

Schmidt, Carsten; Müller, Rudolf

Working Paper

A framework for micropayment evaluation

SFB 373 Discussion Paper, No. 1998,66

Provided in Cooperation with:

Collaborative Research Center 373: Quantification and Simulation of Economic Processes,
Humboldt University Berlin

Suggested Citation: Schmidt, Carsten; Müller, Rudolf (1998) : A framework for micropayment evaluation, SFB 373 Discussion Paper, No. 1998,66, Humboldt University of Berlin, Interdisciplinary Research Project 373: Quantification and Simulation of Economic Processes, Berlin, <https://nbn-resolving.de/urn:nbn:de:kobv:11-10060082>

This Version is available at:

<https://hdl.handle.net/10419/61224>

Standard-Nutzungsbedingungen:

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

Terms of use:

Documents in EconStor may be saved and copied for your personal and scholarly purposes.

You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.

If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.

A Framework for Micropayment Evaluation *

Carsten Schmidt[†] Rudolf Müller[‡]

Abstract

Lacking payment systems become a bottleneck for the vision of the Information Economy. In many cases payments of fractions of a cent, so-called micropayments, are of particular interest. In this paper we propose a framework to evaluate payment systems. The framework consists of a well structured parameter vector of desired attributes. For the evaluation of attribute values we suggest to use VTS diagrams from object oriented analysis and design. The framework is applied to DigiCash, SET and First Virtual.

Keywords: micropayments, electronic commerce

*The financial support of the Deutsche Forschungsgemeinschaft (Sonderforschungsbereich 373) is gratefully acknowledged.

[†]Institut für Wirtschaftsinformatik, Humboldt-Universität zu Berlin, Spandauer Str. 1, 10178 Berlin, Germany, cschmidt@wiwi.hu-berlin.de

[‡]Institut für Wirtschaftsinformatik, Humboldt-Universität zu Berlin, Spandauer Str. 1, 10178 Berlin, Germany, rmueller@wiwi.hu-berlin.de

Contents

1	Introduction	3
2	Driving forces for electronic payment systems	3
3	Evaluation Scheme	5
3.1	Technological dimension	5
3.2	Economic dimension	6
3.3	Social dimension	7
3.4	Reduced evaluation scheme with dimensions	8
4	Vertical Time Sequence diagrams	9
4.1	Analysis of DigiCash	10
4.2	Analysis of SET	12
4.3	Analysis of First Virtual	15
5	Conclusions	17
6	References	17

1 Introduction

The Information Economy [Varian 1995a] and Electronic Commerce are widely discussed topics on the Internet. Many new services are envisioned, and many conventional services have now an on-line version. But most of the services will only be realized if providers can be compensated for their efforts. Access to material protected by copyright, however, and easy search of this material in remote information systems is technologically feasible. Lacking payment schemes thus become a bottleneck for the vision of the Information Economy.

Information goods on the Internet have the particular characteristic that the marginal costs are close to zero. This cost structure poses special problems for pricing. To cover the fix costs, pricing can be based on price discrimination or bundling [Varian 1995b]. But when fix costs are sunk, it may also be desirable for a provider to offer information goods at a low price but not for free. Therefore payments of fractions of a cent, so-called micropayments, are of particular interest. Clearly transaction-costs for micropayments have to be a fraction of a fraction of a cent.

Due to this demand we observe numerous proposals and implementations for electronic payment systems on the Internet, all of them are more or less suited for micropayments. The question arises, by what means could these systems be compared? We propose in this paper a framework to analyse and design electronic payment systems that is based on methods from object oriented analysis and design.

The paper is organized as follows. First we describe what seem to be the driving forces for the development of electronic payment systems. We then propose our framework to analyse and design electronic payment systems. It is based on structuring the space of requirements along an economic, technical and social dimension, and on *Vertical Time Sequence* (VTS) diagrams. Finally, we apply the VTS diagrams to describe existing payment systems and determine their location in the space of requirements.

2 Driving forces for electronic payment systems

An analysis of existing electronic payment methods on the Internet shows that each of them seems to be inspired by a major driving force. Interestingly, we do not identify low transaction-costs as one of these forces. We identify three major forces.

(1) *On-line usage of previously existing payment methods.* Examples are secure credit card presentation and third-party processing. In all cases the clearing of the payment is done via existing institutions. This has the striking advantage of the existence of a critical mass of consumers. As well, a simple, but not necessarily secure implementation could be individually done by each provider. The major focus for improvements is on security: confidential transport of credit card information and authentication of consumer and provider.

(2) *Usage of technology originally developed for other applications.* Here examples are NetCheque and NetCash relying on Kerberos. The Kerberos system was designed for resource management in distributed computing. Due to this original application they have an efficient implementation that scales very well. Reliable implementations are available right in the beginning. The focus is therefore not on technological improvements but is concentrated on embedding the system in existing clearing mechanisms.

