Electronic payment systems : a user-centered perspective and interaction design

E£ECTRONIC PA¥MENT SY$TEMS: a User-Centered Perspective and Interaction Design

Dennis Abrazhevich

JFS
J.F. Schouten School for
User-System Interaction Research

Electronic Payment Systems: a User-Centered Perspective and Interaction Design

Dennis Abrazhevich

The work described in this thesis has been carried out under the auspices
of the J.F. Schouten School for User-System Interaction Research.

CIP-DATA LIBRARY TECHNISCHE UNIVERSITEIT EINDHOVEN

Abrazhevich, Dennis

Electronic payment systems : a user-centered perspective and interaction design / by Denis Abrazhevich. – Eindhoven : Technische Universiteit Eindhoven, 2004. – Proefschrift. -

ISBN 90-386-1948-0

NUR 788

Keywords: Electronic payment systems / Online payments / E-commerce / User acceptance / Technology acceptance / User-centered engineering / Interaction design / Usability / Human-computer Interaction

Cover design: Jan-Willem Luiten, JWL Producties.

Printing: Universiteitsdrukkerij Technische Universiteit Eindhoven.

Electronic Payment Systems: a User-Centered Perspective and Interaction Design

PROEFSCHRIFT

ter verkrijging van de graad van doctor aan de
Technische Universiteit Eindhoven, op gezag van de
Rector Magnificus, prof.dr. R.A. van Santen, voor een
commissie aangewezen door het College voor
Promoties in het openbaar te verdedigen
op maandag 19 april 2004 om 16.00 uur

door

Denis Abrazhevich

geboren te Kerch, Rusland

Dit proefschrift is goedgekeurd door de promotoren:

prof. dr. G.W.M. Rauterberg

en

prof. dr. P.M.A. Ribbers

Copromotor:

dr. P. Markopoulos

To my parents

Моим родителям

Acknowledgements

I would like to express my gratitude to people who supported me in the course of my work. I thank my colleagues at Industrial Design, IPO, TM, and SOBU for interesting and productive work together.

This research would not have been complete without the participation of Comsys BV and Postbank. My special thanks to Diederik Husslage and Jan-Joost Bouwman, who helped me greatly with establishing the experimental environment. I am thankful to Simon Lelieveldt who has brought me in contact with the right people in the right time, and supported me with his valuable advice.

Great thanks go to my family and friends, especially to Bogdan Raducanu, Tim Marsh and dear Diana Flood who supported me in the final phase on my research. My best regards to Florian Egger and Rik Geurts to commemorate our discussions and work together. Great thanks to Wolmet Barendregt for helping with the numerous translations to Dutch.

And finally, I would like to express my most gratitude to my supervisors, to prof. Matthias Rauterberg, who supported me through the course of my research, and especially to my daily supervisor, dr. Panos Markopoulos, who helped me immensely with his advice and to the great extent contributed to the success of this thesis.

Contents

Chapter 1. Introduction **1**

1.1 Electronic payment systems and their place in electronic commerce 1
1.1.1 E-commerce and electronic payment systems 1
1.1.2 Limitations of traditional payment systems in the context of online payments 4
1.1.3 The need for new payment systems designed for e-commerce 6

1.2 User acceptance: understanding and issues 8

1.3 Research objectives 12

1.4 Research scope 13
1.4.1 The role of electronic payments in customer e-commerce activities 14
1.4.2 Approach and methodology 18

Chapter 2. Classification and characteristics of electronic payment systems **23**

2.1 Classification of payment systems 23
2.1.1 Introduction 23
2.1.2 Primary classification of payment systems 24
2.1.3 Further classification of account-based systems 25
2.1.4 Further classification of electronic cash systems 28
2.1.5 Payment mediation services vs. payment systems 29

2.2 Identifying the characteristics of payment systems 33

2.3 Advantages and limitations of payment models 39
2.3.1 Advantages and limitations of the electronic cash model 39
2.3.2 Advantages and limitations of the acount-based model 40

2.4 PayPal.com: Using characteristics for analysis of payment systems 41

2.5 Conclusions 44

Chapter 3. User survey of electronic payment systems 47

3.1 User acceptance of electronic payment systems 47

3.2 Survey of users' attitudes towards characteristics of payment systems 51
3.2.1 Survey participants 52
3.2.2 Questionnaire design and analysis 52
3.2.3 Survey results and discussion 53
3.2.4 Implications for user acceptance 56

Chapter 4. Diary study: a qualitative investigation of user experiences with EPSs 59

4.1 Introduction 59

4.2 Set-up of the diary study 61
4.2.1 Selection of subjects 62
4.2.2 Process and instrumentation 64
4.2.3 Diary study results 66

4.3 Analysis of the results 67

4.4 Conclusions 78

Chapter 5. Validating the design recommendations 81

5.1 Introduction 81
5.1.1 Expert review of the design recommendations 81
5.1.2 Method 83
5.1.3 Hypothesis 83
5.1.4 The system under test 84
5.1.5 Changes made to the Postbank Betaallijn based on the DRs 87
5.1.6 Subjects 89

5.2 Experimental setup 91
5.2.1 Overview 91
5.2.2 Dependent and independent variables 91
5.2.3 Experimental design 92
5.2.4 Tasks and instructions 93
5.2.5 Procedure 94

5.3 Results and Analysis 96
5.3.1 Results: repeated measures 96
5.3.2 Results: task specific measurements 109

5.4 Discussion 113
5.4.1 Validation of the design recommendations 113
5.4.2 Revision of not validated design recommendations 118
5.4.3 Limitations of the experimental study 119

5.5 Conclusions 121

Chapter 6. Discussion and conclusions 123

6.1 Summary of the thesis 123

6.2 Validity issues and limitations 127
6.2.1 Cause-effect validity 127
6.2.2 Generality issues 128
6.2.3 Conclusions 132

6.3 Future work 132

Appendix A 135

Appendix B 147

Appendix C 151

Appendix D 153

Appendix E 173

References 179

Samenvatting (summary in Dutch) 187

Curriculum Vitae 189

Chapter 1

Introduction

1.1 Electronic payment systems and their place in electronic commerce

In the early 1990s the business and consumer world encountered a new way of conducting trade business, which was named *electronic commerce* (e-commerce). Over the years electronic commerce has evolved into a popular and acknowledged way of conducting business. While researchers are still trying to understand it and gauge its importance and turnover, e-commerce is changing and growing incredibly quickly, producing such extraordinary results from both business and customer perspective that its phenomenon cannot be overlooked by anyone who has ever thought of conducting business, whether in online or offline environments. With many organisations and people labouring in the field of e-commerce it has become very clear that e-commerce is here to stay and organisations and customers are trying to get maximum benefit from it.

E-commerce has become especially important in two interrelated dimensions, namely business-to-consumer (B2C) and business-to-business (B2B) e-commerce. Business-

to-consumer e-commerce is enabling customers to have an increasing influence on products created, how products are customised, and how services are delivered. E-commerce offers customers convenient shopping methods for products, information and services, electronic banking, and personal finance management. It is making it easier for consumers to find the desired products and services, match them more precisely to their requirements, and compare prices, (Vulkan, 2003). Several business models have been developed to support various customers' needs, among them are online portals, content providers, transaction brokers and community creators.

For business-to-business relations e-commerce facilitates the form of organisation where companies rely on suppliers and product distribution to respond more effectively to the changing market and customers demand and to achieve more efficient operation. This type of e-commerce relationships offers organisations the possibility to work in the direct contact with producers, giving more room for customization and control over business activities. This helps to reduce the costs significantly by removing 'middlemen' from the supply chain. Good examples of companies that employ this business model are Dell and Cisco, (Guttmann, 2003; Laudon & Traver, 2002).

Consequences that e-commerce brings for business-to-business relationships are eliminating inventory, and operational and distributional costs that indirectly provide customers with lower prices. E-commerce can help businesses to increase production flexibility by ensuring timely availability of components from suppliers, to improve quality of the products by increasing cooperation between buyers and sellers and reducing quality issues, to increase opportunities for collaborating with suppliers and distributors, and to create greater price transparency — the ability to see the actual prices on the market, (Laudon & Traver, 2002). In this way e-commerce responses to the customer demand of lower prices and greater convenience.

1.1.1 E-commerce and electronic payment systems

The most popular definition of e-commerce is based on the *online* perspective of the conducted business. E-commerce provides the capability of buying and selling products, information and services on the Internet and other online environments. As for any trading activity, the issue of safe and reliable money exchange between transacting parties is essential. In an e-commerce environment, payments take the form of money exchange in an electronic form, and are therefore called *electronic payments*. Electronic payments are an integral part of e-commerce and are one of its most critical as-

pects. Generally defined, electronic payment is a form of a financial exchange that takes place between the buyer and seller facilitated by means of electronic communications. An e-commerce electronic payment is a financial exchange that takes place in an online environment, (Kalakota & Whinston, 1997).

Electronic payment systems (EPSs) are summoned to facilitate the most important action after the customer's decision to pay for a product or service – to deliver payments from customers to vendors in a most effective, efficient and problem-free way. The role of e-commerce electronic payment systems is pivotal for future of e-commerce, whose further growth depends on the timely development of EPSs.

The development of new types of e-commerce purchasing relationships and business models has created the need for new ways of money exchange and new EPSs. For instance, online auctions, (Ribbers & Heck, 2004), has spurred the necessity for person-to-person payment systems to allow online money exchange between individuals. Certain types of information products and services require small payments and micropayments. Businesses would like to sell information content that costs very little, accumulating revenues with high turnover. E-commerce EPSs can be designed for selling specific types of products, for example for trading copyrighted online content, such as music. Another unforeseen earlier requirement is conducting e-commerce using wireless mobile devices, such as mobile phones or personal digital assistants (PDA). The need for paying with mobile devices has urged the development of payment systems for mobile electronic commerce, (Laudon & Traver, 2002). In addition, e-commerce provides the possibility to enhance current payment systems or substitute them with online variants.

The need for online payments was first addressed by using extant payment methods of the offline world for online payments. For example credit cards, originally intended as an offline credit instrument, have become the major payment instrument for e-commerce. As e-commerce and online purchasing grows, the weaknesses of credit and debit cards, and cheques are becoming more apparent. These limitations are discussed in section 1.1.2. The lack of the fit-for purpose payment mechanisms and infrastructure is one of the main restricting factors that hold back the growth and evolution of e-commerce, (Guttmann, 2003; Laudon & Traver, 2002; O'Mahony, Peirce, & Tewari, 1997).

1.1.2 Limitations of traditional payment systems in the context of online payments

Three factors are stimulating the development of electronic payment systems: reduced operational and payments processing costs, growing online commerce and decreasing the costs of technology, (Kalakota & Whinston, 1997). Reduction of costs is one of the major reasons for research and development of EPSs. The central impetus for e-commerce and e-business is to provide a more efficient service, primarily in terms of costs. In this light, paying online with traditional payment systems such as credit cards is rather paradoxical, given that credit cards are one of the most expensive of all available mainstream payment means for both end consumers and merchants, defeated perhaps only by paper checks, (Lietaer, 2002; Laudon & Traver, 2002).

Several limitations of traditional payment systems in the context of e-commerce can be outlined. Existing payment systems, such as credit cards, are inadequate for retail customer digital business from the following viewpoints:

Lack of usability. Existing payment systems for the Internet require from the end user to provide a large amount of information, or make payments using complex elaborated web site interfaces. E.g. credit card payments via a web site are not the easiest way to pay, as these require entering extensive amounts of personal data and contact details in a web form, (Kalakota & Whinston, 1997).

Lack of security. Existing payment systems for the Internet are an easy target for stealing money and personal information. Customers have to provide credit card or payment account details and other personal information online. This data is sometimes transmitted in an un-secured way, (Kalakota & Whinston, 1997). In practice this happens even in spite of introduction of secure transactions mechanisms, such as Secured Socket Layer. Providing these details by mail or over the telephone also entails security risks, (Guttmann, 2003; Laudon & Traver, 2002).

Lack of trust. Users tend not to trust existing systems with the long history of fraud, misuse or low reliability, as well as novel systems without established positive reputation. In the present situation, money loss by customers is quite possible when using existing payment systems, such as credit cards, for Internet payments. Potential customers often mention this risk as the key reason why they do not trust a payment service and therefore do not make Internet purchases, (Lietaer, 2002).

Lack of applicability. Not all web sites support a particular payment method, thus limiting customers' ability to pay. Credit cards work only with merchants who have signed-up to the services of the corresponding credit card company, and do not support direct business-to-business or interpersonal payments, (Kalakota & Whinston, 1997).

Lack of eligibility. Not every potential customer with money and intention to pay can make use of certain payment methods. Not all potential buyers can obtain credit cards due to credit history limitations, low income or other reasons, (ibid).

Lack of efficiency. Some payments over the Internet can be too small to be handled by existing payment systems, because of overheads included in the processing of payments and transaction. Credit cards are too expensive for effecting small payments and are unsuited for small transactions. The minimum fixed fee charged to the retailer for processing a transaction could even surpass the value of the goods sold, (Guttmann, 2003).

High usage costs for customers and merchants. Existing payment systems use a rather expensive infrastructure to facilitate the payment process. Credit cards are very expensive for end users, not in the least because of the enormous and growing size of fraud, which amounts to billions dollars per year. This loss is invisibly re-financed by users by the higher costs of credit card services. In addition, credit card payments are still heavily paper-dependent. Most credit card bills are sent in a paper form to customers by post, and the bills are mostly settled by posting paper documents, like checks of giro payments, which makes the whole cycle rather expensive. As mentioned above, this means that resources employed in processing of credit cards transactions render them rather ineffective for small payments, because the high overhead of credit cards, (Laudon & Traver, 2002; Guttmann, 2003).

In online credit card payments credit cards are not physically available for inspection by the payee, (this situation is referred as 'card not present'). This imposes higher charges for merchants, because the chance of fraud is higher; see section 2.1.3 for more discussion. Credit cards have low finality of payments because users can refute or repudiate credit cards payments in certain situations. Moreover, financial regulations in certain countries, e.g. in the USA and the UK, place the risks of repudiation, fraud, or non-payment largely on the merchant and issuing banks, (Laudon & Traver, 2002; APACS, 2002). These issues make credit cards less attractive to merchants. Certain authentication schemes, e.g. Verified by Visa

and SecureCode from MasterCard allow to shit fraud liability from merchant to credit cards issuing banks, and can ease this burden for merchants, (see www.verifiedbyvisa.com and www.mastercard.com). However, end users can found themselves paying more for the cards issued by the banks to refinance bank's losses due to fraud.

There are more concerns related to the credit card use in online e-commerce that are responsible for reluctant users acceptance of credit cards and e-commerce. According to the report published by marketing research firm IDC, (Asmussen, Raschke, & Arend, 2002), almost half of European users of the Internet do not buy goods online because they either do not trust the Web merchants or fear their credit card details will not be secure. According to analysts, total credit card fraud rose to $4 billion in 2002 (i.e. $2 for every card issued). Industry estimates that the amount of online credit card fraud could be in the $500 million range, (Laudon & Traver, 2002).

Authorities believe that hackers have stolen more than one million credit card numbers from E-commerce sites. It would not be a surprise that many customers use their credit cards with reservations. A survey by Visa of 15 Banks from 12 EU countries in 2002 found that online credit card payments account for nearly half of all complaints. More than one in five of these came from people who had not even shopped on the Internet, but were billed for online transactions, (Philippsohn & Thomas, 2003).

Privacy issues are also associated with the use of existing payment systems. There are cases when users' identities (i.e. personal data such as credit card numbers, names and addresses) were stolen when hackers break into websites' databases and obtain personal information of the customers. Fraudsters then attempt to use this information to open new credit and bank accounts using the stolen identity, (Philippsohn & Thomas, 2003). These and other issues with existing payment systems such as credit cards render them not very suitable for online payments.

1.1.3 The need for new payment systems designed for e-commerce

Despite that electronic commerce is a growing phenomenon, its future development is, to a large extent, hampered by the lack of appropriate payment systems. Since most of business-to-consumer payments over the Internet are performed currently via credit cards, an admittedly problematic payment medium due to costs, security and trust

problems, the need for new payment systems clearly emerges from the existing situation, (Lynch & Lundquist, 1996; Wayner, 1997; Laudon & Traver, 2002; Guttmann, 2003).

Research and development in Internet-based payments tried to resolve this situation by conjuring numerous online EPSs, a good proportion of which has been put to use. This was possible due to the stimulating factors listed above, and in the first place due to the availability and reduced costs of the enabling technology. However, the new payment systems, purposely crafted for the Internet, also could not avoid their own share of problems. This has led to the reluctant use of new online electronic payment systems, i.e. resulted in low *user acceptance* of newly introduced payment systems by customers, (see section 1.2).

User acceptance of electronic payment systems

At this stage the situation with the development of online EPSs is far from ideal. A survey on electronic money developments by the Bank for International Settlement reports a rather low level of EPSs use, even in the most advanced countries, (BIS, 2000).

According to the European Central Bank, the proportion of online payments among cashless payment instruments in the European Union is rather low. The report admits that although there has been a lot of discussion on the use of EPSs and their importance "it is still not a widely used medium", (ECB, 2001). The lack of customer demand, the diversity of technological standards and the lack of support by financial institutions are mentioned among the reasons preventing the development of electronic payment systems, (ECB, 2003).

Some experts estimate that about 85% of all Internet transactions are done with credit cards that were not originally designed for the Internet, (Philippsohn & Thomas, 2003). According to a survey by marketing research firm Jupiter Research, credit cards are still the dominant payment method for online purchases, accounting up to 95% of online transactions in the United States, (Jupiter Media Metrix, 2000). This demonstrates still low user acceptance of alternative electronic payment systems, designed specifically for e-commerce.

1.2 User acceptance: understanding and issues

End user acceptance of such sensitive technology as money-circulating payment systems is the critical key aspect of the whole path of payment systems' establishment. Without such acceptance no technology can successfully exist on the market, and payment systems are not an exception. According to Dillon & Morris (1996) user acceptance is "the demonstrable willingness within a user group to employ information technology for the tasks it is designed to support".

This definition can be enhanced with the understanding that the user perception of information technology (IT) can be influenced by objective characteristics of technology, as well as by human factors and interaction with other users and related parties. For example, the social information processing model (SIPM), (Salancik & Pfeffer, 1978), suggests that attitudes towards technology are influenced by opinions, information, and behaviour of others.

User acceptance is a pivotal factor determining the success or failure of any information system project, (Davis, 1993). Many studies on information technology report that user attitudes and human factors are important aspects affecting the success of an information system, (Davis, 1989, Burkhardt, 1994, Rice & Adyn, 1991). The arguments in section 1.1 and in the following paragraphs suggest that this is the case also with EPSs.

Besides SIPM, a well-known approach to explaining and modelling user acceptance is the Technology Acceptance Model (TAM), (Davis, 1989). TAM suggests that users formulate attitudes toward the technology that depends on whether they perceive the IT to be useful and easy to use.

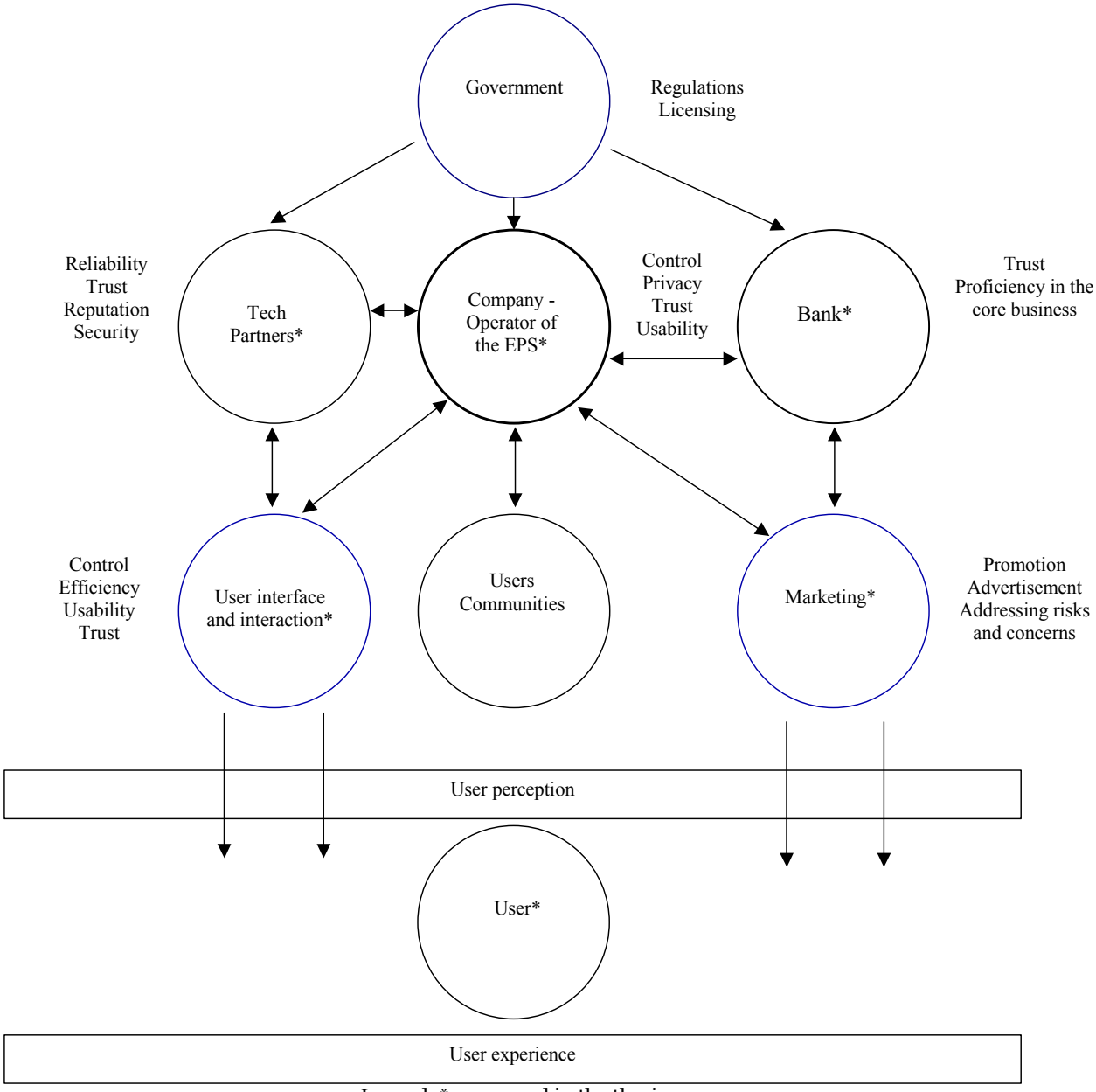
However, TAM does not take into account other factors that may be critical to user acceptance or rejection of such specific technology as EPSs, such as security, trust, privacy and involved risks. Extending the SIPM assumption, user acceptance of online EPSs could be affected by a number of factors and parties, creating a broader sense of the social context of EPSs in the Internet environment. User experience with an EPS can be influenced or manipulated by various aspects, such as marketing, publicity, the reputation of the bank behind the system, trust towards the company operating the system and technology behind the system, and convenience of the user interface, see also Guttmann (2003), Kalakota & Whinston (1997), Egger (2003).

Figure 1.1 attempts to illustrate the social context in which parties and factors could possibly influence user perception and experience with electronic payment systems. These parties and factors should be taken into consideration when exploring issues of user acceptance of online EPSs. They are either required for a successful operation of a payment system (banks), its promotion (marketing organisations), or monitor and regulate its operation (government). For example, the company operating the payment service will have to address users' concerns about security, privacy and trust. Users can be influenced in their experience by other parties than the operator itself, e.g. the bank or financial institution that facilitates the payment transactions, see Figure 1.1. Customers can be influenced by the user interface, or by other parties involved in the payment service, such as technical partners. Since e-commerce EPSs operate in the Internet environment, the reputation and impression of the system can be easily communicated to other users via online communities, creating yet another social impact on the system. Therefore, *social influences*, e.g. opinions and behaviour of other users, like family and friends, and reputation of banks and the parties involved, should be taken into account for user acceptance of EPSs. This argument can be supported by above-mentioned SIPM, (Salancik & Pfeffer, 1978).

Issues such as trust, usability, applicability, security, and convertibility are extremely important because they can influence subsequent decisions of people whether to use a payment system or not.

There are several obstacles to user acceptance of EPSs: developers not only have to sell the service to potential users, they also have to convince the users to entrust their money to a third party institution, to rely on the payment system in their business and personal finance, and to use it frequently for convenience, reliability, specific applications, services and for a variety of other reasons. To achieve this high standard of user acceptance, the creators of a payment system should bear in mind *user-related factors* from the very beginning of the conception of the payment system. Designing for user acceptance of online electronic payment systems is thus the main issue put forward by research described in this thesis.

An open challenge remains for designers and developers of novel Internet-based payment systems to meet user expectations, requirements, preferences and needs in design and operation of the systems. Resolving these issues is critical for the development and operation of new payment systems and future growth of e-commerce.



Legend. * — covered in the thesis.

Figure 1.1 Factors influencing user perception of online electronic payment systems.

1.2.1 User factors in payment technology

The importance of user-related factors can be demonstrated in the example of the notorious problem of security of information systems. There are thousands of security mechanisms, matched with a growing number of hacks and security breaches, (Flynn, 2001, p. 61).

However, the nature of security issues is changing with the constant improvement of information technology. While security technology is becoming increasingly sophisticated and tamper-proof, experts in information security admit that user factors are the most important issues for security problems. The vast majority of all security issues in IT environments is caused or assisted by users inside organisations, rather than hackers and other outsiders. Security experts know many stories about people exchanging their passwords, or IT managers attaching notes with logins and passwords to their monitors, or about hackers finding these notes in the trash. To avoid this kind of mistakes, experts are talking about enforcing security policies in organisations, to be able to address user-related factors in security, (Flynn, 2001). Therefore, security practices have embraced user-related factors. This example helps to illustrate the importance of user-related factors in the design and operation of information systems.

The following example illustrates a failure of a payment system due to neglecting to focus on user and market needs. The Chipknip ™ and Chipper ™ smart card payment technologies, (Nannery, 1998), were introduced in the Netherlands in early 90s. Both systems were intended to provide a way of paying small amounts in everyday transactions, which people would normally pay with cash. However, these two systems competed with each other for some time, being incompatible, so customers could not pay with the competitor's card at certain shops, (BIS, 2001). Eventually, this created problems of interoperability and limited the user base for both systems.

Another obstacle was that the card readers were installed in shops where people already had another method of payment – debit cards, which worked very effectively and efficiently and which were used by most people for all kinds of payments. In a way, Chipknip and Chipper duplicated the functions and applications of debit cards. On the other hand, the real need for Chipknip and Chipper for small payments at parking lots, vending, and public transport tickets machines was not met. A serious situation arose regarding the high costs of accepting Chipknip for merchants. As the result, the union of Small and Medium Enterprises in the Netherlands threatened to boycott Chipknip, (Het Financieele Dagblad, 2001). In this case, an important factor

stimulating the development of EPSs was not met, namely the reduced operational and processing costs. Despite of a certain potential for uses acceptance of e-purse technology (Van Hove, 2004), this situation is changing slowly.

All these issues led to a low acceptance of Chipper and Chipknip technologies. Chipper International decided to stop operations and support of Chipper in the Dutch market, (Libbenga, 2001; BIS, 2001); Chipper has fused with Chipknip, and while some issues have been addressed, the expected applications for this smart-card technology are yet to come.

The example above helps to illustrate the complexity of human and marketing factors in the context of payment systems and their crucial influence on the eventual success of a payment system. Therefore, for successful design of electronic payment systems from the user perspective it is important to find out what user-related factors and systems' aspects have the most direct impact on user acceptance and which of them can cause problems when neglected in design.

1.3 Research objectives

There are several factors that can contribute to user acceptance of an EPS: innovative and reliable technology, effective business practices, smart marketing and promotion, good usability, and a carefully carried out interaction design.

The previous sections illustrate the complex issues that surround online EPSs. They suggest that problems with user factors in the context of EPSs and their crucial influence on the eventual success of EPSs have the design, marketing, and business organisation nature.

This research has been pursuing an interesting and daring task: to explore issues of design and user acceptance of e-commerce EPSs, and to suggest how to design EPSs in such a manner that their acceptance by end users will be maximised, and the number of joined users will justify the system's rollout and its further development. Without ignoring the importance of marketing, business and technological factors, this research focuses on user acceptance and user-centered design of e-commerce EPSs.

The methodology of this research is strongly inclined to human-computer interaction and user-centered interaction design. Human-Computer Interaction (HCI) is a disci-

pline concerned with the design, evaluation and implementation of interactive computing systems for human use, and with the study of major phenomena surrounding them, (Hewett et al., 1992). For discussions of HCI as a scientific discipline see Long & Dowell (1989).

The issue of user acceptance of e-commerce EPSs could equally concern marketing research and user-centered design. The differences between marketing research and user-centered design are discussed extensively in Siegel & Dray (2001), Table 1.1. The goals of this research conform with the objectives of user-centered design to deliver "usage satisfaction by determining how to build identified product to facilitate user's task goals", Table 1.1, Siegel & Dray (2001). Although certain practices of marketing research are still adopted in the research activities reported hereby, (despite of the distinctions of Table 1.1), the objectives of this research is to assist in the creation and improvement of e-commerce EPSs based on user-centred approach and human-computer interaction, rather than suggesting how to position, market, and promote EPSs as commercial products.

This research seeks not only design solutions, but also how to provide a scientific foundation for such solutions. I.e. it is investigated what kind of *validated design knowledge* shall be communicated to designers and developers of EPSs so that users will be willing to use the newly introduced EPSs in an e-commerce environment for payments and personal finance.

1.4 Research scope

Payment systems can be classified from a business relations viewpoint on various types of e-commerce as described in Figure 1.3. The scope of payment systems and payment tasks is defined based on business relationships model in Figure 1.2, and the classification framework of electronic payment systems, presented in Chapter 2.

Table 1.1 Differences in approach of marketing research and user-centered design. Adapted from Siegel & Dray, (2001, p. 24).

Dimension	Marketing Research	User-Centered Design
Purpose	Strategic: to guide product mix, positioning.	Tactical: to guide product realization via design input.
Goal	Build product attractiveness by deciding what products and product features to build to meet perceived needs; develop concise messages and clear global strategies that will quickly influence mass perceptions, at corporate level and product level, to differentiate products from competitors.	Ensure continuing usage satisfaction by determining how to build identified product to facilitate user's task goals.
Who acts on input	Executives, brand and advertising professionals, product managers.	Users, Designers, Engineers, IT developers
Most interested in	Broad patterns of purchasing behaviour, and attitudinal variables that influence it. Based on trends and significant attitudinal differences between groups.	Specific details of design that influence reactions to structure, in-depth analysis of individual differences in performance, cognitive processes, problem-solving approaches, confusions. More interest in idiosyncratic responses.
Phenomena measured	Subjective: perceptions, opinions, expectations, feelings, and preferences, attention, affective reactions as clues to product attractiveness and likelihood of buying.	Objective: Task flows and task performance, usage behaviour, cognitive processes, affective reactions such as confusion or frustration as clues to cognitive processes and performance problems.
Type of data	Survey and self-report, often retrospective; behavioural measures related to purchasing. Preferences, attention, and purchasing.	Real-time behavioural data regarding usage and task performance. Self-report (diary records, thinking aloud) construed only as an indirect clue to inferred cognitive process.
Sampling	Large samples selected to reflect the demographics of purchasers.	Small samples selected to reflect people who are similar to targets in terms of technology usage.
Data analysis	Statistics usually required, often quite sophisticated analyses.	Statistics rarely done, other than descriptive statistics on completion rate, error frequency.

1.4.1 The role of electronic payments in customer e-commerce activities

The process of paying is an essential part of customers' online buying activities. These activities are well described by the Consumer Mercantile Activities Model, (Kalakota & Whinston, 1997). The model comprises prepurchase interaction, purchase consumma-

tion and postpurchase interaction phases. The payment activity takes place within the purchase consummation phase, Figure 1.2.

"The purchase consummation phase specifies the flow of information and documents associated with purchasing and negotiating with merchants for suitable terms, such as price, availability, and delivery dates; and electronic payment mechanisms that integrate payment into the purchasing process", (Kalakota & Whinston, 1997).

The buyer arrives to payment activities after identifying products of services to be purchased. The buyer and seller conduct then a *mercantile transaction*. In a mercantile transaction the buyer and the seller exchange information followed by the necessary payment. The payment methods they use should be mutually negotiated and agreed on (ibid). Therefore, in order to conduct a successful e-commerce mercantile transaction the buyer should at least be willing to use the payment method offered by merchants. From this viewpoint, user acceptance of e-commerce EPSs is critical for the completion of the purchase consummation phase and the whole purchasing process. It can be therefore observed that the payment process and the user involvement in it are highly important for e-commerce activities.

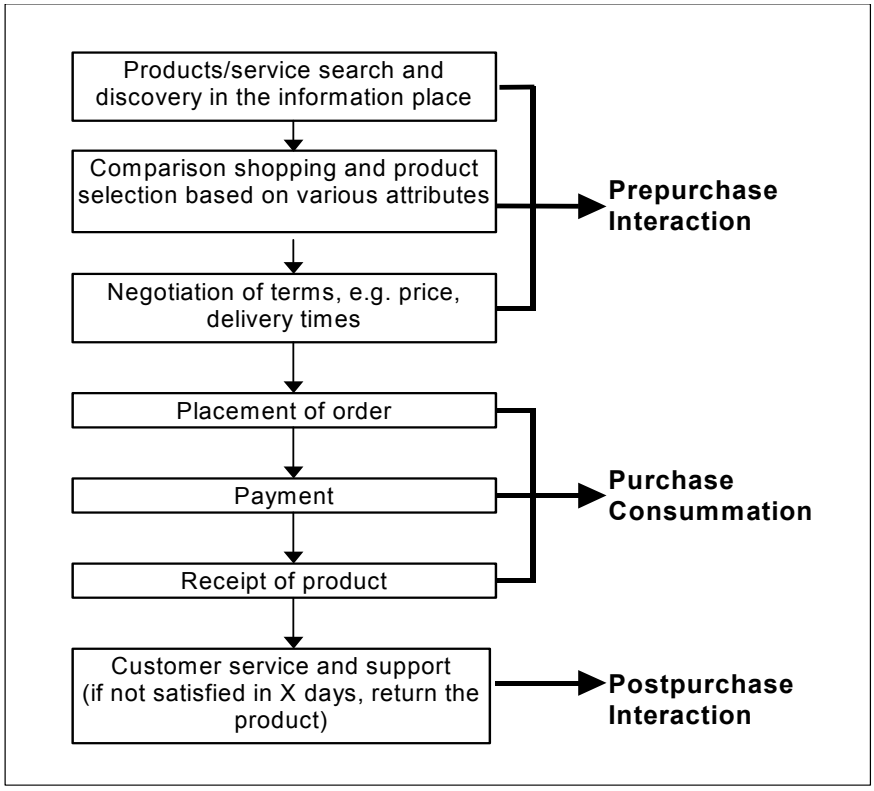


Figure 1.2 Consumer Mercantile Activities Model, Kalakota and Whinston (1997).

Scope of payment systems

Business-to-consumer Payment Systems

This research is focused on user acceptance of new payment systems in consumer e-commerce environments. The main focus of the presented work is therefore Business-to-Consumer e-commerce EPSs, which are designed with the main purpose to facilitate payments for consumer e-commerce. Taking into account the B2B systems would have made the scope too broad to handle within this research.

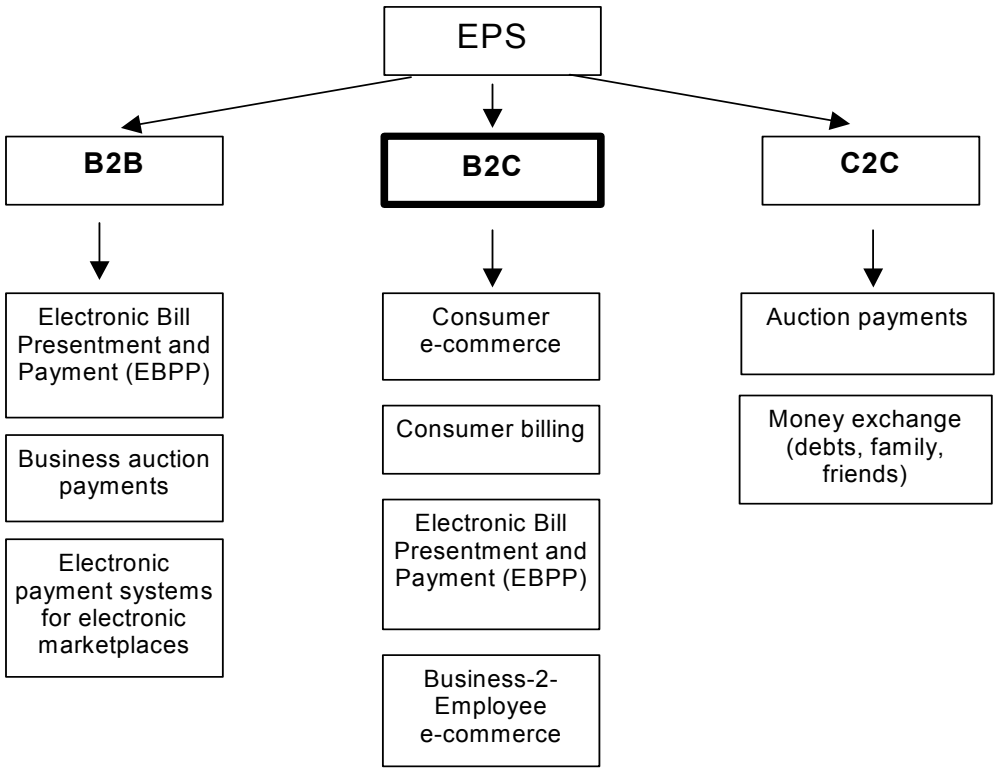


Figure 1.3 Electronic payments for different types of e-commerce.

Payment Systems designed for the Web

Currently, consumer e-commerce is done mainly via the WWW (Web) service of the Internet. The market for conducting e-commerce payments via wireless PDAs, mobile phones and other Internet services is still under development, (Bohle, 2001a), and therefore does not have a wide user basis and usage experience. Thus, in the scope are Web-oriented online e-commerce EPSs and Web e-commerce applications.

Scope of payment tasks

Because the scope of the defined business relations is Business-to-Consumer, the *payment tasks* in the focus of this thesis are related to *consumer* e-commerce and trade of goods and services. In these tasks there should be at least one 1) business party involved and 2) one physical person, who is conducting purchasing activities in an e-commerce environment.

Scope of target activities

These activities include those that are related to buying goods and services, and essentially represent consumer e-commerce. The scope of these activities is embracing a significant and, arguably, the most important part of the consumer e-commerce represented by B2C relations.

- Purchasing goods: tangible, require shipping, intermediated (by shipping companies).
- Purchasing information and software: intangible, immediate, not intermediated (by shipping companies).
- Purchasing services: intangible/tangible, not always immediate, can be intermediated (by service companies).

The following activities are therefore excluded from the scope because they are not in line with the defined scope of electronic payment systems, namely B2C consumer e-commerce.

- Consumer-to-Consumer (C2C) money payments and exchange. C2C payments do not belong to B2C e-commerce, (Figure 1.3), e.g. personal auctions payments, debt settlement.
- Specific payment applications, for instance, gambling or adult-content sites. In this context the sites place specific requirements on B2C relations and user-related factors, e.g. on privacy.

