Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2005 Proceedings

Americas Conference on Information Systems (AMCIS)

2005

Investigating in Security Solutions - Can Qualified Electronic Signatures be Profitable for Mobile Operators?

Heiko Rossnagel
Johann Wolfgang Goethe Universitat Frankfurt am Main, heiko.rossnagel@m-lehrstuhl.de

Denis Royer
Johann Wolfgang Goethe Universitat Frankfurt am Main, denis.royer@m-lehrstuhl.de

Investing in Security Solutions - Can Qualified Electronic Signatures be Profitable for Mobile Operators?

Heiko Rossnagel
Chair of Mobile Commerce and Multilateral Security
Johann Wolfgang Goethe-University Frankfurt
Heiko.Rossnagel@M-Lehrstuhl.de

Denis Royer
Chair of Mobile Commerce and Multilateral Security
Johann Wolfgang Goethe-University Frankfurt
Denis.Royer@M-Lehrstuhl.de

ABSTRACT

Electronic signatures are an established method to ensure the integrity and accountability of electronic transactions. Realizing their potential, the European Parliament and the Council enacted the directive 1999/93/EC in 1999, providing legal requirements for a common introduction of electronic signatures in Europe. However, so far the signature market has failed miserably. Mobile electronic signatures are often seen as a potential and promising way to provide market acceptance for electronic signatures. This paper proposes an infrastructure for qualified mobile electronic signatures that does not require the mobile operator to act as a certificate service provider (CSP). The user can freely choose a CSP and add the signature functionality along with the required certificates later on demand. However, mobile operators will only invest in this infrastructure, if they expect a return on investment (ROI). Therefore, based on our proposed infrastructure and using distinct scenarios, we conducted an investment analysis for mobile operators forecasting the net present value and the internal rate of return of the investment. Our forecast shows that issuing signature capable smart cards can be quite profitable for a mobile operator.

Keywords

Electronic Signatures, Mobile Signatures, ROI, IRR, NPV, Profitability, Business Models

INTRODUCTION

In the directive 1999/93/EC of the European Parliament and of the Council (DIRECTIVE 1999/93/EC, 1999) legal requirements for a common introduction of electronic signatures in Europe were enacted. The directive sets a framework of requirements for the security of technology used for electronic signatures. Based on certificates issued by certification authorities, which certify public keys for a person registered by a registration authority, electronic signatures can be created with a so-called "secure signature creation device" (SSCD), carrying the private keys of a person. The EC-directive distinguishes between "electronic signatures" and "advanced electronic signatures" (DIRECTIVE 1999/93/EC, 1999). Certification Service Providers can issue certificates for advanced signatures that will be qualified if they meet the requirements of Annex I of the directive. Those advanced signatures with qualified certificates will be referred to in this paper as qualified signatures.

The market share of EC-directive conforming signature cards is disappointingly low, failing to meet any involved party's expectations. This has partly been blamed on the incompatibility and missing standards of existing products. Also the lack of customers prevents companies from investing in signature products. As a result almost no commercial usage for qualified electronic signatures exists. Consequently no customers seek to obtain signature products.

There are several activities in Europe trying to enlarge the potential consumer base by putting key pairs on national identity cards (Cock, Wouters, and Preneel, 2004; Project „Feasibility Study Electronic Identity Card"). The rationale behind these initiatives is that a wide availability of signature capable chip cards will increase the potential customer base and therefore increase the availability of signature applications.

Also, mobile signatures are expected to have a great potential. These mobile signatures are electronic signatures that are created using a mobile device and rely on signature or certification services in a location independent telecommunication environment. They allow signatory mobility beyond a fixed, secure desktop workstation with trusted, personal signing equipment (Fritsch, Ranke, and Rossnagel, 2003). Although, using mobile devices for signature creation has several

shortcomings (e.g. display size, communication costs, limited computing power), the high market penetration of cell phones (GSM Association, 2005) and the mobility gained, make this approach potentially successful and promising.

Two possible signing approaches in the mobile environment have been proposed in the past: signatures created in centralized signing server environments located at service providers like mobile network carriers; and electronic signatures created inside the signatory's mobile device using a smart card. Rossnagel (2004) showed that server based signatures are unable to fulfill the requirement of Art.2, 2(c) of the EC-directive (DIRECTIVE 1999/93/EC, 1999) and, therefore, only client signatures can meet the requirements for advanced electronic signatures. Also, it was concluded that signature capable SIM[1] cards provide the most convenient solution for the customer. Therefore, we will limit our analysis to the economic feasibility of client SIM based signatures that meet the requirements of the EC-directive.