(3) *Anonymity as a new challenge for cryptography.* An example is DigiCash. This system is motivated mostly by providing anonymity based on cryptography, in particular blind signatures. The result is a very complex system that has deficiencies in scaling and, possibly, performance. Its acceptance might be negatively influenced by lacking trust based on missing understanding of its security mechanisms.

The fact that payment systems evolved this way by driving forces makes it difficult to analyse and compare them. So MacKie-Mason and White [MacKie-Mason and White 1997] collected 30 attributes that describe payment systems and evaluated 9 systems along these characteristics. They proposed a decision support approach that could be used by a provider of information goods to select a payment method. The approach has several disadvantages. First, many points in the evaluation table are debatable since values are difficult to measure, second the table is very complex for practitioners, third the table does not explain *how* a payment system realizes the postulated values of measurement.

We propose a reduced set of criteria that is further grouped in three dimensions: technological, economic, and social. Orthogonally to this, we show how *Vertical Time Sequence* (VTS) diagrams from the field of object oriented analysis [see Rumbaugh et al. 1991] can assist in describing the implementations of electronic payment systems. The combination of both should give practitioners a framework to evaluate their target criteria.

According to the dependency on traditional financial instruments, we will divide electronic payment systems in digital token-based and credit card-based systems. Digital

token-based are electronic cash and electronic checks. Credit card based are secure credit card presentation and third-party processing. For a complete classification see Neuman and Medvinsky [Neuman and Medvinsky 1995] and Kalakota and Whinston [Kalakota and Whinston 1996].

3 Evaluation Scheme

More than 30 attributes have been proposed in the literature to describe electronic payment systems [Chaum 1985, Medvinsky and Neuman 1993, Neuman 1995, Neuman and Medvinsky 1995, XIWT 1995, Kalakota and Whinston 1996, MacKie-Mason and White 1997]. We use a subset of these and divide them into technological, economic and social requirements on micropayments. We will see that some are closely related attributes and can be summarized into one. The result is a reduced evaluation scheme for electronic payment systems. A caveat of this work is that we make no considerations of possible institutional and legal criteria.

3.1 Technological dimension

The critical technological properties of a micropayment mechanism are security, reliability, scalability, and latency.

Security: As a matter of course, micropayment needs to be secure. In particular, failures in security can be a setback for trust in new payment systems. Since payments are transported in a relatively open environment where modification can easily be made they will be the target of criminal attack [Neuman and Medvinsky 1995]. Recall the three major security problems on public networks: message confidentiality, message integrity, and sender authentication.

Reliability: Commerce will depend on the availability of the billing infrastructure. The infrastructure must be highly available and payments should be possible 24 hours a day. The system should not have a single point of failure.

Scalability: When electronic commerce on the Internet grows, demand on payment services will grow and can produce bottlenecks at centralized services. A scalable distributed design of payment services will be necessary.

Latency: Even during peak load times micropayments should be transmitted in a convenient time. Applications should be able to use the micropayment mechanism without noticeable performance loss. Sources of latency are Internet connections, Internet/banking-net connections, processing, and database access. We do not regard communication being a significant source of latency. This is related to messages being basically constant in size. They are negligible with the growing size of transmitted information goods. Bottlenecks are massive parallel access to currency-/banking servers and access to databases.

3.2 Economic dimension

Economic requirements have both a macroeconomic or monetary level and a microeconomic level. We decided to leave out the monetary questions, because these are mainly of relevance if an electronic payment system does not rely on traditional financial instruments. Desirable properties for a micropayment mechanism in an (micro-)economic dimension are: low transaction-costs, atomic exchange, and a large customer base.

Low transaction-costs: In a microeconomic context transaction-costs are the costs for the buyer/merchant to perform a financial transaction. These costs are mainly given by the price of the payment mechanism, because connection and bandwidth for the communication will have the incremental cost of zero, due to the negligible constant size of messages. The price of the payment mechanism depends on the cost properties of the electronic payment system, the market structure, and the pricing behavior of the payment-provider.

Because we cannot observe a market yet, we only investigate the possible cost properties of the electronic systems. There are fixed costs for developing software, setting up hardware, and connecting to the Internet. The processing of payments consumes computing resources and produces high traffic predominantly at centralized services of the payment system. Therefore to a certain degree marginal costs are related to the scalability of a payment system. Of relevance are as well costs to connect to the traditional banking-net. Here it is important whether a payment system requires a connection for every transaction or on a periodical basis. A credible payment system has to include abuse in prices. Payment systems having weaker security features face higher costs to fix security holes and reimburse customers.