Related activities

Additional activities that have to be explored are the influence of pre- and post-purchase interaction phases, according to Kalakota and Winston (1997) on the user experience with a payment system on the whole. It is very likely that correct introduction, application and follow up of payment products and services in retail e-commerce

are important for user acceptance of EPSs, and therefore the pre- and post-purchase interaction phases cannot be reasonably disregarded when investigating the payment process. The user experience within these phases could affect their decision as to whether to use the e-commerce service at all, without even arriving at the payment process itself.

Amount of money

The minimum amount of money within the scope was chosen to be above €2. This means excluding small and micropayments. The nature of payment tasks in case of micropayments is different from higher amounts. For instance, users may wish to automate this kind of payments to avoid the need to authorize a payment of €0.01 every time, while with bigger amounts they are likely to have control over each transaction. Furthermore, different researches show that at this moment there is little market for services that support small and micropayments, (Bohle, 2001b). In the focus are therefore small to medium sized payments, e.g. from €2 to €1,000.

The upper payment limit is set to €1,000 to indicate that highest amount within the scope of this research. The suggested range of payment amounts is typical for the current status of the domain and is similar to range of payments with existing offline EPSs, like credit, debit and smart cards, (Lelieveldt, 2001; Bohle, 2001a). Larger payments can be expected to raise different user acceptance issues, because of more user attention to risks, security, efficiency and other aspects of transactions with such amounts, (Humphrey, 1995).

1.4.2 Approach and methodology

This research employs practices of the multidisciplinary scientific field of Human-Computer Interaction in order to research issues of user acceptance and user-related factors in online e-commerce electronic payment systems.

Specifics of HCI research

The nature of Human-Computer Interaction is such that it has to employ various scientific, research and design disciplines and cross borders between them for successful research. HCI is different from other disciplines in that it studies interaction between

people and artificially created artefacts, and not an independent natural phenomenon, like in other disciplines.

This complex nature of HCI and its research goals compel researchers to adopt both inductive and deductive approaches to science, as described in Mackay & Fayard (1997). In the deductive approach the purpose is to generate a set of hypothesis that can explain real world phenomena. The scientist proposes a theory about a phenomenon, and formulates a hypothesis to be tested in an empirical research. In order to verify the hypothesis, an experiment is conducted, and with the revision of its results the theory is re-examined and an updated hypothesis is created. This approach is employed by the experimental study of this thesis.

The inductive model aims to construct the most precise *description* of the real world, as opposed to explanation. The scientist observes phenomena in the real world without having a preconception or theory of what they are looking for. Then the scientist attempts to create a model of the world that explains the phenomena. By returning to the real world the model can be validated and changed if there are contradictions between the model and the studied phenomena. The qualitative study in this thesis employ this approach for requirements elicitation and creation of the design recommendations.

The research process applied in this thesis, aimed to gain validated design knowledge, can be described as an iterative circular or spiral movement. This process is best described by Figure 1.4, adapted from the work of Rauterberg (2000). This approach asserts to combine "analytical strength of empirical validation methods (e.g., observation, experiment, inquiry, etc.) with the synthetic strength of system design". This triangle structure conceptualizes the three most important components of HCI research: "(1) the collection of 'design relevant knowledge', (2) the 'interactive system' in different possible representation forms, and (3) the several possibilities to represent a 'user' for (empirical) validation", (ibid). The following sections describe how using diverse research activities helped to combine these components in the research reported in this thesis.

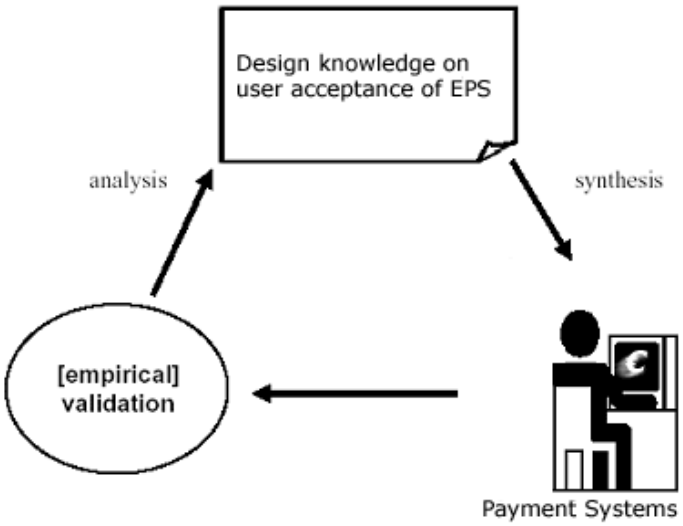


Figure 1.4 Triangle structure for a research approach with a rigorous validation component. Adapted from Rauterberg (2000).

Outline of the thesis

The diagram in Figure 1.5 illustrates a combination of the research and design activities of this thesis. These activities included acquiring design knowledge on e-commerce EPSs, applying the knowledge to a commercial payment system designed by an industrial party, and empirical validation of the design knowledge.

Chapter 2 presents a survey of literature on EPSs, which was necessary for understanding EPSs. The outcome this survey is a classification and a set of characteristics of EPSs.

The importance of the characteristics of EPSs had to be confirmed with potential users of EPSs. Chapter 3 describes an investigation into the importance of the characteristics of EPSs to end users by means of a survey of consumer attitudes towards EPSs. The user survey helped to identify what characteristics should be given more attention in the design of EPSs. However, the knowledge about the importance of the characteristics did not inform how they should be realised in design of EPSs.

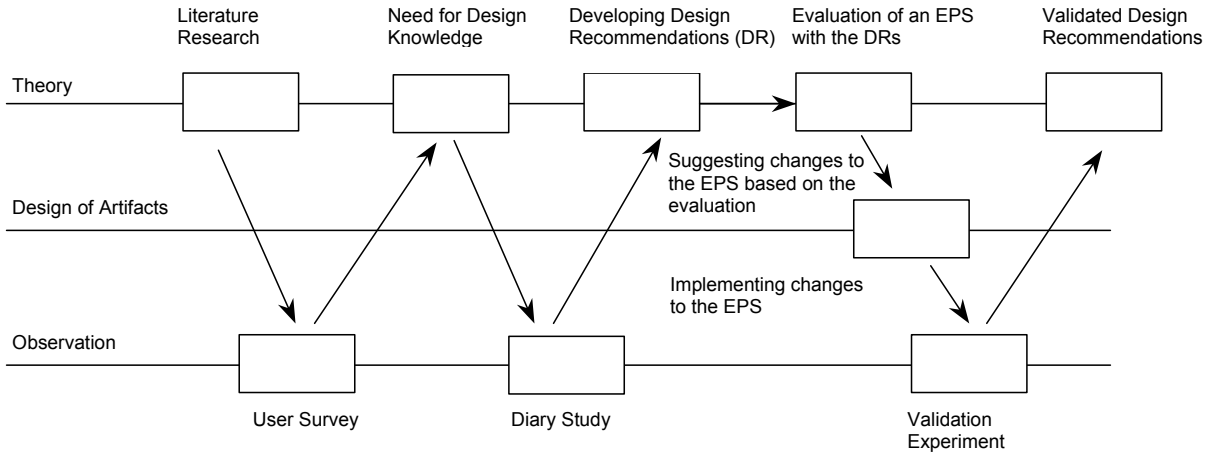


Figure 1.5 Diagram of the activities of this thesis. Developing design recommendations using various research and design methodologies.

To acquire a deeper understanding of these issues, a qualitative research in the form of a diary study was conducted, Chapter 4. The diary study aimed to understand how EPSs are experienced and perceived by users in the context of actual use and how EPSs can be designed to meet users' needs. As the outcome of the diary study, implications for design of Internet-based payment systems have been derived and formulated as design recommendations.

To ensure that the application of the design recommendations benefits user acceptance of EPSs, an experimental study was conducted, that is described in Chapter 5. This study helped to substantiate the validity of a subset of the design recommendations. It was hoped to find the ideal situation where it is possible to apply the hypothesised design knowledge to a real-life system, rather than testing them in the laboratory, in order to achieve high realism of the results. Due to the participation of industrial parties, this situation has become available. The experimental study involved two parts: 1) a real-life EPS was redesigned in accordance with the proposed DRs, 2) an experimental comparison of the redesigned system with the old one has indicated improvements of user attitudes in several aspects, thus demonstrating the validity of the design recommendations.

Chapter 6 describes the contribution and discusses possible validity threats and limitations of this thesis.

Triangulation of research approaches

In this thesis a combination of many research activities of both inductive and deductive models was used: literature research, a user survey, qualitative research in a form of a diary study, and empirical research in the form of a laboratory experiment. More than one research approach is employed to address the same question: how to design for user acceptance of e-commerce EPSs.

Triangulation, which can be defined as using more than one research approach to address a research question, (Mackay & Fayard, 1997), is the proper way to achieve valid results in such specific environments as money-transacting electronic payment system for e-commerce. Mackay et al. (1997) argue that triangulation across scientific and design disciplines is likely to be beneficial in the multidisciplinary field of HCI.

In addition, Gray & Salzman (1998) suggest another type of triangulation, that is replicating an experiment with a different design approach (e.g. interface, interaction design) greatly increases construct validity and generality of the results. This type of triangulation applied in the thesis can be referred to a redesign of a payment system into a new version in accordance with the design recommendations and evaluating the both systems' version in an empirical study, described in Chapter 5.

Yet another type of triangulation is examining different form of *data representation*, collected within the same study. This approach was used in the diary study (chapter 4), combining users' diaries with qualitative interview techniques. Thus, addressing individual problems with multiple research and design methods, as well as different types of data, should produce more generalisable, valid and useful results.

Mackay & Fayard (1997) mention in addition, that individual researchers cannot embrace all disciplines involved in triangulation research, accrediting triangulation research to scientific laboratories and to bigger research programs. Therefore, the combination of several disciplines and data collection methods employed in this thesis adds to the validity of the results and makes this research quite distinctive.

Chapter 2

Classification and characteristics of electronic payment systems

2.1 Classification of payment systems

2.1.1 Introduction

This chapter presents a framework for classification and characterising of electronic systems that facilitate paying in an e-commerce environment. This framework is an attempt to describe and to relate the wide variety of the payment systems, with more than 150 payment mechanisms invented worldwide. This chapter also presents a survey of literature on EPSs, which has been a necessary step for understanding payment systems. The outcome of this phase of the research is a classification and characterisation of electronic payment systems.

2.1.2 Primary classification of payment systems

The principal classification of EPSs is based on the form of money representation and the principle of money transfer. Existing payment systems can be divided into two groups: electronic cash mechanisms (or electronic currency) and credit-debit systems, (Medvinsky & Neuman, 1993).

Electronic cash resembles conventional cash, when parties exchange electronic tokens that represent value, just as banknotes and coins determine the nominal value of conventional cash money. The *credit-debit* approach in the context of electronic payments means that money is represented by records in bank accounts, and this information is electronically transferred between parties over computer networks.

Another terminological approach offered by Wayner (1997), based on the type of information that is exchanged, distinguishes between '*account-based*' and '*token-based*' systems, which, respectively, corresponds to credit-debit systems and electronic cash in the definition of Medvinsky and Neuman. A similar distinction is found in Camp et al. (1995), who distinguish between *notational* and *token* forms of money. A different view on classification of EPSs is offered in Asokan et al. (1997), where payment mechanisms are classified based on the temporal sequence of money flows between the payer and receiver of the payments. Various attempts of classification of payment systems are also reported in Kuttner and McAndrews (2001), and Schreft (2002).

These references are aggregated into the classification of electronic payment systems, illustrated in Figure 2.1, which was first reported in Abrazhevich (2001b). The figure illustrates the further classification of EPSs, described in the following sections. It provides examples of EPSs in each subcategory; some of these systems are described further in the text. The figure illustrates if the systems are only theoretical developments, that were only tested as limited pilots, and that have never been implemented for the commercial use. Payment mediation services that aggregate various EPSs in one payment infrastructure are described in section 2.1.5.

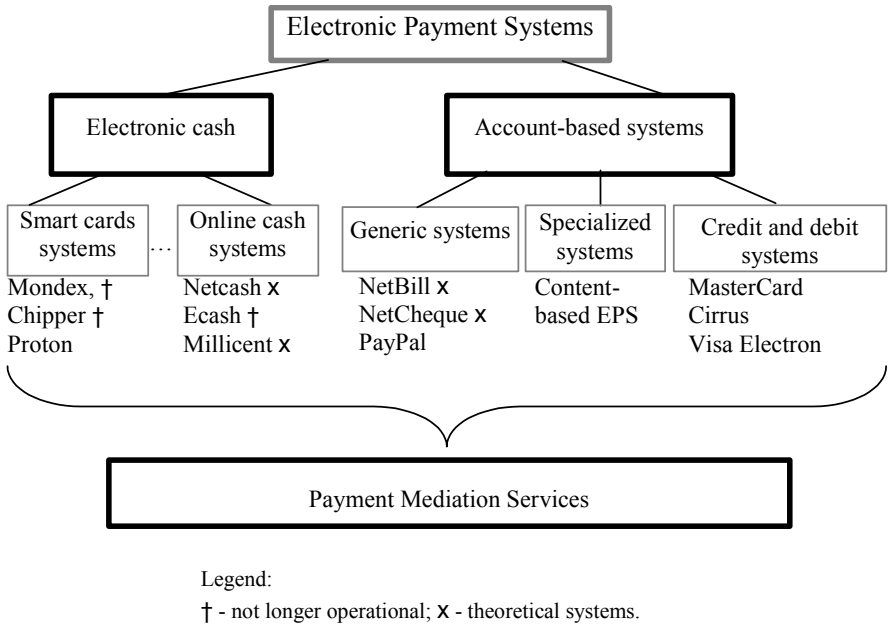


Figure 2.1 Classification of electronic payment systems

2.1.3 Further classification of account-based systems

In the group of account-based systems, one can distinguish between 1) generic online EPSs that use simple account-based model for serving Internet payments, 2) systems that use the debit and credit cards model, and 3) specialized payment systems that, for instance, were designed for trading content online such as music. Some researchers consider credit cards systems as a separate group of payment models, (Medvinsky and Neuman, 1993), others consider them to be a variant of the credit-debit type. This classification adopts the latter distinction.

The basic principle of account-based systems is that the exchange of money between accounts is maintained by a payment service provider. Users can authorize charges against their EPS accounts, as they would do with usual bank accounts, though the ways of authorization are different for various systems. With the debit approach, the customer maintains a positive balance of the account and money is subtracted when a debit transaction is performed. With the credit approach, charges are posted against the customer's account and the customer is billed for this amount later or subsequently pays the balance of the account to the payment service.

One of the most widely used systems for electronic payments is the debit card, which as the name suggest, is a clear example of a debit system, (Evans & Schmalensee, 1999). Debit cards combine the service of Automatic Teller Machines (ATM) cards and cheques. When customers pay with a debit card, the money is automatically deducted from their checking bank account. In contrast with the credit cards, the spent money comes from the bank account directly. Many banks issue a combined ATM/debit card that looks like a credit card and can be used in places where credit cards are accepted. In this case, when users pay with a debit card, the payment will still be processed as a debit transaction.

Other payment mechanisms that use the credit-debit model are Yahoo PayDirect, PayPal.com, and theoretical payment projects like NetBill (Sirbu and Tygar, 1995), and NetCheque (Medvinsky and Neuman, 1993). A special group of account-based instruments that are currently in wide use are credit card systems. A great part of trade on the Internet is done using credit cards and these payment systems should not be overlooked. The biggest advantage of this approach is that the customers, who have already received credit cards offline, can use them directly for online payments. This also results in high scalability, as no additional installations are necessary. Credit cards provide a large customer base for merchants who accept them, thus their applicability is quite high.

There are critical security issues associated with the use of credit cards in an online environment. When using credit cards over open networks, encryption mechanisms, such as widely used Secure Socket Lauer (SSL), in principle can prevent a hacker or eavesdropper from intercepting the customer's credit card number. There are some schemes that even hide card numbers from the merchant, providing protection against intercepting the card details from merchant databases or against fraud by the merchant. Nevertheless, these incidents happen regularly (Caunter, 2001; IFCC, 2003; Wales, 2003).

It is important to note, however, that without some form of customer registration with a payment service or substantial proofs of identity, credit cards can be very risky to pay with and can be easily abused. Even encrypted Internet credit card transactions do not include the owner’s signature, and anyone with knowledge of the customer's credit card number and expiration date can create a payment order. An important aspect of credit card payments in the online world is referred to as *card-not-present* (CNP) transactions. CNP transactions are those where neither the card, nor its holder are present at the point of sale, e.g. in orders by mail, telephone, fax or the Internet. The

buyer does not have to demonstrate the physical presence of the card, or the card and the buyer do not have to be co-located. This imposes issues with card validation, security and fraud.

CNP transactions are widely used in mail order/telephone order purchasing (MOTO) which also do not require co-location of buyer and seller. To secure transactions of this type, credit card companies ask for additional information, such as name, address, etc., that can be used to verify their identity, for instance, if the ordered goods should be mailed to the billing address associated with the credit card. Other information often required is the additional 3-4 digits code, printed on the back side of the card and not present in the credit card number. Merchants ask the customer to read this code from the card in a card-not-present order. The merchant then asks for verification during the authorization process. The issuer (or credit card processor) validates the code and relays the decision to decline or approve the transaction to the merchant. Nevertheless, the MOTO transactions incorporate limited protection against credit card fraud. Credit card CNP transactions could sometimes employ even less identity verification information.

Since no signature involved in CNP transactions, the buyers can opt out of any order, if they claim they did not agree with the purchase, (O'Mahony, Peirce, & Tewari, 1997). The charges for orders cancellation are borne by merchants in the form of the higher costs for processing of CNP transactions. In addition, merchants could be liable for the whole amount of the disputed order, (APACS, 2002). Furthermore, because online payments are administered as standard credit card charges, the costs are too high to make this method unsuitable for payments below €1 and hence inefficient. Credit card companies are constantly lowering the minimum amount that can be paid to enable small payments, but charges for merchants still remain high.

It should be also taken into account that cards are issued by banks and organisations, which after a screening, decide whether they can issue credit cards to certain customers. Customers with a low income, an imperfect credit history, might not be eligible for a credit card. This may restrict the customer base to a certain degree and limit user and merchant acceptance of credit cards as a payment method.

2.1.4 Further classification of electronic cash systems

Electronic cash is stored in a digital form and serves as a cash substitute for the Internet or other information systems. Electronic cash represents value in some form and can be spent with merchants, who deposit money in their own accounts or can spend it in other places. It can be represented by electronic 'bills' and 'coins', certificates, packets of data, or electronic tokens in one form or another. When using electronic cash systems, customers purchase electronic digital tokens from the issuing company using a conventional payment system, e.g. credit cards, electronic checks, or even paper currency (for example, via a reverse automatic teller machine which accepts cash, or when purchasing prepaid cards). Some of the systems allow converting electronic cash back into another form of money (Medvinsky and Neuman, 1993), which is very important for convertibility of the systems.

Another distinction amongst electronic cash systems is between those that use smart cards for the storage of tokens and those where tokens reside only on user's accounts and computer networks. The former are often called electronic purses (*e-purses)*, the latter are sometimes addressed as '*online cash'* or '*Web cash'*.

Examples of e-purse electronic cash systems are CAFE project, (Boly et al., 1994) and Mondex (Martin, 1994). Tokens in these systems exist and travel in the computer environment, for example, on a currency server or customers' hard disk. Mondex is a smart card payment system that was designed to enable person-to-person as well as Internet payments, (Van Hove, 1999, p. 141). The card can be used to make small payments, store personal and application-specific information, and serve as a telephone card. Web cash representatives are E-cash, E-gold, Millicent (Glassman & Manasse, 1995), PayWord and MicroMint (Rivest & Shamir, 1996), and NetCash system (Medvinsky and Neuman, 1993). It has to be noted that these systems are mostly theoretical work and have not been implemented on the market.

Systems that employ smart cards e.g., Chipknip, Chipper in the Netherlands, Proton in Belgium, and Visa Cash can be also placed in the category of electronic cash and also called e-purses, however, in representing money they hardly use tokens. In this case, the numerical data stored on the card is changed when a payment takes place. Judged by the principle of the operation and use they act like electronic purses. The value is stored on a card and if the card is lost, the money is gone, in a fashion similar to cash. It has to be noted that smart cards like Chipknip are not principally designed for Internet payments and are used mainly at point-of-sale terminals. There have been

nevertheless pilot tests of facilitating paying over the Internet with Belgian Proton smart card EPS, but the use of Proton on the Internet is now discontinued.

An important development towards standardisation of e-purses is establishing Common Electronic Purse Specifications with the goal to define requirements needed to implement a globally interoperable electronic purse program, while maintaining full accountability, (see www.cepsco.org). CEPS, which were made available in March of 1999, outline overall system security and certification. Being established by the key parties in electronic purse cards, and supported by organisations from over 30 countries, CEPS paved the way for the creation of an open global electronic purse standard. For cardholders it means that they will be able to use their electronic purse cards domestically and internationally with the knowledge that the card will be accepted wherever the acceptance mark is displayed. Visa Cash is an example of CEPS implementation, (see www.visa.com).

Prepaid card EPSs can be also included in the same category of electronic cash, because the principle of their work resembles the use of e-purses, such as Chipknip. Users can buy a prepaid card for a specified amount. Prepaid card systems are specifically designed for Internet payments. Users can pay with a prepaid card by entering on merchant sites the card's unique number, which corresponds to the card's nominal. The value of the card is decreased by the amount paid to the merchant.

To better understand what issues that surround electronic payment systems, it makes certain sense to introduce a definition of payment mediation services, which use existing payment systems as mediators to provide extra services.

2.1.5 Payment mediation services vs. payment systems

To further refine the focus of this research, we have to make one important distinction, which is between *payment mediation services* and payment systems. This distinction particularly makes sense in the context of electronic and Internet payment mechanisms. Payment mediating services have appeared as a response to the imperfection and inefficiency of current payment systems for the Internet. They extend the services of the existing systems and operate as mediators between merchant, payment systems and users. Their goal is to help merchants to accept as many payment systems users could possibly want to use when paying over the Internet. In payment mediation services the existing payment infrastructure from many payments providers is aggre-

gated to provide broader services, or to overcome shortcomings of the available payment options. Figure 2.2 describes the relations between merchants, EPSs and payment mediation services.

The difference between payment mediation services and payment systems can be summarized in that a payment mediation service is as an *intermediary* between payer, business, and payment system, while there is no such middle tire for payment systems.

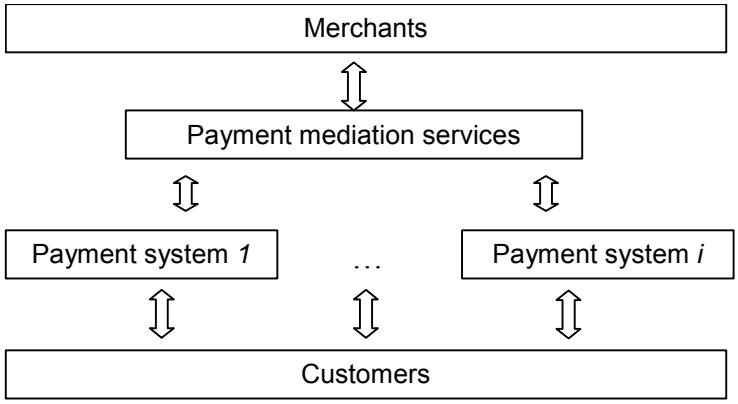


Figure 2.2 Relationships between payment systems and payment mediation services

The payment process in this case is transparent to the users of a site. A mediating service provider 'intercepts' payments from users, processes them, and credits the account of the owner of the site when the authorization and transactions are completed. For example, there are numerous companies among mediating services providers that facilitate acceptance and processing of various credit cards.

A special class of payment mediation services has emerged, that provides convenience for paying bills for businesses and end users. An example of payment mediation services is providing bill payments for end users and companies, for instance, utilities or telephone bills. Over a Web front-end provided by the billing systems, customers and companies can pay bills that are normally paid offline by paper cheques or bank transfers. Some systems even provide additional services such as automated accounting merged with online payment facilities.

Syndication of payment services

Another angle on payment mediating systems is viewing them as a form of *syndication* of payment services in an online environment. The notion of syndication originates from the entertainment world, where it forms the fundamental organizing principle. With the advent of the 'new economy' and the use of the power of Internet distribution, syndication can be recognised as an emerging model for e-commerce. In this context syndication would mean selling the same information to many different customers, who render and integrate it with other information in various value-adding ways and then redistribute it.

According to this principle, businesses involved can play three or more roles: originators, who create original content; syndicators, who collect and package digital information to meet specific customers' needs; and distributors who deliver digital content to customers, (Werbach, 2000). In the context of online payments, payment mediation services can be seen as syndicators of the original services offered by payment systems. Payment mediation services syndicate e-commerce EPSs, offering merchants the way to accept a variety of payment systems.

Examples of payment mediation services

A good illustration a payment mediation service is Bibit Billing Services (www.bibit.com). This Dutch company specializes in Internet payment and billing services. The service supported about 70 payment methods from 18 countries by 2004. When customers want to pay on a Web site of a Bibit's client, they select one of the provided payment methods. The payment process goes as follows:

1. A customer selects products on sale in a virtual shop.
2. For payment, the customer is then redirected to Bibit Payment Service.
3. Within Bibit Payment Service, the customer can select a payment system he or she would like to pay with, provided it is supported by Bibit. The customer makes the payment with the system of his or her choice.
4. After a successful payment, Bibit notifies the merchant that the order can be shipped and transfers the money to the merchant.

The processing of the transactions, which is conducted entirely by Bibit, is therefore transparent to the customers of the site and the client company. The company business model, which utilizes a number of payment systems, relies on providing extra services to facilitate payments, and therefore it fits into the definition of a mediating

system. It is interesting to note that the service allows the use of micropayments, by accumulating charges for products like news, articles, stock and research reports, online games and charging users on a subscription basis. Examples of other payment mediation services are Orbiscom (www.orbiscom.com), iBill (Ibill.com), PayTrust, (www.paytrust.com), DataCash (www.datacash.com), PayNet (www.paynet.ch).

Systems that conceal real customer's credit card numbers by providing them a unique temporary card number for each transaction have gained certain popularity among payment mediation services. The customers can then use this unique number in a normal credit card transaction, and their real credit card will be charged. This temporary card number expires after every transaction and would not be approved for the subsequent use. The data of real credit cards of customers is not exposed to parties online in online transactions. In this case the payment mediation services are using credit cards infrastructure to provide extra security and anonymity (ABN-Amro e-wallet, O-Card by Orbiscom.com). By using these measures merchants expect to accept more secured payments without changing the way shoppers pay and without changing existing payment processes or infrastructure.

The research summarized in this thesis is concerned mainly with payment systems and not with mediating solutions for existing payment infrastructure. Payment mediation services on the Internet emerged because of the absence of relevant payment solutions or have problems that prevent their successful use by merchants and users. Many of EPSs are probably transitory systems, unable to completely solve problems that appear in the context of the Internet paying process, because the problems originate in the payment systems they use; see discussion on PayPal.com in section 2.4. While syndication of EPSs by payment mediation services provides in the end a better level of service than individual EPSs they use, it also places the payment mediation systems out of the scope of this research, which is exploring ways to design better individual EPSs.

2.2 Identifying the characteristics of payment systems

As observed in the example with Chipknip and Chipper in the previous chapter, there are a lot of factors that determine the success or failure of payment systems, and not all of them are of technical nature. As mentioned already, user acceptance depends on many issues, such as consumer choice, preferences, advertisement, a state of the market, etc. The discussion of diverse aspects of electronic payment systems can be found in many works on development and research of payment systems. Attempts to classify and describe the requirements and characteristics of payment systems such as security, reliability, convertibility, efficiency, traceability, and others can be found, among others, in the works of Medvinsky & Neuman (1995), Langdon et al. (2000), Lynch & Lundquist (1996), Wayner (1997). It has to be noted however, that these studies are mainly focused on technical aspects of electronic payment systems, which is not the only facet that is important in this field. Below the characteristics of payment systems are extended to account for user-related aspects of EPSs. These characteristics can be also used for assessment of payment systems, as described further.

The list of characteristics of payment systems

Anonymity, privacy

This characteristic reflects the desire of users to protect their privacy, identity and personal information. In some transactions, the identities of the parties could be protected by anonymity. Anonymity suggests that it is not possible to discover someone's identity or to monitor an individual's spending patterns. Where anonymity is important, the cost of tracking a transaction should outweigh the value of the information that can be obtained by doing so. As an illustration, when a customer pays with a debit card, the purchase is registered at the vendor and bank's databases. It is possible to find out what amount was paid and what actually was purchased. Thus debit card payments are not anonymous.

On the contrary, when one pays with cash at a shop or in a marketplace, no one can say by examining the cash that money came from the payer, as there is no direct information about this payer's personality associated with the banknotes. Thus, cash is an anonymous payment system. Currently, the right of users to choose how their per-

sonal information is disclosed is viewed as *privacy*. There are privacy laws in several countries that limit usage of personal information by banks, authorities and other parties, including online businesses and payment systems, like European privacy acts or similar directives, e.g. European Commission Data Protection Directive.

Applicability

The added value of a payment mechanism is dependent upon how useful it is for buying something. Applicability (or acceptability, as it is often referred in literature, (Medvinsky & Neuman, 1995)) of a payment system is defined as the extent to which it is accepted for payments at points of sale, or at online e-commerce sites in this case. For instance, cash is accepted widely and virtually everywhere in the offline world and thus has a very high level of applicability. Debit cards and credit cards have a very high applicability, as one can pay with them in a variety of places. The applicability of a payment system may vary from country to country. For example, in Germany and in the Netherlands cheques are no longer common due to the steady growth of other payment methods. However, in the UK and the USA cheques are still quite a common method of payment and the level of their applicability is quite high.

Authorization type

Authorization type is referred in the literature as the form of a control over the validity of transactions, (Lynch and Lundquist, 1996; Asokan et al., 1997). The authorization type can be offline or online. Offline authorization means that users of the system can exchange money while not connected to a network, without a third party mediating for the transaction. Paper cheques are an illustration of offline authorization.

The ability to make peer-to-peer payments, however, is not fully dependent on the authorization type. It is possible with both online or offline authorization. However, for peer-to-peer payments with offline authorization users should be physically connected with each other. Payments with conventional cash are an example of peer-to-peer payments with offline authorisation. Some electronic payment systems, e.g. Mondex, also offer this kind of service. Users can exchange money offline by connecting their Mondex cards via hardware card-reading devices.

Convertibility

Naturally, users will select payment mechanisms as financial instruments according to their needs. Numerous payment schemes have emerged up to this date and users can expect new systems to appear, all providing an assorted variety of services and appli-

cations for various purposes. Funds represented by one payment mechanism should be easily convertible into funds represented by other payment systems. Users should be able to transfer money from electronic payment systems to another accepted money form, e.g. receive it in cash, or transfer to a back account.

Efficiency

Much discussion is going about the ability of systems to accept 'micropayments' and small payments, (Rivest & Shamir, 1996; Hauser, Steiner, & Waidner, 1996). Small payments are amounts less than one euro; micropayments are amounts of a fraction of a cent. A system which entertains the characteristic of efficiency should be able to process small payments and micropayments without performance degradation, and without imposing the high transaction costs, (Low, Maxemchuk and Paul, 1994). The costs per transaction should be reasonable for processing small amounts. Adherents of small payment promote numerous applications, from paying for articles, news and stock reports to pay-per-view sites.

Interoperability

A payment system is interoperable if it is not dependent on one company, but is open and allows other interested parties to join. This can be achieved by means of open standards for data transmission protocols and infrastructure. An interoperable system can faster gain the necessary customer base for future development and will have a higher level of applicability. The example of Chipknip and Chipper in the previous chapter illustrates the consequence of low interoperability. It is natural, though, that companies that implement new technologies treat them as know-how, because of the added value they create by investing in new technologies; therefore, it is not always sensible to demand interoperability. Examples of theoretical interoperable initiatives are the SEMPER project (www.semper.org), CEPS (www.cepsco.org), and the CAFE project (Boly et al., 1994). For instance, the last two initiatives were conceived to facilitate interoperability between diverse electronic purse systems.

Multi-currency

Effective and efficient payments between different countries are possible when a system allows processing multiple currencies, as it is currently done with credit cards. This feature however is not implemented or foreseen in payment systems of many countries, binding them to a particular currency region. Multi-currency payments are decidedly required for payments in cross-border electronic business and e-commerce.

Reliability

Naturally, users and businesses want a system that is **reliable,** because the availability of services and the smooth running of an enterprise will depend on the availability and successful operation of the payment infrastructure, (Medvinsky and Neuman, 1993, 1995). Whether in the result of a hackers' attack or simply poor engineering, the costs of breakdowns can be substantial, and the failure to maintain reliable operations can be unrecoverable.

Scalability

As the commercial use of the Internet grows, the demands placed on payment infrastructure will also increase. The payment infrastructure should be scalable, to be able to handle the addition of new users and merchants, so that systems will perform normally without performance degradation and maintain the required quality of service, (Medvinsky and Neuman, 1993). Among the least scalable systems are those that require from merchants to purchase and install additional software and hardware, because this increases the costs of accepting the payment system for the merchants. This often hampers development of token-based systems and e-purses.

Security

One of the most crucial and well-researched issues in payment systems is security, (Wayner, 1997; Lynch & Lundquist, 1996; Chaum, 1992; Brands, 1995). Since the Internet is an open network with no centralised control, the infrastructure, supporting electronic commerce and payment systems in particular, must be resistant to attacks in the Internet environment.

Security can be viewed as a two-fold issue. On the one hand, users would like to be sure that their money is safe when paying online. On the other hand, banks and payment services organisations would like to protect themselves so that no money, financial, or personal information can be stolen or misused. Security of electronic cash systems has an aspect of counterfeiting: no one should be able to produce electronic tokens on their own, otherwise banks or governments will have to pay for such counterfeiting. Another aspect of security of electronic cash is *double spending,* (Chaum, 1992). What cash transactions achieve by the physical nature of cash, is that money can be spent only once. In the computing environment, where copying information and modifying records is easy, this property becomes a challenge for engineers. An EPS operator should ensure that electronic cash cannot be spent twice. In this aspect, security is often viewed in connection to anonymity, cryptography, and unforgeability,

(the inability to create 'counterfeit money' for the use in the system), (Asokan et al., 1997).

Traceability and linkability

Traceability indicates how easy it is to trace money flows and sources of funds that are going through a payment system and used for purchases. In electronic payment systems money can be traced by records that are kept of a payment activity. For example, information about credit card payments is stored by banks and credit card companies, and it is possible to find out what money was used for, and where it came from. In this research traceability is associated with anonymity and privacy of a payment system.

Traceability is related to linkability of payments. Linkability of an EPS implies that payments can be associated with a particular user, or that it is possible to recognize several payments originating from the same user, (Schoenmakers, 1998). Users can be linked to their spending even if the system they use is anonymous. This can be done by using information that is indirectly associated with users, e.g. the physical location where payments take place. Despite that individual payments are anonymous, a relation between a user and his payments can be established based on this indirect information associated with the user.

Trust

Due attention and proper implementation of the above-mentioned characteristics can help to build up the vital attribute of trust, (Wayner, 1997; Lynch & Lundquist, 1996; Egger, 2003). Trust, in this context, refers to the degree of customers' confidence that their money and personal information will be safe, and that all parties involved will not act against users' interests. From the perspective of using a payment system, users need to trust that payments will be conducted in a proper way, and that their money will not be stolen or misused. On the other hand, even if we use an imperfect system, we want to believe that vendors, banks, and credit cards companies will not use the information they hold against us in any harmful way. Conversely, another essential aspect of trust is that other parties *accepting* our payments should trust the payment systems we want to use. On the basis of such trust, they will be willing to accept our payments and conduct commerce.

Usability

It should not be a sophisticated or complex task to pay online, payments are to be done in an easy and user-friendly way, (Guttmann, 2003, p.89). This requirement can

be manifested in *ease of use* of the system, (Lynch & Lundquist, 1996). In such a responsible task as a payment process, users should have minimum factors that make paying complicated or distract them. An overly complex payment process, accompanied by other complications associated with EPSs or an e-commerce payment environment, can turn customers away from a financial transaction and even future e-commerce activities. For example, the processes of paying when you have to fill in a lengthy form with name, address details, a 16-digit credit card number plus expiration date cannot be called an easy one when compared with cash payments. This is the very process that most Internet shoppers have to go through to make their online credit card payments. Poor usability of a web shop or a payment method could also discourage spontaneous purchases. Certain e-commerce companies demonstrate understanding of the importance of this issue. To remedy this situation for credit card payments renown online bookseller Amazon.com has devised a '1-Click' checkout method, (Enos, 2000) to allow customers to make payments with the minimum of authorisation steps and information input, (Source: Amazon.com). Usability is an important characteristic of an interactive product and is defined as "the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use", (ISO 9241, 1996).

Using the characteristics as an assessment framework of EPSs

As it can be seen from the literature, (Medvinsky & Neuman, 1995), the characteristics can be used for describing and evaluating EPSs. The list of the characteristics compiled in this thesis can serve as a framework for assessment of EPSs. Such use of the characteristics can help to obtain a picture about how well a payment system measures against these characteristics, highlight possible limitations of the system, and suggest in what aspects the system can be improved. This kind of information can be used as an input for design of EPSs. Section 2.4 uses the assessment framework for describing a payment system.

2.3 Advantages and limitations of payment models

Having described payment systems and their various characteristics, these characteristics will be used to illustrate advantages and limitations of different payment models.

2.3.1 Advantages and limitations of the electronic cash model

An important advantage of electronic cash is its potential for anonymity. Some systems, like eCash, (Schoenmakers, 1998), (see also Brands (1995)), can block attempts to identify the user to whom a specific token was issued, even if all parties conspire. However, in an attempt of double spending, the user will not be able to use the same electronic 'coin' twice. In the context of offline electronic cash, if a user were attempting to spend the same tokens twice, the systems would reveal enough information to determine the user identity.

Certain systems, such as NetCash and Mondex, provide a weaker form of anonymity, which has to do with linkability, see section 2.2. Theoretically, if all parties join together, it is possible to determine who has spent the 'coin'. However, with NetCash, a user can choose the currency server and can instruct the one he trusts not to retain information needed to track such transactions. In contrast, although Mondex is an electronic cash system, it is not anonymous, because each card has a unique identification number that is linked to the person to whom the card was issued at the bank. Users cannot buy a Mondex card without revealing their identities.

One particular advantage of electronic cash systems is the possibility of payer-to-receiver exchange without the need to contact a central control system. This can reduce the costs of transactions and facilitate micropayments. The system becomes more efficient, because of less information processing, and eventually less organisational overheads.

A significant disadvantage of current electronic cash mechanisms is the need to maintain a large database of past transactions to prevent double spending. For example, in currently discontinued eCash, it was necessary to track all tokens that had been deposited. With the NetCash approach, it is necessary to keep track of all tokens that have been issued, but not yet deposited. Double spending can be an obstacle for system ex-

pansion, because it can reduce the scalability of the system, (Medvinsky and Neuman, 1993).

Another factor that may be perceived as a disadvantage is the necessity to purchase and install extra hardware and software, sometimes for both merchants and customers. While for consumers it means complications with technical issues and learning a new system, for merchants it may suggest even more costs and efforts for integrating new systems into their accounting and financial reporting. This can also lower merchant acceptance of electronic cash systems. However, dedicated hardware may help to solve various problems with security and authentication of this type of EPSs, (Brands, 1995).

