Buckinghamshire Chilterns University College

Buckinghamshire Business School

Számalk Open Business School

MBA

Why are not digital signatures spreading as quickly as it was expected?

Name: István Zsolt BERTA

Intake: MBA-10/A

Submission date: 5th of May, 2004

Contents

1 Terms of Reference

The main purpose of the dissertation is

to investigate
why PKI technologies (and digital signatures) are not spreading
in Hungary as quickly as it was expected.

The objectives of the dissertation are:

- to review literature that explains the special economic mechanisms of a digital signature market
- to analyse the current digital signature market in Hungary using the above literature
- to identify factors that seem to prevent the market from growing
- to evaluate the strategy of market players
- to assess if the market players are conscious of the factors limiting the market
- to develop recommendations for an organisation that considers entering this market in the near future

2 Executive Summary

The Hungarian market for digital signature service is in a *crisis* that is *typical for every network economy*: Developing the product or service is expensive, and few clients are willing to pay the price that would cover the costs of the vendor. However, if digital signature service was widespread, it would become more valuable for clients. Moreover, this would allow vendors to reduce their prices, because each service would need to carry a lesser proportion of the vendor's fixed costs.

Although PKI (public key infrastructure) could benefit the entire economy, most players of the economy (customers) are not willing to make the initial investments to develop this infrastructure, because as long as the infrastructure is not big enough, it is worthless. Even if it means a globally optimal solution, more cost-effective solutions exist locally. This is why most service providers require the government to make the above critical investment.

Naturally, if PKI is paid by the government, it is paid by everybody. I found that it is questionable if everybody needs PKI. Especially, because many substitutes exist that often suit the need of end-users much better than PKI. Many customers are would be satisfied by less secure or less global but significantly cheaper solutions. I found that *PKI would do the most benefit to the government* in developing a centralised, costly but relatively secure solution for the identification of individuals. Though, I found it questionable if individuals (who form the state and elect the government) would require such a system.

I found that while *substitutes pose the highest threat to this market*, very *few CAs are conscious about this threat*. Most of them identified the trivial substitutes only, while very sophisticated and more dangerous ones exist too.

I consider investing in this market a very risky step. Although it may still boom in the future, if too many customers commit themselves to substitutes by investing in them, the market will never reach the size (the 'critical mass') for booming.

3 Abbreviations

Technical terms

PKI: Public Key Infrastructure. The worldwide infrastructure that is used to create and verify digital signatures. In order to participate in the PKI, a party needs to have a digital certificate issued by a Certificate Authority.

CA: Certificate Authority. A company (not an authority!) that sells digital signature service.

ECC: E-commerce corporation

RA: Registration Authority. An organisation that registers users for receiving a certificate from a CA.

IT: Information Technology

PGP: 'Pretty Good Privacy'. A system for secure messaging that can be considered a substitute to PKI.

SMS: Short Message Service.

EDI: Electronic Data Interchange

VCA: Virtual CA.

Business terms

CEO: Chief Executive Officer.

ROCE: Return on Capital Employed.

Hungarian Organisations

APEH: ’Tax and Financial Control Administration’, an organisation in Hungary for taxation.

PSZÁF: ’Hungarian Financial Supervisory Authority’, an organisation in Hungary that supervises the financial operation of state-owned organisations.

Why are not digital signatures spreading as quickly as it was expected?

István Zsolt BERTA

4 Introduction

Electronic commerce is a new area of business. It means much more than companies selling products on the world wide web. For example, it also provides ways for them to accelerate their communication with their business partners or improve the efficiency of their supply chain, or ways to select the best supplier on the Internet.

Electronic commerce requires secure communication. Unfortunately, *the Internet is not a secure medium*: If a message is sent through the Internet, it can be easily intercepted and altered by a malicious party. It is also easy to send a message (e.g. an e-mail) in the name of someone else, several computer viruses are performing this action. This means the Internet is suitable for e-commerce only if certain security countermeasures are used.

Digital signatures provide a way to ensure the authenticity of messages. This means that the receiver of a digitally signed message can be certain that the message was sent by the person whose name appears on it. Moreover, the receiver can also be sure that the message was not altered on the way. (See Appendix B.1 on what a digital signature is.)

Although the market this dissertation focuses on can be informally called 'digital signature market', it is not the digital signature itself that can be bought there. Digital signatures are computed by users (or their computers) when they sign messages.

From players of the digital signature provider market, a customer may buy a service (digital signature service), *the potential to create digital signatures that can be verified by any third party*. Note that computing a signature is a relatively easy and cheap task, while allowing them to be verified by anybody requires a complex infrastructure called 'public key infrastructure' (PKI).

A digital signature service provider is also called CA, Certificate Authority. CAs provide service by issuing certificates (required for the verification of a signature) to users. CAs receive an annual fee for keeping the certificates registered. (See Appendix B.2)

4.1 Why is my research important?

As digital signatures were considered a key foundation of electronic commerce, they were expected to spread rapidly. Such a signature could be used in case of sending every e-mail, signing every contract and performing every payment. Many countries (including Hungary) plan to introduce ID cards and other official documents that are chipcards (or smart cards [Berta and Mann, 2000]) that include certificates and are empowered with digital signature capability. Thus, *the market has the possibility to grow very large.*

Since the marginal cost of selling a certificate is very low, and the market was expected to grow very large, *investors saw great perspective in setting up CAs*. Several companies and governments invested fortunes into developing PKI that is required for the use of digital signatures. The appropriate technology is now available, standards are developed, even the legislation is ready. [EU Directive, 1999], [Hungarian Law, 2001]

However, the big boom has not arrived yet. Some investors still see the above perspectives,

governments and companies still invest fortunes into PKI, and visionaries still predict a boom in the near future. Many vendors offer PKI-related or PKI-enabled products, many companies and organisations have developed their own PKI system, but these stand alone systems are still not integrated into a global *infrastructure* (the term that the I in PKI stands for).

The market of digital signature providers is currently a question mark according to the model of the Boston Consulting Group. Moreover, it has stayed a question mark for too long, and is just devolving into a dog.

Within this dissertation, I investigate, why the market of digital signature service providers does not grow using the methodology introduced in Section 5. In Section 6 I review literature that explains the economic mechanisms of similar (often IT-related) markets, and I also assess to what extent this literature can be applied to the market of digital signature service providers. In Section 7, I perform an analysis of this market. I perform a micro- and macro-environmental audit (PEST and Porter's five forces) of the environment of the five market players, and evaluate the relation of their strategy to the reviewed economic principles. I identify factors that limit the growth of the market and assess if market players consciously counter them. I summarise my conclusions in Section 8. Finally, I develop key recommendations for each market player, and assess the attractiveness of the market for a hypothetical new entrant.

5 Methodology

5.1 Secondary research

The following documents were used as secondary research material:

- Kopint-Datorg has published surveys on the Hungarian infocommunication market, including the market of digital signature service providers. [Kopint-Datorg, 2001a], [Kopint-Datorg, 2001b] Unfortunately, this resource is three years old, and three years

is a long time in the field of IT. When relying on [Kopint-Datorg, 2001a], it should be considered if the data has become obsolete.

- Krasznay and Szabó [Krasznay and Szabó, 2001] have made a survey among the Hungarian Internet users to determine how much they know about digital signatures and how much they are willing to spend to buy one. I consider the main weakness of this survey that since it was voluntary, only those users answered it who knew something about digital signatures. Still, the survey finds that people know very little about digital signatures. This survey was performed in 2001 (the year the Hungarian Law on digital signatures has passed), but I do not think that the average (Hungarian) Internet user knows significantly more about digital signatures today.

- *Netlock* (one of the Hungarian CAs) *has performed a survey* on 'the security of Hungarian websites'. Unfortunately, the survey itself is not available on Netlock's home page, only its reviews were published by some newspapers and magazines. [Origo.hu, 2003] Although some figures might prove to be useful, I think, the survey is *rather confusing* and *gives little help* on the subject because some *key concepts were confused*. What Netlock actually surveyed is the number of PKI-enabled Hungarian websites, and not the number of 'secure websites'.

- Some less important sources of information (e.g. news, websites) were used and are referred when appropriate.

5.2 Primary research

5.2.1 Interviews with each market player

I planned to perform *interviews with all five Hungarian digital signature service providers* (CAs). Some of them are huge companies (e.g. Matáv), while some others are small (e.g. Netlock). (see

Appendix E for figures like sales, equity, etc.) My aim was to interview at each company the person responsible for the strategy of the PKI business unit. In smaller companies this is the CEO, while in larger companies this person is a head of a business unit.

I was able to perform four interviews out of five: Giro, Matáv, Máv Informatika and Microsec. I think, my *80% coverage of the market* is relatively good, but I would feel more happy if I was able to interview Netlock. Fortunately, Netlock is very active in press, so I think I could get a good image of the company from secondary research.

I reckon I was able to find the responsible people with the exception of Microsec, where my interviewee is in a position rather technical than managerial. My interviewees provided a lot of help in the thorough understanding of this topic, and I am very grateful to them for this. Yet, as every human being, my interviewees could have been biased too, when explaining their (or their company's) previous actions.

Some of my interviewees were of technical, some others were of managerial background. When formulating questions, I tried to avoid the use of both technical and managerial jargon to provide equal circumstances for both types of interviewees. (E.g. I would have received completely different answers from interviewees who were engineers if in the 'What can a customer use instead of a digital signature service?' I had used the term PKI[1]. Tough, my aim was not to test the technical knowledge of interviewees but to get a picture of their view about the need of customers that their service fulfils.)

The interviews were performed in Hungarian, and I translated them to English later. Since they were informal conversations, I summarised them and also tried to formalise them by organising them around my key questions. This means the sentences of the interviewees are not quoted directly. Interviewees were given the chance to review and alter the summaries. The summaries of interviews can be found in Appendix

[1]Note that PKI and digital signature service is not the same, PKI can be used for other purposes too. Moreover, the term 'digital signature service' is not a technical one. I use it, because it describes more plausibly what a CA sells.

Since the number of affected companies was relatively small, I was able to customise my questions to my interviewees. This was a good idea because I was able to gain deeper insight into the interviewed company. However, if I had asked all interviewees the same questions, it could have been easier to compare these companies based on the interviews only. Working in this field I already had a basic picture of these companies so this latter was not the main aim of my interviews.

I collected *financial information* (see tables in Appendix E) on the affected companies in order to provide the reader a *gasp of the size of market players*. Note that while information on the profitability of companies that are CAs as one of their core activities (like Netlock) is useful, in case of companies that are involved in other businesses too (like Matáv) such information is going to be rather useless.

A significant part of my primary research is the observation of relevant websites (especially the sites of the Hungarian CAs and that of the Hungarian Communications Authority [Communications Authority, 2004]), and reading materials published by these parties on the Hungarian digital signature service provider market.

5.2.2 Interviews with customers

Interviewing or surveying customers is a rather difficult issue. The group of potential customers is heterogeneous, so a random pattern would range over multinational companies as well as individuals. (Many interviewees from this latter group do not even know what a digital signature is. [Krasznay and Szabó, 2001]) In order to perform a survey on all potential customers, they need to be segmented, and surveys should be made on each segment. However, the number of potential customers would still be large in these segments.

My plan was to perform interviews with some potential customers as *examples*, narrowing my research on *small, IT related companies* (those that may gain significant competitive advantage

from a technology like PKI). These companies already know what a digital signature service is, and have already considered purchasing it. Moreover, they also provide services that rely on PKI or its substitutes, so apart from being potential customers, they also mean a threat to this market if they sell substitutes to PKI. Note that it is realistic to interview only a small percentage of these companies, and I was not able to ensure the randomness of my selection. This is why I did not even attempt to give an overall picture of this market segment.

I included two interviews in this dissertation: Data Contact and NetAlfa. For the above reasons they are not a valid statistical sample, I included these interviews because I found them to express some typical and very clever solutions. I also found it interesting to observe the relation of these interviews and those with CAs. However, outcome of this part of my research should not be a base for conclusion on the opinion of all customers.

5.2.3 The author's publications

The author of this dissertation is a researcher at the Laboratory of Cryptography and Systems Security [CrySyS, 2003] at the Budapest University of Technology and Economics. He is researching some of the security aspects of PKI, and has deep insight into many details in this field. Some of his relevant publications are [Berta et al., 2004b], [Berta et al., 2004a], [Berta et al., 2003], [Berta and Vajda, 2003], [Berta and Mann, 2002], [Berta and Mann, 2000].

6 Literature survey

6.1 Network economy

6.1.1 What is a network economy?

According to [Kelley, 1998], the rapid technological development sometimes not only makes new product appear on the market, but also introduces new rules in the economy. According to

Kelley, the different rules apply on the market of IT companies and traditional, brick-and-mortar companies.

In contrast to the work of Kelley, Shapiro and Varian try to explain the new economy with the traditional disciplines. [Shapiro and Varian, 1998] Shapiro and Varian argue that the Internet develops similarly the telephone network did a hundred years ago. They claim the market for most IT products is a *network economy* that has the following properties:

Demand: From the demand point of view, goods in a network economy are *experience goods*. A vendor cannot show its customers how valuable its product is, without letting them experience it. However, if customers experience a product, i.e. receive some information they need (they watch a movie, download a software, or access a weather forecast), then why would they pay for something they already know? On the other hand, if a vendor does not let customers experience the product, they will not know how much they can benefit from it. According to Shapiro and Varian, perhaps this is the fundamental problem of facing business in the network economy.

Another interesting phenomenon of the demand-side is that the same product (piece of information) has different value for different customers at different locations. For example, the weather forecast of London is of little value to someone who lives in Budapest. However, if the same person decides to make a trip to London, the value of the London weather forecast increases for him.

Shapiro and Varian suggest that *market segmentation* is the solution for the above problem. Since the value of information is different to many people, sellers should find a way to sell it on a higher premium price to those who are willing to pay more for it, and to sell it on a cheaper price to those who are not willing to pay so much. (As an extreme solution, the product can be dumped free of charge to those who would not pay for it.) Naturally, sellers should try to prevent premium price customers from acquiring the product on the cheaper

price.

They also suggest *versioning* as a useful tool of market segmentation (and collecting information on the habits of customers). Different versions of the same product can be offered at different prices and conditions. Customers will buy the version appropriate for them.

Companies like RedHat (`www.redhat.com`) and SuSe (`www.suse.de`) are successful examples for the above strategy. They both sell their own version of Linux, a free operating system. Their product that is freely available on their website, but premium customers may buy it and thus receive additional services like technical support.

[Bradford DeLong, 1995] brings examples from the world of books. Impatient customers who want the book immediately when it is published can buy it in an expensive hardback form. Patient customers can wait and may buy the paperback version later at a cheaper price.

Supply: From the supply point of view, creating information (producing a movie, developing a software) requires very *high fixed costs*, but duplicating it is very cheap – the *variable costs are close to zero*. Moreover, practically no capacity constraints exist: a vendor can always produce more copies of a CD-ROM, without meeting a capacity limit or a limit of inefficiency when large numbers are produced.

This structure makes *perfect competition* almost *impossible* in a network economy. A company failing to become cost leader or differentiate its product (or focus on a market niche [Porter, 1985]) will disappear, because its competitors can easily outproduce and outsell it. It is very difficult to leave such a market, because the fixed setup costs are sunken. For example, in contrast to a building, (that can be reconstructed and used for some other purpose), information products can rarely be used for another purpose. (A word processing software needs to be completely redesigned and redeveloped to make a

shoot'em up computer game from it.)

