Security Issues in Mobile Payment from the Customer Viewpoint

K. Linck and Key Pousttchi and Dietmar Georg Wiedemann

University of Augsburg

2006

Linck, K.; Pousttchi, K.; Wiedemann, D. G.: Security Issues in Mobile Payment from the Customer Viewpoint. In: Ljungberg, J. (Hrsg.): Proceedings of the 14th European Conference on Information Systems (ECIS 2006). Göteborg, Schweden 2006, S.1-11.

SECURITY ISSUES IN MOBILE PAYMENT FROM THE CUSTOMER VIEWPOINT

Linck, Kathrin, University of Augsburg, Universitätsstraße 16, 86159 Augsburg, Germany, kathrin.linck@wiwi.uni-augsburg.de

Pousttchi, Key, University of Augsburg, Universitätsstraße 16, 86159 Augsburg, Germany, key.pousttchi@wiwi.uni-augsburg.de

Wiedemann, Dietmar G., University of Augsburg, Universitätsstraße 16, 86159 Augsburg, Germany, dietmar.wiedemann@wiwi.uni-augsburg.de

Abstract

The perception of mobile payment procedures' security by the customer is one major factor for the market breakthrough of the according systems. In this paper we examine security issues in mobile payment from the viewpoint of customers. Based on theoretical research we analyze empirical data from the MP2 mobile payment study with 8295 respondents in order to develop a set of dimensions, categories and aspects. The results do have a scientific as well as a practical impact: They provide a basis for the selection of appropriate indicators for further empirical studies. Furthermore they can serve as a guideline for mobile payment service providers in order to prevent security concerns through appropriate design and communication of payment procedures and to convince customers of the security of their mobile procedures by meeting concerns in informative advertising.

Keywords: Mobile Payment, Subjective Security, Objective Security, Concept-Specification

1 INTRODUCTION

Mobile payment (MP) is expected to become one of the most important applications in mobile commerce (Varshney & Vetter 2002). Since companies are not going to invest in the development of innovative mobile applications or services unless they can be charged for appropriately, the existence of standardized and widely accepted mobile payment (MP) procedures is crucial for the development of mobile commerce (Pousttchi & Selk & Turowski 2002, Dahlberg & Mallat & Öörni 2003). Whereas in electronic commerce we still see an important role of traditional payment systems (e.g. Krueger & Leibold & Smasal 2006), a payment system for mobile commerce will be typically not adequate until it shares fundamental characteristics of the mobile offer it is to bill for, in particular its ubiquity (Pousttchi & Selk & Turowski 2002, Coursaris & Hassanein 2002, Mallat 2004). As a result MP is crucial for, but not limited to the mobile commerce scenario as we will show later. Pousttchi and Wiedemann (2005) show how customers benefit from an MP procedure: The most important relative advantages over conventional payment systems[1] are ubiquity (the accessibility of a procedure and the reachability of payees at any time from any location), the ability to handle micropayments (smaller than 10 EUR /USD), the avoidance of cash at vending machines, and faster conduction of payments (e.g. customer-to-customer transactions in the use case scenario online auction).

According to the unanimous forecasts of the years 1999/2000 (for examples see e.g. Taga & Karlsson 2004) mobile phones should by now have been firmly established as payment terminals in the most diverse fields. However, whereas merchants and Mobile Payment Service Providers (MPSP) made a multitude of attempts to offer respective services, absence of wide customer acceptance of the offered procedures prevented a market breakthrough in most markets up to now. In addition to the lack of standardization and universality of the procedures, security concerns of customers are one of the main inhibitors (Pousttchi 2005, Ketterer & Stroborn 2002, Ehrhardt 2002, Zieschang 2002).

Although the issue of security has emerged as a major inhibitor of mobile payment acceptance, the research on this issue is quite rare to date, especially from the viewpoint of customers. Therefore, this study seeks to approach the issue from the empirical perspective in order to come to a better understanding of the concept. Based on the basic distinction of the dimensions *objective* and *subjective security* arising from our theoretical research we analyze empirical data with the aim to extract relevant statements and aggregate them to statement groups and categories. For this analysis we employ the data of the MP2 mobile payment study with 8295 respondents which collected data for 40 use cases in different payment scenarios and amount levels.

