Electronic Payment Systems: Issues of User Acceptance

Dennis ABRAZHEVICH
SamenwerkingsOrgaan Brabantse Universiteiten (SOBU),
Technical University of Eindhoven (TUE), PO Box 513, 5600 MB, Eindhoven, Netherlands
Phone +31 40 247 52 46, Fax +31 40 243 19 30, Email: D.Abrazhevich @ tue.nl

Abstract. Electronic commerce and electronic business greatly need new payment systems that will support their further development. This paper discusses issues of user acceptance of electronic payment systems by mass customers and presents results of a user survey on conventional and ele ctronic payment systems that was conducted with the purpose to discover user attitudes towards their chara cteristic properties. The paper presents issues of users acceptance and guiding principles on design of electronic pay- ment systems with high level of user acceptance, which can be a key point in under- standing directions for further development of electronic payment sys tems.

Introduction

Electronic payment systems are an essential part of electronic commerce and electronic business and are greatly important for their further development. However, traditional ways of paying for goods and services do not work properly over the Internet. Existing payment systems for the offline world, such as credit cards, are widely accepted as a means of pay- ment on the Internet, however users don't see in them enough of reliability, trust, security, etc [5]. The existing payment systems are also far from ideal for merchants, because of the high transaction costs, fraudulent activity and the multiple parties involved in payment processing. These problems result in reluctant participation of users in e-commerce activi- ties, and this situation, in its turn, affects merchants who are losing potential customers. New payment systems, specially crafted for the Internet also could not avoid the same and different problems. This leads to reluctant use of the electronic payment systems, i.e. results in low *user acceptance* of newly introduced payment systems by mass customers. The need for new well-performing and user-friendly payment systems is clearly evident. These sys- tems should meet needs of users and merchants, and demonstrate a potential for acceptance on mass market.

To highlight the factors that influence user acceptance in payment systems we conducted a survey with users of payment systems. In this survey conventional (cash, credit cards) and electronic payment systems (debit and smart cards and credit cards on the Internet were addressed.

2. Background

The problems of electronic payment systems that we are facing at the present moment can be described as a failure to address user requirements and needs in the design and deploy- ment of the systems. It can be suggested that in the design of electronic payment systems not only technological but also user-related factors should be taken into account. Even if there are good technical solutions, but they are not accepted by end users or vendors, the whole system would fail. The existing works that discuss the requirements for electronic payment systems don't provide rationalization for selection of the chosen requirements. This omission can be misleading for designers and backers of electronic payment systems. There is a definite need for user feedback on these issues.

It is hereby suggested that it is important to know what characteristics of payment sys- tems have most direct influence on user acceptance. It is interesting to find out what charac- teristics are critical for success and what can be disregarded, if necessary. Thus a survey has been conducted with an aim to asses user attitudes concerning a range of characteristics of payment systems. The investigated characteristics that are cited in the literature [4], [2] are: anonymity (protecting or concealing customers' identity), applicability (ability to pay with a payment system at multiple and diverse points of sale), authorization type (ability to per- form offline or online payments), convertibility (ability to convert money to and from a system to another system), ease of use (usability), efficiency (ability of payment system to service small and micro payments), interoperability (support of open standards and proto- cols), reliability, scalability (ability to accept new users without performance degradation), security, traceability (ability to trace sources of money, income or physical presence), trust. Several characteristics of payment systems (e.g. authorization type, interoperability, scal- ability) were not included in the questionnaire, because of their specific, mainly technical, nature. These characteristics may also be important for user acceptance, but they are mainly transparent to users, as they do not affect directly the interaction during the payment activity. Further research will shed more light on these issues.