2.3.2 Advantages and limitations of the account-based model

Wayner (1997) notes that, at the first stage of the development of electronic payment mechanisms, account-based systems will prevail, as long as the credit card business is well computerised and it is much easier to implement these kinds of systems with the existing technology. As long as a payment system employs existing infrastructure and a computer as a payment terminal, there is no need for creating new hardware or software infrastructure.

EPSs built on the basis of this model have therefore a potential for good scalability, which allows more users to join the system without great loss of performance. The reason is that to support more users, a system should only increase the number of accounts, which can be done relatively easily; there is no need to support large databases tracking all issued tokens to avoid fraud, as it is done in electronic cash systems. An advantage of the account-based model is a potential for usability of payment systems, because the existing infrastructure, familiar to users and merchants can be used for making payments.

There are several limitations of this type of systems. Account-based systems are usually traceable and not anonymous, so clients' spending and money sources can be easily identified. Because account-based systems usually have centralized authorization type, the overhead costs for transaction processing could be rather high. Credit card transactions, for instance, could involve up to five participants: the purchaser and the purchaser's bank, the vendor and the vendor's bank and the settlement company. This leads to the high overhead costs, making credit cards inefficient for small payments.

An important point to mention is that the low level of security of such systems affects banks, users and vendors. Another issue are credit risks imposed on banks or credit card companies when they extend the credit for their clients who are using credit cards.

Account management for EPSs of this model is often under control of a single company that provides service by account-based model; this can affect interoperability, if it is difficult for other parties to join due to closed or proprietary standards, and decrease reliability, because the company may have a single point of failure. This type of systems usually requires a network connection and servicing offline payments can be complex, which is also a limitation in certain contexts of use.

Payment systems, built according to this model have potential for multi-currency support and high scalability. It depends on details of realisation if a payment system will gain enough trust, will have features of convertibility, or how secure and reliable would it be.

2.4 PayPal.com: Using characteristics for analysis of payment systems

As an example, let us look at PayPal.com, one of the most successful online payment systems on the market in the beginning of the 21st century. Paypal.com is a good example of the alternative to credit card payments, providing the payment link between buyers and sellers. A user has to open an account with PayPal.com to be able to pay and receive money. The account then should be funded with credit or debit cards, electronic wire transfers or by other methods. The registered customers can then transfer funds between their accounts, pay at the web sites that accept PayPal.com payments, and receive money from other users, Box 2.1. The PayPal business model is based on charging merchants for accepting PayPal payments. By 2004 it has also become possible to use PayPal credits with the 19 million MasterCard and Visa merchants worldwide, without ever having to go through a bank account. This system is used by big online companies such as e-Bay or Amazon.com and has already attracted more than thirty million users by 2003. Let us see how PayPal.com measures against the characteristics of payment systems described above.

PayPal users can expect a high level of *anonymity* and *privacy* when paying directly from a PayPal.com account. The company claims that "PayPal is committed to protecting the privacy of our users. When you send or request money using PayPal, the only information the recipient sees is your email address, date of sign-up, and whether you have completed PayPal's verification process by confirming an account at another financial institution. Recipients never see your financial information, such as your credit card or bank account numbers", (Source: PayPal.com Help, 2003).

However, privacy of users can be easily compromised upon interference of governmental institutions, such as the police, (Cox, 2001). While these interferences can be justified to fight fraud, they still can still prevent users from adopting PayPal, because they may feel their privacy is compromised.

Incidents when governmental agencies access the records of EPSs operators may be very damaging to the company reputation and undermine user *trust*. Angry customers have formed a number of bodies to inform and protect themselves and new users against the questionable company policies and practices. Among such are www.paypalwarning.com, www.paypalsucks.com, PayPal Victims Club at Yahoo! Groups, and www.aboutpaypal.org.

These problems can also lower the *applicability* of the system. The main reasons for merchants refusing to accept PayPal.com payments, reported at the above-mentioned Internet communities, are periodic changes in the PayPal's policy regulating which products or services can be sold with using the system. For example, one of the policy changes banned selling modern firearms with PayPal. While the company is concerned about its reputation, the measures the firm has taken have irritated many merchants and users.

PayPal.com is a system with a centralised *authorisation type*. What is important from the user viewpoint is that a single company has control over all accounts and transactions, and not being monitored by other parties. It is harder for customers to appeal to the company's decisions, as PayPal.com is the final authority in their own business.

The system has a high degree of *efficiency*, as transaction processing is automated, is done electronically, does not rely on expensive transaction channels as paper checks, and the costs of transactions are not correlated to the transferred amount. The system allows transactions with small and micropayments.

PayPal.com is a quite *convertible* system. Users are able to withdraw money from the system to their checking account, or request a check: "You can withdraw funds from

your PayPal account by requesting an electronic funds transfer to your bank account or by requesting that a check be sent to you by U.S. mail. When you withdraw to your bank account, your money should become available within 3-4 business days, but may take more time depending on your bank's policies… You will receive an automatic email acknowledgement every time you request to withdraw funds", (Source: PayPal.com Help, 2003). PayPal.com supports *multiple-currency* transactions. By the end of 2003 the Multiple Currencies feature of PayPal.com "includes the ability to send and receive PayPal payments in Canadian Dollars, Euros, Pounds Sterling, or Yen, as well as U.S. Dollars", (Source: PayPal.com Help, 2003).

It is assessed that *interoperability* of PayPal is rather low, as there are no signs that other parties, such as financial institutions will join the payment system. Because of its authorisation type, the system is quite *scalable*, at least in theory. The possible user base is limited mostly by technical constraints and the administrative overhead. There was not enough data available to this research to assess how *reliable* is the system.

Due credit should be given to the PayPal.com help, which describes the system in many details for both novel and experienced users, and was widely used to write the current analysis, see Box 2.1. For instance, the relevant help section provides with explanation what measures are used to ensure *security*. Availability of such information can be critical for potential customers considering whether they should use the system for payments. PayPal.com demonstrates understanding of the importance of security to end users stating that "the security of your information, transactions, and money is the core of our business and our top priority at PayPal".

The interaction design of PayPal.com resembles a typical e-commerce shop, and usability guidelines for this type of websites can be applied to the design. There are, however, issues with *usability* of the PayPal's design. For example, design firm 37signals.com suggests redesigning the PayPal's payment confirmation screen, as seen in Box 2.2.

PayPal's close integration with credit cards creates the greatest threat for the business. Legions of fraudsters all over the world with stolen credit card information and identifications are using PayPal.com as a 'money-laundering' system to cash upon the situation when the card is not present. Credit card transactions where the card is not present and personally examined by a human controller account for the overwhelming majority of fraudulent credit card transactions. These and the other issues mentioned in this section can be very damaging to company reputation with users, merchants and

financial circles. Once again, it demonstrates how critical user-related factors could be for the success of an electronic payment system.

Making Payments

Q How do I send money?

A You can send money by going to the **Send Money** tab, clicking the Pay Anyone or Pay for eBay Items subtab, and filling out the form. When you send money through the Pay Anyone subtab, you will be asked to choose a payment type. The payment types are:

- **eBay Items:** Use for eBay purchases and you will be taken to an additional form to enter information such as your item URL, eBay Buyer ID, and a message for the seller
- **Auction Goods (non-eBay):** Use for non-eBay online auction purchase and you will be taken to an additional form to enter information such as your item URL, auction site, and a message for the seller
- **Goods (other):** A purchase of goods in a non-auction context
- **Service:** A payment for the performance of a service.

Quasi-Cash: The transmission of money not involving an underlying service or good. The bank that issued your credit card may treat this 'Quasi-Cash' transaction as a cash advance and charge you cash advance fees. PayPal has no control over these fees. If you select 'Quasi-Cash' you may want to use a payment method other than Credit Card (Instant Transfer or eCheck) to avoid potential fees.

Box 2.1 Making payments with PayPal.com. Source: PayPal.com Help, 2003.

2.5 Conclusions

In this chapter important aspects of electronic payment systems have been identified. They are summarized in Box 2.3. It is clear that the current state of online EPSs is far from ideal and that there are problems that can affect user acceptance of EPSs. Another important observation is that it makes little sense to focus on payment mediation services, because they are trying to compensate for problems that should be resolved in the existing payment systems these mediation services aggregate.

This research aims to define the ways in which user acceptance and, consequently, the success of new EPSs can be improved. The characteristics of EPSs can be used as initial guiding directions for design of EPSs. It can be suggested that designing an EPS

Before: PayPal Confirmation Screen

After: 37signals' Better PayPal

What's wrong with this screen?

This PayPal screen, which confirms payment information, suffers from a lack of focus. This is an important issue since it is the last screen you see before money is sent.

On the existing page (above), the dollar amount and the recipient's email address are treated in the same font size, style, and weight as less significant information like "type," "email subject," "note," etc. This dilutes the page and, in effect, de-emphasizes the critical information. PayPal should strive to make it immediately obvious why you're there and where the focus should be, even at a glance.

Further, the "Check Payment Details" is confusing because some people may think "Check" means bank check when it really just means verify.

How we made it better

We made the dollar amount the most obvious element on the page.

We used more conversational wording to make it easier to understand exactly what's going on and the purpose of the page.

We rearranged the data so the information flows more naturally (dollar amount, then recipient, then type of transaction, then funding source, etc.).

We grouped the dollar amount and the funding source into the same content block (currently they are too far apart for bits of info that are so closely related).

We separated the email subject and body into its own data grouping.

We labelled the "Send Money" button with the actual dollar amount ("Send the $37") for clarity's sake. Further, we grouped the edit and cancel buttons on the right while keeping the primary send money action button on the left in order to reduce the likelihood of clicking the wrong button.

Box 2.2 PayPal payment confirmation screen: usability issues and solutions. Source: 37signals.com, March 2004.

that is reliable, secure, trustworthy and usable would benefit user acceptance of the EPS. However, the contribution of the characteristics to user acceptance and their importance should be confirmed with potential users of EPSs.

Anonymity/privacy	Reliability
Applicability	Scalability
Authorization type	Security
Convertibility	Traceability
Efficiency	Trust
Interoperability	Usability
Multi-currency	

Box 2.3 Summary of characteristics of electronic payment systems.

Designers of future EPSs should be convinced that the characteristics would provide adequate support of user activities and needs. To answer these questions, before suggesting to employ the characteristics for design of payment systems, it has to be found out that they make sense to end users and to establish what importance the users attach to the characteristics. It is quite likely that the users would find some characteristics more important than the others. In this case, it will be more effort- and cost-effective for designers to concentrate mainly on the characteristics that are considered important by the users. With such an approach designers can ensure that their system has a built-in potential for user acceptance from the very beginning of the system's development. The following chapter describes an investigation into the importance of the characteristics of EPSs to end users in more detail.

Chapter 3

User survey of electronic payment systems

3.1 User acceptance of electronic payment systems

The previous chapters suggested that there are lot of factors that determine the success or failure of payment systems, and not all of them are of a technical nature. Several attempts have been made to describe electronic payment systems, mainly from a technological point of view, (Medvinsky & Neuman, 1993; Asokan et al., 1997). However, the characteristics used to describe EPSs should be validated with end users. It has to be found out how the characteristics of payment systems relate to users acceptance.

User acceptance of new information technology has been extensively studied in the context of information systems management, as mentioned in section 1.2. For instance, the Technology Acceptance Model (TAM), introduced by Davis (1989), has gained much popularity for predicting information systems acceptance. TAM serves to

explain and predict information technology acceptance and diagnose problems before users experience the technology. Following TAM, perceived usefulness and perceived ease of use are thought to be able to predict user behaviour that leads to user acceptance of technology, see Figure 3.1.

Perceived usefulness, defined by Davis, et al. (1989), is the user's subjective opinion that using a system will increase the user's job performance within an organisational context. *Perceived ease of use* refers to users' expectations that software use will be free of effort. Perceived ease of use has direct impact on perceived usefulness, but not vice versa. In their work on validating TAM Davis et al. (1989) have discovered stronger relationships between perceived usefulness and behavioural intentions to use, than between perceived ease of use and behavioural intentions. TAM is a theoretic model based on extensive empirical evidence. In the work of Davis (1989) a validated scale for measuring user acceptance along the two model's constructs was presented and substantiated with sufficient empirical evidence.

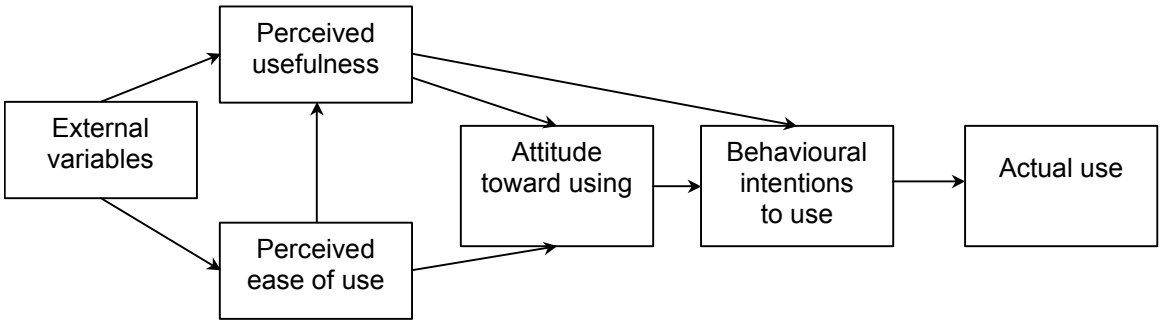


Figure 3.1 Technology Acceptance Model, (Davis, 1989).

While TAM is a good predictor of the intentions to use a software package, it would not be enough to describe the specific nature of user attitudes towards EPSs. The context of use of EPSs, where money transactions are involved, is different from usual information technology applications, where the productivity at work is mainly concerned. Plouffe et al. (2001, p. 209), express concerns that TAM does not take into account the context use in predicting information systems acceptance. It cannot be assumed that TAM will take the specifics of this context of use into account, for instance, in aspects of trust, reputation, or believes about technology. Therefore, in this research employs the theory of reasoned action, which is arguably better suited for predicting user acceptance of EPSs. The theory of reasoned action (TRA), originating in social physiology, defines relationships among beliefs, attitudes, norms, intentions and be-

haviour, (Fishbein & Ajzen, 1975). According to TRA, behaviour, e.g. the use or rejection of technology, is determined by the person's intention to perform the behaviour, and this intention is influenced by the persons' attitude and subjective norms. Subjective norms are defined as "the person's perception that most people who are important to him think he should or should not perform the behaviour in question", (Fishbein & Ajzen, 1975, p. 302). Attitude towards a behaviour is determined by believes and evaluation of consequences of the behaviour. Figure 3.2 describes the theory components and their relationships. This theory justifies a generalised model for understanding of human behaviour, and demonstrated strong predictive utility, even in the situations which fall outside of the original conditions of the theory, such as predicting non-voluntary behaviour, (Dillon & Morris, 1996).

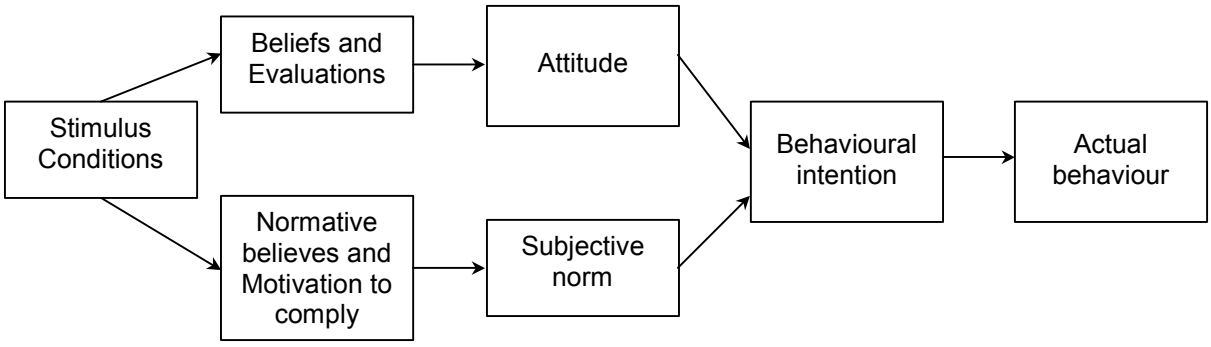


Figure 3.2 Theory of reasoned action (TRA), based on Fishbein & Ajzen (1975).

TRA, which is applicable to a much wider range of situations than only information technology, seems to be better suitable to describe how user attitudes can influence acceptance of payment technology in an e-commerce environment than TAM. Unlike TAM, TRA takes into account social influences (e.g. shared subjective norms) on users of various factors surrounding the usage of EPSs in online e-commerce environments. Since EPSs are intended for personal use, factors such as reputation can be highly important to end users and influence their attitudes. In addition, since perceived usefulness and perceived ease of use are seen to have a significant impact on attitude towards the system, in TAM attitude is not tied to beliefs about technology. Overlooking user believes can be misleading for EPSs. Social influences and user beliefs about technology, such as trust in the technology or understanding of technology, can be very influential on the adoption of the technology.

This thesis argues that for user acceptance of electronic payment systems in an e-commerce environment other factors, in addition to perceived ease of use and perceived usefulness, could be responsible for user acceptance. User believes and attitudes towards privacy, security and trust could be determinants for the final users' decision to utilize a system for payments. Taking into account social influences in the context of e-commerce EPSs can further substantiate the understanding of user acceptance of EPSs. Therefore, it has to be found out what aspects of electronic payment systems are important to end users, and could determine user attitudes, behaviour and intentions to accept the payment technology.

Based on TRA, behavioural intention and consequently the actual system use are determined by user attitudes. It has to be investigated what attitudes users have towards certain aspect of EPSs. Discovering these attitudes will let us understand what are the factors that influence user acceptance of EPSs.

3.1.1 Characteristics of electronic payment systems as determinants of user acceptance

The list of characteristics identified in Chapter 2 was taken as a starting point of exploring what is important for end users in interaction with EPSs. While the list of characteristics originated from the literature, that embraces many aspects of EPSs, hardly any empirical evidence of their importance to end users of online EPSs has been reported. To find empirical evidence a consumer survey was conducted. This survey tried to gauge the extent to which users are influenced in their decision to use systems by the characteristics described in Chapter 2.

The validation step will cover only those characteristics described in Chapter 2 that can be perceived and experienced by users directly. As this research aims to generate knowledge about designing interaction with EPSs, it would not make sense to include e.g. interoperability or scalability, because users do not perceive the aspect of the system described by this characteristic directly in the interaction. Therefore, several characteristics were not included in the survey. These characteristics may be also important for user acceptance over the long-term use, but they are mainly transparent for end users, because they do not have direct interaction or perception of these characteristics in payment activities. Instead, these characteristics should be given attention from an engineering or business perspective.

The characteristics that were selected for validation with users are listed below. See section 2.2 for detailed descriptions of the characteristics.

- Anonymity, privacy, traceability
- Applicability
- Convertibility
- Efficiency
- Reliability
- Security
- Trust
- Usability (ease of use).

This research had to justify the relevance and importance for user acceptance of the characteristics of EPSs described in Chapter 2. It was not aimed to model the decision process of users, but to identify which factors affect user acceptance of EPSs and to use this knowledge to inform design of EPSs.

Hypothesised determinants of user acceptance of EPSs are characteristics which:

- are relevant for user behaviour, attitudes, perception and experience when using EPSs, (i.e. if they make sense to end users).
- are important descriptors of systems' aspects to end users.
- are important for systems' features or functionality.
- are important for describing aspects of social influences and interactions.

3.2 Survey of users' attitudes towards characteristics of payment systems

To reveal how important and well understood are the characteristics of payment systems to end users a survey was conducted in the beginning of 2001 in cooperation with De Consumentenbond, the largest consumer organisation in the Netherlands. In this survey conventional (cash, offline credit cards) and electronic payment systems (debit and smart cards, and credit cards on the Internet) were examined. The EPSs studied were not necessarily online EPSs. The study was performed as a survey of consumer

attitudes. It was previously published in Abrazhevich (2001a) and Abrazhevich (2002). This research did not aim to create an instrument for measuring user acceptance. The main goal was to gain design knowledge and ensure it can be applied to real-world EPSs.

3.2.1 Survey participants

The survey was conducted in a form of self-administered questionnaires sent out by post. Respondents were selected from the database of subjects of De Consumentenbond, which has been assembled in the past from people who reacted to a newspaper advertisement.

Of the 1328 respondents 94.1% were users of electronic payment systems. The respondents were daily users of several offline payment systems, including debit, credit and smart cards and cash. 19.4% had already made payments on the Internet before the study. The sample was balanced in demographic aspects: the respondents were employed in diverse industries and social institutions, there was no bias on sex (women 51.8%), age (mean is close to 50). Occupation of 94.8% of the respondents was not related to payment systems.

3.2.2 Questionnaire design and analysis

Several questionnaire items elucidated each characteristic of payment systems. Users were required to express their opinions on a 5-point scale for most of the questions (e.g. 1 – very important; 2 – quite important, 3 – neutral, 4 – quite unimportant, 5-not important at all). Certain questions were introduced by De Consumentenbond in line with their own research interests, see Appendix A for the survey questionnaire. The survey results are presented in Appendix B. The most important highlights of the survey are summarised in Table 3.1. It has been assessed whether answers contribute to importance or unimportance of a particular characteristic according to the percentage of responses.

3.2.3 Survey results and discussion

Characteristics of less importance

The most interesting finding was the users' reaction to the questions on **anonymity**. Despite that numerous publications emphasize the high importance of anonymity as a requirement for EPSs, (Lynch & Lundquist, 1996; Chaum, 1992), most of the respondents indicated that anonymity is not very important for them. 72.8% of the respondents are never stopped by the fact that they are revealing their identity. Only 13.5% are concerned that vendors can find out what they buy when paying with an electronic payment system. The respondents were quite satisfied with the level of anonymity provided by debit cards, one of the least anonymous systems (52.2%). 72.9% of the respondents would prefer their purchases to be registered, to avoid disputes with merchants and 50.4% agree that this can be used to provide a better service.

The vision of this research of the characteristic of **efficiency** (ability of a payment system to service small payments) is influenced by another interesting survey result. The prevailing number of the respondents (61.4%) did not think that small payments are necessary for shopping on the Internet. This is especially remarkable in view of many attempts to introduce small payments solutions for online trade. The first analysis suggests that users do not regard small payments as an important function of an EPS, because most information commodities that could have been traded for a small fee are given out for free, with the business model relying on online advertisement. This suggests that micropayments are not among the important characteristics for user acceptance in the scope of this research. The efficiency of a payment system cannot be considered an obstacle (at least in the Netherlands) for user acceptance of EPSs. It is possible that efficiency is critical for new business models that the surveyed consumers have not yet experienced.

It can be argued that user attitudes are dependent on the *context* where payments take place for payment applications. For example, for certain applications anonymity may be less important than other factors, as it is shown for debit cards payments, while in other cases the situation may be the opposite. Therefore, payment systems should be designed by taking into account specifics and requirements of concrete applications for specific contexts of use.

Another conclusion in relation to efficiency suggests that consumers may not yet understand well the potential and the benefits of a particular functionality being offered

by industries to support a specific business model. Thus, for future design, attention should be focused on adjusting payment systems for a specific context of use and thoughtful introduction of new applications and business models to customers.

Characteristics of high importance

Ease of use was rated as a characteristic of high priority. The respondents prefer debit cards (75.2%) and cash (10.4%) to other systems, because they find them easy to use. However, users noted that is quite easy to use credit cards for Internet payments. Among 19.4% of the users who had experience with online credit card payments, 96.2% suggested that credit cards are easy to use. This is despite the fact that an online credit card payment requires a user to fill in lengthy forms with personal data and credit card details, and therefore cannot be regarded as an easy one. Thus, it seems that while paying with credit cards is not a convenient process, users perceive it differently. A possible explanation could be that users have become accustomed to these types of payment over years, or that researchers in usability overestimate the complexity and workload of credit card payments. The results on ease of use can imply importance of usability of EPSs for users.

Convertibility of funds to another payment system turned out as expected. Users demonstrated relatively high dissatisfaction with the lack of convertibility of money from smart cards systems: 53.9%. At the same time satisfaction of convertibility from bank accounts to cash is high at 87.1%. Since in the Netherlands bank accounts are linked with debit cards, it can be concluded that convertibility of debit cards is higher, which confirms the reality, because bank accounts are designed to be convertible into cash.

Security is an issue of high importance for most of the respondents (98.4%). 75.3% of the respondents would stop using a payment system if they heard about a security breach in the system.

Expected results were received regarding **reliability** of payment systems; many respondents are aware of and concerned about the incidents of payment systems failures. 55.3% prefer debit cards, and 15.1% prefer cash, because they think that these systems are more reliable than others.

Table 3.1 Summary of the survey results
Legend. * — questions' numbers in Appendix B.
† — summary of percentages of two extremes of the scale

Characteristic	Questions	Responses (%)	Total N (1328)
Anonymity/ Privacy	4*. *Concerned* and *very concerned* that shops can register their purchases†	13.5%	1297
	6. Would like to have registration of purchases so that shops can use the records to provide with better customer service†	50.4%	1257
	3. *Satisfied* and *quite satisfied* with the level of anonymity provided by debit cards†	52.2%	1238
	2. *Never refrain* from paying because of revealing identity when paying†	72.8%	1312
	5. Would prefer that their purchases are registered to avoid disputes†	72.9%	1268
Applicability	24. Agree that a good shop should offer the choice to pay with any payment system users would like	85.8%	1313
Convertibility	8. Convertibility of funds from bank accounts to cash is satisfactory†	87.1%	1285
	8. Convertibility of funds from smart card systems to bank accounts is unsatisfactory†	53.9%	449
Ease of use	9. Preference because of ease of use:		1253
	Cash	10.4%	
	Debit cards	75.2%	
	10. Credit cards on the Internet are easy to use†	96.2%	132
Efficiency	13. Small payments on the Internet are necessary†	13.4%	246
	14. Small payments on the Internet can be used for:		197
	Various applications	45.2%	
	No need for small payments	54.8%	
Reliability	15. Preference due to higher reliability:		990
	Cash	15.1%	
	Debit cards	55.3%	
Security	16. *Important* and *very important*†	98.4%	1295
	17. Would stop using a payment system if hear about a security breach in the system†	75.3%	1302
Traceability	20. Concerned that sources of their income can be known by vendors†	45.3%	1262
Trust	21. Important that other people also trust the payment system they use †	72.4%	1271
	23. Would stop using a system if they felt that it's not trustworthy†	94.4%	1311
	22. Will trust the system introduced *only* by an established organisation†	97.6%	1289

Trust was considered to be a very important issue: 97.6% would trust only a payment system introduced by an established organisation. 94.4% would refrain from using a system if they felt it was not trustworthy. For 72.4% of the respondents it was important that other people trust the systems they use. This supports the prediction that social influences are important for the user acceptance of EPSs.

Questions about **traceability**, i.e. the ability to trace money flows and sources of income, indicated that 45.3% are concerned if such information would become known to merchants. 58.3% find important that they do not leave personal information (name, bank account, address) to merchants (question 19 in Appendix A). While the participants are not concerned about strong anonymity of payments, these reactions to traceability suggest that consumers still would like to have certain privacy.

The respondents place significant emphasis (85.8%) on **applicability** of payment systems, i.e. the ability to pay with a payment system at multiple and diverse points of sale.

In summary, according to the user responses, characteristics of primary importance are: applicability, convertibility, ease of use (usability), reliability, security, traceability, and trust. Lower level of importance was attributed to anonymity and efficiency.

3.2.4 Implications for user acceptance

Based on the results of the survey the list of user-related characteristics of payment systems can be revised further. In refining the original list, the survey results are combined with literature sources, reviewed in previous chapters.

The survey has clearly shown that efficiency is not of a high priority for consumers, though this might be simply a result of the satisfactory status of the current situation in this respect. Efficiency is more relevant where small and micropayments are concerned, which are out of the focus of this thesis, as discussed in section 1.4. Consequently, efficiency of EPSs should not be included in the final list of characteristics that can impact acceptance of EPSs.

Reactions to anonymity bring us to another observation. Users said they are quite satisfied with the level of anonymity provided by debit cards, which is one of the least anonymous payment systems. To explain this interesting result, a distinction should be made between *a*) full anonymity of users and their payments and *b*) privacy on the

level of restricting of access to personal information for non-authorized parties. In this respect, the results on traceability of sources of money actually relate to privacy rather than to full anonymity of payments. Using the term privacy will also cover the characteristic of traceability. Based on the survey results anonymity and traceability are replaced by privacy in the list of characteristics. The characteristics of primary importance are the following:

- Applicability
- Convertibility
- Privacy
- Reliability
- Security
- Trust
- Usability.

Influence of context of use in relation to user acceptance

The survey described in this chapter has assessed how users perceive the importance of different aspects of EPSs as a reason to use them or not. However, this description is independent of any context where payments take place. Clearly this is an insufficient account of the phenomenon. While most of the time users are not concerned about anonymity, they might actually want to be anonymous when engaging in financial transactions they prefer to keep private. The relative ratings, while informative in general, can be misleading if applied to the whole variety of EPSs and payment situations. Therefore, it makes sense to be more specific in targeting payment systems for various applications and contexts of use.

On the other hand, user can perceive certain system's aspects differently from how they are actually realized in the system. This was expressed by the survey respondents, who were quite satisfied with anonymity provided by debit cards, despite that debit cards are among the least anonymous systems. A potential explanation is that these attitudes pertain to situations where anonymity is not the prerequisite for engaging in transactions, or users are unaware about the actual situation, or do not find anonymity important in this situation.

This reasoning has the implication that different systems should be designed for various applications and payment situations, and it is unlikely that there is one solution that covers all emerging user and business requirements, mentioned in section 1.1.

User acceptance of EPSs is therefore dependent on:

- Perception of various aspects of payment systems.
- Contexts of use of specific applications for payment systems.
- Social influences and perception and attitudes towards influencing parties. User acceptance can be manipulated by various factors: technical partners, government, marketing, and user interface, and social influences, e.g. opinions of other users, family and friends, and reputation of banks and the parties involved, see Figure 1.1. Discovering these influencing factors can highlight what is necessary for systems' design.

Implications for design of electronic payment systems

This survey was a necessary step required to find out user opinions and highlight factors of electronic payment systems that are important to the users and can influence user acceptance.

The survey had given a picture what people's attitudes are, and suggested that these attitudes can determine users acceptance of the systems. However, this survey did not discover why users have their opinions and experience, or how they experience the payments online, nor does it help us to prescribe what designers should do to ensure user acceptance and design good EPSs. Using the characteristics or viewing them as requirements can grant a better understanding what aspects a payment system should have. However, there is a need to substantiate the way the characteristics are manifested in the system at the design stage. There is still the lack of specific design knowledge that will prescribe how to construct payment systems and what aspects should be implemented to achieve user acceptance. Moreover, this survey did not sufficiently focus on the issues of social influences and social interactions that also may affect users in their decisions to use payment technology.

One of the reasons for this is that the focus of the study was limited by the original set of the characteristics and the data collection method (user survey). On the other hand, the survey results are based on a sufficiently high number of respondents and should be therefore taken very seriously. The following chapter describes a diary study that aimed to understand how EPSs are experienced and perceived in the context of actual use and how they can be designed to meet users' needs.

Chapter 4

Diary study:
a Qualitative investigation of user experiences with electronic payment systems

4.1 Introduction

Chapter 3 has given an account of current consumer attitudes towards EPSs. The survey had a very broad scope and did not look into user experience with specific payment systems and did not examine the reasons for the reported attitudes.

In this chapter a qualitative study of Internet-based payment systems is discussed, that aimed to gain an insight of what makes users develop positive or negative attitudes towards payment systems, and discovering explanations for user attitudes, experiences and behaviour. This chapter motivates the diary study and the qualitative research approach, discusses its set-up and presents results and implications for design of EPSs. These findings can serve as a foundation for proposing recommendations for design of future electronic payment systems. Preliminary results of the diary study were previously published in Abrazhevich & Markopoulos (2002).

4.1.1 Motivation behind the diary study

The challenge in researching user behaviour during e-commerce activities lies in the sensitive nature of payments and money. Compared to the other types of user-system interaction, Internet-based payments are a very delicate type of interaction, since money transactions are involved. When people deal with money in real life, their behaviour could be different from the one during fictional money transactions in a laboratory, when they are asked to work with mock-ups or to stop interaction right before committing to an actual payment. In other words, a study of fictional payments lacks ecological validity. It was therefore decided to study actual payments by experienced and novice users of Internet-based payment systems through a diary study.

Diaries are increasingly popular as a research method in the field of HCI, as they offer the possibility to capture user opinions and experiences in the context of actual system use and throughout the day, close in time to the phenomenon studied, (Rieman, 1993). Diary studies have origins in multiple disciplines, such as psychology, health and medicine research, education, anthropology, and architecture. From the early 1990s the diary study method was introduced to the HCI community by the works of (Chin, Herring, & Elliott-Familant, 1992; Rieman, 1993; Carayon & Hajnal, 1993).

Palen & Salzman (2002) found diary studies to be effective and non-intrusive data collection methods, that yield informative, naturalistic data for research in the areas of HCI and computer-supported cooperative work (CSCW). They found that “diary studies can impose useful experimental constraints while maintaining ecological validity, because they are conducted in natural settings, but retain some level of researcher control”, (Palen & Salzman, 2002). The diary study method can serve as a middle-ground solution to the limitations of laboratory studies and observation studies, (Rieman, 1993). Diaries are linked to the actual usage and experience, and from the viewpoint of EPSs this technique is more realistic and valid than, for instance, interviews, focus groups, or questionnaires, based on hypothetical situations. During an interview informant might tend to generalise, forget, give attitude statements rather that report facts and experiences. Focus groups have similar limitations; they also can suffer from social influences between participants.

The previous research has identified several likely problems that users may experience of electronic payment systems, (Chapter 3). The survey of user attitudes towards payment systems, revealed no empirically supported evidence for the importance of certain requirements that seem to preoccupy current research on electronic payments

technology. For example, the survey reported that the ability to make micropayments was not considered very important by the respondents.

The goal of the study was acquiring insight on the actual user experience, and discovering and explaining user behaviour and attitudes towards online EPSs. The study searched for problems and positive aspects users can experience with EPSs, what functionality do they need for their payment activity, and how do they prefer to see EPSs designed. This study aimed to generate design knowledge on the user interaction with e-commerce EPSs.

The goals of the study are best answered by the qualitative approach to the data collection and analysis. The qualitative approach presumes broad, holistic, explanatory focus, tries to grasp complex interaction of factors, (Sigel and Dray, 2002). In contrast, a quantitative analysis would require a very reduced and concrete hypothesis to be tested, and may fail to uncover subtle issues, relevant to user acceptance of EPSs. Qualitative research employs inductive strategies that presume creating concepts based on the phenomena studied, rather than starting from theories and testing them, (Flick, 1998). Therefore the qualitative approach is appropriate for the goal of generating design knowledge using the diary study.

The diary study helped to find out what problems really concern users of EPSs, what are users needs and preferences in payment systems, and the ways users interact and experience EPSs. The analysis of the diary study looked into how these findings can inform design of future payment systems and from this viewpoint it complements the user survey and literature research described in the previous chapters.

4.2 Set-up of the diary study

The diary study investigated five account-based payment systems in the middle of 2002. These are 1) 'Internet Bankieren' (Postbank), 2) 'Internet Bankieren' (ABN-AMRO), 3) 'Electronic Banking' (ABN-AMRO), the older version of 'Internet Bankieren', 4) 'Direct Betalen' (Rabobank), and 5) PayPal.com. The first four systems are components of electronic banking systems of reputable Dutch banks. Apart from electronic payments they support many other functions, such as investments, savings and other banking products. Users of these payment systems have prior client relations with the banks, which might influence user perception of the payment systems.

PayPal.com is a representative of a purely Internet payment system, discussed in section 2.4. PayPal users can create payment accounts and use the system for money transfers and payments on affiliated web sites. The system also provides the ability to accept payments from other users or shoppers with credit cards. PayPal is neither a part of a banking system, nor supported by an established financial institution. From this viewpoint, this system provides an interesting contrast with the bank-supported payment systems. This should shed light on how trust towards the payment system is formed.

4.2.1 Selection of subjects

The participants were recruited by means of email and poster advertisement, distributed at the university campus. A web page providing an explanation of the study with requirements of the user profile was established to support participants' enquiries, Figure 4.1.

Individuals interested to participate were screened on the frequency of their electronic payments, so that they would be likely to make 5 or more actual payments within a few weeks. It was not possible to find expert users of PayPal willing to participate in the diary, because none of PayPal users reacted to the advertisement. Thus, for PayPal the diary data for only novice users was collected. The study did not aim for a big sample but rather was concerned to find subjects who would be committed to filling in diaries for several weeks, or who would be using EPSs for actual payments rather than for managing their personal finances.

Among the participants there were 4 students of various departments, 4 educational employees and 2 administrative workers. Five of them were users of Internet banking systems, employing them for most of their payment and banking activities. Five participants reported themselves as experts in online activities, while 5 were at intermediate level of internet experience, measured with appropriate excerpts from the questionnaire used for GVU World Wide Web User Survey (2003), see Appendix C. Four participants had moderate, the other 6 had high computer experience, gauged by the questionnaire adapted from Mayhew (1999), Appendix C.

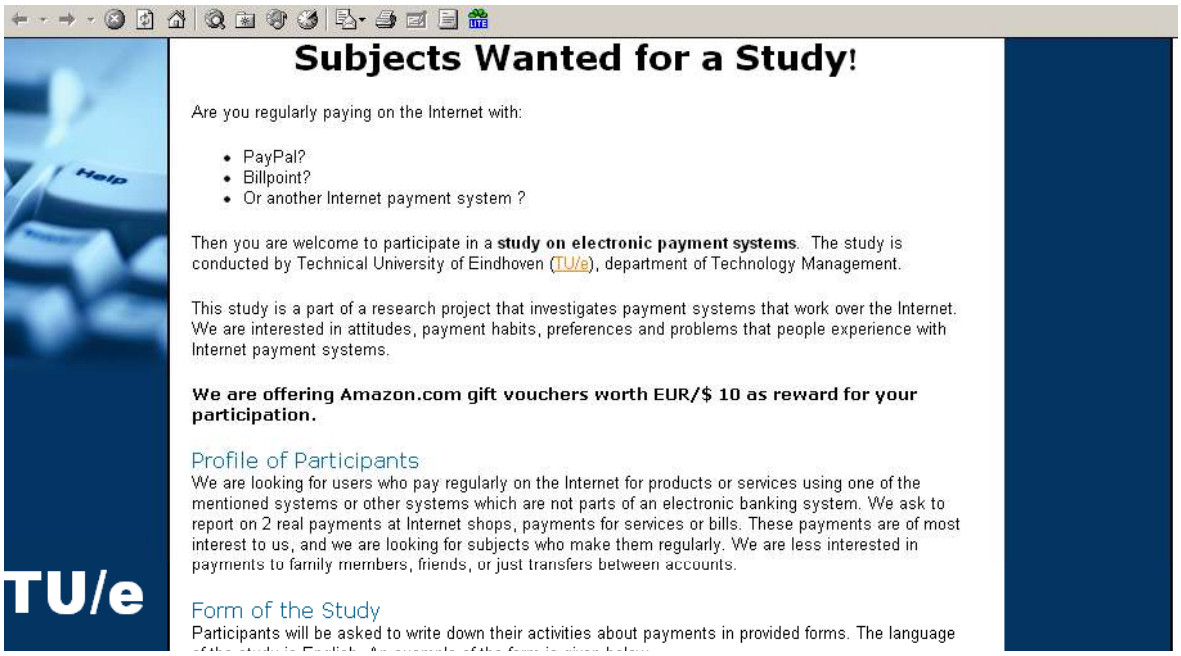


Figure 4.1 Diary study advertisement on the Web.

