

Prepaid-Payment-Solutions for Micropayments from a Technical Point of View

M. Lenord¹ and T. Nisbach²

¹Department of Computer Science, Gerhard-Mercator-Universität-Duisburg, 47048 Duisburg, Germany
E-mail: mti@lenord.net

²ALLCASH GmbH, Eurotec-Ring 10, 47445 Moers, Germany
E-mail: nisbach@allcash.de

Abstract

This document describes aspects of the processing of micropayments. The customer payment procedure is considered with regard to the charge-back problem. Further on a concept is presented which provides an easy implementation for the merchant and a simple but secure access for the customer. The function of a micropayment proxy server and the transaction sequence of the entire payment procedure are explained.

1 INTRODUCTION

During the last years the internet has transformed from an information platform into a marketplace for virtual and real goods. This includes offers of hard- and software, access to sophisticated databases, complex services etc. The opportunity for online-payment-processing has become more and more crucial. Many payment-systems have been created in the commercial and scientific area but yet no standard has emerged. Dr. Beck¹ from the department of communication sociology and psychology estimates that the current stage of development of the internet can be compared to the level of development of the radio in the year 1928. Higher stages can be reached by implementing new payment procedures. "If it were possible to directly account tiniest information bits this would change the medium significantly."

The technical and cryptographic means to realize internet-payment are available. The tough implementation has to do with psychology, standardization and convenience. Especially the payment of small amounts of money (micropayments) is solved in theory and is commercially realized but still failed because of insufficient consumer and merchant acceptance.

This paper describes a method of resolution which has been developed in the scientific area at the University of Duisburg² and has been implemented in a commercial application.

First a short introduction of micropayments is given. Main commercial requirements and technical problems are pointed out. Chapter two describes solutions for the problem of charge backs and a simple implementation concept for online-shops. The communication sequence and security issues are also considered.

¹ <http://www.heise.de/newsticker/data/jk-30.12.00-000/>

² <http://www.mti.uni-duisburg.de/>

2 MICROPAYMENTS

2.1 Principles

The main difference between macro- and micropayments is that for the payment of small amounts of money it is not acceptable to pay the usual transaction fee. If you want to pay 10 cents it makes no sense to use a credit- or debitcard because the costs for the payment process will be higher than the value of the goods. Likewise no merchant will send an invoice for this amount. The principle of micropayments therefore is to accumulate small amounts of money until the sum is worth to be transferred to the bank. This is shown in figure 1.

1. The customer orders a dedicated amount of money from a payment-provider. The sum is entered on the credit side of a so called shadow account.
2. The customer then spends this money in little bits for the virtual goods in the internet. The transactions are registered on the shadow account. No real bank-transfer is initiated at this point of time. No costs occur for this transaction.
3. After the shops have accumulated a profitable amount of money, they initiate the transfer of this sum.
4. The payment-provider requests the bank to transfer the money to the real account of the merchant.

