T U M

I N S T I T U T F Ü R I N F O R M A T I K

Chablis - Market Analysis of Digital Payment Systems

Ricarda Weber

TUM-I9819
August 98

T E C H N I S C H E U N I V E R S I T Ä T M Ü N C H E N

TUM-INFO-08-I9819-0/1.-FI

Druck: Institut für Informatik der
Technischen Universität München

Chabilis - Market Analysis of Digital Payment Systems

Ricarda Weber

Version 1.0

August 18, 1998

Contents

1 Motivation

In digital libraries users can obtain documents or other information online. The requested data can be delivered online. For data with costs users need to render payments.

Of course it is always possible to use traditional financial networks for this, but possible in this case does not mean economically feasible or user friendly. Especially when delivering low cost information with a value of only a few cents or even lower like for a encyclopedia entry the traditional financial networks approach is unsuitable. Digital order and delivery requires in most cases also a method of instant payment especially when dealing with anonymous users. Therefore it should be possible to conduct payments online without major media breaks and time lags.

To allow digital payments across the Internet a great number of schemes and system proposals have been devised. For few there exists a working solution or at least a prototype. The following sections present an overview of proposed digital payment systems.

2 Criteria Catalogue

This section presents a criteria catalogue of requirements to and features of digital payment systems and architectures to allow for their systematic classification and evaluation. The requirements and features have been derived from the evaluation of existing payment systems and system proposals.

2.1 Features

When describing or categorizing digital payment systems, different features [Owe97] have to be analyzed to determine how well requirements of a potential user can be met. There exist several different digital payment system models. However, in every case their basic purpose is to transfer monetary value from one party to another. They differ in many aspects, e.g. the degree of security or privacy granted or the manner of linking the movement of real monetary value to a digital transaction.

2.1.1 Economical

Name: The brand name under which the payment system is known.

Origin: The authors of the payment system, their company or institute and especially the supporting institutions and organizations provide an indication for the possibility of success for a given payment system.

Status: The status of the development of an payment system is of interest when having to choose a payment system for practical employment. As payment system might be a purely theoretical proposal, there might exist a first prototype, it could be in public trial, software could be open to public review, the payment system could provide a working solution already in commercial use or it could have triggered the development of further payment systems.

Milestones: The milestones and dates that lead to the current status of a payment system indicate the acceptance and support of a given system. Consequently dates like when proposed, since when prototyped, since when in public trial or since when operational have to be taken into consideration.

Payment Size: The size of payment supported must be matched against the pricing structure it is to cover. Minimum and maximum size of payments possible and optimum size of payments supported must be compared to the typical size of transaction expected. Macropayments involve large payments from about 10 USD onwards. Small payments are from 0.1 USD or higher. Micropayments can involve fractions of Cents.

Risk: The distribution of risk when using a payment system has to be considered. The risk could be on the payer side, one the payee side or be carried by the bank. Maybe special cover policies are in operation. The risk of financial loss to each party involved in the payment transaction needs to be low and acceptable. The level of risk involved with the use of a digital payment system is related to its security. Loss to customers can be limited by setting a maximum value for each transaction and special approval required for large transactions. Granting low financial risk may involve a tradeoff to ease of use, especially the unobtrusiveness of a payment system.

Fees: Fees imposed by the provider of a digital payment system should be considered to determine whether a digital payment system can be used economically. Fees could be imposed e.g. for the initial set up, per transaction, per withdrawal or deposit of real funds both for merchants and customers.

User Base: The merchant and customer base of a payment system determine its attraction for further merchants and customers to employ this particular scheme for their own usage. Usage statistics would be of special interest in this context.

Prerequisites: The platforms available determine the infrastructure, hardware and software required for the operation of the payment system. They should match the infrastructure already in operation.

Information Policy: The information policy of the company can be an indication of the quality and security of the payment system.

2.1.2 Technological

Participants Picture 1 shows the basic digital payment scenario and its main participants. Participants and involved parties are e.g. broker, issuer, acquirer, payee, payer, observer, arbiter, ... [APASW96]. Aim of a payment is to transfer monetary value from payer to payee.

Payer: The payer is making the payment. Usually it is the customer or buyer in an electronic commerce scenario.

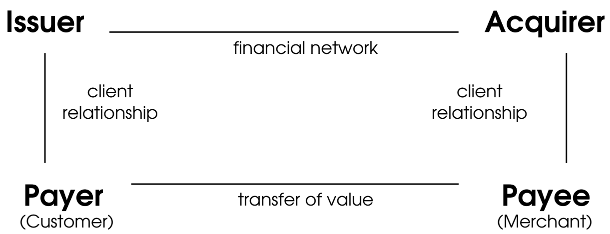

Figure 1: Basic Digital Payment Scenario

Payee: The payee is receiving the payment. Usually this party is referred to as the merchant or seller in an electronic commerce scenario.

Issuer: The issuer is the third party interacting with the payer, i.e. usually the bank or service provider of the payer.

Acquirer: The acquirer is the third party of the payee, i.e. usually the bank or service provider of the payee.

Broker: A broker is a combined issuer and acquirer if a protocol requires a single third party shared by payer and payee.

Observer: An observer is a usually uninvolved third party that is used in the privacy analysis of a payment system. The observer tries to gain information from the transaction.

Certification: Many payment schemes are based on the presence of a registration and certification authority for the management of authentication and symmetric keys like Kerberos [BSK89] or public keys certification [Sch96].

Arbiter: An arbiter may be involved in resolving disputes in the payment system. In most systems the presence of an arbiter is not explicit. Even if proofs of evidence are produced, dispute handling usually is done outside the payment protocol and unspecified or impossible within the payment protocol level but depends on the policy decisions of users and banks.

Trusted Third Parties: Sometimes notaries are used e.g. to enforce payment receipt notifications, clearings or witnessing of transactions. Trusted so called mixes, like proposed in AIMP (see section 4.3), can provide means for making payments untraceable.

Money Models Money Models determine the medium of value exchange in a payment transaction [CST95a].

Token: Medium of exchange is a marker representing value like traditional cash. Tokens either have a value themselves (like gold coins) or their value is based on the trust in the status and solvency of the entities which issue these tokens. Token systems do not support debt. Digital coin systems with tokens of fixed value face the problem of having to render change if the customer does not have tokens to pay the exact price.

Notational: Value is stored and exchanged by authorization like with a bank account. The bank maintains a record of the amount in the account. Notational systems support debt when they permit negative balances. Notational systems do not need to render change. Exchanges based on notational money require the debiting of of the payers account and the crediting of the payees account.

Payment Models Payment Models classify the digital payment systems according to the necessary flow of information between the participants of an electronic transaction [APASW96]. Basic distinction is the presence or absence of a direct communication between payer and payee. In the case of indirect communication the payment itself concerns only the initiator of the payment - which may be the payer or the payee - and the issuer and acquirer. Indirect payment systems are usually considered as part of home banking in the context of digital payments on the Internet. Most current digital payment systems implement direct payments. Another distinction is the time when the monetary value is actually taken from the payer, i.e pre-paid and post-paid systems. These corresponds directly to the token and notational money models described above. Pre-paid systems are commonly referred to as cash-like or token-based and post-paid systems are usually called account-based or notational. Secure credit card presentation over the Internet makes direct use of the existing credit card infrastructure.

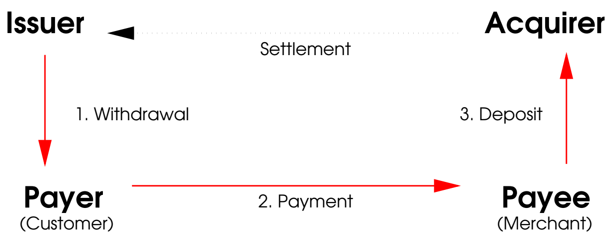

Figure 2: Direct Cash Like Payment Model

Direct Cash Like: In direct cash like systems the payer withdraws money from the issuer, hands the payment tokens over to the payee who in turn deposits the payment with its acquirer. Picture 2 shows this scenario. Direct cash like payment systems use the token money model. The acquirer then asks the issuer for a settlement. Such payment systems usually involve either tamper proof hardware like smart cards, like Mondex (see section 4.29), or online validation by the issuer, like Ecash (see section 4.16), to protect against double spending of digital cash which is of course trivial to copy.

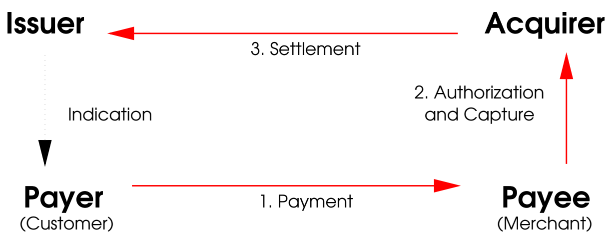

Figure 3: Direct Account Based Payment Model

Direct Account Based: Direct account based payment systems resemble traditional cheque systems. They allow the payer to hand over a payment authorization (cheque) to the payee, who presents the payment authorization to its acquirer who in turn redeems it from the issuer. The issuer the indicates to the payer the completion of the payment. Picture 3 shows this scenario. Direct account based resp. so called cheque like payment systems use the notational money model.

Figure 4: Indirect Push Account Based Payment Model

Indirect Push Account Based: In the indirect push payment model the payer instructs the issuer to transfer funds to the payees account at the acquirer. This model resembles most a traditional bank transfer. The payee is just notified of the incoming payment. Picture 4 shows this scenario.

Figure 5: Indirect Pull Account Based Payment Model

Indirect Pull Account Based: In the indirect pull model the payee instructs the acquirer to charge the payers account at the issuer. The traditional banking equivalent is a debit advice. The payer is just notified of the outgoing payment. Picture 4 shows this scenario.

Secure Credit Card Presentation: Payment systems that are based on secure credit card presentation over the Internet make direct use of the existing credit card infrastructure, like SET (see section 4.47). Most important point in using a credit card for payments through the Internet is the secure transmission of the credit card data. The payer transmits the credit card data or their equivalent to the payee who submits them in turn to the acquirer for online validation. The acquirer resolves the actual payment via the established financial networks. Basically no special accounts for payers and payees besides the existing credit card accounts are required. The drawback for credit cards is their unsuitability for micropayments.

Validation Validation of payments ensures the linking of real value transfer to an electronic payment. The method of validation depends on the particular payment protocol. Validation can comprise a double spending test in the case of a token system, like Ecash (see section 4.16), or a credit check in the case of a secure credit card presentation, like CyberCash (see section 4.12). The time of validation is directly correlated to the efficiency of a digital payment system [Owe97].

Online: Online validation systems require communication of the payer and/or the payee with a third party, i.e. issuer an/or acquirer. In an online payment system, payer and payee are connected online with a third party like the issuer and/or acquirer who validate the payment, so the payee is guaranteed the receipt of the corresponding monetary value by a trusted third party at the time of the payment. Online systems are therefore often considered more secure.

Offline: Offline validation systems involve only communication between payer and payee at the time of the payment. In most offline digital payment systems validation is provided by tamper resistant hardware like smartcards and their electronic wallets. Double spending also can be made provable after the fact by cryptographical means thereby increasing security, like CAFE (see section 4.7).

Semi-online: Semi-online validation systems require some interaction with third parties but not at each payment. Some semi-online systems require the initial payment to be online and subsequent transactions just involve payer and payee, like MilliCent (see section 4.27). Other semi-online systems enforce third party interaction when certain spending limits have been reached, like Mini-Pay (see section 4.28), or at probabilistic intervals like Polling (see section 4.43). Local payee-side validation can e.g. be enabled by localization of tokens, like MilliCent (see section 4.27), or correlated payment sequences, like PayWord (see section 4.40).

Security Mechanisms Security Mechanisms of an individual payment system depend on the features to be provided and the underlaying assumptions of trust. Basic security requirements in all payment systems however usually are integrity, authorization, confidentiality, availability and reliability. The protocol of any payment system should be disclosed to public review as the security of a payment system should not depend on the secrecy of its protocol. Though some payment protocols are not disclosed up to now, like Mondex (see section 4.29). Integrity of a payment system means that only authorized payments can take place. No user may loose money without that user's authorization. To authenticate a message means proving the identity of its origin to the recipient. Payment authorization can be obtained in different ways.

Out-band: Out-band authorization means that the verifying party - usually a bank - sends a notification to the payee and requires that party to approve or deny the payment using a secure out-band channel like traditional mail, telephone or email, like First Virtual (see section 4.18).

Passphrase: In shared key cryptography the verifying party requires a shared secret known only to the authorizing and verifying party to be included in every payment message, i.e. something like a PIN or other shared secret [Sch96] [BSK89]. The message is authenticated via a cryptographic check value, the so called message authentication code (MAC). Non-repudiation can not be provided by passphrase authorization, as the secret is shared between the verifier and the authorizer.

Signature: The verifying party requires a digital signature of the authorizing party. This involves message digests [Riv92] and public key cryptography [Sch96]. In public key cryptography each party has a pair of keys. The signature key is kept secret. The verification key is made public with a certificate binding the identity of the owner to it. Certificates are signed by a well known authority whose verification key is known to the verifier thereby providing the so called chain of trust. Signatures provide non-repudiation as the secret key is only known to the authorizing party.

Dual Signature: There are cases where it is required to link a payment authorization with the offer the payment was authorized for, like SET (see section 4.47). A dual signature allows to combine two separate messages in a way that they can't be misused separately. Still both messages can be sent separately and be verified by the dual signature as belonging to the context of the other message. Dual signatures concatenate the digest of the offer with the digest of the payment authorization and sign the resulting new digest to provide provability of purpose-tied payments without disclosing the offer itself.

Blind Signature: The blind signature technique can be used to provide unconditional untraceability [Cha82]. It allows a issuing bank to authorize digital payment tokens created by the payer without being able to read the probabilistical unique serial number of the token which was generated by the payer. The payer hides the serial number by a so called blinding factor and submits it to the issuer for authorization. The issuer signs the token with the blinded serial number and returns it to the payer deducting the value of the token from the account of the payer. The payer then unblinds the serial number while the token retains its valid signature tendered by the issuer. Unconditional untraceability requires online double spending database checks.

Offline Tokens: For off-line systems with no option to check for double spending before or during the transaction a modification of this technique was developed that provides a once concealed, twice revealed feature, like CAFE (see section 4.7). It includes secret sharing that allows to uncover the identity of a payer by tracing double spending after the fact. Here each token contains a part of the identity of the payer and if the payer double spends it is possible to recover the identity of the payer from those several copies. Two complete payment transactions in which the payer participates, using the same coins, are necessary to reveal the payers identity. If the payer only performs one transaction with each coin, the payer is still untraceable.

Challenge Response: So called challenge response techniques allow for authentication without surrendering any information (zero knowledge proof) [Sch96], thereby protecting against attacks like snooping or replay. One party sends a random message and the challenged party responds with the answer computed by a shared key. This technique is commonly used in smart cards authenticating themselves to each other.

Chained Hash: Subsequent payments to the same payee can be made by means of payment chains, like PayWord (see section 4.40), that can be verified by the payee based on the preceding payments. This method is only suitable for low value micropayments.

Costs Costs of a transaction refer to actual, technically founded costs as contrast to provider imposed policy based fees mentioned above.

Other cost factors of digital payment systems are refunding customers, credit risk, record keeping, advertisement and promotion costs, high profit margins, operation costs of billing server, communication, processing and storage costs.

General storage requirements influence the costs of a system, like the need for double spending detection databases or digital coin deposits, who stores the digital cash and who performs the aggregation of payments. The party that gains pre and post transaction float, gets a cost benefit by that.

System Setup: System setup costs cover the phase from deciding for a particular payment system to its being ready for the first payment. This might e.g. comprise costs for obtaining a smart card and reading equipment, costs for setting up a digital offer in compliance with the payment system or costs for obtaining credentials to enable the payer to make payments or the costs to enable the payee to receive payments, i.e. installation and registration costs, account startup costs. Average cost per transaction of adopting the payment protocol must be low.

Transaction: Transaction costs cover the costs for individual payments. Costs for a payment transaction can be estimated by considering its latency (see below) Transaction costs for the first payment to a particular payee can differ from costs for subsequent payments to the same payee, like MilliCent (see section 4.27). Regular transaction costs for payments can differ from exception transaction costs e.g. if spending limits are exceeded, like Mini-Pay (see section 4.28). Usually micropayment enabling payment system offer detailed cost estimation for different situations.

Latency: Latency describes the time required to complete a transaction, e.g the delay caused by communication, computation, queuing or network. The number of public key operation and/or the amount of messages required to complete a transaction can be used to estimate and compare latency. Latency should be as low as possible.

Genealogy Genealogy of a payment systems often helps to understand a payment system more easily. Relations to other payment systems, like inheritance, influence or similarity can be used to characterize a payment system easily and efficiently.

2.2 Requirements

This section defines requirements to digital payment systems for the Internet. Importance of individual characteristics are determined by actual user needs. For example one user might wish to remain anonymous during transactions as the most important thing, another user might require to do many low value transactions economically and doesn't care so much about anonymity. When deciding for a particular digital payment system [MMW97], the possible characteristics have to be ranked according to the preferences and needs of the decision maker.

2.2.1 Transaction

A monetary transaction should conform to the ACID conditions well known from database systems [CST95a].

Atomicity: Either a transaction occurs completely or it does not occur at all.

- **Transfer of Funds:** Merely funds transfer is atomic. This means, either the account of the payer is debited and the account of the payee is debited with the corresponding amounts or no change of accounts occurs at all.
- **Complete Transfer:** Both funds and money transfer are linked and atomic. This means, if a document delivery is linked to the payment for it and either both happen or none at all. This is the basic idea of the so called fair exchange protocols [CPS95] [SPC96] [Zwi96].

Consistency: All parties concerned must agree on the relevant facts of the transaction. This means all parties concur on the amount to transfer, on the reason for the transfer and also on the fact of the transfer having taken place.

Isolation: Transactions must be independent of each other. The result of a set of concurrent transactions must be equivalent to a serial sequence of these transactions.

Durability: It must always be possible to recover the last consistent state. Even after a system crash a consistent state should be recoverable and transactions and states valid before, e.g. amount of money available, should be valid after as well.

2.2.2 Security

Digital payment systems must address security issues like fraud protection and confidentiality grants to provide a trustable instrument to conduct business with. Customers also often even require anonymity when spending digital money.

Fraud Protection: Digital payment systems must be tamper resistant and robust against attacks. Illegal use of digital cash must be prevented or at least digital payment systems must provide means for detection and punishment of misuse after the fact. A lack of fraud protection would result in a loss of trust in that digital payment system as a store of value exchange medium and render the system worthless. A digital payment system must of offer protection against classical security attacks like any system used to carry sensitive information. Common attacks to be prevented are for example replay, modification or repudiation of payments messages, denial of service or framing. Source and destination of data must be authenticated. Encryption, signatures and message digests can serve to this end. Some systems also use so called out band [AJSM97] security measures like email or fax reconfirmation, like First Virtual (see section 4.18).

- **No Double Spending:** A major issue to be addressed is the double spending problem. Digital cash is represented by bytes that can easily be copied and respent. This concerns not only customers that might reuse digital money for several purchases, but also merchants that could attempt to resubmit digital money for redemption. So called double spending databases serve to register digital money spent.
- **No Counterfeiting:** Money can only represent value, if it is not be possible for individuals to create or counterfeit money. At least one should not

be able to use such money undetected. It should be easy to distinguish legal money from unauthorized illegal money [CST95a].

No Overspending: Prevention of customer overspending, i.e. exceeding of spending limits is another fraud protection issue especially with account based systems.

Non-Refutability: The parties involved should be able to verify that the payment transaction took place, and what the data and amount of the transaction have been. A record of the transaction should be produceable. This might involve a tradeoff with privacy control.

Hardware Tamper Resistance: Various digital payment systems rely on tamper resistant hardware like smart cards to prevent double spending and forgery [Dig95] and can be used offline. However breaking of the hardware would leave the users open to attacks [Ano97]. The reliability of the hardware used should be certified.

Unauthorized Use: The payment device should not be easily stealable and usable unauthorized.