This sample may be limited to people related to the university and may not be fully representative of the general public. Since the intention of this study was to obtain an exploratory account of aspects of interaction design of online EPSs that affect user acceptance, and not to generalise to any target population, this bias is not considered to be a threat to the validity of the findings. The diary study had to trade the breadth of coverage to the detail of investigation, as the aim was not to reach the final conclusion, but to create a hypothesis to be validated with another research approach. The final number of participants has met the goal of the study. The return rate of the diaries was 83%, among the 12 persons applied for the participation. The subjects were awarded a participation fee after they had completed the diaries and interviews.

Another part of the diary study was conducted to embrace users of other online EPSs. This part of the diary study attempted to collect similar data, but used a different form of data collection. The participants were recruited online and filled diaries in electronic forms. At the end of the study they were interviewed by email. However, the most participants were strongly affiliated with the studied EPSs, e.g. as employees or researchers. This demographic bias has disqualified the data collected in this part of the diary study, and therefore it was not included in the final results of the study, to preserve the quality of the data.

4.2.2 Process and instrumentation

The diary was given to the participants in a briefing session where the purpose of the study and the use of the data they would provide were explained to them, and informed consent was obtained. In the briefing section a preliminary interview was conducted, aiming to collect general information about the participants, e.g., demographics, and experience with the Internet and payment systems.

The diary design is defined by the specifics of research. According to Palen & Salzman (2002) diaries can be structured, with specific pre-defined categories of activities to be registered and later counted. They can also be unstructured, with spaces for recording participants impressions, activities, possibly linked to the time flow, e.g. see Adler, et al. (1998). This diary had a mixed design, because it combined place for recording participants' impressions with open questions defined by the characteristics of EPSs. The paper diary consisted of several sections: instructions, a separate section where a number of open questions was asked about each payment, and a blank space for writing the diary notes. No pre-filled examples were provided to avoid biasing the participants, where it might draw their attention to issues that otherwise do not really concern them during actual payments. For instance, if an example mentioning privacy had been given, this might have drawn participants' attention to privacy issues. An example of the diary page is given in Figure 4.2.

The participants were asked to write in the provided forms their problems, opinions, observations and expectations of the interaction process. They were asked to record payments to online shops, bills and services. Payments to relatives, friends, or just money transfers between accounts were of less interest, due to the focus of this research on Business-to-Consumer e-commerce, and users were asked not to fill them in the diary forms.

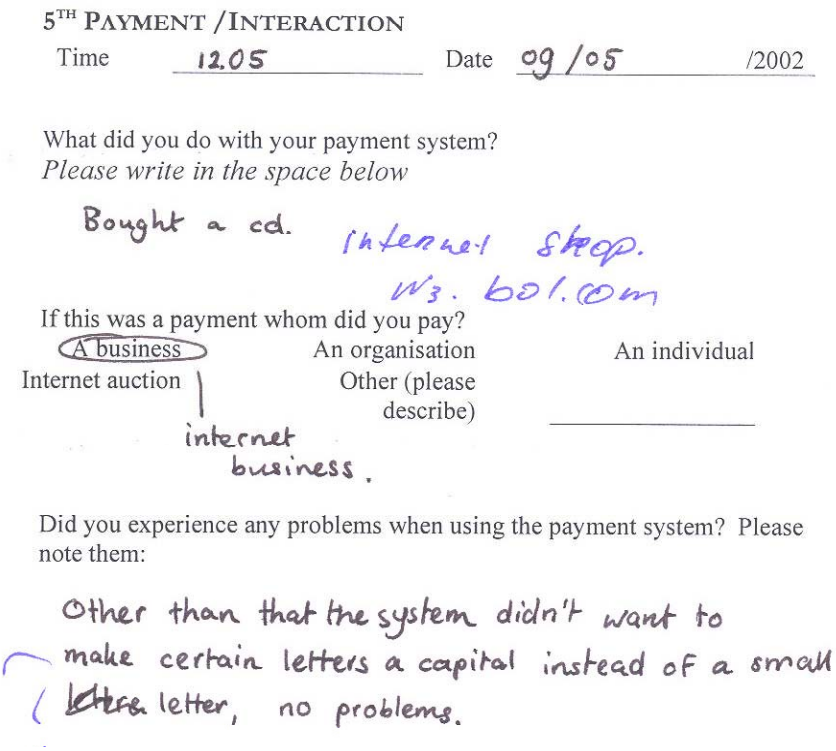
The diary study was informed by the characteristics of EPSs, discovered in the previous research. Subsequent items asked participants directly to express their impressions about security, usability, trust and privacy. The following open questions included in the diary:

- Have you experienced any problems when using the payment system?
- Was there something you especially liked or disliked about using the payment system this time?
- Do you feel there are any risks in using this payment system?

- Were you asked by the payment system to provide any information that was not strictly necessary for the payment activity?
- Are you worried that the company or bank that operate your payment system can misuse the information you provide?
- Do you feel that information about you is safe from third parties?
- Do you feel that your money is safe with this payment system?
- Do you find the authentication (passwords, security questions, calculator) annoying?
- Was interaction with the payment system easy?
- Do any security or privacy measures make it more complicated to use the payment system than you would like?

The subjects were asked to contact the researcher after recording 2 to 3 payments to ensure they are on the right track. In cases where the participants did not contact the researcher within a week, they were contacted anew to bolster the interest in the study and ask them to update their diaries. The participants needed to be reminded of the importance of keeping diary records. Such investigator's involvement is critical to avert declining dedication of participants and is important for the eventual success of diary studies, (Palen & Salzman, 2002).

A debriefing interview was conducted after the diary had been completed, and was used as another data collection method. Notes taken during the interviews were used in the analysis process. The interviews were tape-recorded and the records were reviewed by the researcher after the interview, if there was a need for clarification. The debriefing interviews consisted of going through the diary entries of the participants, and discussing impressions and experiences they reported verbally. The interviews employed the following qualitative interviewing techniques: in-depth interviewing, interviewing with open ended-questions and follow-ups, (Rubin & Rubin, 1995), combined with different types of probing, such as the silent probe, immediate and retrospective clarification and elaboration, and encouragement, (Keats, 2000).



5TH PAYMENT /INTERACTION

Time 12.05 Date 09/05 /2002

What did you do with your payment system?
Please write in the space below

Bought a cd. Internet shop. W3.bol.com

If this was a payment whom did you pay?

A business An organisation An individual

Internet auction Other (please describe) _____

internet business.

Did you experience any problems when using the payment system? Please note them:

Other than that the system didn't want to make certain letters a capital instead of a small letter, no problems.

Figure 4.2 A snapshot of a diary page.

4.2.3 Diary study results

The time spent on filling the diaries ranged from 4 to 6 weeks. Ten people have completed the study; they performed in total more than 30 payments or registration procedures. Those participants who were recording payments have made the target 4-5 payments that conformed to the goals of the study. The participants reported more than 70 problems (issues that users did not like, or experienced difficulty with) and positive findings (issues that users liked, thought as a success, etc). There were about 10 problems or positive findings that were mentioned by more than one user. Most frequently mentioned were the positive comments that the participants trust the bank they use, and that the banks do not ask too much personal information, because they already have client relationships with the participants.

Analysing the execution of the diary study, it has to be noted that the participants were quite responsible in filling the diaries. They have accurately reported the desired number of payments, and were open and willing to go into details in the debriefing inter-

views. The in-depth interviews have not found out many discrepancies with the diaries records, which supports the conclusion that the participants were honest and conscious in their reporting. As the result, a substantial amount of qualitative data was available for analysis. It gave the study the desired depth and met the researcher's expectations for the study.

4.3 Analysis of the results

The analysis of the diary study's raw data has borrowed elements of the Grounded Theory (GT) methodology, (Strauss & Corbin, 1990). GT is used for analysis of qualitative data. This data analysis method is employed widely in social science and psychology research, however, its application to HCI research is quite novel, (Elliott, Jones, & Barker, 2002). To give the reader an overview of GT its method and rationale are discussed in this section.

Grounded Theory overview

(Strauss & Corbin, 1990) define GT as follows: "The grounded theory approach is a qualitative research method that uses a systematic set of procedures to develop an inductively derived grounded theory about a phenomenon". The primary objective of grounded theory is the discovery of theoretically comprehensive explanations about a phenomenon by identifying the key elements of that phenomenon and then categorising the relationships of those elements in the context and process of the study. The techniques and analytical procedures enable investigators to develop a theory that is significant, theory-observation compatible, generalisable, reproducible and rigorous.

GT specifically attempts to generate theory to explain the phenomena to which it has been applied. GT is most accurately described as a research method in which the theory is developed from the data, rather than the other way around. This can be contrasted to hypothesis testing. GT is an inductive approach, meaning that it moves from the specific to the more general. Such approach to understanding of EPSs is important for this research phase, where explanatory accounts of phenomena of user attitudes and experiences with EPSs are needed to prompt the generation of design knowledge, and is not easily achievable by controlled studies. GT is especially renowned for its application on study of human behaviour under field and close-to-real-life conditions.

GT therefore suggests the importance of findings and theorising based on reality, rather that hypothesis testing. In this research phase it is too early to propose a hypothesis that would scale down this research to a study of a particular phenomenon. At this point in the research the overall ontological picture of user interactions with electronic payment systems had to be built. While the diary study was guided and informed by the previously conducted research, for instance, taking into account the characteristics of EPSs, it was believed that applying open-minded approach of GT to the analysis of the diary data would gain many valuable and interesting results.

GT has established guidelines for conducting research and analysis. It is able to incorporate diverse type of data such as users' notes in diaries, interviews, questionnaires, literature, users' self report, and personal experiences of the researchers.

An important reason for choosing GT is making use of its systematic and, to an extent, traceable process, by which literature and survey results are combined with the findings of the diary study. Such analysis and synthesis, aimed to propose design guidelines is typically done ad hoc by researchers, which makes the validity of conclusions weaker than grounding the conclusions in the data. Reliance on GT methodology can counter possible threats to validity of the conclusions based on the study data.

In their work of applying GT in HCI research (Elliott, Jones, & Barker, 2002, p. 566) suggest that "HCI research as science, based on hypothetico-deductive methodology, leads to fine distinctions or observations which may not be as generalisable as desired. HCI as engineering science enables the identification of problems but does not add to the development of a deeper understanding of phenomena".

GT analysis process

There are three distinct processes of analysis involved in grounded theory, 1) open coding, 2) axial coding and 3) selective coding. These processes can be overlapping in analysis activities.

1) In GT, the process of categorising the data is called 'open coding'. Open coding is the process of scrutinizing, examination, comparing and conceptualising data. Open coding tries to establish concepts, relevant categories and their properties in raw data. For example, the codes of the diaries data in this phase could be 'trust in a bank', and 'fear of security risks'.

2) The process to investigate the relationship between categories is called 'axial coding'. Axial coding is most often used when categories are in an advanced stage of development. Axial coding is the process of relating categories and their properties to each other, via a combination of inductive and deductive thinking. Grounded theorists are trying to identify and emphasize causal relationships, and fit observations into a basic frame of generic relationships.

Table 4.1 Axial coding features, adapted from Strauss & Corbin (1990).

Element	**Description**
Phenomenon	The central idea, even, happening towards which a set of action or interactions is directed. In grounded theory it is sometimes the outcome of interest, or it can be the subject.
Causal conditions	The events or incidents that lead to the occurrence or development of a phenomenon.
Context	Represents a set of properties that pertains to a phenomenon. A set of conditions influencing the action or strategy.
Intervening conditions	The broad and general conditions bearing upon action/interaction strategies. These conditions include: time, space, culture, economic status, career, history, and individual biography, etc.
Action strategies	The purposeful, goal-oriented activities that are performed in response to the phenomenon and conditions.
Consequences	Outcomes or results of action and interaction, intended and unintended.

In the process of analysis the memo system proposed by Strauss and Corbin was used: "Writing theoretical memos is an integral part of doing grounded theory. Since the analyst cannot readily keep track of all the categories, properties, hypotheses, and generative questions that evolve from the analytical process, there must be a system for doing so. The use of memos constitutes such a system. Memos are not simply 'ideas'. They are involved in the formulation and revision of theory during the research process", (Corbin & Strauss, 1990, p. 10).

3) Selective coding is used to identify one central category, or 'core category' that correlates to all other categories in the theory. The process continues by relating all other categories to the core category, validating these relationships, and filling in categories that needed further refinement and development. The core category is the central category around all the other categories are integrated. "The core category must be the sun, standing in orderly systematic relationships to its planets", (Strauss & Corbin, 1990). There is a belief that such a core category always exists. The essential idea is to develop a single storyline to form the initial theoretical framework. The storyline de-

scribes the core category, and relationships of other categories to it. Selective coding is about finding the driver of the story. Theory is then based on the storyline and is its expression. For example, for the story line explaining how users develop trust for EPSs, 'Trust development' can be selected as the core category, while "Risk management" and 'Privacy Management' categories would be related to it.

Analysis of the diary study

In the analysis of this study open coding and axial coding stages were performed by the researcher. Open coding has identified basic categories. The set of the categories was open, and not predefined according to a preconceived theory. Axial coding has linked categories together, established subcategories and proposed explanation of users behaviour when using the systems.

The codes based on the diary entries reported by the participants were grouped into categories by the researcher. During the analysis the codes and then, consequently, the categories were written on paper cards and arranged in groups in the categorisation process. In the axial coding phase memos of relationships between the categories were written. A memo is an inductive step in generating theory from axial coding. An example of a memo is presented in Box 4.1.

Taking into account these findings, generic problem descriptions were identified and solutions were proposed on the basis of users opinions, positive findings of the study, practices of existing payment and e-commerce systems, causal relationships, or practices of human-computer interaction. For example, the users reported that they are inclined to use the payment systems with more confidence when they pay on behalf of their employing organisation or company. The conclusion can be drawn that fostering trust becomes more important for a system supporting personal payments.

Memo: Risks Management strategies
Users use several diverse strategies to alleviate risks, i.e. to convince themselves the risks are not likely to harm them. Risks Management is therefore a collection of strategies the users are employing to achieve comfort and accept the systems. (The strategies for Risks Management can be used for Trust Development and are important for user acceptance).

These strategies include reliance on:

- Absence of own negative experiences.
- Absence of negative experiences by others.
- The fact that there is little money on the bank account: risks are low and would not be financially damaging.
- The system is run by the bank (or an organisation), which they trust.
- Professionalism of the bank.
- A conversation with a bank employee who has assured it is safe.
- Guarantee from the operator that the money is safe with the system.
- Information in the booklet explaining the benefits of the EPS.
- The fact that the bank has won a prize for electronic banking services.
- Good previous client relationships with the bank.
- The EPS is safe — has never failed the user.
- Trust that the bank will make corrections and return money in case of an error. The system (and what happens with money within it) is the bank's responsibility.
- Users are not worried about what may happen.
- Reliance on mass media, which treat the system as a safe one.
- Nothing can go wrong with the bank, default in the banking system won't happen in our country.
- The bank would supply the system only if it were safe, and would not otherwise. Trust in safety measures: no one has broken in the system yet.

Box 4.1 Example of a memo on risk management.

Table 4.2 illustrates a snapshot of the analysis process. The right column describes the concepts found in the data, the left column represents categories of the identified problems. For example the finding coded as 'The user did not want to disclose her email address, because she was afraid they'll spam her' was related to problem category 'Absence of a policy on privacy can undermine trust in the system' with subcategory 'Lack of clarity or explanation how the personal details are used', Table 4.2. This problem could be related to problem 'Users may not trust the system that does not provide explanation on how personal details are used and why they are necessary, fearing misuse'. The problem categories were attempted to be related to wider concepts or characteristics of EPSs, as indicated by the letters in the beginning of a prob-

lem category. For example, 'TP' means that this problem relates to trust and privacy issues, and 'U' indicates a usability category.

The GT analysis looked into strategies, actions, thinking and reasoning behind user actions and behaviour, and tried to establish how they can be used to formulate solutions to the problems and to take into account the positive findings. In this respect, the solutions that inform design are grounded in the data and would fit the user behaviour and needs. These solutions were meant to be evaluated in the consequent validation experiment.

While this study employed GT for analysis, this methodology was not applied fully. GT was used to categorise problems and positive findings, and generate explanations about user attitudes, behaviour and experiences. GT in this respect was used as a structured approach for analysis of the raw data, which produced results that can be used in future analysis. This use of GT that stops at the concept generation is consistent with (Strauss & Corbin, 1990) who suggest that application of GT can stop at the stage of axial coding. It is not required that a theory should be the final output of the research if the concept development or theme analysis is enough for the further use of results.

More thorough application of GT would use parallel and iterative data collection. This study used one iteration in the collection of the qualitative data via the diary study. However, the initial analysis has started after the first diaries were finished and therefore the researcher was able to highlight and explore interesting points in the interviews.

The actual details of the analysis are too detailed and uninformative to be presented verbatim in the thesis. The analysis of more that 90 pages of the diaries and interview notes has discovered about 100 open codes and categories, and produced more than 80 memos. The analysis has produced a substantial amount of output, not all of which was relevant to the scope of this research.

Table 4.2 Example of the snapshot of axial coding with relationships identified in the data.
Legend. Codes of problem categories: TP – trust privacy, U – usability.

Problem categories	Information from the diaries and interviews
TP1. Unexpected or unexplained use of privacy data destroys trusts. TP 2. Users may not trust the system that does not provide explanation on how personal details are used and why they are necessary, fearing misuse	Banks are not supposed to draw conclusions from the information they know based on the client relationships
U2. Unnatural and not intuitive interaction process lowers performance and usability.	Acceptgiro, [a standard paper based transfer form] can be filled electronically. The system asks information not in the same order as the original paper version. E.g. users have to enter a code, which they normally are not aware of. >The user could not still get used to it after several months of payments.
U7. Low ease of use on the long term lowers performance (and make people long for an alternative) U8. Too 'strong' measures to ensure security, reliability, or anonymity may lower usability and performance	Design of hardware should be better: the buttons on the code calculator are too small, hard to press and fingers hurt
TP 4. Absence of a policy on privacy can undermine trust in the system + Lack of clarity or explanation how the details are used	The user did not like the question about her nationality, fearing some unexpected or harmful use. The user did not want to give email, because is afraid they'll spam her.
U8. Too 'strong' measures to ensure security, reliability, or anonymity may lower ease of use and performance New U9. Poor design of dedicated hardware may hamper usability and lower user acceptance	Use of the code calculator ° makes authentication more difficult (you have to have the calculator and carry it with you) ° is annoying, because you have to press small buttons ° is annoying, because you have to fill in several codes to make payments ° not ergonomic design BUT Users understand importance of authentication and are willing to use it.
TP 4.Absence of a policy on privacy can undermine trust in the system	Feeling of safety is based on: ° Information in the booklet ° Absence of an own negative experience ° Absence of negative experiences of others ° The fact that there is little money on the bank account: risks are low and would not be financially damaging.

Automatisation features:
- Enable saving of incomplete payments to be completed at a later date.
- Provide the functionality of triggering payments by time or event (e.g. email, SMS message, etc.)
- Provide the functionality of paying for subscriptions for content or services.
- Provide the functionality of scheduled or recurrent payments to be executed on a given date over a certain period of time.
- Provide the ability to make group payments to several parties at once.

Personalisation:
- Provide the functionality of: address books, profiling, retaining session information to avoid frequent re-logins, and saving users' preferences, that are helpful for efficiency of payments tasks.
- Provide support for currency conversion and different languages.
- Provide the functionality of: multiple logins, restricted access for employees or family members.

Control over the payment process and information
- Provide means to easily modify and control personal data, to recover passwords, or alternative authentication systems (e.g. biometrics, code calculators).
- Provide easy access to transaction statements to make control over transition easier and to help to detect problems.
- Provide clear and visible feedback on all payment task and actions.
- Provide possibility of error recovery, e.g. the ability to roll back to the default configuration of the system, or discard all information for a payment order.

Interaction and interface
- The duration of the payment procedure should be in proportion with the duration of the pre-purchase interaction phase, (see section 1.4.1), e.g., a fast purchase should not require a long payment.
- Avoid changes in the logic of interaction over time.
- Avoid frequent changes of user interface.

Privacy, security and help
- Provide clear and extensive help on critical questions such as fraud, security, insurance of funds, handling of personal information.
- Provide with explanations why the system is secure.
- Provide a clear privacy policy.
- User should have a minimal need in reliance on documentation (help, manuals).

Box 4.2 Subset of the proposals for design of EPSs.

The following section illustrates the findings of the analysis. The solutions for design of EPSs were identified on the basis of the data analysis. Following the practice of GT a theoretical memo with implications for payment systems was composed separately. The summary of certain findings is presented in Box 4.2.

Based on the way the diary study was conducted it can be concluded that it has discovered a sufficient number of problems and positive findings, that are comprehensive in their coverage, and therefore are a good basis of design recommendations. In the next stage of the analysis, the results were taken as an input to formulate design recommendations.

Summary of the results

This section renders interesting examples from the diary study in a concise form. The discovered problems and positive findings are grouped into corresponding categories.

Problems

- Users complained about usability aspects of the payment systems, especially with regard to the registration process. Certain security measures reported (long passwords, security questions, 1-hour long registration/installation process, entering multiple security codes) were perceived as “excessive” and “annoying”, and even prevented two participants from completing the registration.
- Inconsistency of online forms in comparison with the previous experience of the users (e.g., different order of filling of information compared to the paper form) was a problem. One payer could not get used to the electronic payment form, even after already using it for several months.
- Users were worried that third parties can get access to their personal information or their money (though this does not deter them from using the system). Others felt that their money is safe, but the personal information is not, and can be revealed to third parties in one way or another.
- Two participants who used PayPal trusted it very little. Their initial impression was that it is hard to trust PayPal, because of possible security risks.
- One user did not like to reveal her nationality and email; she felt the questions threaten her privacy.

Positive findings

- The expert payers found that Internet-based payment of bills, which would normally be paid by post, "saves time and brings convenience".
- Paying the exact amounts electronically was considered easier that in cash, because no change or exact amount of cash money is required.
- Preparing payments in a 'batch' and paying them later was convenient from the efficiency viewpoint, as well as for the user connecting to the Internet via a modem.
- The "address book" function for saving account details of payees was found convenient for repetitive payments, because it makes "it easier to fill in details of [frequent] payees".
- The integrated reporting system allowed easy overview for payment activities over time.
- Scheduled payments were welcomed as they give more control and flexibility over payments activities and improve efficiency. Executing payments on the previously set time was considered to be convenient.
- Participants trusted the banking payment systems because they relied on the bank behind the system and its ability to solve problems.

Design recommendations

The diary study has identified 36 problems that users experienced with online EPSs that could undermine user acceptance of these systems. The study has discovered also positive findings of users' experience with the systems. Implications for the design were, in some cases, directly recommended by the participants. A number of proposals that can inform EPSs design were outlined, Box 4.2. Taking this output to inform interaction design a set of 12 *design recommendations* (DR) has been defined.

The DRs were formulated based on the information originating mainly from the diary study as well as based on the knowledge obtained in earlier research of this thesis. To develop the design recommendations the data from the diary study, user survey and literature sources was grouped, analysed, and the prescriptive design recommendations were hypothesised based on this input. The design recommendations attempted to incorporate solutions to the problems discovered in the study, have taken into account positive findings of the diary study, and embraced the strategies that users employed in the interaction with the systems.

Each of these guidelines was written in an expanded form, adapting the templates used by Smith & Mosier (1986) and ISO 9241 (1996) for presenting user interface design guidelines. A design recommendation has a high level definition and detailed description that tries to embrace possible situations and propose related solutions. The short high-level definition of a guideline is shown as a header, typed in boldface. The detailed description, intended to specify and operationalise a guideline, is presented as bulleted points. The type of the design recommendation describes the relation of a DR to the characteristics of trust, privacy and usability, while general problem depicts what issues this DR is addressing. A design recommendation concludes with comments by an expert in development of new electronic payment systems and payment product at the Dutch bank Postbank.

An example of design recommendation 1 on security policy is presented in Box 4.3. The detailed description of all design recommendations is given in Appendix D. Below the design recommendations are presented in a concise form.

DR 1. Inform users about security measures and provide a security policy.

DR 2. Explain what type and details of personal information are to be retained, why, and how they will be used.

DR 3. Provide clear and explicit policy on privacy and make it noticeable to users.

DR 4. Give users control over the costs of the payment system usage.

DR 5. Allow users to control critical actions and information.

DR 6. Seek reputation and trust transference from reputed partners and technology providers, and communicate trust transference to users.

DR 7. Take measures to address risks and inform users about these measures.

DR 8. Interaction with the payment system should resemble users' expectations about the payments process.

DR 9. The interfaces should be presented in a logical, clear and understandable way.

DR 10. Provide features of automatisation of payments.

DR 11. Provide features of customization of payment environments.

DR 12. Provide well-designed authentication.

Till today, no such set of guidelines has been published for e-commerce EPSs. However, there is a clear overlap with general guidelines for the design of e-commerce web sites. For instance, a Nielsen-Norman Group (NN/g) report on e-commerce user experience suggests similar guidelines on privacy, costs and trust transference, (Nielsen, et al., 2000). Their guidelines "Build on the trust customers have for existing merchants and brands" and "Link to reputable independent sources" overlap with DR 6 on trust transference. Guidelines on Fair Pricing," Show total cost, as soon as possible", and "Justify prices that appear odd", partially overlap with DR 4 on control over the costs of the EPS' use.

The guidelines defined in the NN/g report are widely applied as state of the art practices for the design of e-commerce web sites. Still, the design recommendations developed in this research discover additional aspects and attempt to resolve issues, not covered by the NN/g report. For example, DR 5, 7, 8, 10, 11, 12, are novel and very specific in covering the design of online EPSs. Therefore, these design recommendations would be a highly valuable and concrete contribution to the field, if their validity can be demonstrated.

4.4 Conclusions

The diary study has recorded several usage problems and positive findings of end users, based on their experience with actual payments and in the context of actual use. This study was more concerned with actual design details that influence perceived ease of use, usability, privacy, trust and the eventual decision to use the system, rather than attitudinal variables affecting consumer behaviour, which were captured by user survey, reported in Chapter 3.

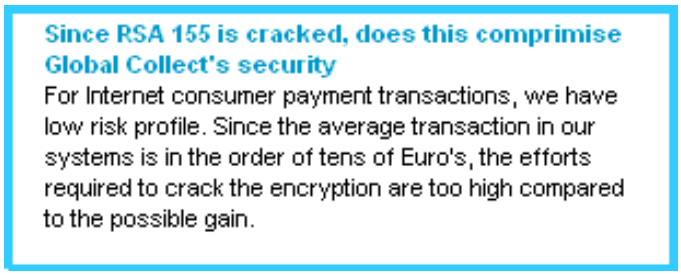
On the other hand, this study was able to elaborate more on social influences. The diary study has provided for this thesis a view of payments in the context of actual use and captured relevant user experiences and opinions. The study has uncovered positive aspects that users liked in the systems and what they thought can be improved. In certain cases, the users took the initiative in suggesting solutions for the problems they encountered. The diary study has found explanations about how and base on what reasons people develop their attitudes towards online EPSs. While many of the experiences recorded by the users could have been anticipated, this study is a valuable con-

tribution, also because a diary study of the user experience of EPS has not been reported before.

DR 1. Inform users about security measures and provide a security policy.

- Security policy: the existence and strength of security measures used in the payment system to protect users should be clearly explained to the users. This can be done by providing information in e.g. a paper manual, online help, or dedicating a part of the web site to the security policy.
- Provide clear visibility of security measures employed. This can be done by describing which security measures and technology have been implemented.
- Explain why the system is secure for transactions.
- Provide customer support (online or telephone) on security-related issues.
- Supply regular information updates on changes and upgrades in security and the security policy; show the date of the latest update.
- Address security issues specific to 1) a single payment (e.g. communicate to the users security of transactions), and to 2) the system's operations in general, (e.g. provide ability to deactivate passwords or block accounts offline by phone).
- If using services or technology from reputed security institutions or companies, inform the users about this cooperation, e.g. demonstrate security seals or logos of the security organisations.
- Explain which security measures are employed for information management and storage, provided that such information will not compromise security.
- Do not try to cheat hackers by providing wrong and misleading information. Hackers will know the real situation via different means, however the potential harm of misinforming the users may be inestimable for the reputation.

Example: Global Collect provides textual information in a dedicated help section describing which security solutions and measures have been implemented. It explains why the system is secure for transactions.



Source: Global Collect, July 2002.

Expert comments

The comments bellow belong to the expert consultant of the Postbank Department of New Business Technology:

'This design recommendation is testable by showing two different product brochures or websites (from accepting merchants).

In our test we have used:

Our trusted brand,
Brochure with information,
No [security] signs, logos.'

Box 4.3 Structured description of the DR 1 on security policy "Inform users about security measures and provide a security policy".

Implications for the design of Internet-based payment systems have been established. It has to be noted that only account-based systems were investigated in the diary study, but the results of the analysis can be possibly applied for other types of EPSs. The approach to the data analysis was systematic, based on the application of GT. It has resulted in a set of recommendations for design of EPSs, which are grounded in the data collected in this phase of the research.

The design recommendations at this point are hypothesised and their validity and applicability cannot be generalised outside the set of data used for the GT analysis. Based on the triangulation of research approaches taken by this thesis, the design knowledge should be validated from another research approach. Therefore, the design recommendations have to be validated in the subsequent experimental study before proposing their application for design of EPSs.

Chapter 5

Validating the Design Recommendations

5.1 Introduction

To verify the claim that the proposed design recommendations can actually benefit user acceptance of e-commerce electronic payment systems, a validation experiment was conducted. In this validation study the design recommendations were first applied to a redesign of an existing payment system, the Postbank Betaallijn (the Postbank Payment Line), and then an experiment was carried out to compare the old version and the redesigned version of the system.

5.1.1 Expert review of the design recommendations

In order to validate the design recommendations it is necessary to see if they can be applied to design or redesign of e-commerce EPSs, and if this will have an improving impact on how users perceive EPSs and on their subsequent acceptance.

An important requirement for design guidelines is that experts, who will apply them to design of payment systems, should be able to understand and apply them as a part of

their established design practice. Because it was difficult to consult experts in payment systems design, it was only possible to get the opinion of one practitioner in EPS design. This expert was asked to comment about applicability of the design recommendations.

This expert was a consultant at the Department of New Business Technology at the Dutch bank Postbank, responsible for the development and the proof of the concept of their new payment system 'the Postbank Betaallijn' designed to facilitate Internet and telephone-order payments. This expert tried to recognize the way in which the current implementation of the Postbank Betaallijn complies with the design recommendations and how they can be applied with the current version of the Betaallijn (see section 5.1.4 for the detailed explanation of the system). Since the reaction of only one expert was obtained, the agreement of other experts cannot be safely assumed. However, this opinion is presented along with the design recommendations, because the opinion of potential users of the DRs is valuable to qualify them. The experts' comments are included in the detailed account on the design recommendations in Appendix D.

The expert discovered that is was possible to evaluate most of the design recommendations with their system. The expert concluded that recommendations DR 1, DR 4, DR 5, DR 6, DR 7, DR 8, DR 9, and D 11 (see Appendix D) were applicable and the system already complied with the recommendations in one way or another.

DR2 and DR3 on personal information and privacy policy were considered to be applicable, but the Betaallijn did not comply with the recommendations, because the information on privacy was not provided in the system at the test stage. The possibility of the evaluation of DR 12 on authentication with the Betaallijn was questioned by the expert, who suggested that their password policy was already an established "model used for years". The correctness of DR 12 itself was not doubted.

According to the expert, the automatisation of payments, and therefore DR 10, was out of the intended scope of the Postbank Betaallijn, and is rather related to the domain of electronic banking, than to EPSs. The diary study has nevertheless demonstrated that automatisation may be beneficial to users of EPSs, therefore this recommendation was not excluded from the further validation.

5.1.2 Method

The following method was chosen to validate the 12 design recommendations:

- An existing payment system was evaluated against the set of the hypothesised DRs. This system was the Postbank Betaallijn; the version the Betaallijn before the redesign described below in section 5.1.4.
- A number of changes were proposed to be made to the system where it fails to meet the DRs of Appendix D, or does not meet them at the appropriate level. A new version of the system was created, implementing the relevant changes.
- Experimental tasks, that would let users experience and form an opinion about those aspects of the system that are affected by the DRs, were devised; see section 5.2.4 for more information about the experimental tasks.
- A questionnaire for measuring user attitudes was developed.
- Pilot testing, which included performing all tasks by 3 pilot subjects, was carried out in order to correct errors, and refine the test environment. The pilot tests were run on the final experimental design and the questionnaire. The setting was improved accordingly.
- The validation experiments were performed.
- The two versions of the EPS were compared along user attitudes, measured by means of the questionnaire. The differences between the systems were analysed statistically.

5.1.3 Hypothesis

The main hypothesis suggests that there will be a difference in users' attitudes towards the two versions of the system, which are caused by the design recommendations.

H_1 The application of the DRs significantly influences users' attitudes towards the redesigned system.

H_0 There is no effect of the application of the DRs, and no difference between user attitudes towards the systems.

User attitudes were measured by means of a questionnaire. See Appendix E for the detailed description of the questionnaire used in the experiment.

5.1.4 The system under test

The experiment was built on the basis of an EPS product called 'Payphone', developed by the Dutch company Comsys BV. The purpose of Comsys is to sell the payment system to banks. The payment system was adapted by Postbank, one of the top 5 Dutch banks, which was interested in the potential introduction of the payment system to its clients, branding it with the Postbank name. The adapted system was named 'De Postbank Betaallijn', (the Postbank Payment Line). Comsys and Postbank were interested in discovering the potential level of success of the system among users. At the moment the researcher contacted the company and Postbank, the payment system had finished the first trial of the concept among Postbank clients, which was a test of functionality, rather than a usability evaluation. By the time this study was conducted the Betaallijn system had not undergone rigorous user testing. Therefore the experiment provided a good opportunity for the parties to test the system against real users. The Postbank Betaallijn can be used for Internet and call center payments, in this thesis the focus was on Internet payments. In the remainder of this thesis, the initial version of the system is called 'Old system', and the redesigned version is called 'New system'.

After initiating payment orders on a merchant's web site, users interact with the system and authorise payments via telephone. From the user viewpoint, the system consists of two parts, the Payphone Betaallijn and the Postbank Betaallijn. When making telephone calls, the users are first connected to the Payphone part of the system, where they can manage and confirm their orders. After the initial confirmation, the users are connected, within the same telephone call, to the Postbank's part of the system where they can actually authorise payments.

The generic process of purchasing on the Internet with the Betaallijn works as following:

- After a customer has selected products to buy at an online shopping web site, he enters his own telephone number at the 'checkout' of the merchant's web site, which is an online form where the order and payment details are entered, and gives a confirmation to pay the products by submitting the form to the merchant's web site, (e.g. pressed button 'confirm payment').
- Then the customer dials the Betaallijn using the same telephone number he entered at the web site. The customer is greeted by the Payphone's part of the system.
- The customer's telephone number is recognised by the system and the matching amount(s) of the purchases made at the web site is played back to the customer.
- The customer interacts with the payment system via a fully automated Interactive Voice Response System (IVR). The customer selects options on a voice menu by pressing buttons on the phone, corresponding to the menu options.
- After a confirmation of the order, the customer is put through to the Postbank's part of system where he or she enters his/her account number at Postbank and the password of the Betaallijn system, and gives authorisation to actually make the payment.
- If the payment is done successfully, the confirmation about the payment is played back to the customer, describing the details of the effected payment.

Suppose a user wants to order a wall poster for €14.95 from web site Posters.nl. The user proceeds to the checkout, enters his or her fixed or mobile telephone number on the web site (e.g. 0401234567), confirms the payment and calls the Betaallijn number (0201234567) from the telephone, corresponding to the telephone number he or she has entered on the web site, (0401234567). The user will be connected to the first part of the dialog system, Payphone IVR (Interactive Voice Response System).

The dialog for one payment using the old system version as it was before the application of the design recommendations would look like the following:

Legend (V: Voice menu playback, A: User action).

V: Welcome to the Payphone Betaallijn system for the payment of your order.

We have an order for you for the amount of 14 euros 95 cents from Posters.nl.

To pay press 1, to repeat press 4, to cancel press 9.

A: By pressing 1 the user is connected to the Postbank Betaallijn IVR.

V: One moment please, we are transferring you to the Postbank Betaallijn.

Welcome to the Postbank Betaallijn.

Please enter your Postbank account number.

A: The user enters the account number.

V: Enter your PIN code.

A: The user enters the PIN code.

V: For the payment of the amount of 14 euros 95 cents to Posters.nl press 1, to cancel the payment press 9.

A: The user presses 1.

V: After your confirmation the payment will be immediately processed and transferred to Posters.nl. To authorise the payment of the amount of 14 euros 95 cents to Posters.nl press 1, to cancel the payment press 9.

A: The user presses 1.

V: Your payment is being processed, one moment please.

<Beep> Your payment has been processed successfully. Thank you for your payment.

(The user is transferred back to the first voice menu system of the Payphone Betaallijn).

V: Welcome back to Payphone Betaallijn system. Your payment has been received, thank you for your payment. There are no more orders for you. The connection will now be broken.

A: At this point the user hangs up.

The web shop receives the confirmation of the payment from Postbank and ships the goods. The amount is immediately deducted from the user's Postbank account.

According to the classification of EPSs, presented in Chapter 2 the Betaallijn system is an account-based debit system. The system has low anonymity, because all transactions are recorded in the user's bank account. The authorisation type is online and centralised. Interoperability of the system is assessed as low, because it is not likely that Postbank would allow other banks or parties to join the Betaallijn system. The values of the other characteristics of the Betaallijn system, such as trust or privacy, were not known at the time of the study and had to be investigated.

5.1.5 Changes made to the Postbank Betaallijn based on the DRs

The Postbank Betaallijn payment system was evaluated against the set of design recommendations, described in Appendix D. Changes that are applicable to this system and to the context of its use, were proposed. Subsequently, the relevant changes were effected into a new version of the system. This means that the validation experiment was restricted to the corresponding design recommendations. Below it is examined how the design recommendations were implemented in the redesigned system. Table 5.1 describes the differences between the systems after the design recommendations were applied.

DR1. Inform users about security measures and provide a security policy; and DR7. Take measures to address risks and inform users about these measures.

A security policy was introduced in the New system.

DR2. Explain what type and details of personal information are to be retained, why and how they will be used.

The privacy policy in the New system explained how personal details will be used.

DR3. Provide a clear and explicit policy on privacy and make it noticeable to users.

An extended privacy policy was introduced in the New system. Links to the privacy policy were added to the payment web pages in the New system.

DR4. Give users control over the costs of the payment system usage.

The users of the New system were informed by the system that they are calling a free number when connecting to the Betaallijn. Since the users of the Old system were call-

ing the Betaallijn from the laboratory telephone, they were informed by the system that they were calling a paid number, and were told by the experimenter in advance that the connection costs would be deducted from their participation fee, to stimulate thinking of the number as a paid one and to make them as cost-sensitive as for real-life payments (actually, no costs were deducted after the experiment).

DR5. Allow users to control critical actions and information.

The ability to block the passwords via the IVR menu was introduced in the New system.