We do not investigate whether there are differences in costs due to the production

of complementary products. For example, a bank introducing a payment system does this under different conditions than a software company. For both the new electronic payment systems can be analysed as an incremental product. Production of electronic payment systems can have higher product specific economies of scale in a multi-product production [for a definition see Baumol, Panzar, Willig 1982] than for single-product production. Therefore a complete analysis of the cost structure would have to consider economies of scope. This problem needs further research.

Atomic exchange: For a frictionless Information Economy instant clearing and settlement of electronic exchange of goods and payments is needed. Payments need to be complete. Incomplete payments will result in an inconsistent state and are not acceptable. A business transaction, involving exchange of goods *and* payment should be complete as well. Receiving goods without payment or committing payment without goods is not desirable.

Customer base: The usefulness of a micropayment mechanism to a buyer depends on the size of the participating merchants. To a merchant the usefulness of the payment system is a function of the number of participating customers and their utility. The utility of a customer will be zero without merchants participating in the payment system and grows with a rising number of merchants. So utility is strongly affected by positive externalities, which results in a start up problem. Below a certain number of subscribers to the payment system we face a market-disequilibrium. When a system is not growing above a critical mass of participants subscription will go back to zero in finite time [Rolfes 1974]. Positive network externalities of an electronic payment system with participants above the critical point will establish market entry barriers.

3.3 Social dimension

Society will have an influence on evolving electronic payments. The discussion about anonymity approaches for payment systems provides an example for this. Desirable properties of a micropayment mechanism for society could be anonymity and peer-to-peer payments.

Anonymity: Anonymity of electronic payments is a controversial topic. Perhaps a totally anonymous payment system is necessary for public acceptance, but most of the traditional financial payment systems are partly anonymous, for example credit cards and

	Requirements	DigiCash (electronic currency)	First Virtual (third-party processing)	SET (secure credit card transaction)
Microeconomic	Low transaction-costs	-	+	+
	Atomic exchange	-	-	-
	Customer base	-	-	o
Technological	Security	++	-	+
	Reliability	++	+	+
	Scalability	-	++	++
	Latency	+	-	-
Social	Peer-to-peer payments	yes	not implemented	no
	Grade of Anonymity	full	some	some

Table 1: Results according to the analysis in the next section.

checks. It may be advantageous to be able to trace your payments, for example business expenditures.

Peer-to-peer payments: A drawback of credit card mechanisms is that only approved sites, stores, restaurants, etc. can receive payments. It is not possible to borrow money from a friend. For the Information Economy it would be desirable to have a payment system where sending and receiving payments is possible for everybody.

3.4 Reduced evaluation scheme with dimensions

We extracted 10 criteria along which payment systems could be evaluated. We propose a qualitative evaluation by assigning the following values: “++” for best fulfillment of the requirement, “+” for good fulfillment of the requirement, “o” for undecided, “-” for bad fulfillment of the requirement, “--” for not meeting the requirement at all.

The following table gives the evaluation result for DigiCash, First Virtual, and SET. The evaluation criteria are discussed in more detail in chapter 4 using the VTS diagrams.

4 Vertical Time Sequence diagrams

Vertical Time Sequence diagrams are a graphical method from object oriented analysis and design to describe interaction between a set of objects in a system. The participating objects are displayed by vertical arrows representing the time scale. Communication between objects is displayed by horizontal arrows, which are labelled by the content of a message. Additionally the vertical object arrow may have descriptions of the action the object takes in response to a message from another object.

We use VTS diagrams to describe business transactions on the Internet. Transactions include the payment process and the transmission of the information good. The objects are the customers client software, the merchants server, and one or more payment system servers. Each horizontal arrow represents a complete session of Internet communication between a client and a server.

We proceed as follows. Starting point is a verbal description of the payment system using linguistic labels on the VTS diagram. These are used to analyse the social attributes of the payment system. The vertical arrows of the VTS diagram will help us to identify the grade of anonymity. We then get to the technical attributes using precise labels on the VTS diagram. We analyze weak points for the attributes security, reliability, and scalability. Internet-connection, processing times, connection to the banking-net, and database access will be considered to determine latency. Technical attributes are also relevant when we get to the economic evaluation. For example a system that does not scale well, gets a deduction in transaction-costs. When the provider of the payment system needs to perform a higher volume of transactions, a less scaleable system will face higher costs to upgrade capacities. For each attribute we concentrate our discussion on crucial regions in the VTS diagram. For other parts of the diagram the reader might convince himself that they are of minor relevance for the particular attribute.

This type of analysis is done for the following payment systems: DigiCash, SET, and First Virtual. The objects in the VTS diagram will be labeled A for the payer and B for the payee. We will use the following notation for cryptography: a public key encryption will denote as $E(\text{message}, k_B)$, where k_B represents the public key of B. A symmetric or secret key encryption has the form $E(\text{message}, s_{AB})$, where s_{AB} is the symmetric key between A and B. A digital signature of A is represented by a term $E(\text{message}, sk_A)$, where sk_A is the secret key of A. MD stands for message digest and D for decryption.

