers thus use codes in order to log in instead of a card. Both solutions have a high security level. All information between the user and the bank is encrypted and secure so that it can not be read or changed by anyone else. A condition for this to be secure is that the customers keep his/her personal code to themselves and keep the smart card in a safe place if they use the solution with card. If a hacker or someone else would do errands in one of the customer's name, the bank takes full responsibility for any loss and promise to compensate the customers. In order to use the two solutions above you must have a computer. An example of a service that is not attached to a computer is the SMS service that is included in SOLO. It works like this: first you call a specific number on your mobile phone and then hangs up. If you wait for a while, you get an SMS where you can see your balance and the latest transactions made. For security reasons no

[7] Martin Ogarp, Nordea IT, 2001
[8] Ibid.
[9] Martin Ogarp, Nordea IT, 2001
[10] Ibid.
[11] WAP is short for Wireless Application Protocol, and is used by wireless devices (e.g. cellular phones) for communication.

customer information is involved in this information exchange. Therefore, a potential intruder can not see whom the information is connected to.

4.3 Different techniques

The bank wants to know what techniques they should provide in order to carry a digital signature. The most important issue is what technique the customers prefer, but which techniques are realistic and possible for the bank to implement? A smart card with a digital signature could be a very good solution for the bank. The customers can do bank errands with the card but also use it when buying items without cash. A theory from the bank is that the customers already have many cards and many codes today and that the customers have a negative point of view regarding introductions of new cards. To avoid this, a chip built in to an already existing card can be used. The alternative with using a fingerprint for example is good. Unfortunately it's not a very cheap solution, but the prices are dropping. Today they have dropped to about 100 Dollars (app. 1000 SEK). The bank doesn't see this alternative as a solution at the moment, but perhaps for the future. To have an application directly in your PC is one alternative that is already used today. This solution is rather static and the bank therefore wants something more mobile. When working with Business to Business or in similar situations where less mobility is required, this however, could be a good thing to use. To have a chip in the mobile phones is also an alternative but today there is not room for a chip belonging to the banks. A solution could be to use SMS, but in the future the bank believes more in a solution that use the bluetooth technique. Nordea IT thinks that the mobile phones are very popular and the bank is very interested in this area for their solutions. Now the bank wants to know if their theories are correct or what technique the customers really prefer and in which situations they want to use digital signatures.

4.4 Summary

It is very important to investigate what technique the customers want in order to know which service the bank should provide. For the bank it is meaningless to develop something that the customers do not want to use.

Today the bank provides two solutions for Internet banking in the concept named SOLO. For both these two a PC is needed, which is very static. The bank wants to provide other solutions that are more mobile for its customers to use.The bank thinks for example that the mobile phones are very popular among the customers and that makes mobile solutions very interesting for the bank. A solution with smart cards is also very interesting for the bank. Nordea IT now wants to know what technique for carrying a digital signature the customers prefer.

V. ANALYSIS AND DISCUSSION

In order to be able to discuss the result from the questionnaire there must be a presentation of the answers. The answers can then be analysed and discussed and comparisons can be made from the theories. The hypothesis must be tested and the validity of the test and the result of the test are going to be discussed.

5.1 Presentation and analysis of questionnaire

In this chapter we will present the answers from the questionnaire, and make comparisons between different questions and answers. We will not specify all the answers depending on categories (e.g. age), just the total answers, from all categories. Further discussion about the answers, both categorised and in general will be found in the discussion parts. We have used our own English translation of the questions in this part

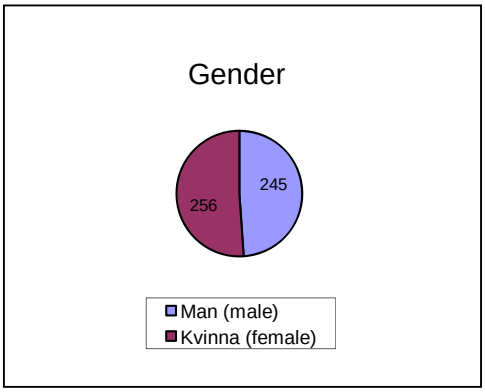
5.1.1 Questionnaire background information

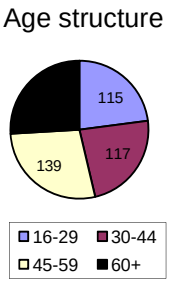
501 successful interviews have been made. Out of these 49% (245 persons) are male and 51% (256 persons) are female.

23% (115 persons) of the respondents are in the age group 16-29. 23% (117 persons) are in the age group 30-44.