Mobile operators will only enter the signature market if they expect a profit in return. Given the current market situation this seems to be very unlikely. But there is also the possibility for the mobile operator to only issue the signature capable SIM card without offering any certification services. In that case, the customer can choose a certification service provider that issues a certificate for the public key stored on the SIM-card (Rossnagel, 2004). Therefore, the mobile operator will only make profits caused by traffic produced by the signature applications. A major benefit for mobile operators using this approach is that they do not have to build up their own trust center. Therefore, they do not face the huge installment and maintenance costs of such an infrastructure. Also, they do not have to compete with existing CSPs for a share of the market, but are able to cooperate with them to increase the overall market size.

However, using a single smart card for multiple purposes raises new questions and challenges. The SIM-card is issued by the telecommunication provider, while the SSCD used to be issued by a certification service provider. Combining both functions in one card raises the question how the CSP can issue a certificate for a card he never had in his possession. Rossnagel (2004) proposed a protocol called "Certification on Demand (COD)" that solves this problem.

As stated above a mobile operator will only invest in signature capable SIM-cards if an increase in revenue can be expected. Therefore, we are going to examine if enough traffic can be generated to make the issuing of signature capable SIM cards profitable for the mobile operator and also provide a prediction of the potential return on investment.

This paper is structured as follows: In section 2 we will outline our proposed infrastructure in detail. Since signature traffic will only occur if signature applications exist, we will show some potential applications for mobile signatures in section 3. In section 4 we will present our method of forecasting the potential benefits, as well as our initial assumptions. The results of our calculations will be presented in section 5 and in section 6 we will conclude our findings.

PROPOSED INFRASTRUCTURE

The mobile operator could sell SIM-cards equipped with a key generator for one or more key pair(s) which can be used for the signing functionality. After obtaining the SIM-card from the mobile operator, the customer can then generate the keys and activate the signature component and the public key(s) can be certified by any Certification Service Provider on demand.

Through the separation of the telephone functionality and the (possibly later) certification of the user's identity by a certification service provider, both functions can be sold separately and can be obtained from different providers.

The carrier will face increased costs for the signature capable SIM-card but can also expect increasing traffic caused by signature services. All distribution channels will remain unchanged.

Figure 1 illustrates the necessary steps for the distribution of the SIM-card and the certification process.