Shapiro and Varian argue that a company in a network economy either has to sell something unique, or be the cheapest on the market. They point out that there is only one way to reach this latter goal. While traditional companies can increase their efficiency or use supply chain management [Slack et al., 2001], a*n information company can only achieve cost leadership by selling more units*, because unit costs are roughly inversely proportional to volume, because the largest costs are the initial fixed ones.

Network externalities: The value of a product to a user heavily depends on the number of users who adopt the product. In contrast to the traditional economy (where quantity and price are negatively correlated), in a network economy, *the larger quantity of a product is sold, the higher price a vendor can ask for it*. The more people use a service, the more valuable it is. For example, if only one person has a telephone, the value of the service is zero – the user cannot phone anyone. The more people by a telephone, the more valuable the service becomes. From the point the telephone becomes a regular way of making business, it becomes essential for everybody to buy one. This means, the more products a company sells, the higher price it can receive for them, and the higher demand it raises. Note the positive feedback in the above loop.

Moreover, most customers do not use stand alone IT products but have information systems and use several products together. Thus, the replacement of one product may require the redesign of the whole information system. This results in *customer lock-in*, so customers getting used to one product may find it very inconvenient or very expensive to switch to a competitor's.

The above reasons explain why Microsoft is able to ask USD 400 for Microsoft Office, while some competing products (OpenOffice.org, KOffice, Abi Application Suite, etc.) with similar (or sometimes even better) functionality are offered free of charge.

This positive feedback prevents perfect competition and creates monopolies. Just like in case of Microsoft, it gets very strong after a certain point, but few companies have such an initial growth advantage so few are strong enough to reach this point. Shapiro and Varian suggests that companies should cooperate in order to grow large. They should promote *compatibility* and *standardisation*, so that an *alliance* would have enough strength to make use of the above positive feedback.

6.1.2 In what extent is a certificate market a network economy?

Although certificates (required for a digital signature service) are IT products, they are not information, but rather tools for gaining confidence in the security of access to information.

Demand: Certificates that CAs issue should be highly standardised. Foreign companies should be able to check and verify them so that Hungarian members of the PKI could appear on the global market. This means, certificates are not experience goods, because the customer should be able to know as much about them in advance, as much they know about a telephone line.

Unfortunately, certificates are a lot less known than telephone lines. Thus, if a CA would like to sell certificates to a customer, it needs to explain and demonstrate what they sell and why it is useful for the customer. Although in this sense the certificate market is a network economy, it is in a *very early stage*.

Supply: The marginal costs of issuing a certificate are very low, close to zero. When the customer uses the certificate, the CA has little or no cost. (However, if the signature creation data is contained by a smart card the card needs to be purchased e.g. by the end-user.),
Setting up a CA has relatively high costs, but (since CAs should function the same way all over the world) these costs are not intolerably high. A smaller part of the costs are required

for setting up a working CA, and a large part of the costs are required to ensure and certify its security, so it can comply with relevant laws.

Unlike in case of many information products, the secure, certifiable system and the knowledge and experience gained when establishing it can be used for purposes other than operating a CA. (Many organisations need a secure system where employees background-checked and are trained to handle confidential information. See the example of Giro in Section 7.7.1.) This means, the *fixed costs are not so high and are not sunken*.

Again, the situation is different, because the market is new. In this case additional investment is needed to demonstrate customers that digital signature service is useful. Perhaps, the cost of this is significantly larger than setting up a working CA that can issue qualified signatures. *The costs of increasing trust in digital signatures is sunken.*

Network externalities: In case of network externalities, we come to different results if we consider a single CA or the certificate market as a whole.

A certificate is a standardised product, so customer lock-in to a certain CA is minimal. If a customer is not satisfied with a CA, moving to another one should mean only minor inconvenience. Similarly, a certificate issued by a CA with high market share is not much more valuable than one issued by a CA with a lesser share, if both CAs are properly connected to other CAs in the PKI. (Still, a certificate issued by a prestigious trusted CA can be more valuable than a certificate issued by a CA with bad reputation. An owner of a certificate should not be more trusted than the CA that issued it. See Appendix B. So, while market share alone does not catalyse the positive feedback in the loop, being a prestigious organisation does. See Giro in Section 7.7 as an example.) This means, *among CAs* (on the market of digital signature service) *the positive feedback effect is not significant*, so there could be a severe competition between them.

However, if the whole certificate market is considered as a participant of the *market of se-*

cure communication, the above *positive feedback effects become very strong*. If a company starts to rely on PKI and digital certificates, switching to another type of products may be very costly. (Apart from certificates, installing and setting up PKI-related software can be very costly.) Similarly, the more people use PKI, the more valuable it becomes. The more people or companies can be identified by digital certificates, the more widespread such systems will become.

6.2 E-commerce

6.2.1 What is e-commerce?

As new technologies emerged, they were often viewed as a revolution in the way business was made. Sometimes, the Internet was viewed as a magic bullet that solves every problem a company had. For example, [O'Brien, 2000] demonstrates many ways for an enterprise to get 'inter-networked'.

[Lindström and Andersen, 2000] list three stages of company's Internet awareness:

1. Presence on the Internet (having a website)
2. The website adds value
3. The Internet has changed the company

Today, most businesses have their own web page, and it is widespread that companies reach step . But is it essential for every business to become an e-commerce corporation (ECC)? Is every shop going to evolve into a web-store?

According to [Coltman et al., 2001], e-business does not mean a revolution in the way business is conducted. Coltman et al. reckon, e-business failed to bring a radical change in traditional business laws. They cite several myths and predictions that did not come true to support their arguments. For example:

- According to Coltman et al., it was a common belief that brands would lose their significance, because low setup costs of e-stores could enable smaller businesses to offer and sell products to large masses as big companies do. But *brands did not disappear*, customers still seek guidance from well-known brands when shopping, so brands have an equal importance in the electronic world as they had in real life. Consumers are not searching the web every time they shop, but tend to buy from sites they regularly visit. This leads to an effect called *cognitive lock-in*.

- People expected that *e-business would bring prices down*. It is true that customers have the possibility to visit several websites to choose the cheapest one. One problem is the above cognitive lock-in. An awaited benefit of e-shopping was that customers could launch electronic agents that do this task automatically. However, Coltman et al. reckon that vendors do the same: they cooperate via their electronic agents to keep their prices similar.

- In spite of forecasts that manufacturers would sell directly to the end-users, *middlemen did not disappear from business*es. Few manufacturers were successful when trying to eliminate resellers, but many faced sever problems when trying to do this. Coltman et al. cite examples for this phenomenon.

- *Being first on the market* was viewed as a key to success in e-commerce. However, just like in case of brick-and-mortar companies, being a market pioneer *does not ensure a company's success*. [Tellis and Golden, 2000] The authors cite the example of Netscape and Microsoft to support their arguments.

On the other hand, Coltman et al. acknowledge the merits of electronic business. Unlike business to consumer (B2C) e-business, B2B communication seems to be successful. In contrast to individuals, businesses like to communicate with their business partners via the Internet. However, many of these processes were done from the distance (via mail or fax) before the e-business era. In this sense, e-business is widespread, but did not bring any revolution.

Coltman et al. summarise their findings as *'there is no such thing as e-business, there is just business and some of it is electronic'*. However, they emphasise that electronic business is developing, the number of Internet users is steadily increasing, and several traditional firms have successfully implemented web based applications. The recent dotcom bubble a slowdown, that brought the economy back to its sense from dreams.

6.2.2 Are CAs e-commerce corporations?

The above literature does not describe CAs directly, because I do not think they are e-commerce corporations. Although they sell information, they cannot simply sell it over the world wide web. First they have to identify the individual they issue a certificate to, and this step (involving the RA) is possible personally only. This means that while CAs sell a service to access a global infrastructure, CAs themselves cannot be global.

While CAs themselves are not ECCs, they belong to the same business sector. They also sell information and services that could develop the information systems of companies. They are not only similar to ECCs in many ways but ECCs constitute one of their potential markets. This means, the future of ECCs has significant impact on the future of CAs too.

6.3 Question mark

According to the model of the Boston Consulting Group, the market of digital service providers can be characterised as a *question mark*. Generally, presence on such a market requires significantly more cash than the market generates.

According to literature, markets that are questions marks can boom and evolve into stars (that later become cash cows), so investors may see perspective in question marks. Unfortunately, not all question marks become stars, some of them devolve and become dogs. [Mintzberg et al., 2003]

Although the market of digital signature providers is a question mark, it has stayed a question mark too long. Investors have been funding digital signature related enterprises for five years and are still not receiving the profit they expected. They are getting impatient. I think, while the market still has potential to become a star, currently it is devolving to become a dog.

Being a new startup market, the question arises: is it good to be a market pioneer? If the market would eventually evolve into a star, would it be good to be the one who successfully penetrates the market? According to literature, the answer to this question is not obvious. Tellis and Golden give a good overview on this topic and suggest that pioneers sometimes make certain investments instead of late entrants. [Tellis and Golden, 2000] Coltman et al. reckons that being a pioneer does not guarantee success in the field of IT either. [Coltman et al., 2001] (See Section 6.2).

6.4 Summary of literature survey

- Based on the above literature, I have decided that the digital signature service provider market is not so special that it cannot be handled with existing disciplines.

- IT products have some special properties that should be taken into consideration. Though certificates are not typical IT products, guidelines for managing an organisation in a network economy should be considered too.

- E-commerce did not revolutionise the way business is done, but B2B e-commerce did bring improvements in areas like supply chain management. B2C e-commerce did not fulfil expectations. One of the most promising markets for digital signature service is lagging behind.

- The market of digital signature service providers is still small and did not fulfil the expectations of investors yet. Although the market still has potential to grow large, if investors withdraw their funding, it might become a dog.

- In case the market would evolve into a star, ferocious competition could evolve among CAs.

7 Market analysis

In this section first I provide a brief overview of the market. Later I analyse the macro and micro environment of digital signature provider companies and evaluate the strategic position of each of these companies.

7.1 Overview of the market

The market of Hungarian digital signature service providers (CAs) is regulated by the Hungarian Communications Authority. [Communications Authority, 2004] If a company would like to provide digital signature service, it needs to be registered (or certified) by the Communications Authority.

Currently, there are five companies registered as CAs in this market: Giro, Matáv, Máv Informatika, Microsec and Netlock. Each one of these market players is evaluated in Section 7.7. It is very hard to estimate the size of the market as most companies have other sources of revenues and they all cross-finance their PKI business unit. Although some market players boast of issuing may certificates, but many of these are issued free of charge for testing purposes. I think, *the current size of the market is insignificant, and is not sufficient to sustain any of the five market players*.

I am going to analyse the market of PKI enabled certificates. There are several types of these, but three main types have substantially different characteristics form the business point of view: qualified certificates (where the CA needs to pass a rigorous certification process), advanced certificates (with a less rigorous process), and server certificates (issued for a machine). See

Appendix B.5 for details. Some CAs sell directly the above certificates (and related services), some others rather sell the right of issuing them.

7.2 Macro Environment

Political factors

- There is a worldwide trend of *deregulation* on the telecommunications market, which affects the market of digital signature providers too. In the Hungarian system, there is no state-owned authority that performs the duty of Certificate Authorities, but profit oriented companies were allowed to enter this market. (There is a similar trend in many countries.)

- Hungary is joining the *European Union* in May, 2004. This may allow foreign CAs to appear in Hungary, but they had this possibility before too. On the other hand it may catalyse the possibilities of Hungarian companies to engage in the global trade.

- The Hungarian *law on digital signatures* was passed in year 2001. [Hungarian Law, 2001] Although this law created the legislative background for the use of digital signatures in Hungary, it was possible to use digital signatures (and other methods for authentication) before this law was passed if both parties in a contract agreed on using them (or one of their substitutes).

  Some customers did not wait until the law on digital signatures was passed, but purchased a certificate from foreign CAs. For example, OTP (the market leader in the Hungarian banking sector) purchased a certificate from Verisign (a leading US CA) to enable confidential and authentic communication for its customers via its website.

  The case of OTP may suggest that a great demand for PKI enabled certificates exists, but OTP needed only *one certificate* (or perhaps a few of them) so that its customers could authenticate the web server of OTP. If OTP would decide to supply all of its customers

with PKI enabled certificates (so that OTP could identify them) that would mean significant demand.

Economic factors

- There is currently a *recession* in the world economy. This recession is especially strong in the IT sector, because we are after an IT bubble. Investors are reluctant to commit themselves to the IT sector. [Coltman et al., 2001]
- Hungary is in poor financial situation today, and the government tries to cut down costs whenever it can.
- *Globalisation* is a worldwide trend, competition is becoming more and more global. PKI and digital signatures provide tools for global companies.
- Compared to Hungary, the digital signature service market is not much more developed in other countries either. Only the market for server-certificates seems to be working abroad. If credit card based payments are made on the world wide web, many users require a secure connection.

Social factors

- Today, there is a strong sense of fear and insecurity globally since the 11th of September, 2001. For markets of security products and services (like IT security markets) this seems to be *beneficial*. Most vendors make use of this fear (and catalyse it) to persuade customers to buy their products and services (even if it has nothing to do with anti-terrorism).
- Hungary and the Hungarian market is different from the global one. According to the dimensions of Hofstede [Hofstede, 1980], the Hungarian society is more *collectivistic* than

western societies. This means, many Hungarians prefer to trade with relatives or friends instead of trading with unknown people.

- As it was pointed out by the interviewee at Giro (interview C.1), the Hungarian society has *very little trust* in the state, in technology, in large companies and in their business partners. Perhaps, frauds are very common in Hungary, or perhaps people just overreact them.

  Lack of trust in organisations may have an effect on the CA business too: if people do not trust company X, why would they trust in anything that company X certifies?

Technological factors

- *Not all aspects of PKI are standardised*, so a buyer may pay for a PKI system that can turn out to be unable to cooperate with other parties, and thus become useless. This is why some customers are reluctant to base their information system on PKI (and digital signature service) and rather choose to wait until the technology fully evolves.

Although there are still some technological factors that slow the spreading of PKI, I do not think that technology is the main reason for this slowdown.

7.3 Buyers

7.3.1 Demand at various customer segments

In this section, I identify various customer segments who may present demand for digital signature service. Each of these segments are targets for one or more CAs. I shall discuss the significance and bargaining power of each segment, and evaluate which of them I consider a good strategic choice.

Individuals: If a digital signature is equal to a regular signature, than anyone who uses regular signatures is a potential customer of digital signature service. This would mean a large mass of people. While masses may have a significant bargaining power, they are seldom organised enough to represent their interests. Although *individuals have little bargaining power*, they *do not need digital signatures* yet.

I reckon, this sector might be very important on the long run, but as long as there are no services for individuals to access this sector is rather a business 'toy', and does not have real significance. Some CAs still offer services for individuals too (this problem is further discussed at e.g. Matáv in Section 7.7.2), perhaps to demonstrate that anyone can have a digital signature. Dealing with individuals is also very troublesome if they are in large numbers, because it requires a network of registration and customer support. I reckon, only Matáv has such a network that could be trained for this purpose.

