Article in T-110.501 Seminar on Network Security 2001 ISBN 951-22-5807-2
Publications in Telecommunications Software and Multimedia TML-C7 ISSN 1455-9749
Helsinki University of Technology, Telecommunications Software and Multimedia Laboratory

http://www.tml.hut.fi/Studies/T-110.501/2001/papers/index.html

# Smart card payment and risk scenarios

Mika Mäntylä
Helsinki University of Technology
Mika.Mantyla@hut.fi

**Abstract**

Current payment methods, that are based on cash and magnetic strip cards, are either expensive to use, or they do not offer enough security for payments. Smart card based payment systems offer several benefits over currently used cash and magnetic strip cards. Building and delivering smart card based payments systems is not an easy task. It includes several risks and some of them are addressed in this paper. We conclude that worst risks in delivering smart card systems are the lacking knowledge of merchants and card users needs and the cost of building wide-scale payment system.

## 1 Introduction

Smart card payment systems offer a new and a more secure way of conducting payments. The technical advance offered by smart cards and the emerge of other technologies such as the Internet, mobile phones, and public key cryptography, enable us for a totally new way of making payments. This paper concentrates on presenting some of the future's payment system, but it also analyzes the problems or risks, that might prevent and hinder the development and use of these systems.

This paper is organized as follows: Section 2 introduces the reader to parties involved in smart card payment, Section 3 gives the reader an overview of different kind of smart card payment systems, in Section 4 we will discuss the risks involved with smart card payment systems, and finally the work is concluded in Section 5.

## 2 Background

This chapter introduces the reader to parties involved in smart card payment. We also see how the transactions are carried nowadays. Finally we give a brief overview of the technology that smart cards contain.

### 2.1 Participating parties

When considering smart card payment, we can identify four different parties, who are involved. The parties are:

- The manufacturers, who create the cards and the software necessary to operate them.
- The card issuers, who are responsible for issuing the cards and making sure that payment system is operational.
- The merchants, who accept the payments made by smart cards.
- The consumers, that get smart cards from the issuer and make purchase at merchants with smart card.

This paper considers things mainly on the card issuers side, where merchants and consumers are the two other parties mainly involved. The manufactures issues are dealt briefly.

## 2.2 Current payment methods

We can identify three different payment methods in today's world. Each of these payment methods have been around for while and all of them have few obvious down sides, which we will present in this chapter.

### 2.2.1 Cash & Checks

Cash and checks both represent a form of manual payment method. In 1998 90% of transactions in US required manual labor [7]. Cost of processing paper based payment is $0.60 per transaction, while electronic payments only cost $0.02 per transaction to process [7]. From these facts it is easy to understand, why it is worthwhile to find a substitute for these manual payment methods.

**Cash** Cash is still the most widely accepted payment method in the world. In France and UK 70% to 75% of total transactions volume is covered with cash [6]. It can be argued that cash will not ever be replaced with smart cards or any other payment method. However the amount of cash used can and should be reduced. For consumers cash is very convenient payment method, but it is expensive for merchants and banks. Handling cash, costs 5% to 7% of its value [6]. Retail business, which has very large revenues and small profit margins, would notably benefit from widely used replacement to cash. Banks would also benefit from reduced cash usage, since providing cash to merchants and consumers is not considered financially as a very good business.

**Checks** Although checks are quite rare in Finland, they are still used in countries like Great Britain and U.S. In Great Britain 80% of households bills are paid with checks [12]. This requires a lot of manual labor from banks, merchants, and households. Although banks get the interests from the money during check transactions, the profits from it are small, because of the manual labor involved. Due to lack of automation 250000 checks are lost every year, which amounts 2,4 billion Finnish marks [12].

### 2.2.2 Credit and other payment cards

Credit cards with magnetic strip are much more technically advanced than cash or checks. The payment processing is mostly electronic, which reduces the cost, although signed receipts still has to be kept in case of disagreements. However card payment is not very suitable for small amounts, since fixed cost from $0.20 to $0.40 is attached to every payment [9]. With current card payment schemes the retailers have no cash handling problem, but they have to pay additional fees to card issuers.

The security mechanism of magnetic strip cards is not up to today's standards. The magnetic strip can be quite easily copied and duplicate cards be made. Also for payments under 300 Finnish marks no identification is required and the payment is accepted by hand written signature, which can hardly be considered as a strong authentication. During credit card payment the merchant gets the consumer's private data from the card, which puts them in perfect position to use their customers credit cards [9].

