Association for Information Systems
AIS Electronic Library (AISeL)

PACIS 2005 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

December 2005

Profitability of Mobile Qualified Electronic Signatures

Heiko Rossnagel
University Frankfurt

Denis Royer
University Frankfurt

Profitability of Mobile Qualified Electronic Signatures

Heiko Rossnagel
Chair of Mobile Commerce and
Multilateral Security –
University Frankfurt
heiko.rossnagel@m-lehrstuhl.de

Denis Royer
Chair of Mobile Commerce and
Multilateral Security –
University Frankfurt
denis.royer@m-lehrstuhl.de

Abstract

In 1999 the directive 1999/93/EC of the European Parliament and of the Council was enacted, providing legal requirements for a common introduction of electronic signatures in Europe. 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 builds upon an infrastructure for qualified mobile electronic signatures proposed by Rossnagel (2004) 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. In this paper we will take a look at the economic feasibility of mobile qualified electronic signatures from the viewpoint of a mobile operator (MO) and try to predict his return on investment. We also examine potential revenues for CSPs using new business models as proposed by Lippmann and Rossnagel (2005) that have the potential to be far more successful than the current ones. Our prediction shows that mobile qualified electronic signatures can be quite profitable for a mobile operator as well as the CSPs.

Keywords: Electronic Signatures, Mobile Signatures, ROI, Profitability, Business Models

1. 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 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). An advanced electronic signature is defined as an electronic signature that meets the following requirements:

"*(a) it is uniquely linked to the signatory;*
(b) it is capable of identifying the signatory;
(c) it is created using means that the signatory can maintain under his sole control; and
(d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;" (DIRECTIVE 1999/93/EC 1999)

Certification service providers (CSP) 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 et al. 2004; Project „Feasibility Study Electronic Identity Card" 2005). 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 to break up this deadlock of missing applications and customers. 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 fixed, secure desktop workstations with trusted, personal signing equipment (Fritsch et al. 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 effort potentially successful and promising.

Two possible signing approaches in the mobile environment have been proposed in the past: signatures created in centralised signing server environments located at service providers like mobile network carriers; and electronic signatures created inside the signer's mobile device using a smart card. Ranke et al. (2003) concluded that only client signatures are capable to meet the requirements for advanced electronic signatures of the EC-directive. Also Rossnagel (2004) concluded that signature capable subscriber identity module (SIM) cards provide the most convenient solution for the customer.

However, 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 if the mobile operator (MO) has to operate its own trust center. 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 has to choose a certification service provider (CSP) 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 the traffic of signature applications. This would also enable CSPs to reach a lot of potential adopters of their technology and to increase their customer base. Of course the CSPs must be willing to accept the standard set by the MO, but given their current losses they should have a major interest in doing so.

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), which solves this problem.

As stated above a mobile operator will only invest in signature capable SIM cards if he expects an increase in revenue. Therefore, we are trying to forecast if enough traffic can be generated to make the issuing of signature capable SIM cards profitable for the mobile operator and also to provide a prediction of the potential return on investment. In addition, we will examine the potential revenues gained by the CSP, when accepting such mobile signatures and using new business models as proposed by Lippmann and Rossnagel (2005).

This paper is structured as follows: In section 2 we will outline the infrastructure proposed in (Rossnagel 2004) on which our calculations are based upon. In section 3 we will present our method of forecasting the potential benefits as well as our initial assumptions. In section 4 the results of our calculation will be presented and in section 5 we will show the limitations of our work. Section 6 concludes our findings.

2. 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 probably face increased costs for the signature capable SIM card but can also expect an increase in 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.