Small companies: I do not think that the situation of small companies is much different from that of individuals. As long as there are no services small companies can use, they are unlikely to purchase digital signature service. Though, small companies are more rational than individuals, so they are are going to pay for such a service only if they find they can increase their profit with it (while certain individuals may invest in this for fun too). Small companies might find it essential to join PKI if their clients (probably large companies) prescribe them to do so, i.e. when the network economy reaches its positive feedback period. Until that point the sector of small companies is unlikely to be important.

Large companies: I consider those companies in this group, who are 'large' enough to have an internal information system of their own, where not only secure communication is a critical issue, but a centralised management is also required. These companies may benefit from having a 'standalone PKI system', even if there is no 'infrastructure' to connect to, because they can use it for their internal purposes. However, these companies will find it

cheaper to have one of the substitutes (see Section 7.6). For example, they may install a server with a self-signed certificate. They may decreases costs if this server implements less security measures than CAs. It is clear that a CA can implement very secure systems more cost effectively than standalone companies, because a CA issues more certificates, so the average cost is of issuing a certificate is lower.

However, it is questionable if clients need that high security that CAs offer. My interviewee with Data Contact argued that most of their clients do not need so high security so investing in it might be futile. Naturally, any security countermeasure should be designed by comparing the cost of threats (the cost of the damage they may impose considering an estimated probability of such a threat) with the cost of the countermeasure. [Pletier, 2001]

CAs may implement strong countermeasures more cost-effectively than their clients, so it might worth for clients to outsource it to CAs. However, outsourcing is risky by itself (see Section 7.3.2), so many clients consider it safer to implement weaker countermeasures, create less secure systems, but retain the control of their security system.

The sector of large companies is an important one, but *substitutes are very dangerous in this sector*. Especially, because clients of this sector are companies and are thus profit-oriented. They will locally consider if it is cheaper and/or safer to use a substitute or use PKI itself, because they need to produce profit locally. Governmental organisations might rise over their local interests and invest in systems that pay off globally (or domestically). Very huge (probably multinational) companies might have a large enough system (located in many countries) that can receive similar benefits from PKI.

If CAs are able to gain customers in this sector, they might accumulate enough digital signature users to help this technology spread, and make the network economy have positive feedback. As far as I know, most attempts of Hungarian CAs to conquer this sector have failed so far, and these CAs rather try to sell their services to the government now. (see

interviews)

Naturally, *large organisations have very strong bargaining power*. However, larger organisations may decide not to buy digital signature service but to use one of its cheaper substitutes instead.

However, there is one particular use of digital signatures that does have significant demand at companies that have many clients. If digital signatures could be used in *electronic billing*, they could significantly reduce paperwork. Unfortunately, APEH currently requires companies to present paper-based bills and receipts in case of an audit, so this use of digital signatures has ran into administrative obstacles. If tax regulations change in the future so that solely electronic receipts can be accepted too, PKI might be a suitable technology for this purpose. However, APEH may decide to create a dedicated CA for this purpose, which would shipwreck this business of commercial CAs.

E-commerce corporations: These companies can be small or large, but they are all IT-driven. They are all at the third stage of the model of [Lindström and Andersen, 2000]. Generally, these companies has a web-based store that – one way or another – sells goods to its consumers. Web-stores obviously mean an important market for CAs, as they process sensitive payment information of their customers. Some works ([O'Brien, 2000]) suggested that most companies should become ECCs to a certain extent, but it seems that this did not happen. (see Section 6.2). While ECCs perform well in some areas, they completely failed in some others. Hungarian web-stores are generally less successful than global ones, this can be explained by the argument of my interviewee at Giro who said Hungarian people have less trust in technology. Many Hungarian web stores do not process payment information online but handle payment by other means (perhaps, for the aforementioned reason), so they might not even need a certificate.

Today, it is widespread that web-stores present a PKI certificate to their customers and the

lit 'lock symbol' of the customers' browsers ensures security to their customers. [**?**] argues that vendors gain competitive advantage from the lit lock symbol and not from the secure connection, and these two often have nothing to do with each-other. Among Hungarian CAs only certificates of Netlock are accepted by most browsers, others are usually rejected. Surveys like [Krasznay and Szabó, 2001] suggest that Hungarian customers know even less about Internet-security issues and countermeasures, so I am afraid, most of them probably do not even know of the lock symbol of the browser.

It used to be a widespread belief that only web-stores (severs) have a certificate today, their clients will have certificates in the future too. This way, clients would not be able to cheat, and identifying them would be easier. Business did not follow this trend. As the work [Ellison and Schneier, 2000] points out, vendors did not choose to exclude clients without a certificate, but rather tried to attract more and more customers. They also decide to trust clients (and rather allow them to cheat) and do not wish to identify them, while clients seem to prefer to retain their anonymity. Ellison and Schneier claim that the market seems to work this way, and neither clients nor vendors seem to be interested in changing the underlying technology. This way, *CAs can sell only one certificate per vendor*, and not one per vendor and one per customer.

There are surprisingly many myths and misbeliefs about the potential of this market. For example, the survey found that only 0.1% of Hungarian servers are secure, because only they have a valid certificate (accepted by law). On one hand, a certificate cannot make a server secure, it can only secure communication with it. On the other hand, *not all servers need secure communication*. For example, communication with a website that provides information (just like a newspaper) need not be encrypted. Anyone can access that website (or buy a newspaper) and get the same information, so why should anyone sacrifice resources to encrypt it?

Hungarian web stores are not as popular as global ones (in proportion to the targeted population). The low number of speakers of the Hungarian language also limits it. Moreover, various surveys ([Kopint-Datorg, 2001a]) find that the number of Internet users is very low in Hungary. Not only compared to Western societies, but compared to other countries of the Central Eastern European region too. Again, the number of Hungarian Internet subscribers does not seem to have increased in the past years, only the proportion of broadband subscribers increased rapidly.

I found that the potential of the market of ECCs is much lower than it was expected a few years ago. Perhaps, it is also significantly lower than CAs perceive it today. Substitutes are very strong in this area, especially simple ones like SMS based payment. Although this market is working worldwide, in Hungary it is stagnating.

Companies providing services that require secure communication: For these companies, PKI can be one alternative. End-users of these companies usually do not require PKI, they require a secure service they can use. Both of my interviewees at Data Contact and NetAlfa claimed that their customers are very sensitive to the price of the service they receive and are willing to make a tradeoff between price and security. Microsec is a good example of selling PKI-based services successfully. However, it seems (see Section 7.7.4) did not wish to purchase service from any of the available CAs, but decided to set one up on its own. As Data Contact seems to be doing something similar with an unofficial CA, it seems that *companies that do have the expertise to apply PKI, also have the expertise to make an own (probably less secure) CA or select and install a more cost-effective substitute*.

Banks: I reckon, banks could be a very important sector in this field. If banks would identify their customers by means of PKI, this sector would distribute certificates to almost the entire Hungarian population. After the infrastructure was ready (and banks would have to

build a good infrastructure with reliable registration), other organisations could use it. (As in some countries a credit card is often accepted as a document for identification.)

As all banks could make use of PKI, the CA of Giro was established to provide PKI services for them. Unfortunately, this CA still withdrew from the market, because of lack of demand (see interview with Giro, and see Section 7.7.1). My interviewee argued that the cost of frauds that could have been prevented by PKI was relatively little, so banks found that the cost of countermeasures exceed the cost of the fraud. I reckon, banks seek to find a way to incorporate PKI into their systems, but they are searching for cheaper alternatives than those that CAs offer.

Non-profit organisations: These organisations might be very large, but sometimes they are unable to pay for PKI. In case they need secure internal communication, they have to use one of the cheaper substitutes (like PGP). They may join PKI if somebody donates them the service. This may be the government or even one of the CAs. According to the rules of the network economies (see Section 6.1.1), CAs might find it a good idea to provide digital signature service to such organisations free of charge. The more users they attract to digital signature service, the more valuable the service becomes, so the more likely other organisations will demand it too. If this organisation is well-chosen (e.g. a university that educates IT specialists), the CA may gain additional competitive advantage.

Note that if the CA requires that the signature creation data has to be protected by a smart card, then the marginal cost of selling digital signature service significantly increases (that has to be covered either by the end-user or by the CA.)

Military organisations: Such organisations are non-profit, but are able to pay for expensive products and services. The centralised philosophy of PKI also meets the requirements of such organisations. Yet, *I do not think that military organisations will become customers of CAs.*

CAs offer service for commercial use. A digital signature service a CA offers can never be trusted more than the CA itself. This is why I strongly doubt if small CAs have any possibility to issue certificates to huge organisations. (see Section 7.7.5) *In case of military organisations, secure communication is* one of the most critical tasks. Such *a security critical task should never be outsourced* to less trusted organisations. The adversaries of military organisations can be very large entities with a vast amount of resources. Such entities can even purchase private companies to alter their behaviour, etc. I reckon, if a military organisation needs PKI services, it should establish its own root CA, outsourcing this task is a serious mistake.

Government: Most of my interviewees at CAs considered that the government should have an important role in catalysing the spreading of PKI. My interviewee at Giro argued that in every country where PKI could spread, the government had an important role. Let us assume that almost every single citizen could benefit from PKI (at least in the far future) if the infrastructure was ready. However, as long as the infrastructure is not ready, and the network economy has no positive feedback, it is worthless. Today, few organisations wish to build their own part of the infrastructure, but rather choose one of its locally cheaper substitutes. They are afraid that other players do not build their part, and the infrastructure will have a positive feedback in the increase, so their investment would never pay off. Thus, it seems logical that the government should pay for PKI, this way every single citizen would pay for it, and they all receive a guarantee that the full infrastructure will be established.

Digital signatures could be a good solution to make the internal communication of governmental offices more efficient. Examples for this are local governments or organisations that belong to PSZÁF that are the main target customers of Máv Informatika and Netlock. Various e-government solutions may also improve efficiency and allow citizens to access

governmental services in a more comfortable way. Moreover, improving the infrastructure, thus improving the competitiveness ([Findrik, 2002]) of the country may benefit the government when attracting investors. The centralised, hierarchical philosophy of PKI better suites the government, than most other substitutes. (see Section 7.6)

While the government may require PKI for its own purposes, the economy and individuals (who compose the state and elect the government), not necessarily require it. PKI is a centralised architecture that allows (among many other things) the identification of individuals, and gives a basis to parties for trusting them to be who they claim to be. In this sense, it is similar to the system of personal ID documents. While some economies invested vast resources to develop and maintain personal IDs, some others (like that of the United States) perform very well without having such documents. It is not obvious that PKI is a must.

However, the government can not only bring blessing to CAs, it can bring doom too. If the government needs PKI for its own purposes, why would it pay to private companies? If the government appears as a competitor, many private CAs will be out of business.

7.3.2 Problems with PKI

Some clients find that PKI suits their needs but they find it too expensive (see interview with Giro). However, there are some problems with PKI. It is no magic bullet, it will not make all systems secure. Some clients may find that these difficulties are severe and (while acknowledging some benefits of PKI) chose not to invest in it, because they find that it does not solve the problems they have.

[Ellison and Schneier, 2000] listed several weaknesses of PKI in their article. Here, I will mention two ones that I consider particularly important for the purpose of this dissertation.

- A CA is not an authority but a company. Why should we trust it?

- Digital signatures are not created by users but by their computers or smart cards. If the computer is infected by a virus, the user cannot control what she signs.

See Appendix B.6 for a detailed explanation.

7.4 Suppliers

The costs of setting up a server that performs the functionality of a CA are minimal. A computer needs to be bought, with a connection to the Internet. There is free software available that can issue certificates, handle revocation lists, etc. However, a server that can issue certificates is not a CA yet.

There are several security requirements a CA has to fulfil. Some of these are prescribed by the law, some of these by common sense. Some others are enforced by CAs themselves in order to gain competitive advantage by demonstrating that they are more secure.

For example, a CA needs to store its signature creation data (that is used to issue certificates) in a secure environment. People should be identified before accessing the building of a CA, well-defined security policies should be elaborated and enforced. This means a CA should have suppliers like security guards, security system providers, etc. A CA might decide to operate in a building with special walls that are not only hard to be breached but also shield against electromagnetic emanations, etc. Establishing this environment can mean *high fixed costs*.

In this secure environment CAs usually choose expensive softwares to operate. Hungarian CAs use products from Utimaco and RSA Laboratories to provide CA functionality. These are global companies, and the Hungarian market does not mean significant business to them (even if it would boom). This means, Hungarian CAs do not have any bargaining power towards them. A CA might need special devices to generate good quality signature creation data (cryptographic keys), which can also be very expensive.

CAs need financial stability and a good reputation. They have to select their employees carefully and may not employ anyone with criminal history.

In order to issue a certificate, the client needs to be registered. This means personal contact, but some CAs also strengthen this procedure by additional countermeasures that may mean additional fixed costs. For example, Matáv also checks registrants in the database of the Ministry of Interior.

Operating a CA that complies with all regulations is costly. Apart from high setup costs the yearly upkeep costs are in the hundred million forint magnitude. *CAs have little or no bargaining power towards most suppliers. Many of them mean high fixed costs that are unavoidable even if the CA issues very few certificates.*

7.5 New entrants

Since the certificate market did not become profitable yet, not many CAs are currently trying to enter the market.

As it was explained in Section 7.4, operating a CA is costly. Although these costs do prevent the entry of the smallest companies, it is not beyond the possibilities of larger ones. For giants like Matáv PKI is not even a large business unit now.

A trusted CA has to undergo rigorous certification, and has to comply with the requirements of the Hungarian laws, and the Communications Authority. [Communications Authority, 2004] Not many companies possess the *expertise* to fulfil such requirements. I think, the certification procedure and complying with all the requirements of the Hungarian law is one of the most important barriers of entry to this market.

Hungary is going to join the European Union in May, 2004. This would allow foreign CAs to enter the Hungarian market. However, this is not necessarily a new threat. The law on digital signatures already prescribes the acceptance of certificates of European CAs. Meanwhile, certain

regulations (or lack of regulations) may prevent foreign entities to enter Hungary.

I think, the most important factor that prevents foreign CAs from entering Hungary is the need to set up registration authorities. Registration always needs to be done locally. While OTP sent an executive to America to receive a certificate from Verisign (see Section 7.2), large masses are going to do the registration locally. My interviewees expressed little fear from competition from foreign CAs. (see e.g. the interview with Máv Informatika)

However, global (American) CAs do mean an important threat in some other areas. For example, the survey of Netlock ([Origo.hu, 2003]) found that most valid Hungarian server certificates were issued by foreign CAs. Although they are not automatically accepted by law, they are often accepted in practice. As most users use American software (Microsoft Internet Explorer or Microsoft Outlook), they automatically accept certificates that are installed into these software. According to [Rosenberg, 2001], only the certificates of Verisign and Entrust are accepted by a large enough percentage of web browsers. This means that while certificates from some official Hungarian CA's are automatically rejected, some certificates from CA's not accepted by the Hungarian government are automatically accepted. Netlock is the only Hungarian CA whose certificates are accepted by Internet Explorer (that has the largest share on the browser market). My interviewee at NetAlfa said this would be one of the main reasons why he would choose Netlock.