Paying in Internet with credit card is not properly authenticated transaction. You only have to get a valid credit card number and the user's name to be able to pay on the Internet. There has been number of cases in public, where crackers have stolen entire databases with credit card numbers and names. Since this is not good publicity for Internet merchants or credit card companies, it would seem likely, that there has been even more incidents, that have been kept away from public. For secure payments over Internet there is a program called SET that has been developed by Visa. However in many cases neither the card user or the merchant has bothered to get the program. Merchant's reluctance to get the SET program is mostly due to the fact, that SET is too expensive to implement [9]. Since most merchants do not have SET program implemented many consumer's will not bother to download it either, and so the deadlock is ready.

Visa's survey in the US from holiday season 1998 shows, that half of the top 20 online stores had charge-back rates from 5% to 10%. Visa also reported that in 1999 half of Europe's charge-backs were from Internet transactions [8]. With these facts it easy to say that current credit card schemes are not in anyway suitable for Internet payment.

## 2.3 Smart cards

Smart card was invented as early as 1974 by Roland Moreno [3]. Smart card is basically credit card sized computer. The basic structure can be seen from Figure 1. Smart cards can perform calculations with their own microprocessor and memory. Smart card has also their own operating system and todays smart cards can contain multiple applications. The way to access smart card is through smart card reader. Smart card also gets the required computing energy through the smart card reader, and thus can only perform calculations, when connected to one.

The trust on smart cards is based on two things. The first is the public key cryptography, which is the foundation for all modern day cryptography. The second is the fact, that smart card is an independent computer, which can be accessed only through the smart card reader. Any attempt to access smart card's data directly is more likely to destroy the card than let secret data leak out. It is also very difficult to duplicate a smart card, since you

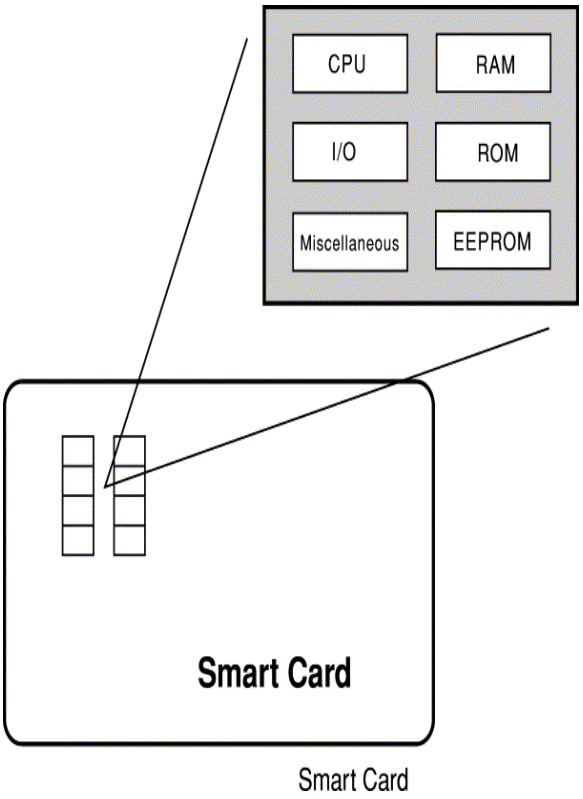


Figure 1: The components of smart card [11].

would then have to capture the complete state of the smart card computer.

Today most smart cards are based on ISO 7816 standard. There are at least four major smart card system in the world. They are the Javacard from Sun Microsystems, MULTOS, Windows for Smart cards by Microsoft, and BasicCard by Germany-based ZeitControl[3].

# 3 Smart card payment systems

This chapter gives the reader an an overview of different kind of smart card payment systems, which are currently used or being developed. We also see, what benefits each of these solutions have and what problems they are solving. We will also look into some of the projects implementing these systems.

## 3.1 E-purse

E-purse (Electronic purse) is virtually an effort to replace cash with smart card based payment system. The basic idea is, that the consumer no longer needs to carry any cash with him. Instead the consumers would handle all of their small transactions, including car parking, meals, magazines and etc, with smart card. To be able to pay with smart card the consumers would have to charge the card in the same way they withdraw money from automatic teller machines (ATM).