Privacy Control: Customers often prefer to keep their spending habits private. At the very least they do not want unrelated observers to track their payments. Often customers prefer also merchants and sometimes even banks to be unable of observing and tracking their spending. When information held by one user is hidden from another user that information is said to be private [CST95a]. Transaction participants may want to control the level of privacy. Different parts of a transaction may be accorded different levels of privacy. Transaction elements include amount, date, time, location, product and the identities of the customer and the merchant. Information may be easily observed, may have a limited range of values, may be observed only under certain conditions, or be completely hidden. Legal restrictions may apply to this. Monitoring of the user's spending patterns and setting up user profiles should be impossible. Traditional payment systems like credit cards and cheques allow the tracing of a user's actions, cash on the other hand doesn't. At least tracing should be hard and require too much effort in comparison to the benefit from tracking down an individual.

Confidentiality: Observability of transactions when using a digital payment system is of particular concern to users who wish to conduct confidential business. Therefore grants of confidentiality by the payment system are essential to user acceptance. Encryption of data flow between customer and merchant payment systems can be made untraceable to third party observers.

Anonymity: The identity of a user of digital money should be protectable. When the identity of a user is hidden, the transaction is said to be anonymous [CST95a]. Anonymity can hold with respect to single parties like customer towards merchant or with regards to all parties, i.e. banks as well, like Ecash (see section 4.16). Pseudonyms can be used instead of real identities to hide the identity of the customer from the merchant, like CyberCash (see section 4.12).

Untraceability: When two different payments by the same user cannot be linked, the transaction is not only said to be anonymous but also called untraceable [AJSM97]. So called trusted mixes can provide means to ensure anonymity and untraceability. Blind signatures [Cha82] can provide anonymity and untraceability not only with respect to the merchant but also towards the issuing and acquiring banks without having to rely on trusted third parties, like Ecash (see section 4.16).

2.2.3 Interoperability

In an electronic commerce scenario lots of different parties in different roles with multiple aims are involved, like different customers and merchants, their banks and service providers, different amounts, currencies and payment systems.

Divisibility: Money should allow both for low value and very high value transactions. So divisibility should allow to replace a single high denomination transaction by several low denomination transactions [CST95a]. This of course applies to token based payment systems only.

Bidirectionality: Not only regular merchants should be able to receive payments but also customers, like Ecash (see section 4.16). Such two way payment systems allow both for efficient refunds as well as for small scale merchants, i.e. trade among private persons. Peer to peer payments should be possible. The payment instrument should work both ways without either party being required to attain registered merchant status. E.g. a cheque is bidirectional, a credit card is not.

Respendability: The receiver of digital money should be able to transfer it to another person just like normal cash without the intervention of a third party (like a bank). The payee should not have to take intermediate steps after receiving a payment to respend it. E.g. a credit card payment must be deposited with a bank, it is not immediately respendable. Digital payment systems that enable such transferability can promote untraceability but are harder to secure than supervised systems.

Acceptability: Electronic cash issued by one bank should be accepted by other banks as well. Customers and merchants should not be required to have the same bank to be able to cooperate. This supports also the scalability of a digital payment system.

Multicurrency Support: The value of a digital payment system increases with the number of users who accept it. A single national currency support impedes a world wide acceptance. So an accepted and relatively fixed way to convert different currencies is required [CST95a].

Exchangeability: Electronic payments of one digital payment system should be easy to exchange for payments for other digital payment systems. Different user needs will most likely facilitate the coexistence of several distinct digital payment systems, allowing users to select the payment system suited best for a given transaction. Therefore digital payment systems should interoperate, so that it becomes possible to convert electronic cash from one payment systems to another. For example a transit fare card is not exchangeable for a money order but a money order is exchangeable for cash.

Transferability: The payment instrument should not be bonded to a particular individual. It should be usable by other persons than the original owner. This will involve a tradeoff with security. E.g. a cash or prepaid phonecard are transferable, a credit card is not.

Portability: Security and usability of a payment system should not be dependent on a certain physical location, e.g. a certain computer.

Flexibility: Different levels of security of payment are required, depending on the needs of the parties involved, like the amount of the payment to transfer, timing of the payment or provability of the transaction. A payment infrastructure therefore ideally will support several payment methods integrated into a common framework [APASW96], like InterPay (see section 7.2), JEPI (see section 7.5) or JECF (see section 7.4). For this the payment system must provide a standardized programming interface.

2.2.4 Scalability

A large customer and merchant base of a given digital payment system is the crucial prerequisite for its user acceptance. When users and resources are added, the digital payment system should continue to work without noticeable performance loss. Digital payment systems should support many consumers buying goods at the same time from many a lot of merchants. Some digital payment systems for example like Ecash (see section 4.16 record on a central server all coins that have been spent to prevent double spending by checking a unique coin identifier before every new transaction. Such a database will grow and so this digital payment system becomes less scalable as the time for searching the database grows and still a single central server is required. The protocol should place to limit on the total number of customers for a given merchant or on the number of transactions that can be made with a given merchant.

Off-line Operation: Customers and merchants should be able to transact securely without a trusted third party having to be online all the time. This reduces delay and increases availability of the payment system as well providing the foundation for scalability. A payment system requiring online operation may be subject of time delays during periods of network congestion, thereby decreasing the reliability of the payment service.

2.2.5 Micro Economy

Information services can and will be offered in highly fragmented, like an entry in an encycolpaedia or a telephone directory, the usage of a general search or a map finder service or a newspaper clipping. These services should not only be offerable via ad sponsoring or subscription but also on a pay per use basis. A payment system should make low value (e.g. less than 1 Dollar or even less then one Cent) transactions economically feasible. Such low priced services should be usable frequently by a multitude of customers. Therefore micropayment techniques need to be both inexpensive and fast.

Low Costs: The cost of executing a payment transaction should be low enough to render low value transactions economical. Even the transfer of tiny amounts should be economically feasible. The payment protocol should be suitable for use in transactions with a value of one Cent or less.

Efficiency: Billing for information services can cause frequent payments for quite low amounts. Digital payment systems must be able to perform such micropayments without noticeable loss of performance. Such efficiency may involve a tradeoff with security. It may allow only for the use of lightweight encryption or no encryption at all.

To this end compromises must be made with regards to security, like Mini-Pay (see section 4.28). This is justified by assuming a lower risk due to the small amounts. Often computationally expensive public key encryption is substituted by cheaper shared key technology to gain efficiency, like NetBill (see section 4.32). Special solutions exist for repeated micropayments to the same merchant based on chained one way hashes, like PayWord (see section 4.40). or on localized vouchers, like MilliCent (see section 4.27.

2.2.6 General Economy

In order to become an accepted economical instrument, a digital payment system needs to provide a trusted, reliable and economically feasible service to a sufficiently large user community. It must be easy to integrate and easy to use to be accepted by customers and merchants.

Operational: A system should be operational today to be employable right away. Purely theoretical proposals are of little worth to solve problems of now.

Large User Base: For a merchant the attraction of a digital payment system is affected by the size of its customer base and vice versa. How many customers are using a particular payment system determines how much effort a merchant is willing to undertake to support it. Customers on the other hand will tend to acquire those payment facilities that offer them access to many merchants.

Low Risk: The risk of financial loss associated with the use of the payments system should be low and controllable.

Reliability: An electronic payment system must be highly available and reliable in its operation. The even temporary failure of such a widely and frequently used infrastructure system can be fatal to economic interests of its users and render this system worthless.

Conservation: Digital money should be easy to store and retrieve and not become invalid with time [CST95a]. This means temporal consistency, i.e. money keeps its value over time, as well as temporal durability, where money is easy to store and retrieve. Users also should be able to store and retrieve digital money remotely.

Ease of Integration: Existing applications and offers need to be modified to allow for the usage of a digital payment system. A standardized common programming interface of digital payment systems would render this task easier [APASW96]. Payment requests should be integrated into standardized challenge response protocols on which applications can be built, like InterPay (see section 7.2).

2.2.7 Ease of Use

A digital payment system must be easy to understand and transparent. Users should find the payment process accessible, easy to effect and quick. Operation must be clear and simple, especially the start of a payment transaction must be clearly defined so users never feel trapped into rendering payments. No special expertise should be required. Further parameters that influence the user acceptance are e.g. portability, account required, customer gains float, hardware independence, ergonomy, no encryption or software installation required and low fixed and transaction fees.

Unobstrusiveness: Unobstrusiveness is an important factor for the ease of use of a payment system. Users should not be interrupted to provide payment information all the time. Most payments should occur automatically. This is particularly important with small transactions. The customer should not need to initiate new actions frequently for payments. Few steps should be required to complete a transaction. Users should be able to set up spending profiles to control their spending. Payments beyond a certain threshold should be presented to the user for reconfirmation.

Low Latency: the payment transaction should be quick and should not delay the purchase action.

Low Transaction Costs: Conducting transactions should not be expensive. Economy of a transaction must be seen relative to the value to transfer. Fees charged by the financial intermediaries must be low per transaction as a percentage of the amount of the transaction. Micro-economy support allows to conduct small value transactions economically (see above).

Low Fixed Costs: Setting up and running the payment system should be inexpensive.

Hardware Independence: Users should not require specialized hardware.

2.3 Profiles

2.3.1 Feature Profile

Table 1 sums up the feature profile used for the description of digital payment systems in the following section.

2.3.2 Requirement Profile

Table 2 shows the requirements profile of traditional payment systems [CST95a]. In the case of cash, the ACID properties are fulfilled. Cheques are not money transfer atomic as there can be a significant delay for clearance. Credit card transaction can appear money transfer atomic to the merchant but the card issuer may lose on the transaction due to clearance delays. Neither system is goods-transfer atomic as

Web Resource	URL.
Name	Brand name of the digital payment system.
Origin	Authors and supporters of the system.
Status & Milestones	Status of the payment system and the milestones that lead up to it.
Payment Size	Optimal, minimum and maximum size of payment
Money Model	Money model the system uses, i.e. token or notational.
Payment Model	Payment model the system uses, e.g. cash-like, account-based, secure credit card presentation
Validation	Time of the validation of the payment, i.e. online, offline, semi-online.
Privacy Control	Level of confidentiality, anonymity, untraceability provided by the solution.
Security Mechanism	Security technologies used, e.g. out-band, passphrase, (blind/dual) signature, challenge response, chained hash
Prerequisites	Hardware, e.g. a smart card, special software, additional prerequisites like a credit card.
Risk	Who carries what risk of financial loss.
Fees	Fees policy of operational payment systems
Latency/Costs	Latency resp. costs for an individual payment transaction.
User Base	Number of customers and merchants who employ this solution.
Limits	Limits of the payment system, e.g. only operational in the USA.
Remarks	Further special features of the system.
Genealogy	Systems that this system inherited from, influenced or is similar to.

Table 1: Feature Profile Definition

Requirement/System	Cash	Cheque	Credit Card
Token System	Yes	No	No
Transaction			
Atomicity	Yes	No	No
Consistency	Yes	Yes	Yes
Isolation	Yes	No	No
Durability	Yes	Yes	Yes
Security			
No Double Spending	Yes	n.a.	n.a.
No Counterfeiting	Some	No	No
No Overspending	Yes	No	No
Non-Refutability	No	Yes	Yes
No Unauthorized Use	No	Some	Some
Anonymity	Yes	No	No
Untraceability	Yes	No	No
Interoperability			
Divisibility	Yes	n.a.	n.a.
Bidirectionality	Yes	Yes	No
Respendability	Yes	No	No
Acceptability	Yes	Yes	Yes
Multicurrency Support	Yes	Yes	Yes
Exchangeability	Yes	Partly	No
Transferability	Yes	No	No
Portability	Yes	Yes	Yes
Scalability			
Scalability	Yes	Yes	Yes
Off-line Operation	Yes	Yes	No
Economical Issues			
Operational	Yes	Yes	Yes
Large User Base	Yes	Yes	Yes
Buyer Risk	Yes	No	Limited
Seller Risk	No	Yes	No
Reliability	Yes	Yes	Yes
Conservation	Yes	Yes	Yes
Ease of Use			
Unobstrusiveness	Yes	Yes	Yes
Low Latency	Yes	Yes	Yes
Micropayments	Yes	No	No
Macropayments	No	Yes	Yes
Low Fixed Costs	Yes	Yes	Yes
Buyer HW Independence	Yes	Yes	Yes
Seller HW Independence	Yes	Yes	No

Table 2: Requirements Profile of Traditional Payment Systems

they deal with the transfer of funds only. A transaction by cheque or credit card is not isolated because of the delay for clearance during which the balance of the cheque or credit card account might have been altered and prevent the completion of the transaction. Divisibility is only an issue with a token based system like cash. Account based systems like cheques or credit cards do not need to render change. The question of storing and retrieving value is not relevant in a credit card system.

2.3.3 Visibility Profile

Issues revolving around privacy control and information disclosure associated with a transaction can be characterized by visibility tables [CST95a]. Visibility tables show the visibility of various pieces of information with respect to the parties involved in the transaction directly or indirectly. Each digital payment protocol has its own intrinsic visibility profile. These characteristics render some protocols better for certain types of transactions than others.

who / what	Merchant	Customer	Date	Amount	Item
Merchant	-	Partial	Yes	Yes	Yes
Customer	Yes	-	Yes	Yes	Yes
Bank	No	No	No	No	No
Observer	Yes	Partial	Yes	Yes	Yes

Table 3: Visibility of a cash transaction

Table 3 shows that a cash transaction is completely private and anonymous with respect to the bank, but not with respect to the customer, merchant or a well placed observer.

who / what	Merchant	Customer	Date	Amount	Item
Merchant	-	Yes	Yes	Yes	Yes
Customer	Yes	-	Yes	Yes	Yes
Bank	Yes	Yes	Yes	Yes	No
Observer	Yes	Yes	Yes	Yes	Yes

Table 4: Visibility of a cheque transaction

Both cheque and credit card transactions are less anonymous than a cash transaction. Table 4 shows the visibility profile of a personal crossed cheque [CST95a].

who / what	Merchant	Customer	Date	Amount	Item
Merchant	-	Yes	Yes	Yes	Yes
Customer	Yes	-	Yes	Yes	Yes
Bank	Yes	Yes	Yes	Yes	No
Phys./Dig. Observer	Yes/Partial	Partial	Yes	Yes/No	Yes/No

Table 5: Visibility in a credit card transaction

Table 5 shows the visibility profiles for an EFTPOS credit card transaction [CST95a]. In the case of credit card transactions two types of observers are possible. Physical observers that are present at the actual point of sales can observe the physical transaction. Digital observers monitor network traffic but are unable to read encrypted information. As payment information in financial networks is sent encrypted, it is invisible to a digital observer.

In digital payment systems and electronic transactions, only digital observers are relevant. Some digital payment transactions can be more confidential, anonymous and untraceable than traditional payment forms, hiding the identity of the customer from the merchant and vice versa.

2.4 References

[Zwi96], [AJSM97], [oPS96], [Ric96], [Dav97], [Dig95], [Faj96], [Het97], [LL96], [Ric97], [Con97], [SW97] , [LSS96], [Sir97] , [CB97], [Owe97], [MMW97], [APASW96]

3 Systems Overview and Clustering

This section gives an overview over the digital payment systems and system proposals analyzed in detail in the following section 4. This section serves to give a quick overview over the different digital payment systems. To support the task of selecting payment systems of interest, payment systems can be clustered according to a nested suitable subselection of their features depending on the interest of the reader or decision maker.

Such clusters need to yield a suitable division, i.e. neither too coarse nor too fine grained to render any useful information. Therefore branching may sometimes have to be aborted at a certain level to avoid empty or nearly empty leaves. Cluster topics need to be tailored to the interest of the decision maker.

3.1 Technological Clustering

Table 6 shows a possible technological clustering of digital payment systems. Money models are token and notational. Payment models are direct cash like, direct account based, indirect push account based and secure credit card presentation. Validation is performed online, offline or semionline. Basic security is provided by smart cards, chained hashes, probabilistic or other means.

Notational indirect push account based systems are validated online per definition, because the bank as a third party is involved in each payment. Notational secure credit card presentation schemes are validated online for security reasons due to the usually larger payments involved in these transactions. Payment systems validated semionline or offline deal with small or micropayments and a certain risk of payment default is accepted to improve efficiency.

Model/ Validation	Token Direct Cash	Notational Direct Account	Credit Card	Push Account
Online	4.16 Ecash 4.25 MagicMoney 4.34 NetCash 4.38 PayMe	4.5 BankNet 4.14 CyberCoin 4.19 FSTC 4.32 NetBill 4.35 NetCheque 4.15 DSR	4.1 ACC 4.10 C.-POINT 4.12 CyberCash 4.18 FirstVirtual 4.22 iKP 4.46 SecureCourier 4.47 SET 4.50 VeriFone	4.3 AIMP 4.4 ATS 4.8 CheckFree 4.17 eVend 4.36 NetFare
Semionline	4.27 MilliCent	4.2 Agora 4.28 Mini-Pay 4.43 Polling		
Offline	*HW* 4.6 Brands 4.7 CAFE 4.20 Geldkarte 4.29 Mondex *Chains* 4.30 MPTP 4.31 Mykro-iKP 4.33 NetCard 4.40 PayWord 4.42 PhoneTicks 4.48 SubScrip *Other* 4.24 Lottery 4.26 MicroMint 4.49 TUB	4.13 CyberCents 4.23 InterCoin		

Table 6: Technological Clustering of Payment Systems

Status / Size	Macropayments	Small Payments	Micropayments
Operational	4.4 ATS 4.5 BankNet 4.8 CheckFree 4.10 CommercePOINT 4.12 CyberCash 4.18 FirstVirtual 4.46 Secure Courier 4.50 VeriFone	4.14 CyberCoin 4.17 eVend 4.23 InterCoin	
Trial	4.35 NetCheque	4.7 CAFE 4.16 Ecash 4.25 MagicMoney 4.29 Mondex 4.32 NetBill 4.34 NetCash	4.27 MilliCent
Development	4.19 FSTC 4.47 SET	4.20 Geldkarte 4.13 CyberCents	4.28 Mini-Pay 4.36 NetFare
Proposal	4.1 ACC 4.3 AIMP 4.22 iKP	4.6 Brands 4.38 PayMe	4.2 Agora 4.15 DSR 4.24 LotteryTickets 4.26 MicroMint 4.30 MPTP 4.31 Mykro-iKP 4.33 NetCard 4.40 PayWord 4.42 PhoneTicks 4.43 Polling 4.48 SubScrip 4.49 TUB

Table 7: Economical Clustering of Payment Systems

3.2 Economical Clustering

Table 7 shows a possible economical clustering of digital payment systems. Payment size can vary from macro- (major bills and above) to small (coins or minor bills) and micropayments (until subcent regions). Status of a payment system can be proposal (including maybe a prototype), serious development, closed or public trial or operational.

Most working systems involve unstandardized solutions about basic secure credit card presentation or simple account keeping schemes either at the merchant or a bank. Systems in trial sometimes may not yet move to an operational status due to security doubts and risks involved if the system were compromised. Various proposals exist about micropayment schemes but still no single solution has found a wider acceptance yet.

4 Individual Proposals

This section introduces individual digital payment systems and system proposals. For each system at least a short or extended feature profile and a summary of its characteristics and properties is given.

All proposals of major significance (as well a some of lesser importance) are headed with a full feature profile, a description of the main data, ideas, security measurements and transaction steps and tailed by their visibility and requirements profiles.

Where the primary material about the system exceeds the Web page indicated in the feature profile, that literature is appended in a special reference paragraph of that payment system description.

4.1 ACC

Web Resource	[ACC97]
Name	ACC.
Status & Milestones	proposal, 1994
Genealogy	extended by followup proposal AIMP (see section 4.3)

Table 8: ACC Feature Profile

ACC, the anonymous credit card protocol aims at providing anonymous credit cards for physical goods purchases. It is a proposal by D. Kristol, S. Low, N. Maxemchuck and S.Paul of AT&T Bell Labs from 1994.

The central idea is to separate all information needed for a transaction into different components and use cryptographic techniques to hide from a party those components that are not necessary for that party to perform its function.

With ACC the customer is physically in the store of the merchant and makes one physical purchase. The identity of the customer is hidden via a trusted mix. The protocol is extended for use on the Internet by further work of the authors about AIMP, the anonymous Internet mercantile protocol (see section 4.3).