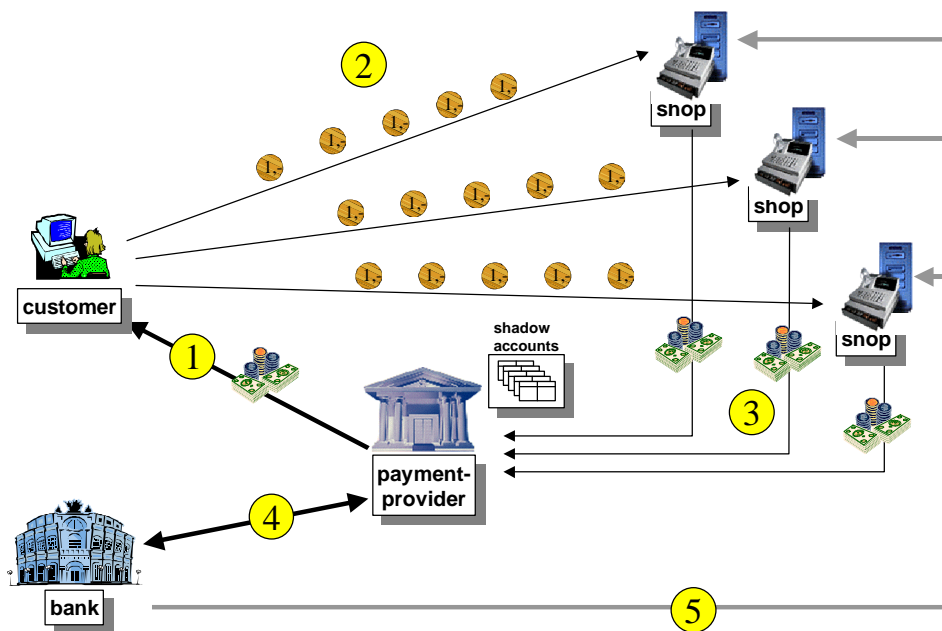


figure 1: principles of micropayments

Many solutions have been invented to realize this mechanism. Examples are PayWord, MicroMint by Rivest and Shamir [RS96], Transactions Using Bets by Wheeler [Whe96], NetCash and NetCheque by Medvinsky and Neuman [MN93],[MN95], CyberCoin by CyberCash Inc. [Cyb99], No3rd by the DFN [DFN99], Millicent by Digital Inc. [Dig95], eCash by David Chaum [DS82], MiniPay by IBM [HY97], Jalda by Ericsson and EHPT [Jal00] or click and buy by Firstgate [FG00].

2.2 The customer payment procedure

The weak point of the payment-procedure is the customer request for a dedicated amount of money (no 1 in figure 1). In the micropayment business typically intangibles are delivered. Therefore the merchant needs a payment guarantee. It is not possible to return the goods or recollect the small amounts of money which have been spread all over the internet. In the following a short evaluation of possible payment procedures with respect to this point are given.

?? Payment on account

The customer orders the dedication amount of money and pays for it upon receipt of an invoice. This method requires a trusted relationship between customer and merchant because of the missing payment guarantee. This is not acceptable for micropayments because customers want to act spontaneously and anonymously in the internet without passing an extensive registration process.

?? Credit cards

The payment procedure can be performed by the transmission of the credit card information. Since there is no established possibility to authenticate the customer the problem of charge-backs has increased in the online-world.

Standards like SET (Secure Electronic Transaction) are offering a solution by certifying the cardholder. But the distribution and administration of the certificates lead to inconvenience for the customer, who will not voluntarily agree to use this method.

?? Debit payment

While the customer settles his account with credit cards at the end of the month, with debit payment an immediate direct debiting is performed. In Europe debit cards are very common. In Germany approx. 90% of the adult citizens possess a debit card e.g. the EC-card. In the real world the customer is authorized by typing in his personal identification number (PIN). Since there is no such possibility in the internet the customer can call back the money.

?? Prepaid-cards

Since the debut of mobile phone cards prepaid-cards have become an inherent part of the assortment of cards in a purse. The customer pays a certain amount of money in advance and can spend it on various occasions. In contrast to debit- and credit-payment no fees have to be paid for the transaction. This makes prepaid-methods predestinated for the payment of small amounts of money. Prepaid mobile phones for example have become more popular than mobiles under contract.

Since prepaid-cards have no possibility for charge-backs they also meet the requirements of the merchants. Once a transaction has been finished they can rely on receiving the money.

2.3 Simple application for online shops

Another problem of current implementations for micropayments is the complexity. Many small online-shops are emerging at the market. They are looking out for low-budget solutions and don't want to pass a complex implementation process. They need a "plug and play" solution which requires no know-how of experts. The proxy-technology can meet best those requirements. A special micropayment-proxy which is operated by a payment provider forwards the online information to the customer and is responsible for the authorization, the accounting and the provision of payment information for the customer. This is performed in five steps (figure 2):

1. First the customer unlocks a dedicated amount of money at the payment provider. He types in his prepaid-card-number and determines the amount of money he wants to spend. This information is delivered to the proxy by a ticket that is stored in a local database.
2. The request of the customer is forwarded to the shop's web-server.
3. The web-server processes the request and returns either a static document or a dynamically created information from the database.
4. The proxy now checks whether this information is liable for costs. This is done by simple rules which are entered into a table of the database. If the customer has to pay for the content his authorization (ticket) is checked. The amount of money is decreased and the account information is automatically displayed in the browser-window.
5. The clearing process is invoked when the customer closes the browser-window or hits the exit button. The sum of the money which has been spent for the intangibles is transmitted to the payment provider and disposed on the customer's prepaid-card account.