**Benefits** The e-purse system, if largely effective, would decrease the amount of cash used. This would clearly benefit the banks and the merchants, who would no longer have to be faced with cash handling costs. Errors and scams involved with cash would also diminish. Banks would benefit even more, while getting the interests from the money, that consumers charge to their e-purse cards. If you estimate that a bank would have one million e-purse users, that carry on average 200 Finnish marks on their cards, it would result 8 million Finnish mark yearly revenue to bank with interest rate of 4%. The e-purse system would be most beneficial to banks, merchants would gain some benefits, but the advantages to consumers are not so clear. Consumers would no longer have to worry about having proper coins for automates, money transactions at stores would most likely be more quicker, and e-purse could possibly be charged through Internet or with mobile phone. It has to be said, that the consumers benefits are not nearly as tempting as the other parties, but still there are good reasons why consumers should get E-purse.

### 3.1.1 CEPS case

CEPS (Common Electronic Purse Specification) currently is the best candidate for bringing Europe wide interoperable e-purse system to use [1, 6]. CEPS presents specifications of e-purse system, that tells different vendors how they components must operate in order to be CEPS compliant. Below there are some of the CEPS's key features [6].

- Several different load transactions e.g through Internet or at a terminal of another e-purse system.
- Multi-currency support enables to have more than one e-purses to reside on a single card and converting purses money to different currency.
- Purchase can be made at stores (attended purchase) or with vending machines (unattended purchase). It is also possible to cancel last purchase
- Security is achieved by authenticating the card with public key and protecting the card with PIN-code. All transactions are auditable and traceable, but that also prevents direct card to card transaction

CEPS defines a solid foundation to build e-purse systems. However it is going to take few years before e-purse can be widely used, because the lack of current infrastructure.

## 3.2 B2B

The purpose of business to business (b2b) payment systems is to help corporations on capturing big deals. With big we mean amounts that are not payable by any of the current credit cards, which basically means amounts greater than 100000 FIM. In large business transactions it is essential, that the opposing party's identity is properly confirmed. This can be achieved through smart card system authentication. Today businesses might be actually losing deals, since business contacts from unknown sources are ignored, because of the effort required to identify the opposing party [11]. The b2b system with smart card could also help parties communicate their business plans more securely.

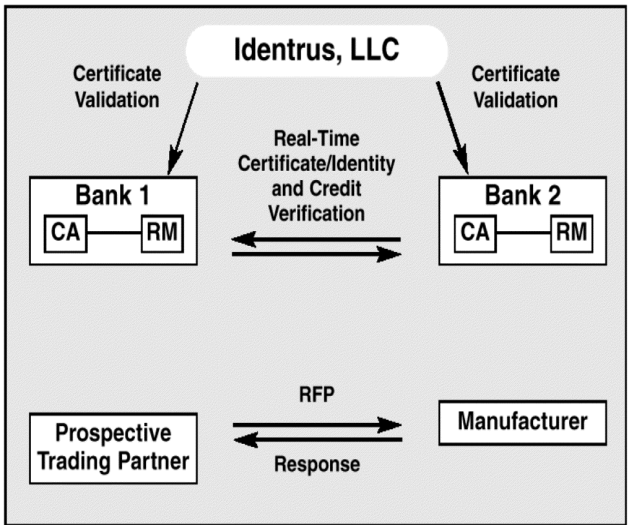


Figure 2: Identrus network in action[11].
CA = certificate authority, RM = Risk Management, RFP = Request For Proposal

**Benefits** This kind of system would largely benefit companies, since new business partners could be trusted with less work on checking the partners backgrounds. Background checking often includes calls to banks that assure the company really has assets. Also the contact person's identity must be checked to prevent scam-artist from pretending as a legitimate company. With b2b payment systems all this hassle could be avoided and lot of resources would be saved. Clearly this kind of system would enable companies to make international deals with less effort. Card issuers would benefit from companies needs for this kind of service, and it is probable that companies are willing to pay for set up and maintenance of this kind of web of trust.

### 3.2.1 Identrus case

Identrus is banking alliance to which most of the world's leading financial institutions have joined [11]. It's purpose is to provide authentication services for companies trading on the Internet [11]. The system is based on public key infrastructure and it has one root certificate authority (CA), that will be extended to a whole certification hierarchy. Identrus system also includes real-time certificate validation, so doing business should speed up significantly if system is widely accepted. Identrus system in use can be seen in Figure 2.

What remains to be seen however, is that how they give certificates to companies. System for issuing certificates must include checks, so that applicant's identity is properly verified and it also needs to have a way of revoking keys and certificates. Identrus needs system that is highly trustworthy, because without great amount of trust the system will have few legitimate business users.