References: [KLM94a], [LMP94]

4.2 Agora

Web Resource	[Ago97]
Name	Agora
Origin	E. Gabber and A. Silberschatz of AT&T Bell Labs.
Status & Milestones	Proposal and small prototype, November 1996.
Payment Size	Micropayments, maybe also larger payments.
Money Model	Notational.
Payment Model	Direct account based.
Validation	Offline, probabilistically online.
Privacy Control	Pseudonymity, limited merchant side untraceability, no encryption.
Security Mechanism	Signatures and certificates, probabilistic online validation.
Prerequisites	Customer payment applet, merchant cgi-scripts and database, no HW.
Risk	Depending on bank policy.
Fees	n.a.
Latency/Costs	Low, piggybacking on normal HTTP messages, fast evaluation of revocation lists required.
User Base	n.a.
Limits	Arbitration only for static, time-insensitive goods.
Remarks	n.a.

Table 9: Agora Feature Profile

Table 9 shows the Agora feature profile. Agora aims to be a minimal distributed protocol for electronic commerce and is a proposal by E. Gabber and A. Silberschatz from Bell Labs. It was presented at the USENIX workshop of electronic commerce in 1996. There supposedly exists a prototype with Java applets for Netscape browser and cgi scripts connected to a database for NCSA Web server. The protocol implements an application layer security on top of HTTP.

Agora intends to support high volume transactions at low incurred cost. It is a credit account based notational protocol, i.e. account identifiers are used for payment. Customers and merchants need to have valid accounts at their respective issuing and acquiring banks which are financial institutions whom they trust. Agora supports multiple banks that are connected via a financial network, and a pay per view cost model.

Agora is authenticated and non-repudiable due to the use of digital signatures. All involved parties require their own pair of public and private keys. Issuer and acquirer respectively provide customer and merchant with signed ids valid for a certain billing period to identify themselves by certifying the public keys of their clients which are contained in those ids together with a unique name, expiry date and account number. It is assumed that both customer and merchant know the public keys of all banks involved. Impostors (man in the middle) are to be detected by checking the unique name against the expected name.

The protocol is termed minimal as the cost incurred is close to free Web browsing. It requires a total of four messages to complete an Agora transaction including the transfer of goods without any online central authority access. When employed as a Web commerce protocol, these messages can be piggybacked on existing HTTP messages and no extra messages are required.

The basic message flow for a purchase transaction is as follows:

1. The customer asks for a offer from the merchant, e.g. by asking for a menu page in a `GET` request.
2. The merchant returns together with its id signed by the acquirer a signed binding offer containing a locally unique offer id, e.g. by returning a menu page as generated order form.
3. The customer verifies both the validity of the id of the merchant and the correctness of the signature on the offer. Then it returns together with its id signed by the issuer a signed binding order based on the data of the offer, e.g. by another `GET` request.
4. The merchant verifies both the validity of the id of the customer and the correctness of the signature on the order as well as that the order data correspond to the offer data. Then the merchant supplies the goods to the customer, e.g. by releasing the pay per view page.

Merchants periodically submit accumulated orders to the acquirer for settlement. Double charging can be detected by the bank due to the unique order id. Offer and order together provide proof of transaction.

Agora is distributed and scalable. Merchants can authenticate customers without accessing a trusted third party online. Customers with valid accounts can purchase from any merchant without any special preparation. Banks broadcast lists of revoked customer ids to merchants who must be able to store and handle these lists. The overspending problem is addressed by introducing a probabilistic algorithm that offers fraud control allowing for a certain low level of fraud at a tradeoff to message minimality. A merchant asks the acquirer for online authorization with a certain probability or each time when the total of outstanding orders from a customer exceeds a predefined limit.

Table 10 shows the visibility profile of an Agora transaction. The protocol can provide a certain pseudonymity for the customer by using account aliases instead of real account names. A limited merchant side untraceability can be obtained by generating new customer pseudonyms every billing period and allowing for several aliases. The protocol does not address any privacy issues. The use of HTTP reveals much information about the client to the server and encryption is not part of the present Agora protocol.

The protocol introduces online arbitration by a trusted third party arbiter to resolve disputes about falsely, partially or undelivered goods that are assumed static and

who / what	Merch.	Cust.	Date	Amount	Item
Customer	Yes	-	Yes	Yes	Yes
Merchant	-	Partly	Yes	Yes	Yes
Issuer	Yes	Yes	Yes	Yes	No
Acquirer	Yes	Partly	Yes	Yes	No
Arbiter	Yes	Partly	Yes	Yes	Yes
Observer	Yes	Partly	Yes	Yes	Yes

Table 10: Agora Visibility Profile

time-insensitive. For this the merchant includes a digest of the goods in the offer so customer can verify them. When making a complaint the customer submits offer and order to the arbiter who in turn submits a signed request for the goods to the merchant. If they correspond to the offer, the arbiter reroutes them to the customer, otherwise it revokes the order at the acquirer.

Table 11 shows the requirements profile of Agora.

Reference: [GS96]

4.3 AIMP

The anonymous Internet mercantile protocol (AIMP) aims at anonymous funds transfer over the Internet. It is a proposal by D. Kristol, S. Low and N. Maxemchuck of AT&T Bell Labs, Murray Hill, New Jersey from March 1994. The protocol applies the principles of information separation derived from prior work of the authors about ACC (anonymous credit cards, see section 4.1) and is an extension of that protocol for its application on the Internet. An implementation on top of FTP was supposedly aimed at.

Main issues of AIMP is to facilitate anonymous funds transfer and goods over the Internet while protecting the interests of the involved parties. It aims at firstly to protect the interest of the merchant by transferring funds first, secondly to grant anonymity to the customer by information separation and as a third to protect the interest of the customer by providing a transaction proof.

AIMP is a debit account based notational protocol, i.e. account identifiers are used for payment. To place the deposit with the merchant, the indirect push account model is used, i.e. the customer transfers funds to the merchant's account as payment. Customers and merchants need to have valid accounts at their respective issuing and acquiring banks which are financial institutions whom they trust. AIMP supports multiple banks. Funds are transfered only among trusted entities. The protocol introduces a further party, the so called information exchange and federal reserve, i.e. one or more trusted mixes. These mixes allow customers and sellers to communicate without knowing each other's identity and to transfer funds between banks. For the latter every bank has an account with the mix, the accounts are settled up periodically and the banks do not need to know each other. All transfers are signed and logged by the mix.

Requirement/System	Agora
Token System	No
Transaction	
Atomicity	Yes
Consistency	Yes
Isolation	No
Durability	Yes (merchant needs good DB)
Security	
No Double Spending	n.a.
No Counterfeiting	Yes
No Overspending	Limited, probabilistic approach
Non-Refutability	Yes
No Unauthorized Use	Yes
Anonymity	Yes, weak pseudonymity
Untraceability	Yes, limited and merchant side only
Interoperability	
Divisibility	n.a.
Bidirectionality	No
Respendability	No
Acceptability	Yes
Multicurrency Support	Yes, via banks
Scalability	
Scalability	Yes
Off-line Operation	Yes, just probabilistic online verification
Economical Issues	
Operational	No
Large User Base	n.a.
Buyer Risk	No or Limited, but depending on bank policy
Seller Risk	Yes, but depending on the bank policy
Reliability	n.a.
Conservation	Yes
Ease of Use	
Unobstrusiveness	Yes
Low Latency	Yes
Micropayments	Yes
Macropayments	Maybe, limited
Low Fixed Costs	n.a.
HW Independence	Yes

Table 11: Agora Requirements Profile

Web Resource	[AIM97]
Name	AIMP
Origin	D. Kristol, S. Low and N. Maxemchuck of AT&T Bell Labs.
Status & Milestones	Proposal and maybe a small prototype, March 1994.
Payment Size	Macropayments, maybe repeated micropayments.
Money Model	Notational.
Payment Model	Direct account based with merchant local session accounts. Indirect push account based for deposit payments to the merchant's bank account.
Validation	Online!
Privacy Control	Anonymity, untraceability, privacy.
Security Mechanism	Signatures, public key encryption and passphrases, online validation, deposit payments, kind of 'one-time' public key usage.
Prerequisites	Various unspecified SW, no HW.
Risk	No merchant risk, limited seller risk.
Fees	n.a.
Latency/Costs	High, communication via mix, lot's of encryption.
User Base	n.a.
Limits	-
Remarks	n.a.
Genealogy	Derived from ACC (see section 4.1)

Table 12: AIMP Feature Profile

The basic steps for a purchase transaction are as follows (note: unless stated otherwise, all communication is performed via a trusted mix, all messages are encrypted with the public key of the recipient):

1. The customer has the public key of the merchant and - sending its own public key - requests and obtains anonymously and encrypted the account of the merchant via the mix. Enquiries about goods and negotiation of prices is performed in a similar manner.
2. The customer has the public key of the merchant's bank and transfers funds anonymously to the merchant's account via the issuer and the mix as follows:
   (a) The issuer authenticates the customer via a passphrase, debits the customer's account and authorizes the mix to transfer the debited amount.
   (b) The mix transfers funds from the account of the issuer to that of the acquirer and authorizes the acquirer to transfer the credited amount.
   (c) The acquirer credits the account of the merchant, generates as receipt and sends it to the customer anonymously via the mix and to the merchant enabling it cross-check the receipt for the session account.

   The customer gets the receipt which it presents to the customer to open a session account.
3. The customer anonymously makes no, one or multiple goods requests from the merchant who deducts their price from the session account. The merchant delivers the goods encrypted with the public key specified by the customer. Depositing additional funds during a running session adds more session accounts to that session.

4. When the customer has finished obtaining goods, it sends a quit message to the merchant containing anonymous the customer's account. Any remaining balance from the session account(s). is refunded anonymously to the customer analogous to the deposit process. The customer gets a signed deposit receipt by the issuer. For repeated small purchases from the same merchant the customer might choose to retain a session account over a longer time.

AIMP is private, authenticated and mutually non-repudiable due to the use of encryption and digital signatures. All involved parties require their own pair of public and private keys. Timestamps and counters prevent replay. From the protocol description it appears that a kind of 'one-time' public key usage is intended.

who / what	Merch.	Cust.	Date	Amount	Item
Customer	Yes	-	Yes	Yes	Yes
Merchant	-	No	Yes	Yes	Yes
Issuer	No	Yes	No	Sum	No
Acquirer	Yes	No	No	Sum	No
Mix	Partly	Partly	Yes	Sum	No
Observer	No	No	Yes	No	No

Table 13: AIMP Visibility Profile

Table 13 shows the visibility profile of AIMP. After a transaction the merchant knows it has been paid for certain goods but not by whom. The issuer and acquirer each know about the amount of deposit and withdrawal, but neither destination resp. source nor reason of the payments. The mix knows the issuer and acquirer concerned, but not the individual accounts. Without collusion, no party can associate the customer with the purchase.

Table 14 shows the requirements profile of AIMP.

Reference: [KLM94b]

4.4 ATS

Automated Transaction Services (ATS) provides secure credit card and account presentation payments facilities in a funds transfer manner. The payment details interaction occurs between customer and ATS gateway, the merchant is indicated success or failure. Confirmation emails are sent by ATS as an additional security to both customer and merchant.

4.5 BankNet

BankNet, a MarketNet company, operates in UK and offers an electronic cheque system in GBP. It is similar to homebanking. It allows users to check their accounts and write electronic cheques. Other facilities are currently under development.

BankNet is payment provider for MarketNet, a SSL based shopping mall. For

Requirement/System	AIMP
Token System	No
Transaction	
Atomicity	No
Consistency	No
Isolation	Yes, prepaid
Durability	Yes
Security	
No Double Spending	n.a.
No Counterfeiting	Yes
No Overspending	Yes, prepaid
Non-Refutability	Yes
No Unauthorized Use	Yes
Anonymity	Yes, but trusted mix
Untraceability	Yes, tracing needs collusion
Interoperability	
Divisibility	n.a.
Bidirectionality	Yes
Respendability	No
Acceptability	Yes
Multicurrency Support	Yes, via banks
Scalability	
Scalability	Yes, many mixes possible
Off-line Operation	No!
Economical Issues	
Operational	No
Large User Base	n.a.
Buyer Risk	Limited by deposit
Seller Risk	No
Reliability	n.a.
Conservation	Yes
Ease of Use	
Unobstrusiveness	Questionable
Low Latency	No
Micropayments	Partly, if repeated payments, but then locally traceable
Macropayments	Yes
Low Fixed Costs	n.a.
HW Independence	Yes

Table 14: AIMP Requirements Profile

Web Resource	[ATS97]
Name	ATS
Status & Milestones	Currently operational.
Payment Model	Indirect push account based, funds transfer model. Secure credit card and account presentation are performed in an indirect push manner.
Security Mechanism	SSL and out-band, i.e. confirmation emails.

Table 15: ATS Feature Profile

Web Resource	[Ban97]
Name	BankNet
Origin	BankNet and MarketNet from GB.
Payment Model	Direct account based, digital cheques.
Status & Milestones	Operational since may 1995
Privacy Control	No anonymity, full user authentication.
Prerequisites	No HW, for digital cheques WorkHorse for Windows.
Security Mechanism	SSL, electronic cheques use full length public key encryption and signature. Going for SET (see section 4.47).
Fees	Special services are charged at various rates.
User Base	About 2000 visitors per day.
Limits	Not accessible between 1.30am and 7.00am, electronic cheques currently only usable between BankNet accounts, available only in GBP.
Remark	Account checkable online, no transaction charges, self defined limits.

Table 16: BankNet Feature Profile

128 bit SSL a WorkHorse client software is required. MarketNet certificates are signed by Eurosign. The BankNet ECheque digital cheque system is available to all BankNet account customers. MarketNet will be integrating SET (see section 4.47) into the BankNet banking service.

4.6 Brands Cash

Web Resource	[Bra95b]
Name	Brands Cash
Payment Model	Direct token based.
Status & Milestones	Proposal from 1994
Privacy Control	Confidential, anonymous, untracable.
Security Mechanism	Public key cryptography, signatures, offline tokens, tamper resistant HW.
Prerequisites	Smartcard and reader, special SW.
Genealogy	Base for CAFE (see section 4.7).

Table 17: Brands Cash Feature Profile

Internet payment mechanism involving Smart Cards. Base for the CAFE project (see section 4.7). Author is now research scientist at Digicash (see section 4.16).

Reference: [Bra93], [Bra94], [Bra95a], [Bra95c]

4.7 CAFE

The European Union project CAFE (Conditional Access For Europe) is a offline direct cash like scheme which guarantees customer anonymity. The CAFE project ended in mid 1997, but is continued in the follow up project OPERA. The partners

Web Resource	[CDS+96a] [CDS+96b]
Name	CAFE
Origin	Digicash, CWI, Siemens, universities of Leuven, Aarhus, Hildesheim, Karlsruhe, etc. and many others, an EU project.
Status & Milestones	In trial. Project ended in 1997, pilot phase since 1997, follow up project OPERA.
Payment Size	Optimal, minimum and maximum size of payment
Money Model	Token.
Payment Model	Direct cash-like.
Validation	Offline.
Privacy Control	Encrypted, anonymous, untraceable.
Security Mechanism	Passphrase, public key encryption and signature, blind signature, offline token, tamper-resistant hardware, spent token database.
Prerequisites	HW wallet, smart cards resp. merchant terminal
Risk	POS transactions, depending on bank policy either bank or merchant, some risk for customer at loss or damage to wallet.
Fees	Multiparty security, multicurrency and -bank support
Latency/Costs	Low, local authorization, double spending detection after the fact.
User Base	?
Limits	Trial only, presently not for Internet use.
Remarks	n.a.
Genealogy	Based on Digicash Ecash (see section 4.16) and Brands Cash (see section 4.6).

Table 18: CAFE Feature Profile

in OPERA, i.e. banks that are support CAFE, are continuing the trial of and improving the CAFE system.

About thirteen partners from several European countries were involved in the project, Digicash and Siemens among them. Basically the system is designed for use in shops rather than over the Internet. In a way it is the offline, portable versions of the Digicash Ecash system (see section 4.16). Is is based on the system proposed by Brand's cash (see section 4.6). The protocol is disclosed for public review. Important feature of CAFE is the multi-party security. No mutual trust between parties of conflicting interest is assumed.

CAFE is an open secure system. It supports multiple issuers of electronic value and multiple currencies, including currency exchange during a payment. It provides the customer with a history log of their payments. The system uses public key signature and encryption and allows for offline purchase transactions. The basic purchase transaction mode is anonymous and untraceable for the customer and performed offline, there is no need to connect to a third party online. Withdrawals and deposits are identified, traceable and online. If payments exceeding a certain level must be confirmed, then some online interaction becomes necessary.

CAFE provides recovery of lost, stolen, and damaged cards. Although prepaid it is loss tolerant and allows customers to recover their money if they lose their wallet. For this an encrypted version of all tokens issued to the customer is held in a save place. The customer must surrender its anonymity and untraceability, then the issued token backup can be decrypted and matched against the redeemed token database. To provide some loss tolerance for stolen wallets, the customer must authenticate itself to the wallet via a passphrase (PIN) prior to a purchase.

The device receives coins by withdrawing them from the issuer account via an ATM using the blind signature method known from Ecash. CAFE is prepaid and the tokens on the device do not exist as currency anywhere else. When the customer spends money the device transmits one or more tokens to the merchant and marks them as spent on the device. Transmissions are performed contactless via infrared channels. The merchant then owns the value of those tokens which need to be deposited with an acquirer and accepted by the issuer for that value to be realized for the merchant. Thus, the primary flow of value in CAFE is that of withdraw, pay and deposit, i.e. the payment model is the typical direct cash like approach.

The basic HW device is a pocket calculator like electronic wallet, to be used for customer payments, access to information services and also identification. It aims to be non-proprietary. The electronic wallets and smart cards, i.e. the hardware, should become standardized and be available in shops just like other electronic consumer goods. The wallet contains a so-called guardian, a smartcard with a dedicated cryptographic processor. The wallet protects the interests of the customer, the guardian protects the interests of the money issuer, both are holding part of each token withdrawn. No transactions are possible without the cooperation of the guardian, the guardian maintains a record of all the tokens spent to avoid doublespending. The guardian chip authorizes each payment by signing it. CAFE tokens do not remain in circulation like real cash tokens do. Respendability is broken explicitly, the wallet signs to whom it pays a token and so only that payee can deposit the token.

As fallback - when the guardian is compromised - CAFE uses so called offline digital coins that provide a once concealed, twice revealed feature. The money is encrypted and the identity of the customer signed by that customer is encoded into the token number. This is done in a way that the identity of the customer can only be recovered if the customer double spends. This feature basically works as follows: When the customer uses a token in payment, it is challenged by the merchant to reveal a certain part of the encoded customer identity. One part on its own however does not reveal anything useful. If however the customer tries to respend the same token the merchant again is revealed a part of the customer identity and now with a high probability the identity of the customer can be traced. For this the issuer must hold a database of all reimbursed tokens that it already needs for the fault tolerance feature.

As a fixed denomination token system that distinguishes between customers and merchants, CAFE needs to address the making change problem. It allows the construction of coins that can be split into smaller coins if need be and of coins that -being more expensive than their denomination- may be spent more than once. These measurements reduce the unlinkability of the payments but not their integrity. For repeated very small payments to the same merchant, so called phone ticks, CAFE provides a special way of surrendering a token in installments.

who / what	Merch.	Cust.	Date	Amount	Item
Seller	Yes	Partial	Yes	Yes	Yes
Buyer	Yes	Yes	Yes	Yes	Yes
Broker	Yes	No	Yes	Yes	No
Observer	Yes	Partial	Yes	Yes	Yes

Table 19: CAFE Visibility Profile

For the CAFE visibility profile in table 19 it is assumed that there is a physical observer, as the transaction is offline and the information traffic is just in a infrared channel. Also, as the wallet can only be used with a passphrase (PIN), the buyer is assumed to be the legitimate customer of the device. Further it is assumed that the wallet keeps a basic record of transactions to allow the customer to review its spending. Although normally there is no visibility of customers, their identity can be revealed if they somehow double spend.

Table 20 shows the CAFE requirements profile. In CAFE transactions appear atomic to the user but not to the merchant. The tokens a merchant accepts in payment must be deposited with an acquirer and accepted by the issuer before their monetary value can be realized by the merchant. The value leaves the customer, but does not immediately arrive at the merchant.