[1] Subscriber Identity Module

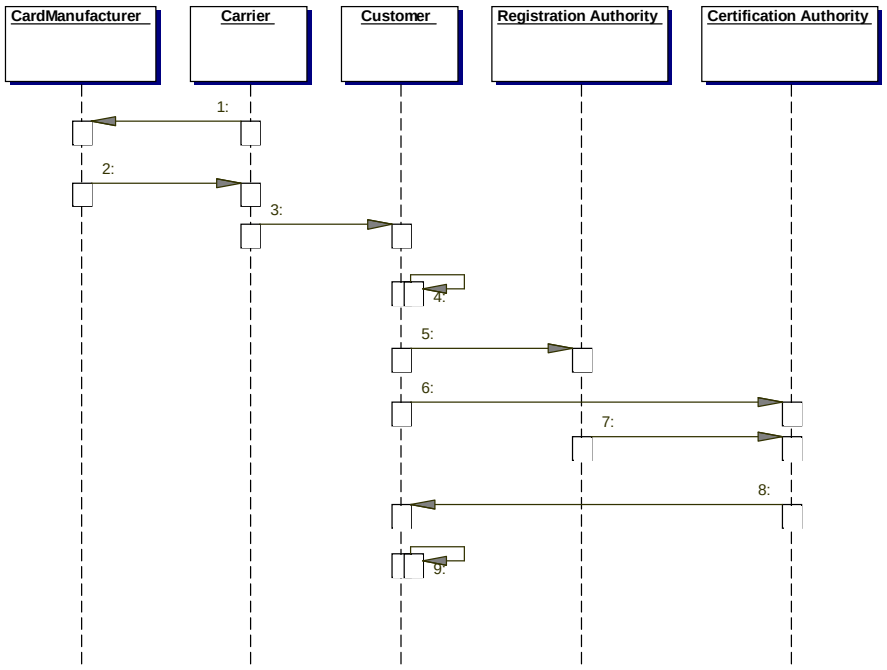

Figure 1. Certification on Demand Protocol

1. The carrier gives his IMSI[2] / Ki[3] pairs to a card manufacturer.
2. The card manufacturer returns a SIM card containing an IMSI/Ki pair, a key generator for the signature application and the public key of the RootCA[4] to the carrier.
3. The SIM card is sold to the customer and the carrier provides a nullpin that is used to generate the keys and activate the signing functionality.
4. The customer generates the keys and activates the signing functionality by entering the nullpin.
5. The customer registers at a Registration Authority of his choice, providing identification information and his public key.
6. The customer sends his identification information signed with his private key over the air to the Certification Authority.
7. The Registration Authority sends the public key and the identification information to the Certification Authority.
8. If the information provided by the customer and the Registration Authority match, the Certification Authority issues a certificate for the customer and sends it over the air to his mobile phone.
9. The user can verify the validity of his certificate by checking the certificate issued by the RootCA of the Certification Service Provider.

This protocol makes no changes to the existing distribution infrastructure of mobile operators. The steps 1 to 3 remain the same way they used to be before, apart from the fact that the card manufacturer puts additional information and functionality (signature key generator, public key of RootCA) on the SIM card. In order to ensure that the card manufacturer does not know the private key of the user the key generation should be done by the card. The customer is not forced to certify his keys and can use the SIM for telephone functionality only. He could also activate the signing functionality without going through

[2] International Mobile Subscriber Identity
[3] Individual subscriber authentication key
4 Root Certification Authority

the certification process for example as a security token. If he wants to be able to make legally binding electronic signatures, he has to go through the complete process to obtain a qualified certificate. He can do this by freely choosing the CSP.

The nullpin to generate the keys and activate the signing functionality in step 4 is used to ensure that no signatures can be created before the customer has control over the SIM card. If the signature application has been activated before, the user will recognize this when entering the nullpin.

Step 6 could be omitted but serves as insurance for the customer to ensure him that the integrity of his identification information will be preserved.

If the customer wants to change his CSP, he only has to repeat steps 5 to 9 with his new CSP. If the customer wants to change his carrier, he has to go through the whole protocol again, but can register with his current certification service provider. (Rossnagel, 2004)

POSSIBLE APPLICATIONS

Enabling Security Infrastructures

There is a need of corporations to provide their mobile workforce with secure access to the corporate backend. So far security tokens have been used to allow this functionality. These tokens are expensive and stored on extra hardware that needs to be carried around and can easily be lost. Putting these credentials on a SIM, that will be placed in the mobile phone, reduces the risk of losing the credential as well as the costs. But some corporations greatly object to leave their private keys and certificates in the hands of their mobile operator.

With Certification on Demand the corporation's IT security department can obtain COD enabled SIMs from the corporation's cellular contractor and initializes them for the corporate mobile security infrastructure. The WiTness project (WiTness, 2005) sponsored by the European Union implemented such an infrastructure.

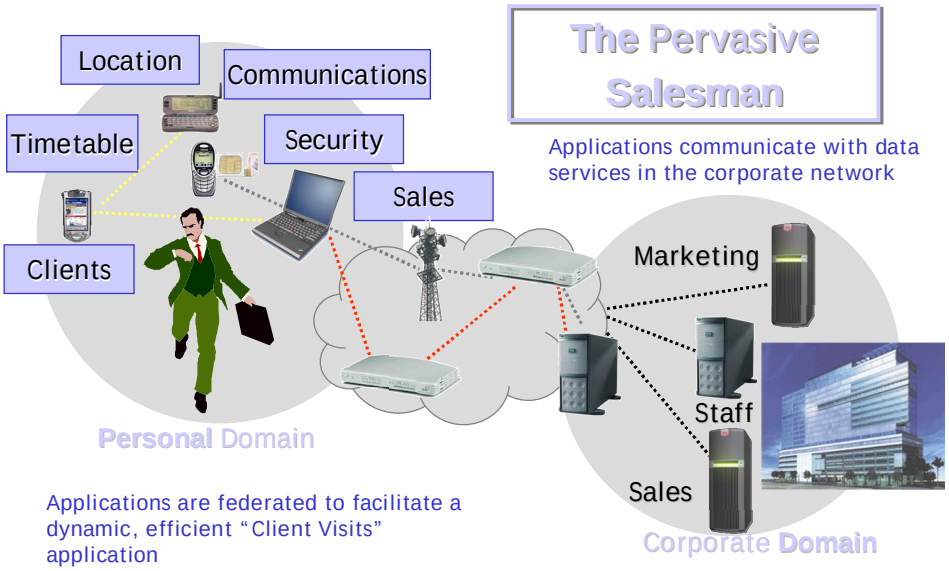

Figure 2. WiTness Pervasive Salesman Scenario

Figure 2 shows an application scenario where a "*pervasive salesman*" has secure, corporate-controlled access to all data available to him in the corporate information system. Access is controlled by a security module based on a SIM with additional security functionality.