The outcome of the paper is an empirically developed set of dimensions, categories and aspects which is of scientific as well as of practical importance: They provide a basis for the selection of appropriate indicators for further empirical studies. Furthermore they can serve as a guideline for MPSP in order to prevent security concerns through appropriate design and communication of payment procedures and to convince customers of the security of their mobile procedures by meeting concerns in informative advertising.

The rest of the paper is organized as follows: In section 2 we define mobile payment and provide related work. In section 3 we describe the research methodology. In section 4 we present and discuss our results: In section 4.1 we identify the relevant dimensions. In 4.2 we derive categories and statement groups of subjective security. Section 4.3 presents implications and recommendations for MPSP. In section 5 we summarize and outline the main findings.

[1] Please note that our discussion of a general payment method, such as credit card usage, electronic payment, or MP, refers to the term *payment systems*. When we talk about concrete solutions such as Paybox or Crandy, we use the term *payment procedures*.

2 BACKGROUND

2.1 Mobile Payment

On closer examination we have to differentiate two basic functions of MP: payments inside and outside mobile commerce (Pousttchi 2005). Inside mobile commerce MP is used for payments of mobile offers and is ideally system inherent. In the area of charging mobile services we distinguish two basic terms: mobile billing and mobile payment. We refer to *mobile billing* as billing of telecommunication services by a mobile network operator or a mobile virtual network operator within an existing billing relationship (Turowski & Pousttchi 2004). We define *mobile payment* as that type of payment transaction processing in the course of which – within an electronic procedure – (at least) the payer employs mobile communication techniques in conjunction with mobile devices for initiation, authorization or realization of a payment (Pousttchi 2003). If a mobile payment procedure is provided by an MNO/MVNO, we will have the intersection of mobile billing and mobile payment.

Outside mobile commerce, an MP procedure can be understood as a mobile commerce application to complete payments in different situations. For this purpose four general settings – referred to as *payment scenarios* – are to be considered (Kreyer & Pousttchi & Turowski 2002b, and the extension in Khodawandi & Pousttchi & Wiedemann 2003): transactions on the stationary Internet *(electronic commerce scenario)*, at any kind of vending machine *(stationary merchant automat scenario)*, in traditional retail *(stationary merchant person scenario)* and between end-customers *(customer-to-customer scenario)*.

2.2 Related Work

Security and privacy concerns of transactions are not novel concepts (Westin 1967). At merchants with no good reputation consumers have always been concerned about using debit or credit cards. This real world example holds also true for commercial transactions on the Internet (Chellappa & Pavlou 2002). Hence, Friedman, Kahn and Howe (2000) and Shneiderman (2000) argue that improving positive security and privacy perceptions are most important for sustained activity in electronic commerce.

Security issues in electronic payment procedure have already had a significant amount of discussion in the literature (e.g. Ketterer & Stroborn 2002, Strube 2002, Zieschang 2002). In order to evaluate possible risks related with electronic payment procedures, Reichenbach (2001) uses criteria of multilateral security (Rannenberg 1989) and refines them. Also Jakubowicz, Hanssens and Henriksen (2003) develop a framework for analyzing the risks involved in electronic payments. They include the scenarios in which there may be a loss of money or privacy, the probability of these scenarios and the major possible negative consequences. Both approaches are based on the individual and therefore subjective viewpoints of the researchers. This entails the risk that relevant issues are not included and might lead to a loss of information, or that irrelevant issues are taken into account without any information gain (Fürtjes 1982).

Chari, Kermani, Smith and Tassiulas (2000) argue that mobile commerce solutions differ from electronic commerce solutions because the underlying technology has basic differences which create a range of new security exposures. For instance, the portability of mobile devices makes theft, loss, and damage of client devices much more likely. Therefore they assume that also the perception of security in mobile commerce may differ from that one in electronic commerce.