Key Elements of the Payment System

Payment systems are central to the efficient operation of the economy since they determine SCHWERPUNKTTHEMA Seite 30 TA-Datenbank-Nachrichten, Nr. 2, 7. Jg., Juni 1998 how quickly and how securely a seller of goods and services will receive payment. The associated transaction costs will play a key role in which payment system is selected from the range of alternatives on offer. There are two basic types of exchange mechanism. Payments can be made in cash (i.e. notes and/or coin) or they can involve the transfer of funds held with a bank. A third possibility also applies (but is not taken into account here), namely barter, where only goods are exchanged without any financial payment. Non cash payments require three separate elements. The buyer must have an agreed means of *payment authorisation* and instructing its bank to effect a transfer of funds. The seller's bank and the buyer's bank need an agreed

method of exchanging payment instructions. This is referred to as *payment clearing*. Finally the buyer's bank and the seller's bank must have an authorised method of *payment settlement*. Payment settlement can be done in a number of ways. It can involve adjusting accounts which the two banks have with each other, or it can be achieved through accounts each bank holds with a third-party, often a Central Bank. It is important to distinguish between these three key elements when considering electronic payments using the Internet. Payment authorization and payment clearing essentially involve exchanging messages. The Internet is ideally suited to perform this role, providing there can be sufficient security safeguards incorporated.

However, payment settlement is a separate process which must be linked to existing payment mechanisms and which will have much broader implications for financial stability and wider monetary policy. A payment system can only function successfully when it operates within a secure legal environment. It can only function properly if there are clearly defined rights and obligations governing the actions of the various parties which are involved. A buyer giving payment authorisation details must be secure in the knowledge that this information will not be misused, that it will be acted upon promptly and that there will be adequate compensation if operational mistakes are made. Similarly, a seller has to be secure that there will be sufficient penalties attached to any fraudulent issuance of payment authorisation (e.g. writing a cheque which will not be accepted by the buyer's bank). Ideally, a seller prefers to be protected against the risk that goods or services released to the buyer will not ultimately be paid for. This is why credit cards offer a very effective payment mechanism for Internet commerce. The structure of a particular legal system and the broader system of governance of which it forms a part, will have important implications for how a payment system will operate on a day to day basis. A payment system that has a strong statutory basis will depend on rules and regulations previously defined in detail having the force of national law. The Central Bank will often have the power to change or amend regulations with full statutory backing. Such a system is likely to offer the necessary transparency in its normal operation but may encounter problems of definition and liability when there are unforeseen problems or if new developments take place. Alternatively, the legal framework can be contractually based. Instead of depending on statute, the rules and regulations governing the operation of the payment system is based on a series of contracts. These may be explicit and in written form, or the contracts may be implicit, based on legal precedent. In the UK, the legal framework for payment systems is principally contract based although in key areas, legal statutes have been enacted. As new methods of electronic payment using the Internet are developed, the legal framework needs to be amended and adapted to fit the new

circumstances. Both a statute based or contract based legal framework have certain advantages and disadvantages in this respect. A contract based systems can be more adaptable in its detailed application. However, a statute based system will be more effective at introducing step changes in the payment system, for example when introducing the new Euro currency. In each of the major developed economies there is a need to settle very large payment amounts resulting from financial transactions. All of the major industrial countries have developed separate, same-day electronic payment systems for handling these large payments. They consist principally of foreign exchange transactions, debt service on large loans (i.e. payments of principal and interest) and the sale and purchase of bonds or company shares. The SCHWERPUNKTTHEMA TA-Datenbank-Nachrichten , Nr. 2, 7. Jg., Juni 1998 Seite 31 need to make the corresponding payments results in a diametrically opposed relationship between payment volume and the number of payments . Electronic same day payments will typically account for over 90 % of payment monetary value but will represent only a small fraction of the total payment transactions carried out on any particular day. This is particularly true for the UK where the payment system has to accommodate the large value payments generated by financial institutions operating in the City of London, arguably the largest and most important international financial centre in the world.[1]

Hiding the Identity and Blind Signatures

The first anonymous electronic cash scheme was based on the following principles, which also play a role in the concrete scheme we present later on.