4.1 Analysis of DigiCash

DigiCash is an example for electronic currency. The goal is to provide anonymity to a payer, even when the digital token issuing bank and the payee will collude. Since 1996 the Mark Twain Bank issues e-cash in US\$. The customer base is still small.

A special software called “Cyberwallet“ is required on the buyers machine to handle payments. After withdrawing digital coins from the digital token issuing currency server, the user can buy goods by visiting virtual web stores accepting DigiCash. A good is represented by an URL, by clicking on it the user gives his intention to buy. The http-server at the payee starts via the Common Gateway Interface (CGI) the program “Merchant“. It receives the location of the request and sends a payment request to the Cyberwallet program of the buyer, which replies with sending the digital coins. To protect from double spending the merchant needs to contact the currency server. At the currency server the serial number of the forwarded coins is compared to a large database of all spent coins. When the coins are valid, the Merchant software sends a receipt for the successful payment to the buyer. Now the goods can be transmitted to the buyer. Peirce and O’Mahony [Peirce and O’Mahony 1995] discuss the DigiCash payment system in more detail.

Our analysis starts with the social attributes. Anonymity is the most prominent attribute of DigiCash. It is provided by a technique called *blind signature*. The buyer generates a random serial number N . This serial number is “blinded“ by applying a hash function Rec to it. The blinded serial number is sent to the currency server, where the blinded serial number is signed (U' in Figure 2). At the client a function r-1 , the inverse of Rec , is applied to U' . This generates a signed serial number that is the same as if N instead of $\text{Rec}N$ would have been signed by the currency server. The seller receives the signed serial number N , but even if the seller and the bank collude (the bank has only seen $\text{Rec}N$) they could not get hold of the buyers identity. DigiCash is a payment system that provides full anonymity. However, to avoid double spending, a database of spent serial numbers is required.

We now proceed with the technical analysis. We did not identify major security risks. Messages sent over the Internet are secured by public key cryptography and resist the three threats to security. Also the buyer does not need to keep payment system specific information on his computer. This results in a “++“ for security. The system seems to be reliable, since we could only identify the currency server as a point of failure. When a transaction fails, there is always the possibility to send the coins again. This results in a

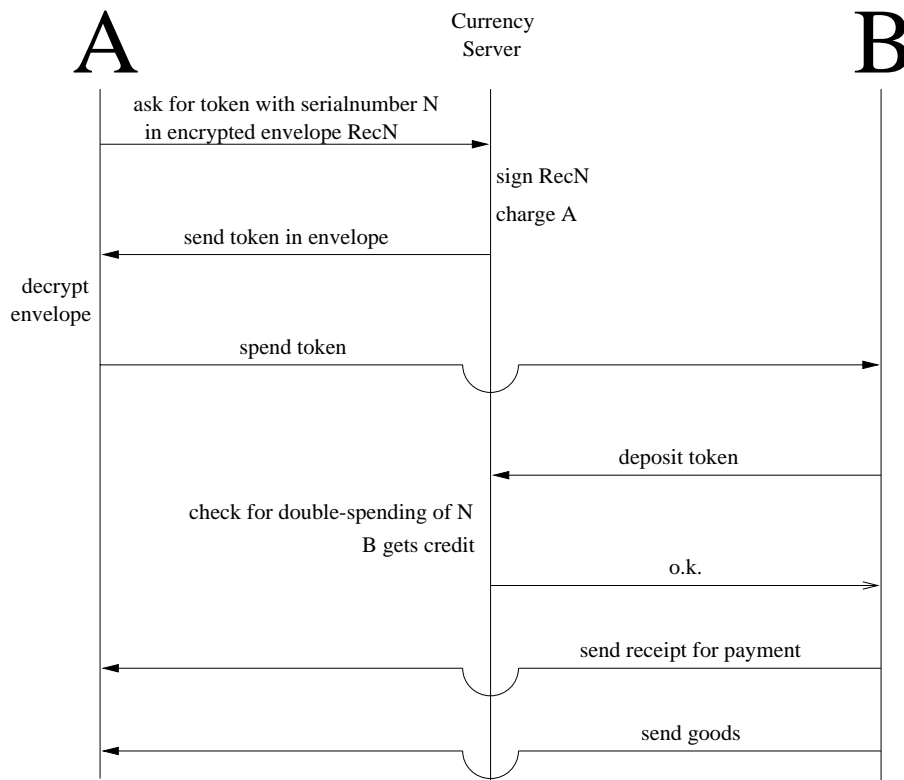


Figure 1: A coarse, verbal description of DigiCash as a VTS diagram.

“++“ for reliability.