I reckon, the threat of new entrants is more significant in some areas than most CAs admit.

7.6 Substitutes

The trivial substitute to digital signatures are regular paper based signatures. However, we can consider that CAs sell *basis for the proof of trust*, so a customer of a CA is able to prove to a third party that she is who she claims to be. In this case a vast amount of substitutes appear in addition to paper based signatures. Some of these solutions are IT based, some are not. Some of

these cost money, some of these are free.

7.6.1 Customer requirements a certificate can fulfil

If we define the market 'the market for digital signature service', the trivial substitute is the regular signature of a notary certifying that the user's signature.

We can also define the market by observing the need of customers the product or service fulfils.

Customers would like to trust their business partners. If we define trust as trustworthiness, a digital signature surely cannot fulfil such a need. We can also *trust somebody to be who he or she claims to be*. A certificate fulfils this need, because based on a certificate a user can gain confidence that the owner of the certificate is the one he or she claims to be. While this problem appears in the real world too, it has extreme importance in the virtual world of e-business. Moreover, the owner of a certificate can *send* digitally signed *messages* that are *authentic and non-repudiable*. [Schneier, 1996] This means, if the certificate owner turns out to be untrustworthy, it can be proven to any third party (e.g. in court).

Thus, the need a certificate or a digital signature service fulfils is *basis for trust* or *basis for secure and authentic communication*. Now we can examine what substitutes fulfil the same need.

7.6.2 Possible substitutes

In this subsection I will list various types of substitutes I could collect. I will start with those that are very close to the digital signature service, and move towards those that are non-IT methods of gaining confidence in the identity of a business partner. Many of these substitutes do not provide all the benefits of digital signatures (or PKI). However, they do provide certain benefits that CAs offer to users when selling their service.

I apologise if this section is hard to understand for non-technical people, but it is still interesting to compare it with the view of CAs on this topic in Section 7.6.15.

7.6.3 Using a certificate for an unintended purpose

This substitute means buying one kind of service from a service provider and using it for some other purpose that only a more expensive service (of the same provider) could fulfil.

There are several type of certificates, each of them may have a different purpose and have different restrictions. Some of these restrictions are posed by legal regulations, some of them by CAs to segment their market. For example, every CA sells certificates for individuals at a different price (usually cheaper) than certificates for organisations. Another example are the monetary value restrictions of Máv Informatika, or the differentiation between server certificates and certificates for digital signature. Since the technology behind them is the same, using them for another unintended purpose might be sound in some cases. Naturally, our business partner must accept these certificates. Some software may reject such misused certificates, but some of them may accept them if configured properly.

It is questionable if this solution is a substitute, because the user of this solution does buy service from the digital signature service provider. However, the user pays significantly less money than the CA would ask for the original service.

7.6.4 CA with self-signed certificate

The substitute means setting up an own CA to issue certificates. In case the certificate of this CA is properly signed by a higher level CA, we already speak of a new market player and not a substitute vendor.

If the certificate of this new CA is not signed by any other CA, it is not connected to PKI, so any third party cannot verify certificates this CA issues. (This is why I call this solution a substitute and not a competing product.) Such an unofficial CA usually issues a certificate to itself so it is called a self-signed certificate.

However, those who receive this certificate in any authentic way (e.g. personally), can commu-

nicate with any person or server this CA issued a certificate to, just as if they were members of PKI. For example, if a company installs a CA for itself, it can install its certificate on all of its workstations.

The *cost* of this substitute is *minimal*, because setting up a working CA is not significantly more than operating a web server (even free software exist for this purpose too), most costs of a 'real' CA are related to having a certified secure system. (See Section 6.1.2.)

No doubt that *many companies choose this alternative* to purchasing real certificates. My interviewees at NetAlfa and Data Contact both mentioned that their company is using this substitute to PKI.

Note that if users who cannot acquire the self-signed certificate of the CA in an authentic way cannot have secure communication with owners of certificates signed by this CA.

7.6.5 'Piggybacking' a certificate

This rather tricky solution is an extension of the above one. It provides an authentic way to acquire the self-signed certificate of the CA using a regular PKI certificate. In this solution, the CA with the self-signed certificate purchases *one* regular certificate from a digital signature service provider and enables users to establish secure communication with its web page. The CA also publishes its self-signed certificate on this authentic web page. This way users all over the world are able to download the CA's self-signed certificate, and are thus able to verify all certificates this self-signed CA issued (and thus the digital signatures of the self-signed certificate CA's customers). Naturally, it is possible to buy a special certificate setup an official PKI sub-CA, but such certificate has additional very high costs and legal requirements. All CAs sell this kind of sub-CA or VCA service (see interviews with CAs), but it is only available to premium customers.

This way, *one product is bought, and even millions can be resold* (or given away free of charge).

In the physical world this is impossible, but in a network economy (Section 6.1.1) this is typical. However, in many network economies copyright laws govern this field of business, so 'pirates' are not allowed to sell copies of copyrighted software or other media.

The digital signature provider business is not fully a network economy, copyright laws do not apply for this situation. Actually, the above CA does not 'copy' anything. It provides a way for users to *transfer the basis for trust* to other parties.

For example, my interviewee at NetAlfa considered this solution. NetAlfa does not wish to purchase a certificate for all of his domains, but considers it important that its users can access the company's websites securely.

This substitute is notable, because it provides *all the functionality of PKI*. Its cost is minimal (only one certificate is purchased and a working unofficial CA is set up). However, I do not think this substitute is dangerous for digital signature service providers for the following reasons:

- It is rather uncomfortable for a user to download and install additional certificate. In a PKI system this is not necessary. While one can do this for the regular business partners, installing certificates all the time is annoying.
- One has to understand the way PKI works very well to understand which certificate is risky to install and which is not. (Installing every certificate you see is definitely dangerous.)
- Hierarchical solutions are extremely uncomfortable (and possibly dangerous), so they cannot be implemented on large scale.

While it is unlikely that such service providers would successfully compete with CAs, their clients can (and tend to) develop such semi-PKI-based solutions that avoid CAs. My interviewees at Giro and Máv Informatika both complained about this phenomenon.

7.6.6 PGP (and similar solutions)

'Pretty Good Privacy' (`http://www.pgpi.org`) is a free product that allows users to send and receive/verify digitally signed messages, so it is a substitute to PKI. In PGP, no CA or no central system exists, everyone is responsible for his or her signature. People publish data that can be used to verify their signature (this is similar to a certificate), and people – who know and trust each-other – sign this data (so called public key, see Section B) for each-other. Thus, everybody may issue certificate-like information.

Naturally, if unknown people certify something, this information cannot be relied upon. However, if you receive a message from someone who's public key was countersigned by someone you know (and whose public key you have obtained authentically), you may place some trust upon the sender of the message.

Users of PGP form a huge, ad-hoc community, a *web of trust*. Although it is a very chaotic system, it may provide some good results. PGP is free, and small communities can benefit from using it too. However, it does not guarantee that two members of a PGP web can obtain each-other's public key (certificate-like information) authentically. Perhaps, this is why I do not know of any large commercial organisation that uses a PGP-like system for critical communication. (However, a non-profit organisation, Debian, the provider of the largest non-commercial Linux distribution, does use a PGP-like system to secure all of its communication and to deploy its products and services to its users.)

PGP is widespread in many communities, especially in non-profit organisations that cannot pay the costs of PKI or other expensive systems. PGP is often considered the 'poor man's tool for digital signatures', but I find that more and more people express that PGP better suits their need than PKI (see the interview with Data Contact in the Appendix). Users of PKI are *told* whom to trust, they have to trust in the hierarchical system. If a PKI user connects to a partner in a foreign country, she needs to trust the foreign CA who issued that partner's certificate, while the user

has little or no knowledge on that country's laws and that CA's security procedures. (Some CAs issue certificates with much easier and much less secure registration procedures. [**?**]) If there is a chain of CAs to that CA, a PKI user has no other alternative but to trust all CAs in the chain. (see Appendix B.3)

In contrast to PKI, a PGP user can *select* whom she trusts, and she can also select if she wants to trust people trusted by whom she trusts. While a PKI user is usually – one way or another – certified by her government, a PGP user may choose not to trust her government. (Perhaps, PGP suits more the security conscious – or paranoid people.) If a PGP user connects to an unknown partner, she (her software) finds many alternate links in the web of trust to the partner. For example she can see that three of her friends considered this partner trusted (and perhaps so did many other people whom she does not know), so she may decide to trust her. *PGP users make decisions based on the decisions of people they know, and not based on the decisions of governments and large companies.*

Having received significant funding from many governments, PKI is still struggling and is on the edge of existence. On the other hand, PGP received no funding and is blooming in certain communities (e.g. universities). I think, *though PGP might suit the need of users better, PGP is unlikely to receive any funding from governments*. PGP is a distributed system with no central authorities, and governments prefer centralised systems where there is a 'Big Brother' who can see everything. PGP can also be an excellent tool for criminals and terrorists to exchange encrypted messages. (PGP is banned and restricted in many countries. The United States failed to prevent PGP from being exported and this led to the revision of US export control regulations.) [Gimon, 1995]

I think there are other problems with PGP that prevent it from knocking PKI out. Being a distributed (not centralised) system, it is not obvious, who is legally responsible if there are any defects. Again, it might be easier for a criminal to get a position in the web of trust, because the criminal needs to trick everyday people and not security experts of a CA.

Although PGP might better suit the needs of users than PKI, I do not think, PGP could take the place of PKI.

7.6.7 Other home-grown (IT) solutions

Various other solutions may exist for other secure electronic communication. They are all accepted by the law to be authentic, if both sides agree to accept it in a contract.

Such solutions may rely on IT to a certain extent. One extreme solution is the fully automated and computerised EDI (Electronic Data Interchange) that is often used in supply chain management. However, such solutions can be quite simple too. For example in book [Follett, 1978], two World War II spies (who work for the same side but never met before) establish a secure channel between themselves in the following way: Both agents show up at a specific street at a specific time, and they are carrying a Bible. One of them asks the question 'What is today's chapter?' and the reply is 'One Kings thirteen'. After this, they start a conversation on the chapter. If both of them made sure that they were not followed, they agree on that this chapter is 'most inspiring', otherwise one of them would make an excuse 'I am afraid, I haven't read it yet.' Although no computers were involved, this is an IT solution indeed.

The common flaw of many similar solutions is that the parties need to *exchange a confidential* piece of *information* (or sign a contract) *in advance*. This makes the use of such solutions awkward when two parties need to authenticate themselves and make business on the fly. However, if two parties did agree on such a password in a secure way, the *cost* of secure communication is *minimal*, so they may mean competition to PKI in certain fields.

7.6.8 Regular (unauthenticated) email messages

While many companies base their communication on this technology, it should be clear that it provides *no protection against IT specialist attackers*. Some very basic knowledge is enough

to intercept, alter or counterfeit email messages. Many users and many companies are not conscious of this threat, this is the main reason I consider it an important substitute. Yet, against non-specialists even this simple technology may provide some very low degree of protection. [Office of the e-Envoy, 2002], a set of IT security guidelines prepared by the UK government identifies this a countermeasure, but a very weak one. CAs should establish the demand for more secure solutions by educating users and explaining them the threats they are exposed to when using this solution. Though, not very aggressively, some CAs are doing this.

7.6.9 Payment via SMS

This solution is simple and easy to understand for every user. Users who would like to pay a small amount of money at a website, can do this by sending an (extra cost) SMS to a phone number found on the site. They instantly receive a password by SMS to access the site. This way, they pay the money from their mobile phone account.

In this case, the communication itself is not as secure as if PKI was used. (The PKI solution is the following: The user accesses a website via a secure PKI connection, enters his or her credit card number, and the vendor receives the money from the user's bank.) However, paying by SMS fulfils an important customer requirement: it protects the interests of the customer if the vendor is malicious. Unfortunately, some vendors charge more money that the service costs. Some vendors 'fail to receive' the user's message if the user calls of a subscription. Sometimes the vendor does not have a secure server to store credit card numbers, and crackers can obtain this confidential information. Sometimes the user even has trouble complaining at the bank.

Users feel more secure to pay via SMS, because they can have more control over when they pay, and the vendor does not receive any confidential information. Users can even control how much they pay: On one hand, an SMS cannot cost as much as a credit card transaction. On the other hand, most users have a pre-paid mobile phone account, so they do not put more money to risk than they have on their account.

This solution is spreading very rapidly, and is often used in business solutions for payment. Payment via SMS does not fulfil in important requirement credit card number based payment (via PKI) seems to neglect: it gives protection against malicious partners. It seems, customers consider this threat more important than others, so they are willing to be subject to other threats. (They not only download the phone number via an insecure channel, but they also use a phone company as a bank.)

7.6.10 Paper-based signature

The classical equivalent of a PKI-based certificate is the handwritten signature of a person (and some other data) countersigned by a notary. This solution is not only awkward, but most business partners do not (and cannot) verify the notary's signature. An attacker may not only try to counterfeit the users signature, but may also attack the notary's. To gain more confidence in the identity of a person (or company), some companies request additional documents that are not much harder to counterfeit. However, if one party would question the signature to be real, a court does have enough resources to verify it.

In spite of its security flaws and inconveniences, this solution is the most accepted one today.

7.6.11 Personal meeting

Meeting someone personally and taking a look at his or her *ID card*. Gives us some confidence that this person exists, and we deal with this person. In case we do business locally, this is a *very secure solution*. (Naturally, we assume that we can tell the difference between a real ID card and a counterfeited one.) However, this does not work if the trading parties do not meet.

7.6.12 Dealing with friends or relatives

Another widespread approach is also simple: not to deal with strangers if possible. People in collectivistic societies prefer to trade with their friends or relatives, or their friends' friends or friends' relatives, etc. They prefer to approach a partner if someone (a friend or relative) advised them to do so.

Note that this approach also provides some confidence on the *trustworthiness* of the partner, while PKI only proves his or her identity. Naturally, this solution is simple and easy to use. However, if it is not necessarily cheap, because the friends or relatives might not be the cheapest provider of the product or service we seek. (The above mentioned PGP is based on this real world principle.)

7.6.13 Prestigious organisations

If people have no friends, but would like to turn to someone (or something) they know, they may approach well-known, prestigious organisations. Practically, they may seek advice from *brands*. If a building has the McDonald's sign on it, people may assume it to be a McDonald's. Thus they can trust it to hold McDonald's quality standards. Although this works quite well in the physical world, on the Internet it is not so simple. Sometimes crackers hijack connections to the websites of known, prestigious organisations, and users see the cracker's malicious website in their browsers. This website might be totally identical to the original, but it performs malicious activities too (e.g. stealing credit card numbers).

Unless the organisation is properly authenticated (e.g. by PKI), this solution does not guarantee the same safety as it does in the physical one. *Relying on this approach alone in the virtual world is unsafe*.

7.6.14 Blind trust – human stupidity

We speak of blind trust if we trust someone we have *no reason to trust*. Even though it sounds irrational, this is not uncommon. People have much less experience in the virtual world, and they often fall for the very simplest tricks. People in the physical world have learned not to trust strangers without limits, but still, several frauds exist.

For example, if a complete stranger approaches you and asks you to lend him money, most people refuse. (Or at least, they would like to see some guarantee that the person would give the money back.) People will learn not to trust anything they see on the Internet, and will also learn that the ownership of a website, a domain name or an email address does not say anything about the identity or trustworthiness of the owner.