References: [BBC+94], [SW95]

4.8 CheckFree

CheckFree Corp. provides a wide range of electronic commerce solutions, including on-line share portfolio management (in conjunction with the PAWWS system (http://www.pawws.com) and general on-line bill payment systems.

Requirement/System	CAFE
Token System	Yes
Transaction	
Atomicity	Yes for user, no for merchant
Consistency	Yes
Isolation	Yes, prepaid
Durability	Yes
Security	
No Double Spending	Yes, tracing after the fact
No Counterfeiting	Yes
No Overspending	n.a.
Non-Refutability	Yes
No Unauthorized Use	Yes
Anonymity	Yes, but identity revealed after double spending
Untraceability	Yes
Interoperability	
Divisibility	Yes
Bidirectionality	No
Respendability	No
Acceptability	Yes
Multicurrency Support	Yes, on the card
Scalability	
Scalability	Yes
Off-line Operation	Yes
Economical Issues	
Operational	Partly, trial ongoing
Large User Base	?
Buyer Risk	Limited by content of card
Seller Risk	No
Reliability	?
Conservation	Yes
Ease of Use	
Unobstrusiveness	Questionable
Low Latency	Yes
Micropayments	Yes
Macropayments	No
Low Fixed Costs	?
HW Independence	No, smart card system

Table 20: CAFE Requirements Profile

Web Resource	[Che97]
Name	CheckFree
Payment Model	Indirect push account based
Status & Milestones	1988
Privacy Control	None
Security Mechanism	Built-in security codes in the cheque processing system
Prerequisites	Software for Windows, OS/2 and Macintosh
Fees	First 30 days free, then USD5.95 for the first 20 payments and USD2.95 for each set of ten payments thereof; at least USD5.95 per month.
User Base	?
Limits	Only for checks in the USA.
Remark	Wallet from CyberCash (see section 4.12).

Table 21: CheckFree Feature Profile

It offers a so called electronic check payment service as replacement for traditional paper checks. This payment system results in a service similar to money order. Their software is compatible to the wallet software from CyberCash (see section 4.12). The Checkfree payment process is described as follows:

1. Customer receives a bill and sends the payment information to CheckFree.
2. CheckFree pays the bill.
3. Bills paid are listed on the monthly customer invoice.

It is not quite clear how CheckFree gets the money to pay the bills from, or when the customer exactly is required to settle up. Presumably the CheckFree account is linked by direct debit to the customers account. From the sparse information available, this system seems to be aiming at providing a convenient way of paying bills, rather than at providing an online transaction system.

4.9 ClickShare

Web Resource	[Cli97] [New97]
Name	Clickshare
Payment Model	Hub account based log keeping followed by invoices.
Status & Milestones	?.
Privacy Control	None.
Security Mechanism	Passphrase.
Prerequisites	Account at a Clickshare merchant.
Fees	None for the customer, ”small” transaction fee for merchant.
User Base	?.

Table 22: ClickShare Feature Profile

Clickshare is a passphrase based, commercial system from Newshare. The Clickshare customer has a single login and password to access all Clickshare merchants.

The system permits registering, validating and profiling customers and enables buying and selling of information among distributed, independent customers and merchants.

It allows for economical and secure microtransactions over the Internet without requiring any special customer software. Clickshare aggregates many small per-page charges and applies them periodically (monthly) to a credit-card, conventional credit or digital cash account.

Customers need to have have an account with one of the Clickshare merchant. This allows them as well access to the offers of all the other Clickshare merchants. Clickshare validates the customers, tracks their content requests and provides billable records to the merchant that keeps the account of that customer.

The business model implies that Newshare takes a small transaction fee on each transfer of information and call this "billable hypertext links".

4.10 CommercePOINT Payments

Web Resource	[Com97]
Name	CommercePOINT
Origin	IBM.
Payment Model	Secure credit card presentation.
Status & Milestones	Development, 1997.
Privacy Control	Confidential.
Security Mechanism	SET compliant.
Genealogy	a SET (see section 4.47) compliant application

Table 23: CommercePOINT Payments Feature Profile

The IBM CommercePOINT Payments system aims at the development of a SET (see section 4.47) compliant credit card payment system.

CommercePOINT will provide the following Software: Wallet for the customer, eTill for merchants and Gateway for payment processors.

4.11 Cybank

Cybank provides an account based payment service for customers with a credit card. It works with a software based virtual smartcard. A list off all transactions is accessible via the Web. The system claims to support transaction as low as one Cent.

The Cybank account is portable, insofar as it can be downloaded on a floppy disk and used on another computer. Each account has an unique id that is used for identification. Multiple accounts for one customer are permitted.

As security features their Web site lists triple DES encryption and public key en-

Web Resource	[Cyb97a]
Name	Cybank
Status & Milestones	Operational, 1996.
Payment Model	Account based, settlement via a credit card.
Payment Size	Small payments, as low as 1 Cent.
Privacy Control	Confidential, pseudonyms, Cybank traces customers via transaction logs, multiple accounts allowed.
Security Mechanism	Public key encryption, Triple-DES encryption passphrase.
Prerequisites	Virtual smartcard software, available for Windows, a credit card.
Fees	5% charge for withdrawing money from the Cybank account to a real account.
User Base	About 2000 users.
Limits	?.
Remark	Transaction reversible if customer not satisfied.

Table 24: Cybank Feature Profile

cryption for the DES key transmission. Cybank provides a so called Secure Relay Proxy (SRP) to protect transactions between customer and merchant and to prevent bookmarking of the delivery URL.

4.12 CyberCash

CyberCash was founded in 1994 and is performing secure credit card presentations since April 1995. They claim to do several thousand transactions per day.

Cybercash provides a range of commerce solutions from credit card based payment systems to secure micropayment systems. Little detailed technical information is available about the CyberCash system. The basic CyberCash system forms a gateway to tie merchants to existing payment systems like credit cards or bank accounts. A second system is their CyberCoin (see section 4.14) mechanism, designed for online transactions and to support small payments from 25 Cents to 10USD. They also will offer the PayNow service, an electronic cheque system, which is currently in trial, offers about the same features as the basic CyberCash system for US citizens with a checking account but aims to be bidirectional at a later stage.

The CyberCash payment system is based on secure credit card presentation payments making use of the existing credit card systems and also bank account systems and simply integrating the merchant software as if it were a real POS terminal, with CyberCash servers acting as a gateway between the Internet merchant and the banks on the secure financial networks.

The CyberCash system uses 1024-bit RSA and 56-bit DES encryption. CyberCash has been granted a worldwide export license for the 1024-bit encryption algorithm as used in the CyberCash system. CyberCash is trying to protect the privacy of their customers by providing them with pseudonyms, i.e. their Wallet ids and by hiding their credit card information from the merchants. The CyberCash software will be made compliant to SET (see section 4.47) standard.

Web Resource	[Inc96]
Name	CyberCash
Origin	CyberCash Inc., cooperations with major banks and providers, like Netscape, Oracle, VeriFone, etc. German projects with Dresdner Bank AG and Sachsen LB.
Status & Milestones	Operational since April 1995.
Payment Size	Macropayments.
Money Model	Notational.
Payment Model	Secure credit card presentation, going to be SET compliant.
Validation	Online.
Privacy Control	Customer uses pseudonyms, CyberCash can read the credit card information, the merchant cannot. The banks can trace all transactions.
Security Mechanism	RSA and DES encryption, signatures, passphrases.
Prerequisites	CyberCash Wallet software, For non-US citizens, a credit card is necessary, US citizens also can use their bank account.
Risk	Credit card company.
Fees	Merchants will be charged a transaction fee.
Latency/Costs	15-20 seconds per transaction.
User Base	Over 500.000 wallets distributed.
Limits	Only US citizens can bind their bank account to the Wallet software.
Remarks	Only limited technical information available
Genealogy	Both input for and going to be SET (see section 4.47) compliant.

Table 25: CyberCash Feature Profile

The CyberCash Wallet is used by the customers on their PC. Some Wallets bear private labels, like Checkfree or Compuserve. Over 500.000 of these Wallets have been distributed. The merchant server is supported by a Vendor server. There are about 77 merchants which use the Wallet software. The Wallet and Vendor server software is available for free and for many Unix and Windows platforms. CyberCash itself provides a gateway to the financial networks. About 80% of the US banks support these transactions.

The Wallet allows customers to create their Wallet Id, i.e. their representation needed for the process of identifying themselves to authenticate a transaction. To set up a Wallet for personal use customers need to register. The customer must provide a personal password, a Wallet id and a verification id. These data are encrypted and sent to CyberCash. The Wallet id is linked to a credit card or bank account. It can be backuped on a floppy disk to provide portability.

The Wallet resides on the customer PC will be started automatically when customers click on a designated button in the merchant order page. To open the Wallet passphrase authentication is required, then the Wallet connects to CyberCash. When customers make a purchase, the merchant uses the encrypted payment information to inform CyberCash, who in turn decrypt the payment details, reformat and send them to the acquirer. After the acquirer and issuer approved of the payment, the CyberCash server encrypts the result and returns it to the merchant who sends the customers an electronic receipt and transmits the goods.

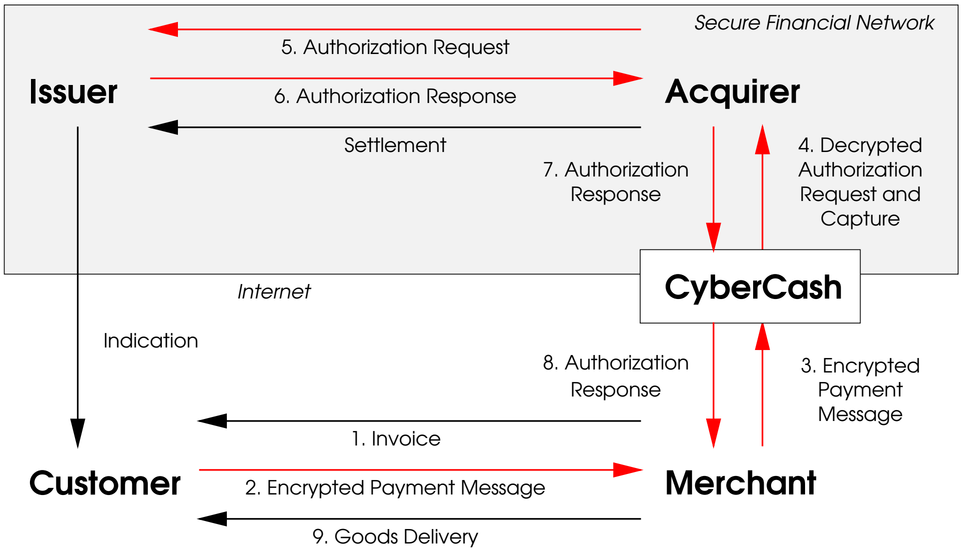

Figure 6: CyberCash Payment Transaction

Picture 6 shows a CyberCash payment transaction. A typical CyberCash transaction is as follows:

- The customer places an order with the merchant and receives an invoice, detailing the purchase agreement and the total charges.
- The customer uses the CyberCash wallet to pay by entering the credit card details. This generates an encrypted payment message which is sent to the merchant together with the original invoice.

- The merchant removes the order details from the message, signs the payment advice and sends it to the CyberCash server. The merchant cannot see the credit card number as the payment message is encrypted and can only be decrypted by CyberCash.
- The CyberCash server removes the transaction from the Internet, decrypts the payment message, reformats it and forwards it to the acquirer.
- The acquirer then forwards the payment message to the issuer who sends approval or denial back to acquirer.
- That response is returned to the CyberCash server.
- CyberCash then forwards the approval or denial message the vendor.

Steps 1,2,3 and 7 take place on the Internet and involve a combination of public key and symmetric key operations. Steps 4 and 6 take place over dedicated lines. Step 5 takes place on secure financial networks. CyberCash claim to complete a payment transaction in 15-20 seconds. Because the CyberCash system makes use of existing secure transaction networks banks like this system very much. Additionally it does not require merchants to establish new bank relationships.

who / what	Merch.	Cust.	Date	Amount	Item
Merchant	-	No	Yes	Yes	Yes
Customer	Partial	-	Yes	Yes	Yes
CyberCash	Yes	No	Yes	No	No
Bank	Yes	Yes	Yes	Yes	No
Observer	No	No	Yes	No	No

Table 26: CyberCash Visibility Profile

Table 26 shows the CyberCash visibility profile. CyberCash is distinguished from the bank (issuer and acquirer taken together) because CyberCash acts as an intermediary in the payment transaction.

Table 27 shows the CyberCash requirements profile. CyberCash transactions are non-anonymous, authenticated and verified online. Towards the merchant the customer uses a pseudonym provided by the CyberCash wallet. The system is not economic for small payments because of the use of credit cards as the grounding financial instrument. Also there is a question mark over its scalability due to the use of central servers at CyberCash to interface between the Internet and the secure financial networks. CyberCash hint at franchising these services to third parties, and in that case the problem will be ameliorated.

The CyberCash system uses credit cards, so it is no economical for small payments. As a result of this, CyberCash Inc. are adding two new payment systems: a cash-like system and a cheque-like system. These will be implemented as extra payment options in the existing CyberCash software wallet. The CyberCoin (see section 4.14) small payments system is already operational. Their someday do be bidirectional PayNow electronic cheque system is currently in trial and right now offers about the same features as the basic CyberCash, but is only available for US citizens with a checking account.

References: [Gmb98], [Cyb96a], [Cyb97b], [Cyb97d], [Cyb97f], [Cyb97c], [EBCY95]

Requirement/System	CyberCash
Token System	No
Transaction	
Atomicity	No
Consistency	Yes
Isolation	No
Durability	Yes
Security	
No Double Spending	n.a.
No Counterfeiting	No
No Overspending	Yes, online authorization
Non-Refutability	No, but merchant authentication
No Unauthorized Use	Yes
Anonymity	Partly, among merchant and, if CyberCash is trusted, among CyberCash.
Untraceability	No
Interoperability	
Divisibility	n.a.
Bidirectionality	No
Respendability	No
Acceptability	Yes
Multicurrency Support	Yes, via the credit card
Scalability	
Scalability	Yes
Off-line Operation	No
Economical Issues	
Operational	Yes
Large User Base	Yes
Buyer Risk	No, credit card company at risk
Seller Risk	No, credit card company at risk
Reliability	Yes
Conservation	Yes
Ease of Use	
Unobstrusiveness	Yes
Low Latency	No, 15-20 seconds per transaction
Micropayments	No
Macropayments	Yes
Low Fixed Costs	No
HW Independence	Yes

Table 27: CyberCash Requirements Profile

4.13 CyberCents

Web Resource	[Cyb97g]
Name	CyberCents
Origin	Outreach Communications.
Payment Model	Direct prepaid merchant account based on an initial secure credit card presentation.
Status & Milestones	Development, 1997
Privacy Control	None. Merchant keeps a customer account.
Security Mechanism	Passphrases, SSL based STOMP Commerce Engine of the same company provides security for the initial credit card data transmission.
Prerequisites	Customer needs credit card, merchant needs account keeping SW.
Fees	?. Presumably they sell their software to the merchants and will charge transaction fees on the credit card transactions.
User Base	They claim to have a customer base of 200.
Limits	Merchants might have to handle lots of customer accounts. Not for casual spending, but for longer customer merchant relationships only.
Remark	Simple. And they claim to be Year 2000 compliant. Very little technical information available.

Table 28: CyberCents Feature Profile

Outreach is a privately held, software and services company with headquarters in Austin, Texas, founded in June 1995. CyberCents 2.0 by Outreach is a Web server micropayment software specially designed to enable secure, automated sales transactions as small as one Cent. It is prepaid customer at merchant account based. The customer does not need any wallet software.

There is no information available if and where the system is actually operational or in trial. Therefore it is put as in development, although this is a guess as well.

Customers buy blocks of CyberCents account credits from their respective merchant in an automated, secure credit card presentation transaction and then spend them for different items over time. Consumers e.g. purchase CyberCents in blocks of 5USD or 10USD. and the merchant gains bank float by this.

Credit card transactions are processed using the Outreach Secure Transaction and Order Management Processor (STOMP) that is based on SSL. Outreach provides this service on their own server for the merchant using the merchant's card processor and bank relationships. Outreach Communications intends the incorporation of SET (see section 4.47) into its products.

4.14 CyberCoin

The CyberCoin system is designed to be an extension to the basic CyberCash (see section 4.12) wallet. CyberCoin is a service designed for what CyberCash

Web Resource	[Inc96]
Name	CyberCoin
Origin	CyberCash Inc.
Status & Milestones	Operational since October 1996.
Payment Size	Small payments. Between 25 Cents and 10USD.
Money Model	Notational.
Payment Model	Direct account based.
Validation	Online.
Privacy Control	Customer uses pseudonyms, CyberCash can read the account information, the merchant cannot. The banks can trace all transactions.
Security Mechanism	RSA and DES encryption, signatures, passphrases.
Prerequisites	CyberCash Wallet software, For non-US citizens, a credit card is necessary, US citizens also can use their bank account.
Risk	Bank.
Fees	Merchants will be charged a transaction fee.
Latency/Costs	?, but presumably high, as several banks and a goods transaction protocol are involved.
User Base	Over 500.000 wallets distributed.
Limits	Only US citizens can bind their bank account to the Wallet software.
Remarks	Only very limited technical information available
Genealogy	A CyberCash (see section 4.12) product.

Table 29: CyberCoin Feature Profile

calls micropayments, meaning from USD 0.25 up to USD 10.00 per transaction. CyberCoins can be withdrawn in multiples of 20USD up to 80USD per month. CyberCoin is not implementing a token system, but a notational one.

Customers can use their existing bank account for CyberCoin transactions. The money is transferred from the customer bank account to the CyberCoin account at CyberCash resp. the CyberCoin supporting bank via financial networks. Currently, CyberCoins are only available in US dollars and only at merchants who have a US bank account. Customers with a credit card can also use this service but they can not move any CyberCoins back to their credit card again the way account using customers are allowed with their accounts.

During the installation of the electronic Wallet customers can register their existing bank account and bind it to their Wallet. Then they can “load” their Wallet, i.e. transfer money from their bank account to their CyberCoin account at the CyberCash supporting bank. The customer does not store any monetary value on its PC. Therefore customers loses no money, if the their PC crashes and they can access their CyberCoin accounts from other PCs as well. Double spending is no issue with CyberCoin also because it is no token system, but a notational one. Equally they do not need to address the making change problem.

During the payment transaction the CyberCoin supporting bank is informed that the customer wants to spend money at a CyberCoin enabled merchant and will moved the amount in question to the account of that merchant. No monetary value leaves financial networks.

who / what	Merch.	Cust.	Date	Amount	Item
Merchant	-	No	Yes	Yes	Yes
Customer	Partial	-	Yes	Yes	Yes
CyberCash	Yes	No	Yes	No	No
Bank	Yes	Yes	Yes	Yes	No
Observer	No	No	Yes	No	No

Table 30: CyberCoin Visibility Profile

Table 30 shows the CyberCoin visibility profile. CyberCash is distinguished from the bank (issuer and acquirer taken together) because the CyberCoin system merely provides a secure notifying interface supported by several banks.

Table 31 shows the CyberCoin requirements profile. The system is not anonymous, and transactions can be traced the same way CyberCash transactions can. For financial information of CyberCoin transactions 768-bit RSA encryption and signatures are used. The CyberCoin protocol contains also some kind of goods transaction security. The Wallet will release CyberCoins to the merchant only after the goods have been received by the customer. Therefore CyberCoin is termed Regulation E compliant which means customers are protected from losing money from errors or fraud in electronic transfers. CyberCoin does not support peer-to-peer transactions.

References: [Cyb97e], [Cyb96b]

4.15 Digital Silk Road

Agorics, Inc. is a software development company specializing in all facets of electronic commerce.

The basic idea is an inter site link level protocol that includes a money field in some packets. This field is not ciphered and is never negative. It is 32 bits long and its value is the worth of the packet. It is denominated in units of one thousandth of a cent or less. As such packets pass over an interface between two sites, X and Y, an up-down accumulator that is conceptually between X and Y tracks the net money flow. The accumulator is probably implemented at both sites. The respective operators of X and Y periodically read the accumulator and pass real money according to the accumulator value, then reset the accumulator. This funds transfer is accomplished by conventional EFT.