The problem of DigiCash is scalability. Every spent coin needs to be stored at the currency server. This can result in large amounts of data. There are possibilities to issue coins locally or let them have an expiration date, but these solutions will affect scaling, too. Partly anonymous electronic currency systems have an advantage here because only issued but not spent coins have to be stored. We rank scalability for DigiCash “–“.

Concerning latency, we observe that only 7 Internet-connections are required, each sending a relative small amount of data. Latency may however be a problem at the points where public key decryption is needed. Of minor impact on latency seems to be the query on the database of spent coins since it is a simple key search for the serial number. A connection to the banking-net is only necessary on a periodical basis and has no influence on latency. So latency is mainly deducted by the frequent use of public key cryptography. We set a “+“ for latency.

The cost structure of DigiCash is mostly influenced by the goal for anonymity. The

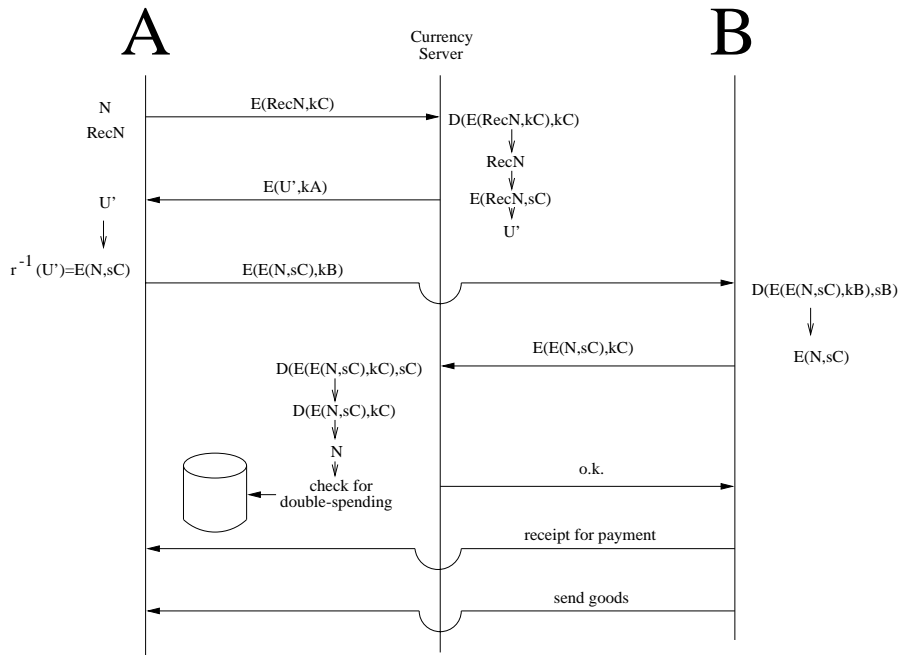


Figure 2: A detailed, formal description of DigiCash as a VTS diagram.

protection against double spending by storing spent serial numbers implies bad scalability. This requires periodically new investments in its infrastructure. Cost will increase stepwise with the number of DigiCash transactions. However, connection to traditional financial instruments which we assume to be costly, is only needed for periodical clearing. Overall we assign a “-“ for low transaction-costs. Exchange will be atomic for the payment process. If a transaction fails the coin can be spend again. For the whole business transaction an atomic exchange is not guaranteed, because the payment is separate from the transmission of the good. The best rating of the attribute atomic exchange for systems having payment and transfer of goods in a serial order will be “-“, which we also assign for DigiCash.

4.2 Analysis of SET

Secure Electronic Transaction (SET) is an open industry standard to allow for secure payments on the Internet using the credit card mechanism. On the one hand, the goal is to provide security to the customer for credit card payments to approved sellers, on the other hand it is to protect the seller by an authentication of the customer. Release 0.8 was tested for a year before SET specification 1.0 was released June 1997 by Visa and

Mastercard. Applications are expected to conform to SET in early 1998.

The parties of a payment transaction include a card holder, seller, card issuing bank (issuer), and the bank of the seller (acquirer). To provide authentication of the parties a certification authority is needed. The card holder sends an initial request to the seller. The seller responds with a certifying document that the buyer verifies at the certification authority. Now the buyer sends encrypted ordering information and credit card information separately to the seller. The seller can decrypt the ordering information, but is not able to see the credit card information. The seller contacts his bank, which uses the banking-net to contact the credit card-issuing bank to receive payment authorisation for the transaction. When this authorisation has been forwarded to the seller the payment process is completed and goods can be exchanged.

