Individual Risk Management for Digital Payment Systems

M. Reichenbach, T. Grzebiela, T. Költzsch, I. Pippow
Institut für Informatik und Gesellschaft
Friedrichstr. 50
D-79098 Freiburg
{marei, grzebiela, koeltzsch, pippow}@iig.uni-freiburg.de

***Abstract*-Despite existing security standards and security technologies, such as secure hardware, gaps between users' demand for security and the security offered by a payment system can still remain. These security gaps imply risks for users. In this paper, we introduce a framework for the management of those risks. As a result, we present an instrument enabling users to evaluate eventual risks related with digital payment systems and to handle these risks with technical and economic instruments.**

I. INTRODUCTION

With the growing number of digital transactions, Information and Communications Technology will be faced by with enormous challenges in the near future. Security and efficiency of Digital Payment Systems will be essential requirements for this. They must enable value transfers at low transaction costs and at a level of security similar to that of traditional payment instruments like e.g. cash or account based remittances. As a case in point, consider the traditional payment instrument cash which offers an almost perfect degree of anonymity.

Currently, however, the evolution of new payment systems as well as the persistence of traditional payment methods can be observed. This perseverance of traditional methods [1] is due to several aspects:

- The **institutional surroundings are insufficient**. There is neither a satisfying exterior framework, e.g. legal aspects are unresolved, nor have interior solutions for handling risks specific to the digital world evolved, e.g. common practices for conducting business via the Internet do not exist [2];
- **Confidence** in digital transaction infrastructures **is unsatisfactory**. Users either naively trust Information Systems like digital payment systems [3], or they are insecure about the security of their digital transactions. „Trusted Third Parties“ are not really trusted yet, either.
- **Security is not a built-in feature of payment systems**. Even the most advanced digital payment systems cannot emulate the anonymity, unobservability, and untraceability of traditional cash transactions.
- One can detect **opacity** for users because of the huge number of different Internet payment systems and their influence on individual security requirements.

Existing architectures for securing electronic commerce via the Internet, e.g. SEMPER[1] and payment interface projects like JECF,[2] aim to unify access to payment systems and to integrate different payment systems. At most protocols like JEPI[3] enable some automated payment negotiation between computers, determining the most appropriate payment mechanism on hand for a transaction. However, this determination occurs regardless of user requirements concerning risk management. In the end the user is coerced to 'juggle' with the payment systems available in his portfolio and to make a selection. He remains in the dark about the effects of his choice.

In this paper, we will therefore focus on the question of how users can handle the risks of making digital payments and thus gain confidence in the payment systems, respectively. The course of the paper is:

- to describe digital payment systems in a way that the underlying flow of information and thus potential security hazards appear, aiming to evaluate the security of a digital payment system [Chapter II];
- to analyze how payment system risks can be handled [Chapter III];
- to describe an instrument realizing the framework for measuring and handling these risks [Chapter IV]. Fig. 1 shows the steps that must be initiated in order to realize this;
- finally, to give an outlook on further research [Chapter V].

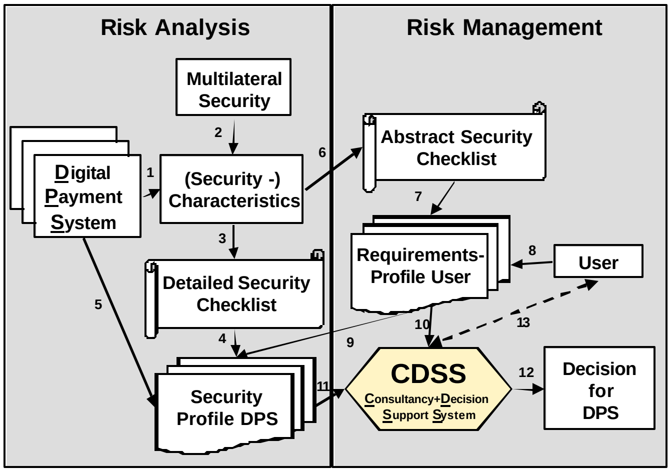

Risk Analysis
Risk Management
Multilateral Security
Digital Payment System
(Security -) Characteristics
Detailed Security Checklist
Security Profile DPS
Abstract Security Checklist
Requirements-Profile User
User
CDSS
Consultancy+Decision Support System
Decision for DPS
1
2
3
4
5
6
7
8
9
10
11
12
13

Fig. 1. Individual Risk Management for Digital Payment Systems (DPS).

[1] Secure Electronic Marketplace for Europe, ACTS Project AC026.

[2] Java Electronic Commerce Framework, originated by Sun, Javasoft.

[3] Joint Electronic Payments Initiative, originated by the W3 Consortium.

II. Risk Analysis - Evaluation of Digital Payment Systems Security

In the context of open communication systems security requirements of all parties involved in a transaction must be regarded. Therefore, we introduce the concept of multilateral security [cf. Chapter A]. In Chapter B, we describe a generic concept of how to classify digital payment systems. The model is a prelude to risk analysis, referencing fundamental information flows and the criteria of multilateral security. Chapter C deals with potential security hazards in digital payment systems. Finally, in Chapter D, the criteria of multilateral security will be applied to digital payment systems. The criteria will be detailed both for the context of digital payment systems as well as for user requirements concerning the execution of payments.