4.16 Ecash

Ecash is an anonymous, untraceable, online token payment system by DigiCash. Ecash is purely software based and The customer requires a graphical Wallet software. For merchants there exists a corresponding Wallet that also can be accessed via a command line interface. In fact, Ecash allows for bidirectional payments. There is no distinction between customers and merchants with regards to payments.

Requirement/System	CyberCoin
Token System	No
Transaction	
Atomicity	No
Consistency	Yes
Isolation	No
Durability	Yes
Security	
No Double Spending	n.a.
No Counterfeiting	No
No Overspending	Yes, online authorization
Non-Refutability	No
No Unauthorized Use	Yes
Anonymity	Partly, banks can see every transaction, CyberCash as well.
Untraceability	No
Interoperability	
Divisibility	n.a.
Bidirectionality	No
Respendability	No
Acceptability	Yes
Multicurrency Support	Potentially, via the banks, but not yet implemented
Scalability	
Scalability	Yes
Off-line Operation	No
Economical Issues	
Operational	Yes
Large User Base	?, Potentially
Buyer Risk	No
Seller Risk	No
Reliability	Yes
Conservation	Yes
Ease of Use	
Unobstrusiveness	Yes
Low Latency	No, lots of online interaction required
Micropayments	No, not really, minimum of 25 Cents
Macropayments	No
Low Fixed Costs	No
HW Independence	Yes

Table 31: CyberCoin Requirements Profile

Web Resource	[HT97]
Name	Digital Silk Road
Origin	Norman Hardy and Eric Dean Tribble of Agorics.
Status & Milestones	Proposal, 1997
Payment Model	Link level protocol that includes a money field in some packets.
Payment Size	Nanopayments.
Privacy Control	None.
Security Mechanism	None.
Remark	Suitable for Nanopayments.

Table 32: Digital Silk Road Feature Profile

Web Resource	[Dig97a]
Name	Ecash
Origin	Digicash, D.Chaum, formerly of CWI, cooperations with major banks, German projects with Deutsche Bank AG.
Status & Milestones	Operational since October 1995.
Payment Size	Small payments.
Money Model	Token.
Payment Model	Direct cash like.
Validation	Online.
Privacy Control	Confidential, anonymous, untraceable.
Security Mechanism	RSA and DES encryption, blind signatures, passphrases, online double spending.
Prerequisites	Bank account at one of the issuing banks, Wallet (Unix, Macintosh, Windows).
Risk	Customer at limited risk with the tokens in the Wallet. Merchant at no risk because of online validation and prepaid accounts.
Fees	Set up fee of 11USD, monthly fee of 1USD.
Latency/Costs	Sometimes not too short.
User Base	Over 3.000 at Mark Twain Bank.
Limits	Bank account at one of the issuing banks required.
Remarks	GUI, offline possible, but not recommended, lots of scientific documentation, bidirectional system.
Genealogy	Online version of CAFE (see section 4.7), Double spending detection in the reverse manner of NetCash (see section 4.34).

Table 33: Ecash Feature Profile

Both sides can give and receive payments.

After having installed that software, a connection to the customer's bank is made and the customer can convert some of the money on its account into digital Ecash tokens held in the customer Wallet on the customer PC. With these tokens payments can be tendered to merchants. The bank gains pre-transaction float by this.

The launch of commercial Ecash with several banks involving real money was preceded by a large trial involving trial money. The trial involved about 30,000 customers, about 60 merchants and four banks. Presently there is a second trial running with a new software release which is incompatible to the prior release. In the USA Mark Twain Banks, in Europe the Finnish Eunet Merida Bank and in Australia, Advance Bank are providing an Ecash service with local currency. Mark Twain Banks e.g. charges a set up fee of 11USD and a monthly fee of 1USD as well as transaction fees. The German Deutsche Bank has launched a closed trial service recently.

The Ecash software is available for various platforms e.g. Unix, Macintosh and Windows. A graphical user interface is provided as well as a command line one.

Ecash uses RSA public key cryptography for its transactions. It used blind signatures to authorize the tokens and provide anonymity and untraceability for the customers. Double spending is detected via online reference to the central double spending database that keeps track of all tokens redeemed. The NetCash (see section 4.34) double spending detection has been designed in the reverse manner of this, keeping a list of coined issued and crossing of the redeemed ones. Ecash cannot do this, because of the blind signature scheme to ensure anonymity.

The cash is stored locally, but requires that the customers have an account with a digital bank, from which they then withdraw cash. The system is coin-based, therefore requiring clearing of the coins by the issuing bank.

Ecash is capable of supporting full anonymity for all parties, however the current implementation only provides a customer resp. payer side anonymity. When clearing a transaction the merchant resp. the payee is identified by the bank, but customers may remain anonymous unless they chose to reveal their identity. In addition, like the CAFE (see section 4.7) system, coins can be signed to detect the buyer should they double spend, however this feature is currently not implemented in Ecash.

Picture 7 shows an Ecash payment transaction. The Ecash system works as follows:

1. A customer connects to an Ecash issuer and purchases electronic coins to some value. These coins are generated involving the blind signature schema to make the tokens anonymous. The customer generates the token ids, blinds them, determines their denominations, transmits them to the issuer that blind signs them and returns them to the customer who in turn unblinds them and stores them on its PC in the Wallet.

2. The user can then spend those coins by transmitting them to a merchant over the network.

3. The merchant must on receipt at once present the tokens to the issuing bank

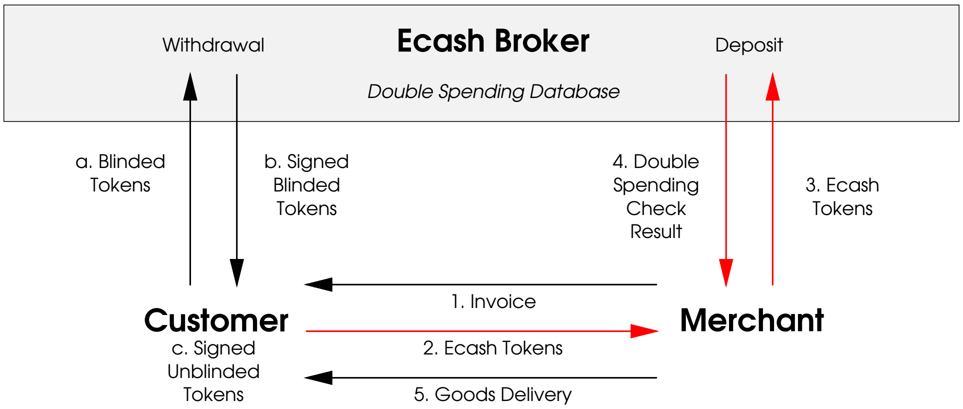

Figure 7: Ecash Payment Transaction

for verification. The issuer consults the double spending database that keeps track of all tokens redeemed.

The generation of token ids by the customer could lead potentially to duplicate token ids by different customers without double spending having occurred, but using a sufficiently long token id this is highly improbable. D. Chaum suggests that using 100 digit ids as token serial numbers should reduce this likelihood to negligible proportions.

who / what	Merch.	Cust.	Date	Amount	Item
Merchant	-	Partial	Yes	Yes	Yes
Customer	Yes	-	Yes	Yes	Yes
Bank	Yes	No	Yes	Yes	No
Observer	Partial	Partial	Yes	No	No

Table 34: Ecash Visibility Profile

Table 34 shows the Ecash visibility profile.

Table 35 shows the Ecash requirements profile. The general lack of atomicity in the basic transaction can be caused by a corrupted transfer between the customer and the merchant. Then it is possible for both or neither parties to believe that they own the token. This also violates isolation and durability. A simple handshake token exchange protocol would help in this situation and restore atomicity, consistency and isolation to the protocol.

References: [Dig97b], [Bar97], [CFN88], [Cha92], [Cha89], [Cha94], [Cha95], [Dig96a], [Dig96c], [Dig96b], [Gol96],

4.17 eVend

Sausage Software subsidiary eVend proposes a hub payment system. eVend is a Java-based electronic commerce system for pay-per-view transactions on information goods. It is based on secure credit card presentation to bring the money into

Requirement/System	CyberCoin
Token System	Yes
Transaction	
Atomicity	No
Consistency	No
Isolation	No
Durability	No
Security	
No Double Spending	Yes, online validation
No Counterfeiting	Yes
No Overspending	n.a.
Non-Refutability	Yes
No Unauthorized Use	Yes
Anonymity	Yes, for the payer.
Untraceability	Yes, for the payer.
Interoperability	
Divisibility	Yes
Bidirectionality	Yes
Respendability	No
Acceptability	Maybe potentially, not yet, as the different Ecash issuers still not interoperate.
Multicurrency Support	No
Scalability	
Scalability	No, central double spending database
Off-line Operation	No
Economical Issues	
Operational	Yes
Large User Base	Yes, in trial, potentially in operational
Buyer Risk	Limited to prepaid amount
Seller Risk	Yes, if not online validation
Reliability	Yes
Conservation	Yes, but tokens have a limited life span and need to be refreshed regularly
Ease of Use	
Unobstrusiveness	Yes
Low Latency	No, but usually acceptable
Micropayments	Yes, but rather low than micro
Macropayments	No
Low Fixed Costs	?
HW Independence	Yes

Table 35: Ecash Requirements Profile

Web Resource	[eVe97]
Name	eVend
Origin	eVend Inc., Sausage Software Ltd.
Payment Model	Indirect push debit account.
Status & Milestones	Operational, 1997.
Privacy Control	None.
Security Mechanism	Passphrase, data encryption (no details available), secure credit card presentation and account details transmission via SSL.
Prerequisites	For the merchant a vendor server and suitably prepared Web pages with Cashlets, i.e. payment processing applets on them. Customers need no special preparation, but a credit card to fill the eVend account.
Fees	50USD for the InfoSeller software, minimum of 20 Cent transaction fee. Above 2USD 30 Cent plus 2.95% of content price transaction fee, monthly account settlement, details "negotiable".
User Base	Claims to have 380 merchants, 19 of them are disclosed.
Limits	Customer accounts 50USD deposit limit.
Remark	Hub system.

Table 36: eVend Feature Profile

the system. Merchants need the InfoSeller software and place so-called Cashlets on their Web pages, Java applets that perform the payment transactions for the customer. Customers do not need no install software themselves. Merchant systems are available for Windows. eVend provides the back end transaction processing system to do the credit card processing.

eVend is a indirect push debit account based system. Customers can use the Cashlets provided by the merchants to open eVend accounts and fill them with money via a secure credit card presentation. eVend gains pre and post transaction float that way, as it also administrates the merchant accounts. Accounts are passphrase protected. Once customers have obtained and filled their account, they can use it to purchase goods from eVend enabled merchants.

A purchase transaction starts with a customer clicking on a Cashlet displayed on a merchant Web page. The customer must authenticate itself to the eVend account via the Cashlet and the price for the ordered goods is deducted from the customer account and added to the merchant account. Their first purchase customers can make with the Cashlet that helped them to set up their account.

4.18 First Virtual

First Virtual was founded in 1994. Since then, more than 2,650 sellers and 180,000 buyers in 166 countries have registered to use First Virtual. InfoHaus is an Internet shopping mall founded by First Virtual, there about 180 sellers are organized. First Virtual offers an Internet payment system that takes advantage of email for message exchange between merchant, First Virtual and customer. First Virtual does not require customers and merchants to have special hardware or software. Email is

Web Resource	[Fir96]
Name	First Virtual
Origin	First Virtual Inc.
Payment Size	Macropayments.
Money Model	Notational.
Payment Model	Credit card payment intermediator
Status & Milestones	Operational since October 1994
Validation	Online.
Privacy Control	Pseudonyms.
Security Mechanism	Outband security. Customer reconfirmation via email for each purchase. VirtualPIN instead of credit card number.
Prerequisites	Credit card.
Risk	Merchant at risk, escalation risk for customer with credit card company.
Fees	USD2 annual fee
Latency/Costs	High.
User Base	Over 2.650 sellers and 180.000 buyers registered.
Limits	n.a.
Remarks	Very simple system.
Genealogy	Both input for and going to be SET (see section 4.47) compliant.

Table 37: First Virtual Feature Profile

sufficient and First Virtual does need no encryption.

Customers require a credit card. When registering with First Virtual customers are accorded a so called VirtualPIN as pseudonym for their credit card details and themselves. The credit card details are transmitted to First Virtual via phone, fax or letter. Annual customer fee is 2USD which also is charged on the credit card. Each First Virtual account has an email address and a real account with a predefined currency associated and a defined state (active, seller-only, suspended, or invalid). Customers are required to supply a credit card account, merchants must have a checking account as well.

After registering customers can purchase at First Virtual accepting merchants using their VirtualPIN. The merchant will notify First Virtual about the intended purchase. The customer gets an email from First Virtual for reconfirmation of the transaction. The customer can respond with "Yes", no or fraud. The answer yes confirms the transaction and the customer credit card is charged by First Virtual, not by the merchant. "No" cancels the purchase. "Fraud" is used when the customer thinks it is asked to confirm a transaction it never initiated. By this the customer's VirtualPIN is assumed to be misused and the VirtualPIN is invalidated. The customer then needs to set up a new one. The default risk limitation for the customer is its credit card company in case of fraudulent confirmation mails.

The system offers anonymity to the buyer towards the merchant by means of pseudonymity, i.e. the merchant sees only the VirtualPIN, but no credit card details of the customer. The First Virtual system is based on the so-called Green Commerce model. This model says that the (minimized) risk of payment defaults is carried by the merchant.

A typical First Virtual transaction is pseudonymous, traceable and online and runs as follows:

1. The customer initiates the purchase by entering their VirtualPIN details in the merchant order form.
2. The merchant emails the customer VirtualPIN, its own VirtualPIN and a suitable description of the purchase to First Virtual.
3. First Virtual automatically sends an email to the customer asking for reconfirmation.
4. The customer replys "Yes" as confirmation to First Virtual.
5. First Virtual uses existing secure financial networks to process the credit card transaction.
6. After successful completion of the card transaction the merchant is sent an authorization number.

who / what	Merch.	Cust.	Date	Amount	Item
Merchant	-	Partial	Yes	Yes	Yes
Customer	Partial	-	Yes	Yes	Yes
First Virtual	Yes	Yes	Yes	Yes	Yes
Bank	Yes	Yes	Yes	Yes	No
Observer	Partial	Partial	Yes	Yes	Yes

Table 38: First Virtual Visibility Profile

Table 38 shows the FirstVirtual visibility profile. The individual customer is relatively anonymous towards the merchant in the transaction because of their VirtualPIN, but the transaction is traceable through the bank account that the VirtualPIN is tied to. The visibility of the customer and merchant to each other and to an observer is partial to the extent that they can see each other's email address and the merchant can see the customer VirtualPIN. An observer can see VirtualPIN and email address of both parties but cannot use this information to link either party to their bank account.

Table 39 shows the First Virtual requirements profile. Because the transactions are linked to the customer credit card, the transaction properties are essentially those of a standard credit card purchase.

References: [RB96], [SSBR96]

4.19 FSTC Electronic Check

The Financial Services Technology Consortium (FSTC) is a large (over 90 members) consortium of banks, financial services providers, national laboratories, universities and government agencies sponsoring and participating in collaborative research and development on technical projects. Their digital cheque project is part of the bank Internet payment system (BIPS, see section 7.1) framework, which is investigating

Requirement/System	First Virtual
Token System	No
Transaction	
Atomicity	No
Consistency	Yes
Isolation	No
Durability	Yes
Security	
No Double Spending	n.a.
No Counterfeiting	Yes, fraud detection via confirmation email.
No Overspending	Yes, online validation
Non-Refutability	No
No Unauthorized Use	Yes, fraud detection via confirmation email.
Anonymity	Yes, for the customer.
Untraceability	No
Interoperability	
Divisibility	n.a.
Bidirectionality	No
Respendability	No
Acceptability	Yes
Multicurrency Support	Yes
Scalability	
Scalability	Yes
Off-line Operation	No
Economical Issues	
Operational	Yes
Large User Base	Yes
Buyer Risk	Limited to credit card risk.
Seller Risk	Yes
Reliability	Yes
Conservation	Yes
Ease of Use	
Unobstrusiveness	No
Low Latency	No
Micropayments	No
Macropayments	Yes
Low Fixed Costs	Yes
HW Independence	Yes

Table 39: First Virtual Requirements Profile

Web Resource	[FST97c]
Name	FSTC Electronic Check
Origin	Financial Services Technology Consortium (FSTC).
Payment Size	Macropayments.
Money Model	Notational.
Payment Model	Direct account based, electronic cheque, different protocol variants.
Status & Milestones	In trial, 1997.
Validation	Online.
Privacy Control	None enforced.
Security Mechanism	Tamper resistant HW, signatures, certificates, certification authorities.
Prerequisites	Electronic cheque book HW, smart card, and appropriate SW.
Risk	Merchant at risk.
Fees	?.
Latency/Costs	High.
User Base	?.
Limits	n.a.

Table 40: FSTC Electronic Check Feature Profile

a general architecture for accessing existing banking facilities over the Internet. The FSTC Electronic Check is modeled to resemble the traditional paper cheque applied to a digital context, trying to replicate the traditional paper check workflow and aiming to be and Regulation E compliant It is initiated digitally, payers use digital signatures for signing and payees do likewise for endorsing. Digital certificates authenticate payer, issuer and bank account.

The FSTC Electronic Check provides a generic model for all electronic, digitally signed and authenticated payment instruments. It can not only represent basic personal cheques but also resemble other financial payment systems, such as charge card slips, travelers checks or certified checks. Primary purpose of FSTC Electronic Checks is to make electronic payments over public networks. Writing a cheque is to be integrated into cash registers and personal financial management software. The familiarity of the customer with the traditional cheque mode and the use of existing, trusted financial institutions as certifying agents are hoped promote fast customer acceptance. But the project also aims at enabling FSTC Electronic Checks to be used in any traditional cheque situation, e.g. banks using cheques to collect deposits from their clients and thus offering home banking facilities. A a later stage also the implementation of POS transactions is targeted at provided there will be a market for this.

The FSTC Electronic Check can be delivered directly or by email. Payments are collected by banks via email and cleared through the existing financial networks, thereby integrating them in a secure manner with the Internet. Tamper resistant signature smartcards or other hardware devices are considered necessary to compute signatures without compromising the private key of the signer. The customer signs the cheque and includes its authenticating certificate signed by the issuing bank which is signed by someone like the Federal Reserve. For this the customer will own a portable electronic cheque book. Such a FSTC Electronic Check book can be seen as the cheque book equivalent of the CAFE (see section 4.7) cash wallet. The cheque book is to store the customer private key and to maintain a log of all cheques issued. Main possibility of for abuse will remain lost or stolen cheque books.

FSTC intends to provide an API for the basic applications:

Write: Generates a cheque, if applicable, binds it to an attached bill and signs it.

Co-sign: Appends a further signature to the cheque.

Verify: Validates the signatures on a cheque and if applicable the binding to an associated bill.

Endorse: Validates signatures on the cheque, appends endorsement and signs the cheque to be deposited or cashed.

Register read: Reads the cheque log in the cheque book.

Register entry: Appends an entry to the cheque log.

The FSTC Electronic Check system wants to be able to support the following scenarios, which somehow emulate the present banking situation in Europe:

Deposit and Clear: The payer receives a bill or invoice from the payee, writes an electronic cheque and sends it to the payee. The payee presents the cheque to the acquirer, which, in turn, will settle it with the issuer.

Cash and Transfer: The payer receives a bill or invoice from the payee, writes an electronic cheque and sends it to the payee. The payee presents it directly to the issuer to be paid to the payee account at the acquirer.

Lockbox: The payer receives a bill or invoice from the payee, writes an electronic cheque and sends it to the acquirer either directly or via a lockbox. The acquirer then notifies the payee and clears the payment with the issuer.

Funds Transfer: The payer receives a bill or invoice from the issuer, writes an electronic cheque and sends it to the issuer. The issuer, in turn, transfers funds to the payee account at the acquirer.

who / what	Merch.	Cust.	Date	Amount	Item
Merchant	-	Yes	Yes	Yes	Yes
Customer	Yes	-	Yes	Yes	Yes
Bank	Yes	Yes	Yes	Yes	No
Observer	?	?	Yes	?	No

Table 41: FSTC Electronic Check Visibility Profile

Table 41 shows the FSTC Electronic Check visibility profile. Mostly these resemble traditional cheque transactions. However, the FSTC protocol does not enforce encryption of the cheque, it merely requires digital signatures for authentication purposes. It is not quite clear how much of the transaction information in the cheque is encrypted, if any. Without encryption FSTC transactions would be visible to a digital observer. The FSTC documentation however says that electronic cheques might be encrypted when sent over the Internet.