### 3.3 Raising trends in smart card payment

There has been a lot of discussion, that different digital equipment will converge in to one digital device. By no means are smart cards and smart card payment systems out of this scope. This chapter takes a look into two of the possible solutions, that can be combined with smart card, to be used in electronic payment systems.

#### 3.3.1 Mobile phone

The mobile phone manufacturers and operators are pushing mobile phones to be the user's Personal Trusted Device (PTD). This naturally includes making payments with the mobile phone. To make this work there are different scenarios, but most of them trust to smart card for securing the system. It is already possible to use a mobile phone for small transactions, like parking or buying soda from automate. However protection offered by the GSM technology is not adequate enough so smart cards are needed to enhance the security.

The mobile phone offers few considerable advantages. First of all many people already have cell phones and they are comfortable using them. This is clear advantage, since adoptation of new techniques is always unpredictable. The consumers would no longer have to bother to have or use separate smart card reader, since the phone would be directly attached to smart card. However using cell phone at the point of sail could be very clumsy, when compared to cash, e-cash or credit cards.

#### 3.3.2 Digital TV

Digital television promises more interaction between the broadcasters and TV-viewers. This could mean, that consumers would be able to decide whether they want to buy to nights movie or not (pay per view TV). Also commercials with possibility to buy products, would be natural extension to what TV-shopping is today. Yet again smart cards would be embedded to these digital televisions to provide security and authentication, that these payment applications need.

## 4 Risks in smart card payment system

In this chapter we will discuss the risks involved, while creating smart card payment systems. In most risks the main stake-holder is the card issuer. This is due to the author's assumption, that if using card based payment system comes too risky for clients (consumers and merchants) they will just not use it and by doing that they simply realize one the card issuers risks. Bearing this in mind we can conclude that card issuer is the one, who takes the ultimate risk.

This chapter outlines some of the most critical risks, and it is organized as follows. First we look at technical problems involved with smart card systems. In the second Section we discuss the client issues, who's support is essential to card issuers. Section three looks at the smart card devices interoperability. In Section four we look at E-business risks from

the parts that apply to domain under study. Section five discusses the cost of building international payment system. In the final Section we review all the risks found. In each chapter we also visualize some possible risk scenarios with visualization used in Riskit method [5].

## 4.1 Technical problems

There can be number of technical problems, when developing smart card payment system. Some of the problems may even exists after the system is delivered. These numerous technical risks however are more of an interest to projects, who actually implement the system. As we try to get larger perspective to smart card payment systems as whole, there virtually exist two technical questions with greater interest:

- Can the smart card be cracked and how much would it cost?
- How reliable are smart card chips?

In smart card payment systems the smart card itself is the most interesting component, because it provides the security and trust to the system. If smart cards are easily cracked that will take away one of the key reasons, why smart card systems are built. All the smart card systems that are being designed put more trust to the card than they would do with traditional magnetic strip card. This means that smart cards must also live up to these expectations.

There are ways how smart cards can be cracked and copied. The attack can be invasive, or non-invasive. Invasive attack means that card is physically challenged. In a non-invasive attack the card is studied from outside by monitoring it during operations. Invasive attack can be physically conducted by chemically peeling away the layers of the smart card, and then studying the cards internal state and structure with microscopes and probes [2]. Other way of doing physical attack is to bombard chips surface with electrons, and by analyzing that it is possible determine the electronic potential and the activity at different parts of the chip [2]. The way to do non-invasive attack on smart card is to monitor the cards power consumption, when the card is performing different tasks [2]. Smart cards can also be cracked by breaking the secret keys that smart card carries. This however is more an issue to cryptanalysis than a smart card design.

Cracking smart card is not easy at all. The physical attacks are very expensive to perform and require special equipment not available to ordinary criminals. Card manufacturers are constantly developing new means to protect the card, so that physical tampering would be more likely to destroy the card. The non-invasive attacks require much time and effort, since a lot of data must available for them to be effective [2]. There are also hardware and software camouflages to prevent these attacks [2].