A. The Concept of Multilateral Security

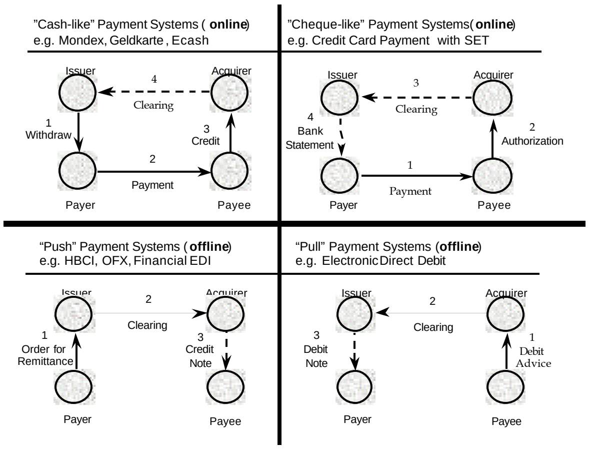
Multilateral security means taking into consideration the security requirements of all parties involved in a transaction [12]. It is a concept that fits security requirements in open communication systems in a way that users are enabled to act at their own risk [13]. It yields a set of criteria for facets of security: confidentiality, integrity, availability, and accountability. These criteria summarize security demands perceived by various standardization boards and have been verified in practice [14]. Since digital payment systems typically involve several parties with potentially diversified security requirements, this concept is applied within the scope of this project.

B. A Generic Concept of Digital Payment System Classes

There is a large number of digital payment systems at hand or at least on trial.[4] Some are for offline usage at the “Point of Sale” only, some are designed for Internet usage only. However, with advancements in Smart Card based technologies (like the German “Geldkarte”), these two directions merge. In the near future, payment systems applicable to the digital as well as the physical world will play an important role [5].

In order to identify common risks, payment systems must be classified. There are several proposals of how to do this which can be summed up in a generic concept [6]. Payment systems can be distinguished, e.g., upon the time of value transfer (cf. [7]), the binding to account processing, the kind of payment information communication and the initiation of value transfer.

As in [6], these categories can be pooled according to the underlying flows of information in order to gain generic payment system classes. Fig. 2 depicts the classes “**cash-like”** payment systems (online), “**cheque-like”** payment systems (online), “**push”** payment systems (offline) and “**pull**” payment systems (offline).



”Cash-like” Payment Systems (**online**)
e.g. Mondex, Geldkarte , Ecash
Issuer
Acquirer
4
Clearing
1
Withdraw
3
Credit
2
Payment
Payer
Payee
”Cheque-like” Payment Systems(**online**)
e.g. Credit Card Payment with SET
Issuer
Acquirer
3
Clearing
4
Bank
Statement
2
Authorization
1
Payment
Payer
Payee
“Push” Payment Systems (**offline**)
e.g. HBCI, OFX, Financial EDI
Issuer
Acquirer
2
Clearing
1
Order for
Remittance
3
Credit
Note
Payer
Payee
“Pull” Payment Systems (**offline**)
e.g. Electronic Direct Debit
Issuer
Acquirer
2
Clearing
3
Debit
Note
1
Debit
Advice
Payer
Payee

Fig. 2. Fundamental information flows of the generic payment system classes.

C. Potential Security Hazards in Digital Payment Systems

Taking into account the flows of information of the generic model above, it is possible to evaluate security hazards in payment systems. Generally, the security of complex information systems, such as payment systems, can never be absolute. Not all leaks can be known and put right by technical means at the outset. The relationships of parties involved in each transaction are far too complex,[5] and points of attack in an open communication system similar to the Internet are numerous (cf. Fig. 3). However, identifying security not as some static value, but rather by analyzing the fundamental information flows from a dynamic point of view, is the first step towards handling risks of each participant in the system.

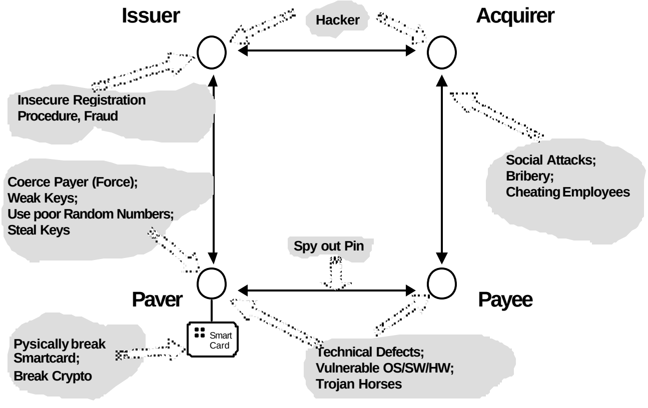


Fig. 3: Information flows and exemplary potential points of attack in a digital payment system

[4] Currently, examples for digital payment systems are the Ecash pilot of Deutsche Bank and Bank Austria among others; the SET trial of Commerzbank AG in cooperation with EUROCARD/Mastercard and Karstadt AG; Cybercash, CyberCoin and electronic direct debit at Commerzbank AG, Dresdner Bank and other private banks and savings banks.