Multilateral secure financial transactions

Storing bank credentials on a SIM may help the migration from plastic to mobile phones. A COD infrastructure allows financial institutions to certify and enable mobile subscribers to use banking services online through their mobile terminal and SIM. Credentials could be certified by the bank itself, like the credentials used on bank cards. Therefore, the bank can still have the control over the credentials while the mobile operator still can issue the SIM cards without giving their IMSI/Ki pairs away to the bank. This would enable the bank to offer services like transactions, brokerage or checking the account balance based on the credentials stored in the SIM. This functionality can and has been realized without the Certification on Demand protocol but only if the banks and carriers are willing to cooperate. In the Czech Republic T-Mobile (T-Mobile) and the Czech banks agreed to send their critical information to Giesecke & Devrient, a card manufacturer who started producing banking enabled SIMs (Giesecke & Devrient, 2005). However, the COD protocol would enable banks to use SIMs as credentials without having a contract with the mobile operator. This would also enable the banks to offer new services for their customers. Price shocks on the capital market following company announcements are one example. As efficient capital markets react very quickly to new information available, private investors require combined mobile notification and transaction services. So far, existing concepts can not fulfill these requirements which results from inappropriate implementation of the security mechanisms in order to realize secure and trustworthy processing. A COD based system could provide secure information and transaction processing in time by permitting a smart integration of notification and transaction services (Muntermann, Rossnagel and Rannenberg, 2005).

Enabling mobile electronic consent and identity management

Many mobility applications rely on a user's consent towards reducing his privacy for a particular service. Examples are location based services on cellular networks, situation based marketing scenarios and tracking technology following users to support them with information they need in-time and in-place. A secure provable electronic consent of users can be achieved using electronic signatures on SIM-created credentials that may contain information about time, intent and recipient of the electronic consent. Research has found SIMs to be on the edge of a global identity management infrastructure (Rannenberg, 2004). In the near future, personal or role attributes customized for particular application areas (e.g. online dating, identity management) could be managed on SIMs on demand from their owners.

OUR FORECASTING APPROACH

Forecasting Method

The complex nature of the mobile communication market and its key players make it difficult to come up with a generalized approach for the prediction of future trends. Nevertheless, using a combination of different methods, such as simulation, investment theory, or scenario techniques, one can analyze the possible direction of the future development of such technologies and their diffusion into the market (Potthof, 1998).

Looking at the approach taken for this analysis, the market for mobile signatures was modeled from the mobile operator's perspective. In order to display the diffusion rate of the COD technology, it is important to anticipate the willingness of the customers to switch to the technology. Based upon the number of users in the market for mobile signatures, one can forecast the additional data traffic, produced by the signature applications by each individual user. Furthermore, this data traffic generates revenue for the mobile operator.

An evaluation scheme must fulfill several prerequisites in order to produce an adequately complete and thorough analysis of the subject matter:

- Firstly, the underlying assumptions taken as basis for an analysis need to be realistic. This can be done by analyzing similar technologies and using their results as analogies.
- Moreover, the collected data should be complete, in order to present a self-contained view of the analyzed market.
- The modeling of the underlying environment should also take other market effects into account, such as additional costs, switching costs, network effects, etc.
- Based upon the gathered data, it is important to determine the impact of the different parameters on each other. One possibility of doing this is to analyze the network effects of the market and its participants (Shapiro and Varian, 1998).
- Static evaluations (e.g. ROI analysis) of an investment should be avoided. A better way of determining the worth of an investment is to use dynamic methods, such as the internal rate of return (IRR) or the net present value (NPV)

(Franklin, 2002). While the static methods work with periodic mean values, the dynamic methods examine the actual present value over the complete runtime of an investment. The main difference is the consideration of the cash in- and outflows and their present value over time. This gives a more accurate view upon the development of the investment (Blohm and Lüder, 1995).