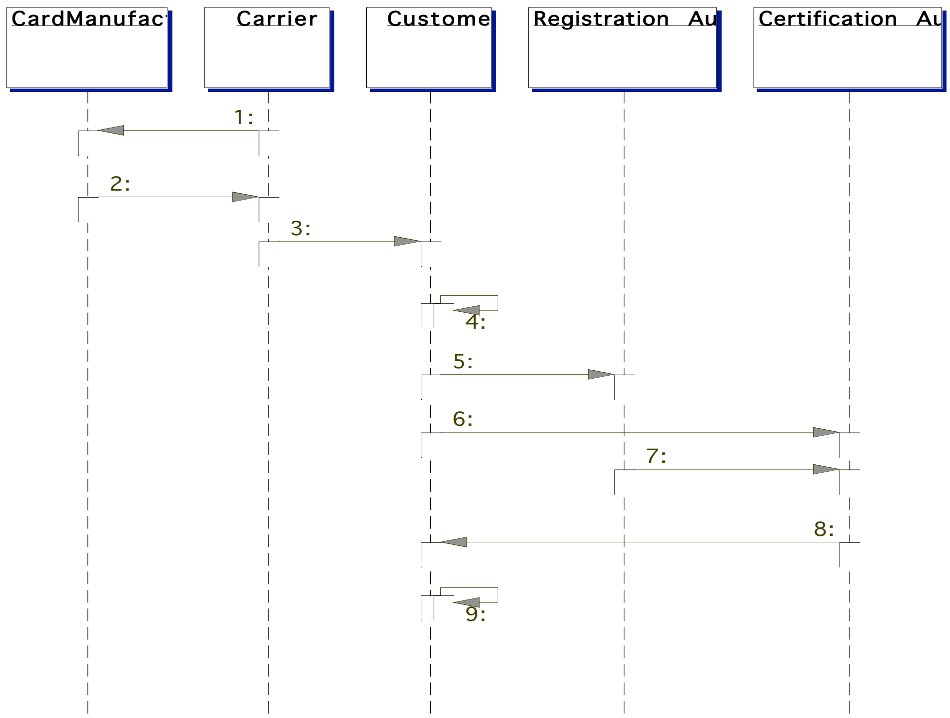

Figure 1 Certification on Demand Protocol

1. The carrier gives his international mobile subscriber identity (IMSI) / individual subscriber authentication key (Ki) 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 root certification authority (RootCA) 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 (RA) 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 (CA).
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 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 recognise 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)

3. Our Forecasting Approach

The complex nature of the mobile communication market and its key players make it difficult to come up with a generalised approach for the prediction of future trends. Nevertheless, using a combination of different methods, such as simulation, investment theory, or scenario techniques, one can analyse 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 modelled 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 and certification transactions for the CSP.

An evaluation scheme must fulfil 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 analysing 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 analysed market.
- The modelling of the underlying environment should also take other market effects into account, such as additional costs, switching costs, or network effects.
- 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 analyse the network effects of the market and its participants (Shapiro and Varian 1998).
- Static evaluations (e.g. return on investment (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 modelling, dynamic investment calculations, and market analogies.

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 for both market players. 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 internal rate of return (IRR).

3.1 Initial Assumptions for a Mobile Operator

Starting with the general segmentation of the market for mobile signatures, we assumed that the market can be split into three different consumer panels, representing the different usage by the users (*assumption MO1*), 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 (Gruber and Verboven 2001). Furthermore, we assumed that the distribution of the panels is mainly composed of pro and mid users (*assumption MO2*). This is based upon the fact that mobile signatures will most likely be used for professional or corporate purposes, as outlined before. Though having the biggest future potential in the market growth, the private users only play a minor role here. Table 1 gives an overview of the market composition and segmentation for the chosen scenarios analysed 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

Using a 5KB payload per transaction (UMTS 2003) and taking the optimistic case for a pro user in year 1, this would sum up to about 200 transactions per quarter (about 63 working days). This results in approximately 3 transactions per day (*assumption MO3*). However, these figures are still considerably low and conservative numbers, considered that a lot of the traffic will not be caused by certification services themselves, but instead by new applications that have not been possible to be offered without electronic signatures. An example for such an application is the usage of information and transaction services in a mobile brokerage scenario as proposed by Muntermann, et al. (2005).

Furthermore, the market growth for the given period must also be taken into consideration. In the past, 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 make our projections for the market development. Looking at our optimistic scenario, we chose to use the development of Secure Socket Layer (SSL) as the basis of our prediction of the rate of market growth (IDC 2004) (*assumption MO4*).

This technology is similar to electronic signatures in two major ways:

1. 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).
2. Secondly, electronic signatures, as well as SSL, are interactive innovations. This means that they are of little use to an adopting individual unless other individuals with whom the adopter wishes to communicate also adopt (Mahler and Rogers 1999).

Based on the notion that this interactive quality creates interdependence among the adopters in the system (Rogers 2003), we concluded that the more market participants are available and the more services are offered, the more people are actually willing to enter the market for mobile qualified electronic signatures. These positive network effects (Shapiro and Varian 1998; Economides 1996; Katz and Shapiro 1986) are represented by an increasing market growth of the customer base per quarter (*assumption MO5*).