Requirement/System	FSTC Electronic Check
Token System	No
Transaction	
Atomicity	Yes
Consistency	Yes
Isolation	No
Durability	Yes
Security	
No Double Spending	n.a.
No Counterfeiting	Yes, digital signatures and tamper resistant HW
No Overspending	No (?)
Non-Refutability	Yes
No Unauthorized Use	Yes, if electronic cheque book not lost or stolen
Anonymity	No.
Untraceability	No
Interoperability	
Divisibility	n.a.
Bidirectionality	Yes, potentially
Respendability	No
Acceptability	Yes, potentially
Multicurrency Support	Yes, via the banks
Scalability	
Scalability	Yes
Off-line Operation	No, if security for payee required
Economical Issues	
Operational	No, trial only
Large User Base	n.a., put potentially yes
Buyer Risk	No
Seller Risk	Yes
Reliability	Yes
Conservation	Yes
Ease of Use	
Unobstrusiveness	No
Low Latency	No
Micropayments	No, unlikely, although they claim to be, but without defining exact amounts.
Macropayments	Yes
Low Fixed Costs	?, depending on bank policy
HW Independence	No, electronic cheque book is HW

Table 42: FSTC Electronic Check Requirements Profile

Table 42 shows the FSTC Electronic Check requirements profile. It shows the transaction properties expected for an electronic cheque mostly resembling those of a paper cheque.

References: [FST97b], [FST97b], [FST97a]

4.20 Geldkarte

Web Resource	[Gie97]
Name	Geldkarte im Internet
Origin	Giesecke & Devrient
Status & Milestones	First trial scheduled for Q1 1998
Payment Size	Small payments.
Money Model	Token (involving counters).
Payment Model	Direct cash like, shadow accounts.
Validation	Offline.
Privacy Control	None, if required, use of SSL is recommended. If a Geldkarte is linked to a bank account, it can be linked to a customer. The system is non-anonymous and traceable. A version of Geldkarte, that is not linked to a customer account is being planed.
Security Mechanism	Tamper resistant HW, signatures, certificates, shadow accounts.
Prerequisites	Geldkarte reader resp. merchant terminal HW and corresponding SW.
Risk	Both customer and merchant carry risk of loss.
Fees	0.3% per transaction, at least 2 DPF.
Latency/Costs	Low.
User Base	n.a.
Limits	Amount, that is loaded on the Geldkarte.
Remarks	Interoperability.
Genealogy	?.

Table 43: Geldkarte Feature Profile

A proposal to use the Geldkarte in Internet is from Giesecke & Devrient. It involves tamper resistant hardware and smart cards. The Geldkarte can already be used on Eurocheque (ec) cards having a Geldkarte chip for POS transactions at some merchants. It involves real money in the currency of the issuing bank. The ZKA (Zentraler Kredit Ausschuss, an independent central bank control institution) still has to certify the Geldkarte in Internet proposal before a trial involving real money can start. The protocol of the Geldkarte in Internet is basically the same as that of the ec card with chip, supplemented by a suitable handling of timeouts. The protocol is open for public review. All hard- and software used in Geldkarte transactions needs to be certified by the ZKA to be fully protocol compliant prior to being used operationally. A customer needs Windows 95 or NT as platform, a merchant requires Windows NT. First trials will start in Q1 1998, extended trials with an extended infrastructure are currently planed for Q3 1998.

Picture 8 shows the conventional Geldkarte scenario. The Geldkarte contains a counter from which is deducted at each payment. A Geldkarte can not be locked

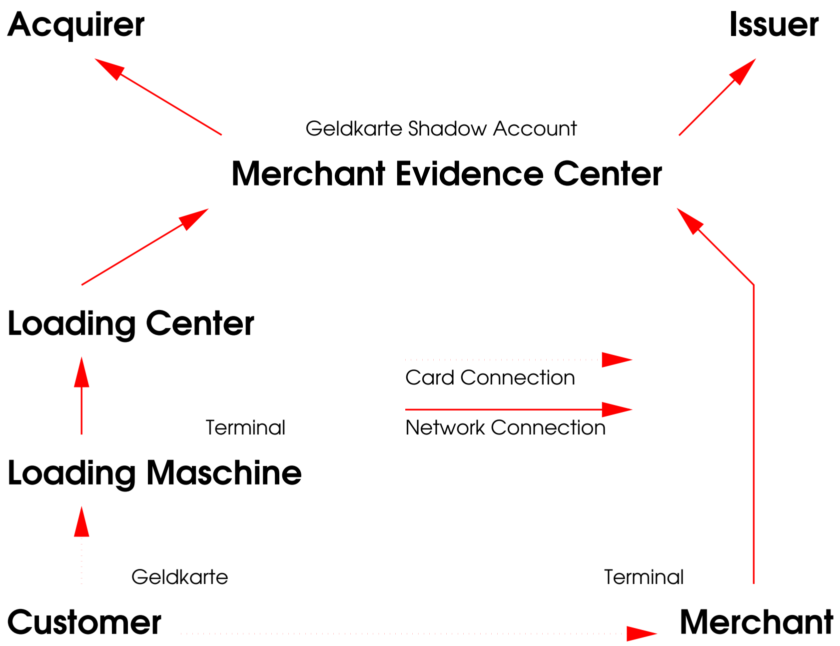

Figure 8: Conventional Geldkarte Scenario

if lost and is not passphrase protected. A customer needs a Geldkarte which is identified by its number. A merchant needs a Geldkarte merchant terminal. Each Geldkarte has its own shadow account at a clearing center. Each bank consortium has its own clearing center, but the system is interoperable, i.e. a merchant terminal can contact any of these clearing centers. The merchant collects Geldkarte payments offline during the day and submits them in a batch to the various clearing centers at the end of a business day. The merchant carries the potential risk if a customer uses a compromised card. Reimbursed payments are deducted from the Geldkarte shadow account. So a compromised Geldkarte is at least detected fairly soon. The banks take a commission of 0.3% of each payment transaction, but at least 2 DPF. That means, the Geldkarte is suitable for small payments, but not for micropayments.

In POS transaction the customer must insert its Geldkarte into this merchant terminal. In Internet transaction the customer will insert the Geldkarte into its PC Geldkarte reader and with the support of some local software the card will set up a connection with the remote merchant Geldkarte terminal. Customer card and merchant terminal (merchant "card") mutually authenticate themselves by exchanging certificates. A secure communication channel provided by SSL is recommended. The Geldkarte infrastructure also involved a certification infrastructure. The Geldkarte signs each payment.

Picture 9 shows a Geldkarte payment transaction. A typical Geldkarte payment transaction is as follows:

1. The customer obtains a Geldkarte. The Geldkarte has an id and contains a bank certificate. For the Geldkarte there is a shadow account at the clearing center. The customer loads the Geldkarte via the Internet or at a ATM terminal. The bank gains pre- and post transaction float.
2. The customer selects a merchant offer and places an order for it.

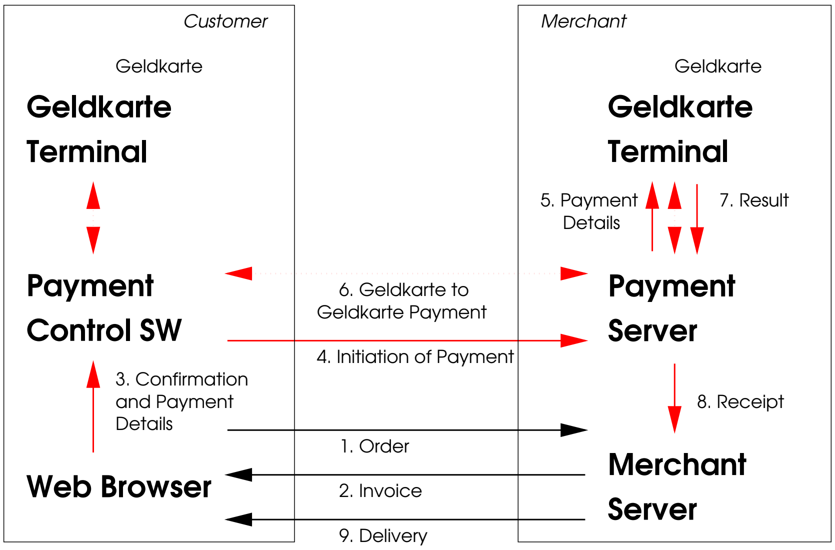

Figure 9: Geldkarte on Internet Payment Transaction

3. The merchant sends an invoice to the customer.
4. The customer confirms the invoice and authorizes its payment control software to perform the payment.
5. The Geldkarte payment control software initiates the payment transaction. The merchant payment server software cooperates with the customer payment control software to connect Geldkarte and merchant terminal, which authenticate each other and then conduct the payment transaction. The Geldkarte signs each payment.
6. The merchant terminal hands over a receipt to the merchant payment server software which in turn hands it to the merchant who gives it to the customer together with the goods requested.
7. At the end of each day the merchant terminal submits the payments of the day to the appropriate clearing centers for reimbursement.

How the integrity of the customer payment control and merchant payment server software is to be authenticated still is an open problem. Many producers can provide Geldkarte readers for customers. The merchant terminal and software as well as the customer software is provided by Giesecke and Devrient. They claim that first unofficial Internet trials have shown the system working. The system is not bidirectional, just very limited merchant stornos are possible.

who / what	Merch.	Cust.	Date	Amount	Item
Merchant	-	Partial	Yes	Yes	Yes
Customer	Yes	-	Yes	Yes	Yes
Bank	Yes	Yes	Yes	Yes	No
Observer	Yes	Partial	Yes	Yes	Yes

Table 44: Geldkarte Visibility Profile

Table 44 shows the Geldkarte visibility profile. The customer is only visible to the merchant by its Geldkarte id. The bank can trace the Geldkarte id to a personal account.

Table 45 shows the requirements profile of the Geldkarte. Geldkarte provides a small payment system, that not only can be used in the Internet but also in everyday POS small change transactions. The risk of compromised cards is limited by the use of shadow accounts. The system has a potential of being accepted by the banks for the use of real money.

References: [Die97], [Die98]

4.21 Globe ID

The GlobeID payment prototype by GCTech is operated by the French Bank of Mars and enables consumers to test secured and certified purchases from merchants over the Internet without involving real money. The GlobeID payment software is running on KLELine web site. Kleline is a trusted intermediary operating the GlobeID payment services in nine European countries (Belgium, France, Germany, Italy, Luxembourg, Portugal, Spain, Switzerland and the United Kingdom).

Customers need a GlobeID wallet called WIM (Wallet Interface Module). This Wallet contains the payment systems like cash, credit cards or frequent flyer cards. Both consumers and merchants need to be registered with a suitable bank that offers both GlobeId and traditional banking services.

The GlobeID Wallet Servicing Center enables the customer to carry out home banking and payment transactions with its GlobeID and Wallet. These operations are the same which are offered by a bank to its customers: Create an account, close an account, refill the wallet, change the pin, etc.

4.22 iKP

The IBM proposed architecture and protocols for secure payments over networks, Internet Keyed Payment Protocols (iKP) implements encrypted secure credit card based transactions. iKP is a family of secure credit card payment protocols, i denoting the number of public key owners involved. iKP was designed to overcome US export restriction problems and to be browser and server transparent. The protocol is disclosed for public review.

The iKP proposal is by now obsolete and superseded by SET (see section 4.47), but many details of iKP influenced SET and IBM was a major contributor to the SET specification. Also Europay (see section 4.47) has used iKP as foundation of its smart card based electronic commerce protocol, but is going fro SET now.

iKP was intended to be an open protocol avoiding problems raised by proprietary solutions. It also uses strong cryptography techniques without violating current US export rules. An initial prototype was aimed at credit cards, but claims to be

Requirement/System	Geldkarte
Token System	Yes
Transaction	
Atomicity	Yes
Consistency	Yes
Isolation	Yes, if HW is not broken
Durability	Yes
Security	
No Double Spending	n.a., counter system
No Counterfeiting	Yes
No Overspending	Yes, if HW not broken
Non-Refutability	Yes
No Unauthorized Use	No, whoever has the Geldkarte, can use the money that has been loaded on it.
Anonymity	No, but merchant only sees the Geldkarte id.
Untraceability	No
Interoperability	
Divisibility	n.a.
Bidirectionality	No
Respendability	No
Acceptability	Yes
Multicurrency Support	Yes
Scalability	
Scalability	Yes
Off-line Operation	Yes
Economical Issues	
Operational	No, but pilot trial about to start
Large User Base	Yes, potentially
Buyer Risk	Yes, goods might not be delivered
Seller Risk	Yes, customer might use broken HW
Reliability	Yes
Conservation	Yes
Ease of Use	
Unobstrusiveness	Yes, potentially
Low Latency	Yes
Micropayments	Limited, small payments only due to the minimum bank commission of 2 DPF.
Macropayments	No
Low Fixed Costs	Yes, potentially
HW Independence	No

Table 45: Geldkarte Requirements Profile

Web Resource	[Glo97] [Kle97] [GCT97]
Payment Model	Home banking
Status & Milestones	Working prototype, October 1997
Prerequisites	Wallet Interface Module

Table 46: Globe ID Feature Profile

Web Resource	[iKP97]
Name	iKP (1KP, 2KP, 3KP)
Payment Model	Secure credit card presentation.
Status & Milestones	Proposal, spring 1996
Privacy Control	Depends on the parameters; at best no real anonymity towards the banks
Security Mechanism	RSA encryption, signatures
Prerequisites	ikP SW, Credit Card
Remarks	Browser- and server-transparent; no use of restricted cryptography software; protocol is disclosed for public review

Table 47: iKP Feature Profile

extendible to any payment system. The Internet allows customers to place orders while existing secure financial networks serve to execute the actual payment.

Reference: [BGW+95]

4.23 InterCoin

Web Resource	[Int97]
Name	InterCoin
Status & Milestones	Trial, 1997.
Money Model	Notational.
Payment Model	Direct account based (presumably).
Privacy Control	InterCoin kept customer data confidential, merchants see account pseudonym only.
Security Mechanism	Passphrase, SSL.
Fees	10USD registration fee.
Remarks	First get goods, pay later.

Table 48: InterCoin Feature Profile

InterCoin wants to provide a customer friendly service. Customers need to have an InterCoin account.

InterCoin enabled kind of shareware purchases over the Internet. Customers can use the goods first and pay later when they are satisfied with them. The goods will be billed at the end of the month.

4.24 LotteryTickets

LotteryTickets is a proposal by Rivest for a probabilistic payment system. Not every payment is associated with monetary value, but just those involving winning tokens. Justice is reached by the law of large numbers and tiny values.

Merchants can compute if a token is a winning token and the need to collect and

Web Resource	[Riv97]
Name	LotteryTickets
Origin	R.Rivest, MIT Computer Lab.
Status & Milestones	Proposal, 1997.
Money Model	Notational.
Payment Model	Direct account based, probabilistic cheques.
Privacy Control	Basically none, but use of pseudonyms possible, only a few transactions are reported to the bank.
Security Mechanism	Not every payment is associates with monetary value, but just those of winning tokens, law of big numbers.
Genealogy	Similar to TUB (see section 4.49).

Table 49: LotteryTickets Feature Profile

reimburse just these. Customers do not know which tokens are winning tokens. LotteryTickets is a very efficient protocol in terms of highly frequent micropayments, it works offline, is validated locally and has low storage requirements. LotteryTickets is not an anonymous scheme, but pseudonyms could be used and only very few of the transactions are brought to the notice of a bank.

A LotteryTicket with a 10 USD price and a 1/1000 chance of winning has an expected value of 1 cent. If a customer wants to pay a merchant one cent, it must tender one of these LotteryTickets. A LotteryTicket contains a ticket number and a winning number indicator. This indicator can be a hash of a winning number that was defined by the merchant before the LotteryTicket generation and whose hash was given to the issuer to include in each LotteryTicket of that series. This way the merchant can detect the winning tickets easily, but the issuer does not know the winning number.

The chance of a ticket being a winning ticket must be clear to allow determining the expected ticket value. The merchant has to bear the risk, that the issuer could be insolvent, but bad issuers get weeded out with time. Customers could be certified by the issuer to create their own LotteryTicket series.

4.25 MagicMoney

Magic Money is a digital cash system designed to be used via electronic mail. The system is online and untraceable. Each transaction involves an exchange with a central broker to prevent double spending. It is impossible for any involved party or observer to trace transactions, or to match a withdrawal with a deposit, or to match two tokens to a customer in any way. Magic Money is a kind of public domain implementation of Digicash Ecash (see section 4.16) for email (MagicMoney.tar.Z).

The system consists of two modules, Server and Client. Magic Money uses PGP for all communications between Server and Client and all messages are encrypted. Messages from Server to Client are signed as well. Untraceability is provided by a blind signatures.

Magic Money uses fixed value tokens, the denominations of which are chosen by the

Web Resource	[Mag97]
Name	Magic Money
Origin	Product Cypher.
Payment Model	Direct cash like.
Status & Milestones	Public domain implementation, 1997.
Privacy Control	Anonymous (kind of), untraceable, confidential.
Security Mechanism	PGP, blind signatures.
Prerequisites	Server, Client, email, PGP.
User Base	?
Remarks	For email.
Genealogy	Derived from Digicash Ecash (see section 4.16). Simulates respendability like NetCash (see section 4.34).

Table 50: MagicMoney Feature Profile

Server operator. Tokens are signed with a different pair of keys for each denomination. The Server accepts old Tokens, blind signs new tokens, and lists reimbursed tokens on the double spending list.

The Server does not store any tokens, but all tokens are stored by the Client module. Received tokens are immediately reimbursed at the server and exchanged into matching fresh tokens that are stored in the payee Client. This simulates respendability for the user the same way is with NetCash (see section 4.34).

4.26 MicroMint

Web Resource	[RS95]
Payment Model	Direct cash like.
Status & Milestones	Proposal, 1996.
Security Mechanism	Public key, hash collisions.
Remarks	Very high initial and setup costs.

Table 51: MicroMint Feature Profile

MicroMint is a proposal by Rivest and Shamir about coins that can only efficiently be produced in very large quantities and are hard to produce in small quantities. The validity of a coin is easily checked. MicroMint is optimized for unrelated low-value payments. It uses no public key operations at all. However the scheme is very complex and would require a lot of initial and operational effort. Therefore it is unlikely that it ever will gain any practical importance.

A broker will issue new coins at the beginning of a period and revoke those of the prior period. Coins consist of multiple hash collisions, i.e. different values that all hash to the same value. The broker mints coins by computing such hash collisions. For that process many computations are required, but more and more hash collisions are detected with continued computation. The broker sells these MicroMint coins in batches to customers. Unused coins can be returned to the broker at the end of a period, e.g. a month.

Customers render MicroMint coins as payment to merchants. Merchants can check the validity of a coin easily by applying the hash function to each coin and verifying that they all has to the same value. Merchants redeem their coins at the end of each day and the coins are checked by the broker against the double spending database. In case of double spending all but one randomly selected merchant lose. The broker takes a redemption fee from the merchant.

MicroMint offers little motivation to cheat in a small scale way because of the small sums involved and bad credit and removal of offending users after the fact is considered sufficiently. MicroMint however does not offer any protection against pure malicious framing. Personalizing coins for customers by the broker and for merchants by the customer can reduce that risk.

Large scale forgers that would attempt to produce coins in bulk like the broker are faced with great difficulties. The broker uses a running period to produce the coins for the next period which takes a lot of computing power and requires even specialized hardware. At the beginning of the new period the broker publishes the hash function and sells the coins. A forger only then could start to forge coins which requires much time and computing power. Several other techniques are proposed to hinder would be forgers.