[5] Note that all parties involved must be considered, i.e. payer, payee, issuer, acquirer, credit card companies, trusted third parties, and so forth. Throughout the paper, we will focus on payers.

Besides, security must be economically feasible. Thus, even the - theoretically – maximal conceivable “technical” security (which we call the largest achievable security level) need not necessarily be implemented. Increasing usage of technical means is combined with decreasing rates of growth of security scale, and thus with disproportionate increases in costs.[6]

Thus, the problem arises that a given security level (given by technical means) can be lower than required by users. In other terms, remaining (security) risks must be handled, either by institutional constraints or by – individually applicable – economic instruments.

Institutional constraints, like rules and laws, conduct human behavior by restricting options for acting and thus reduce risks. For instance, banking regulations and banking supervisions restrict the creation of money to companies defined as banks, and thus reduce risks of monetary instabilities. Institutions can provide incentives for people on the other hand as well. For instance, the German Digital Signature Act regulates the usage of digital signatures. It supports a framework for authentication and non-repudiation for electronic commerce. Thereby, incentives are given for usage of digital signatures according to the law, eventually shifting security risks away from market participants.

Economic instruments providing non-technical security for transactions, e.g. insurance or liability limits, are in demand as well [2]. This way risks will be shifted even further away from users, which should facilitate the usage of digital payment systems.

After all, it is important to note that, from a dynamic perspective, not just security hazards appearing within the information flows must be disclosed, but endogenous and exogenous risks in the form of attackers[7] as well [12]. Thus, beside the attackers’ strengths, also the plausibility of attacks must be considered when judging fulfillment of the security requirements [11].

D. Applying Multilateral Security to Digital Payment Systems

In order to evaluate the security of digital payment systems, we generate security profiles expressing the security levels of the payment systems examined. The criteria of multilateral security themselves do not support the generation of these security levels, however. They are too abstract and may serve only as generic security criteria. Therefore, in a first step, these generic criteria have been detailed and adapted to meet the specific attributes of digital payment systems (cf. steps ‘1’, ‘2’ in Fig. 1), giving detailed security characteristics (cf. step ‘3’ in Fig. 1). The detailed security characteristics can then be matched with users’ security requirements (cf. Chapter C and Fig. 6) in order to determine the security scale of a payment system at one point in time.

Fig. 4 illustrates the detailed security characteristics of the generic security criterion ‘integrity’. A comprehensive checklist of detailed security characteristics concerning digital payment systems is in [15].[8]

This checklist may be utilized by security experts or legal institutions in order to evaluate payment systems and to build up digital payment systems’ security profiles. The evaluation will be done by taking account of the payment systems’ information flows (cf. steps ‘4’, ‘5’ in Fig. 1). Experts will assess the fulfillment of the detailed security characteristics of each payment system examined (e.g. “payment system x complies with ..., complies partially with ..., does not comply with ...”).

The overall assessment yielding the security scales will be realized technically by a scoring method. This method has several advantages for the purposes focused on in this paper.

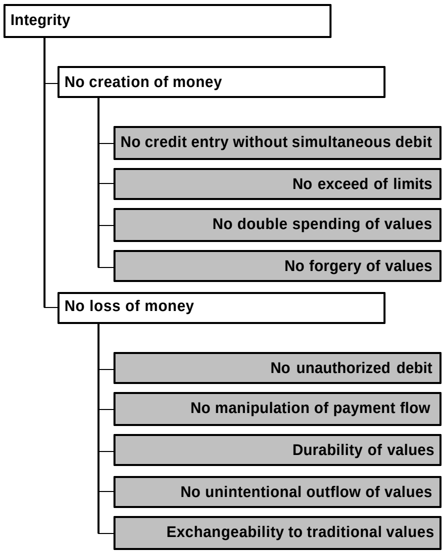

Integrity
No creation of money
No credit entry without simultaneous debit
No exceed of limits
No double spending of values
No forgery of values
No loss of money
No unauthorized debit
No manipulation of payment flow
Durability of values
No unintentional outflow of values
Exchangeability to traditional values

Fig. 4. Detailed security characteristic “integrity.”

On the one hand, non-quantifiable criteria like the ones mentioned above can be assessed. On the other hand, this method supports users to weight each criterion in order to get, as a result, an individual order (ranking) of their abstract security requirements. The weighting expresses the meaning of a criterion during a (single/special) transaction for users and makes the criteria comparable.

The security profiles generated are an image of the overall fulfillment of single criteria by the payment systems examined. They reveal which security requirements are met by the payment system, to what extend they are met, and thus the remaining risk for the user.

A comparison of the payment systems’ security profiles (cf. Fig. 6) facilitates a prioritization of these payment systems, enabling users to choose among different payment systems in a more systematical way.

[6] In this context, security is the result of the use of security technology. Increasing use of security technology is related with decreasing marginal revenues of “security.” This implies that the cost for each additional unit of security will increase by a factor greater than 1, i.e. that the costs for an additional unit of security technology will stay constant, cf. [8] and [9].

[7] Outsiders, users of the system, operators of the system, maintenance services, producers of the system, designers of the system, and so on.

[8] In form of the ‘Detailed Security Checklist for Experts.’