Examining barriers to adoption of MP, Khodawandi, Pousttchi and Wiedemann (2003) indicate that the lack of perceived security (later defined as subjective security) is the most frequently called reason for a refusal. Rogger and Celia (2004) found similar results. Little empirical research has been undertaken to understand the nature of the concept *perceived security* regarding mobile commerce and

especially mobile payment. A notable exception is the study of Dahlberg, Mallat and Öörni (2003). They identify six different types of security risks in focus group interviews. The differences between their study and the study at hand lies in the level of detail of the results (section 4.2) and the greater sample size (46 for Dahlberg et al. versus 3930 extracted from the MP2, as shown in section 3).

3 METHOD

Empirical research on security from the end-customers' viewpoint faces a major problem: Theoretical concepts like security are too abstract and generally formulated to allow a direct definition of indicators to measure them or to use them for informative advertising. Thus, it is necessary to specify their content. For this purpose, we use a method called *concept-specification* (Schnell & Hill & Esser 1999) that originates from the social sciences and is used here to break down the concept of security into *dimensions*, *categories* and *statement groups*. The concept-specification follows a step-by-step approach.

In a first step, the concept security is split into relevant dimensions. On the top level we use the security definition of Kreyer, Pousttchi and Turowski (2002b) who distinguish between the dimensions objective and subjective security as described in section 4.1. After that, a much more detailed splitting into categories and statement groups is undertaken. To minimize the risks mentioned in section 2.2 (Fürtjes 1982), categories and statement groups are derived from the results of the study MP2 which was conducted by the University of Augsburg from August 2003 to January 2004 with the participation of 8295 respondents. This study is based on an online questionnaire according to Dillman (2000) and mainly aims to analyze the different payment scenarios and concrete use cases. Besides demographic questions and other questions related to MP (for detailed results see Eisenmann & Linck & Pousttchi 2004), respondents were asked the open-ended question "What would you require to feel secure about using mobile payments?" The aim of this question was to explore categories and statement groups of subjective security. We decided in favor of an open-ended question because this allows people to express themselves in their own words which lead consequently to richer, more detailed information (Schnell & Hill & Esser 1999, Friedrichs 1990). In order to avoid drawbacks of open-ended questions the opportunity to answer "no response" was explicitly offered.

The answers were analyzed by first sifting all statements and then categorizing them into statement groups. As very detailed answers were given partly it was necessary to form large numbers of statement groups. The statement groups were afterwards summarized to categories (Schnell & Hill & Esser 1999). The category names presented in section 4.2 represent the most frequent statements. In order to achieve a usable and thus manageable result we tried to restrict the analysis to the category level wherever possible and extended it to the level of statement groups only when a significant number of statements showed up in these or important information was contained at the lower level.

After we have illustrated the concept-specification, we will now describe the sample of the study. We checked plausibility, integrity and completeness of the 8295 received questionnaires with the result that 6343 could be used for further analysis. The sample was not a representative sample of the total population (since already the appliance of an online questionnaire prevents this). However, the sample was relatively balanced in demographic aspects, e.g. 0.6% were younger than 16 years, 5.8% between 16 and 20 years, 22.6% between 21 and 25 years, 22.8% between 26 and 30 years, 29.7% between 31 and 40 years, 12.8% between 41 and 50 years und 5.6% older than 50 years. The most important occupational groups are salaried employees (43.6%), students (27.3%) and self-employed persons (10.5%). The affinity to technology and their adoption among the respondents was very high (for a more detailed description of the sample see Eisenmann & Linck & Pousttchi 2004).

In view of the highest education attained we can believe that most of respondents had no problem with expressing their own opinion regarding the open-ended question. Since completing the questionnaire took about 20 minutes, we assume that it was necessary for most of the respondents to have a certain interest in MP. Moreover, when talking to MPSP about their target group we see remarkable

similarities to the sample represented above. Also respondents' direct statements let the sample appear as the target group for MP: While even 14.8% indicated that they have already used a MP procedure, only 6.9% took no stock in MP. Our conclusion is that we can not make general statements about security concerns of the total population but very well of the current MP target group. Thus, with regard to the objective of the study the sample seems to be ideal.