The simple answer for the second questions is that smart cards are very reliable. An example of that can be a French phone card that has failure rate less than *0.03%* [9]. However it has to be kept in mind, that as smart cards get more complex (e.g multi-application cards) the failure rate is likely to increase. An example of this occurred last spring, when

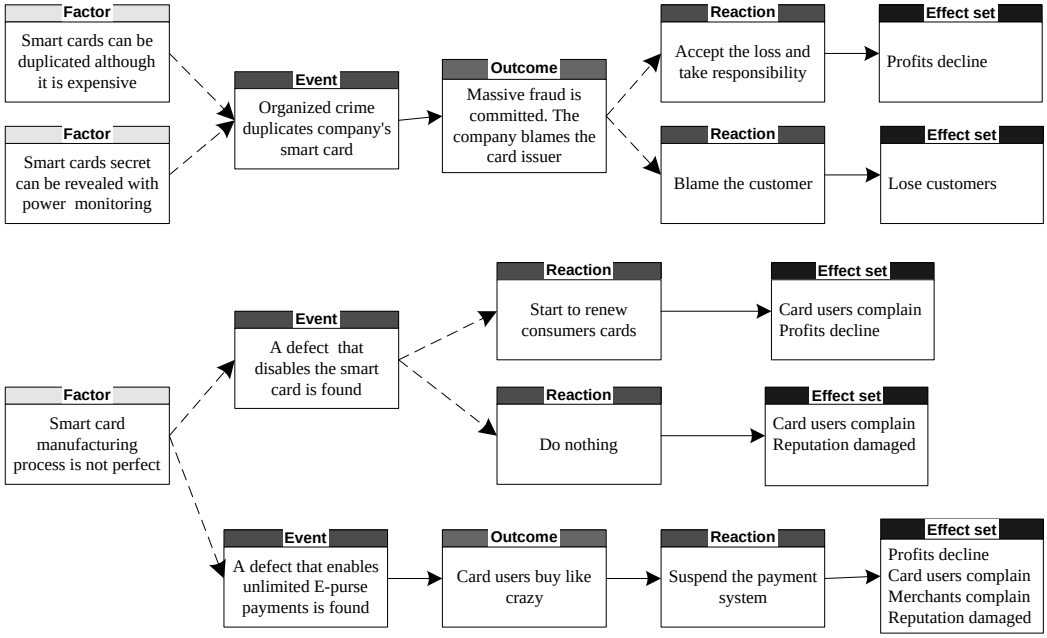


Figure 3: Technical risks visualization

Finnish telecommunication operator Sonera had to change 360000 SIM/smart cards from their GSM phone subscribers, due to a smart card software fault [14].

From the earlier presented questions one can derive two risks. First of them is smart card cracking problem that is in interest, when building b2b systems. This is because in b2b systems only one duplicated smart card can cause major damage. In ordinary people's smart card payment systems one duplicate card possess only a minimal risk to the card issuer. The second risk is smart card failure problem, that effects the cards already in use. This has the most effect, when consumer cards like e-purse are effected by the failure, since in those systems there are so many cards out there, and updating all of them is long and expensive process. Figure 3 gives you a visualization of the technical risk discussed here.

## 4.2 Client issues

With client we mean both the smart card users and merchants. One of the biggest challenges of the card issuer is to get enough clients so that the system is profitable. It must be noted, that the card issuer must get both the merchants and consumers to accept the system, otherwise it will not work.

### 4.2.1 Customer issues

When building smart card payment systems, customers should be carefully studied. A good example of negligence to consumers was made, when American companies tried to sell gene modified food to European consumers. The companies handled their communication with consumers very badly, and downplayed their influence in public. As a result of that

gene modified food was quickly named to "Franken food" and bringing it to market would have led to a major disaster. This example is not from IT industry however it illustrates the point that consumers should be taken very seriously and downplaying them will be a mistake. Also wrong assumptions about consumers, may slow down the adoptation of new technology. SET system was suppose to be a widely accepted digital payment solution. However creators of SET assumed, that consumers would bother download extra software to their PC's and that consumers number one concern in Internet shopping was security [8]. Regardless of that there still is little knowledge of consumers expectations for payment systems like e-purse, stated SmartEuro work group in their study to European Union [6].

A study made in Canada showed that relative advantage and compatibility, where the two biggest factors influencing the smart card payment system adoption among the card users [10]. Two other major reasons were voluntariness and image [10]. This study indicates that people will not easily change they consuming habits, unless:

1. they benefit of it (relative advantage)
2. it fits their current shopping habits (compatibility)
3. they are not forced (voluntariness)
4. it makes them look "cool" (image).

From that one can state that consumers are not likely to get card readers quickly. They do not get relative advantage from getting through the hassle of investing to and installing a card reader. Using smart cards at home is not compatible to way they are doing things at the moment. However they might start to charge they smart cards at ATM's and start using them to do payments. Mobile phones will also help the smart card adoptation, as people are already used to them and they enable payments far a way from the point of sale.