III. Risk Handling

To determine individual transaction risks, the user must be able to establish the desired level of security. For this purpose, we introduce the concept of "user profiles" in Chapter A. Chapter B describes several basic approaches for the configuration of user's security requirements. Finally, Chapter C describes how matching the payment systems' security profiles with user's security requirement profiles ascertains the measure of risk remaining in the best case.

Later, we will address the question of what kind of risks remain and will describe technical measures [Chapter D] as well as economic ways [Chapter E] to overcome these remaining risks.

A. User Profiles

According to the concept of multilateral security users should be able to specify the level of security they want. They will want some form of protection for their transactions, e.g. privacy.[9] Therefore, in order to use a payment system, users must specify their security requirements. These requirements are collected in so-called user profiles. Each user may define several individual user profiles, according to his transaction or situation specific needs (cf. Chapter B).

Typically, users are not security experts. Their requirements will differ from the detailed security characteristics checklist described in Chapter D. Users generally may define their security requirements in the form of a few so-called abstract protection goals like, e.g., trust, anonymity, and costs. Such user security requirements must be matched with the detailed security checklists (cf. Chapter C).

B. Configuration of User Profiles

To record the user's security requirements, the security characteristics of the payment systems available and possible protection goals should be represented in a simple and clear way. Confronting users with the full bandwidth of the detailed security characteristics explained in Chapter D would put excessive demands on them. The process of configuration would take too much time and would perhaps be much too confusing. For this reason, we must find abstract protection goals for the users which abstract from technical details.[10] The abstractions of protection goals should orient themselves towards the users' (subjective) security requirements (cf. step '6' in Fig. 1).

A possibility of abstracting security requirements is shown in [16]. The authors identify so-called 'Business Relationship Properties' as abstract security requirements, enabling a user to define his relationship to business or payment partners. As an example, the property 'identification of the user' defines which electronic commerce participants are allowed to obtain some knowledge about the user's real identity. The authors identify at least three levels as possible values for this property: everybody, only the business partner, and nobody.

A further approach to determine abstract security criteria of users as well as some insight into individual risk perception are given in [3]. In this empirical study, bank customers' security requirements for Internet transactions have been approximated. There was a detailed questionnaire aimed to reveal users preferences concerning digital payment systems security characteristics by means of statistical methods.

The gap between a simple operation of the user's security configuration oriented to subjective targets and the detailed security characteristics could possibly be closed by a layering, as it is described by [17] for the Privacy Preferences Project (P3P) of the World Wide Web Consortiums (W3C).

Thus a user

- may once determine general defaults of his requirements, according to which his system should act automatically;
- may also determine special requirements for special situations beyond the general defaults and
- may be asked to act on warnings and proposals from his system in the event that none of the requirements defined before can be satisfied.

We proceed in a first step from the following abstract security requirements,[11] i.e. the user can determine

- his actions' non-visibility in relation to other users;
- his willingness to trust other users and
- his demand for non-repudiation of origin and of receipt.

At the same time, the user defines his abstract security requirements he is able to weigh these criteria against each other (cf. steps '7', '8' in Fig. 1). These weights flow into the payment systems security profiles and help to prioritize them at the time of transaction (cf. step '9' in Fig. 1 as well as Chapter D).

In order to simplify the configuration of user profiles users may predefine their requirements as a type of default configuration with respect to different types of (payment-) transactions respectively to different user-defined situations (cf. [4] and [28]). Types of transactions may be differentiated, e.g. on the basis of the payment recipient, the amount payable, the transaction charges or the time of value transfer. Different user-defined situations could be, for instance, the purchase of digital products with online-delivery or the purchase of material products with offline-delivery (cf. Fig. 5).

[9] Since for the user interface we focus on security characteristics as qualitative aspects, we will not determine quantitative levels of requirements. We rather aim to show how these qualitative aspects are achieved by digital payment systems.

[10] In form of the "Abstract Security Checklist for Users."

[11] Other requirements than the ones mentioned could be for instance the cost and speed of a transaction.

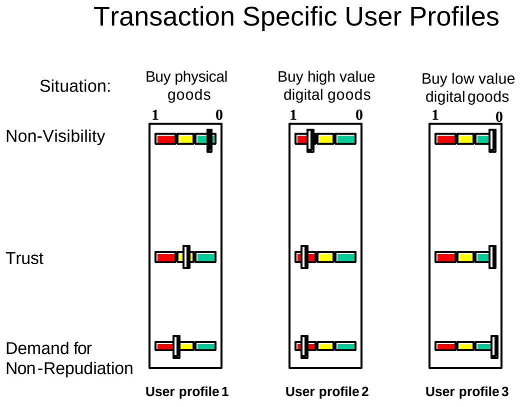

Transaction Specific User Profiles
Situation:
Buy physical goods
Buy high value digital goods
Buy low value digital goods
1
0
Non-Visibility
Trust
Demand for Non-Repudiation
User profile 1
User profile 2
User profile 3

Fig. 5. Examples for transaction specific user profiles.

In a concrete transaction situation it is now possible to assume the users security requirements depending on the transaction type and the predefined settings of requirements for this type of transaction. With these suppositions, the most suitable payment system for this type of transaction may be chosen. Even in this case, it is helpful for users to receive experts' suggestions for meaningful configurations.