4 RESULTS AND IMPLICATIONS

4.1 Dimensions of Security

Examining the conditions for actual utilization of MP procedures from the viewpoint of customers, Pousttchi (2003) differentiates between *essential* and *commensurate conditions*. Fulfilling all essential conditions causes a customer to accept a MP procedure as a usable method of payment in principle. However, the infringement of one single essential condition will prevent the customer from using the procedure. Fulfilling one of the commensurate conditions could turn, then, this acceptance into actual usage. Each of these two represents a single step of change of the customer's attitude towards MP.

The issue of acceptance of MP procedures has already had a significant amount of discussion in the literature (e.g. Dahlberg & Mallat & Penttinen & Sohlberg 2002, Ding & Hampe 2003). For the customer, the arguments can typically be subsumed into three aspects: security, costs and convenience (Kreyer & Pousttchi & Turowski, 2002a), put in an order of relevance according to Pousttchi (2003). Essential conditions may occur as functionality requirements such as the capability to pay in a certain scenario or to use a certain method of settlement. Typically, these can also be assigned to the above aspects.

In this paper, we focus on the essential condition "security" that is of prime importance for customers accepting a MP procedure (Kieser 2001, Khodawandi & Pousttchi & Wiedemann 2003, Rogger & Celia 2004). According to Kreyer, Pousttchi and Turowski (2002b) we distinguish the concept security between the two dimensions objective and subjective security. *Objective security* is a concrete technical characteristic, given, when a certain technological solution responds to all of five security objectives: confidentiality, authentication, integrity, authorization and non-repudiation (Merz 2002). In table 1 we define these security objectives and name technologies and criteria securing MP.

Security objective	Definition	Enabling concept/technique
Confidentiality	Property that ensures that transaction information cannot be viewed by unauthorized persons	Encryption
Authentication	Property that the transaction information actually originates from the presumed transaction partner	Possession (e.g. of a mobile phone), knowledge (e.g. of a PIN) und property (e.g. biometric property)
Integrity	Property that the transaction information remains intact during transmission and cannot be altered	Digital signatures
Authorization	Property that parties involved must be able to verify if everyone involved in a transaction is allowed to make the transaction	Digital certificates
Non-repudiation	Property that no one should be able to claim that the transaction on his/her behalf was made without their knowledge	Digital signatures

Table 1. Sub-goals of objective security according to Merz (2002)

In recent years also the availability of a system is frequently called which provides functionality to ensure that the service is accessible and usable (Turowski & Pousttchi 2004).

As it is unlikely that the average customer is able to evaluate the objective security of a procedure (e.g. Egger & Abrazhevich 2001), the essential condition for MP acceptance is the perception of security. In the following we denote the latter as subjective security. *Subjective security* is defined as the degree of the perceived sensation of the procedures' security from the viewpoint of the customer. Therefore, subjective security can be seen as the mirror image of risk affinity.

It is important to mention that the two dimensions objective and subjective security are neither disjoint nor independent. As subjective security has no effect on objective security, the empirical results in section 4.2 can only affect subjective security whereas objective security itself stays with the sub-goals from table 1 as categories. However, the other way round, the level of objective security influences the level of subjective security. This can be seen in the great amount of objective security criteria named by respondents as factors for their perceived security level.

4.2 Subjective Security

The statements on the open-ended question *"What would you require to feel secure about using mobile payments?"* were categorized into statement groups and these aggregated to categories according to the exploration process described in section 3. 3930 respondents expressed in all 4998 statements, whereas only 2413 chose the given possibility to state "no response". In case of a respondent stated more than one security issue, the statements were disaggregated and each was put in its respective statement group. Afterwards statement groups were aggregated to overriding categories. The analysis of data results in 15 categories with very different frequencies; the latter allows for conclusions about the importance of the respective subjective security features for customers.

The most frequent category was *confidentiality* with 646 answers. Above all, this category comprises the statement groups *data protection* (241), *data security* (159), *unauthorized access* (62) and *no data transfer* (61).

The second category is *encryption* with 611 answers. It includes just two main statement groups: *general demand for encrypted data transfer* (539) and *concrete answer of an encryption level or procedure* (72); the latter summarizes statements as "128 / 256 / 512 bit", "SSL" or "PKI".

The third category consists of statements which only contained the tautological declaration *"security"* (586).