4.27 MilliCent

Web Resource	[Mil97]
Name	MilliCent
Origin	M. Maneasse, S. Glassman of Digital Equipment.
Status & Milestones	Public Trial since December 1997.
Payment Size	Micropayments.
Money Model	Token.
Payment Model	Direct cash-like, local money, customer accounts at the broker.
Validation	Semi-online, transactions involve customer and vendor only, but some preparations involve broker as well.
Privacy Control	Scalable, from unconfidential to confidential, not anonymous, traceable.
Security Mechanism	Passphrase, hashes, general lightweight security.
Prerequisites	MilliCent Wallet or Vendor Server, which act as proxies between the customer browser and the merchant Web server.
Risk	Customer.
Fees	?
Latency/Costs	Low.
User Base	?
Limits	?
Genealogy	Influenced MPTP (see section 4.30).

Table 52: MilliCent Feature Profile

MilliCent is a proprietary voucher based digital microcommerce system from Digital Equipment. It aims at the micropayment segment of electronic commerce and supports transactions with values oh fractions of a cent. MilliCent considers that coins are treated differently than paper money, where also small denomination notes are treated differently than high denomination notes. As MilliCent represents very small coins, it uses lightweight security measures. A public trial of the MilliCent system involving toy money started in December 1997.

The system uses merchant specific vouchers, the so called scrip, a form of token that is only valid with a particular merchant for a limited period of time. Brokers act as intermediaries between merchant and customers. The fact that any type of scrip is only valid at a particular merchant means the merchant does not need to connect to a central issuer to validate the token. This reduces network traffic and the validation cost. To avoid customers having to maintain separate accounts with the individual merchants for mostly short term relationships, brokers act as intermediaries. The longterm relationships are between brokers and customers, and brokers and merchants

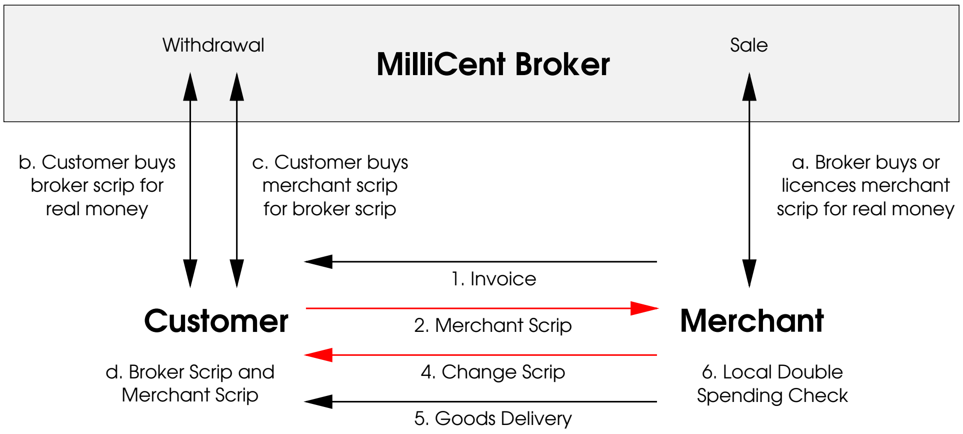

Figure 10: MilliCent Payment Transaction

Picture 10 shows a MilliCent payment transaction. The basic sequence of interactions is as follows:

1. The customer obtains a quantity of broker script at the outset.
2. The customer requests some specific vendor scrip, which they pay for with broker scrip.
3. The broker obtains the required vendor scrip from the vendor.
4. The broker sells the vendor scrip to the customer.
5. The customer buys the services with the vendor scrip.
6. The vendor gives change in vendor scrip.

Steps 1 to 4 are not required for every transaction, the customer can buy sufficient scrip from the broker for a period of time. Likewise the broker can store enough vendor scrip to serve many customer requests or it can have a license from the vendor to create that vendor scrip directly. Although at first glance a a lot of message passing seems to be required, there is no bottleneck like one single currency issuer to be contacted during each transaction, especially once steps 1 to 4 are completed. Experiments at Digital indicated that MilliCent is efficient enough for transactions as low as 1/10 of a Cent.

Besides the reduction of messages another side of the economic MilliCent protocol is the use of lightweight encryption. Aim of MilliCent is to make the cost of breaking the protocol greater than the value of the scrip itself. Scrip is minted very low value. MilliCent offers three protocol versions. Private and secure, secure without encryption and script in the clear. Basically, the system depends on shared secrets and one way hash functions. Secure without encryption means, the customer and the vendor share the customer secret, it is appended to a purchase request from the customer to the vendor and hashed. The hash value (signature) and the request are sent to the vendor who recomputes the signature from the transaction request and its copy of the customer secret. If the two signatures match the request is valid.

who / what	Merch.	Cust.	Date	Amount	Item
Merchant	-	Partial	Yes	Yes	Yes
Customer	Partial	-	Yes	Yes	Yes
Broker	Yes	Yes	No	No	No
Observer	Partial	Partial	Yes	?	No

Table 53: MilliCent Visibility Profile

Table 53 shows the MilliCent visibility profile. There are three distinct MilliCent protocol versions, each offering a different level of visibility. The least private form is scrip in the clear. Here scrip is transferred between customer and vendor without any encryption or protection. This would allow observers to copy the change scrip and spend it themselves. Although amounts stolen that way would be very small, it would be very annoying for the legitimate customers to discover their small change invalid. But it is relatively inexpensive to improve the system, either with full encryption, or with secure hashing.

The seller needs no knowledge of the buyer besides the minimal account information for the scrip. However MilliCent does include a field in the scrip to carry customer information, e.g. age, residence information for taxation purposes or any information required for discounts, such as student status. Unless this field is encrypted an observer can see this information. If an observer can see any other aspects of the transaction depends on whether the MilliCent protocol version is secure without encryption. Then the transaction details including the customer id (which does not give access to the customer identity outside of the scrip system) of are observer readable, but can not be replayed. If the MilliCent protocol version is private and secure, then the observer can gain no information.

Table 54 shows the MilliCent requirements profile. Atomicity, consistency and durability are not directly supported by the MilliCent protocol. Yet the amounts at risk in any transaction are sufficiently small as not to present a major drawback. Although each vendor has its own proprietary scrip (vouchers), interoperability of the system is granted on two levels. On the one hand many vendors use the same broker, so there is broker-local vendor interoperability. On the other hand there is a cooperation between the different brokers to make scrip brokered locally available to a broader customer base. The conservation property is questionable, as vendors issue their own scrip and are free to reinterpret its purchasing power at will.

MilliCent transactions are not anonymous and mostly offline. The customer is not anonymous and account details are kept by the broker. The system is offline as no connection to a central server is required at every transaction.

Requirement/System	MilliCent
Token System	Yes
Transaction	
Atomicity	?
Consistency	?
Isolation	Yes
Durability	?
Security	
No Double Spending	Yes
No Counterfeiting	Yes
No Overspending	n.a.
Non-Refutability	Yes
No Unauthorized Use	Yes (?), wallet lockable
Anonymity	No, but no authentication.
Untraceability	No
Interoperability	
Divisibility	No, but change given.
Bidirectionality	No
Respendability	No
Acceptability	n.a., local money
Multicurrency Support	Yes, possible via the broker
Scalability	
Scalability	Yes
Off-line Operation	Yes, partly
Economical Issues	
Operational	No, trial only
Large User Base	n.a., put potentially yes
Buyer Risk	No
Seller Risk	Yes
Reliability	Yes
Conservation	Questionable
Ease of Use	
Unobstrusiveness	Yes
Low Latency	Yes
Micropayments	Yes
Macropayments	No
Low Fixed Costs	Yes, potentially
HW Independence	Yes

Table 54: MilliCent Requirements Profile

References: [Cen96], [Cen97], [Man95], [GMA$^+$95]

4.28 Mini-Pay

Web Resource	[MP97]
Name	Mini-Pay
Origin	A. Herzberg,IBM, Haifa.
Status & Milestones	Closed trial, 1998
Payment Size	Micropayments.
Money Model	Notational.
Payment Model	Direct account based, merchant aggregation.
Validation	Semi-online, bank is only contacted, if spending limits are exceeded or at random intervals.
Privacy Control	None, if required, use of SSL recommended, non-anonymous, all payments are signed, traceable.
Security Mechanism	Signatures, certificates, hashes, spending limits.
Prerequisites	Mini-Pay merchant and customer software.
Risk	Both customer and merchant carry risk of loss.
Fees	Idea to bill 1% or .01 cent per transaction on redemption.
Latency/Costs	Low, little communication and cryptographic overhead.
User Base	n.a.
Limits	Self defined limits to avoid overspending, total of about 25 to 50 USD spending per customer per day.
Remarks	Solution with short delay; interoperability.
Genealogy	Basic idea somewhat similar to Agora (see section 4.2).

Table 55: Mini-Pay Feature Profile

Mini-Pay from IBM Haifa is a micropayment solution ('pay cent per click'). They want to provide an open standard and low-cost toolkits for vendors. The system is about to start a semipublic trial.

Mini-Pay aims at reducing the costs of the payment system in various ways. Refunds being a merchant policy, making all sales final, payee-side aggregation, prepaid accounts, automated record keeping, interoparating billing systems, being open to competition, offline payments, few computations, pre-distribution of public keys, one or no public key operations per purchase, almost no extra messages and support to include the Mini-Pay system into an existing Web site. For the latter issue Mini-Pay has developed a compiler tool, that transforms certain Html links into MiniPay links that are billable.

Basic idea of this protocol is that issuer and acquirer are the respective internet service providers of customer and merchant, so issuer and acquirer are online if their customers are online. Each customer gets authenticated and assigned a spending limit per merchant each day by its ISP. Merchants accept payment promises from authenticated customers offline and only verify them online if the exceed their spending limits or at random intervals.

The Mini-Pay parties are:

Customer: runs the Mini-Pay Wallet.

Merchant: online content or service provider.

Issuer: Typically an IAP (Internet Access Provider). The issuer charges only the customer.

Acquirer: Typically an ISP (Internet Service Provider) or a bank. In the basic Mini-Pay prototype issuer and acquirer are represented by a single broker. The acquirer charges only the merchant.

Clearing: An exchange connecting the issuer and the acquirer, e.g. one or more banks.

MiniPay uses and extends the existing account and billing relationship between the IAP (issuer) and the customers and between the merchant and its ISP (acquirer).

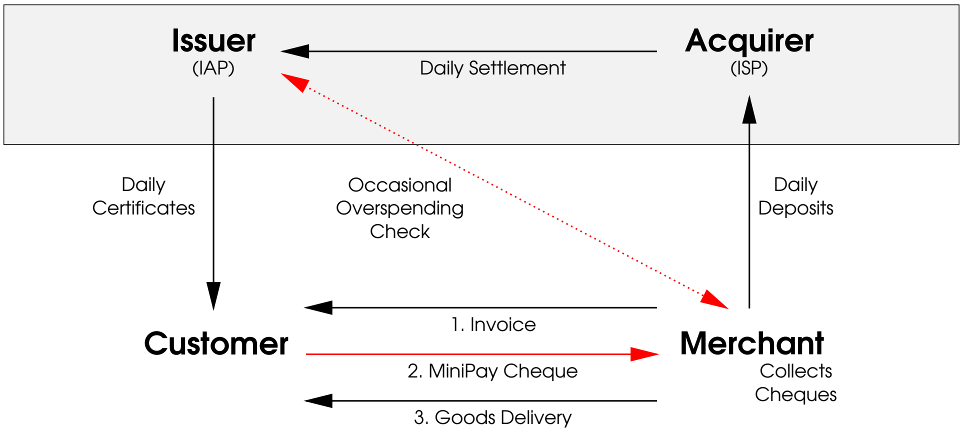

Figure 11: Mini-Pay Payment Transaction

Picture 11 shows a Mini-Pay payment transaction. A typical Mini-Pay transaction runs as follows:

- The customer receives a daily spending and authentication certificate from the issuer each morning at login time.
- A customer clicks on a designated Mini-Pay link at the merchant Web site. A Mini-Pay payment order is generated and signed and piggybacked on the normal GetURL message. This payment order includes the current customer certificated from the issuer.
- The merchant verifies the certificate, extracts the public key of the customer, verifies the signature and checks the recommended offline spending limit indicated in the certificate.
- If the daily limit is not exceeded, the merchant immediately returns the requested information and stores the payment order offline.
- If the daily limit is exceeded, the merchant contacts the issuer to reconfirm the payment order. The issuer can confirm or deny the request.

- At the end of the day the merchant sends the aggregated payment orders to the acquirer for clearing. The acquirer aggregates the payments of its merchants and submits them to the issuer for clearing. The clearing process allows for additional billing servers between acquirer and the issuer to act as exchanges.
- Each day at login time the customer contacts its issuer and they also sign the balance and sum of purchases to each other, so they can delete some of their records.

All of these operations are performed automatically by the Mini-Pay modules at each of the parties. The Mini-Pay protocol supports a routing protocol, which allows exchanges to distribute the identities of the issuers and acquires they are connected to, and the fees involved. The routing protocol is supposed to ensure an efficient and competitive market.

who / what	Merch.	Cust.	Date	Amount	Item
Merchant	-	Yes	Yes	Yes	Yes
Customer	Yes	-	Yes	Yes	Yes
Bank	Yes	Yes	Yes	Yes	No
Observer	Yes	Yes	Yes	Yes	Yes

Table 56: Mini-Pay Visibility Profile

Table 56 shows the Mini-Pay visibility profile. Mini-Pay is not anonymous and operates offline, but issuer and acquirer get full information when the merchant reimburses the payment orders. Privacy is not guaranteed, SSL is proposed if privacy is demanded.

Table 57 shows the requirements profile of Mini-Pay. Mini-Pay provides low cost and latency, scalability, multiple currency support, and security including non-repudiation, overspending prevention, and protection against denial of service. Customers and merchants are forced to take certain risks for efficiency reasons. No receipts or signed offers are given. The buyer is not prevented from redistributing the content bought.

Reference: [HY97]

4.29 Mondex

Mondex provides electronic cash on a smart card and its aims are partly similar to CAFE (see section 4.7), but the Mondex project is at a much further stage of development. Several field tests have been performed in UK and other countries using Mondex as an everyday payment system in POS transactions. Recently, MasterCard has acquired 51% of Mondex. Mondex is a non-anonymous online token system. Very little concrete technical information is available about the Mondex protocol. The system uses special purpose hardware smartcards to grand cryptographic security.

Plans exist to use Mondex over the Internet in scenarios where simply a Mondex compatible card reader is attached to the customer computer. When a transaction

Requirement/System	Mini-Pay
Token System	No
Transaction	
Atomicity	No
Consistency	Yes
Isolation	No
Durability	Yes
Security	
No Double Spending	n.a.
No Counterfeiting	Yes
No Overspending	No, limited overspending can occur
Non-Refutability	Yes
No Unauthorized Use	Yes
Anonymity	No
Untraceability	No
Interoperability	
Divisibility	n.a.
Bidirectionality	No
Respendability	No
Acceptability	Yes
Multicurrency Support	Yes
Scalability	
Scalability	Yes
Off-line Operation	Yes, most of the time
Economical Issues	
Operational	No, but pilot trial about to start
Large User Base	Yes, potentially
Buyer Risk	Yes, goods might not be delivered
Seller Risk	Yes, customer might overspend
Reliability	Yes
Conservation	Yes
Ease of Use	
Unobstrusiveness	Yes, automated handling of payments
Low Latency	Yes
Micropayments	Yes
Macropayments	No
Low Fixed Costs	Yes, potentially
HW Independence	Yes

Table 57: Mini-Pay Requirements Profile

Web Resource	[Mon96]
Name	Mondex
Origin	Mondex, MasterCard, UK based.
Status & Milestones	Closed Trial since July 1995.
Payment Size	Micropayments.
Money Model	Token.
Payment Model	Direct cash-like, smart card.
Validation	Offline.
Privacy Control	None (?).
Security Mechanism	Smart cards, signatures, passphrases, almost no concrete information available.
Prerequisites	Mondex card and lots of other HW.
Risk	Customer.
Fees	No charges for the pilot projects.
Latency/Costs	Low.
User Base	48000 customers.
Limits	Closed, propriatary system. Maximum of 500 GBP per transaction.
Remark	Very little technical information available.
Genealogy	Some aims similar to CAFE (see section 4.7).

Table 58: Mondex Feature Profile

needs to be processed the computer and the card communicate via the card interface. This way the Mondex system can be used both for POS transactions and in the Internet.

To use the Mondex system customers need a Mondex smart card that stores digital money and can handle up to five different currencies. With Mondex customers can pay at merchants equipped with a Mondex retailer terminal, which is used to transfer money from the customer Mondex card to the merchant Mondex card.

The Mondex system uses the following hardware:

- Mondex smart card
- Mondex retailer terminal used to transfer funds from the customer card to the merchant terminal.
- Mondex wallet, a pocket sized unit to store higher amounts of digital money than the card does. The wallet allows private persons, to transfer between their cards.
- Mondex balance reader, a small device to check the current balance on the Mondex Card. This item was demanded by pilot users.
- Mondex hotline used to access the bank account to transfer money to the card, to check the balance and to transfer money to other cardholders.
- Mondex ATM (Automated Teller Machines) used to recharge cards or] to transfer money back into the account, etc.

Basically customers do not need any other hardware than the card itself, but pilot projects have shown that customers want at least to read the balance of their card at any time.

Basically no authentication is required, but it is possible to lock the Mondex card with a passphrase. The limit per transaction currently is 500 GBP. The Mondex card logs all transactions. It stores a unique 16-digit customer id registered at the bank where the personal information about the customer is stored. So lost Mondex cards can be returned to their owners. The Mondex card generates a digital signature that is recognized by the other transaction party, so two Mondex cards can authenticate each other. Monetary value can only be transfered from one proprietary Mondex card to another resp. a Mondex compatible terminal or stored on Mondex devices. It is assumed, that fraud would be uneconomical, as it would involve hardware duplication. To further this, Mondex intents to change the complex chip security on a frequent but irregular basis to minimize the risk of such attacks. Mondex plans to use so called transaction sampling to identify fraud and illegal use of Mondex cards quickly.

Mondex is not anonymous, the banks can trace all transactions and build customer profiles. However due to the lack of technical specification available for public review it is not possible to generate a useful visibility profile for Mondex.

Table 59 shows the Mondex requirements profile in a best guess way based on the information currently available.

References: [Ano97], [Jon96]

4.30 MPTP

Micro Payment Transfer Protocol (MPTP) is a proposal from the W3 consortium electronic payments group. It was launched in 1995 and there is seemingly no progress at all. MPTP is a protocol to transfer payments through a common broker, which aims to be economical for small payments and interactive applications. The protocol claims to implement a variation of the PayWord (see section 4.40) proposal of Rivest and Shamir and to be inspired by the MilliCent (see section 4.27) proposal by Manasse and the iKP (see section 4.22) proposal by Bellare et. al.

For efficiency it is desirable to be able to combine transfer of payments instructions with those accomplishing the delivery of goods. For this reason MPTP may be layered on a variety of Internet protocols including HTTP and SMTP/MIME. Although the protocol is optimized for use as a payment scheme it is suitable for the transfer of larger amounts. The protocol is also suitable for use as an access control or resource allocation mechanism. With modification the protocol could be made to provide anonymity guarantees.

4.31 Mykro-iKP

This proposal from IBM involves chained hashes similar to PayWord (see section 4.40). It implements a micropayment system on top of ikP. A detailed description

Requirement/System	Mondex
Token System	Yes
Transaction	
Atomicity	Yes
Consistency	Yes
Isolation	Yes
Durability	Yes
Security	
No Double Spending	Yes, hopefully unbroken hardware ensures this
No Counterfeiting	Yes
No Overspending	n.a.
Non-Refutability	Yes
No Unauthorized Use	Yes, potentially, wallet lockable
Anonymity	No, banks have user data
Untraceability	No, banks can and do build profiles
Interoperability	
Divisibility	Yes (?).
Bidirectionality	Yes
Respendability	No (?)
Acceptability	Yes, potentially
Multicurrency Support	Yes, possible via the broker
Portability	Yes
Scalability	
Scalability	Yes
Off-line Operation	Yes
Economical Issues	
Operational	No, trial only
Large User Base	Yes, potentially
Buyer Risk	Yes, loss of card
Seller Risk	Yes
Reliability	Yes
Conservation	Yes
Ease of Use	
Unobstrusiveness	No (?)
Low Latency	Yes
Micropayments	Yes
Macropayments	Yes, up to 500 GBP per transaction
Low Fixed Costs	No
HW Independence	No, smart card and other HW

Table 59: Mondex Requirements Profile

Web Resource	[HB+95]
Name	MPTP
Origin	W3 consortium.
Status & Milestones	Working Group, 1995.
Payment Size	Micropayments.
Money Model	Token.
Payment Model	Probably cash like.
Remarks	Seemingly no progress at all.
Genealogy	Implements PayWord (see section 4.40), ideas from MilliCent (see section 4.27) and iKP (see section 4.22).