People have also learned (at least in Hungary) that whenever they leave their home or their car, they should always lock it. Soon, people will have to learn the same about their 'virtual doors' and security systems of their computers.

Until people become more experienced in IT security and will think consciously about it, *blind trust should be considered as a substitute*. Today, the vendor of any IT security product or service has to demonstrate to its customers not only that the product or service is a useful countermeasure against certain threats, but the vendor also need to explain that the threat exists and are common.

7.6.15 Are the CAs conscious of these substitutes?

Each interviewee was asked the question: 'What can customers use instead of a digital signature service?'

- My interviewee at Máv Informatika named handwritten signatures or regular unauthenticated emails. (He did mention the case of APEH, but he did not identify that they lost market because of a substitute.)

- My interviewee at Matáv answered that there is no electronic substitute.
- I could not interview anyone from Netlock. However, in their published survey ([Origo.hu, 2003]) they differentiate between two classes of web servers: *insecure ones* and *those that use PKI*[2]. There are several similar articles and press releases on the website of Netlock, many of them emphasise the use of PKI.
- I did not directly ask the above question from my interviewee at Giro, because she mentioned many of the above substitutes in the interview. (see Section C.1) I found it only at Giro (the market player who withdrew) that substitutes were thoroughly considered.
- While I have not met most of my interviewees before, the interviewee at Microsec used to be a college of mine. Perhaps, this is why at certain questions of the interview (including this one) she became very cautious and was expecting a trap (generally she was right). Thus, I should not compare her answer with that of others.

I found it astonishing that most CAs only name handwritten signatures or unauthenticated emails as substitutes to their own services. However, each of them suffer from lack of demand (lack of security conscious way of thinking in the public, according to my interviewee at Giro), and they also suffer from the phenomenon that their potential customers develop their own home-grown solutions (see the case of APEH in the interview with Máv Informatika).

I think, PKI solves problems that people have, so the number of PKI users will grow. Though the market for PKI services is growing slowly, sooner or later it should reach the point of positive feedback for the network economy.

I reckon, the greatest threat to this market is the threat of substitutes because they may limit the size this market can reach, and thus may prevent it to reach the positive feedback period. Substitutes are dangerous, because it is usually cheaper for the client to apply a substitute locally

[2]Note that PKI does not make a server secure. It can make the *connection* to it secure. Note that the above mentioned document was a press release and not a scientific paper.

than to connect to a world wide infrastructure. Blind trust is the cheapest on the short run, but the costs of fraud and security breaches should be taken into consideration on the long run. (Tough, surprisingly an expected wave of frauds did not come yet, according to the interview with Giro.) I consider the various home-grown substitutes around the top of the list the most dangerous ones that can make this market suffocate.

I am surprised that CAs are not combating substitutes more consciously.

7.7 Competition and the competitors

The market of CAs is a new one. The companies that entered the market in the past years, could enter only by creating *startup CA*. (E.g. it was not possible to enter the market by acquisition of an existing CA.) The new CA could be a startup company or a business unit of a larger company. The CAs are either small companies or small business units of large ones. If they would like to grow, they have two possibilities. One of them is to increase market share, the other one is to make the market grow. Currently the market is too small for five CAs, perhaps it is small for even one.

Although the market cannot sustain all five CAs they did not seem to have started a competition to death. Instead of ferocious competition these companies rather *coexist*. It is interesting that small companies (that have no other business units) are trying to penetrate the market to cover their costs. Meanwhile, larger companies are rather passive. Perhaps the market is not large enough for them to be interesting, and there is no urge for them to cover the costs.

I discuss market players in alphabetical order.

7.7.1 Giro

Giro Elszámolásforgalmi Rt is an inter-bank clearing system (`http://www.giro.hu`) owned by several Hungarian banks. An inter-bank clearing system needs quick but secure communica-

tion channels. Since many banks cooperate in this clearing system, basing this IT system on PKI and certificates seemed to be a good technical solution. However, a certificate is as trusted as the CA that issues it, so Giro considered to set up a CA itself.

Giro was among the first three companies who entered the market when the law on digital signatures was passed. Moreover, Giro was the *first who* (at least temporarily) *withdrew*.

Giro was primarily interested in the market niche of banks, and showed no intention of leaving this niche. Although, the niche of banks involves very few companies if banks would supply all of their customers with certificates, this niche could cover almost the whole Hungarian population.

Within this strategically important market niche Giro had an enormous competitive advantage. Not only the fact that they had the expertise to operate a critically secure system that their clients were familiar with, but their reputation and their history of operating this system was also a great advantage. My interviewee at Giro pointed out that practically no other CA had enough reputation to compete with Giro in the sector of banks. If a bank had chosen another CA to implement a PKI based system, and if there had been any problem with the security of the system, the security manager of that bank would have had to explain why not Giro was chosen.

Giro was in a very special (probably more advantageous) position on this market. Since its owners are its most important clients, it is not their primary interest that Giro should make profit. The owners of Giro are interested in receiving a secure, reliable and *cheap* service. This means, Giro is not fully profit-oriented like the other CAs. This means, Giro could afford to issue certificates without making profit with them on the long run.

As Giro worked for only one business sector, its services could be more specialised. Unlike other CAs, Giro was not selling certificates directly, but allowed its clients to perform the registration of users, and issued certificates based on this registration. Naturally, only distinguished companies could become clients of Giro who were not likely to make frauds around the registration. To the best of my knowledge, Giro did not issue server certificates.

The high reputation and the smaller profit margin and the specialisation made the position of Giro very promising on this strategically important market. According to my interviewee, Giro was able to offer services cheaper than its competitors. There is a large bank that was originally affiliated with Matáv, but decided to chose Giro later, for financial reasons.

Yet, instead of penetrating the market, Giro decided to withdraw. My interviewee reasoned that they did not see any demand for digital signature service at the price they offered it. Giro could issue only a few thousand certificates at the price of 2000-3000 forints, while the yearly upkeep costs of the PKI business unit were in the 100 million forint magnitude. Giro refused to lower this price by reducing security, because insecure solutions could have spoiled the reputation of the inter-bank clearing system. For example, Giro issued certificates on smart cards only, and refused to do it otherwise. My interviewee said that they did not see that the demand would rise in the near future, so Giro stopped cross-financing its PKI business unit. According to my interviewee, the business unit is now hibernated, and will be revived if demand would rise. (My interviewee at Matáv did not mention Giro as a future competitor.)

It seems to me that while most banks understand the benefits of PKI, they do not wish to pay for establishing it. As long as their customers do not require it, they do not wish to raise prices because of PKI, and they do not wish to lose profit either. Again, as long as in the areas where PKI could benefit security the costs of fraud are lower then the costs of the security measure, the security measure will not (and should not) be applied. My interviewee pointed out that in certain critical fields (like home banking) we cannot speak of any history of significant fraud.

Giro was first in the market and was in a very attractive position, but still large investments have to be done to establish the market. Perhaps, the sensitiveness for risk in customers (the society) should be established to raise demand for PKI. Giro refused to perform this large investment, and decided that it is the task of the remaining market players. Perhaps, Giro decided to lose the money already invested.

The example of Giro also supports the view of [Coltman et al., 2001] that being first on an IT

market is not necessarily a good thing, and it does not ensure success.

7.7.2 Matáv

Magyar Távközlési Részvénytársaság (`http://www.eszigno.matav.hu`) is one of the largest IT companies in Hungary. It used to be the only Hungarian telecommunications company. The CA of Matáv is one of its business units, compared to the other businesses of Matáv (telephone service, Internet service, etc.) the CA business unit required relatively little investment.

Matáv has an enormous competitive advantage: the company has access points everywhere in the country, it has direct connection to most individuals, etc. Surprisingly, Matáv does not seem to make use of this advantage, and is currently not a very active player.

Among the companies I interviewed, Matáv was the only one that seemed to be interested in the sector of individuals and small businesses. Personally, I do not think that there is any possibility for profit in these two sectors in the near future. I do not see why large masses of individuals would purchase digital signature service as long as there is no infrastructure present. Before this network economy reaches its positive feedback period (see Section 6.1.1), *individuals cannot use this service for any useful purpose*. In particular, I disagree with my interviewee at Matáv, I do not think a group of friends would ever invest money to use PKI for exchanging emails. They would use PGP (see Section 7.6) which is free and may better suit their needs. (See the interview with Data Contact in Appendix D.2.) However, if the infrastructure was already present (and each of them already had a PKI certificate), it would require no additional investment for them to use PKI, so PKI could provide the most simple solution. While the law allows that certain e-government services (like tax returns) can be handled electronically – protected by qualified digital signatures – as long as organisations (like APEH) do not specify the exact format of these documents, such possibilities remain theoretical only.

Naturally, Matáv also offers services for *large organisations*, and also offers a VCA service to outsource the registration function. (This service targets a similar sector to the sub CA of Máv Informatika and the services of Giro.) I think, *this latter sector is the most promising one* that is likely to be profitable in the foreseeable future.

As it was pointed out by my interviewee, unlike Netlock and Máv Informatika, Matáv invested a relatively small amount of resources into the PKI business. I think, Matáv considers this market a dog that may have a potential to become a star. I reckon Matáv exerts minimal effort to maintain its presence on this market.

If the market reaches a size that is interesting for Matáv, then perhaps more resources will be invested. In that case Matáv will have a history of operating on this market from the very beginning, and will also have expertise in this field. Being the most powerful of the three active market participants, it will be relatively easy to seize significant market share. This means, Matáv can afford short term losses (that are large for other companies but still small for Matáv) in this field and may remain in this market and seize it if it booms.

I reckon, if Matáv consciously follows the strategy of passively waiting until other players establish the market, it might be very effective in the future.

7.7.3 Máv Informatika

MÁV INFORMATIKA Kereskedelmi, Szolgáltató és Tanácsadó Kft (`http://www.mavinformatika.hu/ca/`) is a middle-size IT company that was founded by MÁV (Hungarian Railways) in 1996 when MÁV outsourced its IT functions to its subsidiary. As years passed, Máv Informatika became less and less dependant on contracts from MÁV, while MÁV is still the 100% owner. Máv Informatika ventured into various IT businesses like the digital signature service provider business. Together with Netlock, Máv Informatika qualified for issuing certificates for qualified digital signatures.

Máv Informatika is a very active player on this market. I think, Máv Informatika is either the market leader or the challenger of Netlock for this position. According to my interviewee, these Máv Informatika and Netlock compete, but sometimes form alliances to represent their common interests. For example, they cooperated to persuade APEH to base its electronic services on their qualified digital certificates, but this project failed and APEH created a system on its own. (an example of such a cooperation is [Netlock – Mav Informatika, 2003])

Based on the home page of Máv Informatika, I found that this company follows the principles of [Shapiro and Varian, 1998] the most. They offer (technically very similar) services at different prices, for different clients. I thought the different liability insurance associated with each service differentiates between customers and ensures that premium customers buy premium services. I reckoned that this is market segmentation as it was proposed by [Shapiro and Varian, 1998]. Recently, [PrimOnline, 2004] Máv Informatika started a project of issuing certificates for local governments free of charge. [Shapiro and Varian, 1998] claimed that it might be sensible to dump a product or service free of charge to the market just to increase its value. (See Section 6.1.1)

Based on the interview, my opinion of the market segmentation policy of Máv Informatika was fully revised. I found that Máv Informatika focuses on large organisations, and the different prices of digital signature service are aimed at different levels of the hierarchy. This way, a CEO could sign contracts to a higher monetary value, a middle manager for a mediocre value, and a subordinate to a very small value. This policy suits the need of a large organisation, because it limits the possibilities of lower levels of the hierarchy while allowing the company to save money on these levels. Meanwhile, I think, this policy prevents small organisations from using the digital signature service effectively, because they have to purchase an expensive version to perform significant transactions[3]. Naturally, a client can decide to buy a certificate that allows with zero monetary value, and can make contracts with its business partners to accept it for

[3]E.g.: I consider buying a computer a transaction that every organisational client should require to be able to perform.

infinite monetary value. Since the same technology is behind all certificates, this solution can be technically sound. I consider this unintended use of a certificate a substitute, it is discussed in Section 7.6.2. Naturally, Máv Informatika offers certificates to individuals too according to its home page, but my interviewee did not mention it, perhaps because this sector is not considered important.

The other advice of [Shapiro and Varian, 1998] were to reduce costs by increasing output, and to form alliances. I found that Máv Informatika follows these principles.

Any alliance on this market (like the above one of Netlock and Máv Informatika) might benefit all players. [Cauley de la Sierra, 1995] has listed several reasons for alliances, and this is typically the case of an alliance for *building market capabilities*. As there is currently little demand, market players should cooperate to convince clients and end-users to think security consciously. (At least, my interviewee at Giro identified this as the main problem.)

I found that alliances have particularly great potential in this market, because it is a possible situation that *if one market player pioneers new a new market segment, it benefits all market players*, even its competitors. According to [Shapiro and Varian, 1998], if the number of digital signature users increase, the value of a digital signature service increases. While we can speak of lock-in to digital signature services, we cannot speak of lock-in to one specific service provider. (see Section 6.1.2) Unlike other network economies, free competition is possible inside the market. This means, if the value of services offered by one market player increases, the value of services offered by other players increase the same way.

I found that Máv Informatika has a very conscious and sophisticated strategy aiming to penetrate the market.

7.7.4 Microsec

Microsec Számítástechnikai Fejlesztő Kft is a small company. It functioned as a software developer company (in the field of IT security and PKI) before it decided to enter the digital signature service provider business.

Generally, Microsec is considered a small company, but its sales are 5-10 times as high as those of Netlock. Moreover, the profit of Microsec is 50-70 times as high as that of Netlock, while their equity is approximately 5 times higher. Microsec has an astonishingly high ROCE, much higher than any other player. See Appendix E.

First of all, it was clear for me that a it would be surprising if a company could have such a high ROCE while others on the same market are struggling. While Microsec is CA, its financial information do not suggest that the company is carrying the heavy burden of a suffocating CA business unit. Thus, I supposed that Microsec is on a different, more profitable market.

I organised my interview (Appendix C.4) to seek an answer to the following question: Why did a company that already found an extremely profitable market engage into the CA business that has more than questionable profitability?

Based on the interview I found that (unlike other CAs) *Microsec is selling what customers do demand*: various security-related services that (among many other things) require secure communication. (Some key services are listed in the interview.) Unlike its competitors, this company does not provide PKI for its own sake, *Microsec provides services that customers require, and also provides PKI as a platform for these services*. Based on the above findings, I reckon *Microsec can not only be viewed as a CA*, but also as a *customer of a CA* who chose to *backward-integrate into the CA business*.

(In this sense, Microsec is similar to Data Contact, another company I interviewed. Data Contact has a very wide portfolio of services and is also a provider of substitutes to PKI. Thus, Data Contact is not only a customer but also a threat to this market.)

The phenomenon that a service provider backward integrates into the business of the infrastructure required for the service is not typical for other infrastructures likes roads, rails, telephone, etc. It is more typical that a service provider forward integrates into a service business (e.g. the phone company Matáv has an burglar alarm service that can notify the police). Generally, service providers are small, and infrastructure providers are large and require large investments. This is why taxi drivers seldom backward-integrate into the business of roads.