In order to coordinate these three user-oriented security requirements with the great number of concrete security characteristics described in Chapter D they have to be mapped on each other (cf. Fig. 6). There exists a set of interdependencies between particular abstract and concrete security criteria as well as interactions between individual security criteria which have to be considered. For a detailed examination of interdependencies and interactions between security criteria, see [32].

C. *Matching User Profiles with the Digital Payment Systems Security Profiles*

After the configuration of the user's security profile it may be matched against the security scales of payment systems in the user's portfolio (cf. steps '10', '11' in Fig. 1). For this purpose the results of the payment systems' prioritization based on the scoring model (cf. Chapter D) are consulted. This procedure will be supported at run-time by a Consultancy and Decision Support System (CDSS, cf. Chapter IV).

We assume that the demand for security varies across different transactions, depending on types of transactions (e.g. the value of transactions) and surroundings (e.g. the level of trust among the participants). Among the variety of payment instruments available to the user,[12] for conducting a transaction he will only choose a system with a security scale at least as high as required. This minimum security scale required by the user is called the level of adoption (cf. Chapter A).

It is apparent that there currently exists no payment instrument which fulfills all security requirements at once and which may therefore be suitable for all types of transactions – regarding their specific requirements – equally. As a consequence, users might not automatically choose the payment instrument with the highest security scale as a default.

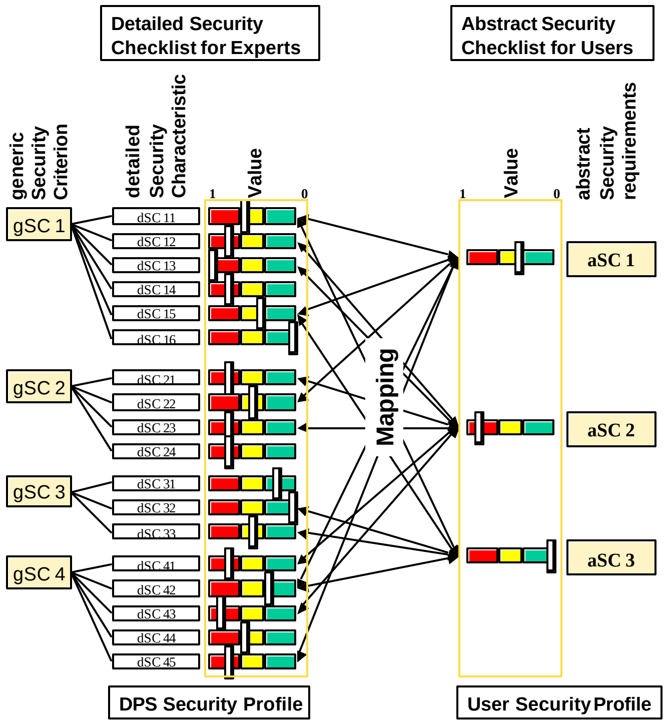


Fig. 6. Mapping user profiles with the digital payment systems' security profiles.

Subsequently, that payment system from the user's portfolio is suggested, which achieves the adoption level best or which would require least concession of the user in order to be eligible. For all payment systems in the users portfolio with a security scale higher than the level of adoption, selection is straightforward (cf. Fig. 7).

If there is one system that meets the users adoption level, then this system is chosen (cf. step '12' in Fig. 1). However, if this adoption level cannot be realized, the user will be informed about

- potential upcoming security hazards;
- the maximum security scale available at transaction time (maximization of security);
- a payment system with a security level nearest to the user's level of adoption that would require as little user's concession as possible (minimization of user's concession);
- possible combinations with individual economic tools in order to handle remaining risks (cf. step '13' in Fig. 1).

[12] Note that we presume that a portfolio of different payment systems will be available in the market.

Yet, with higher security requirements or poorly designed systems, risks remain for the user.[13] In case additional risk handling is not provided users can only choose to bear remaining risks themselves or not to conduct the transaction. In order to raise payment system acceptance, however, individual risk management should be allowed for. Thus, we are looking for technical and economic solutions for individual, transaction specific risk reduction or risk transformation.

The result of the matching process will, at first, be a response as to whether all user requirements are met or not.[14] Since users security requirements themselves are weighed against each other, however, even the percentage of fulfillment as an actual measure of the security scale can be achieved. It is important to note that, because of the fact that the weighting factor is transaction specific, the security scale itself is also temporary.

D. *Technical Solutions For Handling Remaining Risks*

Technical measures for risk reduction are procedures in prevention, perception, and containment of risk [18]. These measures are taken before the execution of the transaction. At the time of execution there is no further supplementary technical mean securing remaining risks.

At most remaining risks may be distributed among the participants of a payment system by employment of some additional protocols like [19].