- Although a thorough collection and analysis of the present data is a good foundation for an evaluation, one has to deal with uncertainties in the development of the parameters (Potthof, 1998). In order to adequately forecast such effects, methods such as the scenario technique presented by Geschka and Hammer (1997) offer a good approach to estimate those effects.
- Lastly, the results have to be comprehensible for third parties, in order to allow the validation of the initial assumptions (Franklin, 2002).

Based upon these requirements, we conducted our analysis by combining the scenario technique (using 2 distinct scenarios), market modeling, dynamic investment calculations, and market analogies.

Initial Assumptions

For the analysis conducted here, we chose a time period of 3 years and two basic scenarios (namely: *optimistic* and *conservative*) for the development of the market segmentation, the market composition, and the market growth:

Starting with the segmentation of the market for mobile signatures, we assumed that the market can be split into three different consumer panels, representing the different usages by the user (*assumption 1*), namely pro, mid, and private users. While for example private users only generate a small amount of data traffic, it is more likely that pro users will be the key players in this market, similar to the early days of mobile telecommunications (Grüber and Verboven, 2001). Furthermore, we assumed that the distribution of the panels is mainly composed of pro and mid users (*assumption 2*). This is based upon the fact that mobile signatures will be initially used for professional purposes, as described in the WiTness scenario. Though having the biggest future potential in the market growth, the home users only play a minor role here. Table 1 gives an overview of the market composition and segmentation for the chosen scenarios analyzed here:

		Optimistic			***Conservative***		
		Traffic per Quarter:					
Panel / Market Segmentation		*Year 1*	*Year 2*	*Year 3*	*Year 1*	*Year 2*	*Year 3*
Pro Users	*(60,00%)*	1000kB	1500kB	2500kB	600kB	800kB	1200kB
Mid Users	*(30,00%)*	500kB	750kB	1000kB	150kB	200kB	250kB
Private Users	*(10,00%)*	100kB	200kB	250kB	50kB	75kB	125kB

Table 1. Development of the data-traffic per quarter

Based on usage studies for mobile services, we used an average amount of 5kB for a certification service transaction (UMTS Forum, 2003). Taking the optimistic case for a pro user in year 1 as an example, this would sum up to 200 transactions per quarter (about 63 working days), which would mean that an average "pro" user would conduct about 3 certification service transactions per working day (*assumption 3*). This is still a considerably low and conservative number. Especially, if you consider that a lot of the traffic will not be caused by certification services themselves, but instead by applications that have been impossible to be offered without electronic signatures. An example for such applications is the usage of information and transaction services in a mobile brokerage scenario (Muntermann, Rossnagel and Rannenberg, 2005).

Furthermore, the market growth for the given period must also be taken into consideration. Studies have overestimated the PKI market and predicted an annual growth until 2003 of 73% (Datamonitor, 1999). In order to avoid the same mistake we used the actual growth rate of a similar technology to predict our projected market development. We chose to use the development of Secure Socket Layer (SSL) (IDC, 2004) as the basis of our prediction of the rate of market growth in the optimistic scenario, because this technology is similar to electronic signatures in two major ways (*assumption 4*). Both are preventive innovations because they lower the probability that some unwanted event (loss of confidentiality for SSL; loss of integrity and accountability for electronic signatures) may occur in the future (Rogers, 2003). Also, electronic signatures, as well as SSL, are interactive innovations, meaning that they are of little use to an adopting individual unless other individuals with whom the adopter wishes to communicate also adopt (Rogers, 2003).

Since this interactive quality creates interdependence among the adopters in the system (Rogers, 2003), we acknowledged that the more market participants are available and the more services are offered, the more people will actually enter the market for mobile qualified electronic signatures. These positive network effects (Shapiro and Varian, 1998) are represented by an increasing market growth of the customer base per quarter (*assumption 5*). For the optimistic scenario we based our

predicted growth rates on the current growth rates for SSL products (35%). We started with a growth rate of 15% for the first year and increased it, for simplification purposes, by a fixed annual value of 15% (*assumption 6*) (see Table 2). For the conservative scenario on the other hand, the initial starting point for the market growth is 10% with an annual fixed growth rate of 2.50% (*assumption 7*). Again, this is used as a simplification, assuming that the market for mobile signature services will mostly be used for certain specialized applications (e.g. access to company portals). This also takes into consideration that the overall market for additional services will not be as successful and innovative as anticipated before. However, even in this niche market scenario, a small but steady growth of 2.50% per year can be expected, especially in the sector of applications targeted on the professional market.