3.2.1 Commitment-Based Identity Hiding A first very simple (but very ine_cient) example of how to hide the user identity in the coin is to use an unconditionally hiding commitment scheme, with commitment function com, which takes as input a string of the same length as a user identity and some random input. Then the user should created the coin as a set of k pairs of commitments

$c = ((c_{01} ; c_{11}); (c_{02} ; c_{12}); :::; (c_{0\,k}; c_{1\,k}))$

where $(c_{02} ; c_{12}) = (com(x_{0i} ; r_i); com(x_{1i} ; s_i))$ and x_{0i} ; x_{1i} are chosen at random, subject to $U = x_{0i}$ _ x_{1i} . Of course a dishonest user may not do this correctly, but it is then the role of the withdrawal protocol to ensure that the user does not get the banks signature on something invalid. The validation key simply consists of all the random strings r_i; s_i that are needed to open the commitments. This coin reveals nothing about U,by the hiding property of commitments.

Now, in the payment phase, the Shop sends the string $e = e_1; :::; e_k$, and the user

must now for each i open $c_{e_i i}$. The deposit key consists of the $x_{e_i i}$'s and r_i's or s_i' revealed. Note that if the same coin is spent twice, and the string e_0 is sent the second time, except with negligible probability there will be an i for which $e_i \neq e_{0\,i}$, and this means by the binding property of commitments that the two deposit keys contain $x_{0i}; x_{1i}$
and so we we can end u easily.
We will not use this principle later, as it is ineficient, but included it to demonstrate how an identity can be hidden in a way to reveal it only after double-spending.

Blind Signature Schemes

A blind signature scheme is one in which the receiver gets a signature on a message of his choice while the signer remains ignorant about what he is signing. A bit more precisely, the receiver has the message m as private input. Then there is interaction between signer and receiver, as a result of which the receiver gets a signature _ on m as private output. The signer has no information on m, _, in the sense that from his point of view, all pairs $m_0; \__0$ where $\__0$ is a valid signature, are equally likely.
Exploiting the multiplicative properties of the basic RSA signature scheme, it can be turned into a blind signature scheme as follows.
Let n; e be the signer's public RSA-key, and d his secret key.
_ The receiver has message m 2 ZZ_n. He selects a blinding factor r 2 ZZ_n at random, and computes $R \quad m \_ r^e \bmod n$;
and send R to the signer.
_ The signer computes
$S \quad R^d \bmod n$;
and returns S to the receiver.
_ The receiver finally computes
$\_ \quad S \_ r^{-1} \bmod n$:
Note that _ is indeed a valid signature, since
$\_^e \_ S^e \_ r^{-e} \_ R \_ r^{-e} \_ m \bmod n$:
This blind signature together with the identity hiding technique discussed above are by themselves are not sufficient for an e-cash scheme, one obvious problem is that if we simply make a withdrawal protocol by having the bank blindly sign a coin of the form we sketched above, the bank cannot be sure that it is signing a coin of the correct form, and we cannot be sure that double spenders can be traced.
In principle the user could prove using general zero-knowledge techniques that he executed the protocol correctly. This would solve the problem, but would be very ineficient.

References

[1] Chaum, D. (1992) Achieving electronic privacy *Scientific American,* August, vol. 267, no.2, pp. 96-101.
[2] Lynch, DC and Lundquist, L. (1996) *Digital money : The new era of Internet commerce* . Chichester: Wiley. p.165
[3] Medvinsky, G. and Neuman, BC (1993) Netcash: A Design for Practical Electronic Currency on the Internet. *In Proceedings of first ACM Conference on Computer and Communication security,* pp.102-196.
[4] Medvinsky, G. and Neuman, BC (1995) Requirements for Network Payment: The NetCheque ™ Perspective, *In Proceedings of the IEEE CompCon'95*, San Francisco.
[5] Wayner, P. (1997) *Digital cash: Commerce on the net* 2nd ed. London: AP Professional.