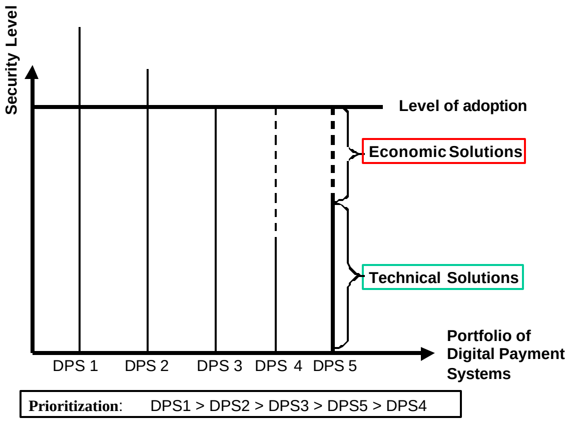


Fig. 7. The Selection of a Digital Payment System according to the Prioritization.

Generally, technological advancements like security hardware will further increase the security scale.[15] However, beyond this, economic tools are necessary in order to further facilitate usage of digital payment systems.

E. *Economic Solutions for Handling Remaining Risks*

Risks can be reduced economically by involving intermediaries. On the one hand, intermediaries can help to recognize risks and thus yield increased transparency. Like a technical supervisory institution, e.g. the German "Technischer Überwachungsverein (TÜV)," they can analyze, judge, and certify the security of digital payment systems.[16] Also, as a Certification Authority, they can issue and administer certificates.[17] On the other hand, they can play the role of marketplace providers who facilitate trade among participants by actually organizing exchange of property, monitoring of liabilities, limits or assuming del credere liabilities, or by handling disputes [21].

For risk transformation, we focus on two possibilities: individual contracts and insurance [22]. Risks in-between the security scale and the level of adoption can be distributed among participants ex ante by negotiation and contract. Negotiation aims at achieving a balance between the various security requirements of different parties [23].

On the other hand, risk can be transformed to a third party by insurance, a traditional economic tool. The insurer will bear a specified risk during a particular period of time [24].

The rise of insurance depends crucially on the question of whether or not the security risks of e-commerce, especially of using digital payment-systems, are insurable. Principally, there will be an insurance-deal when both parties, the insurant and the insurer, are able to achieve utility gains by the risk-transfer. But there is no commonly defined limit of insurable risks [31]. From the insurer's viewpoint, there are ideally six conditions of an insurable risk given in the literature[25]. These conditions need to be adapted to security risks, which is an issue for further research. However, we exemplify below some of the problems:

- A *large number* of individuals threatened by the same kind of losses must exist. This is undoubtedly given on the Internet.
- The loss must be *accidental* and *unintentional*. A potential insurer of security risks will have to judge this condition carefully, because of the possibility of intentional attacks by intruders or losses caused by insurants themselves, just to get the insurance payment.
- The entrance of loss must be *determinable* and *measurable*. This can be problematic because proving the existence of a loss may be impossible for immaterial goods like, e.g. a privacy invasion.
- The loss should *not* be *catastrophic*. A large number of insurants should not be in danger of suffering losses at the same time. This condition is problematic since there may be massive hacker attacks breaking a digital payment system.

[13] "Risk" means in this context, the threat of discrepancy between expectations and outcome. That is, the user expects a certain security level, according to the criteria of multilateral security. There may be the risk that his demands, his adoption level, are not complied with.

[14] Note that it is easily imaginable that a security requirement can be fulfilled to a certain degree rather than just fully or not at all. E.g., most digital payment systems give partial anonymity only. Also, the risk of an attack, that is its plausibility or eventually the probability, must be accounted for.

[15] Some current developments are asymmetric encryption with elliptic curve cryptography (ECC) [20], eventually leading to cost reductions with lower hardware requirements for saving private keys; user hardware which is portable and trustworthy, i.e. cannot be manipulated; biometric technology (fingerprint reader or iris scans) for user authentication.

[16] In this case the intermediary can attest the fulfillment of very special security criteria for one payment system [10].

[17] In this case the intermediary is a necessary assumption for trustworthy use of digital certificates in order to authenticate the participants

- The chance of loss must be *calculable*.
- The insurants must be *able to pay the insurance premium*. Thus, the insurance must be an attractive purchase.

Besides insurance, it is conceivable that security risks can also be traded at a marketplace in the future. Financial markets have inflated throughout the past decades because of risk trading, so why not trading security risks as well? The advantage of this would not only be the increased options for risk sellers, but also the market mechanism for finding a fair price for security risks. This does not necessarily mean end-users take up risk trading by themselves. Correspondingly, private households today do not participate in financial markets on a large scale. However, intermediaries who participate can offer their customers assets with reduced risk, such as stocks or bonds, and thus help reduce overall risk. By analogy, trading security risks may yield evolution of security handling services available to end-users from intermediaries in the security risk market.

Some research has already been undertaken in this direction. First of all, security must be an economic item. This is the case as long as individuals are willing to pay a certain price (not necessarily money, but time and effort as well) in order to achieve more security, which can be observed. Security damages cannot always be accounted for (what would a privacy invasion cost?), but individuals could define a value of their risk. In other words, as long as property rights are defined, that is saying who bears which risk, security can be handled as an economic good which should be tradable. The idea of trading privacy has been proposed by [26] in a model where individuals sell personal information about themselves but buyers cannot take unrecognized advantage of this. Reference [27] then shows pricing mechanisms for privacy related information. These mechanisms should be extended to an overall pricing of personal security.