	Optimistic			*Conservative*		
	Year 1	*Year 2*	*Year 3*	*Year 1*	*Year 2*	*Year 3*
Market Growths	15.00%	30.00%	45.00%	10.00%	12.50%	15.00%

Table 2: Market growth

For the initial customer base, we assumed a quantity of 10,000 (conservative) to 15,000 (optimistic) SIMs in the market, depending on the taken scenario (*assumption 8*). These customers could for example stem from prototype projects, conducted by the mobile operator or certification service providers, which will stay in the market after the inital testing phase of this technology.

In order to calculate the actual revenue for the financial analysis, we used the current average price for GPRS data-traffic of mobile operators in Germany of 0.01€ per KB (*assumption 9*). Moreover it is likely that future prices for data traffic will be significantly lower. So, a decline of the price for data traffic of 25% per year has also been taken into consideration (*assumption 10*).

Looking at the investment that has to be done by the mobile operator, we identified the costs for the initial evaluation of the SIM against EAL 4+ of the Common Criteria (150,000 €) (*assumption 11*) and the costs for the initial setup of the infrastructure (500,000 €), such as additional personnel costs and billing systems (*assumption 12*). Furthermore, the mobile operator has to issue the crypto enabled SIM to its customers, whereby additional, variable costs will arise (*assumption 13*). For our calculation we used the average price, a mobile operator charges to its customers for the exchange of a SIM-card (about 20.00€ per card). These costs are bound to the number of new mobile users, being added to the market (*assumption 14*). Moreover, a fixed sum of 200,000€, for the additional annual personnel and process costs, is added to the cash outflows (*assumption 15*). By using a higher value for this parameter, the actual cash outflows would be overcompensated, due to the fact that parts of the personnel and process costs are already covered by the exchange fee for the crypto enabled SIM (*assumption 16*). Finally, we used the current yield of 3.85% as interest rate for our financial calculations, representing the market's interest rate for general investments and being our comparative value for the IRR (*assumption 17*).

RESULTS

Starting with our initial customer base of 10,000 SIMs for the conservative scenario and 15,000 SIMs for the optimistic one and using our assumption for the market growth (see Table 2) we projected the customer base development. By the end of year 3 and using the optimistic scenario, about 300,000 customers have entered the market, while in the conservative scenario only 40,000 users are actively using the proposed infrastructure. Figure 3 illustrates this prediction of the market development.

In the optimistic scenario the critical mass of customers in order to induce positive network effects (Shapiro and Varian, 1998) will be reached in quarter 9. These positive network effects lead to a very high diffusion rate of the product in the following quarters.

In the conservative scenario, however, the critical mass necessary to achieve positive network effects will not be reached within our 3 year time frame of this analysis. Therefore, the adoption of the proposed technology will be significantly slower.

Based upon this customer base development, we calculated the potential annual cash in- and outflows for a 3-year period, using the projected traffic per user and group and the projected price per KB. Also, the temporal variances of the price and the traffic usage were taken into consideration. The results are shown in Table 3.

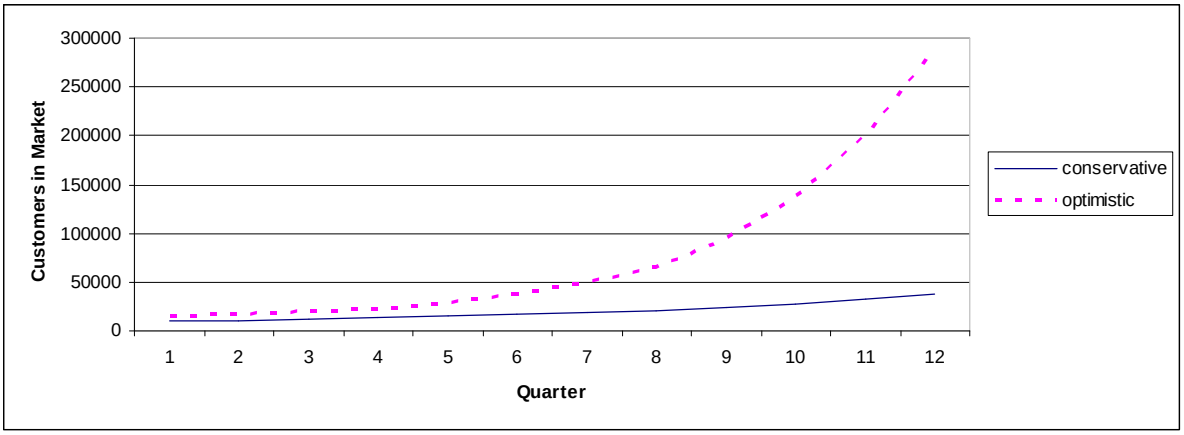

Figure 3. Customer base development.