I asked my interviewee why they chose to backward integrate, and she answered that they see perspective in this market. She also answered that they would like to contribute to the spreading of the infrastructure.

My speculation is that they had more clear (and less selfish) reasons to enter this business. They needed PKI for certain services, and also had the expertise to provide these services. Perhaps, they did not trust other market players to provide a reliable and standardised service. Perhaps, they wanted to have a control over the costs of PKI and they were afraid that another CA would abuse its situation. Perhaps, they considered that they can eventually make profit from being a CA.

Whatever the reason was, the *strategy of Microsec has proven to be viable*. (See Appendix E)

Websites of Microsec:

`http://www.microsec.hu/Web/doc/hu/microsec.htm`, `https://www.e-szigno.hu/`)

7.7.5 Netlock

Netlock Hálózatbiztonsági és Informatikai Szolgáltató Kft (`http://www.netlock.hu`) is a small company compared to most of the other players on the market of digital signature service providers. However, Netlock was one of the first entrants. The company is very dynamic and tries to penetrate the market.

Netlock is not only a *market pioneer*, but aims to be the market leader too. (I reckon, Netlock is the market leader and Máv Informatika is the main challenger.) Netlock has very aggressive marketing activity, whenever the press writes about digital signatures, Netlock is usually mentioned. Netlock was the first company to qualify for issuing certificates for qualified digital signatures. (Later, Máv Informatika joined Netlock too.) Today, Netlock is the only CA whose certificates are accepted by Microsoft products. Based on its home page and press activity, I reckon that Netlock targets every segment of customers that may present demand for digital signatures.

However, Netlock is a small company, and I strongly doubt that small companies have long-term perspective in the CA business. A CA needs to be trusted by nature, and a company with small capital power should not be trusted without limitations. I think, the secure internal communication of a large bank (that performs transactions of much higher magnitudes too) should not be based on a small external CA company. For example, the hostile takeover of the small CA may compromise the security system of the large bank. I think, in security critical applications an organisation should not never rely on certificates issued by a CA that is much smaller than it.

Unfortunately, the CEO of Netlock did not respond to my request for an interview. This company could have been very interesting to examine. I would have asked the question if Netlock suffers from the above problem of being small and if it has any strategy to manage it. The other interesting question could have been if the CA business unit of Netlock is self-supportive. Netlock often boasts of issuing several certificates, it would be interesting to know how many of these are test certificates (that are issued free of charge but cannot be used in real applications) and how many of them are real ones that are *sold* to meet a real demand. (As far as I know, Netlock has other PKI-related activities too that may cross finance the CA business unit.)

Although *Netlock might be the market leader*, my interviewee at Matáv named Máv Informatika as their main competitor, and considered Netlock too small to be dangerous. Clearly, *the current market is so small* that for giants like Matáv *it is not really interesting who the market leader is*.

This is a very strange market, because the (perceived) market leader is a very small company (see

financial information in Appendix E). This company has a good brand name, and a significant market share, while it is small and not too profitable either. If the market becomes attractive, other players (or a new entrant) might wish to attempt the aquisitionacquisition of Netlock. (see Section 9)

In spite of the above, both potential customers I interviewed said that they would probably buy a certificate from Netlock. It seems, Netlock is working very hard and invests a lot into establishing the market and creating demand for PKI.

8 Conclusions

Is literature able to explain the special economical mechanisms of a digital signature market? Yes, most mechanisms of a digital signature service market can be explained using the disciplines of a network economy. However, the market for digital signature service is not totally a network economy. For example, unlike in many network economies, free competition may exist among market players of the digital signature service provider market (but may not exist between market players and substitute vendors). Another example is that marginal cost of selling digital signature service is not zero if chipcards are involved. I assessed these factors and tried to refine the model to be applicable to this situation. See Section 6.

I performed an analysis of the digital signature market in Hungary using the above literature. I analysed the market for digital signature service in Hungary by a PEST analysis and Porter's five forces in Section 7. My findings are summarised in the following points.

Which factors prevent the market from growing?

1. *Lack of demand* is a key problem.

2. I reckon, *substitutes* are responsible for the small demand.

(a) *Blind trust* (ignorance of clients) is an important substitute.

(b) Several other (IT and non-IT) substitutes exist that clients find a lot more cost-effective than PKI. Many clients do not need that high grade of security that is offered by CAs.

What are the strategies of current market players?

- Netlock and Máv Informatika compete face-to-face for the position of market leader. Sometimes, they make alliances to fight for common goals. These two players are the most active ones, and perform significant investments to establish the market. If their strategy is good depends on their success in establishing the market and keeping it (e.g. against Matáv).

- Matáv exerts minimal effort to maintain its position on this market. It does not find it interesting at its current size, but may try market penetrate if the market would boom. I think, the strategy of Matáv is a compromise between entering the market and not entering it. If this compromise is good or bad depends on how much resources Matáv is wasting for upkeeping its presence. I think, this might be the right strategy for a company like Matáv. (Though, it is possible that this strategy is not conscious, but Matáv is just clumsy.)

- Microsec is a vendor of PKI-based services and backward integrated into this market. Unlike most other CAs, Microsec is making profit with this activity. I reckon, the survival of the CA of Microsec is less dependent on the future of PKI and this market than the survival of other CAs.

- Giro withdrew from the market.

Are market players conscious of the factors limiting the market?

1. Though the expression 'lack of demand' was mentioned by Giro only, *all CAs feel this phenomenon*.

2. Most CAs defined the market as the market for digital signature service, and not more broadly, like the market for *services that provide basis for trust*. Most of them did not mention vendors of substitutes as competitors or threats to their business. (see Section 7.6.15)

   (a) *CAs are conscious of blind trust*. Netlock and Máv Informatika invest significant resources to confront this substitute and thus establish the market by making clients more security conscious.

   (b) Few of them mentioned substitutes different from the trivial ones like regular email messages (which is almost blind trust) and handwritten signature. I reckon that their view of the market that systems that are not based on their services are insecure, is false. Customers can choose between a wide range of secure and sophisticated solutions, and they perceive some of them to be more valuable to PKI.
   I think, *the threat of substitutes is far more dangerous than CAs perceive* (or perhaps, they do not admit it).

9 Recommendations

9.1 Key recommendations for each market player

- Netlock and Máv Informatika should cooperate more closely and consciously. If one of them pioneers a new market, it benefits the other one too by increasing the size of the network economy. They should also develop a solution to counter Matáv when it enters the market. Perhaps, they should artificially create customer lock-in.

- Matáv should wait for the right moment to step out from the shadows and spring to action

(if the market booms). Moreover, it should find a legal way to supply its telephone subscribers with certificates, without requiring them to go to an office of Matáv. Apart from keeping the law on digital signatures, the company should also consult laws and regulations on fair competition when doing this, because in this case the enormous competitive advantage is gained by making use of monopoly on one market to penetrate another one. Matáv may also attempt the acquisition of Netlock to gain market share quickly.

- I reckon, Microsec does not need my advice. I found that this is the only company that has a strategy that has proven to be viable. (Still, they should take care to keep their customers.)
- I think, Giro had a very clear view of the market, and very clear priorities (that were different from engaging in profitable businesses). Giro withdrew from this market. I do not think I need to give any advice to Giro.

9.2 Recommendations for a new entrant

Having considered various groups of potential customers, I found only one customer who might find it beneficial to invest in PKI now: the government. However, many governments invested millions of dollars and euros into PKI worldwide, and this area still seems to be struggling.

Although many people find PKI the best technical solution available, I am not fully convinced that the market will eventually emerge. Perhaps, other solutions are more cost-effective or better fulfil the need of users. This market has the potential to become very attractive in the far future, but there are good chances that it will shipwreck. Any investment to this field should be done very cautiously.

I reckon, this is not the time to start major investments in this field. This is the time to sit back and *wait until the current players of the market perform the investments to establish demand*, and make the network economy reach its positive feedback period. Unlike other network economies, this market does allow perfect competition, so customers will not be locked in to current service

providers. I found that *on this market is preferable to be a late entrant to being a pioneer*, because pioneers pay the sunken costs of building the network, they may overexhaust themselves and they might not be able to get their money back at the end.

A References

[Berta et al., 2004a] Berta, I., Buttyán, L., and Vajda, I. (2004a). Mitigating the Untrusted Terminal Problem Using Conditional Signatures. Proceedings of International Conference on Information Technology ITCC 2004, IEEE, 2004, IEEE, Las Vegas, NV, USA, April.

[Berta and Mann, 2000] Berta, I. and Mann, Z. (2000). Smart Cards – Present and Future. Híradástechnika, Journal on C^5, 2000., vol 12.

[Berta and Mann, 2002] Berta, I. and Mann, Z. (2002). Evaluating Elliptic Curve Cryptography on PC and Smart Card. Periodica Polytechnica, Electrical Engineering, 2002, vol. 46/1-2, pp. 47-75, Budapest University of Technology and Economics.

[Berta et al., 2003] Berta, I. Z., Buttyán, L., and Vajda, I. (2003). Mitigating the untrusted terminal problem using conditional signatures. CrySyS Lab Technical Report, `http://www.crysys.hu/publications/files/BertaBV2004condsig.pdf`.

[Berta et al., 2004b] Berta, I. Z., Buttyán, L., and Vajda, I. (2004b). Privacy protecting protocols for revokable signatures. Cardis2004, Toulouse, France (to appear).

[Berta and Vajda, 2003] Berta, I. Z. and Vajda, I. (2003). Documents from Malicious Terminals. SPIE Microtechnologies for the New Millenium 2003, Bioengineered and Bioinspired Systems, Maspalomas, Spain.

[Bradford DeLong, 1995] Bradford DeLong, J. (1995). Rules, New and Old, for Tomorrow's Economy. WorldLink: The Magazine of the World Economic Forum, Draft 2.1; October 7, 1998, `http://www.j-bradford-delong.net`.

[Cauley de la Sierra, 1995] Cauley de la Sierra, M. (1995). Managing Global Alliances. Addison-Wesley.

[Chen, 2001] Chen, L. (2001). A Computational Model of Virus Propagation. The Proceedings of the Conferences of in Computational Social Organisational Science, July, 2001, Pittsburgh.

[Coltman et al., 2001] Coltman, T., Devinney, T., Latukefu, A., and Midgley, D. (2001). E-business: Revolution, evolution, or hype? California Management Review; Berkeley; Fall 2001.

[Communications Authority, 2004] Communications Authority (2004). Home page of the Hungarian Communications Authority. `http://www.hif.hu`.

[CrySyS, 2003] CrySyS (2003). BME, Adatbiztonság Laboratórium (Laboratory of Cryptography and Systems Security) honlapja. `http://crysys.hit.bme.hu`.

[Ellison and Schneier, 2000] Ellison, C. and Schneier, B. (2000). Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure. Computer Security Journal, Volume XVI, Number 1, 2000.

[EU Directive, 1999] EU Directive (1999). Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[Findrik, 2002] Findrik, M. (2002). Competitiveness and its main factors. Evolution of Institutions and Knowledge of Economy, University of Economics and Business Administration.

[Follett, 1978] Follett, K. (1978). Eye of the Needle. Penguin Group, Penguin Putnam Inc., New York, USA.

[Gimon, 1995] Gimon, C. (1995). The Phil Zimmerman Case. InfoNation, June, 1995, `http://www.skypoint.com/members/gimonca/philzima.html`.

[Hofstede, 1980] Hofstede, G. H. (1980). Culture's consequences: Comparing values, behaviors, institutions and organizations across nations. 2nd Edition, Thousand Oaks CA: Sage Publications.

[Hungarian Law, 2001] Hungarian Law (2001). Act XXXV of 2001 on electronic signatures. `http://www.hif.hu/english/menu4/m4_8/es.pdf`.

[Kelley, 1998] Kelley, K. (1998). New Rules for the New Economy: Ten Ways the Network Economy is Changing Everything. London, Fourth Estate, ISBN: 1857028716.

[Kopint-Datorg, 2001a] Kopint-Datorg (2001a). Az IT szolgáltatások piaca Magyarországon. Kopint-Datorg Rt. Piackutató F?osztály.

[Kopint-Datorg, 2001b] Kopint-Datorg (2001b). Infokommunikációs irányt? Kopint-Datorg Rt. Piackutató F?osztály.

[Krasznay and Szabó, 2001] Krasznay, C. and Szabó, Á. (2001). A digitális aláírás elterjedésének leht?ségei és korlátai. Budapest University of Technology and Economics, Scientific Student Circles (TDK).

[Lindström and Andersen, 2000] Lindström, M. and Andersen, T. (2000). Brand Building on the Internet. Kogan Page Ltd. London, 1st edition, ISBN: 0749433132.

[Mintzberg et al., 2003] Mintzberg, H., Lampel, J., Quinn, J., and Goshal, S. (2003). The strategy process. Prentice Hall.

[Netlock – Mav Informatika, 2003] Netlock – Mav Informatika (2003). Veszélyben az elektronikus aláírás magyarországon. http://news.mavinformatika.hu/cikkmutat.phtml?cikkid=1081.

[O'Brien, 2000] O'Brien, J. (2000). Introduction to information systems: Essentials for the internetworked enterprise. McGraw-Hill, ISBN: 0-07-116973-3.

[Office of the e-Envoy, 2002] Office of the e-Envoy (2002). Security Architecture e-Government Strategy. e-Government Strategy of the UK government, www.eenvoy.gov.uk.

[Origo.hu, 2003] Origo.hu (2003). Nem elég biztonságosak a hazai webszerverek. http://www.origo.hu/techbazis/internet/20030606siralmas.html.

[Pletier, 2001] Pletier, T. (2001). Information security risk analysis. Auerbach Pub, 1st edition.

[Porter, 1985] Porter, M. (1985). Competitive Advantage: Creating and Sustaining Superior Performance. Simon & Schuster Trade, ISBN: 0684841487.

[PrimOnline, 2004] PrimOnline (2004). Elektronikus aláírás már polgármestereknek is. http://hirek.prim.hu/cikk/38339.

[Rosenberg, 2001] Rosenberg, J. (2001). Quickssl(tm) Breakthrough automated authentication technology that provisions SSL server certificates in 10 minutes not four days. GeoTrust white paper.

[Schneier, 1996] Schneier, B. (1996). Applied Cryptography. John Wiley & Sons, ISBN: 0471117099.

[Schneier, 2000] Schneier, B. (2000). Why Digital Signatures Are Not Signatures. Crypto-Gram Newsletter, November, 2000.

[Shapiro and Varian, 1998] Shapiro, C. and Varian, H. (1998). Information Rules: A strategic guide to the Network Economy. Harvard Business School Press, ISBN: 0-87584-863-X.

[Slack et al., 2001] Slack, N., Chambers, S., and Johnston, R. (2001). Operations Management. Pearson Education Limited, Third Edition, ISBN 0273-646557-5.

[Tellis and Golden, 2000] Tellis, G. and Golden, P. (2000). First to Market, First to Fail? Real causes of enduring market leadership. Sloan Management Review, 37/2 (Winter 1996): 65-75.