In a market for security risks, new intermediaries will evolve. How can they be established besides insurance companies? Basically, besides low transaction costs they must reduce agency costs, that is they must be trusted by market participants. Therefore, trust evolution is an issue for further research. One idea is that participants rate each other; trustworthy agents will then get high rankings and thus be able to signal even more trustworthiness. Reference [17] shows some basic ideas about the evolution of trust.

Finally, risk will be distributed among all parties involved. Those who explicitly bear risks, like insurers or individuals whose adoption level cannot be met, need to build risk reserves [22].

These basic approaches depicted, enabling individuals to reach their adoption level with non-technical means, will be integrated into our concept of risk management.

IV. Towards Individual Risk Management

With the theoretical background derived from Chapters II and III we are building a software tool (the "CDSS," cf. Chapter C) enabling users to put transaction specific risk analysis and risk handling into practice. For that purpose the software tool in form of a dialog component provides users both with consultancy and with decision support handling their digital payment systems. Finally, it would be useful to integrate this component in these above mentioned existing architectures for securing electronic commerce.

The dialog component proposed consists of two constituents, the consultation and the decision support one. With the consultation dialog, users can obtain common information about payment systems in his portfolio, e.g. provider, time of debit and encryption algorithms deployed. Abstract security requirements are explained as well. This information is permanently updated by experts according to alterations on the market of digital payment systems.

The decision support dialogue serves to determine the user's security requirements (adoption level) as well as the prohibitive price in a situational way. Default settings for user requirements are given in order to simplify usage.[18] On the other hand, based on the security profiles (cf. Chapter D) and the user profiles (cf. Chapter A), a payment system suitable for the transaction is recommended.

The configuration panel displays the current user profile in a constantly visible way. It enables a quick and easy configuration at any time. Finally it is important to note that users get away from defining numerous detailed security requirements, but may define some few abstract protection goals (cf. Chapter B).

V. Outlook For future research

At first, the software component will be used as a prototype in an environment of simulated payment transactions.[19] Attacks as well as human and technical failure will be simulated. Later on, in order to further broaden the application basis of the software tool, interfaces should be developed, allowing for an integration of additional services. Thus, offers for risk insurance by an insurance company could be integrated into the guidance tool (CDSS), for instance.

The perception of security risks is a current field of study at our institute. We are awaiting results from three diploma theses about security requirements for digital payment systems [29]. Some insight into security understanding and needs by users have already been attained by questionnaires with selected bank customers [3]. Further empirical studies are on their way. Many problems of risk handling can only be recognized in real life situations, however, because of the complexity of intertwined technique, organization, legal issues, etc. [30]. Thus, to obtain the desired effects in practical usage and to evaluate the acceptance of the software, lab tests accompanying theoretical research will be conducted,[20] including attack scenarios for later field tests.

Acknowledgment

We would like to thank Julia Bär, Jürgen Englert and Dr. Kai Rannenberg for their constructive and helpful advice.

[18] Basis for those default settings are the results of an empirical study, which was conducted in cooperation with Commerzbank, AG.

[19] Probands will have to work with the developed advice and decision-support system in different trials, to evaluate its functionality.

[20] The laboratory-tests will be conducted with reference to the well proven method of "simulation-study." These tests can apply the Experiences made with an "simulation-study" conducted by the Daimler-Benz Kolleg "Security in Communication Technology" in autumn 1997 will flow into those laboratory-tests., [30].

REFERENCES

[1] K. Kurbel and F. Teuteberg, "Betriebliche Internetnutzung in der Bundesrepublik Deutschland – Ergebnisse einer empirischen Untersuchung", 2., erweiterte Auflage, Frankfurt (Oder), April 1998, p.14.

[2] D. Schoder, R. Strauß and P. Welchering, "Electronic Commerce Enquete 1997/98, Empirische Studie zum betriebswirtschaftlichen Nutzen von Electronic Commerce für Unternehmen im deutschsprachigen Raum", Executive Research Report, Stuttgart, 1998.

[3] T. Kiefer, "SITRAVEC – Sichere Transaktionen und Vertrauen im E-Commerce: Empirische Analyse der Sicherheitsanforderungen und relevante Produkte aus Kundensicht", Arbeitspapier, IIG, Abteilung Telematik, 1999.

[4] H. Damker, M. Reichenbach, "Personal Reachability Management in a Networked World", in: Proceedings of IWNA98; *1998 IEEE Workshop on Networked Appliances*, Kyoto, Japan, November 1998

[5] M. Krochmal, "Where Economics Fits In With Technology", in: TechWeb, 1998.

[6] J.L. Abad-Peiro, N. Asokan, M. Steiner, and M. Waidner, "Designing a generic payment service", Technical Report 212ZR055, IBM Zurich Research Laboratory, 1996.

[7] N. Asokan, P. Janson, M. Steiner, and M. Waidner, "The State of the Art in Electronic Payment Systems", in: IEEE Computer, Sept. 1997, pp. 28-35.

[8] E. Petzel, "Integration von Versicherungen in Sicherheitskonzepten", Lecture on Congress *IT-Sicherheitsmanagement*'98 in München.

[9] F. Damm and F.-W. Menge, "Cost Comparison of Traditional and Alternative Telecommunication Security Approaches", in: G. Müller and K. Rannenberg (ed.), *Multilateral Security in Communications – Technology, Infrastructure, Economy*, München, 1999.