### 4.2.2 Merchant issues

Merchants are as vital as the customers for the smart card payment systems. Traditionally merchants have not been viewed as adopting group, but more as a distribution channel for new technology [10]. Studies clearly suggest the adoptation approach to merchants is more suitable [10]. In France the Cyber-Comm project is distributing free smart card readers to customers, but has not been able to get many merchants to use their system [13], which could prove to be problem. In Finland e-purse initiate Avant failed, because consumers could not use it in most stores. This examples clearly indicates that merchants should be studied in the same manner as consumers.

The same study in Canada that was previously referred shows, that merchants adoptation is influenced mostly by the same factors as consumers [10]. Merchants top two priorities were also relative advantage and compatibility. Merchant also appreciated image and visibility [10]. Other more concrete studies show that merchants are interested in long term system, that greatly reduce the cash handling [6]. From that we can argue that merchants are willing to accept the smart card system, if it helps their business and does not require a lot of effort for maintenance.

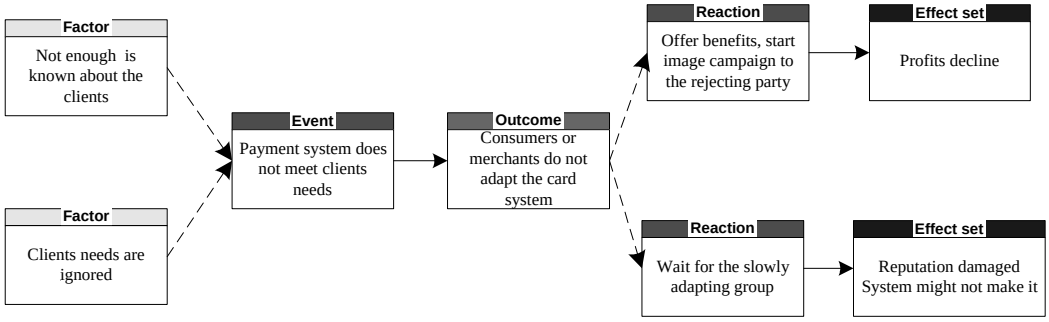


Figure 4: Client risks visualization

### 4.2.3 Conclusion

In order to get smart card payment systems smoothly adopted, the card issuer must pay attention to both adopting parties. Each groups needs must be studied and acted upon, and this should preferably happen simultaneously [10]. Figure 4 visualizes a client based risk scenario that might occur to a smart card system, if the issuer is not working properly.

## 4.3 Interoperability

Smart card interoperability is important, because there are many smart card systems coming to a market. There most promising smart card based payment systems seem to be: e-purse, traditional credit card with chip, mobile phone, and digital television. The fact that all of these could require a different smart card does not sound too promising. People hardly want more cards and separate incompatible ways to use smart card could slow the adoptation of smart card payments technologies. Since there already are a combined bank-account and credit card, it would seem reasonable that all of the payment systems could be used with one card.

ISO 7816 set the standards for smart cards, however it does not concern about interoperability. It is possible to have ISO compliant card, that is strictly vendor specific. This means, that changing the card vendor also requires one to do considerable changes to their software that is run on the card. There are however smart card platforms that allows application development without direct access to cards design. These platforms are based on the concept of virtual machine (VM). So application developed on top these VM's can be run on any vendor's card as long as it contains the appropriate VM. [3]

The smart card platforms do not mean that all smart card based system, even with in one platform will be interoperable. The smart card payment systems is built up on many different components and some of these also have to be interoperable, that two system would work together. CEPS introduced in chapter 3.1.1 is a major push to get interoperability to work in one application and even they are a few years away. So it is still going to take

