



Global Business Dialogue on Electronic Commerce

Consumer Confidence Internet Payments Sub Group Recommendations

October 29, 2002

Leading Co-Chair (Europe/Africa)	<i>Dr. Klaus Mangold</i> CEO DaimlerChrysler Services AG & Member of the Board, DaimlerChrysler AG
Leading Co-Chair (Americas)	<i>Carleton S. Fiorina</i> Chairman & CEO Hewlett-Packard
Leading Co-Chair (Asia/Oceania)	<i>Akinobu Kanasugi</i> Executive Vice President & Member of the Board NEC Corporation

1. INTRODUCTION

Electronic, as well as mobile business to consumer (B2C) commerce, requires the availability of adequate payment systems. Hence, there is a strong need for e/m-payment systems.

Many existing payment systems cannot be used in the e/m-commerce environment, either because they are paper based (cash, check) or usually require a hand-written signature on some receipt (credit card payment). Some classical systems, most prominently credit cards, can be used for e/m-commerce if the merchant does not insist on a hand-written signature. However, this increases the fraud risk, causing potential loss for the merchant and inconvenience for the consumer (in case of dispute).

In recent years, many new payment systems have been invented that have been specially designed for e/m-commerce. However, none of these systems achieved a critical mass of users – merchants as well as customers – subscribed. Some of these systems have already ceased service since they were not able to create sufficient revenues. Electronic substitutes for cash (like digicash) are prominent examples. In addition, there are legal requirements and different banking systems that make cross border

payments more complicated (and expensive) than domestic ones. As a consequence, payment systems are still a bottleneck for e/m-commerce.

Following the Tokyo conference, the GBDe has continued its research on Internet payments in order to identify, in more detail, the barriers to Internet payment systems and to explore possible solutions. Chapter 2 summarizes the results of this research. Chapter 3 contains some observations on the current situation and identifies the major problems. Finally, Chapter 4 draws some preliminary recommendations, based on this year's research results.

The GBDe will continue this work next year before producing final recommendations to business, consumers and governments. In this way it will be possible to evaluate more profoundly all relevant aspects of Internet payments including new e-payment systems and changes in technology, which may enhance some of the known systems.

2. STATUS QUO IN INTERNET PAYMENTS

The GBDe's own research produced the following findings:

2.1 Types of Internet Payment Systems

Currently, most Internet payment systems are either based on credit cards or on direct debiting (which requires the existence of a bank account). In general, systems based on credit cards have higher transaction costs than those based on direct debit. However, systems that rely on direct debit cannot be used cross border. Many new Internet payment systems make use of mobile devices such as mobile phones. Some of them use the billing engine of a telephone company for their purposes, others make use of the mobile phone for authentication purposes only.

There are only very few pre-paid systems that require neither a bank account nor a credit card, but they have not yet managed to get a significant share of the market.

In addition to a credit card, bank account or mobile device, some systems need the installation of software, new hardware (mostly smart card readers) or an offline initiation process that can be compared to opening a regular bank account. It can be seen that some form of enrollment is frequently necessary, sometimes online (spontaneous first use possible). In many cases, however, a formal registration process is required (precludes spontaneous first use). Some Internet payment systems require special hardware tokens, which may be smart cards and card readers, or have other special prerequisites, like paper TAN lists, special SIM cards, or an email address.

2.2 Liability and fraud protection

Due to the variety of systems and different legislation in different regions of the world, it is not possible to make a general statement on liability. In most Internet payment systems, the customer's risk is limited to a fixed amount for card losses like in real world applications. Whether the merchant or the payment service provider is liable for losses is up to the contract between them. In general, one can state that Internet payment service providers are willing to take over these losses if they obtain a compensation in terms of higher transaction fees and if the merchant takes certain security measures.

In order to provide protection against fraud, almost all Internet payment systems use cryptographic measures like SSL (secure socket layer) for end-to-end-encryption. Several payment providers are using customer authentication in general and consumer identification and authorization via a mobile phone number and a PIN. In addition, some providers take specific fraud protection measures like consumer scoring, credit card authorization, threshold supervision, or punishment after the fact, i.e. removing of

offending parties from the Internet payment system.

2.3 Internationality

Since only credit card payments can be processed efficiently from anywhere in the world, the only Internet payment systems that work fully internationally are credit card payments. All other systems are still limited to one or two countries in which the services can be accessed.

2.4 Challenges

The insufficient number of customers using a particular payment system is still the major problem. Payment service providers state that this might be a lack of consumer trust, consumers' habits changing too slowly, and the lack of critical mass of users (customers and merchants) that is necessary to make the system attractive. As a consequence, payment service providers fear not getting a sufficient return on investment.

Furthermore, the lack of appropriate standards is another reason that hampers the success of Internet payment systems. The absence of open and global standards and of interoperability between Internet payment systems and with legacy systems as well as the lack of suitable standardized consumer equipment and infrastructures is seen as detrimental to the development of successful Internet payment systems.

Security in general is a field for concern to many payment providers – in particular insufficient facilities for reliable and cost-effective authentication of users.