DR6. Seek reputation and trust transference from reputed partners and technology providers, and communicate trust transference to users.

The logotype of Postbank was exposed on the web site for the New system.

DR8. Interaction with the payment system should resemble users' expectations about the payments process.

This design recommendation presumes that the interaction process could be rendered in a familiar way to users. From this respect the Betaallijn is similar to the existing telephone banking system of Postbank. It was hoped that the above-mentioned changes introduced by the DRs would result in a better interaction design and usability of the redesigned system. In case the system would not be intuitively understood by the users, the more detailed explanation of how the system operates was introduced for the New system in online help and the paper brochure.

DR10. Provide features of automatisation of payments.

The functionality of multiple (batch) payments was implemented, i.e. ability to make several payments with one authorization. The functionality of scheduled payments was implemented, i.e. ability to set the date for the payments execution.

DR12. Provide well-designed authentication.

The password length was changed: the PIN code for authorisation was reduced to 4 digits in the New system. The authentication process was augmented: the number of confirmations of a payment was reduced from 3 to 2 steps in the New system.

Table 5.1 Changes made to the system, the corresponding design recommendations, and the tasks designed to test the changes, (see tasks in section 5.2.4 below).

DRs	Old system	New system	Task
DR 1, DR 7. Security policy	Absent/ or minimal	Added / Present	Tasks 1-5
DR 2. Links to the privacy policy on payment screens at the merchant shop	Absent	Made salient on the payment page	Tasks 1-5
DR 3. Privacy policy	Standard Postbank style	Made more salient at Postbank web site	Tasks 1
DR 4. Costs	Paid number notification	Free number notification	Tasks 3, 5
DR 5. Blocking passwords	Via customer service only	Blocking passwords via the system	Task 2
DR 6. Logos	No (Postbank) logos at the payment page	Postbank logos are present at the payment page	Tasks 1-5
DR 8. Help means	Standard	Enhanced with information about security, blocking passwords, etc.	Tasks 1-5
DR 8. Interaction design	Standard	Enhanced by the DRs	Tasks 1-5
DR 10. Batch payments	No	Yes	Task 5
DR 10. Scheduled payments	No	Yes	Task 3
DR 12. Password length	6	4	Tasks 1-5
DR 12. Authentication	Standard: 3 steps	2 steps (1 step less)	Tasks 1-5

5.1.6 Subjects

The 46 subjects were recruited by the Postbank call center among the banks' clients who are familiar with Postbank's existing payment systems (e.g. Girofoon, Girotel; see Postbank.nl for more information). 25 subjects used the Old, and 21 used the New system. All participants had a good understanding of English. The summary of the demographic data collected through a pre-test questionnaire is listed in Table 5.2. In general, this sample is quite balanced to represent the most users' groups of interest well.

Table 5.2 Profiling of the participants of the study

Demographic parameter	Dimensions	System Version	
		Old	New
Age	<30	8	9
	31-50	11	10
	>50	6	2
Gender	Female	11	5
	Male	14	16
Internet payment systems experience	No	14	14
	Yes	11	7
Credit cards on the Internet	No	14	11
	Yes	10	9
Yearly income (€)	< 26 000	9	8
	27 000 - 36 000	5	2
	> 36 000	7	6
Computer experience	Low	2	0
	Moderate Low	5	3
	Moderately High	11	10
	High	7	7

The participants were divided in two groups based on the demographic criteria, although it was not always possible to ensure that the groups are completely balanced, due to scheduling constraints of the participants. The groups were checked on a demographic bias. Based on the statistical analysis of the comparison of the two groups, no significant difference for any of the six demographic criteria was found, see Table 5.3. It can be assumed that the samples are properly balanced along the demographic factors and experience with payment systems.

Table 5.3 Chi-Square Tests of the data sample

Demographic parameter	N	CHI^2	df	p
Age	46	1.772	2	.41 ns
Gender	46	2.051	1	.15 ns
Internet payment system experience	46	.545	1	.46 ns
Credit cards on the Internet	44	.049	1	.82 ns
Yearly income (€)	37	.760	2	.68 ns
Computer experience	45	2.017	3	.56 ns

5.2 Experimental setup

5.2.1 Overview

To simulate the online shopping experience, a working prototype of the website of an actual business that sells wall posters was created. The participants were requested to use the Betaallijn to purchase goods on this site. In order to bring realism to the experimental tasks it was not mentioned that the test web site is just a copy of the real one. The subjects were using a test Postbank account, and no money transfer was effected in reality, but this fact was not mentioned to the participants. All transactions were realistic in that they were experienced exactly as they would be during the actual use of the system in reality. The tests were conducted at the usability laboratory of the Eindhoven University of Technology (TU/e). The author of the thesis acted as an experimenter, i.e. facilitating the process, receiving subjects, introducing the system and the tasks, and keeping observation notes. During the tasks he was seated behind a one-way mirror.

The subjects were asked to find the best way for them to do the tasks. They were advised to use the paper brochure that was given to them, and online help, if necessary, but they were not obliged to do so. After each task they were required to fill in a questionnaire that assessed their attitudes towards the system, see Appendix E. When finished, the subjects were interviewed about their experience and were able to comment freely about the system. In the end they were given the full participation fee.

It took subjects from 56 to 140 minutes to complete the tasks. Subjects' interactions with the system were video-recorded. The videos were used as a back up and reference to the notes taken.

5.2.2 Dependent and independent variables

Dependent variables are measures of subjects' attitudes regarding the following system's aspects: batch payments, scheduled payments, password length, authentication, help means, security policy, blocking passwords, privacy policy, costs, usefulness, usability, trust, etc. The system version and the tasks are the *independent variables*.

Users' attitudes and opinions about aspects of the payment system under test were measured by means of a questionnaire, Appendix E. The questionnaire was designed to evaluate user attitudes to those aspects that were changed according to the design recommendations. Answers to the questions were measured by semantic differentials scales. Questions that can be interpreted as bipolar had scales ranging from –3 to +3; monopolar questions had scales from 1 to 7. The questions assessing usability of the system are a subset of SUS questionnaire, (Brooke, 1996); questions on perceived usefulness and perceived ease of use were adapted from Davis (1989). These questionnaires are validated tools that have been shown to be reliable, and are widely used, (Perlman, 2000). In addition, they are both quite short and generic which helped to create a concise questionnaire.

5.2.3 Experimental design

In this experiment there were a number of dependent measurements repeated for each task. The task is the independent within-subjects factor. The system version is the independent between subjects factor. The mixed experimental design can be described as A × (B); where A is the system version and B is the task factor. It is a 2 × 5 design, where the repeated factor has five levels, according to the 5 specified tasks, (Maxwell & Delaney, 2000).

1) System version (Two levels: Old version, New version)

2) Repeated measurements (Five levels: Task1, Task2, Task3, Task4, Task5).

To analyse the differences between the two systems, a general linear model analysis of ANOVA for repeated measures was performed with SPSS version 11.0. In this experiment there were a number of dependent measures taken only after certain tasks. They were used to gauge user attitudes to the systems' aspects specific to a particular task. For these measures, a one-way ANOVA was conducted, with only the system version as the independent variable.

5.2.4 Tasks

The subjects were provided with a 10-minute introduction to the system. They were told that Betaallijn is a payment system for Internet payments designed by Postbank and that the system gives the ability to pay online via a bank account of Postbank. The subjects were informed that the study would like to find out their attitudes, opinions, impressions and feelings about the Betaallijn.

The subjects had to perform five different tasks with the payment system. The reason that only 5 tasks were chosen for evaluation of 12 DRs is that certain systems aspects, (e.g. privacy, trust) are better evaluated in the contexts, rather than in a dedicated task, to avoid threats to ecological validity.

Task 1. Paying at a web site. Please browse Posters.nl web site, select and pay for an item you would like to purchase.

Task 2. Suppose you suspect that the PIN-code (payment code) of your account is stolen. Please find the best way to block your payment code, so that no one else can use it anymore.

Task 3. Suppose you have to pay rent for your house for a certain period of time. Please find the best way to arrange paying rent of €100 every month for 2 months (e.g. April and May). The rent has to be paid on the first day of the month, and should not be paid in one payment.

Task 4. Suppose that the PIN-code of your account is blocked and you would like to reactivate it. Please find out what would be the best way to reactivate the account.

Note. The users were asked only to find out how to do the task, since the reactivation of the account would require a physical or postal communication with the customer service, which could not be simulated.

Task 5. Suppose that you have to make 3-4 payments. Please go to *Posters.nl* web site, and select 3-4 items to purchase. Pay for these items in a way you think is the most efficient and fast.

Table 5.4 describes how the DRs map to the tasks and measures that are intended to test the desired effect of the DRs applied (measures are described in section 5.3).

5.2.5 Procedure

During the introduction a couple of examples were given to illustrate how the Betaallijn works. The participants were told how to select products and make payments at the web site. They were instructed how to use the telephone.

The participants were given a paper brochure and shown the Postbank Betaallijn web site describing how the system works. They could read this information if they wanted to, but were not obliged to do so. By this it was indented to simulate a real-life situation, e.g. at home, where the users would refer to help only in case of problems.

The participants were given the tasks and questionnaires in the paper form and were instructed to fill the questionnaire after every task. The subjects were told that they could ask a question whenever they did not know how to proceed, however, they were encouraged to find a solution on their own first. The experimenter communicated with the participants from the control room via an intercom system whenever it was necessary, this setup minimised possible influence on users of the experimenter's presence in the laboratory during the experiment.

The subjects who got confused or stuck were given about 5 minutes to find a solution. Then a general high-level hint was given to them, e.g. where to look at the web site on their own, or what they could try to do the task. If this did not help, they were given a more detailed instruction on how they could solve the problem.

If the subjects attempted to start filling the questions before completing the task, e.g. not making enough or any attempts to complete the task, they were asked why they did not do the task first. If necessary, they were given a hint, and requested to finish the task.

Experimental situations

Task1

Task1 was naturally understood by the participants and they had very little problems doing it. The most common issue was typing a wrong telephone number at the web site checkout, which was not recognised by the Betaallijn afterwards. This was remedied by checking the number and re-entering it again.

Table 5.4 Relationships between DRs, measures and tasks

Design recommendations	Measure	Tasks
DR 1. Security policy	RM2 SM4	1-5 4
DR 2. Personal details	RM3	1-5
DR 3. Privacy policy	SM1	1
DR 4. Costs	SM17 SM18, SM19	3 5
DR 5. Control of critical actions and information	SM3 SM15	2 2
DR 6. Trust transference	SM7	5
DR 7. Risks	RM1 SM2 SM16	1-5 2 2
DR 8. Interaction design/ Help means	RM 4, RM5, RM6-10 SM8	1-5 5
DR 10. Batch payments	SM9-11	3
DR 10. Scheduled payments	SM12-14	5
DR 12. Authentication / Password length	SM5 SM6 SM20	5 5 5

Tasks 2 and 4.

During task 2, which required blocking their account password, 10 participants tried to call the customer service line to do that. They were stopped at the moment they tried to dial the number. (During the experiment there was no actual and active customer service line with Postbank for the Betaallijn). Some of the participants asked the experimenter if they have to call service line and were instructed not to do so. When users had to reactivate their password in task 4, none tried to call the service line again, as instructed.

Task 3: Paying rent.

Task 3 was unnatural for some people and they refused to do it (2 participants), saying they would not pay rent in such way. In addition, the Old system did not have the option to enter the date for the payments' execution and therefore payments could not be made on the respective dates, which could make the task awkward for some users.

Task5: Multiple payments

The New system had the functionality of batch payments where users could pay several payments by grouping them together, and then giving a single authorisation about the whole amount. Eight users chose to do to it in the 'old' way, paying the orders one by one, and 3 combined the two ways of paying multiple payments, the rest used the multiple payments feature.

5.3 Results and Analysis

5.3.1 Results: Repeated measures

This section presents the most interesting results of the *repeated measures* (RMs) component of the experiment. The repeated measures are based on the users' answers to the five questions that were repeatedly asked as a part of the post-task questionnaire, thus there are 5 levels for every repeated measure. For example, the question "How do you assess your trust in the system?" was asked after each of the five tasks, to provide a standard measure of trust. Below the significant results are presented. The number of participants varies for different measures, because of the cases excluded due to missing data, where the participants opted for the 'don't know' answer.

RM1. A significant difference was observed between the systems in the *trust* measure, $F(1, 40) = 4.195$, $p = 0.047$. Users tend to trust the New system (mean 5.26) more than the Old one (mean 4.57). Figure 5.1 and Table 5.5 show the statistics and the chart of the results. There was a significant main effect in the within-subjects variable Task in this measure, $F(1, 4) = 3.083$, $p = 0.018$, which is based on a significant 4^{th} order effect, $F(1,1) = 5.997$, $p = 0.019$. There was no interaction effect between the 'system version' factor and the 'tasks' factor , $F(1, 4) = 0.563$, $p = 0.690$.

RM2. Overall the participants felt that it is *safer to use* the New system (mean 1.52) than the Old one (mean 0.82), see Figure 5.2 and Table 5.6, and this difference is significant, $F(1, 40) = 4.293$, $p = 0.045$. There was a significant main effect in the within-subjects variable task in this measure, $F(1, 4) = 3.262$, $p = 0.023$, which is based on a significant cubic order effect, $F(1,1) = 9.54$, $p = 0.004$. There was no interaction effect between the 'system version' factor and the 'tasks' factor, $F(1, 4) = 0.119$, $p = 0.952$.

RM3. The New system scored higher in user perception about *how personal information* is *protected* than the Old one, (Old 4.76, New 5.42), $F(1, 35) = 4.487$, $p = 0.041$. This is illustrated by Figure 5.3 and Table 5.7. There was no significant main effect in the within-subjects factor task in this measure, $F(1, 2.38) = 1.676$, $p = 0.188$, and no interaction effect between the 'system version' factor and the 'tasks' factor, $F(1, 4) = 0.326$, $p = 0.759$.

RM4. The participants *would use* the New *system* more *frequently* (New 1.04 vs. Old 0.06) than the Old one, (see Figure 5.4 and Table 5.8), $F(1, 36) = 4.368$, $p = 0.044$. There also was a significant main effect in the within-subjects variable task in this measure, $F(1, 4) = 3.497$, $p = 0.023$, which is based on a significant 4th order effect, $F(1,1) = 6.913$, $p = 0.013$. There was no interaction effect between the 'system version' factor and the 'tasks' factor, $F(1, 4) = 0.574$, $p = 0.611$.

RM5. The Old system scored surprisingly higher in users' evaluation of *ease of use* than the redesigned New system (Old 2.20 vs. New 1.61, Figure 5.5 and Table 5.9), and this difference is significant $F(1, 34)= 5.353$, $p = 0.027$. There was a significant main effect in the within-subjects factor task in this measure, $F(1, 4) = 3.31$, $p = 0.013$, which is based on a significant linear effect, $F(1,1) = 5.705$, $p = 0.023$ and a significant 4th order effect $F(1,1) = 4.64$, $p = 0.038$. There was no interaction effect between the 'system version' factor and the 'tasks' factor, $F(1, 4) = 0.574$, $p = 0.611$.

For all remaining repeated measures (RM6-10), no significant between-subjects main effect in differences between the systems was found. Tables 5.10 - 5.14 and corresponding Figures 5.6 - 5.10 summarise the non-significant results of the repeated measures analysis.

RM6. *Found the system complex*. There was a significant main effect in the within-subjects factor 'task' in this measure, $F(1, 4) = 6.747$, $p = 0.0$, which is based on a significant linear effect, $F(1,1) = 11.762$, $p = 0.01$ and a significant cubic effect $F(1,1) = 6.915$, $p = 0.012$. There was no interaction effect between the 'system version' factor and the 'tasks' factor, $F(1, 4) = 0.29$, $p = 0.865$.

RM7. *System's functions are well integrated*. There was a significant main effect in the within-subjects factor 'task' in this measure, $F(1, 4) = 4.400$, $p = 0.002$, which is based on a significant linear effect, $F(1,1) = 8.540$, $p = 0.006$ and a significant 4th order

effect $F(1,1) = 6.767$, $p = 0.014$. There was no interaction effect between the 'system version' factor and the 'tasks' factor, $F(1, 4) = 0.966$, $p = 0.333$.

RM8. *Felt confident using the system*. There was a significant main effect in the within-subjects factor 'task' in this measure, $F(1, 4) = 3.575$, $p = 0.008$, which is based on a 4th order effect, $F(1,1) = 6.510$, $p = 0.015$. There was no interaction effect between the 'system version' factor and the 'tasks' factor, $F(1, 4) = 0.067$, $p = 0.796$.

RM9. *Need to learn a lot of things before using the system*. There was a significant main effect in the within-subjects factor 'task' in this measure, $F(1, 3.15) = 2.996$, $p = 0.031$, which is based on a significant linear effect, $F(1,1) = 6.986$, $p = 0.011$. There was no interaction effect between the 'system version' factor and the 'tasks' factor, $F(1, 4) = 0.966$, $p = 0.333$.

RM10. *The instructions on the web page and the paper help were useful for the task*. There was a significant main effect in the within-subjects factor 'task' in this measure, $F(1, 4) = 10.506$, $p = 0.0$, which is based on a significant linear effect, $F(1,1) = 11.692$, $p = 0.002$ and a significant 4th order effect $F(1,1) = 20.011$, $p = 0.0$. There was no interaction effect between the 'system version' factor and the 'tasks' factor, $F(1, 4) = 0.334$, $p = 0.855$.

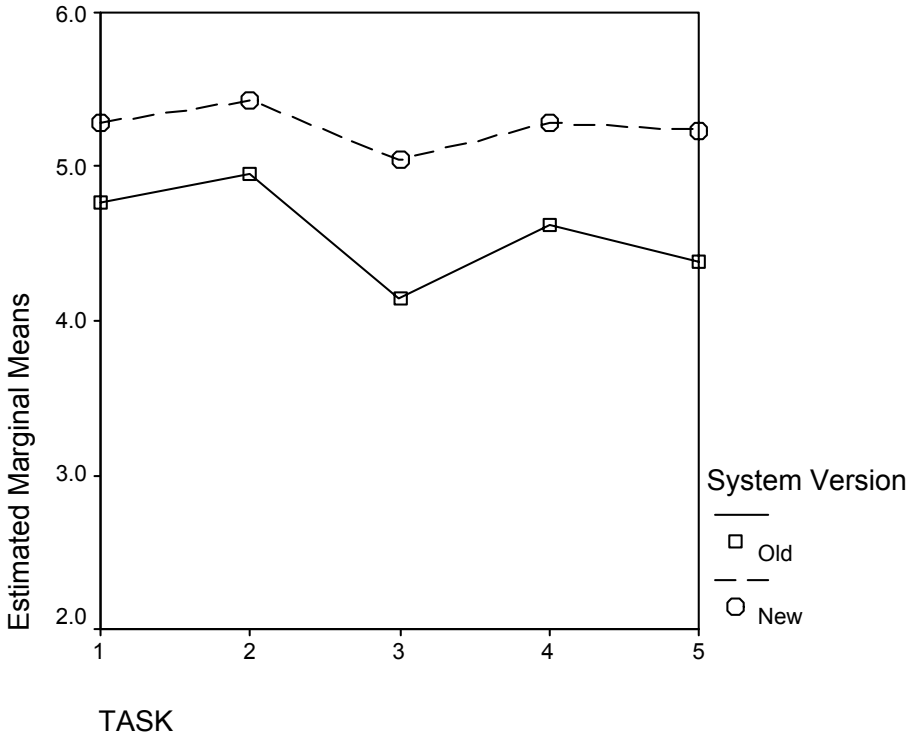


Figure 5.1 RM1. Measure 'trust in the system' (monopolar scale [1..7])

Table 5.5 RM1. Measure 'trust in the system'.

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	24.69	1	24.685	4.195	. 047
Within Groups	235.37	40	5.88		

	Task1		Task2		Task3		Task4		Task5		Total	
System Version	Old	New	Old	New	Old	New	Old	New	Old	New	Old	New
Mean	4.76	5.29	4.95	5.43	4.14	5.05	4.62	5.29	4.38	5.24	4.57	5.26
Std. Dev.	1.64	.96	1.28	.81	1.82	1.24	1.28	.90	1.69	1.09		
N	21	21	21	21	21	21	21	21	21	21	21	21

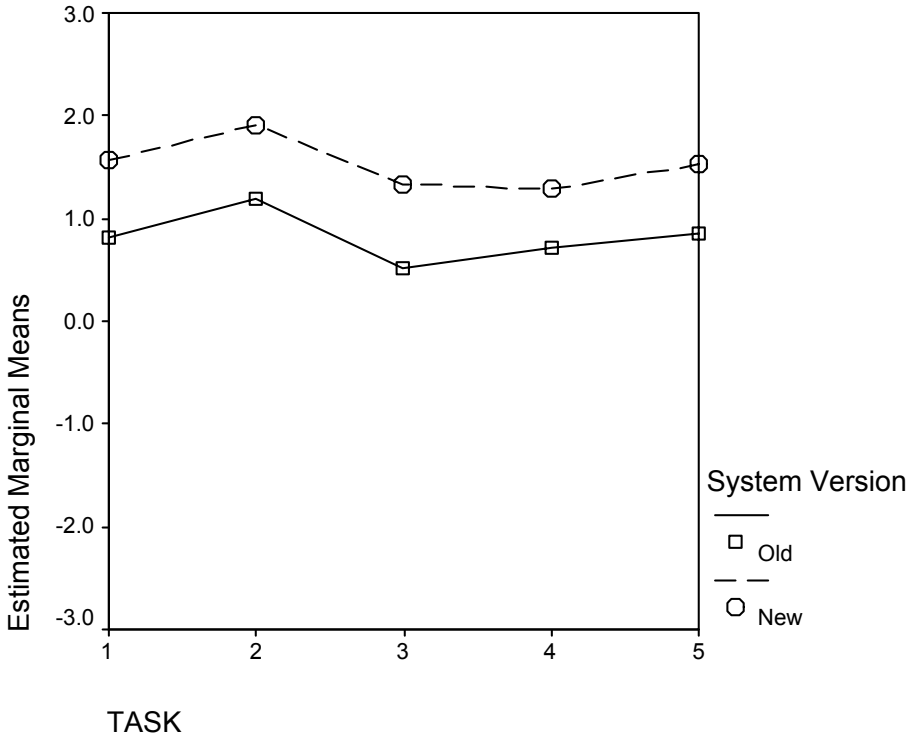


Figure 5.2 RM2. Measure 'Safe to use the system', (bipolar scale [-3..0..+3]).

Table 5.6 RM2. Measure 'Safe to use the system'.

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	26.076	1	26.076	4.293	.045
Within Groups	242.952	40	6.074		

	Task1		Task2		Task3		Task4		Task5		Total	
System Version	Old	New	Old	New	Old	New	Old	New	Old	New	Old	New
Mean	.81	1.57	1.19	1.90	.52	1.33	.71	1.29	.86	1.52	.82	1.52
Std. Dev.	1.78	.87	1.29	.83	1.78	1.35	1.68	1.06	1.42	.93		
N	21	21	21	21	21	21	21	21	21	21	21	21

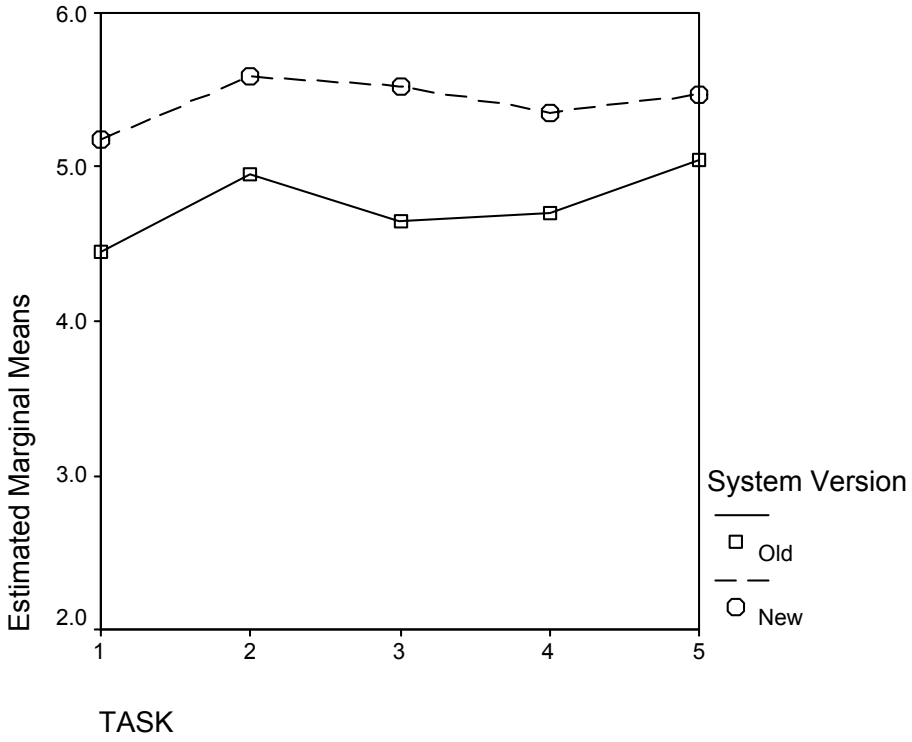


Figure 5.3 RM3. Measure 'how personal information is protected', (monopolar scale [1..7]).

Table 5.7 RM3. Measure 'how personal information is protected'.

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	2.229	1	2.229	4.487	.041
Within Groups	157.793	35	4.508		

	Task1		Task2		Task3		Task4		Task5		Total	
System Version	Old	New	Old	New	Old	New	Old	New	Old	New	Old	New
Mean	4.45	5.18	4.95	5.59	4.65	5.53	4.70	5.35	5.05	5.47	4.76	5.42
Std. Dev.	1.64	1.01	1.39	1.06	1.76	.72	1.34	.86	1.05	.80		
N	20	17	20	17	20	17	20	17	20	17	21	17

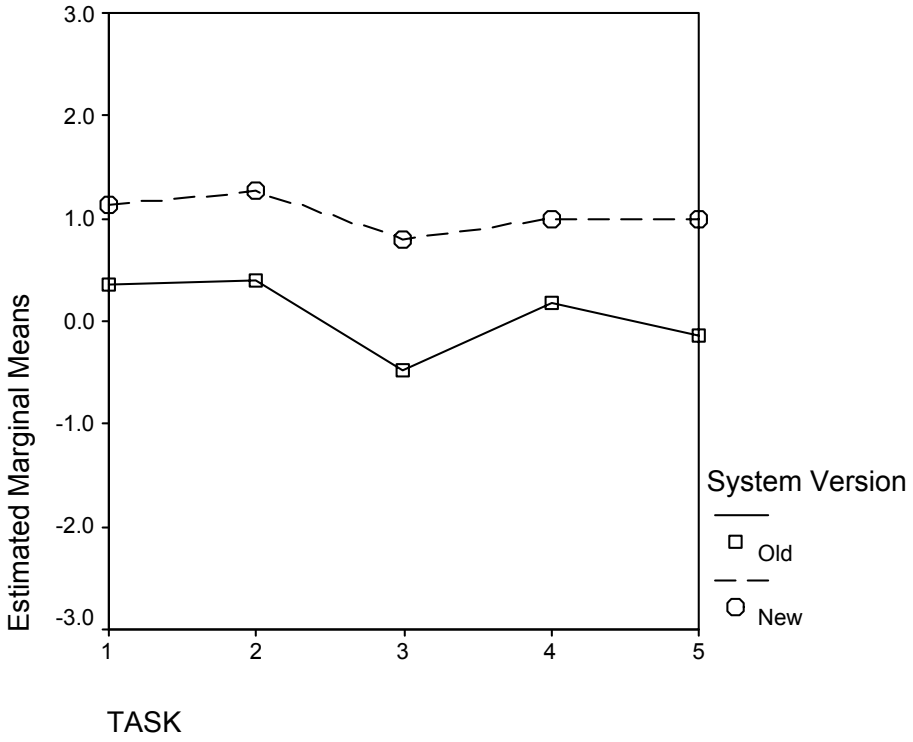


Figure 5.4 RM4. Measure 'Would use the system frequently', (bipolar scale [-3..0..+3]).

Table 5.8 RM4. Measure 'Would like to use the system frequently'.

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	43.520	1	43.520	4.368	.044
Within Groups	358.654	36	9.963		

	Task1		Task2		Task3		Task4		Task5		Total	
System Version	Old	New	Old	New	Old	New	Old	New	Old	New	Old	New
Mean	.35	1.13	.39	1.27	-.48	.80	.17	1.00	-.13	1.00	0.06	1.04
Std. Dev.	1.85	1.06	1.80	.80	1.90	1.15	1.83	1.13	2.01	1.00		
N	23	15	23	15	23	15	23	15	23	15	23	15

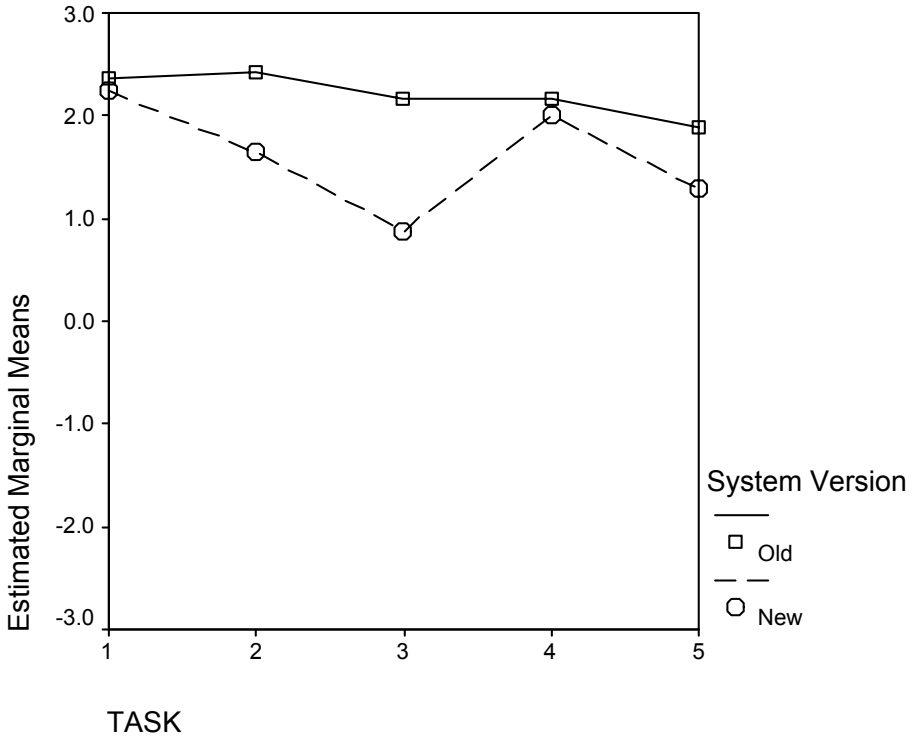


Figure 5.5 RM5. Measure 'Ease of use of the system', (bipolar scale [-3..0..+3]).

Table 5.9 RM5. Measure 'Ease of use of the system'.

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	15.523	1	15.523	5.353	.027
Within Groups	98.588	34	2.900		

	Task1		Task2		Task3		Task4		Task5		Total	
System Version	Old	New	Old	New	Old	New	Old	New	Old	New	Old	New
Mean	2.37	2.24	2.42	1.65	2.16	.88	2.16	2.00	1.89	1.29	2.20	1.61
Std. Dev.	.76	.75	.61	1.50	1.07	1.87	1.01	1.17	1.29	1.86		
N	19	17	19	17	19	17	19	17	19	17	19	17

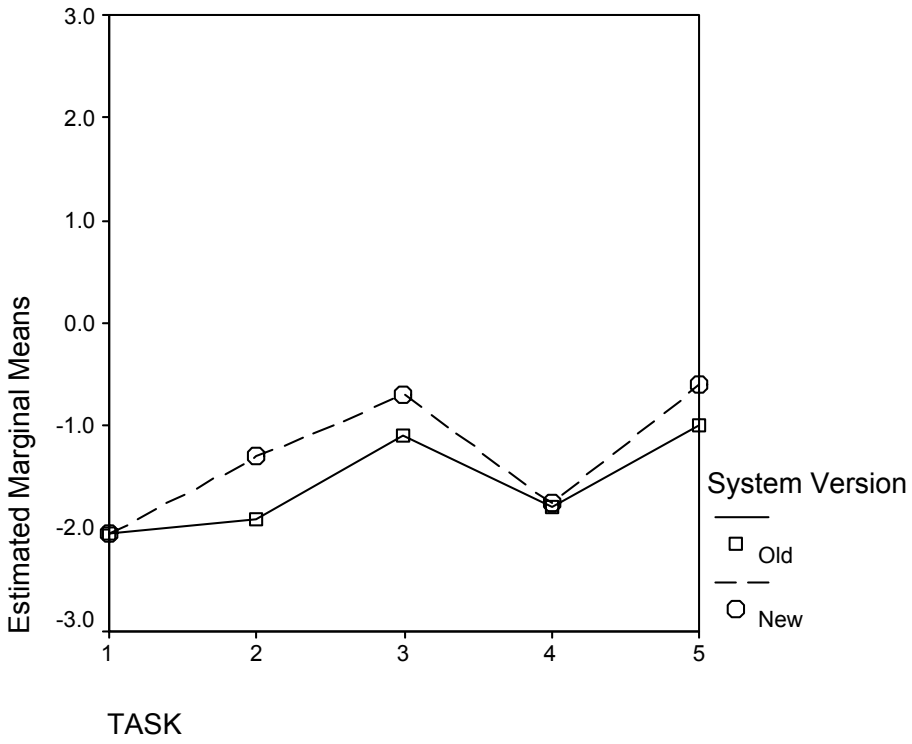


Figure 5.6 RM6. Measure 'Found the system complex', (bipolar scale [-3..0..+3]).

Table 5.10 RM6. Measure 'Found the system complex'.

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	4.351	1	4.351	.591	.447, ns.
Within Groups	302.021	41	7.366		

	Task1		Task2		Task3		Task4		Task5		Total	
System Version	Old	New	Old	New	Old	New	Old	New	Old	New	Old	New
Mean	-2.04	-2.05	-1.91	-1.30	-1.09	-.70	-1.78	-1.75	-1.00	-.60	-1.56	-1.28
Std. Dev.	1.11	1.00	1.70	1.78	1.98	2.08	1.54	1.68	2.11	1.98		
N	23	20	23	20	23	20	23	20	23	20	23	20

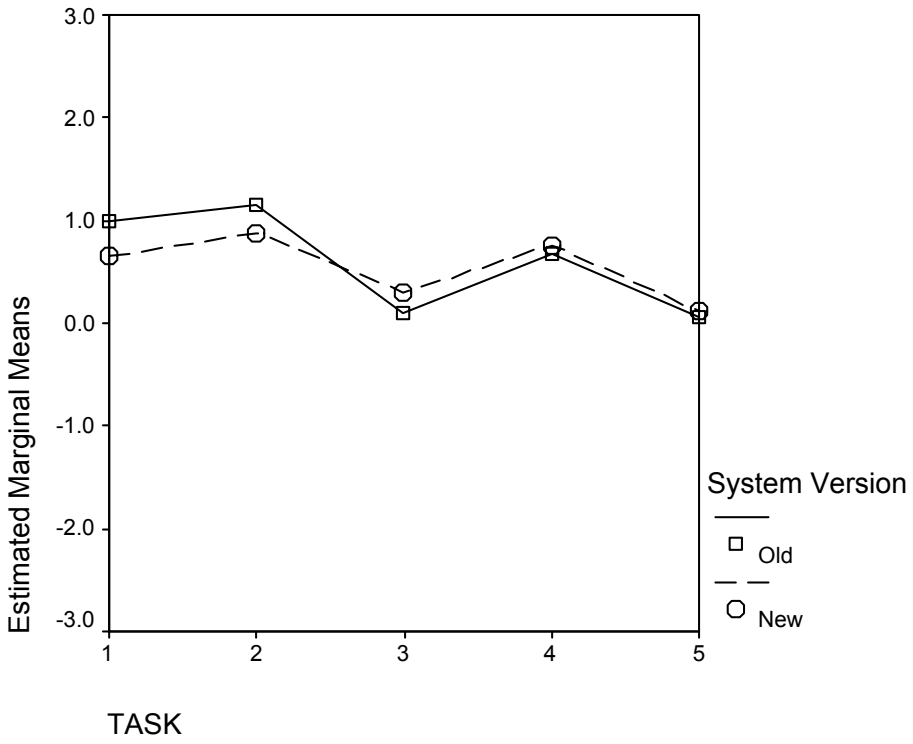


Figure 5.7 RM7. Measure 'System's functions are well integrated', (bipolar scale [-3..0..+3]).

Table 5.11 RM7. Measure 'System's functions are well integrated.

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	.155	1	.155	.023	.88, ns.
Within Groups	229.506	34	6.75		

	Task1		Task2		Task3		Task4		Task5		Total	
System Version	Old	New	Old	New	Old	New	Old	New	Old	New	Old	New
Mean	1	.65	1.16	.88	.11	.29	.68	.76	.05	.12	.60	.54
Std. Dev.	1.56	1.46	1.30	1.69	2.03	1.45	1.34	1.30	1.72	1.58		
N	19	17	19	17	19	17	19	17	19	17	19	17

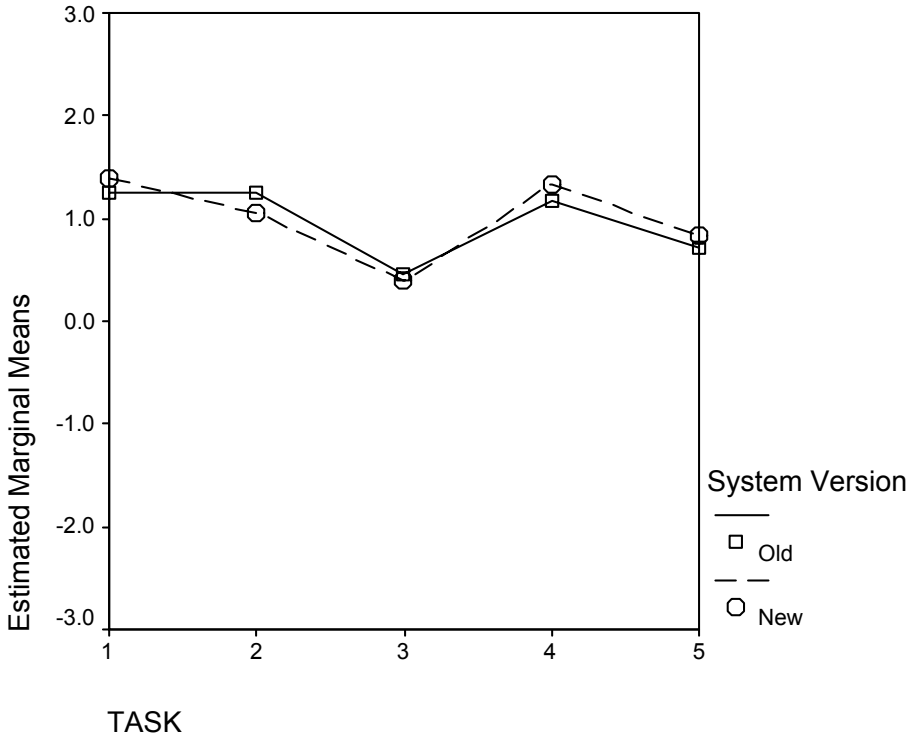


Figure 5.8 RM8. Measure 'Felt confident using the system', (bipolar scale [-3..0..+3]).