Transparency and traceability of the MP procedures play an important role for the subjective security feeling. This category contains 578 statements, main statement groups are *traceability of costs* (149), *traceability of account* (139) and *confirmation of payment* (116).

Authentication and authorization as a further important security category was named by 424 statements wherein the most stated by far was *using PIN* (personal identification number) and/ or TAN (transaction number) (303). Other statement groups were *authentication* (39), *authorization* (16) and *unambiguous identification* (49). Herein, mostly particular methods were named such as password enquiry.

The category *trust in MPSP* (109) mainly contained the statement groups *MPSP has to be reliable* (92) and *MPSP has to be familiar* (79), *the claim for safety guarantees* (54) and *the availability of an information service for customers* (37).

Fraud protection (202) includes some detailed statements concerning *integrity* (41), *protection against hackers* (39) or *no possibility of unauthorized usage* (27).

The category *anonymity* was only named in 70 statements. This may seem surprising as the feature is an important issue in most discussions on MP security, however, this result confirms the respective outcome of the precedent survey MP1 (Khodawandi & Pousttchi & Wiedemann 2003).

In the first view it not obvious why respondents mentioned *broad acceptance and diffusion* as a security feature. One possible explanation could be that customers feel secure if many other customers use a certain payment procedure. Another explanation could be a broad acceptance by merchants. If many merchants offer the opportunity to pay with a particular procedure the customer will assume it to be secure.

The category "others" includes a couple of smaller statement groups like *comparisons with other payment procedures* (69), *amount limit* (43) or *trust in settlement* (20) as well as a number of not attributable statements (36) and the *statement none or low costs* (105). As the latter statement is clearly off-topic it is subsumed under the category "others" – only regarding the frequency of statements it would be to place as an own category on rank 12. A possible explanation for this is that some respondents are supposed to use the first open-ended question to place emphasis on their most important feature for using an MP procedure. Table 2 shows the aggregated categories along with their frequency.

Rank	Category	Frequency of statements
1	Confidentiality	646
2	Encryption	611
3	Stating "security"	586
4	Transparency and traceability	578
5	Authentication and authorization	424
6	Trust in MPSP	413
7	Fraud protection	348
8	Convenience and ease of use	298
9	Secure infrastructure	263
10	Liability issues	111
11	Cancellation	107
12	Third party certification	89
13	Technical reliability	81
14	Broad acceptance and diffusion	76
15	Anonymity	70
16	Others	297
	Total number of statements	**4998**

Table 2. Resulting categories for the dimension subjective security

4.3 Implications

The results of section 4.2 allow for certain implications, especially recommendations to (prospective) MPSP.

First of all, on account of the large number of voluntary answers, it can be concluded that respondents are interested in expression of their opinion to this subject. Strongest doubts concerning security features were mentioned in the category *confidentiality*, especially in the statement group *data protection*. This empirically confirms the respective assumption of Pousttchi, Selk and Turowski (2002). The naming of *encryption* as second most named security feature is a confirmation and concretization of this trend. The concrete answers are also technical features as a diversion and strengthening of data protection. These provide an MPSP with evidence where he has to start the efforts to achieve a security feeling for the customers.

A very large number of respondents indicated "security" (or a similar statement) as most important feature for them to feel secure. This tautological answer allows for the conclusion that these customers do have a need for security which is strong – according to the generally high importance of security in the survey results (Eisenmann & Linck & Pousttchi 2004) – but somewhat undetermined. An important mean to provide subjective security at that point is marketing activity, especially the

creation and/or use of brands. Other MP2 results indicate that especially the existing brands of banks are suited for this purpose (Eisenmann & Linck & Pousttchi 2004). An attempt to create a respective MNO-owned brand accompanied the renaming of the Mobile Payments Service Association (MPSA) in Simpay[2].

The category *transparency and traceability* defines clear requirements to the provider: Respondents demand knowledge as a condition to control and the MPSP has to provide this knowledge. MP documentation especially with the feature *confirmation* is desired. The availability of transparency and traceability has considerable advantages.

Authorization is also a clear requirement that is to be met by the MPSP. Password enquiry and use of PIN and TAN are the most stipulated forms.