For the optimistic scenario we based our predicted growth rates on the current growth rates for SSL products 35% (IDC 2004). For simplification purposes, we started with a growth rate of 15% for the first year, increasing it, by a fixed annual value of 15% (*assumption MO6*) (see Table 2). For the conservative scenario on the other hand, the initial market growth is 10% with an annual fixed growth rate of 2,50% per quarter (*assumption MO7*). Again, this is used as a simplification, assuming that the market for mobile signature services will mostly be used for certain specialised applications (e.g. access to company portals) or other niche-market constellations. This also takes into consideration that the overall market for additional services will not be as successful and innovative as expected in the optimistic scenario. However, even in the outlined 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 MO8*). 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 initial testing phase of this technology.
In order to calculate the actual revenue for our financial analysis, we used the current average price for GPRS data traffic of mobile operators in Germany of 0,01 € per KB (*assumption MO9*). Moreover, it is likely that future prices for data traffic will be significantly lower. In order to compensate this effect, a decline of the price for data traffic of 25% per year has also been taken into consideration (*assumption MO10*).
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 M11*) and the costs for the initial setup of the infrastructure (500.000 €), such as additional personnel costs and billing systems (*assumption MO12*). Furthermore, the mobile operator has to issue the crypto enabled SIM to its customers, whereby additional, variable costs will arise (*assumption MO13*). 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 MO14*). Moreover, a fixed sum of 200.000 € for the additional annual personnel and process costs is added to the cash outflows (*assumption MO15*). By using a higher value for this parameter, the actual cash outflows would be overcompensated. This is based on the assumption that parts of the personnel and process costs are already covered by the exchange fee for the crypto enabled SIM (*assumption MO16*).

3.2 Initial Assumptions for a Certification Service Provider

For the CSP, we took a similar approach: Based upon the traffic figures for a mobile operator and using the scenario laid out by Lippmann and Rossnagel (2005), we modelled the market for a CSP. Table 3 gives an overview of the pricing scheme for a certification transaction (*assumption CA1*) and the distribution of the market segments with regard to the mobile operator (*assumption CA2*). Moreover, the average size of a transaction is presented (*assumption CA3*), which is used to calculate the actual number of transactions per user, using the traffic data of the mobile operator as a starting point (cp. Table 1):

User Panel / Rate / Market share		*Initial Costs*	*Basic Rate / Year*	*Certification Transaction*	*Average KB / Transaction*
Pro Users	*Public (33,3%)*	0,00 €	60,00 €	0,05€	60KB
	Business (33,3%)	0,00 €	30,00 €	0,10€	60KB
	Flatrate (33,3%)	0,00 €	85,00 €	0,00€	60KB
Mid Users	*Independence*	0,00 €	15,00 €	0,25€	35KB
Private Users	*Starter*	15,00 €	0,00 €	0,40€	20KB

Table 3: Pricing scheme and market composition for the CSP

Looking at the investment that has to be done by an existing CSP, we estimated 5 Mio € for the setup, the initialisation of the needed infrastructure, and the adaptation of the existing processes, in order to offer such services (*assumption CA4*). Furthermore, 1 Mio € per year has to be spent for the additional running costs, including items such as personnel cost (*assumption CA5*).

4. Results

Starting with an initial customer base of 15.000 SIMs for the optimistic and 10.000 for the conservative scenario and using our assumptions 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 56.000 users are actively using the proposed infrastructure. Figure 2 illustrates this prediction of the market development.

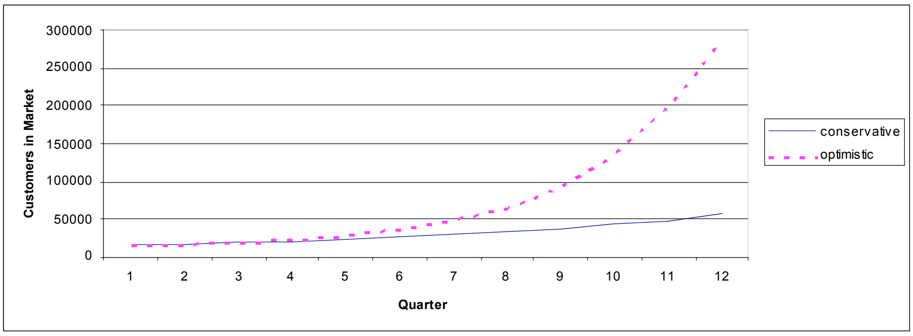

Figure2: Customer base development

Looking at the optimistic scenario, the critical mass of customers, in order to induce positive network effects (Shapiro and Varian 1998; Economides 1996; Katz and Shapiro 1986), will be reached in quarter 9, leading 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, compared to the optimistic scenario.

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 for the MO and the CSP are shown in Table 4 and 5.