Table 5.12 RM8. Measure 'Felt confident using the system'.

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	.057	1	.057	.009	.927, ns.
Within Groups	268.267	40	6.707		

	Task1		Task2		Task3		Task4		Task5		Total	
System Version	Old	New	Old	New	Old	New	Old	New	Old	New	Old	New
Mean	1.25	1.39	1.25	1.06	.46	.39	1.17	1.33	.71	.83	.97	1.00
Std. Dev.	1.94	1.09	1.75	1.43	1.91	1.75	1.49	1.37	1.73	1.34		
N	24	18	24	18	24	18	24	18	24	18	24	18

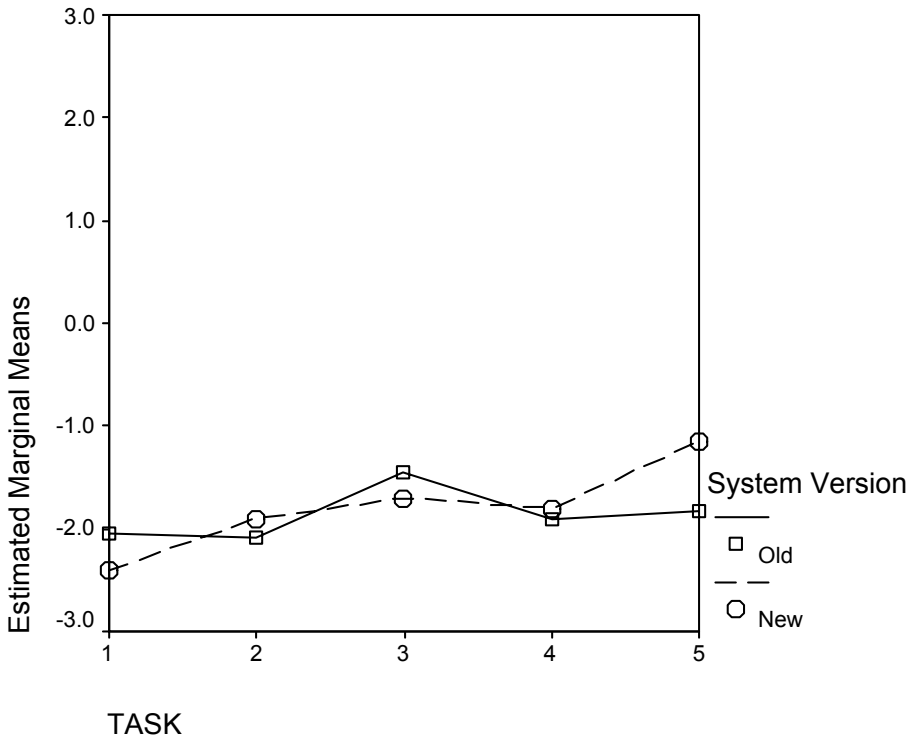


Figure 5.9 RM9. Measure 'Need to learn a lot of things before using the system', (bipolar scale [-3..0..+3]).

Table 5.13 RM9. Measure 'Need to learn a lot of things before using the system'.

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	.321	1	.321	.037	.848, ns.
Within Groups	362.057	42	8.62		

	Task1		Task2		Task3		Task4		Task5		Total	
System Version	Old	New	Old	New	Old	New	Old	New	Old	New	Old	New
Mean	-2.04	-2.4	-2.08	-1.9	-1.46	-1.7	-1.92	-1.8	-1.83	-1.15	-1.87	-1.79
Std. Dev.	1.63	1.10	1.47	1.83	1.72	1.78	1.67	1.61	1.74	1.95		
N	24	20	24	20	24	20	24	20	24	20	24	20

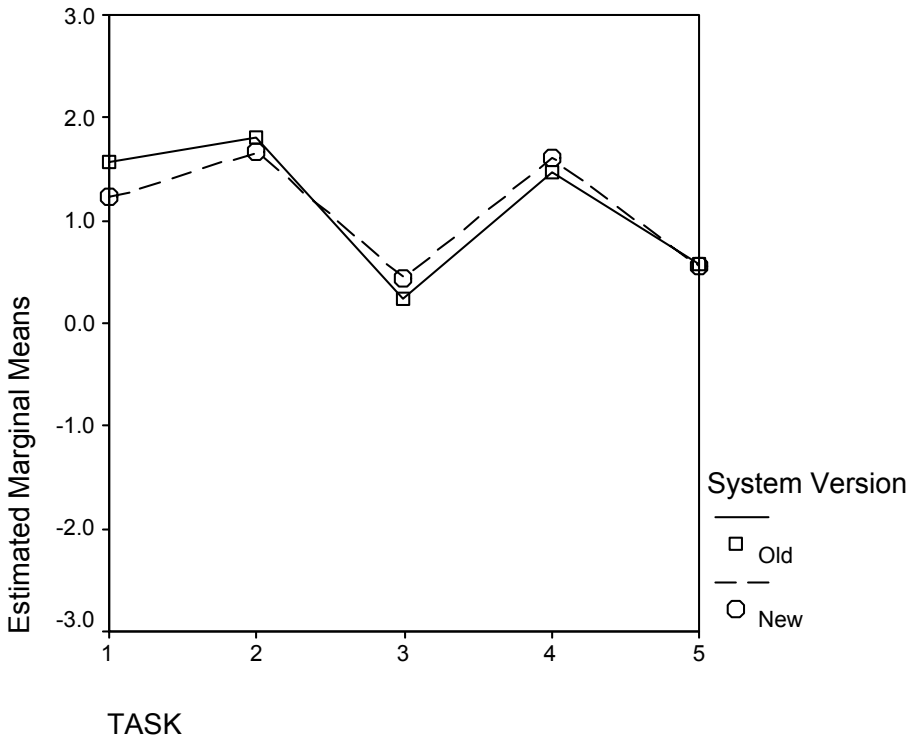


Figure 5.10 RM10. Measure 'The instructions on the web page and the paper help were useful for the task', (bipolar scale [-3..0..+3]).

Table 5.14 RM10. Measure 'The instructions on the web page and the paper help were useful for the task'.

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	.053	1	.053	.01	.921, ns.
Within Groups	198.633	37	5.368		

	Task1		Task2		Task3		Task4		Task5		Total	
System Version	Old	New	Old	New	Old	New	Old	New	Old	New	Old	New
Mean	1.57	1.22	1.81	1.67	.24	.44	1.48	1.61	.57	.56	1.13	1.10
Std. Dev.	1.08	1.31	1.44	1.41	1.90	1.58	1.44	1.54	1.57	1.50		
N	21	18	21	18	21	18	21	18	21	18	21	18

5.3.2 Results: Task Specific Measurements

After each task several measurements of user' attitudes, *specific* to the task (SMs), were collected. These measurements were intended to evaluate users' opinions about particular aspects of the systems after each task; see Table 5.4 for the mapping of the questions to the tasks. For these measurements the two systems were compared with a one-way ANOVA. The ANOVA was performed with users' responses as the dependent variable and the system version as the independent variable (between-subject factor). Several measures indicated significant differences between the two system's versions.

1. Personal information

SM1. The participants indicated that they were significantly more comfortable to use personal information with the New system than with the Old system, $F(1, 42) = 5.106$, $p = 0.029$, see Table 5.15.

2. Influence of **security information upon trust in the system**

SM2. The information about security provided to the users of the payment system contributed to higher trust of the New system in this aspect, $F(1, 43)= 4.389$, $p = 0.042$, see Table 5.15.

3. Ability to block the payment code gives a sense of control over the situation

SM3. The users of the New system considered that the way the payment code can be blocked in the New system gave them significantly more sense of control than using the Old system, $F(1, 44) = 5.161$, $p = 0.028$, see Table 5.15.

4. Safety of the system use

SM4. The participants considered that it is significantly safer to use the New system than the Old system, $F(1, 39) = 5.067$, $p = 0.030$, see Table 5.15.

5. Authorisation in the system

SM5. The users were more **comfortable** with the way they can **identify themselves** to the New system than to the Old one, $F(1, 41) = 5.451$, $p = 0.024$, see Table 5.15.

6. The length of the payment code

SM6. The differences in the length of the payment code (6 in the Old version, and 4 in the New system) are considered to be significant. The 6-digit password appears a bit

too long (-0.33), while the 4-digit password appears a little too short (0.24), $F(1, 43) = 6.795$, $p = 0.013$, see Table 5.15. However, the length of the 4-digit password is closer to the middle of the bipolar sale, which is zero (0.00), and this is a slightly better result for the New system than for the Old one.

7. The branding of Postbank influences trust

SM7. The fact that the system was introduced by Postbank influenced positively users' opinion about the trust in the New system (Old 1.52, New 2.10), $F(1, 41)= 4.650$, $p = 0.037$, see Table 5.15.

8. Would use the system in the future (perceived usefulness)

SM8. The New system scored significantly higher than the Old one in perceived usefulness of the system, $F(1, 43) = 7.363$, $p = 0.01$, see Table 5.15.

9. Multiple payments

SM9. The users' perception of the speed of making several payments was significantly better in the New system than in the Old system, $F(1, 44) = 4.169$, $p = 0.047$, see Table 5.15.

SM10. This can be linked to perceived usefulness of the multiple payment feature in the New system version. It showed significant results $F(1, 41) = 5.100$, $p = 0.02$, see Table 5.15.

SM11. For ease of use of multiple payments there was no significant differences between the systems, $F(1, 42) = 0.096$, ns., see Table 5.15.

10. Scheduled payments

SM12. The usefulness of scheduled payments in the New system was considered significantly higher in the New system than in the Old one, which can be attributed to the scheduled payment functionality implemented in the New system, $F(1, 41)= 5.500$, $p = 0.023$, see Table 5.15.

SM13. There was no significant difference between the systems for ease of use of scheduled payments, $F(1, 39) = 0.165$, ns., see Table 5.15.

SM14. There was no significant difference between the systems in speed of scheduled payments, $F(1, 41) = 0.089$, ns., see Table 5.15.

11. Other results

SM15. The attempt to assess if the ability to block the payment code influences trust, has not delivered significant results $F(1, 44) = 0.053$, ns., see Table 5.15.

SM16. The question how a customer service line operated by real people would affect trust has not indicated a significant difference between the systems, $F(1, 43) = 0.284$, ns., see Table 5.15.

There was no significant difference between the systems in the measure if paying for the telephone call to the Betaallijn would be appropriate for the users, SM18, $F(1, 44) = 0.675$, ns., or how much the users of both systems would be prepared to pay for the call, SM17, $F(1, 41) = 0.045$, ns., see Table 5.15. The means indicate that the users would be prepared to pay about 2-3 cents for the call, which equals to the standard tariff for the short-distance calls in the Netherlands on January 2004.

SM19. There was no difference between the systems in the measure if the users felt they would be in control of the costs of the Betaallijn usage, $F(1, 42)= 0.225$, ns., see Table 5.15.

SM20. In task 5, where the users had to make multiple payments, the number of confirmations was considered to be slightly excessive for both systems without a significant difference, $F(1, 42) = 0.147$, ns., see Table 5.15.

Table 5.15 summarises these results, listing the means for the measures, the level of significance and F-statistics. The number of answers N varies for various measures, because of the cases excluded due to missing values, where the participants opted for the ‘don’t know’ answer.

Table 5.15 Results of task specific tests
(* — bipolar scale [-3..0..+3], † — monopolar scale [1..7])

Dependent variable	System version	N	Mean	Std. dev.	df	F	p
SM1. Comfortable to use personal Information with the system†	Old	24	4.79	1.91	1, 42	5.106	.029
	New	20	5.85	.93			
SM2. Security information provided influences trust*	Old	24	.33	1.52	1, 43	4.389	.042
	New	21	1.14	.96			
SM3. Ability to block the payment code gives control over the situation*	Old	25	1.04	1.56	1, 44	5.161	.028
	New	21	1.90	.83			
SM4. Safe to use the system†	Old	22	4.64	1.49	1, 39	5.067	.030
	New	19	5.58	1.12			
SM5. Are comfortable with the way they can identify themselves in the system*	Old	25	.52	1.96	1, 43	5.451	.024
	New	21	1.05	1.19			
SM6. The length of the payment code (too long, too short)*	Old	24	-.33	.70	1, 43	6.795	.013
	New	21	.24	.76			
SM7. The branding of Postbank influences trust*	Old	23	1.52	.94	1, 41	4.650	.037
	New	20	2.10	.78			
SM8. Would use the payment system in the future*	Old	25	-.12	1.98	1, 43	7.363	.010
	New	20	1.30	1.38			
SM9. Multiple (batch) payments: speed†	Old	25	2.28	1.76	1, 44	4.169	.047
	New	21	3.38	1.88			
SM10. Multiple (batch) payments: usefulness*	Old	24	-.71	1.87	1, 42	5.100	.002
	New	20	1.11	1.66			
SM11. Multiple (batch) payments: ease of use†	Old	24	4.54	2.10	1,42	.096	.758, ns.
	New	20	4.35	1.95			
SM12. Scheduled payments: usefulness*	Old	23	-.35	1.96	1, 41	5.55	.023
	New	20	.90	1.41			
SM13. Scheduled payments: ease of use*	Old	22	-.35	2.17	1, 39	.165	.687, ns.
	New	19	.90	1.70			
SM14. Scheduled payments: speed†	Old	23	1.52	1.85	1, 41	.089	.767, ns.
	New	20	2.10	1.97			
SM15. Ability to block the payment code influences trust*	Old	25	1.04	1.18	1,44	.053	.819, ns.
	New	21	1.9	1.22			
SM16. Customer service line operated by real people influences trust*	Old	21	1.24	1.10	1, 43	.284	.597, ns.
	New	46	1.28	1.14			

Dependent variable	System version	N	Mean	Std. dev.	df	F	p
SM17. How much would you be prepared to pay for the call? †	Old	23	2.22	1.08	1, 41	.045	.833, ns.
	New	20	2.15	.98			
SM18. Would paying for the telephone call be appropriate for you? †	Old	25	3.68	1.77	1, 44	.675	.416, ns.
	New	21	3.24	1.86			
SM19. Do you feel you would be in control of the costs of the Betaallijn usage? †	Old	25	3.8	1.75	1, 43	.225	.638, ns.
	New	20	4.05	1.76			
SM20. Number of confirmations is appropriate*	Old	24	-.71	1.80	1, 42	.147	.704, ns.
	New	20	-.9	1.44			

5.4 Discussion

This section discusses how the findings of the experiment reflect upon the validity of the design recommendations. The summary provided in Table 5.16 and Table 5.17 illustrates the relation between the experimental measures and the design recommendations.

5.4.1 Validation of the design recommendations

DR 1. Security measures, applied to the redesign of the New system have resulted in a better assessment of the New system by the participants. The information about security contributed to the better rating of the New system in the aspect how *safe it is to use the system*, RM2, Figure 5.2 and Table 5.6. The participants have also considered that it was safer to use the New system in measure SM4, Table 5.15. It can be interpreted as an evidence of the successful validation of DR 1 on security measures and security policy.

DR 2. As the proof of DR 2 on personal information, the observation can be exploited that the New system scored higher in users' perception about how *personal information* is protected in the system, RM3, Figure 5.3 and Table 5.7.

Table 5.16 Design recommendations with confirmed validation

Design recommendations	**Experiment Results**	**Validation Status**	
DR 1. Inform users about security measures and provide a security policy	RM2. It is '*safer to use*' the New system. SM4. 'Safe to use the system' is rated higher in the New system.	Confirmed	✓
DR 2. Explain what type and details of personal information are to be retained, why, and how they will be used	RM3. Personal information is protected better in the New system.	Confirmed	✓
DR 3. Provide clear and explicit policy on privacy and make it noticeable to users	SM1. More comfortable to use personal information with in the New system.	Confirmed	✓
DR 5. Allow users to control critical actions and information	SM3. Ability to block the payment code gives more control over the situation in the New system.	Confirmed	✓
DR 6. Seek reputation and trust transference from reputed partners and technology providers, and inform users about such partnerships	SM7. The branding of Postbank influences trust: higher in the New system.	Confirmed	✓
DR 7. Take measures to address risks and inform users about these measures	RM1. Trust in the New system is rated higher. SM2. Security information influences trust: higher in the New system.	Confirmed	✓
DR 10. Provide features of automatisation of payments	SM0. Speed of the multiple payments is perceived higher in the New system. SM10. The usefulness of the scheduled payments is perceived higher in the New system.	Confirmed	✓
DR 12. Well-designed Authentication	SM5. Users are comfortable with the way they can identify themselves in the system. SM6. The length of the payment code makes difference between the two systems.	Confirmed	✓

Table 5.17 Design recommendations which were not confirmed during the experiment

Design recommendations	Experiment Results	Validation Status	
DR 4. Give users control over the costs of the payment system usage	SM17-19. Measurement against validation: No significant difference between the systems in control over costs.	Not confirmed	X
DR 8. Interaction with the payment system should resemble users' expectations about the payments process	RM5. Measurement against validation: Ease of use is higher for the Old system.	Not confirmed	X
DR 9. The interfaces should be presented in a logical, clear and understandable way	Out of the scope of the study.	Not confirmed	X
DR 11. Provide features of customisation of payment environments	Out of the scope of the study.	Not confirmed	X

DR 3. As the proof of DR 3 on privacy policy the results of measure SM1 can be used, see Table 5.15, which indicated that participants of the New system are more comfortable to use personal information than in the Old system, and this can be interpreted as an evidence of the validation of DR 3 on privacy policy.

DR 5. The participants of the New system have considered that the way the *payment code* can be blocked in the New system gave them more control than in the Old system, SM3, Table 5.15. This corroborates the validity of DR 5 on control of critical actions and information. Another supporting evidence for the validity of DR 5 are users' attitudes on *how safe it is to use the system*, RM2, Figure 5.2. Based on the significance of within-subjects main effect for the tasks and the cubic effect in this measure, it can be suggested that task 2 (exploring DR 5) indicated a higher rating of safety of the system than the rest of the tasks, and this measure is higher for the New system than for the Old one.

DR 6. The fact that the system was introduced by Postbank has influenced positively users' opinions about the trustworthiness of the system, and it is in favour of the New system, SM7, Table 5.15. This supports the validity of DR 6 on trust transference.

DR 7. The overall improvement of the participants' opinions on *trust* in the New system can be interpreted as an evidence of the validation of DR 7 on taking measures to address risks, RM1, Figure 5.1 and Table 5.5.

It cannot be though completely excluded that the higher trust in the New system was a consequence of the whole complex of changes applied according to the design recommendations. Taking into account a significant main effect for the difference between the tasks and significance of the 4-th order effect of factor tasks in measuring trust in the system, RM1, it can be concluded that task 3 indicated relatively lower trust in the system, while tasks 2 and 4 indicated relatively higher trust, Figure 5.1 and Table 5.5. Since tasks 2 and 4 were focused mainly on the privacy and security policies and control over the critical information (DRs 1, 2, 3, 5), it can be inferred that these aspects were important in increasing trust and alleviating risks for both systems. The fact that the New system performed better in the *trust* measure than the Old one gives another supporting evidence to the validity of these DRs.

DR 10. The experiment has demonstrated that the feature of *multiple payments* brings benefits to users in terms of speed and usefulness, SM10 and SM12, Table 5.15. This serves as evidence for validation of DR 10 on automatisation of payments.

Regarding the other aspect of automatisation of payments, pertaining to scheduled payments, which were tested in the form of paying a rent for a house, the conclusion about its contribution to the evaluation of DR 10 should be drawn carefully. A proper execution of this task was supported only in the New system, while the participants of the Old system had to pay individual rent payments repeatedly, which was considered a bit artificial by the participants.

On the other hand, scheduled payments have significantly decreased *ease of use* in the New system, RM5, see task 3 in Figure 5.5, which is demonstrated by the significance of the differences between the tasks in the 4^{th} order effect. The possible reasons of this outcome are the incorrect implementation of the task or the correspondent design recommendation. Rent payments could be a wrong way to test the task, or the participants may have experienced difficulties understanding the task. Some of the participants even refused to do the task, saying they would not pay rent in this way. This experimental task arguably favours the New system, which automated the task completely, while in the Old system the task is not supported as such. Not surprisingly, the subjects reported the higher usefulness for this task in the New system, SM12, Table 5.15. Clearly, this seems a rather circular experiment, and the validity of advice on scheduled payments cannot be confidently concluded. However, repeated payments are an actual and frequent task for users, and it is justified to use them for drawing comparisons between the two systems.

DR 12. The difference in the length of the PIN code has indicated the importance of authentication and suggests that a shorter 4-digit *payment code* could be better than the longer 6-digit. Perhaps the 5-digit code could be recommended as the optimum in this case. This result, in combination with the observation that the participants were more comfortable with the *way they can identify themselves* in the New system, Table 5.15, supports the validity of DR 12 concerning authentication.

It has not been possible to find convincing evidence for validity of the other design recommendations in this experiment.

DR 4. The results on control over the costs of the EPS' use, (SM 17 and SM 18, Table 5.15) do not significantly distinguish between the systems, and therefore this DR cannot be considered as validated.

DR 8. The participants would be more willing to use the New system than the Old one, RM4, SM8, and this perceived usefulness could be partially attributed to the improved interaction design. However, another interesting result demonstrates that despite that the changes to the system were aimed to improve its usability, they did not create an observable improvement in the usability goal *ease of use*, RM5. The better rating for *ease of use* of the Old system than for the New one prevents from making claims about the validity of this DR, Table 5.9 and Figure 5.5. Despite that there is supporting evidence for the validity of DR 8 on interaction design, has not been validated sufficiently in the experiment.

DR9 and DR 11. This experiment was not designed to evaluate of DR 9 on the logic of interfaces. DR 11, regarding the customisation of payment environments, was not evaluated within the scope of this experiment.

In conclusion, the application of the design recommendations has resulted in improvement of users' attitudes towards the New system and has raised the overall user acceptance of the redesigned system. The New system has scored higher than the Old one in *trust* and *perceived usefulness*. The analysis of the results has indicated that the participants would be more likely to accept the New system. This is a good indicator of positive influence on user acceptance of the set of design recommendations on the whole.

While certain design recommendations could not be sufficiently validated, this does not undermine the success of the experiment. Literature on EPSs and the research activities of this thesis reported in Chapters 3 and 4 emphasise the high relative importance of the aspects of trust, privacy and usefulness for end users. The improvements

in these aspects that have been made with the application of the design recommendations indicate the high positive impact of the recommendations on design of e-commerce EPSs.

A word of caution must be said regarding the validation experiment. The design recommendations as described in Appendix D include the detailed description that serves to operationalise them. The experiment has not attempted to validate each and every detail of the DRs. Rather, the DRs were applied by selecting the applicable details, and the impact this had on the system, has been evaluated. However, in all cases this validation is subject to the way these details were applied and to the personal interpretation and application of the DRs by the experimenter.

It is also hard to conclude that certain system's aspects were affected solely by the correspondent design recommendations, other factors may have influenced the participants' attitudes. However, applying the set of recommendations as a whole has shown the overall positive impact that cannot be disputed. In conclusion, the experimental results provide supporting evidence for the validity of DRs 1, 2, 3, 5, 6, 7, 10, 12, but this should not be taken that every detail of these design recommendations is proven to be valid.

5.4.2 Revision of not validated design recommendations

Regarding the design recommendations that were not validated in this experiment some considerations should be given about how they can be revised, so that the chance of their validity will be improved in future validation studies. DR 4 on control over the costs of the payment system usage failed to be validated. A possible explanation might be that the issue of costs may be not as important as it seemed prior to the validation experiment, but this would disagree with other studies on costs of electronic payments, (Humphrey et al., 2001).

Assuming that this DR has some potential, one of the reasons it is not validated is that the DR was not applied sufficiently, or that the context of the experiment did not allow to observe the benefit of its application, which might still develop, e.g. over time. One of the possible changes that can be made to this DR is suggesting more salient exposure of the fact that the use of the system to customers is free of charge. Another way to improve the effect of this DR would be awarding costumers incentives for using EPSs, e.g. via loyalty schemes such as Air Miles.

DR 8 on interaction design has failed to be validated due to decreased usability of the New system. In spite of possible problems in the way this DR was implemented, such as limitations in implementing the changes to the New system, or limitations of the experimental setup, described in section 5.4.3, there is still a room for improvement of this DR. Interaction design is a broad and complex issue, and existing knowledge about it can be applied to the context of e-commerce EPSs. For instance, various practices of interaction design for successful EPSs, payment products and electronic banking could be referred to, and adapted to online EPSs. Another way to revise this DR would be employing guidelines for interaction design applied to the related technology, such as mentioned earlier guidelines on e-commerce user experience, (Nielsen, et al., 2000), or heuristics for Web design, (Nielsen, 1999).

The analysis of the results demonstrates that task 3, which was designed to evaluate scheduled payments, resulted in the lower ratings of users' attitudes than the other tasks, section 5.3.1. It can be the case that task 3 was the most complex, or it exposed most limitations of the systems. It may suggest that a better specification of DR 10 that advises on scheduled payments is needed. DR 10 could be revised and extended to include practices of scheduled payments of existing EPSs or related technology. It can be iteratively implemented and evaluated to find the best way to formulate this DR. In addition, research for relevant applications for scheduled payments could be conducted.

5.4.3 Limitations of the experimental study

In some cases, the design recommendations were applied to the design of the New system, but no improvement was shown in the users' rating of the system. They are listed in Table 5.17. Of course, a simple explanation would be that there are inherent flaws in the design recommendations. Alternatively, these DRs might not create an impact large enough to affect users' attitudes. They might have also been applied incorrectly, or a too small sample of users was taken. DRs might be too abstract to guide the design, or be conflicting. However, this is not true for all cases, as application of some design recommendations still showed improvement in users' attitudes. Chapter 6 discusses validity issues of the results in more detail. Possible reasons for not being able to validate all DRs are discussed here. Let's look at them in detail step by step.

Too little impact of the changes on the system.

The Old system could be already well designed in some of the aspects, therefore the changes made to the system might not have been able to improve significantly the already good design of the Old system.

Let's illustrate the last statement on the implication that there is no improvement of usefulness of help in the New system. The systems could be understood quite well intuitively, therefore subjects did not have the need to revert to the help means in both systems, and the improvements made to the help system were not salient enough to find a difference in the aspect of help.

Limitations in implementation of the design recommendations in the New system

A number of changes to the system according to the design recommendations were not implemented in the completely right manner. For example, it was not possible to record some of the new Payphone IVR voice menu items, due to the absence of the person who had recorded the original items, therefore the developers had to cut and paste existing audio files to make the new menu items. This workaround made some voice menu items sounding a bit unnaturally. This and several other implementation problems could be responsible for the lack of statistically significant improvement in users' opinions and may even account for the lower users rating of usability of the New system.

Limitations of the experimental setup

There were constraints in the ability to replicate the actual context of use and operation of the payment system, e.g. a customer support line, a full-fledged web site for help and support, seamlessly integrated into the Postbank's online help system, etc. Therefore the findings may be limited due to these compromises.

Gap between the design recommendations and their actual realisation

A high-level design recommendation might omit important details of the problem it is addressing. The design recommendations may not be describing particularly important aspects of the systems' implementation, and being correct in general might not target certain minor but still important facets of payment systems.

Lack of specifications how the design recommendations should be implemented

The design recommendations do no specify the exact formulation and manifestation of the system's aspects they suggest to change or improve. For example, suggesting to use privacy and security policies, the design recommendations do not give specific in-depth instruction about how these policies should be implemented. The experimenters had to refer to the industrial practice, reference sources and their best practice. This may confound with the experimental results, as it can be argued that all findings (positive or negative) are predicated upon the way the DRs are applied to the design of the New system. On the other hand, it is exactly the problem that will accompany the application of the design recommendations by practitioners in real life, and this is why the study has a high degree of realism.

5.5 Conclusions

This empirical study has succeeded in demonstrating the potential validity of certain design recommendations, acquiring new validated design knowledge, which was not available before the study. This experiment has given us a better insight in the design of user acceptance of electronic payment system from the user perspective. The design recommendations are a valuable output of the study, suggesting a design approach to e-commerce EPSs unmatched by any previous work in this direction, as far as it was possible to establish.

Chapter 6

Discussion and conclusions

6.1 Summary of the thesis

With the rapid development of Internet e-commerce the need for appropriate electronic payment systems (EPSs) to support online trade clearly emerges. An open challenge remains for developers of novel Internet-based payment systems to meet users' expectations, requirements, preferences and needs in design and exploitation of payment systems. Failure to meet them results in low usability, insecurity and inefficiency of payment systems and in eventual refusal of customers to use such systems. Design of new electronic payment systems from the user perspective is critical for the development and operation of payment systems that are well accepted by users, Chapter 1.

This thesis has described research activities aimed to investigate how e-commerce EPSs could be designed from the user-centered perspective in order to achieve user acceptance. The research has explored what validated design knowledge that should be communicated to designers of EPSs, so that end users will be willing to use the newly introduced EPSs for payments and personal finance in an e-commerce environment. This research aimed to understand the notion of user acceptance in the con-

text of e-commerce EPSs, which is defined as the demonstrable willingness of users to employ information technology for the tasks it is designed to support, (Dillon & Morris, 1996). This research has taken into account various factors that determine user acceptance of electronic payment systems, such as usability, privacy, security, trust and others, (Chapter 2).

A combination of various scientific and design activities, and practices of Human-Computer Interaction were involved: a literature study, a consumer survey, a qualitative diary study, and experimental research. These research activities helped to develop an in-depth view of user experience with payment systems and have suggested how to design or redesign EPSs to improve their chances of acceptance by end users.

In the first phase of the research, the characteristics and classification of EPSs were discovered, based on literature research. The literature review helped to generate ideas about why user acceptance is important for e-commerce EPSs. One of the challenges of this phase was conceptualising and understanding user acceptance in the specific context of EPSs.

To reveal actual user attitudes to the hypothesised determinants of user acceptance of EPSs, a consumer survey was conducted. It helped to identify what characteristics should be given more attention in the design of EPSs:

- applicability
- usability
- convertibility
- privacy
- reliability
- security
- trust.

However, the knowledge of the characteristics and their importance did not inform interaction design in terms of how the characteristics should be realised in EPSs. To acquire a deeper understanding of these issues, qualitative research in the method of a diary study was conducted.

The qualitative diary study investigated the user experience with e-commerce EPSs in the context of real use and over time. It helped to reveal problems that end users experience with electronic payment systems. Moreover, the study has discovered a number of positive findings. In many instances users took the initiative in suggesting solu-

tions for certain problems they encountered, and said what could be improved in the payment systems they used. This study was able to obtain more insight on social influences on users of online EPSs, a highly significant factor for users acceptance.

Implications for design of Internet-based payment systems have been derived and formulated as design recommendations. This stage marked the end of the data collection and the start of the development of design recommendations.

Design recommendations

A set of *recommendations for design* of e-commerce EPSs has been developed on the basis of research findings of this thesis, to assist design of future and improve current payment systems, Chapter 4. However, before suggesting to apply these recommendations for actual design of electronic payment systems there was a need to find evidence that their application would improve user acceptance of e-commerce EPSs.

To ensure the validity of these design recommendations, an experimental study of their application on an actual system from Postbank (the Netherlands) was conducted, Chapter 5. It helped to substantiate the validity of a subset of the design recommendations, gaining validated design knowledge that was not available beforehand. The design recommendations validated in the course of this work are the following (Chapter 5 and Appendix D):

DR 1. Inform users about security measures and provide a security policy.

DR 2. Explain what type and details of personal information are to be retained, why, and how they will be used.

DR 3. Provide a clear and explicit policy on privacy and make it noticeable to users.

DR 5. Allow users to control critical actions and information.

DR 6. Seek reputation and trust transference from reputed partners and technology providers, and communicate trust transference to users.

DR 7. Take measures to address risks and inform users about these measures.

DR 10. Provide features of automatisation of payments.

DR 12. Provide well-designed Authentication.

The design recommendations that were not validated or were out of the scope of the experiment, described in Chapter 5, are the following:

DR 4. Give users control over the costs of the payment system usage.

DR 8. Interaction with the payment system should resemble users' expectations about the payments process.

DR 9. The interfaces should be presented in a logical, clear and understandable way.

DR 11. Provide features of customisation of payment environments.

Contributions

The contribution of this research is deeper knowledge about the user experience and users acceptance of EPSs. This research has discovered empirical evidence of the importance to users of various characteristics of EPSs, which have been traditionally used to describe electronic payment systems. The main contribution of this thesis is the set of recommendations for interaction design of electronic payment systems, with the scientific evidence of their validity.

The studies described in this thesis were conducted in realistic conditions and with potential users. The user survey, eliciting user attitudes towards EPSs, was able to embrace more than 1300 Netherlands-based respondents nation-wide. The recommendations for design were reviewed and applied by the actual developers of a commercially produced electronic payment system. This suggests the high realism of the application of the design recommendations and the high ecological validity of the research.

Before this research, the creation of the user experience and design for user-related factors of EPSs were mainly based on ad hoc practices, coming from related industries, such as banking. Interaction design was based on the models of banking web sites, e-commerce portals, online shops and similar applications. For instance interaction design of payment system Paypal.com resembles to a great degree a typical online shop, in both layout and interaction design. Designers of existing EPSs could use state-of-the-art methods to guide interaction design, for instance Nielsen's heuristics for Web design, (Nielsen, 1999). However, there have been no specific prescriptions for the design of e-commerce EPSs from the user perspective, besides technical or high-level requirements.

From the technical viewpoint, research and development of EPSs used to concentrate on general requirements for EPSs, such as functionality and technology, cryptography, networking, etc. However, the critique of literature in Chapter 2 has demonstrated

that this approach does not inform design for user acceptance of online EPSs sufficiently.

The in-depth knowledge received during this research about interaction design, understanding of user-related factors and issues of user acceptance in the context of online e-commerce EPSs was not available or well systematised prior to this thesis. This research has provided a more elaborate knowledge regarding design of electronic payment systems from a human-centered perspective compared to what was available before. This knowledge has been validated. Validity issues are described in the following sections.

6.2 Validity issues and limitations

There are several possible threats to validity of any empirical research. Gray & Salzman (1998) define two important issues that could permit making valid inferences from experimental results: cause-effect and generality. Let us look at these issues in the light of the empirical research activities of this thesis. The discussion below is based on work of Cook & Campbell (1979) and Gray & Salzman (1998).

6.2.1 Cause-effect validity

Cause-effect validity is concerned with making false inferences from the results, either false right or false wrong conclusions. The validation experiment was conducted to determine an effect of the design recommendations on users' attitudes and preferences of the systems under test. Causality lets us infer that the users' attitudes and preferences were influenced by the application of the DRs, and not other some other confounding factors.

An important aspect of cause-effect validity is internal validity, which is the approximate truth about inferences, regarding cause-effect or causal relationships. The question for internal validity is whether we can conclude if the controlled independent variable caused changes in the dependent variable, or whether another unaccounted covariate is responsible for the results.

Selection of users

One of the possible threats to internal validity of the experimental study, described in Chapter 5, is the selection of certain types of users and assigning them to experimental groups in such a way, that the effect is due to the individual differences between users, rather than the treatment, (Gray & Salzman, 1998).

To avoid a possible confounding effect of demographic parameters and experience, the participants where screened using demographics filters. The sample was further balanced based on these parameters and the users were divided in groups. The sampling model presumed further random assigning of the participants to the groups. This was done to avoid the bias of the selection, when participants assigned to the groups are unequal in some characteristics. The sample was checked for a possible imbalance of the demographics factors between the two groups, and no significant covariating variables were discovered.

In the user survey described in Chapter 3, the large sample size of more than 1300 respondents can be treated as representative of the population of Dutch users of payment systems, and can justify the conclusion about the stable effect. The large sample size also minimizes the influence of *wildcards*, i.e. people who significantly differ in positive or negative opinions from the average respondents, and whose responses to the conditions of the study reflect only their wildcard status.

6.2.2 Generality issues

Apart from the internal cause-effect validity, it is important to consider if we are allowed to *generalise* the results of the research activities to different types of systems, settings and times. Cook & Campbell (1979) refer to generality issues as *construct validity* and *external validity*.

Construct validity

Construct validity concerns if the experimenters manipulating what they claim to be manipulating, and if they are measuring what they claim to be measuring. Some of the design recommendations prescribe in what direction the system's functionality, features or content should be implemented. Different developers of e-commerce EPSs may have a varied understanding of a particular functionality or features. The exact

interpretation of the advice can be different from one practicing designer to another specifications developer. For example, when implementing a privacy policy according to the correspondent design recommendation, DR 3, there could be an endless number of variations for policies, based on how organisations view their attitudes to privacy. The reason for this is that the design recommendation, while prescribing the use of a privacy policy, does not specify the content of the privacy policy in every detail for every situation. The detailed description of a design recommendation is used to highlight the general direction of its use.

Claiming that the design recommendations are validated for *all* their detailed features is therefore not possible, because only some of these features were tried in the validation experiment. The multifaceted design recommendations were applied in one single way only. E.g. an alternative form of the privacy policy was not examined with the payment system under test. This limits the generalizing power of the results to some extent because of the threat of applying the design recommendations with *mono-operation bias*. Therefore, the design recommendations can be generalised only at the high level, where concrete details of realization do not step down from the general high-level advice. This is the cost one has to pay in order to test the application of design guidelines for the prescriptive use.

In addition, the design recommendations were applied to the validation of only *one* type of payment systems. From construct validity viewpoint this may comprise a limitation of *mono-method bias*. To avoid this threat to validity, validation experiments with other systems could have been conducted.

There was a little room for the threat of statistical *interaction* of different treatments in the validation experiment, because the participants worked with only one version of the payment system, i.e. were given only one treatment, which is determined by the between-subjects design, Chapter 5. However, a possible threat to generalisation is the interaction between system's features and their consequent influence on users' attitudes, especially between those features that were implemented in the New system. It is not always possible to draw the conclusion that a particular change in the system resulted in the intended change of user attitudes towards the EPS. For example, the claim that the design recommendations on trust are the only source of increased trust in the New system would have been unjustified due to the possible influence of other system's features and factors, such as reliability, new functionality or interaction design.

Finally, it should be considered whether the test users entertained the idea of *hypothesis-guessing*, i.e. the guesses participants make about how they should behave to make experimenters happy. While this threat cannot be completely dismissed, it is expected to have a low effect on the results, because the between-subjects experimental design presumes that the users were exercising with only one version of the system, and were not aware about existence of the other version, nor did they know which version they were using. The participants could of course have tried to give better marks to both systems than these would deserve, in order to please the experimenter. However, the New system has scored nevertheless better in many instances, and the differences are significant.

External validity

The results of the study may be prone to threats of external validity. External validity concerns the correctness of generalising towards particular target users, settings and times. Let us look at the possible threats to external validity of the generalisation of the research results.

Target users

One of the possible threats to external validity is a choice of certain types of users, who may be not representative of the target population of potential end users. It has been attempted to collect the most representative sample available. Some limitations are noted in this respect.

The participants for the diary study (Chapter 4) were selected mainly from the employees of the university campus. The reason for this was a very low reaction to the advertisement placed in the local newspaper. Participation of university administrative employees was a solution. The diary study involved 10 people who cannot possibly be considered representative of a population as large as the market for online EPSs. The participants related to the university may be a rather homogenous group in many respects, but their involvement in the university is irrelevant to their relation to EPSs. They were of course geographically very similar, but this seems to be a difficult effect to avoid. However, the diary study served as a data collection technique, and attempted to provide explanations of users' opinions and experiences, rather than generalise to a target population. The focus of the study was on the detail and depth of explanations, rather on the breadth of coverage. The final number of the participants was in accordance with the goals of the study.