	Year 1	*Year 2*	*Year 3*
	Optimistic Scenario		
Cash Inflows	569,233.00 €	1,575,567.00 €	7,371,262.00 €
Cash Outflows	-356,240.00 €	-1,046,760.00 €	-4,656,860.00 €
Result	212,993.00 €	528,807.00 €	2,714,402.00 €
	Conservative Scenario		
Cash Inflows	190,282.00 €	295,990.00 €	555,987.00 €
Cash Outflows	-266,200.00 €	-360,140.00 €	-519,280.00 €
Result	-75,918.00 €	-64,150.00 €	36,707.00 €

Table 3. Projected Cash In- and Outflows

The results of the preliminary stages can now be used for the assessment of the investment. As Table 4 shows, the optimistic scenario will reach the break-even within 1.91 years and the IRR will reach a 90.52% for the analyzed 3-year period. The conservative scenario on the other hand will not reach the break even point within the timeframe of our analysis, due to its slower growth of the customer base. The same effects also apply to the IRR, which is negative. The development of the net present value of both alternatives is illustrated in Figure 4.

	Optimistic	Conservative
NPV after 3 Years	2,468,986.91 €	-749,811.26 €
Payback Period	1.91 Years	> 3 Years
IRR after 3 Years	90.52%	Negative

Table 4. Results of the investment calculation.

In the optimistic scenario the investment into mobile signatures would be very advisable for mobile operators, generating a considerable amount of revenue.

Although not looking attractive from a mobile operator's perspective, the conservative scenario will break-even, once reaching the critical mass. Due to our further calculations, this scenario will be profitable by year 5.

Since both scenarios represent extreme cases, we expect that the actual market development will be within this range. Therefore, the investment into mobile signatures based upon our proposed infrastructure seems to be profitable.

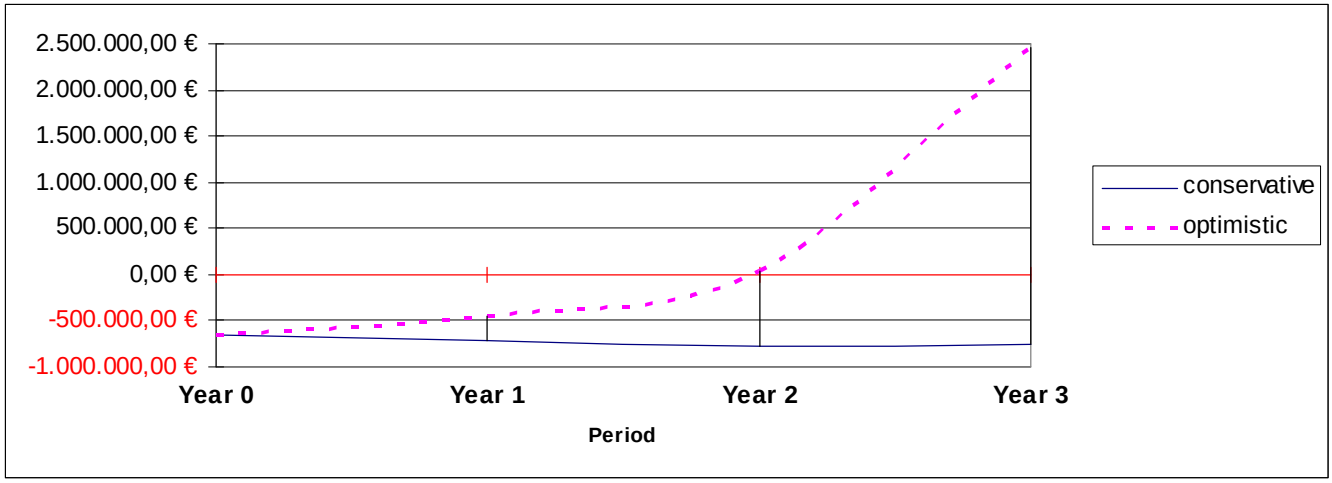

Figure 4. Development of the investments' NPV

CONCLUSION

Mobile signatures are a promising approach to break the deadlock between missing customers and missing applications. The high market penetration of mobile phones enables certification service providers to target millions of potential customers. We proposed an infrastructure that allows the mobile operator to only act as the card issuer while earning revenue from the transferred data, caused by signature services. The qualified certificate of the user will be issued by a certification service provider of his choice, enabling market competition between CSPs. However, a mobile operator will only issue signature capable SIM cards if a positive return on investment can be expected.