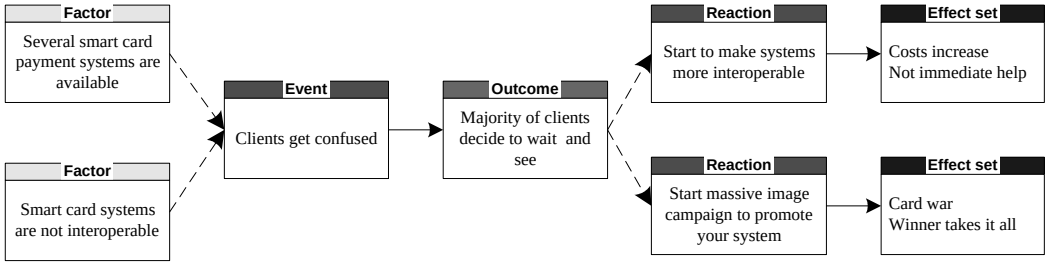


Figure 5: Interoperability risk visualization

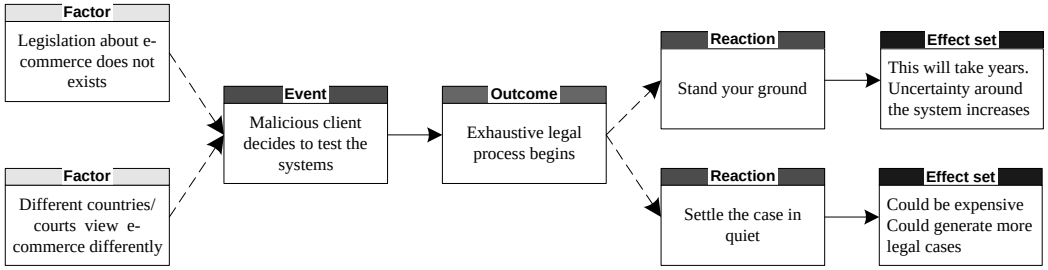


Figure 6: Legal risk visualization

several years before throughly interoperable systems are in the market. In some cases the interoperability might made unavailable for competition reasons. However interoperability is an issues that need to addressed while designing systems. Figure 5 represent the risk analysis on interoperability.

## 4.4 Legislation

Legal issues are not considered as major problem, when developing smart card payment systems. Although, these issues should be addressed, before the system is delivered. In the U.S the layers decided after a long debate that e-cash is not legally same as cash [7]. This means the merchant can reject the payment with e-purse the same way they can reject other card payments today.

In recent years the legislation has been developing behind the technology, examples of this are the “Napster” and “Adobe E-book” cases. This is not likely to change in future, as technology’s advance seems continuously gain speed. In smart card payment systems the legal issues could be quite difficult, as they often combine new technology and international business. So not only is legislation outdated, but it could be difficult to tell, which laws apply to the deal made on Internet. The legislation in different countries could also vary from non-existing to strictly controlled, in some countries could digital signatures be valid and in others they may be worthless. In b2b to smart card payment system such as the Identrus in chapter 3.2.1 should a separate agreement be made, between the card issuer and the user, to solve the possible disputes. This approach is not obviously suitable for b2c (business to consumer) deals, since consumers rights in different countries might oppose some restrictions.

Possible legal risk are shown in Figure 6.

## 4.5 Cost of building systems

Although smart card itself is not very expensive (5$), the costs of building international payment system are enormous. In US a mutual funds company was interested to provide remote access account to it's 12 million customers with smart card ID's and CA's [8]. The offer from the vendor included a price tag over 1 billion dollars or 85$ per account, after that the project was ceased, since client was expecting the price to be 10-15$ per account [8].

High cost itself is not a risk, but it increases the loses when some of the other risks realize. It also means that project are likely to last longer and involve more people. Thus projects are big, and bigger projects usually involve more risk and uncertain issues. Example about uncertainties in smart card project can be taken from Finland where the Matkakortti project has changed vendor during the project and the project has also been delayed several times. In an estimate made in summer 1996 people were suppose to start using smart cards in summer 1998 [15], however the first cards were delivered on October 18th 2001 [4]. This project is certainly over budget, however even on authors request no exact number were made available.

It is also important to look at the cost of system on based on other risks. An example from Europe estimated that pay back time to e-purse project according to CEPS standards would be seven years with following parameters from [6]:

- 400000 cards
- cost of card 5$
- card holder fee 7,5$
- load fee 0,3$
- merchant commission 0,55%
- 250 transaction per year per card

From what we have studied in chapter 4.2, we can argue that these numbers certainly do not offer relative advantage to consumer. The merchants advantages are questionable at best, when we keep in mind that merchants terminal and other cost for are not included in these numbers. So as long as seven years break-even time the project is still likely to fail, because it cannot offer advantages to clients.