To address this type of threat in the experimental study (Chapter 5) the users were carefully selected by the call centre of Postbank, based on the requirements of the study. The users of the nation-wide consumer survey (Chapter 3) with the sample size of more than 1300 respondents can be treated as representative of the population of potential users of payment systems in the Netherlands.

It would be possible to generalise the results to the heterogeneous population represented by all participants, and not possible to single out specific subpopulations. It cannot be said that the payment system under test would successfully appeal to e.g. just young people, pensioners, or students. It would be an error of external validity to generalise across these subgroups of the whole sample. Consequently, the DRs can be assumed to hold for the average user and not to be applied to any subgroup.

Context of use and the scope

The studies of this research attempted to be as realistic as possible. However, we should be cautious in claiming that generalisation of the results could transcend the setting and the context of the studies and be generalised to a wider range of settings, i.e. other EPSs, applications and context of use.

While admitting this, it has to be noted that the scope of the research was clearly defined from the very start and followed through the whole course of the research activities. Moreover, this research has identified a number of cases where the context of use is highly important for certain systems' requirements, users' attitudes towards EPSs, and consequently user acceptance. Therefore, the implications for design can be treated as valid only for the given scope and the context of use, described in Chapter 1.

The design recommendations emerged out of the qualitative research that considered electronic payments in real life situations, with the diary study recording real payments. The design recommendations were applied to a commercial payment system by the company-developer and therefore their application is tested in a realistic context. It can be said with confidence that the validation experiment and the diary study had a quite high degree of realism. In both studies the setting was consistent throughout the process of the studies and data collection. It can be concluded that the studies in this thesis are done with the high degree of ecological validity.

6.2.3 Conclusions

Having examined a comprehensive list of potential threats to the validity and generaliseability of the research presented in this thesis, it is argued that the design knowledge provided is useful and valid. The research activities of this thesis have a high degree of realism. The research included the nation-wide consumer survey, eliciting user attitudes towards EPSs of a large sample of Netherlands-based respondents. The qualitative diary study was able to investigate the actual user experience with online EPSs, and has provided grounded data, used for the hypothesising of the design recommendations.

For the validation of the design recommendations it was possible to form an alliance with the actual developers of an EPS and validate the DRs with a commercial payment system. The outcome of the experiment makes it possible to draw conclusions about the validity of certain DRs and the possibility to use them for the design of e-commerce EPSs. The high ecological validity and realism of the studies allow us to conclude about the success of this research.

6.3 Future work

This research attempted to embrace a wide spectrum of possible issues with user acceptance of e-commerce EPSs. Future research may focus on the further development and validation of the concept of user acceptance of EPSs. For instance a model of user acceptance of e-commerce EPSs may be developed and validated to become a reliable tool for gauging user acceptance of electronic payment systems and similar related technology. Future work can be concentrated on the validation of specific factors that can influence user acceptance. It can concern itself solely with just one of the issues, e.g. privacy, trust or security, usability.

Of course, the most natural continuation of this research would be to take the design recommendations even further. They can be further validated, enhanced and substantiated in the context of actual use or in larger scale experiments. It would be an interesting long term study to observe the effect of the design recommendations in a real life system on the market, to observe their relevance in a longer span of time, and to track down their development.

Further work on the design recommendations should try to resolve potential threats to their validity. On the one hand, the design recommendations can be used differently than in the presented study. Another way of the application and implementation of the design recommendations can improve a chance to avoid mono-operation bias, i.e. applying the design recommendations only in one way. This can also help to refine the details of the design recommendations. On the other hand, the design recommendations should be applied to other types of payment systems in order to avoid mono-method bias that could emerge if applying the DRs only to one type of EPSs. While the system used for the experimental study suits the scope of this research well, it would be interesting to test the design recommendations with a different type of payment systems. This will allow generalising the validity of the design recommendations to different EPSs and contexts of use.

A promising direction of future research is developing a system for evaluation of EPSs. This direction presumes creating evaluation models, methods, tools and techniques, etc. For instance, heuristic evaluations or checklists can be created for revealing problems with EPSs at the design stage, paving the way for improvements and changes in the current and future systems. These evaluation methods and tools can be then validated empirically.

In conclusion, future research has a great number of exciting opportunities. It can transcend the field of online EPSs and delve into other areas of e-commerce and future information technology.

Appendix A

User Survey Questionnaire

ALGEMEEN

1. Heeft u beroepsmatig te maken met betalingssystemen, bijvoorbeeld als bankmedewerker, onderzoeker of als software ontwikkelaar?
1 Ja
2 Nee

1a. In welke branche bent u werkzaam?

1 Landbouw & Visserij
2 Industrie en bouwnijverheid
3 Handel
4 Horeca
5 Vervoer & Communicatie
6 Financiële instellingen
7 Zakelijke dienstverlening
8 Openbaar bestuur
9 Onderwijs
10 Gezondheids- en welzijnszorg
11 Cultuur en overige dienstverlening
12 Wetenschap & Onderzoek
13 Anders

2. Wat is uw beroep?

_____

GEBRUIK BETAALMIDDELEN
Wilt u de juiste getallen invullen en de relevante tijdsperiode omcirkelen. Indien u van een bepaald betaalsysteem geen gebruik maakt, kunt u een 0 invullen.

3a. Hoe vaak gebruikt u contant geld?

_____ keren per dag /week /maand/ jaar

3b. Hoe vaak gebruikt u een bankpas (of giropas)?

_____ keren per dag /week /maand/ jaar

3c. Hoe vaak gebruikt u een creditcard?

_____ keren per dag /week /maand/ jaar

3d. Hoe vaak gebruikt u een Chipknip/ chipper?

_____ keren per dag /week /maand/ jaar

3e. Hoe vaak gebruikt u een ander betaalmiddel, namelijk _____?

_____ keren per dag /week /maand/ jaar

4. Vindt u het belangrijk dat u met één betaalmiddel op de meeste plaatsen kunt betalen?

1 Zeer belangrijk
2 Enigszins belangrijk
3 niet belangrijk, niet onbelangrijk
4 Enigszins onbelangrijk
5 Zeer onbelangrijk

5. Wilt u voor onderstaande betaalmiddelen de mogelijkheid hebben om op meer plaatsen te betalen (dan u nu doet)?

		Helemaal niet	Enigszins	Zeker wel	Niet van toepassing
1	Contant	1	2	3	4
2	Bankpas/Giropas	1	2	3	4
3	Creditcard	1	2	3	4
4	Chipper	1	2	3	4
5	Creditcard op internet	1	2	3	4

Hieronder staan enkele soorten uitgaven. Wilt u voor elke uitgave aangeven op welke wijze u meestal betaalt?

		Contant	Pinnen	Eurocheque/giro-betaalkaart	Chipper	Creditcard	Klantenkaart	Anders1)
1	Dagelijkse levensmiddelen	1	2	3	4	5	6	7
2	Wekelijkse levensmiddelen	1	2	3	4	5	6	7
3	Meubelen	1	2	3	4	5	6	7
4	Duurzame huishoudelijke app. (audio video/tv/koelkast/etc.)	1	2	3	4	5	6	7

5	Kleding	1	2	3	4	5	6	7
6	Benzine	1	2	3	4	5	6	7
7	uit eten	1	2	3	4	5	6	7
8	Vakantie/dagje uit BINNENLAND	1	2	3	4	5	6	7
9	BINNENLAND geldopnames	1	2	3	4	5	6	7
10	BUITENLAND betalingen	1	2	3	4	5	6	7
11	BUITENLAND geldopnames	1	2	3	4	5	6	7

1) Namelijk:

_____

7. Met welk betaalmiddel betaalt u meestal bij onderstaande bedragen?

	Bedrag:	Contant	Pinnen	Eurocheque/giro-betaalkaart	Chipper	Creditcard	Klantenkaart	Anders
1	Tot fl. 25,00	1	2	3	4	5	6	7
2	Van fl. 25,00 tot fl. 50,00	1	2	3	4	5	6	7
3	van fl. 50,00 tot fl. 100,00	1	2	3	4	5	6	7
4	van fl. 100,00 tot fl. 150,00	1	2	3	4	5	6	7
5	van fl. 150,00 tot fl. 250,00	1	2	3	4	5	6	7
6	van fl. 250,00 of meer	1	2	3	4	5	6	7

8. Bij welke bank heeft u uw belangrijkste betaalrekening?

1 Postbank
2 ABN Amro
3 Rabobank
4 Fortis Bank
5 SNS Bank
6 ING Bank
7 Andere bank, nl._____

9. Hoeveel betaalrekeningen heeft u?

1 één betaalrekening
2 twee betaalrekeningen
3 drie betaalrekeningen
4 vier of meer betaalrekeningen

10. Hoe neemt u meestal contant geld op, aan de balie of bij de geldautomaat?
1 altijd aan de balie
2 meestal aan de balie
3 soms aan de balie, soms bij de geldautomaat
4 meestal bij de geldautomaat
5 altijd bij de geldautomaat

11. Hoeveel belang hecht u eraan om aan de balie van uw bank uw geld op te nemen?

1 zeer veel belang
2 redelijk belang
3 maakt niet zoveel uit
4 matig belang
5 geen belang

12. Wist u dat banken en winkels bijhouden wat uw betalingen zijn als u gebruik maakt van een bankpasje of een ander elektronisch betaalmiddel?

1 Ja
2 Nee

13. Als u gebruik maakt van elektronisch betalen wordt soms uw identiteit bekend bij de winkel. Weerhoudt u dat om gebruik te maken van een elektronisch betaalmiddel?

1 Ja, altijd
2 Soms
3 Nee, nooit

14. Bent u tevreden over de mate waarin een bankpas/ giropas u privacy biedt?

1 Zeer tevreden
2 Tevreden
3 Niet tevreden, niet ontevreden
4 Ontevreden
5 Zeer ontevreden
6 Weet niet

15. Bent u bezorgd over het feit dat een winkel weet wat u koopt als u elektronisch betaalt via een creditcard of bankpas?

1 Zeer bezorgd
2 bezorgd
3 Niet bezorgd, niet onbezorgd
4 Onbezorgd
5 Zeer onbezorgd
6 Weet niet

16. Banken en winkels kunnen fouten maken met uw geld. Zou u registratie willen van uw aankopen om deze fouten te kunnen aantonen, zoals verkeerde bedragen?

1 Zeker wel
2 Waarschijnlijk wel
3 Misschien wel, misschien niet
4 Waarschijnlijk niet
5 Zeker niet
6 Weet niet

17. Denkt u dat winkels de informatie over uw betalingsverkeer kunnen gebruiken om tot een betere dienstverlening te komen?

1 Zeker wel
2 Waarschijnlijk wel
3 Misschien wel, misschien niet
4 Waarschijnlijk niet
5 Zeker niet
6 Weet niet

18. Hoe belangrijk is het voor u dat gelden gemakkelijk overgezet kunnen worden van het ene naar het andere betaalsysteem bijv. van rekening naar contant geld?

		Zeer belang-rijk	Enigszins belangrijk	Niet belang-rijk, niet onbelangrijk	Enigszins onbelangrijk	Zeer onbe-langrijk	Niet van toepassing
1	Contant -> Rekening	1	2	3	4	5	5
2	Rekening -> Contant	1	2	3	4	5	5
3	Rekening -> Chipper	1	2	3	4	5	5
4	Chipper -> Rekening	1	2	3	4	5	5

19. In hoeverre bent u tevreden over de huidige situatie met betrekking tot het overzetten van geld tussen de verschillende betalingssystemen?

		Zeer tevreden	Tevreden	Niet tevre-den, niet ontevreden	Ontevreden	Zeer onte-vreden	Niet van toepassing
1	Contant -> Rekening	1	2	3	4	5	5
2	Rekening -> Contant	1	2	3	4	5	5
3	Rekening -> Chipper	1	2	3	4	5	5
4	Chipper -> Rekening	1	2	3	4	5	5

GEBRUIKSGEMAK

20. Soms functioneren betaalmiddelen niet zoals het hoort. Wat voor problemen heeft u wel eens ervaren met onderstaande betaalmiddelen bij een betalingsactiviteit?

		Bank-pas/Giropas	Chipper	Creditcard
1	Betaalapparaat werkte niet waardoor ik niet met pas kon betalen	1	2	3
2	Transactie werd niet geaccepteerd	1	2	3
3	Mijn pas werd niet geaccepteerd	1	2	3
4	Er is meer van mijn rekening afgeschreven dan ik heb betaald	1	2	3
5	Anders, nl. _____	1	2	3
6	Geen problemen	1	2	3

21. Heeft u een voorkeur voor een bepaald betaalmiddel omdat het makkelijk in het gebruik is?

1 Ja, voorkeur voor bankpas/ giropas
2 Ja, voorkeur voor Chipper
3 Ja, voorkeur voor Creditcard
4 Ja, voorkeur voor contant geld
5 Ja, voorkeur voor ander betaalmiddel, namelijk _____
6 Nee, geen voorkeur

BETALEN VIA INTERNET

22. Bestelt u wel eens via Internet artikelen of diensten, die vervolgens betaald moeten worden?

1 Ja
2 nee => ga door naar vraa 34

23. Wanneer u wel eens via Internet bestelt, op welke wijze betaalt u dan meestal?

1 Creditcard
2 Credit card met SET-certificaat
3 Maestro met SET-certificaat
4 Betalen met digi-pas
5 Telebankieren
6 Contante betaling
7 Betaalcheque
8 Pinpas
9 Chipper
10 Via een eenmalige machtiging
11 D.m.v. een factuur of acceptgiro
12 Op rekening
13 Anders

24. Welke betalingswijze bij internet-aankopen heeft in het algemeen uw voorkeur?

1 Creditcard
2 Credit card met SET-certificaat
3 Maestro met SET-certificaat
4 Betalen met digi-pas
5 Telebankieren
6 Contante betaling
7 Betaalcheque
8 Pinpas
9 Chipper
10 Via een eenmalige machtiging
11 D.m.v. een factuur of acceptgiro
12 Op rekening
13 Anders

25. Bent u bezorgd, wanneer u via Internet betaalt, dat er misbruik kan worden gemaakt van uw gegevens?

1 Nee
2 Ja, omdat

_____
_____
_____

26a. Wat is volgens u het meest veilige betaalmiddel voor betalingen via Internet?

1 Creditcard
2 Credit card met SET-certificaat
3 Maestro met SET-certificaat
4 Betalen met digi-pas
5 Telebankieren
6 Contante betaling
7 Betaalcheque
8 Pinpas
9 Chipper
10 Via een eenmalige machtiging
11 D.m.v. een factuur of acceptgiro
12 Op rekening
13 Anders

26b. Wat is volgens u het minst veilige betaalmiddel voor betalingen via Internet?

1 Creditcard
2 Credit card met SET-certificaat
3 Maestro met SET-certificaat
4 Betalen met digi-pas
5 Telebankieren
6 Contante betaling
7 Betaalcheque
8 Pinpas
9 Chipper
10 Via een eenmalige machtiging
11 D.m.v. een factuur of acceptgiro
12 Op rekening
13 Anders

27. Heeft u ooit een creditcard gebruikt om te betalen op het Internet?

1 Ja
2 Nee => ga door naar vraag 30

28. Hoe gemakkelijk was het om op het Internet met een creditcard te betalen?

1 Zeer gemakkelijk
2 Gemakkelijk
3 Niet moeilijk, niet makkelijk
4 Moeilijk
5 Zeer moeilijk

29. Wat zijn de voornaamste problemen die u heeft ervaren bij creditcard betalingen via Internet?

1 Weigering Creditcard
2 Verkeerd bedrag afgeschreven
3 Creditcardnummer gestolen
4 Het moeten opgeven van allerlei persoonsgegevens voordat transactie plaats kon vinden
5 Anders, namelijk _____
6 Geen problemen

30. Hoe belangrijk vindt u het om kleine betalingen (minder dan fl. 3,00) te kunnen doen via Internet?

1 Zeer belangrijk
2 Enigszins belangrijk
3 niet belangrijk, niet onbelangrijk
4 Enigszins onbelangrijk
5 Zeer onbelangrijk

31. Voor wat voor producten zou u het handig vinden kleine betalingen via Internet te kunnen doen?

1 Artikelen
2 Rapporten en verslagen
3 Advies over producten en diensten
4 Kranten en tijdschriften
5 Bieden bij veilingen
6 Muziek, video op internet
7 Anders, namelijk _____
8 Ik vind kleine betalingen via internet niet nodig
9 Weet niet

32. Heeft u ooit geld verloren als gevolg van een beveiligingsprobleem op het Internet?

1 Ja
2 Nee => ga door naar vraag 34

33. Heeft dit u weerhouden van verdere betalingen via dit Internet betaalmiddel?

1 Ja
2 Nee

BETROUWBAARHEID & VEILIGHEID

34. Heeft u een voorkeur voor een bepaald betaalmiddel omdat het betrouwbaarder is?

1 Ja, voorkeur voor bankpas/ giropas
2 Ja, voorkeur voor Chipper
3 Ja, voorkeur voor Creditcard
4 Ja, voorkeur voor contant
5 Ja, voorkeur voor ander betaalmiddel, namelijk _____
6 Nee, geen voorkeur

35. Is de beveiliging van betalingen belangrijk voor u als u gebruik maakt van een elektronisch betaalmiddel?

1 Zeer belangrijk
2 Enigszins belangrijk
3 niet belangrijk, niet onbelangrijk
4 Enigszins onbelangrijk
5 Zeer onbelangrijk
6 Weet niet

36. Houdt u op met gebruik te maken van een betaalmiddel als u hoort dat er beveiligingsproblemen mee zijn?

1 Zeker wel
2 Waarschijnlijk wel
3 Misschien wel, misschien niet
4 Waarschijnlijk niet
5 Zeker niet
6 Weet niet

37. Welke van genoemde elektronische betaalmiddelen vermijdt u omdat u de beveiliging ervan wantrouwt?
(meerdere antwoorden mogelijk)

1 bankpas/ giropas
2 Chipper
3 Creditcard
4 Ander betaalmiddel, namelijk _____
5 Geen

38. Is het belangrijk voor u dat er geen sporen zijn van uw elektronische betalingen, zoals uw naam, rekeningnummer, of adres?

1 Zeer belangrijk
2 Enigszins belangrijk
3 niet belangrijk, niet onbelangrijk
4 Enigszins onbelangrijk
5 Zeer onbelangrijk
6 Weet niet

39. Bent u bezorgd over het feit dat uw bronnen van inkomsten bekend zijn bij organisaties waar u koopt?

1 Zeer bezorgd
2 bezorgd
3 Niet bezorgd, niet onbezorgd
4 Onbezorgd
5 Zeer onbezorgd
6 Weet niet

VERTROUWEN

40. Is het belangrijk voor u dat andere mensen vertrouwen in het betalingsysteem hebben dat u gebruikt?

1 Zeer belangrijk
2 Enigszins belangrijk
3 niet belangrijk, niet onbelangrijk
4 Enigszins onbelangrijk
5 Zeer onbelangrijk
6 Weet niet

41. Als een nieuw systeem wordt geïntroduceerd, vertrouwt u dan elk willekeurig organisatie, of alleen gevestigde organisaties zoals banken?

1 Elk
2 Alleen gevestigde organisaties

42. Houdt u op om een betaalmiddel te gebruiken als u er vertrouwen in verliest?

1 Zeker wel
2 Waarschijnlijk wel
3 Misschien wel, misschien niet
4 Waarschijnlijk niet
5 Zeker niet
6 Weet niet

43. Vindt u dat een winkel u de keus moet bieden om te kunnen betalen met het betaalmiddel van uw keuze?

1 Ja
2 Soms
3 Nee
4 Weet niet

44. Voelt u zich meer op uw gemak bij betalingen waar u gebruik maakt van iets tastbaars (bijv. een bankpas)?

1 Zeker wel
2 Enigszins
3 Helemaal niet
4 Weet niet

45. Is het belangrijk voor u dat u op elk moment kunt zien hoeveel geld u heeft?

1 Zeer belangrijk
2 Enigszins belangrijk
3 niet belangrijk, niet onbelangrijk
4 Enigszins onbelangrijk
5 Zeer onbelangrijk.

Appendix B

Survey Results

Demographic data

Number of participants N = 1328.
Mean age= 53.26 years, std. deviation = 10.9, N = 1328.
Gender: Men = 48.2% (640), Women = 51.8% (688).
Occupation related to payment systems: Yes= 5.2%, (69 participants).
Have performed Internet payments: 19.4%, (258 participants).

Legend

N = number of responses. Smart cards are: Chipper and Chipknip.
Questions marked with * were answered only by those who made Internet payments (19.4%).
The questionnaire was translated from Dutch.

Anonymity

1. Are you aware that banks or shops can keep records about your payments when you use debit cards and other electronic payment systems?

Yes	No	Total N
60.5%	39.5%	1320

2. When using an electronic payment, you can reveal your identity to a shop. Does it sometimes stop you from using the particular payment system?

Yes	Sometimes	Never	Total N
4.0%	23.2%	72.8%	1312

3. Are you comfortable with the level of privacy that is provided by debit cards?

Very much	Quite comfortable	Neutral	Not really	Not at all	Total N
5.4%	46.8 %	39.6%	6.4%	1.9%	1238

4. Are you concerned that a shop may know what kind of things you buy when you pay electronically, e.g., with a credit card or debit card?

Very much	Quite likely	Neutral	Not really	Not at all	Total N
2.5%	11.0%	54.5%	24.9%	7.0%	1297

5. Banks and shops can make mistakes with your money. Do you want to have records of your purchases to be able to prove these mistakes, like overbilling?

Very much	Quite likely	Neutral	Not really	Not at all	Total N
38.7%	34.2%	14.6%	9.9%	2.5%	1268

6. Do you think that shops can use your payment records to provide you with better customer service?

Very much	Quite likely	Neutral	Not really	Not at all	Total N
9.8%	40.6%	24.8%	19.0%	5.8%	1257

Convertibility

7. Is it important for you, when using a payment system, that funds can be easily converted into other payment systems?

	Cash -> Account	Account -> Cash	Account -> Smart cards	Smart cards -> Account
Very important	49.6 %	73.4 %	15.6 %	10.5 %
Quite important	31.3 %	20.7 %	19.3 %	13.8 %
Neutral	11.5%	4.6 %	20.5 %	23.9 %
Quite unimportant	4.3 %	.5 %	9.7 %	12.1 %
Very unimportant	3.3%	.8 %	34.9 %	39.8 %
Total N	1292	1294	834	812

8. Are you satisfied with how your money is converted between different payment systems?

	Cash -> Account	Account -> Cash	Account -> Smart cards	Smart cards -> Account
Very satisfied	16.5%	32.1%	12.7%	3.6%
Satisfied	53.3%	55.0%	34.5%	17.6%
Neutral	19.6%	9.1%	20.1%	24.9%
Dissatisfied	7.6%	2.7%	6.3%	7.1%
Very dissatisfied	3.1%	1.0%	26.4%	46.8%
Total N	1243	1285	527	449

Ease of use

9. Do you prefer using one particular payment system over another because it's easier to use?

Debit cards	Cash	Credit cards	Smart cards	Other	Total N
75.2%	10.4%	5.0%	3.0%	.8%	1253

10. To what extent did you find it easy to pay over the internet with a credit card? *

Very easy	Easy	Neutral	Difficult	Total N
68.2%	28.0%	3.0%	.8%	132

11. Do you feel more comfortable with payments when you are using something tangible to pay with (e.g. a debit card)?

Very much so	Quite likely	Not at all	Total N
46.5%	35.2%	18.4%	1166

12. Is it important that you are able to find out at any moment how much money you have?

Quite important	Very important	Neutral	Quite unimportant	Very unimportant	Total N
36.0%	42.1%	15.0%	4.8%	2.2%	1310

Efficiency

13. How important it is for you to be able to make small payments over the Internet? *

Very important	Quite important	Neutral	Quite unimportant	Very unimportant	Total N
2.0%	11.4%	25.2%	13.0%	48.4%	246

14. Can you think of cases where small payments over the Internet can be useful? *

Don't need small payments	54.8%	Biding at auctions	5.1%	Total N
Goods	17.8%	Advice on products and services	3.6%	197
Stock research, report	8.6%	Press	1.5%	
Music/video	7.1%	Other	1.5%	

Reliability

15. Do you prefer one particular payment system to another because it is more reliable?

Debit cards	55.3%	Credit cards	2.8%	Total N
No preference	24.7%	Other	1.3%	990
Cash	15.1%	Smart cards	.8%	

Security

16. Is security of payments important for you when you use an electronic payment system?

Very important	Quite important	Neutral	Quite unimportant	Very unimportant	Total N
84.7%	13.7%	1.2%	.3%	0%	1295

17. Will you stop using a payment system if you hear about a security breach in the payment system?

Absolutely yes	Quite likely	Neutral	Probably not	Not at all	Total N
25.9%	49.4%	19.7%	4.1%	.8%	1302

18. Would you refrain from using any electronic payment system because you think it's not secure?

	Debit cards	Smart cards	Credit cards	Other	No preference
Yes	3.3%	17.1%	18.8%	5.0%	62.4%
No	96.7%	82.9%	81.2%	95.0%	37.6%
Total N	1314	1314	1314	1314	1311

Traceability

19. Is it important that no traces are left of your electronic payments, like your name, bank account, or address?

Very important	Quite important	Neutral	Quite unimportant	Very unimportant	Total N
27.0%	31.3%	27.5%	8.0%	6.1%	1269

20. Are you concerned that sources of your income can be known by vendors, i.e. the organisations you buy from?

Very concerned	Concerned	Neutral	Not concerned	Not at all	Total N
16.1%	29.2%	41.4%	10.4%	2.9%	1262

Trust

21. Is it important that other people also trust the payment system you use?

Very important	Quite important	Neutral	Quite unimportant	Very unimportant	Total N
34.9%	37.5%	19.3%	3.9%	4.4%	1271

22. If a new payment system is introduced, will you trust *any* organisation that issues it, or only an established one, like a bank?

Established	Any	Total N
97.6%	2.4%	1289

23. Would you stop using a system if you feel that it's not trustworthy?

Certainly	Quite likely	Neutral	Rather not	Not at all	Total N
46.1%	48.3%	4.8%	.8%	.1%	1311

Applicability

24. Do you think a good shop should offer you the choice to pay with any payment system you like?

Agree	Partly agree	Disagree	Total N
85.8%	12.9%	1.3%	1313

25. Is it important that you can use one single particular payment system in most places you have to pay?

Very important	Quite important	Neutral	Quite unimportant	Very unimportant	Total N
59.8%	28.3%	9.6%	1.2%	1.0%	1285

26. Which of the following payment systems you would like to use in more points of sale?

	Cash	Debit cards	Credit cards	Smart cards	Credit cards on the Internet
Not at all	52.4%	21.3%	31.0%	48.3%	65.7%
Sometimes	11.8%	25.5%	31.4%	17.3%	23.5%
Certainly	35.7%	53.2%	37.6%	34.4%	10.8%
Total	1123	1255	827	729	591

Appendix C

Questionnaire

for measuring computer and Internet experience in the diary study (Chapter 4).

How do you feel about working with computers?

☐ I don't like working with computers
☐ I have no strong like of dislike working for with computers
☐ I like working with computers
☐ Other

Do you enjoy learning how to use new software applications?

☐ Yes ☐ Sometimes ☐ Never
☐ Other (please describe)

How enthusiastic you are about technology?

Very little ①☐ ②☐ ③☐ ④☐ Very enthusiastic

Have you performed the following activities online? (check all that apply)

☐ ordered a product/service from a business, government or educational entity by filling out a form on the web
☐ made a purchase online for more than €50/fl.100
☐ created a web page
☐ customized a web page for yourself (e.g. MyYahoo, CNN Custom News)
☐ changed your browser's "start-up" or "home" page
☐ changed your "cookie" preferences
☐ participated in an online chat or discussion (not including email)
☐ listened to a radio broadcast online

☐ made a telephone call online
☐ used a nationwide online directory to find an address or telephone number
☐ taken a seminar or class about the Web or Internet
☐ bought a book to learn more about the Web or Internet

How would you describe your general level of computer experience?
☐ None (I have never used any software applications)
☐ Low (I have used only one two software applications)
☐ Moderately low (I have used between three and ten software applications)
☐ Moderately high (I have used more than ten software applications)
☐ High (I have used more than ten software applications and have programming experience)
☐ Other

Do you have experience with one or more of the following? (check all that apply)
☐ Credit cards on the Internet
☐ Credit cards offline
☐ Credit or Debit cards with pin-code
☐ An electronic payment system on the Internet

What is the name of the payment system you are going to use for this study?

How long have you been using the system (tick one time period that applies)?
_____ **weeks** ☐ **months** ☐ **years** ☐

How frequently do you use your payment system for payments (tick one time period that applies)?
_____ times per: **day** ☐ **week** ☐ **month** ☐ **year** ☐

How many payments on average do you do in one session (tick one time period that applies)?

_____ payments **per session**

Appendix D

Design recommendations

Structure of a design recommendation

The design recommendations are laid out in a structured template form:

- Number and title
- Detailed description
- Recommendation type
- General problem
- Examples, known uses
- Expert comments.

The following section lists all design recommendations in detail. For the ease of the overview a summary is provided below.

Overview of the design recommendations

DR 1. Inform users about security measures and provide a security policy.

DR 2. Explain what type and details of personal information are to be retained, why, and how they will be used.

DR 3. Provide a clear and explicit policy on privacy and make it noticeable to users.

DR 4. Give users control over the costs of the payment system usage.

DR 5. Allow users to control critical actions and information.

DR 6. Seek reputation and trust transference from reputed partners and technology providers, and communicate trust transference to users.

DR 7. Take measures to address risks and inform users about these measures.

DR 8. Interaction with the payment system should resemble users' expectations about the payments process.

DR 9. The interface should be presented in a logical, clear and understandable way.

DR 10. Provide features of automatisation of payments.

DR 11. Provide features of customization of payment environments.

DR 12. Provide well-designed authentication.

The expert comments on the recommendations were made by an expert consultant of the Postbank's Department of New Business Technology in relation to Postbank Betaallijn (Chapter 5), and quoted as personal communication, (Krabbenbos, 2003).

Design recommendations in detail

DR 1. Inform users about security measures and provide security policy.

Detailed description:

- Security policy: the existence and strength of security measures used in the payment system to protect users should be clearly explained to the users. This can be done by providing information in e.g. a paper manual, online help, or dedicating a part of the web site to the security policy.
- Provide clear visibility of security measures employed. This can be done by describing which security measures and technology have been used and implemented.
- Explain why the system is secure for transactions.
- Provide customer support (online or telephone) on security-related issues.
- Supply regular information updates on changes and upgrades in security and the security policy; show the date of the latest update.
- Address security issues specific to 1) a single payment (e.g. communicate to the users security of transactions), and to 2) the system's operations in general, (e.g. provide ability to deactivate passwords or block accounts offline by phone).
- If using services or technology from reputed security institutions or companies, inform the users about this cooperation, e.g. demonstrate security seals or logos of the security organisations.
- Explain which security measures are employed for information management and storage, provided that such information will not compromise security.
- Do not try to cheat hackers by providing wrong and misleading information about the system. Hackers will know the real situation via different means, however the potential harm of misinforming the users may damage the reputation severely.

Recommendation type: trust, security.

General Problem: Without believing or understanding that the payment system is secure, users will not use it because they may fear certain risks, be afraid they could lose

their money, and as a result will not trust the system. Even a secure system is not necessarily perceived as such, because security technologies and measures are not always visible to the users. This can be repaired by this recommendation.

Example: Dutch payment system Global Collect provides textual information in a dedicated web site section describing which security solutions and measures have been implemented. It explains why the system is secure for transactions, Figure D1. Example of a security logotype is presented in Figure D2.

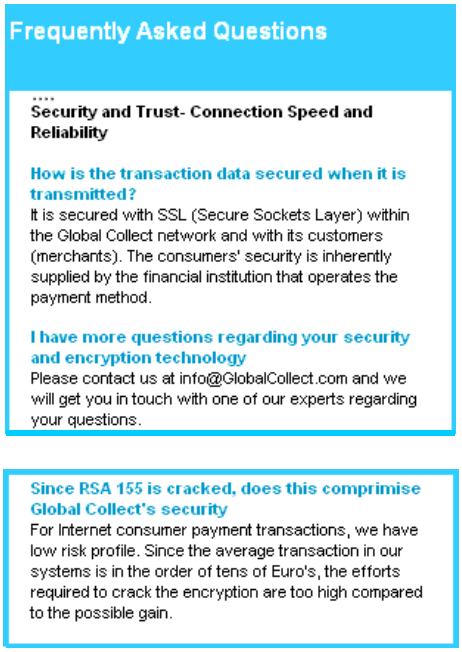


Figure D1. Example of a security policy and help. Source: Global Collect, July 2002.

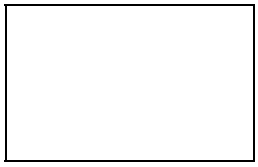


Figure D2. SSL security logo. Source: Thawte

Expert comments: 'This design recommendation is testable by showing two different product brochures or websites (from accepting merchants).

In our test (the proof of concept of the Betaallijn) we have used:

- Our trusted brand
- A brochure with information
- FAQ list online
- No [security] signs, logos.'

DR 2. Explain what type and details of personal information are asked, why, and how they will be used and retained

Detailed description:

- Provide explanations why the requested personal details are necessary and how these details will be used in the system.
- Do not request users to supply more personal information than necessary, even if you do not consider this information to be of (critical) importance to the users.
- Be sure that information asked is within context of this particular payment situation, and no unrelated or loosely connected information is asked.
- Take into consideration how critical the personal information is 1) to the *users* in the given payment situation and 2) to the *context and types of payments* which the users are planning to make. If the requested information is too critical in any of these cases, the users may refrain from paying with the system.

Recommendation type: trust, privacy.

General Problem: Users may not trust and avoid using a system that does not provide explanation on how personal details are used and why they are necessary, fearing misuse and possible risks associated with revealing their personal information.

Example: Payment system for ebay.com auctions Billpoint provided the detailed explanation about what information is colleted, Figure D3.

Expert comments: "Testable by showing two different product brochures or websites (from accepting merchants). In our test we have used: No information about personal information".

Help

Who will see my information?

eBay Payments / Billpoint is fully committed to protecting the privacy of all of your personal information, as well as information related to your transactions. eBay Payments / Billpoint does not sell or share any of your personal information.

eBay Payments / Billpoint only provides the seller with the information necessary to communicate with you effectively and to successfully complete your order. eBay Payments /

Billpoint shows the seller the following information:

Name
Telephone Number
E-mail Address
Billing Address
Shipping Address

eBay Payments / Billpoint does NOT show the seller your credit card number or your checking account number, and the seller will not need to collect it from you for any reason in order to complete a transaction.

To find out more about how eBay Payments / Billpoint safeguards your privacy, please visit the eBay Payments / Billpoint Privacy Policy.

Privacy policy

Our Commitment to Privacy

To help customers better understand the personal information we gather and the practices we employ, Billpoint has developed a set of privacy policies. These policies encompass several categories and attempt to answer the following questions:

How is personal information collected, used, and disclosed?
How can users cancel the service?
How does Billpoint use cookies?
How does Billpoint secure your information?
….

How is Personal Information Collected?

Personal information might be collected from you in several ways:

When you first registered with Billpoint

When you initially open a Billpoint account, we require your name, phone number, e-mail address, mailing address, billing address, credit card number, and credit card expiration date.
....

When you buy

When you purchase an item from a Billpoint seller, we require your name, e-mail address, phone number, billing address and shipping address. For credit card transactions, we require your credit card number and credit card expiration date.
....

When you register with co-branded partners

Billpoint is sometimes offered through other Internet services. We refer to these services as "our co-branded partners". If you pre-register for the Billpoint service through one of our co-branded partners, that website may provide personal information about you to Billpoint.

Figure D3. Example of help and a privacy policy. Source: BillPoint, a payment service for e-bay auctions, July 2002.

DR 3. Provide a clear and explicit policy on privacy and make it noticeable to users

Detailed description:

- Have a privacy policy for the payment system; explain the privacy policy in a clear and understandable way. Explain how personal information is stored and protected and who will have access to it, taking into account DR 2. Convince users that you will not sell or give out the personal information.
- Make the privacy policy visible and easily accessible by providing a link to it on all pages of the web site, include it in the manual, other documentation and in press advertising campaigns. Even if the users do not read the privacy policy, its presence could support a more trustworthy impression.
- Expose 'seals of privacy' issued by privacy monitoring organisations, or other similar privacy-related attributes.
- If the privacy policy is compliant with privacy laws or directives inform users about that (European privacy acts or directives, e.g. European Commission Data Protection Directive 95/46/EC).
- Do not use any personal information in another way than is stated in the privacy policy, unless the different use of this information is regulated or imposed by laws, (e.g. ordered by court).
- Provide regular updates on changes in the payment system's privacy policy.

Recommendation type: trust.

General Problem: Absence of a policy on privacy can undermine trust in the system. Unexpected or unexplained use of the personal information destroys trusts.

Examples: Most e-commerce web sites, e.g. Amazon.com, provide links to privacy at the registration pages. A considered privacy policy is present at the biggest e-commerce and business web sites, (e.g. ebay.com, idc.com, Amazon.com), see Figure D3 for the privacy policy of ebay.com's Billpoint payment system. An example of a privacy seal is in Figure D4.

*Expert comments: "*Testable by showing two different product brochures or websites (from accepting merchants). In our test we have used: No information on privacy/anonymity".

Figure D4. Privacy seal of BBBOnline.org

DR 4. Give users control over the costs of the payment system usage

Detailed description:

- Give users a complete and transparent overview of the costs associated with the use of the payment system.
- Provide a clear explanation of the costs involved in using the system (ownership costs, transaction costs). Hiding the costs can initially attract a number of users, but may also create bad publicity, which could be very harmful for the reputation.
- In costs calculations include all the taxes that a physical person should pay, e.g. VAT.
- If possible, offer sponsoring of any new EPS hardware and software required for the payment system, or consider providing it free charge.
- If the business model allows it, consider providing free use of the payment system to end users, relaying the transaction fees onto the merchants or the payees.

Recommendation type: control, trust.

General Problem: Promotion and usage costs that are placed on users may make the system less attractive to them. Hidden costs that appear in the course of later use may undermine trust in the payment system.

Example: Dutch banks ABN-AMRO and Rabobank provide hardware code calculators required for authentication in their e-banking services for free, as on June 2003. Online payment system PayPal is clear about the fee schedule for payments and offers discounts for loyal users. PayPal does not charge end users for sending and receiving

money; instead the merchant side pays the transaction fee. Figure D5 illustrates the fee schedule of PayPal.com.

	Personal Account	Premier/Business Account
Open an Account	Free	Free
Send Money	Free	Free
Withdraw Funds	Free for U.S. bank accounts Fees for non-U.S. banks	Free for U.S. bank accounts Fees for non-U.S. banks
Add Funds	Free	Free
Receive Funds	Free	0.7% + 30¢ to 2.9% + 30¢†
Multiple Currency Transactions	Exchange rate may apply*	Exchange rate may apply*

Figure D5. Example of the fee schedule of PayPal.com, August 2002. Source: PayPal.com.

Another interesting example of promotion of a payment system through the cost reduction for consumers is the use of Dutch payment system Moxmo for SMS payments on a Dutch TV show web site. It was possible to submit a vote to the show by sending SMS messages via the web site, paying for the messages with money from the Moxmo-wallet, instead of sending them via telecom operators. As a result, an SMS was 10 cents cheaper. Moxmo offered a clear overview and control over the costs of the paid SMS messages, Figure D6. This feature might attract some customers to use the payment system in the future.