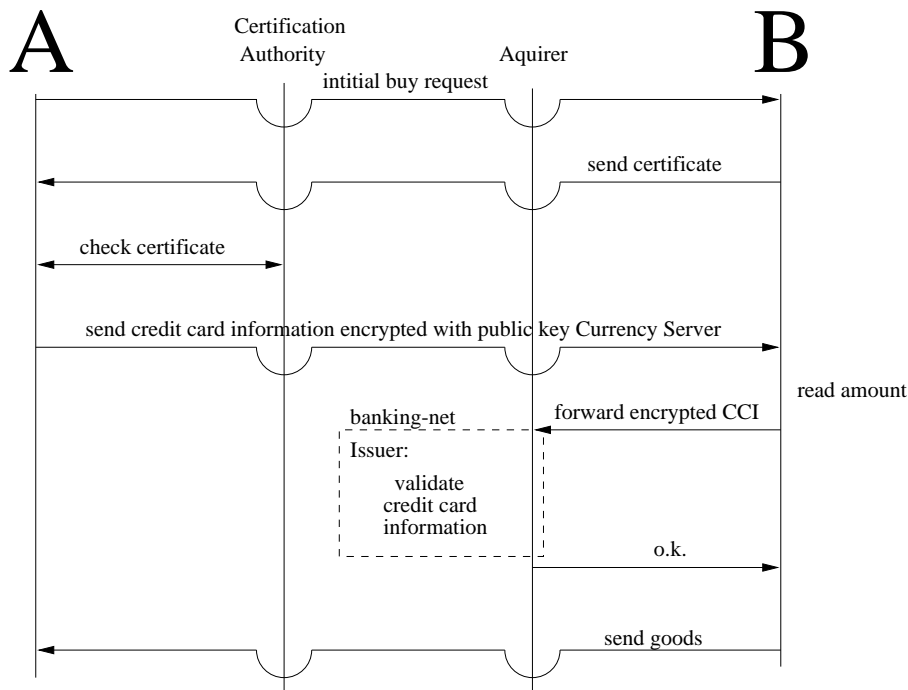


Figure 3: A coarse, verbal description of SET as a VTS diagram.

Interestingly the social analysis of the system is not quite the same as a social analysis of the traditional credit card. Anonymity is different to that of credit cards, since the seller does not see credit card information (CCI). Due to the authorization of the payment by his bank an authentication of the buyer is not necessary for him. However, in contrary to DigiCash the credit card issuing bank can trace the spendings of the buyer. Peer-to-peer

payments are not possible because the role of the payee is restricted to shops that have a contract with the credit card issuing institution.

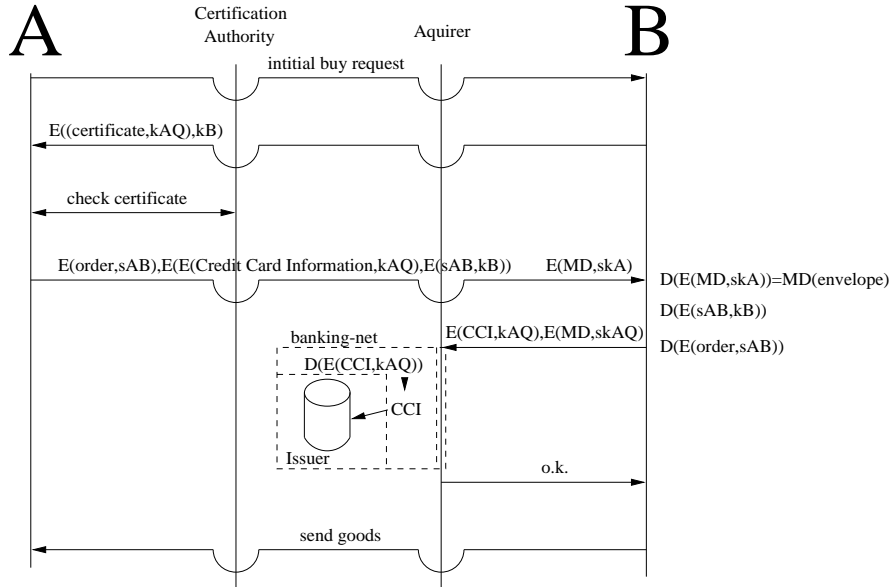


Figure 4: A detailed, formal description of SET as a VTS diagram.

The merchant cannot add fake charges because the credit card information is connected to the order and he has no access to the encrypted credit card information. As long as the acquirer and issuer can be trusted to handle authorization requests properly, security is given for all involved parties. Since this is not controllable, security is ranked "+". Reliability can be assumed to be high where transactions are performed through the traditional banking-net. Only the connection between Internet and the banking-net is a possible point of failure. Reliability will have the grade "+". The system has a scalable design and allows for different credit card issuers. This is reflected in a "++" for scalability.

Latency is crucial because of payment authorization by the issuer for every payment through financial networks. So this part of the transaction will have similar latency as credit card accepting automated teller machines (ATM). Access to the server of the acquirer seems not to be a problem, because there will be competition between banks. Because latency of authorization between acquirer and issuer seems to be quite high, we rate a "-" for latency.