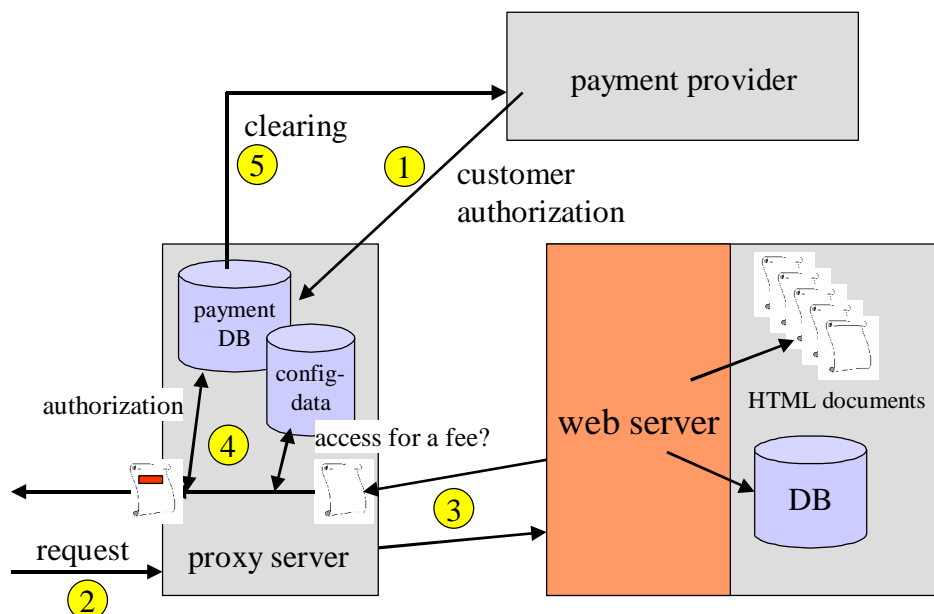


figure 2: proxy-server of micropayments

2.4 The communication sequence

The communication sequence of the total payment procedure is shown in figure 3. The session starts when the customer requests a content which is liable for costs. The shop-proxy checks whether a valid ticket has been delivered and sends back a web-page which provides information about the payment provider who is in charge of the ticket certification. The customer can be directed to the payment provider by mouse click and receives a form to fill in his prepaid-card-number and the amount of money which he wants to reserve for the shop. This number is checked in the third step. If the corresponding shadow account covers the dedicated amount the reservation is performed. The payment provider certifies a ticket and sends it to the browser. The customer is automatically redirected to the charged content. The shop-proxy validates the ticket and forwards the request to the web-server of the shop. If the response is valid the reserved amount of money is decreased and the content is forwarded to the customer. This procedure can be repeated until the money is eaten up or the customer terminates the session by closing the browser or clicking on the close button. In this case (6) the ticket is devaluated and the clearing process to the payment provider is started. The amount of money which has been used in the micropayment shop is disposed on the shadow account of the prepaid-card.