	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	285.422,00 €	444.008,00 €	834.056,00 €
Cash Outflows	-299.300,00 €	-460.260,00 €	-678.980,00 €
Result	-13.878,00 €	3.748,00 €	138.460,00 €

Table 4: Projected Cash In- and Outflows for the Mobile Operator

	Year 1	*Year 2*	*Year 3*
		Optimistic Scenario	
Cash Inflows	452.903,00 €	2.550.297,00 €	14.221.343,00 €
Cash Outflows	-1.000.000,00 €	-1.000.000,00 €	-1.000.000,00 €
Result	-547.098,00 €	1.550.297,00 €	13.221.343,00 €
		Conservative Scenario	
Cash Inflows	253.803,00 €	794.524,00 €	2103.045,00 €
Cash Outflows	-1.000.000,00 €	-1.000.000,00 €	-1.000.000,00 €
Result	-746.197,00 €	-205.476,00 €	1.103.045,00 €

Table 5: Projected Cash In- and Outflows for the CSP

The results of the preliminary stages can now be used for the evaluation of the investment. As Table 6 shows, the optimistic scenario for the mobile operator will payback within 1,91 years and for the CSP within 2,35 years. The IRR will reach a 90,52% for the MO and 42,01% for the CSP for the analysed 3 year period. The conservative scenarios on the other hand will not reach the break even point within the timeframe of our analysis, due to their slower growth of the customer base. The same effects also apply to the IRR, which is negative in both cases. The development of the net present value of both market players is illustrated in Figure 3.

	Opt. MO	Con. MO	Opt. CSP	Con. CSP
NPV after 3 Years	2.468.986,91 €	-521.428,01 €	7.715.396,02 €	*-4.924.198,16 €*
Payback Period	1,91 Years	> 3 Years	2,35 Years	> 3 Years
IRR after 3 Years	90,52%	Negative	42,01%	Negative

Table 6: Results of the investment calculation

In the optimistic scenario the investment into mobile signatures would be very advisable for mobile operators and CSPs, generating a considerable amount of revenue. Although not looking attractive, the conservative scenarios will break even, once they reach a critical mass of adopters. Due to further calculations we conducted, investing into mobile signatures 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 the proposed infrastructure seems to be profitable for all market players.

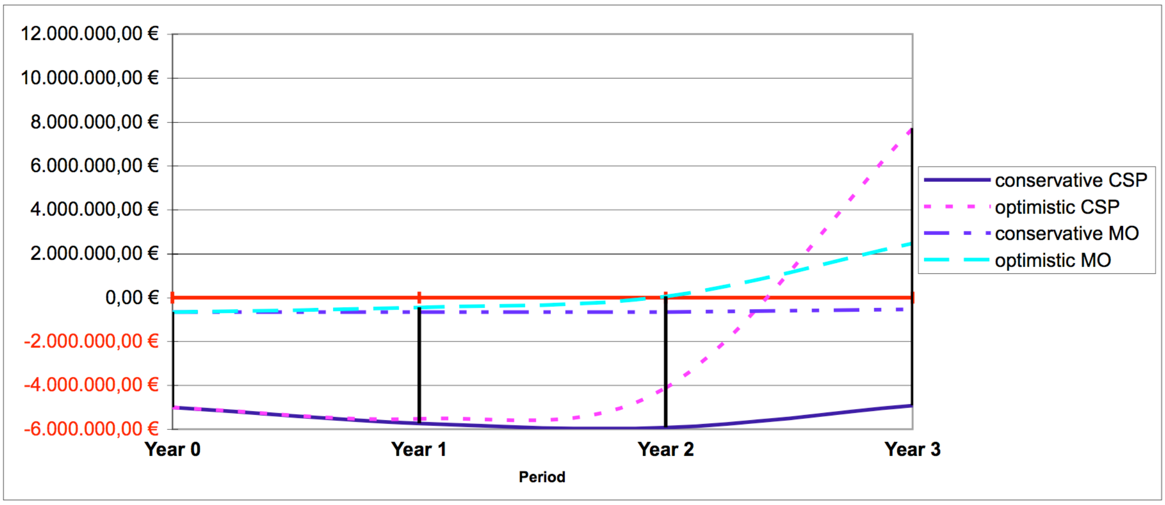

Figure 3: Development of the investments' NPV – MO & CSP

5. Limitations

The present research has several limitations that bear upon the likely validity of its findings. First, all of our results are dependent on the validity of our initial assumptions. Although, we used technological analogies as well as current pricing schemes to justify our assumptions, it is still possible, that we missed some important aspect that will thwart our results.

Second, some of our basic instrumentation in this research was rudimentary. For example, the model of diffusion is very simplistic using a fixed annual growth rate. Although, we used a technological analogy for this prediction in the optimistic case, a more thorough analysis using a more complex diffusion model would improve the validity of our findings.