*Expert comments: "*Testable by offering two different product brochures or different online information.

In our test we have used:

- 020 – phone number as only cost.
- Testable by offering [free] 0800 and [paid] 0900 number".

Figure D6. Promoting Moxmo payment system via cost benefits, Source: www.idols.nl

DR 5. Allow users to control critical actions and information

Detailed description:

- Users should have ability to rollback and cancel a payment any time before finally committing to it. The 'point of no return' when the payment is definitely made should be delayed as far as possible. A common practice of respectable Internet shops is to charge for an order just before the shipping is ready, e.g. even if the order is placed users may want to cancel it before it is dispatched. Despite the fact that merchants want to receive the payment as soon as possible, cancelling the payment may be easier and cheaper for the merchant than refunding it.
- Provide the ability to change all personal information, such as names, addresses, email, contact details, etc. Provide reasonably easy ways to change the data, for example, make it easier than going through the registration process once again to create a new account.
- Provide the possibility to recover passwords that is relatively easier in comparison to the registration process to create a new account.

- Provide the ability to deactivate passwords or block accounts offline, for instance by telephone.
- Provide alternative ways of authentication (e.g. biometrics, code calculators).
- Provide a clear and visible feedback on all payment tasks and actions. Provide transactions statements to make control over transactions easier and to help to detect problems.

Recommendation type: control, trust, usability.

General Problem: The inability to correct errors or cancel wrong actions deprives users from the feeling of control over the situation and can eventually undermine trust. Unable to recover passwords, or change their personal data, users may have to register once more, which is unacceptable from the perspectives of usability and performance. Limited ability to change, modify and remove data can undermine trust and lower usability.

Example: Rollback and order cancellation of an order are implemented at the web site of bookseller Amazon.com, and in most of Internet shops. An example of account management is presented in Figure D7.

*Expert comments: "*Testable by offering two different processes or two different product brochures. In our test we have used:

1a. [Possibility of a] rollback

1b. 'Point of no return' is very late

1c. Cancellation is possible.

2a. Refund is not possible within the system, paid = paid

2b. Deactivate and block the code was a test-period-only procedure".

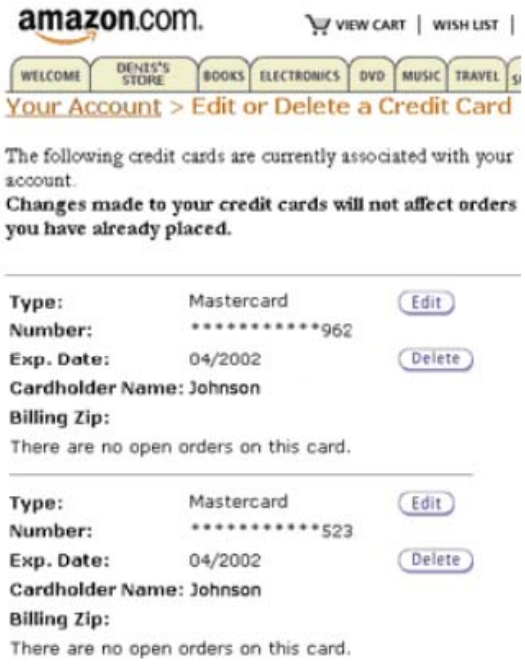


Figure D7. Updating credit card information in the account management of the web site. Source: Amazon.com, account management, July 2002.

DR 6. Seek reputation and trust transference from reputed partners and technology providers, and communicate trust transference to users

Detailed description:

- Seek cooperation and backing from reputed organisations to achieve transference of their reputation and users' trust to the payment system.
- Inform users about partnerships or business relationships with reputed technology, financial, business and government institutions.
- The place to communicate this information to users is help, about, documentation, FAQ sections, etc.
- Be reviewed by trusted third parties, display their logos for and provide links to their websites. Expose 'seals of trust' or other similar trust related attributes.

Recommendation type: trust

General Problem: The lack of trust from other organisations can undermine users' trust. A new, unknown company may fail to gain user trust without trust transference from other trusted organisations.

Example: See Figures D2 and D4 for examples of using logos of reputed organisations for trust transference.

Expert comments: 'Testable by showing two different product brochures or websites (from accepting merchants) with and without logo, brand, etc. In our test we have used:

- Our own trusted brand with an unknown product name;
- No additional [trusted] signs".

DR 7. Take measures to address risks and inform users about these measures

Detailed description:

- Make sure that customers are aware of the risks associated with the use of the payment system, communication channels, with the destination and amount of payment, with revealing personal information to a payee, etc. Communicate these risks to users in an understandable manner. Explain what measures are taken to counter these risks and reassure users it is safe to use the payment system.
- Demonstrate the image of the company operating the system as professional and competent. Provide detailed company and contact information.
- The system should create its added value to justify the risk taking, and it should be clearly communicated and evident to users.
- There should be a clear statement that the money used in the system originate from a real government monetary system and will be accepted by other parties.
- Create a policy to resolve situations when feared events happen (e.g. define a refund policy in case of losses).
- If applicable, provide users and merchants with an insuring coverage for losses, damages, etc., caused by the use of the payment system.
- Communicate to users encouraging publicity about the system. It can help to alleviate certain users' fears about risks.

- Address risks associated with the use of novel or controversial technology, such as biometrics systems for authentication, explain how EPS customers are protected from these risks and how they will benefit from the new technology.

Recommendation type: trust.

General Problem: Not addressing risks undermines trust. Misconception about risks can lead to insecure user behaviour, and can eventually decrease trust.

Examples: Insurance provided by online stock broker E*Trade provides protection of customers' money in case of calamities. Many web sites, e.g. Amazon.com, PayPal, Global Collect, provide protection of transactions with a secure SLL connection and explain in detail why paying at their sites is secure.

*Expert comments: "*Testable by showing two different product brochures or websites (from accepting merchants). In our test we have used:

- Our trusted brand
- Brochure with information and product conditions
- FAQ list online".

DR 8. Interaction with the payment system should resemble users' expectations about the payments process

Detailed description:

- Interaction should resemble users' model and expectations of payments process based on their previous experience and current needs. If the system introduces new concepts and models of paying, the users should be educated to get used to these innovations.
- Employ user testing to find out if users perceive the interaction with the system adequately.
- Avoid frequent changes in the logic of interaction over time.
- Ask user input in a sequence of simple and well-explained steps.
- Render the interaction and user interface in a form of familiar payment applications (e.g. automatic teller machine, bank payment blanks and records, credit cards, etc.). Consider if it is appropriate to render user interactions in a way that

resembles corresponding types of payments (bills, Internet payments, etc), or if it would be better to provide a uniform interaction process for all types of payments.

- Interaction should be presented in a style that is familiar to users, e.g. that is adopted from existing popular payment services and e-commerce sites, (in a similar fashion as Amazon's style is copied by many booksellers).
- 'Wizards' guiding users step-by-step in the interaction process may be helpful to educate them on how to perform novel or previously inexperienced sequences of tasks.

Recommendation type: usability.

General Problem: Unnatural and unintuitive interaction lowers performance and eventual acceptance. If a system works in a different way than users expect from a system of its kind, it may create a steeper learning curve. Time to adapt may grow, and reduce performance. Example of a problem: the sequence of the input fields for giro payments in ABN-AMRO Internet Banking does not resemble a real-life paper giro form. A customer had problems getting used to this interaction sequence.

Example: The step-by-step payment process in Rabobank Direct Betalen (online banking) resembles the familiar offline payment procedure (as recorded on June, 2002).

Expert comments: "Testable by showing two different product brochures. In our test we have used:

- A similar user model of standard voice banking functionalities.
- A step-by-step example in the brochure.

Our interaction system is based on a model used for years and resembles the popular PIN-system".

DR 9. The interfaces should be presented in a logical, clear and understandable way

Detailed description:

- Minimise the number of steps (consecutive web pages) and actions (e.g. authorisation procedures) to complete a payment. For example, minimise the number of consecutive web pages for registration and authorisation, informing the users about the numbers of pages beforehand.
- The duration of a payment should not be too long. It should be proportional to the whole process (on average) of purchase interaction phase (see section 1.4.1).
- Render the interface style according to industry standards, or in a style familiar to the users from similar web sites of the correspondent domain. For instance many online booksellers render their interface similar to Amazon.com, which is becoming an interface standard for online bookshops.

Recommendation type: usability.

General Problem: A messy, clumsy interface will result in low usability and performance.

Example: In ABN-AMRO Electronic Banking details of completed transactions are presented in a form similar to bank's paper records sent to customers by regular post, this makes it easy to read and find information.

*Expert comments: "*Testable by offering two different interfaces. Our interface is not visible but audible. Our interaction system is based on a model used for years and resembles the popular PIN-system".

DR 10. Provide features of automatisation of payments

Detailed description:

- Provide the functionality of *scheduled payments*, or periodic payments, enabling users to set time and time span for the payments execution. Enable setting exceptions to the payment schedules.
- Provide the functionality of *multiple* (batch) *payments*: executing several payments at once, with one authorisation.

- Provide the functionality of *address books*, a user-managed contacts database for quick access to frequent payees' information, such as account number, addressed, and frequent payment details.
- For standard payments like utilities, bills, or direct debits provide templates that resemble well-known offline forms, where users can quickly fill in required fields.

Recommendation type: usability.

General Problem: Absence of automatisation of payment actions could decrease performance and eventual user acceptance.

Example: The address book function in ABN-AMRO Electronic banking. In ABN-AMRO Electronic banking payments can be effected by a scheduled time period.

Expert comments: "Not testable [at the current stage]. We offer a "direct payment", belonging to "direct purchasing". Your recommendation have to do with transferring money instead of paying money ("e-banking systems" instead of "payment systems"). A payment includes a direct notification to the receiving party. Comsys [the company developer of the EPS] shall investigate if it's possible to do any automatisation".

DR 11. Provide features of customization of payment environments

Detailed description:

For improving ease of use, satisfaction and performance provide the following features of the payment environment:

- Provide features of locale customisation: currency conversion, language.
- Provide ability to personalize payments with details of payments, (personal) messages, gift cards, etc.
- Provide ability to attach invoices, bills, etc. in electronic form along with a payment.
- Provide the functionality of multiple logins, restricted access for employees, family members.

Recommendation type: usability.

General Problem: Lack of customisation and features could lower performance and (perceived) usefulness.

Example: For different family members a parent could set up restricted logins e.g. setting payment limits and selecting adequate web sites for payments of the children.

Expert comments:

"Testable. [...] We do not yet provide utilities to recover passwords, or alternative authentication (e.g. biometrics, code calculators) systems".

Protect your password.

Don't write down your password - memorize it. In particular, don't write it down and leave it anywhere, and don't place it in an unencrypted file! Use unrelated passwords for systems controlled by different organisations. Don't give or share your password, in particular to someone claiming to be from computer support or a vendor unless you are sure that are who they say they are. Don't let anyone watch you enter your password. Don't enter your password to a computer you don't trust or if things Use the password for a limited time and change it periodically.

Choose a hard-to-guess password.

[Our system] will try to prevent you from choosing a really bad password, but it isn't foolproof; create your password wisely. Don't use something you'd find in a dictionary (in any language or jargon). Don't use a name (including that of a spouse, parent, child, pet, fantasy character, famous person, and location) or any variation of your personal or account name. Don't use accessible information about you (such as your phone number, license plate, or social security number) or your environment. Don't use a birthday or a simple pattern (such as backwards, followed by a digit, or preceded by a digit. Instead, use a mixture of upper and lower case letters, as well as digits or punctuation. When choosing a new password, make sure it's unrelated to any previous password. Use long passwords (say 8 characters long). You might use a word pair with punctuation inserted, a pass phrase (an understandable sequence of words), or the first letter of each word in a pass phrase.

Figure D8. *Example of password guidelines*. Source: cPanel X, January 2004.

DR 12. Provide well-designed authentication

Detailed description:

- Preserve login status or retain session information for access to non-critical operations so that users do not have to authenticate themselves unnecessarily frequently. Do not require users to re-log in or authenticate themselves prior to less significant operations, such as viewing account status.
- Refer to the industry practice (such as employing authentications mechanisms used at the popular e-commerce and EPS web sites) in managing authentication and passwords, including practices for recovering lost passwords, cashing passwords in the web browser for further use, retrieving, resetting, and renewal of passwords. Even if the password is lost, its retrieval or resetting should be done as quickly and easily as possible, and with minimal workload for users without compromising security.
- Limit the number of authentication steps (a password or challenge-response authorisation) required for access to the system (for logins, account overview, payments) to preferably not more than 2 steps.
- Suggest guidelines on selecting effective and easy to remember passwords.
- Strive to balance password length, symbols, and case sensitivity. E.g. too short passwords are dangerous, too long are hard to remember. If users are afraid of losing their passwords, and have to rely on recording passwords in any form (e.g. written down on paper) this can compromise their passwords.
- Warn users to avoid using symbols that can be dependent on the language layout, such as logins and passwords in their own language. This can limit or complicate access to the EPS in other countries with a different language.
- Take into account the relation of the system's login to existing passwords (e.g. for an EPS based on electronic banking examine if it would be reasonable to a use the existing e-banking PIN-code). Consider if this can compromise security.
- Provide ability to change passwords easily and quickly, without compromising security.

Recommendation type: usability, trust.

Example: To ensure high security, Paypal.com never allows saving the password in the browser cash in the default mode, users will have to re-enter it again. Figures D8 and D9 suggest password guidelines.

General Problem: Users are ready to go through authentication, even if they find it inconvenient, because they understand its need and importance. However, excessively hard authentication can still lower usability and scare the users away, especially if compared with relatively easier authorisation in other systems.

Expert comment: "Our authentication process is based on a model used for years. The code used in the test is 6 digits (for test reasons), the real code will be the already known and [there will be] used 5-figure Girofoon-code or a new code".

Figure D9. PayPal password tips.
Source PayPal, 2003.

Appendix E

Questionnaire for the experimental study

Repeated measures

The following questions were repeated after each task, this would let see how user attitudes change from task to task and run repeated measures analysis.

Q1 How high would you rate your trust in the system at this moment?

Very low Very High

1	2	3	4	5	6	7	☐ Don't know

Q2 Do you feel it would be safe to make transaction with your money using this system?

Completely unsafe Completely safe

-3	-2	-1	0	+1	+2	+3	☐ Don't know

Q3 Do you feel your personal information is sufficiently protected in this system?

Completely un-protected Completely protected

1	2	3	4	5	6	7	☐ Don't know

Q4 I think I would like to use this system frequently (often).

Strongly Disagree Strongly Agree

-3	-2	-1	0	+1	+2	+3	☐ Don't know

Q5 I found the system complex.

Strongly Disagree Strongly Agree

-3	-2	-1	0	+1	+2	+3	☐ Don't know

Q6 I thought the system was easy to use.

Strongly Disagree Strongly Agree

-3	-2	-1	0	+1	+2	+3	☐ Don't know

Q7 I think that I would need the support of a technical person to use this system.

Strongly Disagree Strongly Agree

-3	-2	-1	0	+1	+2	+3	☐ Don't know

Q8 I found the various functions in this system were well integrated.

Strongly Disagree Strongly Agree

-3	-2	-1	0	+1	+2	+3	☐ Don't know

Q9 I felt very confident using the system.

Strongly Disagree Strongly Agree

-3	-2	-1	0	+1	+2	+3	☐ Don't know

Q10 I need to learn a lot of things before I could get going with this system.

Strongly Disagree Strongly Agree

-3	-2	-1	0	+1	+2	+3	☐ Don't know

Q11 The instructions on the web page and the paper help are useful for the task.

Strongly Disagree Strongly Agree

-3	-2	-1	0	+1	+2	+3	☐ Don't know

Task-specific questions

Task 1

Q13 Do you find the system fast to use?

Very slow Very Fast

1	2	3	4	5	6	7	☐ Don't know

Q14 How quick could you do the task?

Very slow Very quick

1	2	3	4	5	6	7	☐ Don't know

Q15 Are you comfortable using your personal information with this system?

Not comfortable at all Very comfortable

1	2	3	4	5	6	7	☐ Don't know

Q16 What do you think about the number of confirmations you have to make for one payment?

Too many confirmations (bevestigingen) Too few confirmations (bevestigingen)

-3	-2	-1	0	+1	+2	+3	☐ Don't know

Task2

Q13 Do you feel sufficiently informed about security in the Betaallijn?

Not informed at all — Fully informed

1	2	3	4	5	6	7

☐ Don't know

Q14 How does the information provided about security measures influence your trust in the Betaallijn as a payment system?

Decreases your feeling of trust — Increases your feeling of trust

-3	-2	-1	0	+1	+2	+3

☐ Don't know

Q15 How does the ability to block your betaalcode give you a feeling of control over the situation?

Decreases the feeling of control — Increases the feeling of control

-3	-2	-1	0	+1	+2	+3

☐ Don't know

Q16 How does the ability to block the betaalcode influence your trust?

Decreases your trust — Increases your trust

-3	-2	-1	0	+1	+2	+3

☐ Don't know

Q17 Do you feel you were in control over the situation when using the Betaallijn for this task?

Completely out of control — Completely in control

1	2	3	4	5	6	7

☐ Don't know

Q18 How does the fact that there is a customer service line operated by real people influence your trust?

Decreases your trust — Increases your trust

-3	-2	-1	0	+1	+2	+3

☐ Don't know

Task3

Q13 What's your opinion about the way you had to do these rent payments?

Very difficult — Very easy

-3	-2	-1	0	+1	+2	+3

☐ Don't know

Q14 Very slow — Very fast

1	2	3	4	5	6	7

☐ Don't know

Q15 Rather useless function — Very useful function

-3	-2	-1	0	+1	+2	+3

☐ Don't know

Q16 Do you feel that the costs associated with using the Betaallijn (paying for the call) are appropriate?

Completely inappropriate — Completely appropriate

-3	-2	-1	0	+1	+2	+3

☐ Don't know

Q17 How much you would be prepared to pay for the call to the Betaallijn, per minute?

1	2	3	4	5	6	7	☐ Don't know
0 cents p/m	2-3 cents p/m	10-15 cents p/m	15-25 cents p/m	25-50 cents p/m	51cents - €1 p/m	as much as I'm asked	

Q18 Do you think the length of the betaalcode is appropriate?

Too long — Too short

-3	-2	-1	0	+1	+2	+3	☐ Don't know

Task 4

Q13 I think that the procedure to re-activate the betaalcode would be easier than to register again.

Strongly Disagree — Strongly Agree

-3	-2	-1	0	+1	+2	+3	☐ Don't know

Q14 Do you feel you were in control when using the Betaallijn for this task?

Completely out of control — Completely in control

1	2	3	4	5	6	7	☐ Don't know

Q15 How does the way you can reactivate the betaalcode influence your trust?

Decreases your trust — Increases your trust

-3	-2	-1	0	+1	+2	+3	☐ Don't know

Q16 How does the ability to reactivate the betaalcode give you a feeling of control over the situation?

Decreases the feeling of control — Increases the feeling of control

-3	-2	-1	0	+1	+2	+3	☐ Don't know

Q17 Do you feel it's safe to use the system?

Completely unsafe — Completely safe

1	2	3	4	5	6	7	☐ Don't know

Task 5

Q13 What's your opinion about the way you had to make these several payments in the system?

Very difficult — Very easy

-3	-2	-1	0	+1	+2	+3	☐ Don't know

Q14 Very slow — Very fast

1	2	3	4	5	6	7	☐ Don't know

Q15 Rather useless function — Very useful function

-3	-2	-1	0	+1	+2	+3	☐ Don't know

Q16 Would paying for the telephone call to de Betaallijn be suitable for you (if you you'd use de Betaallijn for your payments)?

I would definitely not pay for the call — I would certainly pay for the call

1	2	3	4	5	6	7	☐ Don't know

Q17 Are you comfortable with the way you have to identify yourself in the system?

Very uncomfortable — Very comfortable

-3	-2	-1	0	+1	+2	+3	☐ Don't know

Q18 Do you feel that the telephone costs associated with using the payment system are appropriate?

Completely inappropriate — Completely appropriate

-3	-2	-1	0	+1	+2	+3	☐ Don't know

Q19 Do you feel that you are in control of the costs of when using the Betaallijn?

Completely out of control — Completely in control

1	2	3	4	5	6	7	☐ Don't know

Q20 Do you think the number of confirmations is appropriate to do your payment?

Too many confirmations (bevestigingen) Too few confirmations (bevestigingen)

-3	-2	-1	0	+1	+2	+3	☐ Don't know

Q21 Do you think the length of the betaalcode is appropriate?

Too long Too short

-3	-2	-1	0	+1	+2	+3	☐ Don't know

Q22 Does the fact that the system is offered by Postbank influence your trust in the system?

Decreases your trust Increases your trust

-3	-2	-1	0	+1	+2	+3	☐ Don't know

Q23 Would you be likely to use the system for your Internet payments?

Very likely Very unlikely

-3	-2	-1	0	+1	+2	+3	☐ Don't know

References

Abrazhevich, D. & Markopoulos, P. (2002). Diary study on internet payment systems. In Sharp, H., Chalk, P., LePeuple, J. & Rosbottom, J. (Ed.), Proceedings of the Conference on Human Computer Interaction HCI 2002, London, UK, September 2-6, 2002. (pp. 42-46). London: HCI 2002.

Abrazhevich, D. (2001a). A survey of user attitudes towards electronic payment systems. The 15th Annual Conference of the Human Computer Interaction Group of the British Computer Society, IHM-HCI-2001, vol. 2. (pp. 69-71). Toulouse, France: Cepadues-Editions.

Abrazhevich, D. (2001b). Classification and characteristics of electronic payment systems. In K.Bauknecht, S. K. Madria, & G. Pernul (Eds.), Lecture Notes in Computer Science 2115, (pp. 81-90). Berlin: Springer-Verlag,.

Abrazhevich, D. (2001c). Electronic payment systems: issues of user acceptance. In B.Stanford-Smith and E.Chiozza (Eds.), E-work and E-commerce, (pp. 354-360). IOS Press .

Abrazhevich, D. (2002). Importance of user-related factors in electronic payment systems. In J.E.J.Prins, P. M. A. Ribbers, H. C. A. van Tilborg, A. F. L. Veth, & J. G. L. van der Wees (Eds.), Trust in Electronic Commerce - The Role of Trust From a Legal, an Organisational and a Technical Point of View, The Hague : Kluwer Law International.

Adler, A., Gujar, A., Harrison, B. L., O'Hara, K., & Sellen, A. (1998). A diary study of work-related reading: design implications for digital reading devices. In C.Karat, A. Lund, J. Coutaz, & J. Karat (Eds.), Human Factors in Computing Systems. CHI 98 Conference Proceedings, (pp. 241-248). New York, NY, USA: ACM.

APACS (2002). Card-not-Present (CNP) Transactions. Fraud prevention guidelines for CNP retailers. London: Association for Payment Clearing Services.

Asmussen, C. G., Raschke, T., & Arend, C. (2002). User perception of internet security - European consumer survey 2002, IDC Report, IDC.

Asokan, N., Janson, P., Steiner, M., & Waidner, M. (1997). The state of the art in electronic payment systems. IEEE Computer, 30(9), 28-35.

BIS (2000). Survey of electronic money developments, May 2000. Switzerland: Bank for International Settlements.

BIS (2001). Survey of electronic money developments, November 2001. Switzerland: Bank for International Settlements.

Bohle, K. (2001a). Electronic Payments 2001 – Food for thought. Electronic Payment Systems Observatory (ePSO). Seville, Spain: Joint Research Center of the European Commission.

Bohle, K. (2001b). The Potential of server-based internet payment systems. Electronic Payment Systems Observatory (ePSO). Seville, Spain: Joint Research Center of the European Commission.

Boly, J. P., Bosselaers, A., Cramer, R., Michelsen, R., Mjolsnes, S., Muller, F., Pedersen, T., Pfitzmann, B., & Rooij, P. d. (1994). The ESPRIT Project CAFE - High security digital payment systems. Lecture Notes in Computer Science 875, (pp. 217-230). Springer.

Brands, S. A. (1995). Off-line electronic cash based on secret-key certificates. Amsterdam: Centrum voor Wiskunde en Informatica.

Brooke, J. (1996). SUS: a Quick and dirty usability scale. In P.W.Jordan, B. Thomas, B. A. Weerdmeester, & I. L. McClelland (Eds.), Usability Evaluation in Industry, London: Taylor & Francis.

Burkhardt, M. E. (1994). Social interaction effects following a technological change: A longitudinal investigation. Academy of Management Journal, 37 (4), 869-898.

Carayon, P. & Hajnal, C. (1993). A diary study of computer use and worker stress: preliminary results. In G.Salvendy & M. J. Smith (Eds.), Human Computer Interaction. Proceedings of the Fifth International Conference on Human Computer Interaction HCI International '93, (pp. 715-720). Amsterdam, Netherlands: Elsevier.

Caunter, N. (2001). The real cost of fraud to E-tailers. Computer Fraud & Security, 2001 (1), p. 17.

Chaum, D. (1992). Achieving electronic privacy. Scientific American, August 1992, 96-101.

Chin, J. P., Herring, R. D., & Elliott-Familant, M. (1992). A usability and diary study assessing the effectiveness of call acceptance lists. In Proceedings of the Human Fac-

tors Society 36th Annual Meeting. Innovations for Interactions, (pp. 216-220). Santa Monica, CA, USA: Human Factors Society.

Cook, T. D. & Campbell, D. T. (1979). Quasi-experimentation: design and analysis issues for field settings. Rand McNally.

Corbin, J. & Strauss, A. (1990). Grounded theory research: procedures, canons, and evaluative criteria. Qualitative Sociology, 13, 3-21.

Cox, P. (2001, June 22). PayPal and FBI team up. Wall Street Journal. WSJ Online, US edition.

Davis, F. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13 (3), 319-340.

Davis, F. (1993). User acceptance of information technology: systems characteristics, user perceptions and behaviroal impacts. International Journal of Man-Machine Studies, 38 (3), 475-487.

Davis, F., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: a comparison of two theoretical models. Management Science, 35, 982-1003.

Dillon, A. & Morris, M. G. (1996). User acceptance of information technology: Theories and models. Annual Review of Information Science and Technology, 31, 3-32.

ECB (2001). Payment and securities settlement systems in the European Union. European Central Bank.

ECB (2003). E-payments in Europe – the Eurosystem's perspective. European Central Bank.

Egger, F. N. (2003). From interactions to transactions: designing the trust experience for business-to-consumer electronic commerce. PhD Thesis. The Netherlands: Eindhoven University of Technology.

Elliott, G. J., Jones, E., & Barker, P. (2002). A grounded theory approach to modelling learnability of hypermedia authoring tools. Interacting with Computers, 14, 547-574.

Enos, L. (2000). Apple licenses Amazon's 1-click technology. E-Commerce Times. Retrieved Jan. 12, 2004, Available from:
http: //www.ecommercetimes.com/perl/story/4322.html

Evans, D. S. & Schmalensee, R. (1999). Paying with plastic: the digital revolution in buying and borrowing. Cambridge: MIT Press.

Fishbein, M. & Ajzen, I. (1975). Belief, attitude, intention and behavior: an introduction to theory and research. Reading, Mass.: Addison-Wesley.

Flick, U. (1998). An Introduction to qualitative research. London: Sage.

Flynn, N. L. (2001). The E-policy handbook : designing and implementing effective E-mail, Internet, and software policies. New York: Amacom.

Glassman, S. & Manasse, M. (1995). The Millicent protocol for inexpensive electronic commerce. In Proc. of the 4th International World Wide Web Conference, (pp. 603-618), Boston, Massachusetts, USA.

Gray, W. D. & Salzman, M. C. (1998). Damaged merchandise? A review of experiments that compare usability evaluation methods. Human-Computer Interaction, 13(3), 203-261.

Guttmann, R. (2003). Cybercash: the coming era of electronic money. Basingstoke: Palgrave.

GVU (1998). GVU's 10th WWW User Survey. GVU. Retrieved Jan. 12, 2004, Available from: http: //www.gvu.gatech.edu/user_surveys/survey-1998-10/

Hauser, R., Steiner, M., & Waidner, M. (1996). Micro-payments based on iKP. In Proceedings of the 14th Worldwide Congress on Computer and Communications Security Protection, (pp. 67-84).

Het Financieele Dagblad (2001, March 20). MKB dreigt met boycot chipknip. The Netherlands: Het Financieele Dagblad.

Hewett, T. T., Baecker, R., Card, S., Carey, T., Gasen, J., Mantei, M., Perlman, G., Strong, G., & Verplank, W. (1992). ACM SIGCHI Curricula for Human-Computer Interaction. New York: ACM.

Humphrey, D. B. (1995). Payment systems: principles, practice, and improvements. Technical paper 260. Washington, D.C.: The World Bank.

Humphrey, D. B., M. Kim, M. & Vale, B. (2001). Realizing the gains from electronic payments: costs, pricing, and payment choice, Journal of Money, Credit and Banking, 33(2), 216-234.

IFCC (2003). IFCC 2002 Internet fraud report. The Internet Fraud Complaint Center.

ISO 9241 (1996). ISO 9241. Ergonomic requirements for office work with visual display terminals, Part 11.

Jupiter Media Metrix (2000). Internet Payments. Jupiter Media Metrix.

Kalakota, R. & Whinston, A. (1997). Electronic commerce: a manager's guide. Addison-Wesley.

Keats, D. M. (2000). Interviewing: a practical guide for students and professionals. Buckingham: Open University Press.

Krabbenbos, M. (2003). Personal communication.

Kuttner, K. N. & McAndrews, J. J. (2001). Personal on-line payments. Economic Policy Review, New York Federal Reserve Bank, December 2001, (pp. 35-50).

Langdon, C. S., Roghe, F., & Shaw, M. J. (2000). Consumer mass market online payment solutions. In M.J. Shaw, R. Blanning, & T. Strader (Eds.), Handbook On Electronic Commerce, (pp. 273-288).

Laudon, K. C. & Traver, C. G. (2002). E-commerce: business, technology, society. London: Addison Wesley.

Lelieveldt, S. (2001). E-Purses and Chip Cards in the Netherlands. ePSO-Newsletter, 3. Seville, Spain: ePSO.

Libbenga, J. (2001, March 9). Ondergang Chipper markeert nieuw begin. Automatisering Gids, No. 10. The Netherlands.

Lietaer, B. (2002). The Future of Payment Systems. Unisys Corporation.

Long, J. B. & Dowell, J. (1989). Conceptions of the discipline of HCI: craft, applied science, and engineering. In A. Sutcliffe & L. Macaulay (Eds.), People and Computers: The theory and practice of HCI. British Computer Society Human-Computer Interaction Specialist Group, (pp. 9-32), Cambridge: CUP.

Lynch, D. C. & Lundquist, L. (1996). Digital money: the new era of Internet commerce. Chichester: Wiley.

Mackay, W. E. & Fayard, A. L. (1997). HCI, natural science and design: a framework for triangulation across disciplines. In Proceedings of Designing Interactive Systems, DIS'97, (pp.223-234) Amsterdam, the Netherlands: ACM.

Martin, R. (1994). Mondex: the way forward? Cards International, 104, 9-14.

Maxwell, S. E. & Delaney, H. D. (2000). Designing experiments and analyzing data: a model comparison perspective. London: Lawrence Erlbaum Associates.

Mayhew, D. J. (1999). The usability engineering lifecycle: a practitioner's handbook for user interface design. San Francisco: Morgan Kaufmann.

Medvinsky, G. & Neuman, B. C. (1993). Netcash: A design for practical electronic currency on the internet. Proceedings Of First ACM Conference On Computer and Communication Security, ACM.

Medvinsky, G. & Neuman, B. C. (1995). Requirements for network payment: the netcheque perspective. Proceedings of IEEE Compcon 95, San Francisco.

Nannery, M. (1998). Smart cards: stalled in Holland? Chain Store Age, 74 (11), p. 172.

Nielsen, J. (1999). Designing web usability. Indianapolis: New Riders Publishing.

Nielsen, J., Molich, R., Snyder, C., & Farrell, S. (2000). E-commerce user experience. Fremont, CA: Nielsen Norman Group.

Palen, L. & Salzman, M. (2002). Voice-mail diary studies for naturalistic data capture under mobile conditions. Proceedings of CSCW '02, (pp. 87-95), New Orleans, Louisiana, USA.

Perlman, G. (2000). Web-Based user interface evaluation with questionnaires. G.Perlman's Home Page. Retrieved Dec. 20, 2003, Available from: http: //www.acm.org/~perlman/question.html

Philippsohn, S. & Thomas, S. (2003). E-fraud - what companies face today. Computer Fraud & Security, 1, 7-9.

Plouffe, C. R., Hulland, J. S. and Vandenbosch, M. (2001). Research report: Richness versus parsimony in modelling technology adoption decisions - Understanding merchant adoption of a smart card-based payment system, Information Systems Research, 12 (2), 208-222.

Rauterberg, G. W. M. (2000). How to characterize a research line for user-system interaction. IPO Annual Progress Report, 35, 66-86.

Ribbers, P. M. A. & Heck, E. v. (2004). Introducing electronic auction systems in the Dutch flower industry - a comparison of two initiatives. Wirtschaftsinformatik, 40 (3), 223-231.

Rice, R. & Aydin, C. (2004). Attitudes toward new organisational technology: network proximity as a mechanism for social information processing. Administrative Science Quarterly, 36(2), 219-244.

Rieman, J. (1993). The diary study: a workplace-oriented tool to guide laboratory studies. Proceedings CHI'93, Conference on Human Factors in Computer Systems, (pp. 321-326), New York: ACM Press.

Rivest, R. L. & Shamir, A. (1996). Payword and Micromint: two simple micropayment schemes, (pp. 69-87). Cambridge, UK.

Rubin, H. J. & Rubin, I. S. (1995). Qualitative interviewing: the art of hearing data. London: Sage.

Salancik, G. R. & Pfeffer, J. (1978). A social information processing approach to job attitudes and task design. Administrative Science Quarterly, 23, 224-253.

Schoenmakers, B. (1998). Basic security of the ecash payment system. In B.Preneel & V. Rijmen (Eds.), Computer Security and Industrial Cryptography: State of the Art and Evolution, (pp. 342-356). Springer-Verlag.

Schreft, S. (2002) Clicking with dollars: how consumers can pay for purchases from e-tailers, Economic Review, Federal Reserve Bank of Kansas City, First Quarter 2002, (pp. 37-64).

Siegel, D. & Dray, S. M. (2001). New kid on the block: marketing organisations and interaction design. Interactions, March+April 2001, 19-24.

Siegel, D. & Dray, S. M. (2002). Exploring and using qualitative data. Tutorial presented at BCS-HCI 2002.

Smith, S. L. & Mosier, J. N. (1986). Guidelines for designing user interface software. MA, USA: Mitre Corporation.

Strauss, A. & Corbin, J. (1990). Basics of qualitative research: grounded theory procedures and techniques. London: Sage.

Van Hove, L. (1999). Electronic money and the network externalities theory: lessons for real life. Netnomics, 1 (2), 137-171.

Van Hove, L. (2004). Cost-based pricing of payment instruments: the state of the debate. M&F working paper nr. 2002-02, Free University of Brussels, December 2002, to be published in De Economist, vol. 152, No. 1.

Vulkan, N. (2003). The economics of e-commerce: a strategic guide to understanding and designing the online marketplace. Princeton, NJ: Princeton University Press.

Wales, E. (2003). E-commerce counts cost of online card fraud. Computer Fraud & Security, 2003, 1, 9-11.

Wayner, P. (1997). Digital cash: commerce on the Net, (2nd ed.) London: AP Professional.

Werbach, K. (2000). Syndication: the emerging model for business in the internet era. Harvard Business Review, May-June 2000, 85-93.

Samenvatting

(Summary in Dutch)

Door de snelle ontwikkelingen op het gebied van elektronische commercie op het Internet ontstaat de behoefte aan elektronische betalingssystemen die deze on-line commercie ondersteunen. Dergelijke elektronische betalingssystemen vormen een integraal onderdeel van de elektronische commercie en zijn een van de meest kritieke aspecten van een e-commerce omgeving.

Het blijft voor ontwikkelaars van nieuwe Internetgebaseerde betalingssystemen een open uitdaging om te voldoen aan de verwachtingen, eisen, voorkeuren en behoeften van de gebruikers met betrekking tot het ontwerp en gebruik van deze systemen. Als hieraan niet wordt voldaan zal dit resulteren in een lage bruikbaarheid, onveiligheid en inefficiëntie van de betalingssystemen en uiteindelijk in de weigering van klanten om deze systemen te gebruiken. Het ontwerpen van elektronische betalingssystemen vanuit het perspectief van de gebruiker is van levensbelang voor de ontwikkeling en het gebruik van systemen die geaccepteerd worden door de gebruikers.

Dit proefschrift beschrijft onderzoek dat verricht is met als doel te bepalen hoe elektronische betalingssystemen ontworpen kunnen worden vanuit het perspectief van de gebruiker en welke gevalideerde ontwerpkennis overgedragen kan worden aan ontwerpers van dergelijke systemen waardoor eindgebruikers de nieuwe betalingssystemen willen gebruiken in een e-commerce omgeving voor betalingen en hun persoonlijke financiën.

Dit onderzoek bekijkt elektronische betalingssystemen vanuit het perspectief van de gebruiker en betrekt daarbij onder andere menselijke factoren zoals bruikbaarheid, privacy, veiligheid en vertrouwen. Verschillende onderdelen van het multidisciplinaire vakgebied Mens-Computer Interactie worden gebruikt om de juiste invalshoek op de onderzoeksdoelen te bepalen en om de complexe problemen die hiermee samenhangen te adresseren.

Dit onderzoek omvat een combinatie van verschillende onderzoeks- en ontwerpactiviteiten: een literatuurstudie, een gebruikersonderzoek, kwalitatief onderzoek en experimenteel onderzoek. Toepassing van deze onderzoeks- en ontwerpactiviteiten heeft ertoe bijgedragen dat grondige kennis is opgebouwd met betrekking tot de gebruikerservaring van elektronische betalingssystemen. Bovendien heeft het suggesties opgeleverd voor het ontwerp en herontwerp van elektronische betalingssystemen, waarmee acceptatie door de eindgebruikers kan worden gewaarborgd. Om het ontwerp van elektronische betalingssystemen te ondersteunen is een verzameling van ontwerpaanbevelingen van elektronische betalingssystemen ontwikkeld.

Om de validiteit van deze ontwerpaanbevelingen te garanderen is experimenteel onderzoek gedaan naar de toepassing ervan op een bestaand systeem van de Postbank (Nederland). Dit onderzoek droeg bij aan de substantiëring van de validiteit van een subset van deze ontwerpaanbevelingen en genereerde gevalideerde ontwerpkennis die voorheen niet voorhanden was. De belangrijkste bijdragen van dit onderzoek is, aan de ene kant, de nieuwe kennis van het ontwerp voor gebruikersacceptatie van elektronische betalingssystemen vanuit het perspectief van de gebruiker, en aan de andere kant, de ontwerpaanbevelingen met de wetenschappelijke evidentie voor hun validiteit.

Curriculum Vitae

Dennis Abrazhevich

1974, August 17	Born in Kerch, Crimea.
1991 — 1996	Belarusian State University of Informatics and Radioelectronics, Minsk, Belarus, *MSc in Computer Science and Engineering*.
1999 — 2004	Eindhoven University of Technology, the Netherlands *PhD in Human Computer Interaction*.

Website:	www.epayresearch.com
Contact:	dennis@epayresearch.com