Trust in the MPSP is an important (subjective) security feature which was already stated by Khodawandi, Pousttchi and Wiedemann (2003). This can be empirically corroborated by our results. Again here, the use of a bank's brand name makes sense.

The claim for *fraud protection* results from the general human fear of misuse and fraud. MPSP has to accredit the user. While the objective solution to this issue is technical, the subjective concern should be answered utilizing marketing techniques in order to state that fraud protection can be taken for granted.

Desire for *convenience* and ease of use in conjunction with security leads to the conclusion that users do not feel secure if they do not understand an MP procedure. Frequently this item was mentioned along with the items secure and quick. Statements belonging to this category often recurred in combination with the statement "secure" (153). This forms a general claim for MP procedures to be easy to use, secure and quick.

With the statements belonging to *secure infrastructure*, respondents ask for objectively revisable technical features. Here again, the MPSP is postulated to supply the want of the user and to give notice to this.

Also *liability issues* are a necessity on the part of the user. Respondents want to have information about the consequences in case of fraud; especially they want to be protected against the risk of loss. Thus the knowledge of the contingencies (in the best case shaped favorable to the user) promotes subjective security.

Cancellation also concerns the after-payment process. The user wants to be protected against the risk of loss. According to the system of the bank, mistakes on either side in erroneous entry should be possible to adjust.

The demand of *third party certification* is easy to satisfy by using advertisement and publication of certificates. It is, however, named in a relatively low number of statements. Additionally, this demand for independent experts leads to the conjecture that users feel insecure and not competent; thus they may be affected by marketing measures.

Just a few of the users express *concrete doubts on technical reliability*. These may feel more competent and rely merely on the objective security of the system. Nearly the same number of respondents called the *broad acceptance and diffusion* as main security feature. These users probably belong to the group of laggards which are not supposed to use such a system in the current (early) phase anyway.

The last feature in the list is *anonymity* which is often considered as an important security feature. In our empirical study this proposition can be disproved. According to these results anonymity can be nearly disregarded in consideration of security of MP procedures from the customers' viewpoint.

[2] This vertical alliance of Orange, Telefonica Moviles, T-Mobile and Vodafone stopped its activities in June 2005.

5 CONCLUSION

In this paper we examined security issues in MP from the viewpoint of the customer. We distinguished the dimensions of objective and subjective security. It is easy to operationalize the first one as this is only a special case of IT security (and the examination of existing MP procedures shows that *objective security* can almost be regarded as a given). Despite that, customers don't feel safe even if they could do so – the real security problem is the missing *subjective security*.

The outcome of the paper is an empirically devised set of dimensions, categories and aspects which is suitable to serve as a basis for the selection of appropriate indicators for further empirical studies. We will use them for our next study MP3 in order to examine the influence of the subjective security on the intention to use a mobile payment procedure. Furthermore we drew conclusions and gave recommendations for MPSP to prevent security concerns through appropriate design and communication of the payment procedures and to convince customers of the security of their MP procedures by meeting their concerns in informative advertising.

MPSP must meet security requirements; otherwise customers will ignore the respective payment procedure. It is however important to realize that security is an essential condition, not a commensurate one. Fulfilling all essential conditions causes a customer to accept an MP procedure as a usable method of payment in principle (and thus, at least, not to exclude its usage), while fulfilling one of the commensurate conditions could turn, then, this acceptance into actual usage. Beneath security, further essential conditions are to be found in the area of cost and convenience (e.g. Kreyer, Pousttchi & Turowski 2002a). On many markets a further important requirement from the customer side is the universality of a payment procedure (Pousttchi 2005).

Build on this foundation, MPSP must try for meeting the commensurate condition for actual MP usage – the creation of added values for the user.

References

Chari, S., Kermani, P., Smith, S. and Tassiulas, L. (2000). Security Issues in M-Commerce: A Usage-Based Taxonomy. In E-Commerce Agents: Marketplace Solutions, Security Issues, and Supply and Demand (Liu, J. and Ye, Y. Eds.), 264-282. 1st Edition. Springer, Berlin.

Chellappa, R.K. and Pavlou, P. (2002). Perceived Information Security, Financial Liability, and Consumer Trust in Electronic Commerce Transactions. Journal of Logistics Information Management 15 (5/6), 358-368.