[Zou et al., 2003] Zou, C., Gao, L., Gong, W., and Towsley, D. (2003). Monitoring and Early Warning for Internet Worms. `http://tennis.ecs.umass.edu/ czou/research/monitoringEarlyWarning.pdf`.

B Technical background

B.1 What is a digital signature?

A digital signature is not the digitalisation of a regular, paper-based signature. *A digital signature is the result of a complex mathematical computation* that takes two parameters as input: One of them is the message that is going to be signed, the other one is a piece of secret information that is related to the identity of the signer. This means, the digital signature of the same person is different for each document he or she signs.

A digital signature operation can only be performed by computers (because it is very time consuming for humans), it takes two parameters as input. One of the is the message the user intends to sign, while the other parameter is a secret piece of information that represents the identity of the user. This is called the user's private key or secret key.

In a public key system, every user has two keys (a key pair). The *private key* is secret, it is known by the user only, while the *public key* should be known by anyone. A message encrypted by a user's private key can be decrypted by her public key only, and vice versa: a message encrypted by a user's public key can be decrypted by her public key.

If user Alice sends a message to user Bob, and she encrypts it with Bob's public key, it can be read by Bob and noone else. Thus, she can ensure the *secrecy* of the message.

If Alice sends a message to Bob, and she encrypts it with her private key, it can be read by anyone (because everybody knows the public key of Alice). However, a third party cannot replace this message, because the private key of Alice is needed in to produce a data block that becomes a (valid sensible) message when encrypted with the public key of Alice. By encrypting a message with her private key, Alice can ensure its *authenticity*.

A message encrypted by the private key of a user is called the user's digital signature. See e.g. [Schneier, 1996] for details.

The most famous public key cryptosystem is RSA, other famous systems are ECC [Berta and Mann, 2002], DSA and NTRU.

B.2 What is a digital signature service?

From players of the digital signature provider market, a customer may buy a service, *the potential to create digital signatures that can be verified by any third party*. Note that computing a signature is a relatively easy and cheap task, while allowing them to be verified by anybody requires a complex infrastructure called 'public key infrastructure' (PKI).

Taking part in PKI requires a *digital certificate* that contains the user's name and information that allows the verification of the user's signatures. Certificates are issued (and digitally signed) by trusted parties called *certificate authorities* (CA). In contrast to its name, a certificate authority is not necessarily an authority, it is often a profit oriented company. *CAs provide digital signature*

service by issuing and certificates for users.[4] (The CA issues a new certificate for the customer, whenever the old one expires. The user may revoke a certificate for security reasons, and the CA has to maintain a list of revoked certificates on its website. The CA receives an annual fee for these services.)

In order to create a digital signature, a customer does not need any help from a CA. However, a digital signature cannot be verified by any third party unless the customer has a certificate. It allows the customers to prove their identity to any third party, who – based on the certificate – can trust a customer to be who he or she claims to be. In a nutshell, *when a CA sells digital signature service, it signs a certificate – sells basis for trust*.

On one hand, the Hungarian CAs have to comply with Hungarian laws (in addition to international standards and regulations), on the other hand they have to identify and authenticate customers that can only be done personally (based on e.g. their ID card). Although this latter functionality can be outsourced to an entity called registration authority (RA), but the Hungarian market for digital signature service is small, so in Hungary the CA and RA are usually the same entity.

The benefit the customer receives when subscribing to a digital signature service is the ability for secure communication on a *global* network – the Internet. However, CAs are usually *local* companies.

Since CAs offer access to PKI, a global infrastructure (accessible from any country), their service should be highly standardised, so foreign partners of their subscribers should be able to understand and accept their certificates. In this sense, a CA is similar to a telephone company: it operates locally, but sells the service of accessing a global infrastructure. On the other hand, a CA does not provide communication, it is performed on the Internet, independently from the CA. A CA does not have any costs when the user computes a digital signature. (Though, some

[4]Note that certificates issued by CAs may be used for purposes other than digital signature (e.g. they can be used for encrypted communication). However, this dissertation only focuses on certificates for digital signatures, authentication and authentic communication.

extremely little costs may occur when a partner verifies it.)

B.3 What is a certificate?

In every public key cryptosystem it is vital that a private key may only be known by its owner. Otherwise, other people would be able to sign messages on her behalf, or decrypt her confidential messages.

Similarly, it is also vital, a public key should be available to anyone, because it is required to verify a digital signature. Moreover, a public key must be available to anyone in an *authentic way*. Otherwise if the evil Mallory generates a fake key pair, he may convince Bob that Mallory's public key is the public key of Alice. Thus, Bob would believe that messages signed by the fake private key of Mallory are signed by Alice.

The above problem can be solved if Charlie knows the authentic public key of both Alice and Bob, and both Alice and Bob know the authentic public key of Charlie. This way, Charlie can create and sign a message certifying that a key is in fact the public key of Alice. *A certificate is a document digitally signed by a trusted third party that contains (along with many other pieces of information) the name of the user and her public key.* Relying on the certificate, anybody who knows the authentic public key of the trusted third party can learn the user's authentic public key. The trusted third party who issues certificates is called certificate authority (CA).

Thus, the certificate of Alice is a digital representation of her identity. She can prove her identity by showing her public key (certificate) and using her private key. Note that unlike an ID card, a certificate is allowed to be copied. (Moreover, copying a certificate is even encouraged so that it can be accessed easier.) However, modifying a certificate is not possible, because it would violate the CA's digital signature. Thus, a modified certificate is not valid anymore.

The situation can get more complicated if the certificates of Alice and Bob are issued by different CAs. (For example, they live in different countries.) The solution is that CAs have certificates

too issued by CAs on higher levels. On the top level there is a root CA to whom every CA belong. Using a so-called CA chain, users of ever CA can learn any public key in an authentic way. This infrastructure is called PKI. *A public key infrastructure is an IT system that enables people to learn the public key of each-other in an authentic way.*

B.4 Lifecycle of certificates

1. If a customer would like to take part in PKI, then she generates a key pair: a public key and a corresponding private key. (See Appendix B.3 for details) These keys are not physical objects but very large numbers, approximately 100 to 200 digits.

2. A customer arrives at the Registration Authority and identifies herself using her ID card. The customer also presents her public key. (She keeps her private key secret.)

3. Being convinced of the customer's identity, the Registration Authority requests a certificate from the CA for the customer.

4. The CA creates a certificate for the customer by digitally signing a document containing the customer's name and her public key and an expiration date. (Naturally, the certificate may contain additional information on the customer and the CA.)

5. The customer can use her certificate for various purposes (identification, digital signature, and decryption). For example, she can identify herself by presenting her certificate and proving that she knows the corresponding private key. In these cases the certificate of the CA needs to be presented too.

6. If the customer thinks that someone else has learned her private key, she can revoke her certificate at the CA. The CA maintains a list of revoked certificates.

7. The CA receives an annual fee for keeping the customer registered and maintaining the certificate revocation list.

For more details on the above process see [Schneier, 1996].

B.5 Qualified, Advanced and Server certificates

Although there are many types of certificates, I differentiate between three main types in this dissertation.

Qualified: This type of certificate is issued to an individual (or to an individual on behalf of a company) and is needed for *qualified digital signature service*. The CA that is able to issue such a certificate needs to be certified (by a certifier organisation) that it complies with all the regulations prescribed by the law. [Hungarian Law, 2001]

Only Netlock and Máv Informatika are able to provide qualified digital signature service today.

Advanced[5]**:** This type of certificate is issued to an individual for *advanced digital signature service*. In this case the *CA does not need to be certified*. Advanced digital signature service is simpler (and cheaper) to provide, because there are less security regulations, but the law prescribes qualified digital signatures for certain critical applications (see interview C.2).

All five CAs are able to provide advanced digital signature service. (Giro suspended providing it.)

Server: This is an advanced type of certificate that is issued to a *device* and not to an individual. Typically, such certificates are issued to a world wide web server, so users connecting to it may establish a secure (authenticated and encrypted) connection. Although these certificates are not used for digital signatures, I sometimes mention them in the dissertation because they require the same infrastructure.

B.6 Explanation of problems with PKI

- A CA is not an authority, but a company. Although it goes through a procedure of certification, it should not be trusted much more than any other company. A CA does not abuse the trust its customers put in it, because it *promises to do so*. Although it may be unlawful to break such a promise it is possible. It should always be considered what trust we put into a CA, and if it may be the interest of the CA to break its promise. Naturally, a CA that loses the trust of its clients will be out of business. However, it has to be compared, how much the owner or operator of the CA loses by sacrificing his or her company and how much the same owner can gain by breaking such a promise. Naturally, a digital signature should be trusted no more than the CA that issued the certificate that proves its validity. (And no more than the higher level CA that issued the certificate for the CA, etc.)

  This is why I strongly doubt the viability of small CAs issuing certificates for large organisations that control goods with value much larger than that of the CA.

- PKI may solve the problem of secure (encrypted and authenticated) communication. However, to encrypt or to authenticate messages, complex computations need to be performed. These computations are beyond the capabilities of most humans, so computers are used for assistance. PKI protects communication from the computer of the sender until the computer of the receiver. An attacker, who is able to tamper with these computers, can tamper with communication between the human sender and the receiver. To solve this problem both parties need secure computers for the communication.

  Unfortunately, today's personal computers are far from being secure, regardless of the software and operating system they use. Most computers are vulnerable to viruses (certain viruses can spread by the Internet and infect millions of machines in hours [Chen, 2001], [Zou et al., 2003]). The belief in today's computer science is that while it is possible to design extremely strong encryption and digital signatures, it is almost impossible to have

a networked machine that a distant attacker cannot take control of. At least, operating and keeping up-to-date such a machine requires much time and significant expertise that a very small percentage of users possess today. (And it is also unlikely that everybody shall become a computer security expert in the future.) Does it have sense to guarantee the security of a communication as long as we cannot guarantee the security of endpoints? [Schneier, 2000]

The works [Berta et al., 2004a], [Berta et al., 2003] and [Berta and Vajda, 2003] also throw more light on this problem.

C Summary of interviews with digital signature service providers

Originally, the interviews were performed in Hungarian, I translated them to English. They were performed as informal conversations and lasted approximately half an hour. I summarised them and also tried to formalise them by organising them around my key questions. This means the sentences of the interviewees are not quoted directly.

I had the following key areas to guide the interview:

- definition of the market
- relation of the interviewee's organisation to its competitors
- identification of the key customer segments
- the perspective the interviewee's organisation sees in qualified signatures
- the interviewee's view of substitutes

I tried to avoid the use of both business and technical jargon to give equal chances to interviewees of these areas.

C.1 Giro

I interviewed Gabriella Hradszky, head of the Division of Marketing and Sales Management at Giro Ltd.

Berta: *Why did Giro enter this market?*

Hradszky: Giro is in a very special position, because its owners are those banks for whom Giro provides its clearing services. This is why *profit maximisation is not the primary objective of Giro*. Our primary task is to operate the Hungarian inter-bank clearing system. In order to fulfil this task, many of the security requirements for operating a CA were already available. (We have a secure server room, a building with security system, and our staff is already trained to be security conscious, etc.)

We wanted to support our clients/customers in introducing and using electronic communication and payment systems, so we decided that Giro could establish a secure central CA that banks could use. (The other option was that each bank has to establish its own CA.) Our clients/owners accepted this paradigm.

Unfortunately, there was little demand for PKI services.

Berta: *What do you think, what are the reasons for this little demand?*

Hradszky: There are many reasons for this:

- There are few applications where PKI can be used. (Perhaps, because there are few application developers.)
- There is no sensitiveness for risk in users. Today there are many home banking systems that use very weak authentication (based on a username and a password). Since there were

not any frauds with these systems, both banks and their clients seem to be satisfied with them.

- In case of Internet banking systems (where the user is not limited to a dedicated computer but can access the banking system from any computer with a web browser) there are severe risks. Giro did not wish to take part in any insecure systems, our policy was to issue private keys for certificates only on smart cards. Unfortunately, smart card based Internet banking systems could not work because of compatibility issues of smart cards.

- There is no strong commitment from the government to use PKI. In every country where PKI could spread, the government had an important role in starting this process.

- The law on digital signatures does not regulate the whole processes of issuing and using a certificate but only certain elements of them.

- The Hungarian (and Central Eastern European) society is very special. People have little trust in business partners, and little trust in technology. IT experts, who follow the the development of technology, would like to bring the newest technologies to Hungary, but sometimes Hungarian customers do not welcome it. Some technologies are able to penetrate the market, some are not. For example, mobile telephony and SMS could spread very rapidly, but PKI and chipcards could not. (For some reason, these two are not successful in other countries either.) It took a long time till bank cards could get spread in Hungary, but today they are a successful area of business.

Berta: *You said your customers were banks. Is their demand homogeneous? Do they expect the same service from Giro?*

Hradszky: Our clients are mainly banks and financial institutions. We also include all organisations under PSZÁF into the group of potential clients. Probably, if the government would request a large number of certificates, we would also sell our service to the government too.

We sell a different service than other CAs. While they encapsulate the CA and RA functionality, we only established a CA, and let our customers do the registration procedure. Naturally, every bank has a way to register customers. Thus, we do not register customers directly, we issue certificates via external RAs (our customers) only. This is why we prefer to distinguish between customers. If anybody could become an RA, it would spoil the security of our CA.

Berta: *Who do you consider your competitors?*

Hradszky: Giro established a system with focus on security. We have a very stable background: we have financial stability (While smaller CAs are fully dependant on their PKI business, we are able to cross-finance this business unit), we have reputation, and we have expertise in security. I think, very few other CAs are able to compete in the sector of banks.

On one hand, banks are just a niche in the Hungarian market. On the other hand, customers of banks cover the whole Hungarian population. In this sense, we could threaten the market of every CA.

Unfortunately, PKI services do not seem to be successful. Since we saw little demand for digital signature services, *we decided to suspend our CA*. We did not withdraw from this market, but we revoked all of our certificates and 'hibernated' our CA.

The yearly upkeep costs of our CA was in the magnitude of a hundred million forints, which was intolerably high. Especially because we could not issue more than a few thousand certificates, and we charged 2-3000 forints for each.

We still have the expertise and we still have the resources to provide digital signature service. *If we see any significant demand in the future, we would restart our CA* and return to this market immediately. I do believe that this will happen, but I do not think that this will come in the near future.

C.2 Matáv

I interviewed Balázs Tapasztó, head of the PKI business unit at Matáv.

Berta: *How would you call the market where the CA of Matáv operates?*

Tapasztó: There are currently four companies on this market, but it seems that Microsec provides its services to the Ministry of Justice only, and did not try to open towards the rest of the market. Netlock is much smaller than the two other 'real' players of the market, we do not consider it a serious threat. I consider MÁV Informatika the main competitor of Matáv. Giro was on this market before too, but they decided to withdraw.

Berta: *What is your relation to your competitors?*

Tapasztó: We wish to compete with them, and we do not wish to enter an alliance. There is MELASZ (Magyar Elektronikus Aláírás Szövetség), the Hungarian Alliance for Electronic Signatures, a forum for digital signature service providers. Matáv is lobbying less actively in this forum than its competitors. Lobbying and appearing on various digital signature conferences requires a significant amount of resources and Matáv does not have a large group dedicated only for this task. Matáv decided to maintain its presence on this market for its strategic importance.