Transaction-costs will be influenced by setting up the certification authorities and interconnection fees. Interconnection should be less costly, because of existing infrastructures

of credit card companies. Low transaction-costs will be “+“. Atomic exchange of the payment is provided through traditional banking transactions. For the business transaction atomic exchange is not provided. We apply a “-“ for atomic exchange.

4.3 Analysis of First Virtual

Third-party processing differs from electronic currency by depending on existing financial instruments [Kalakota and Whinston 1996]. In contrast to credit card transactions they do not transmit credit card information over the Internet. Buyer and seller need to register with the payment system provider.

First Virtual is using the telephone to transmit credit card information for the registration of buyers. When registered, the payment transactions are authenticated by an identification number. At First Virtual they are called VirtualPIN.

In a business transaction the buyer clicks on a web-page accepting payments using the First Virtual payment method. The merchant sends the VirtualPIN of the buyer and his own to the payment server of First Virtual. On receipt of the sellers transaction request, First Virtual sends an e-mail to the buyer to let him confirm the order. After confirmation the credit card transaction will be processed on secure conventional financial networks.

Note, that different from other payment systems the transaction will only be conducted if the customer explicitly confirms by an e-mail to First Virtual.

Some anonymity is provided to the buyer by allowing nicknames. The seller will not get the identity of the buyer. The bank, however, has to know the identity for the confirmation and thus can observe buying habits. Peer-to-peer payments are possible with this kind of third-party processor. The current implementation of First Virtual is not supporting peer-to-peer payments.

Messages used by the payment system are sent by the *Simple Mail Transfer Protocol* (SMTP). First Virtual is using public key cryptography only for signing the confirmation message to the seller. So secure messaging is not part of the payment system but relies on individual agreements between the participants. Authentication between buyer, seller, and First Virtual is provided by the VirtualPIN. The buyer is protected from fraud by his confirmation to First Virtual. We rate security “-“.

Scalability can be provided by using several payment servers. We apply a “++“ for scalability. Reliability of the payment mechanism is up to the processing at First Virtual.

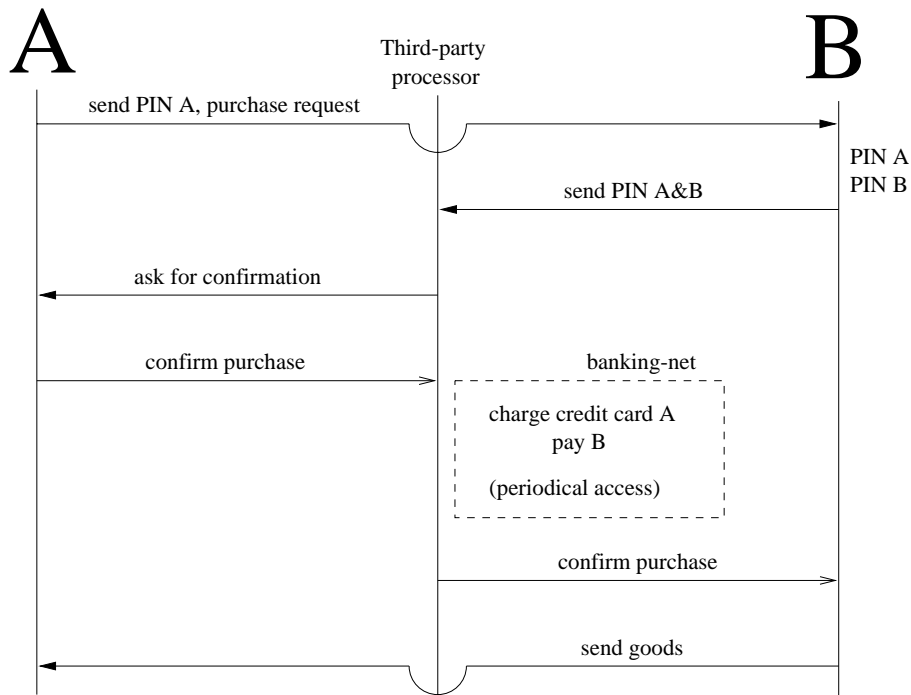


Figure 5: A coarse, verbal description of First Virtual as a VTS diagram.

The clearing will take place external to the Internet, using existing financial instruments. A problem can be the connection between Internet and banking-net, influencing the evaluation negative. We set a “+“ for reliability.

At first glance latency seems to be low. The system uses only 6 communication contacts and the lack of cryptography will result in less demanding processing power at the payment server. However, if we count the e-mail reply by the customer as a part of the payment process, latency gets very high. So we grade this attribute with “-“.