Last but not least, inhomogeneous international trading rules and lack of interoperable central bank systems are still barriers to the evolution of Internet payment systems.

3. GENERAL OBSERVATIONS

3.1 The critical mass problem and its consequences

All payment systems face the problem of attracting a sufficient number of Internet merchants and customers. Clearly, the value of a payment system for a user increases dramatically with the number of merchants supporting it. Hence, a critical mass of participants is necessary. Subscription to a new payment system causes costs for the merchant (integration costs) as well as the customer (initiation effort). This hampers the start-up of any new payment system. If this critical mass cannot be obtained,

the costs for subscribing will exceed the benefit – no matter how innovative the system may be.

Over the last five years, many payment systems were developed that could not reach this critical mass, and therefore disappeared. Despite this consolidation, the e/m-payment market is still fragmented.

As a consequence, most consumers and merchants still prefer classical payment methods like credit card payment or invoicing. However, these systems were not designed for e/m-commerce. Invoicing causes a break of media (if not presented electronically via EBPP) and transfers the whole risk to the merchant. Credit card transactions are easily exposed to fraud since the payment is not authorized by a signature.

Although there seems to be a need for a payment infrastructure, the problem of critical mass has become a barrier to all e/m-payment solutions developed so far.

If there was an infrastructure that allowed authorization of electronic transactions like a PKI, then Internet payment systems could be built upon it. As long as each payment service provider has to create a new authentication infrastructure on his own, he will hardly achieve the necessary critical mass. Building such an infrastructure is a major challenge for the future of e-commerce and should be done in a joint effort with public authorities rather than by single payment providers.

Furthermore, global interoperability is an important issue to overcome the problem of critical mass. The GBDe advocates the development of international Internet payment systems to support world-wide and competitive global e-commerce. The GBDe encourages payment service providers to ensure interoperability between different systems by establishing global and open Internet payment system standards. The GBDe strongly recommends harmonized international trading rules, which are an essential prerequisite for global interoperability.

3.2 Special aspects of stationary Internet payments & mobile payments

3.2.1 Stationary Internet payments

In principle, PCs or other stationary end devices are very much qualified for any kind of online-transaction, in particular online-shopping, since they provide fast and cheap Internet access. However, the Internet protocol does not provide any

features that allow secure user authentication. This causes problems for all post-paid systems in which the customer authorizes a payment that is later debited to some (bank or credit card) account. If there was an infrastructure that allowed user identification and authorization of transactions, such as a global PKI (Public Key Infrastructure), then payment systems would be able to build their services upon it. If, however, each post-paid-payment-provider has to set up his/her own authentication infrastructure – satisfying all legal requirements – then the cost would be too high, and one would run into the critical mass problem discussed above.

So-called pre-paid systems in which the customer buys some cyber coins or transfers money to an (often anonymous) account prior to his visit at the online-shop, do not need an expensive authentication procedure. However, such systems can only be used if the customer has transferred a sufficient amount of money before the purchase. Experiences with such systems show that it is difficult to convince users to exchange money into some cyber units before they wish to purchase a good.

Legal requirements (mostly based on money laundering laws) sometimes prevent instantaneous usage of Internet payment systems – simply because a paper-based user authentication is required. Such requirements easily become a barrier to the usage of such systems. Therefore, at least for micropayments and macropayments not exceeding some amount, the initiation process must be carried out in a way to ensure that spontaneous usage of the system is not prevented.

3.2.2 Mobile payments

Mobile payments (payments for goods or services that occur from a mobile device) include the purchase of not only content over the mobile network, but also the purchasing of goods and services from a third party merchant. These payment systems can be used for both face to face and remote payments, as well as for micro and standard payments. The high market penetration rates for mobile phone usage and the introduction of 3G networks and applications could make m-payments a standard feature in the near future.

A major difference between stationary and mobile Internet usage lies in the fact that the user of a mobile device has a business

relationship with his/her mobile network provider that can be used for identification. Furthermore, each mobile network provider has a billing engine that could be used – in particular for micropayments, where the credit risk is limited.

3.3 Public key infrastructures and general remarks on fraud

Like all other payment systems, e/m-payment systems have to face the problem of fraud, i.e. the criminal use of the payment system. Electronic money (like cyber coins) has a security level comparable to normal cash. However, such electronic coins are very rarely used. Payment systems like credit card payment or direct debit, in which the amount is charged to a (bank) account, have to ensure that the transaction is correctly authorized and that non-repudiation is guaranteed. Otherwise, a fraudulent customer could pretend to be someone else (e.g. stolen credit card number) or claim that he never authorized the payment. On the other hand, if the integrity of the payment information is not ensured, a fraudulent merchant could charge more than was actually agreed.

Although the problem of fraud comes along with any payment system, the problem is even more discussed in the e-commerce environment. The reason is that today most online purchases are still settled using a classical payment system like credit cards or direct debit. Fraudulent users can exploit the fact that the usual authentication process (via a hand-written signature) cannot be realized.