28% (139 persons) are in the age group 45-59 and 26% (130 persons) are 60 years or more.

34% (172 persons) live in Stockholm, Göteborg or Malmö. 55% (278 persons) live in cities and 10% (52 persons) live in thinly populated areas.





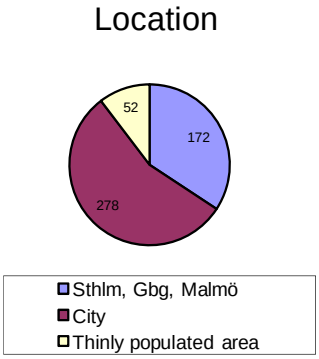


Fig. 5.0 : Diagram over the respondents' gender, age group and location.

63% (316 persons) has a cellular phone that they use continuously.

5.1.2 Presentation of the answers

Question number 2 reads: *Have you received information from your bank regarding security when using their Internet services?*

Out of 501 persons interviewed, 51% (255 persons) stated that they had *received information*, 37% (186 persons)

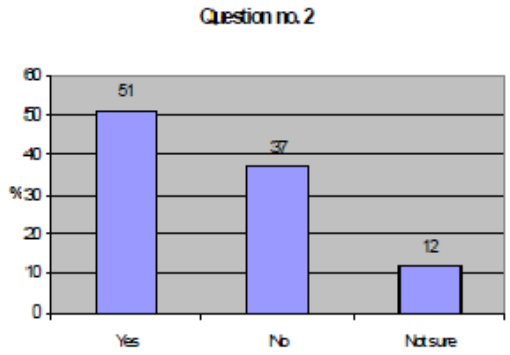
0% of the respondents answered that the bank doesn't have Internet services. This is therefore not included in the diagram.

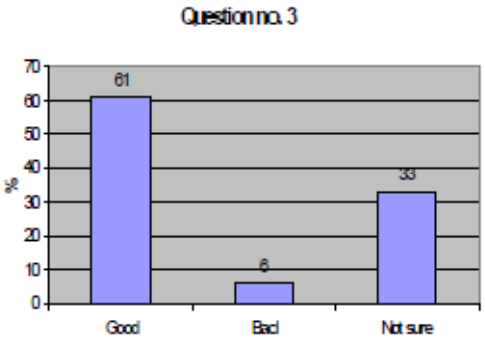
Question number 3 reads: *Was the information...* This question relates to question no. 2 and was asked to 255 persons, those who have received information from the bank.

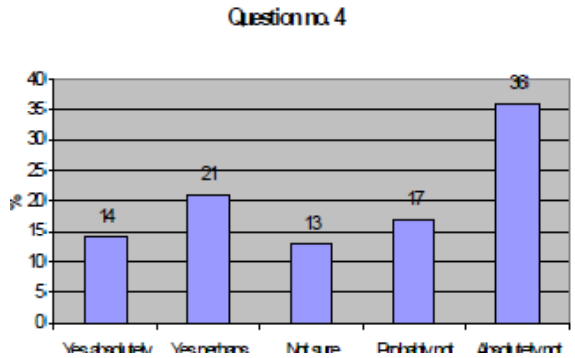
61% (156 persons) answered *good*, 6% (15 persons) answered *bad* and 33% (84 persons) answered *Not sure*.

Question number 4 reads: *Could you consider using a digital signature instead of using a hand-written?* This question was asked to all the respondents (501 persons). The answers have been merged in the same way as in question no. 5.

35% (175 persons) answered *yes absolutely* or *yes perhaps*, 13% (65 persons) expressed the opinion *not sure* and 53% (265 persons) answered *probably not* or *absolutely not*.







REFERENCE

[1] Arledal, Krister (1999-06-03), Cash-kortet döfött, Computer Sweden.

[2] Ricknäs, Mikael (1998-10-15), PKI – nyckeln till en säker framtid, Computer Sweden.

[3] Byttner, Karl-Johan (2001-01-10), Svenskt genombrott för digitala id-kort, Computer Sweden.

[4] Hultqvist, Jesper (2000-12-04), 25 000 Teliaanställda får digitala signaturer, Computer Sweden.

[5] Ottoson, Maria (1998-11), Krav på lag om digitala signaturer, Computer Sweden.

[6] Lotsson, Anders (1998-04), Ordboken nr 29/98, Computer Sweden.

[7] Jenselius, Michael (2000-11-20), Fingeravtryck ersätter lösenord, PC för alla.

[8] Hultqvist, Jesper (2001-04-20), Fingeravtryck förenklar och ökar säkerheten i Rinkeby, Computer Sweden

◈◈◈