Therefore, we presented a forecast of the potential market development, using two extreme scenarios (optimistic and conservative) and a set of initial assumption, based upon the market mechanisms of related technologies. By means of these basic figures, we projected the potential cash in- and outflows for each scenario. As our results show, mobile qualified electronic signatures seem to be a profitable investment for mobile operators.

REFERENCES

1. Blohm, H. and Lüder, K. (1995) Investition: Schwachstellenanalyse des Investitionsbereichs und Investitionsrechnung, 8th edition,Vahlen, Munich
2. de Cock, D., Wouters, K. and Preneel, B. (2004) Introduction to the Belgian EID Card, in Sokratis K. Katsikas, Stefanos Gritzalis and Javier Lopez, eds., *Public Key Infrastructures*. Berlin Heidelberg: Springer, pp. 1 - 13.
3. Datamonitor (1999) Global PKI Markets, 1999- 2003.
4. DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures
5. Franklin jr, C. (2002) The ABCs of ROI, in: Network Computing, 29th April 2002, p.93–95
6. Project Feasibility Study Electronic Identity Card (2005), www.uni-kassel.de/fb10/oeff_recht/english/projekte/projekteDigiPersoeng.ghk
7. Fritsch, L., Ranke, J. and Rossnagel, H. (2003) Qualified Mobile Electronic Signatures: Possible, but worth a try? In: Information Security Solutions Europe (ISSE) Conference, Vienna Austria
8. Geschka, H. and Hammer, R. (1997) Die Szenario Technik in der strategischen Unternehmensplanung, in: D. Hahn, B. Taylor (1997): "Strategische Unternehmensplanung - strategische Unternehmensführung", 7th Edition, Physica , Heidelberg, 1997, pp.464-489
9. GSM Association (2005) GSM Statistics, www.gsmworld.com/news/statistics/index.shtml

10. Giesecke & Devrient (2005) STARSIM® Applications, STARSIM®banking; www.gdm.de/eng/products/04/index.php4 ?product_id=386
11. Gruber, H. and Verboven, F.(2001) The Diffusion of Mobile Telecommunication Innovations in the European Union, European Economic Review 45: 577-588.
12. Kolodgy, C. and Pintal, G. (2004) IDC - Worldwide SSL-VPN Appliance 2005-2009 Forecast and 2004 Vendor Shares:
Delivering Secure Application Access.
13. Muntermann, J., Rossnagel, H. and Rannenberg, K. (2005). Mobile Brokerage Infrastructures - Capabilities and Security Requirements. Proceedings of the 13th European Conference on Information Systems (ECIS 2005), Regensburg, 2005.
14. Potthof, I. (1998) Kosten und Nutzen der Informationsverarbeitung: Analyse und Beurteilung von Investitionsentscheidungen, DUV/Gabler, Wiesbaden, 1998
15. Rannenberg, K. (2004) Identity Management in Mobile Cellular Networks and Related Applications In: Information Security Technical Report, Vol. 9, No. 1; 2004; pp. 77 – 85; ISSN 1363-4127; Elsevier Sciences
16. Rogers, E. M. (2003) The Diffusion of Innovations, Fifth Edition, Free Press, New York, London, Toronto, Sidney
17. Rossnagel, H. (2004) Mobile Signatures and Certification on Demand, in Sokratis K. Katsikas, Stefanos Gritzalis and Javier Lopez, eds., Public Key Infrastructures. Berlin Heidelberg: Springer, 2004, pp. 274-286.
18. Shapiro, C.; Varian, H.R. (1998): Information rules: A strategic Guide to the Network Economy, Boston.
19. T-Mobile (2005) Czech Republic: m-payment becomes a universal payment tool for customers; www.t-mobile.net/CDA/news_details,20,0,newsid-1799,en.html?w=925&h=588
20. UMTS Forum (2003) 3G Offered Traffic Characteristics, UMTS Forum Spectrum Aspects Group (SAG), No. 33, Nov 2003
21. European IST Project (2005) Wireless Trust for Mobile Business (WiTness), www.wireless-trust.org