Berta: *For which groups of customers do you offer these products?*

Tapasztó: Matáv only offers advanced digital signature service today. We see a great perspective in large organisations. For them, we have a service called VCA (virtual CA). A client can have a virtual CA that is operated by Matáv but is under the control of a client. The client can register individuals and issue certificates to them, but does not need to give the database of clients to Matáv. For example, banks often do not wish to provide data on their clients to third parties. Naturally, this service can only be offered to an organisation that can be trusted to perform the registration procedure.

For the rest of the customers we can perform the registration and we may issue certificates to them directly. Important target customer groups of this sector are individuals and small enterprises.

(Naturally, if larger clients are interested in this service, we would sell it to them too.)
We are also planning to provide qualified digital signatures in the near future, its target customers are going to be larger enterprises and organisations. According to the law, for certain tasks (e.g.: issuing receipts, sending tax returns) only qualified signatures can be used.

Berta: *What can individuals do with a digital signature service today?*

Tapasztó: They can use it to digitally sign (and encrypt) their private emails. For example, a group of friends can exchange emails in a secure way using our digital signature service.

Berta: *You have a significant database on customers, and you have regular relations with many of them (telephone subscribers). Are you using these relations to gain competitive advantage? For example, would it be possible to give a certificate to all phone subscribers?*

Tapasztó: Yes, we do have a large database, and in case Matáv would decide to start a large marketing campaign on digital signatures, we would surely use it or telemarketing. Unfortunately, the law forbids us to provide our customers certificates without identifying them again for this special purpose. Although we know them, we must ask them to come to our office again to get a certificate.

Berta: *I saw on your website that you issue certificates for 'standard' and 'advanced' digital signature service, and in case of 'standard' certificates the issuance procedure is simpler.*

Tapasztó: Still, the law prescribes us that clients need to be identified personally. Both of them are certificates for advanced digital signature service, but in contrast to 'standard' certificates we perform further background checking in case of 'advanced' ones.

Berta: *If a customer does not want digital signature service what other options can he or she choose instead?*

Tapasztó: Electronically? Nothing. They can just print the contract, and sign it with their handwritten signature.

C.3 Máv Informatika Kft.

I interviewed Pál Kocsi, director of the PKI Business Unit at Máv Informatika Kft.

Berta: *How would you call the market where the CA business unit of Máv Informatika operates?*

Kocsi: As a CA, we operate on the same market with Netlock, Matáv, Microsec and the late Giro, the market of digital signature providers.

Berta: *Máv Informatika offers certificates at several different prices. What is the difference between these services? Is it a different level of liability insurance?*

Kocsi: Not only. The main difference is that they are valid for different monetary values. People at different ranks in an organisation have different competences, different authority. For example, while a CEO may sign contracts of very high magnitudes, a middle level manager has much less authority. A subordinate may sign contracts of some very low values only. Based on such a certificate, the receiver of a message may determine if the sender had the authority in his or her organisation to make a decision (sign a contract or send an order) of such a monetary value.

Naturally, different insurance applies for different monetary values.

We also offer a service that other CAs do not. If a company does not have the expertise to operate a CA of its own, it can outsource this task to us. In this case we establish a new CA that issues certificates to our client. We operate this CAs, but it is under the client's control.

This service could be beneficial for an organisation that does not want us to register their members because then we would know too much about their internal secrets. This way, they can have a CA where they control the registration process. Even if we operate this CA, we cannot see its contents. Naturally, they are responsible if they make a mistake in the registration process.

Berta: *Does it mean you put the government and large organisation into primary focus?*

Kocsi: Yes. An initial funding from the government is definitely needed so this technology can start to spread. After there are real applications where it can be used, people will require digital signatures.

Berta: *You offer qualified digital signatures. Does it mean competitive advantage for your company?*

Kocsi: There was always great inquiry around the topic of qualified digital signatures, but we could not make business of them (in large volume) until recently. The law prescribed APEH to accept tax returns signed using qualified digital signatures, so APEH was considering the introduction of a PKI based system for this task. Unfortunately, APEH decided to create a system on its own, so we seem to have lost this area of business. The law was changed to legitimise this situation.

Currently we cooperate with PSZÁF and Kopint-Datorg and plan to introduce qualified digital signatures in organisations supervised by PSZÁF. It seems that the demand for qualified digital signatures is rising, but we cannot speak of a great breakthrough yet.

Berta: *What is your relation to your competitors?*

Kocsi: The competition is ferocious, but it does not mean we are enemies. For example, in the above mentioned case of APEH we cooperated with Netlock and emphasised together in the press that such weak authentication should not be used for such sensitive information like tax returns.

Berta: *Do you consider foreign CAs (like Verisign) dangerous competitors?*

Kocsi: Not really. Perhaps, after Hungary joins the EU, they will be more dangerous. In order to issue a certificate to someone, he or she needs to be registered first. This step can only be done personally, so the place of residence will determine which CA they choose.

It is a strong point of MÁV Informatika that we have offices all over Hungary. Clients in the country do not need to travel to Budapest to get registered.

Berta: *What can a customer choose instead of a digital signature service?*

Kocsi: Well, in that case they have to use papers. Or they may also use regular emails. However, regular (not digitally signed) emails can be counterfeited, so this latter is not a secure solution.

C.4 Microsec

I interviewed Csilla Éva Endrődi, PKI expert at Microsec.

Berta: *How would you call the market where the CA of Microsec operates?*

Endrődi: This is a very small and undeveloped market, and we can speak of but little competition yet. I think, the main reason for this is that people are going to buy digital signature service only if they can use in various applications and services. Moreover, customers are going to pay for digital signature service, only if they see that they can gain from it (either money or comfort). Sending tax returns would be a good example for such a useful service, but unfortunately APEH decided to set up an unofficial CA of its own. We perceive that some customers would be willing to pay for digital signature service if they can use it to access e-governmental services from their home computer.

Berta: *I heard some organisations characterising your company as "the service provider that works for the Ministry of Justice only, and does not try to open towards the rest of the market". Do you wish to make a comment on this? Do you have any other major client?*

Endrődi: We are the official service provider of the Ministry of Justice, but we are open for other clients too. If a customer is wishes to purchase our service, we serve the customer. Though, the Ministry is our main client, many of our competitors would be more than happy to have a client of this size.

Berta: *Are there any other services you provide that are related to your being a CA?*

Endrődi: We operate an information system for the Ministry of Justice that allows provides its users with access to public information on every company authentically. We also provide services for various governmental offices to help in accessing each other's databases and in transferring sensitive information.

We also develop various PKI-related software. We are the only CA that (apart from providing certificates) provides its own software for creating and verifying digital signatures. Our compet-

itors usually advise their clients to buy certain third party software, sometimes they even resell it to them. In contrast to our competitors, we are able to provide complete service.

Berta: *What is the proportion of your revenues that originates from your CA business unit?*

Endrődi: The revenues of our CA business unit are relatively small compared to the revenues of the whole company.

Berta: *As far as I know, you are in very profitable businesses. Why did you enter this particular market?*

Endrődi: We entered the CA business to provide an infrastructure that our applications and services can use. We consider certificates as tools that can support applications. We would like to provide applications and services to our clients that need a public key infrastructure to be present. Thus, we would like to help in spreading this culture, this infrastructure. We consider selling certificates as one but necessary step towards our main goal.

Berta: *If it is only the infrastructure that you need, then why don't you let other companies (e.g. Netlock or Máv Informatika) provide it?*

Endrődi: Because we see perspective in this market.

Berta: *Is your CA business unit profitable or do you have to cross-finance it?*

Endrődi: Its revenues approximately cover its costs. However, we can use it to make more attractive some other services we offer. Altogether, it is beneficial for the company to maintain this business unit.

Berta: *What segments of customers do you target?*

Endrődi: Our primary client is the Ministry of Justice, but our CA also targets governmental offices, because we can offer applications and services for those. We are planning to offer qualified digital signature service too in the future, because we think we can provide services for the Ministry that require this highest level of security.

We also target lawyers, judges, notaries and representatives of companies (people who are en-

titled to sign e.g. contracts on behalf a company). Though, as I told you before, we are open to the public. If a client is willing to pay for our services, we serve the client.

Berta: *What is your relation to your competitors? Do you form alliances?*

Endrődi: I cannot speak of any ferocious competition on this market yet. Naturally, we have connections with our competitors, but we do not take part in alliances.

Berta: *What can a customer choose instead of digital signature service?*

Endrődi: If a user wishes to prepare electronic documents in a way that their integrity is guaranteed, the documents can be connected to him or her, and are non-repudiable, than the use of a digital signature is the only solution. However, if a user does not need all of the above requirements, some other solutions can be used. For example, if non-repudiability is sacrificed, several solutions become available that are based on symmetric key cryptography. If the integrity needs to be preserved only, our PKI-based timestamping service can be used. If we do not consider electronic documents only, various solutions are available like handwritten signature or signature of a notary, etc.

D Summary of interviews with potential customers

D.1 Questions

- Do you have a PKI-enabled certificate? / Do you plan to buy one? Approximately, how many?
- Why do you think, you need (or do not need) a certificate?
- From which CA you have the certificate from? Why?
- If your business would expand, would you need more certificates?

D.2 Data Contact Kft.

Data Contact Kft. is a small dynamic company that provides various IT services to its customers. It not only provides consultancy, web hosting, mail server hosting and system administration but it also differentiates from other players on this market by providing highly customisable and high quality security services. This way, the company has significantly more knowledge on security-related issues and on PKI than its competitors.

I interviewed Boldizsár Bencsáth, the CEO of Data Contact Kft.

Berta: *Do you have a PKI-enabled certificate or do you plan to buy one?*

Bencsáth: Yes, we do use the technologies of PKI, but *no, we do not have* a PKI enabled certificate. We set our own CA up at Data Contact and we also set CAs up at our clients. Our CA signs the certificate of our clients', and our CA has a self-signed certificate. This solution is cheaper than total PKI, and our client is in a better situation than in case of a simple self-signed certificate. If somebody tries to contact our client, they can verify another company signed their certificate.

Berta: *This means, you are using a PKI system in PGP-like architecture?*

Bencsáth: Exactly. Actually, it is a PGP-like architecture that seems to fulfil our customers' need.

Berta: *Why do you think, you do not need a PKI certificate?*

Bencsáth: Our clients want security, but they do not need so high security that PKI provides. They are satisfied this a compromise between price and security.

Moreover, we do not use PKI for digital signatures but for other purposes like virtual private networking for example. The law on digital signatures does not provide any legal aid in this subject, and certificates are used in a less secure environment that certificates that CAs issue.

In case we would introduce digital signatures in communication with our business partners, we could include it in our contracts. This way we still would not need to pay to a CA.

Berta: *If you intended to by a PKI-enabled certificate, which CA would you choose? Why?*

Bencsáth: First of all, we would investigate this problem more thoroughfully, and than choose the proper CA. I think, the services of Verisign are very expensive, and I don't like that company's services, but I am afraid, I would end up at Verisign at the end.

Berta: *What is your problem with Verisign?*

Bencsáth: I find too many companies certified by Verisign need to refresh their expired certificates. Perhaps, Verisign could warn them in advance not to forget this.

Berta: *Did you consider any Hungarian CA?*

Bencsáth: If it would be a Hungarian CA, it would probably be Netlock. However, I think, it would take about two years till the services of Netlock would be mature enough. I don't think, I would get the same customer support from Netlock as I could get from Verisign. On the other hand, Verisign is a US company and it is hard to provide support from overseas. It is also the problem of foreign CAs that our company's papers have to be translated to English, which is quite awkward.

Berta: *If your business would expand, would you need more PKI certificates?*

Bencsáth: Not necessarily. Naturally, if one of our clients would request such service, we would organise for the client to buy one, but we do not plan to purchase more certificates in the future. I think the main problem of PKI is that clients know too little about it. They do not know that cheap (often free) tools exist for it too, and in case of tools that are advertised, they are very much frightened by the price.

D.3 NetAlfa Kft.

NetAlfa Kft. is a small company. NetAlfa provides various Internet-related services to its customers, and is also a reseller of notebook computers. Netalfa differentiates itself from its competitors by laying emphasis on security, reliability and providing customisable high-quality services.

Note that this company has significantly more knowledge on security-related issues and on PKI than its competitors.

I interviewed Attila Bognár, the CEO of Netalfa Kft.

Berta: *Do you have a PKI-enabled certificate or do you plan to buy one?*

Bognár: No, we don't have one, but I am considering buying one.

Berta: *Why do you think, you need a certificate?*

Bognár: In order to provide secure access to our web based services and mail servers. Currently we use certificates signed by our internal CA.

Berta: *If you intended to by a PKI-enabled certificate, which CA would you choose? Why?*

Bognár: If I bought a certificate, I would probably buy it from Netlock. Their CA's certificate is included in Internet Explorer, so users of Internet Explorer can access sites with Netlock certificates securely and conveniently. In case of certificates issued by other Hungarian CAs, Internet Explorer cannot verify if the website is authentic and the connection is secure. Thus, buying a certificate from a CA whose certificate is not included in Internet Explorer would not improve the situation significantly compared to our current self-signed solution.

Berta: *If your business would expand, would you need more PKI certificates?*

Bognár: With time, we would certainly buy more certificates, mainly for the sites and services that are used by non-professional users: customer portal, webmail site, mail services. Our web-sites intended for professional users/customers would not need it: the information of an in-house CA could be published on a site (customer portal) secured by a bought certificate, thus a secure chain can be built and these services can be considered secure enough for their purpose.

Our services can be found under `netalfa.net` domain. There is a possibility to buy wildcard (e.g. `netalfa.net`) certificates which could secure the whole domain, but this solution has two main problems:

- some client/customer domains are also hosted under `netalfa.net`, the company does

not want to take any responsibility for a third party

- this kind of philosophy that "let’s take a lot that will fit" does not conform to security: control can be loosed very quickly rising more and more problems

As we are a very small company the first step is to secure the customer portal buy a bought certificate, this way we can provide a reasonable security for all of our domains and can expand this infrastructure step by step.

E Basic financial information on market players

I have collected financial information on all five market players. These figures are presented to illustrate the size and profitability of these companies. To the best of my knowledge, each of these companies have other activities than being a CA, and the sales of the CA business unit does not constitute an important part of the sales of any of these companies. (Netlock might be an exception.)

In case of some companies, the proportion and significance of the CA business unit is little to the whole company. In these cases the following information cannot be used to judge the performance of the CA business unit. Matáv is clearly a giant, its figures were available in million HUF.

All figures are in thousand HUF.

Year: 2001	Giro	Matáv	Máv Info	Microsec	Netlock
Revenue	N.A.	547 735 000	4 528 051	540 260	24 064
Profit	996 942	82 560 000	41 055	269 474	973
Total Assets	7 666 939	1 104 196 000	2 484 405	335 219	89 014
Equity	6 924 635	460 300 000	866 221	106 703	27 725

Table 1

Year: 2002	Giro	Matáv	Máv Info	Microsec	Netlock
Revenue	N.A.	590 585 000	4 810 872	545 182	51 462
Profit	1 252 499	68 128 000	49 966	343 908	5 114
Total Assets	8 336 631	1 077 451 000	2 291 551	285 650	91 256
Equity	5 394 094	516 144 000	877 560	145 353	33 470

Table 2