[10] K. Rannenberg, *Zertifizierung mehrseitiger Sicherheit – Kriterien und organisatorische Rahmenbedingungen*, Dissertation Universität Freiburg, Vieweg (DuD-Fachbeiträge), 1998.

[11] A. Pfitzmann, *Diensteintegrierende Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz*, Dissertation Universität Karlsruhe 1988/89, Springer-Verlag Heidelberg u.a., January 1990.

[12] K. Rannenberg, A. Pfitzmann and G. Müller 1999, "IT Security and Multilateral Security", in: G. Müller, K. Rannenberg (ed.): *Multilateral Security for Global Communication - Technology, Application, Business*. Vol. 3, Addison-Wesley-Longman, 1998, Bonn; Reading, Massachusetts, July 1999.

[13] G. Müller, "Sichere Kommunikation – Vertrauen durch Technik oder Vertrauen mit Technik?", in: G. Frhr. zu Putlitz and D. Schade (ed.), *Wechselbeziehungen Mensch, Umwelt, Technik*, Stuttgart 1997, pp. 147-173.

[14] G. Müller, U. Kohl and D. Schoder, *Unternehmenskommunikation: Telematiksysteme für vernetzte Unternehmen*, Bonn, 1997, p. 306.

[15] M. Reichenbach, *Entscheidungsunterstützung bei der Zahlungssystemwahl im Internet - Kriterien für die Auswahl digitaler Zahlungssysteme*, Thesis, University of Freiburg, 1999, http://www.iig.uni-freiburg.de/~marei/publications/degdiss99.pdf.

[16] J. L. Abad Peiro, P. Steiger, "Making Electronic Commerce easier to use with novel user interfaces", in: *Electronic Markets*, p. 8-12, 1998.

[17] L. Faith Cranor, J. Reagle Jr., "Designing a Social Protocol: Lessons Learned from the Platform for Privacy Preferences Project", April 1998.

[18] Bank for International Settlements, *Security of electronic money*, Basel, 1996.

[19] N.Asokan, B. Baum-Waidner, M. Schunter, M.Waidner, "Optimistische Mehrparteien – Vertragsunterzeichnung", in: R. Baumgart, K. Rannenberg, D. Wähner, G. Weck (ed.), *Verläßliche Informationssysteme*, Braunschweig, Wiesbaden, 1999, pp. 49-66.

[20] Certicom, *ECC Tutorials and Whitepapers*, http://www.certicom.com/ecc.

[21] A. Hamamtzoglou, T. Hecht, I. Papadopoulos, A. Weber, "The Fair Internet Trader", in: G. Lacoste, B. Pfitzmann, M. Steiner, M. Waidner (ed.): *SEMPER Final Report*, LNCS, Springer, Berlin, Forthcoming.

[22] M. Haller, "Risiko-Management – Eckpunkte eines integrierten Konzeptes", in: H. Jacob (ed.), *Schriften zur Unternehmensführung – Risiko-Management*, Wiesbaden, 1986, p. 32.

[23] H. Damker, U. Pordesch, M. Reichenbach, "Personal Reachability and Security Management", in: G. Müller and K. Rannenberg (Eds.), *Multilateral Security in Communications – Vl.3. Technology, Infrastructure, Economy*, München et al., 1999, pp. 95-112.

[24] D. Farny, *Versicherungsbetriebslehre*, Karlsruhe, 1995, p. 14.

[25] G. E. Rejda, *Principles of Risk Management and Insurance*, 1992, pp. 24-26.

[26] K. Laudon, "Markets and Privacy", in: *Communications of the ACM*, Vol. 39, No. 6, 1996, pp.92-104.

[27] K. Laudon, "Extensions to the Theory of Markets and Privacy: Mechanics of Pricing Information", in: US Department of Commerce: *Privacy and Self-Regulation in the Information Age*, Washington D.C., 1997, pp 41-49, http://www.ntia.doc.gov/reports/privacy/.

[28] M. Reichenbach, H. Damker, H. Federrath, K. Rannenberg, "Individual Management of Personal Reachability in Mobile Communication", in: Proceedings of the *IFIP TC11 SEC 97, 13th International Information Security Conference*, 14-16 May 1997 in Copenhagen.

[29] T. Költzsch, M. Reichenbach, "Ein nutzerorientiertes Konzept zur Risikoeinschätzung und Risikohandhabung bei der Zahlungssystemwahl", in: A.W.Röhm et al. (ed.), *Sicherheit und Electronic Commerce*, Workshop Proceedings, pp. 79-91.

[30] E. Ammenwerth, A. Buchauer, H.-B. Bludau, A. Roßnagel, "Simulation Studies for the Evaluation of Security Technology", in: G. Müller, K. Rannenberg (ed.): *Multilateral Security for Global Communication - Technology, Application, Business*, Vol. 3, Addison-Wesley-Longman, 1998, Bonn; Reading, Massachusetts, July 1999.

[31] D. Farny, *Versicherungsbetriebslehre*, Karlsruhe, 1995, p. 27.

[32] G. Wolf, *Charakteristika von Schutzzielen und deren Umsetzung in Benutzungsschnittstellen*, Dissertation Universität Dresden, 1999.