In case of micropayments, pre-paid systems reduce the risk of fraud since the money was transferred prior to the purchase. In particular, there is no risk for the merchant (as long as the cyber money itself cannot be copied). For the customer, the potential risk is limited to the deposit. Since cyber money (like cash in the real world) can be stolen, such systems do not solve the security problems for macro-payments.

Therefore, user authentication, data integrity, non-repudiation of a transaction and, last but not least, confidentiality of the data is essential for any kind of high-value electronic financial transactions. Only a public key infrastructure can solve this problem to complete satisfaction. The introduction of such an infrastructure that allows digital signatures would be the ultimate solution to this problem. Since setting up such an infrastructure comes along with high costs. Such a measure is most likely to be successful in a joint effort, e.g. the introduction of digital identity cards, issued either by government authorities or private

companies under the patronage of the local government that can be used to authenticate electronic transactions including payments. If each identity card was fitted with a chip that could process digital signatures, one would obviously solve the hen-and-egg problem of reaching a critical mass of users.

The GBDe is aware of the fact that, as a first step, domestic authentication infrastructures will be built up rather than one single global authentication system. However, the initiators of such projects should bear in mind that it should be possible to link these “islands” in a second step.

3.4 Micropayments

Micropayments (USD 5 or less) are often stated as a crucial success factor for the development of electronic commerce. Electronic content and services are often low priced. Furthermore, micropayments seem to be important for the first step in the evolution of the Internet into an e-commerce platform.

Most classical systems (invoicing, credit card) fail in processing very small payments because of the minimum transaction costs. In particular, when dealing with payments less than 1 USD, these minimum transaction costs can exceed the total amount of payment.

Therefore, most micropayment solutions either use an existing billing engine (telco) or aggregate the payments. However, these aggregators are either based on a pre-paid system (and require money transfer prior to the purchase) or on usual credit/debit-card systems, which can be adapted to micropayments using a mobile device.

In particular, when dealing with micropayments, the effort to prevent fraud as well as to comply with legal regulations in general should be adequate compared to the size of the typical payment. Therefore, micropayment systems should not be over-regulated to avoid that innovative and promising initiatives become impossible to implement.

3.5 Cross border payments

Due to different legal systems (including different central bank systems) cross border payments are still much more difficult to process than domestic ones. As a consequence, many e/m-payment systems work only in one country or in some region. Even if the system allows cross border payments, the additional effort causes costs, which limits its usage for micropayments.

In order to allow efficient cross border payments, administrative barriers must be lowered. In particular, countries should harmonize their legal systems and their payment formats (e.g. for direct debit) as well as guarantee interoperability in their central bank systems.

3.6 Conclusion

Although there is a clear need for a secure and efficient e/m-payment infrastructure, the investment only pays off if the system is used by a sufficiently large number of customers and merchants. Therefore, the critical mass problem has become the most important barrier for Internet payment systems to evolve.

In order to overcome this stalemate, a joint effort seems to be most promising. Partnerships among private companies of different sectors as well as public-private-partnerships can be such initiatives. If, in addition, a payment system can be built upon an existing infrastructure – which might be a classical payment system, a mobile network, or a PKI that comes along with an ID-card – then this will be an important advantage.

RECOMMENDATIONS

Based on the current trends and general observations, the GBDe survey led to the following preliminary recommendations in order to stimulate the development of Internet payments and to overcome the problems identified.

The recommendations address the private sector as well as governments. They should be looked at as a further development of the GBDe Tokyo Recommendations on Internet payments (September 2001) and will be tested and elaborated further during the year to come.

- 1) The lack of critical mass is one of the main barriers for the development of Internet payment systems. Therefore, Internet payment systems should be built on open standards and common and interoperable specifications.
- 2) In order to overcome the problem of critical mass, governments should proactively assist in the development of infrastructures like PKI on which Internet payment systems can be built. Public authorities should stimulate joint projects with the private sector in order to create such an infrastructure. In particular, initiatives for the introduction of digital identity cards, issued either by government authorities or private companies under the patronage of the

Government, that can be used to authenticate electronic transactions including Internet payments would be most useful.

- 3) For the adoption of an Internet payment system it is essential that the initiation process is simple and effective. Therefore, governments should develop an appropriate (international) legal framework that allows online registration to Internet payment systems.
- 4) The establishment of partnerships like those between the financial and telecommunications sectors in the development of mobile Internet payment systems are most welcome. Such collaboration allows each player to focus on its core competencies and to increase efficiency to the benefit of all, customers, merchants and payment service providers.
- 5) The level of regulation should be kept proportionate to the importance of the payments and to real life needs, i.e., light and simple micropayment systems, so that innovative and promising initiatives are not prevented from being developed. For macropayments, the best protection against fraud is not detailed and demanding regulation but an infrastructure that guarantees authentication and non-repudiation of the payment.
- 6) Together with the payment industry, governments should work on harmonization of payment formats (e.g. for direct debits) and promote that payment providers as well as central-banks guarantee interoperability in their systems."