High fixed cost is a big factor contributing to other risks involved in smart card payment systems. The smart card systems also include a great deal of uncertainty, so it is obvious that no reasonable vendor will take fixed priced project. It can be argued that high costs quickly turns in to one of the biggest risks, when you have project that deals with new and uncertain domain, and your break-even numbers are based on vague assumptions over a long period of time.

| ID | Risk name | Relavance | Impact |
|---|---|---|---|
| 1 | Clients do not adopt the payment system | This problem alone could make a system failure. | High |
| 2 | An expensive project went over budget. | Break-even periods will expand. Could trigger risk 1 if clients cost are raised. | High |
| 3 | Technical problems | When releasing the systems this could genrate bad image. Later they could increase cost, and if combined with risk 2, could set the card issuer into financial problems. | Medium |
| 4 | Legal problems | A pending law suit could damage reputation. Can be combined with 3 if it is technical issue. | Low |
| 5 | Interoperability problems | Can produce a negative image about the system. May increase the likelyhood of risk 1. | Low |

Table 1: Risk summary

### 4.6 Risk summary

Table 1 concludes the risks, tries to link them together, and it also presents the impact of risks when they occur. Likelihood of risks occurring is not presented here since it greatly fluctuates depending on the people delivering the system. Also risk indicators are omitted from Table 1, since the risks are in so common level that there would be several possible indicators.

## 5 Conclusion

In Section 2 starting on page 1 we studied the current payment methods and their weaknesses. It is obvious that current payment systems are not as efficient as they could be. Cash and checks are expensive to use and magnetic strip cards do not offer enough protection for the users assets.

Smart card however offers a better solution for to today's payment methods. Smart card increases the level of trust and cost-effectiveness to payment schemes. Smart card together with digital communication system like mobile phone or digital television can also enable completely new and unseen payment schemes. Some of the different payment solutions, that smart cards enable were introduced in Section 3 starting on page 4.

Bringing smart card based systems to use is not as tempting as it could be, because of the different risks that exists in developing, introducing, and maintaining these systems. These risks and their possible effects were studied in Section 4 starting on page 7. The summary of the risk can be seen in Table 1 on the current page.

From what we have studied here, we can conclude, that smart cards offer an excellent solution for today's payment systems weaknesses. Smart cards offer a security and pro-

tection that enable entirely new payment schemes to be built. It is imperative, that these new schemes should not be built just because it is possible, because of the risks that lie in building and introducing a new payment method. Instead managers should carefully study the client's true needs and the domain they plan to address, while keeping in mind that many years could pass before the system breaks even financially.

## References

[1] Devolder S. & Martiny L. & Linkens A. & Baptie C. How close are Europe's bankers to creating a cross-border purse?. Card Technology Today, 2000, Volume 11, Issue 5

[2] Faust M. & Tischle R. & Costa C. & Baptie C. & O'Kelly R. & Troy E. New approaches to smart card security threats, Card Technology Today, 2000, Volume 11, Issue 6

[3] Husemann D., Standards in the smart card world, Computer Networks, 2001, Volume 36, Issue 4

[4] Karuvuori A. Kari kävi lataamassa heti viiden viikon matkat, Helsingin Sanomat, 19.10.2001

[5] Kontio J., Doctoral Dissertation, Software Engineering Risk Management: A Method, Iprovment Framework, and Empirical Evaluation, Suomen Laatukeskus, Helsinki, 2001, 247 p.

[6] Martiny L. Why CEPS has to be the basis for the Euro-purse, Card Technology Today, Volume 12, Issue 2

[7] Mcelroy D. & Turban E., Useing Smart Cards in Electronic Commerce, International Journal of Information Management, 1998, Vol 18, No 1

[8] Mott S., The second generation of digital commerce solutions, Computer Networks, 2000, Volume 32, Issue 6

[9] M'Raïhi D. & Yung M., E-commerce applications of smart cards, Computer Networks, 2001, Volume 36, Issue 4

[10] Plouff C. & Vandenbosc M. & Hulland J., Intermediating technologies and multigroup adoption: A comparison of consumer and merchant adoption intentions toward a new electronic payment system, The Journal of Product Innovation Management, 2001, Vol 18

[11] Rime L., Global Internet Trading, Card Technology Today, 2000, Volume 11, Issue 10

[12] Sipilä Annamari, Britit hävittävät vuodessa 250000 sekkiä, Helsingin Sanomat, 2.10.2001

[13] Sitruk H., Cyber-Comm set to get consumers to buy on the Web, Card Technology Today, 2000, Vol 12, Issue 4

[14] Sharma L. Sonera vaihtaa 360 000 viallista sim-korttia, Helsingin Sanomat, 17.5.2001

[15] Tuohimaa P. Kymmenvuotispäiväänsä juhliva seutuliikenne näkee tulevaisuutensa valoisana, Helsingin Sanomat, 1.10.1996