Lastly, when it comes to highly interconnected correlations of effects, such as intangible benefits that occur from using COD (such as higher flexibility, etc.), our calculation scheme will not be capable of displaying these kinds of correlations. With regard to such effects, other methods have to be applied to asses the value of general IT investments (Kumar 2004).

6. 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 CSPs 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 CSP 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-/outflows for each scenario. As our results show, mobile qualified electronic signatures seem to be a profitable investment for mobile operators.

References

Blohm, H., and Lüder, K.: "Investition: Schwachstellenanalyse des Investitionsbereichs und Investitionsrechnung," 8th ed., Vahlen, Munich, 1995.

Datamonitor "Global PKI Markets, 1999- 2003", 1999.

DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures.

De Cock, D., Wouters, K., and Preneel, B. "Introduction to the Belgian EID Card BELPIC," *Public Key Infrastructures*, Katsikas, S., Gritzalis, S., and Lopez, J. (eds.). Springer, Berlin, Heidelberg, 2004, pp. 274-286.

Economides, N. "The Economics of networks," *International Journal of Industrial Organization*, (1996), pp. 673-699.

Fritsch, L., Ranke, J., and Rossnagel, H. "Qualified Mobile Electronic Signatures: Possible, but worth a try?" in *Information Security Solutions Europe (ISSE) 2003 Conference*, Vienna, Austria.

Franklin jr., C.: "The ABCs of ROI," in *Network Computing*, April 2002, pp. 93–95.

Geschka, H., and Hammer, R.: "Die Szenario Technik in der strategischen Unternehmensplanung", in *Strategische Unternehmensplanung - strategische Unternehmensführung*, 7th ed. Hahn, D., Taylor, B., Physica, Heidelberg, 1997, pp. 464-489.

Gruber, H., and Verboven, F. "The Diffusion of Mobile Telecommunication Innovations in the European Union", *European Economic Review* (45), 2001, pp. 577-588.

GSM Association, GSM Statistics, www.gsmworld.com/news/statistics/index.shtml, (accessed 2nd June 2005)

IDC "Worldwide SSL-VPN Appliance 2005-2009 Forecast and 2004 Vendor Shares: Delivering Secure Application Access," Kolodgy C., and Pintal G. (eds.), 2004.

Katz, M.L., and Shapiro, C. "Technology Adoption in the Presence of Network Externalities," *The Journal of Political Economy* (94), 1986, pp. 822-841.

Kumar, R.L. "A Framework for Assessing the Business Value of Information technology Infrastructures," *Journal of Management Information Systems* (21:2), 2004, pp. 11-32.

Lippmann, S., and Rossnagel; H. "Geschäftsmodelle für signaturgesetzkonforme Trust Center," in Ferstl, O., Sinz, E., Eckert, S., and Isselhorst, T., (eds.) Wirtschaftsinformatik 2005. Heidelberg: Physica-Verlag, 2005, pp. 1167-1187.

Mahler, A., and Rogers, E.M. "The diffusion of interactive communication innovations and the critical mass," *Telecommunications Policy*, 1999, pp. 719-740.

Muntermann, J., Rossnagel, H. and Rannenberg, K. "Mobile Brokerage Infrastructures - Capabilities and Security Requirements". *Proceedings of the 13th European Conference on Information Systems (ECIS 2005)*, Regensburg, 2005.

Potthof, I. "Kosten und Nutzen der Informationsverarbeitung: Analyse und Beurteilung von Investitionsentscheidungen", DUV/Gabler, Wiesbaden, 1998.

Project "Feasibility Study Electronic Identity Card", http://www.uni-kassel.de/fb7/oeff_recht/english/projekte/projekteDigiPerso_eng.ghk, (accessed 2nd June 2005)

Ranke, J., Fritsch, L., and Rossnagel, H. "M-Signaturen aus rechtlicher Sicht," *Datenschutz und Datensicherheit* (27:2), 2003, pp.95-100, Vieweg & Sohn.

Rogers, E. M. "The Diffusion of Innovations", Fifth Edition, Free Press, New York, London, Toronto, Sidney, 2003

Rossnagel, H. "Mobile Signatures and Certification on Demand," in *Public Key Infrastructures*, Katsikas, S., Gritzalis, S., and Lopez, J. (eds.), Springer, Berlin, Heidelberg, 2004, pp. 274-286.

Shapiro, C., and Varian, H.R. "Information rules: A strategic Guide to the Network Economy," Boston, 1998.

UMTS Forum "3G Offered Traffic Characteristics", UMTS Forum Spectrum Aspects Group (SAG), No. 33, Nov 2003