Coursaris, C. and Hassanein, K. (2002). Understanding M-Commerce – a Consumer Centric Model. Quarterly Journal of Electronic Commerce, 3 (2), 247-271.

Ding, M.S. and Hampe, J.F. (2003). Reconsidering the Challenges of mPayments: A Roadmap to Plotting the Potential of the Future mCommerce Market. In Proceedings of the 16th Bled Electronic Commerce Conference, 873-884, Slovenia, Bled.

Dillman, D.A. (2000). Mail and Internet Surveys. The Tailored Design Method. John Wiley & Sons, New York.

Dahlberg, T., Mallat, N., Penttinen, E. and Sohlberg, P. (2002). What Characteristics of Mobile Payment Solutions Make Them Valuable to Consumers? In Proceedings of the Global Information Technology Management Conference, USA, New York.

Dahlberg, T., Mallat, N. and Öörni, A. (2003). Consumer Acceptance of Mobile Payment Solutions – Ease of Use, Usefulness and Trust. In Proceeding of the International Conference on Mobile Business (Giaglis, G.M., Werthner, H., Tschammer, V. and Froeschl, K. Eds.), 211-218, Austria, Vienna.

Egger, F.N., Abrazhevich, D. (2001). Security & Trust: Taking Care of the Human Factor. Electronic Payment Systems Observatory Newsletter, Vol. 9. September 2001, available at http://epso.jrc.es/newsletter/vol09/ 6.html, accessed 09.06.2005.

Eisenmann, M., Linck, K. and Pousttchi, K. (2004). Nutzungsszenarien für mobile Bezahlverfahren. Ergebnisse der Studie MP2. In Proceedings of the 4th Workshop on Mobile Commerce (Pousttchi, K. and Turowski, K. Eds.), 50-62, Germany, Augsburg.

Ehrhardt, M. (2002). Banken im Electronic Commerce – eine Neudefinition? In Handbuch ePayment. Zahlungsverkehr im Internet: Systeme, Trends, Perspektiven (Ketterer, K.-H. and Stroborn, K. Eds.), 79-95, Deutscher Wirtschaftsdienst, Köln.

Friedman, B., Kahn, P.H. and Howe, D.C. (2000). Trust Online. Communications of the ACM, 43 (12), 34-40.

Friedrichs, J. (1990). Methoden empirischer Sozialforschung. 14th Edition. Westdeutscher Verlag, Opladen.

Fürtjes, H.-J. (1982). Das Gestaltungspotential von Instrumenten der empirischen Wirtschafts- und Sozialforschung. G. Marchal und H.-J. Matzenbacher Wissenschaftsverlag, Berlin.

Jakubowicz, Z, Hanssens B. and Henriksen S. (2003). Is Paying on the Internet Risky?, ePSO Discussion Starter 1, No. 2, available at www.e-pso.info/epso/index.html, accessed 12.06.2003.

Ketterer, K.-H. and Stroborn, K. (2002). Zahlungsverkehrssysteme im Internet – eine Einführung. In Handbuch ePayment. Zahlungsverkehr im Internet: Systeme, Trends, Perspektiven (Ketterer, K.-H. and Stroborn, K. Eds.), 7-14, Deutscher Wirtschaftsdienst, Köln.

Khodawandi, D., Pousttchi, K. and Wiedemann, D.G. (2003). Akzeptanz mobiler Bezahlverfahren in Deutschland. In Proceedings of the 3rd Workshop on Mobile Commerce (Pousttchi, K. and Turowski, K. Eds.), 42-57, Augsburg, Germany.

Kieser, M. (2001). Mobile Payment – Vergleich elektronischer Zahlungssysteme. In Mobile Commerce, HMD 220 (Meier, A. Ed.), 27-36, DPunkt, Heidelberg.

Kreyer, N., Pousttchi, K. and Turowski, K. (2002a). Characteristics of Mobile Payment Procedures. In Proceedings of the ISMIS 2002 Workshop on M-Services (Maamar, Z., Mansoor, W. and van den Heuvel, W.-J. Eds.), France, Lyon.