The economic analysis shows that costs are low regarding processing power and bandwidth. Therefore lower security can be a cost-factor when the system grows: Fixing problems and reimbursing customers have to be included in prices. We rate the attribute low transaction-costs “+“. Atomic exchange of the payment is provided through traditional banking transactions. Again atomic exchange is not provided for the business transaction. We apply a “-“ for atomic exchange.

5 Conclusions

We have proposed a framework to evaluate electronic payment systems in general, and its applicability for micropayments in particular. The approach is based on two ingredients: first, to set up a well-structured, not too complex parameter vector of desired features. Second, to use VTS diagrams for a better understanding of transactions in a system. Together they provide a framework for micropayment evaluation. While we used the VTS diagram as a point of orientation in a qualitative analysis of attributes, it might be interesting to apply them in a more formal approach for a quantitative analysis.

6 References

- Baumol, Panzar, Willig 1982** Baumol, W.J, Panzar, J.C., Willig, R.D.; “Contestable Markets and the Theory of Industry Structure“, Harcourt Brace Jovanovich, New York, 1982.
- Becklehimer 1994** Becklehimer, Jeff; “How do you cite URL’s in a bibliography;“ [web page] Aug 1994; <URL: <http://www.nrlssc.navy.mil/meta/bibliography.html>>.
- Chaum 1985** Chaum, David; “Security without Identification: Transaction Systems to Make Big Brother Obsolete“; Communications of the ACM, Vol. 28 (10), pp. 1030-1044, October 1985 [web page] Chaum, David; “Security without Identification: Card Computers to Make Big Brother Obsolete“; <URL: <http://www.digicash.com/publish/bigbro.html>>.
- Kalakota and Whinston 1996** Kalakota, Ravi; Whinston, Andrew B., “Frontiers of the electronic commerce“, Addison-Wesley, 1996.
- MacKie-Mason and White 1997** MacKie-Mason, Jeffrey; White, Kimberly; “Evaluating and Selecting Digital Payment Mechanisms. “, In: Rosston, Gregory L.; Waterman, David (eds.): Interconnection and the Internet. Selected Papers from the 1996 Telecommunications Policy Research Conference. Mahwah, NJ: Lawrence Erlbaum, 1997, [web page] Nov 96; <URL: <http://www-personal.umich.edu/~jmm/papers/digidoll.pdf>>.

- Medvinsky and Neuman 1993** Medvinsky, Gennady; Neuman, B. Clifford; “Net-Cash: A design for practical electronic currency on the Internet“, In Proceedings of the 1st ACM Conference on computer and Communication Security November 1993 [postscript file] URL: <ftp://prospero.isi.edu/pub/papers/security/netcash-cccs93.ps.Z>
- Neuman 1995** Neuman, B. Clifford; “Security, Payment, and Privacy for Network Commerce“, IEEE Journal on Selected Areas in Communication, Vol. 13 (8), October 1995 [postscript file] <URL: http://204.178.16.7/jsac/unprot/jsac13.8/neuman/abs_neuman.html>.
- Neuman and Medvinsky 1995** Neuman, B. Clifford; Medvinsky, Gennady; “Requirements for Network Payment: The NetCheque Perspective“, Proceedings of IEEE Compton’95 March 1995 [postscript file] <URL: <ftp://prospero.isi.edu/pub/papers/security/netcheque-requirements-compton95.ps.Z>>.
- Peirce and O’Mahony 1995** Peirce, Michael; O’Mahony, Donal; “Scalable, Secure Cash Payment for WWW Resources with the PayMe Protocol Set“, Source, [web page] <URL: <http://www.w3.org/pub/Conferences/WWW4/Papers/228/>>.
- Rolfs 1974** Rolfs, Jeffrey; “A Theory of Interdependent Demand for a Communication Service“ Bell Journal of Economics and Management Science, Vol. 5 (1), pp.16-32.
- Rumbough et al. 1991** Rumbaugh, J., Blaha, M., Premerlani, W., Eddy, F., Lorenson, W.; “Object Oriented Modelling and Design“, Prentice Hall, 1991.
- Varian 1995a** Varian, Hal R.; “The Information Economy: How much will two bits be worth in the digital marketplace;“, Scientific American, September 1995, pp. 200-201 [web page] <URL:<http://www.sims.berkeley.edu/~hal/pages/sciam.html>>.
- Varian 1995b** Varian, Hal R.; “Pricing Information Goods“, June 1995, [web page] <URL: <ftp://alfred.sims.berkeley.edu/pub/Papers/price-info-goods.ps.Z>>.
- XIWT 1995** XIWT (Cross-Industry Working Team); “Electronic Cash, Tokens and Payments in the NII.“, [web page] <URL: http://www.cnri.reston.va.us:3000/XIWT/documents/dig_cash_doc/ElecCashToC.html>.