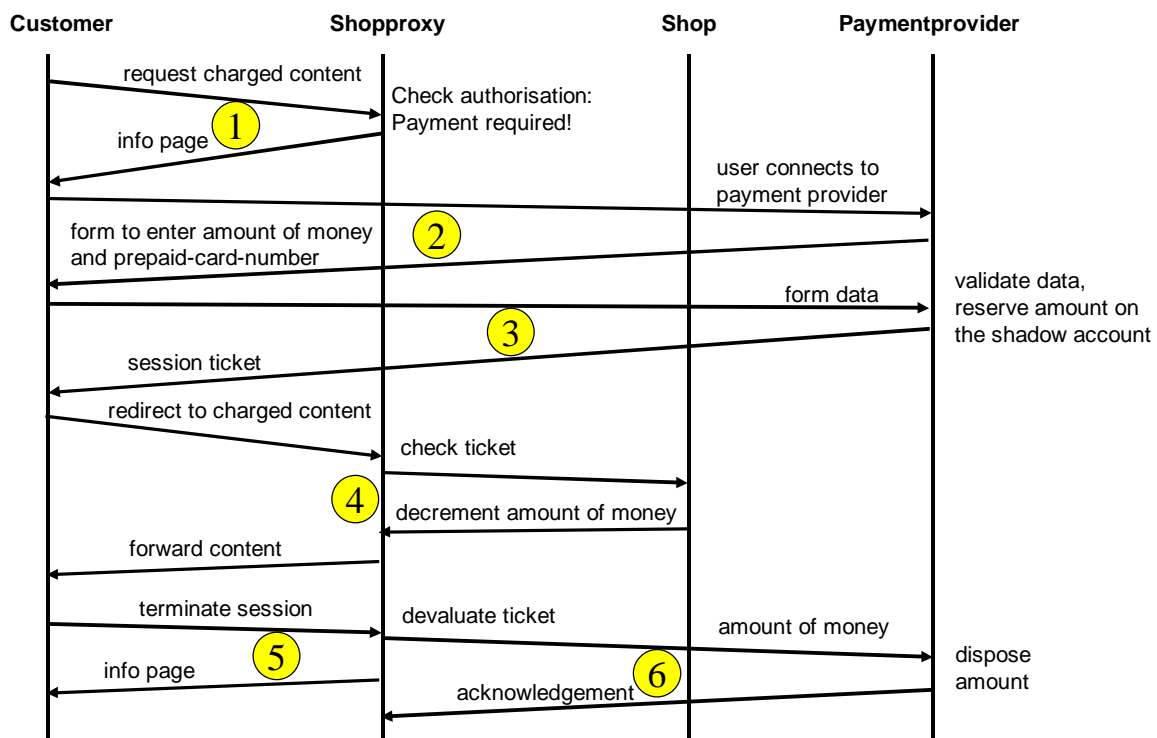


figure 3: communication sequence

2.5 Security

The most important question is how security is obtained. Of course the communication over the internet is encrypted by the secure socket layer (SSL). This guaranties the confidentiality of the data but provides no authentication of the customer. Therefore the core element of this micropayment system is a virtual ticket which has to resist against wiretapping, forgery and replay attacks. The ticket contains the following parameters:

- ?? The **amount** of money and the **currency** determine the value of the ticket.
- ?? The **session ID** is a number which gives the ticket an unique identifier.
- ?? The ticket is only valid for a dedicated micropayment shop which is identified by the **merchant ID**.
- ?? The ticket is valid for a time slot which is determined by the **date** and **time**. If a session is not terminated correctly the clearing process automatically is invoked when the end of this time slot has been reached.
- ?? The ticket can only be used from a browser which is non-ambiguously identified by a special **hash value**. This prevents replay attacks from other computers.
- ?? A **checksum** enables to detect formal errors of the parameters.

The ticket is encrypted with a symmetric algorithm. The private key is declared between the shop-proxy and the payment provider.

3 CONCLUSION

A prototype of this micropayment concept has been implemented by a payment provider³ who cooperates with a prepaid-card issuer. The next step is to obtain a validated and predictable implementation. An UML-model will be realized to detect security lacks or error handling problems and to generate the code frame for Java and C++. Finally the usability of UML for the concepts phase will be evaluated.

³ ALLCASH GmbH, Germany, <http://www.allcash.de/>

4 REFERENCES

- [Cyb99] *CyberCash* Homepage 1999 <http://www.cybercash.de>
- [DFN99] *No3rd* Homepage 1999: <http://www.itm.uni-sb.de/projects/zv/deutsch/>
- [Dig95] Steve Glassman, Mark Manasse, Martín Abadi, Paul Gauthier, Patrick Sobalvarro, *The Millicent Protocol for Inexpensive Electronic Commerce*, 1995
<http://www.research.digital.com/SRC/personal/steveg/millicent/millicent.html>
- [DS82] D. Chaum, Blind Signatures for Untraceable Payments, *Advances in Cryptology Proceedings of Crypto 82*, D. Chaum, R.L. Rivest, & A.T. Sherman (Eds.), Plenum, pp. 199-203.
- [FG00] *Firstgate* Homepage: <http://www.firstgate.de>
- [HY97] A. Herzberg, H. Yochai, *Mini-Pay: Charging per Click on the Web*, Tel Aviv 1997 <http://www.hrl.il.ibm.com/mpay/docs/papers/mpay-long.html>
- [Jal00] *Jalda* Homepage: <http://www.jalda.com/home/>
- [MN93] M. Medvinsky and C. B. Neuman, NetCash: A design for practical electronic currency on the Internet. In *Proceedings of 1st the ACM Conference on Computer and Communication Security*, November 1993
<ftp://prospero.isi.edu/pub/papers/security/netcash-cccs93.ps>
- [MN95] M. Medvinsky and C. B. Neuman, Requirements for Network Payment: The NetCheque Perspective, *Proceedings of IEEE COMPCON'95*. 1995
<ftp://prospero.isi.edu/pub/papers/security/netcheque-requirements-compcon95.ps>
- [RS96] R. Rivest, A. Shamir, PayWord and MicroMint: Two simple micropayment schemes, *MIT Laboratory for Computer Science 1996 CryptoBytes*, volume 2, number 1 (RSA Laboratories, Spring 1996), 7--11.
<http://theory.lcs.mit.edu/~rivest/RivestShamir-mpay.ps>
- [Whe96] D. Wheeler, *Transactions using Bets*, Computer Laboratory, University of Cambridge, England 1996
<ftp://ftp.cl.cam.ac.uk/users/djw3/tub.ps>