Kreyer, N., Pousttchi, K. and Turowski, K. (2002b). Standardized Payment Procedures as Key Enabling Factor for Mobile Commerce. In Proceedings of the EC-Web, E-Commerce and Web Technologies (Bauknecht, K., Quirchmayr, G. and Tjoa, A.M. Eds.), 400-409, France, Aix-en-Provence.

Krueger, M., Leibold, K. and Smasal, D. (2006). Online Payment Methods from the Viewpoint of Customers – Results of the Study IZV8. University of Karlsruhe.

Mallat, N. (2004). Theoretical Constructs of Mobile Payment Adoption. Information Systems Research Seminar in Scandinavia (IRIS), Falkenberg, Sweden.

Merz, M. (2002). E-Commerce und E-Business: Marktmodelle, Anwendungen und Technologien. 2nd Edition. Dpunkt Verlag, Heidelberg.

Pousttchi, K. (2003). Conditions for Acceptance and Usage of Mobile Payment Procedures. In Proceedings of the 2nd International Conference on Mobile Business (Giaglis, G.M., Werthner, H., Tschammer, V. and Froeschl, K.A. Eds.), 201-210, Austria, Vienna.

Pousttchi, K. (2005). Mobile Payment in Deutschland – Szenarienbasiertes Referenzmodell für mobile Bezahlvorgänge. 1st Edition. Deutscher Universitätsverlag, Wiesbaden.

Pousttchi, K., Selk, B. and Turowski, K. (2002). Akzeptanzkriterien für mobile Bezahlverfahren. In Proceedings of Mobile and Collaborative Business. Multikonferenz Wirtschaftsinformatik 2002. (Hampe, F., Schwabe, G. Eds.), 57-67, Germany, Nuremberg.

Pousttchi, K. and Wiedemann, D.G. (2005). Relativer Vorteil bei mobilen Bezahlverfahren - mobiles Bezahlen aus Sicht der Diffusionstheorie. In Proceedings of the 1st Mobile Business Day (Stucky, W. and Schiefer, G. Eds.), 35-50, Germany, Karlsruhe.

Rannenberg, K. (1998). Zertifizierung mehrseitiger IT-Sicherheit – Kriterien und organisatorische Rahmenbedingungen. Vieweg, Braunschweig.

Reichenbach, M. (2001). Individuelle Risikohandhabung elektronischer Zahlungssysteme. 1st Edition. Deutscher Universitätsverlag, Wiesbaden.

Rogger, A.J. and Celia, I. (2004). Akzeptanz des Kaufens und Bezahlens mit dem Mobiltelefon. In Proceedings of the 4th Workshop on Mobile Commerce (Pousttchi, K. and Turowski, K. Eds.), 79-85, Augsburg, Germany.

Shneiderman, B. (2000). Designing Trust into Online Experiences. Communications of the ACM. 43 (12), 34-40.

Schnell, R., Hill, P. and Esser, E. (1999). Methoden der empirischen Sozialforschung. 6th Edition. Oldenbourg, Munich.

Strube, H. (2002). ePayment, Phantom des Netzes. In Handbuch ePayment. Zahlungsverkehr im Internet: Systeme, Trends, Perspektiven (Ketterer, K.-H. and Stroborn, K. Eds.), 96-108, Deutscher Wirtschaftsdienst, Köln.

Taga, K. and Karlsson, J. (2004). Arthur D. Little Global M-Payment Report. Arthur. D. Little Austria GmbH, Vienna.

Turowski, K. and Pousttchi, K. (2004). Mobile Commerce. Grundlagen und Techniken. 1st Edition. Springer, Heidelberg.

Varshney, U. and Vetter, R. (2002). Mobile Commerce: Framework, Applications and Networking Support. Mobile Networks and Applications, 7(3), 185-198.

Westin, A.F. (1967). Privacy and Freedom. 1st Edition. Atheneum, New York.

Zieschang, T. (2002). Maßnahmen zur Entwicklung sicherer Zahlungssysteme. In Handbuch ePayment. Zahlungsverkehr im Internet: Systeme, Trends, Perspektiven (Ketterer, K.-H. and Stroborn, K. Eds.), 323-337, Deutscher Wirtschaftsdienst, Köln.