Table 60: MPTP Feature Profile

Web Resource	[HSW96]
Name	Mykro-iKP
Origin	Waidner, M. et al. from IBM.
Status & Milestones	Proposal, 1997.
Payment Size	Micropayments.
Money Model	Token.
Payment Model	Probably cash like.
Remarks	Could be transfered to SET (see section 4.47).
Genealogy	Similar to PayWord (see section 4.40), based on iKP (see section 4.22).

Table 61: Mykro-iKP Feature Profile

of a chained system is given for NetCard (see section 4.33). Here just some aspects special to Mykro-iKP are pointed out.

The system is based on chained hashes. It is performing micropayments by revealing pre-images of a bootstrapped Winternitz signature. The payments are secured by being pre-authorized in an initial iKP transaction, that assures the merchant of the customer credit. Each individual micropayment is signed by the customer. A kind of dual signature scheme seems to be used to tie a micropayment to a microdelivery.

The system requires a repetitive spending habit from customers. For non-repetitive spending habits Mykro-iKP proposes a so called micro payment brokers, a mechanism that does not seem economical at all.

4.32 NetBill

NetBill is the Carnegie-Mellon University Internet billing server project, which is used as payment method for buying information goods and services via the Internet. It aims at secure payment for and delivery of information goods, e.g. library services, journal articles, CPU cycles etc. The NetBill system charges for transactions and requires customers to have a prepaid NetBill account from which all payments are deducted. The NetBill payment system uses both symmetric key and public key cryptography. It relies on Kerberos for authentication purposes.

Web Resource	[Net96a]
Name	NetBill
Origin	CMU.
Status & Milestones	Local Trial, 1997.
Payment Size	Small payments.
Money Model	Notational.
Payment Model	Direct account based, including secure transaction model.
Validation	Online.
Privacy Control	Non-anonymous, traceable, NetBill server supposed to keep data confidential.
Security Mechanism	Public/symmetric key cryptography and Kerberos.
Prerequisites	Money Tool SW.
Risk	?.
Fees	Merchants are charged.
Latency/Costs	Relatively high, therefore unsuitable for micropayments.
User Base	About 100.
Limits	?.
Remarks	Financial security and fraud protection.
Genealogy	n.a.

Table 62: NetBill Feature Profile

An account server, called NetBill server, maintains accounts for both customers and merchants. NetBill acts as an aggregator to combine many small transactions into larger conventional transactions, thus amortizing conventional overhead fees. Therefore, both customers and merchants have to trust the NetBill server third party.

The basic NetBill protocol is as follows:

1. Merchant sends goods in encrypted form to customer computer.
2. Software on customer computer verifies that the goods were received correctly and sends verification of this to the merchant software.
3. Merchant sends customer verification message, customer account information and decryption key to NetBill server.
4. NetBill server verifies that money in customer account is sufficient to pay for the goods. If so, it transfers funds, stores decryption key, and sends report to merchant software.
5. Merchant then sends customer decryption key, which customer software uses to decrypt the goods. If the merchant server fails before completing this step, customer software can retrieve key from NetBill server.

The NetBill server keeps accounts for all the merchants and customers. The accounts are corresponding and linked to accounts at a traditional bank. The system is currently in trial on the Carnegie Mellon campus. An online demo of the NetBill system is available. The software for NetBill is currently available for Solaris, Windows NT and Windows 95.

who / what	Merch.	Cust.	Date	Amount	Item
Merchant	-	Yes	Yes	Yes	Yes
Customer	Yes	-	Yes	Yes	Yes
Bank	Yes	Yes	Yes	Yes	Partial
Observer	Partial	Partial	Yes	No	No

Table 63: NetBill Visibility Profile

Table 63 shows the NetBill visibility profile. NetBill is no anonymous system, as is notational and cheque-based. The NetBill group suggests an alternative system, where transactions are mediated via a trusted mix, e.g. the NetBill server at the bank acting that part.

who / what	Merch.	Cust.	Date	Amount	Item
Merchant	-	No	Yes	Yes	Yes
Customer	No	-	Yes	Yes	Yes
Bank	Yes	Yes	Yes	Yes	Partial
Observer	No	No	Yes	No	No

Table 64: Mediated NetBill Visibility Profile

Table 64 shows the mediated NetBill visibility profile. When using a trusted mix and encryption, amount, goods, merchant and customer are hidden from observation. Customers and merchants may remain mutually anonymous. The NetBill server still has full knowledge of the identities of the parties and most transaction details.

Table 65 shows the requirements profile of NetBill. Microeconomy and scalability are questionable because of the extensive network traffic required during the transaction and the interaction with the central NetBill server.

References: [ST95], [CST95b]

4.33 NetCard

NetCard was specifically designed for micropayments and was developed by the university of Cambridge computer laboratory. The participation of smart card experts GIS and a major UK clearing bank are to ensure technological and financial integration. The aim of the framework project, of which the NetCard project is a part, is to develop a network protocol and gateways to support high data rate communication networks including control functions that will form the basis for standards for high speed gateway protocols.

NetCard is a payment mechanism addresses repeated consecutive payments to a merchant involving signed chained hashes similar to PayWord (see section 4.40), Mykro-iKP (see section 4.31) or PhoneTicks (see section 4.42) and smart cards for signing and double spending control. NetCard supports multiple banks insofar as an interbank settlement infrastructure is taken for granted.

The NetCard project itself aims to provide solutions by the development of a set

Requirement/System	NetBill
Token System	No
Transaction	
Atomicity	Yes, even goods atomic
Consistency	Yes
Isolation	Yes
Durability	Yes
Security	
No Double Spending	n.a.
No Counterfeiting	Yes
No Overspending	Yes, prepaid
Non-Refutability	Yes
No Unauthorized Use	Yes
Anonymity	No, basically not, but maybe via trusted mix
Untraceability	No
Interoperability	
Divisibility	n.a.
Bidirectionality	No
Respendability	No
Acceptability	?
Multicurrency Support	Potentially, via NetBill server
Scalability	
Scalability	No, central NetBill server required, multiple NetBill servers questionable
Off-line Operation	No
Economical Issues	
Operational	No
Large User Base	n.a.
Buyer Risk	?
Seller Risk	?
Reliability	?
Conservation	Yes
Ease of Use	
Unobstrusiveness	Questionable
Low Latency	No
Micropayments	Maybe low, but not quite small payments
Macropayments	Yes
Low Fixed Costs	n.a.
HW Independence	Yes

Table 65: NetBill Requirements Profile

Web Resource	[Net96b]
Name	NetCard
Origin	University of Cambridge computer laboratory.
Status & Milestones	Demonstration prototype, 1996.
Payment Size	Micropayments.
Money Model	Token (kind of).
Payment Model	Direct cash like.
Validation	Offline.
Privacy Control	Non-anonymous, but customer may use pseudonyms, traceable, not very confidential.
Security Mechanism	Chained hashes, public key encryption, certificates, signatures, tamper-resistant smart cards for signing and double / over spending protection.
Prerequisites	SW and smart card equipment.
Risk	Merchant.
Fees	Merchants are charged.
Latency/Costs	Low.
User Base	n.a.
Limits	?.
Remarks	n.a.
Genealogy	Similar to PayWord (see section 4.40), Mykro-iKP (see section 4.31) or PhoneTicks (see section 4.42), proposal based on SET (see section 4.47).

Table 66: NetCard Feature Profile

of protocols and smartcard based mechanism to manage the necessary functions of authentication, delegation, authorization, accounting and revocation. The NetCard group has developed and implemented a micropayment protocol set involving signed chained hashes and smart cards for signing and and accidental double spending protection. The NetCard technology was evaluated in a trial multimedia system connecting Cambridge and Manchester universities. The main deliverable from Cambridge University consists of a demonstration system together with documentation of the protocols used in it.

NetCard customers get their public key and payment context, e.g. credit limit or pseudonym, certified by their issuers.

A basic NetCard transaction is described as follows:

1. The issuer supplies the customer with so called signed coin sticks, i.e. bundles of consecutively numbered tokens, in encrypted form.
2. If the customer wishes to purchase at a merchant, it hashes the tokens of a signed coin stick recursively, including an unique transaction identifier, e.g. merchant and customer pseudonym and a sequence number, starting with the last token and the first transaction id, then including the previous hash in the current hash each time and this way progressing to the first token. Then the customer signs the final hash (of the first token) together with the customer certificate. Signing, hashing and token storing is performed and supervised by the tamper resistant smart card.
3. To start the repeated consecutive payment transaction, the customer sends the

merchant the signed certificate and hash of the first token (i.e. the last hash computed). The merchant verifies the customer signature with the issuer's customer certificate.

4. To spend the first token, the customer sends the merchant the first token together with the hash of the second token (i.e. the last but one hash computed). If the hash of the first token sent in the previous message matches the hash computed by the merchant of the first token and the hash of the second token, the merchant accepts the token as valid. Consecutive tokens are treated in a similar way.

5. To redeem the tokens, the merchant presents the acquirer with the customer signature, the tokens actually spent and the corresponding hash values. The bank verifies the tokens and checks for double spending.

Further and improved versions of the NetCard protocol involve the customers creating the signed payment sticks themselves, or the issuer supplying a so called root coin from which the customer creates the payment stick.

A NetCard transaction on top of SET (see section 4.47 involving customer payment stick creation is described as follows:

1. The customer creates a series of coins, that form a payment stick, signs and hashes it as described above. The sum of the coins in the payment stick represent the upper limit of the purchases intended at that merchant.

2. The customer sends the signed certificate and first hash and the upper purchase limit to the merchant together with its credit card details in a SET transaction. The merchant gets a credit card pre-authorization for that amount in the SET environment to prevent over spending.

3. The customer performs repeated consecutive payment transactions revealing one token at each step as described above.

4. After the customer signaled the end of the transaction, the merchant sends a SET capture message to redeem the amount of the tokens tendered including the tokens, signatures and hashes received as proof of transaction.

This version of the protocol represents a notational short term direct account based transaction on top of a secure credit card presentation rather than a token based payment protocol.

who / what	Merch.	Cust.	Date	Amount	Item
Merchant	-	Partly/Yes	Yes	Yes	Yes
Customer	Yes	-	Yes	Yes	Yes
Bank	Yes	Yes	Yes	Yes	No
Observer	Yes	Partly/Yes	Yes	Yes	Yes

Table 67: Mediated NetCard Visibility Profile

Table 67 shows the mediated NetCard visibility profile. The extent on which the identity of the customer involved is revealed depends on the customer using a pseudonym.

Requirement/System	NetCard
Token System	Yes (first version), no (second version)
Transaction	
Atomicity	?
Consistency	?
Isolation	?
Durability	?
Security	
No Double Spending	Yes, protection against accidental double spending by a smart card, bank must detect double spending on purpose via double spending databases
No Counterfeiting	Yes
No Overspending	Yes, on top of SET pre-authorization
Non-Refutability	Yes
No Unauthorized Use	Yes, smart cards and signatures
Anonymity	No, but customer may choose pseudonym, non-anonymous on top of SET
Untraceability	No
Interoperability	
Divisibility	No, payment sticks must be made to fit, equal sized payments presumed
Bidirectionality	No
Respendability	No
Acceptability	Potentially
Multicurrency Support	Potentially, if on top of SET or supported by banks
Scalability	
Scalability	Yes
Off-line Operation	Yes
Economical Issues	
Operational	No
Large User Base	n.a.
Buyer Risk	No, protocol seems credit based
Seller Risk	Yes
Reliability	n.a.
Conservation	Yes
Ease of Use	
Unobstrusiveness	n.a.
Low Latency	Yes
Micropayments	Yes
Macropayments	No
Low Fixed Costs	n.a.
HW Independence	No, smart card for signing and double spending check

Table 68: NetCard Requirements Profile

Table 68 shows the requirements profile of NetCard. Whether the ACID properties hold with NetCard cannot be resolved with the information available on the system.

Reference: [AMS96]

4.34 NetCash

Web Resource	[Net96c]
Name	NetCash
Origin	G. Medvinsky and B.C. Neuman from the Information Sciences Institute of University of Southern California.
Status & Milestones	Closed trial, 1996.
Payment Size	Micropayments.
Money Model	Token.
Payment Model	Direct cash like.
Validation	Online.
Privacy Control	Anonymous and untraceable (on demand), but not with respect to the NetCash currency server, confidentiality issues not mentioned.
Security Mechanism	Certificates, signatures, double spending database.
Prerequisites	NetCash SW.
Risk	Customer.
Fees	?.
Latency/Costs	Fairly high due to online authorization.
User Base	n.a.
Limits	?.
Remark	Their web site does not contain any recent material.
Genealogy	Reverse double spending system to Ecash (see section 4.16), similar respendability simulation as Magic-Money (see section 4.25), integrated with sibling project NetCheque (see section 4.35).

Table 69: NetCash Feature Profile

NetCash by G. Medvinsky and B.C. Neuman from the Information Sciences Institute of University of Southern California describes a framework for electronic currency whereas the NetCheque project (see section 4.35) by the same authors is a distributed accounting service for electronic cheques.

NetCash offers a framework for a secure and anonymous real time digital payment system. A research prototype has been implemented. NetChash tries to integrate anonymous electronic currency into the existing banking and accounting infrastructure. The system claims to be scalable and commonly acceptable for most transactions offering some anonymity and requiring only a limited form of online interaction. For higher security demands the NetCash framework is supposed to be extendible. NetCash does not require tamper resistant hardware or secure networks and is basically suitable for use on the Internet.

The basic NetCash structure consists of independent, distributed currency servers providing a link between anonymous electronic currency and non anonymous services, such as NetCheque digital cheques. Currency server provide customer services, like double spending detection, coin exchange to allow untraceability, purchases of coins with cheques and redemption of coins for cheques.

NetCash uses a multiple layer authentication, similar to the system adopted by the Financial Services Technology Consortium (see section 4.19). To set up a new currency server, the new currency needs to be ensured by an insurance agency, like the Federal Reserve. The new currency server is integrated into the existing network by establishing a secure connection between the server and the insurance agency to get their public key and unique server id certified. This certificate enables the new server to create and manage digital currency that will be accepted by the other currency servers and banks. The currency produced by the new server needs to be linked to the balances of existing traditional bank accounts.

A NetCash coin contains the name of the issuing currency server, a unique serial number, a reference to the insurance agency certificate and is signed by that currency server. Anyone receiving a NetCash coin therefore can validate the chain of trust for this coin.

NetCash uses a double spending detection system, implemented in the reverse manner to the DigiCash Ecash (see section 4.16) system. A NetCash currency server records the unique serial number of each coin issued. All coins redeemed are removed form that list of issued coins. If a customer tries to spend a faked or double spent coin with a serial number not registered in this list, the currency server will refuse to accept it. The NetCash group claims this system to be more efficient than the Ecash system. With Ecash, either the list of spent coins must be maintained for an indefinite time to prevent double spending, or all coins must have an expiry date. The trade off between NetCash and Ecash is determined by ratio of tokens unredeemed to tokens redeemed. If the number of unredeemed tokens exceeds that of redeemed tokens, Ecash requires less overhead. If the ratio is the other way round, NetCash means less overhead. Anyway Ecash can not keep a list of coins issued because of the blind signature scheme to ensure anonymity.

NetCash tokens pretend to be respendable just the way MagicMoney does (see section 4.25). However, this is a fake impression. If a merchant presents a token to the currency server for validation, the server returns a new, but equivalent token to the merchant (if the initial token has been valid). But this process is hidden from the user. If coins were respent offline, NetCash transactions could not grant any protection against double spending.

who / what	Merch.	Cust.	Date	Amount	Item
Merchant	-	No	Yes	Yes	Yes
Customer	No	-	Yes	Yes	Yes
Bank	Yes	Yes	Yes	Yes	No
Observer	No	No	Yes	Yes	Yes

Table 70: NetCash Visibility Profile

Table 70 shows the NetCash visibility profile. NetCash transactions are validated online and claim to maintain customer anonymity. However this anonymity does not hold with the currency server that potentially can trace who bought and who redeemed which coins. Customers and merchants are required to trust the NetCash currency server that it does not log these transactions. The NetCash group says that "it is expected that currency servers will not do so, and it is likely that the agreement with clients will specifically preclude it". With DigiCash Ecash (see section 4.16) and its system of blind signatures anonymity is actually enforced by the protocol.

NetCash offers a scalable degree of anonymity, depending on the transaction needs. This makes it difficult to define the visibility profile. NetCash can trace the issued coins and is just bound by word of honor not to do so. Therefore the visibility profile in table 70) shows the possible rather than the honorable visibility.

Requirement/System	NetCash
Token System	Yes
Transaction	
Atomicity	?
Consistency	?
Isolation	?
Durability	?
Security	
No Double Spending	Yes
No Counterfeiting	Yes
No Overspending	n.a.
Non-Refutability	?, most probably
No Unauthorized Use	?, most probably
Anonymity	Yes, but not towards the NetCash currency server
Untraceability	Yes, but not towards the NetCash currency server
Interoperability	
Divisibility	Yes
Bidirectionality	Yes
Respendability	No, just simulated
Acceptability	Potentially
Multicurrency Support	Potentially, if supported by banks
Scalability	
Scalability	Yes
Off-line Operation	No
Economical Issues	
Operational	No
Large User Base	n.a.
Buyer Risk	Yes, limited by amount of coins
Seller Risk	No
Reliability	n.a.
Conservation	Yes
Ease of Use	
Unobstrusiveness	n.a.
Low Latency	No
Micropayments	Yes
Macropayments	No
Low Fixed Costs	n.a.
HW Independence	Yes

Table 71: NetCash Requirements Profile

Table 71 shows the requirements profile of NetCash. Whether the ACID properties hold with NetCash cannot be resolved with the information available on the system, as the main NetCash issues are anonymity and security. Scalability relies on multiple currency servers and interoperability the cooperation between these different currency servers. Especially an efficient clearing and rerouting system is required for this.

Reference: [MN93]

4.35 NetCheque

Web Resource	[Net96d]
Name	NetCheque
Origin	G. Medvinsky and B.C. Neuman from the Information Sciences Institute of University of Southern California.
Status & Milestones	Prototype available, December 1994.
Payment Size	Micropayments.
Money Model	Notational.
Payment Model	Direct account based, cheque like.
Validation	Online.
Privacy Control	Non-anonymous, traceable, unconfidential.
Security Mechanism	Kerberos authentication.
Prerequisites	NetCheque SW.
Risk	Merchant.
Fees	?.
Latency/Costs	Fairly high due to online authorization.
User Base	n.a.
Limits	Kerberos export restrictions.
Remark	Their web site does not contain any recent material.

Table 72: NetCheque Feature Profile

NetCheque by G. Medvinsky and B.C. Neuman from the Information Sciences Institute of University of Southern California is a distributed accounting service for digital cheques. whereas the NetCash project (see section 4.34) by the same authors describes a framework for electronic currency.

NetCheque allows customers to use accounts on bank servers of their choice to allow scalability. With a NetCheque account clients can issue and reimburse digital checks. The NetCheque system could also be used to clear NetCash accounts between different currency servers.

Originally, the NetCheque accounting system has been designed to maintain quotas for distributed system resources, like printing, which involved transactions of small amounts. This renders NetCheque suitable for micropayments of some sorts. The performance requirements for micropayments are to be met by using shared key cryptography, i.e. Kerberos authentication. Usually cheque based systems use public key signatures and encryption, e.g. like the FSTC (see section 4.19) digital cheque system. The NetCheque group states that symmetric keys are faster and therefore more suitable for micropayment systems. Due to Kerberos export restrictions the NetCheque system is only available inside the USA. Its software is currently available for SunOS and HPUX.

NetCheque transactions are identified and online. A NetCheque transaction runs as follows:

1. Currency and amount of the cheque, expiry date, account the cheque is drawn on and payee are written on the cheque in the clear.
2. To issue a cheque the NetCheque system obtains a Kerberos ticket to authenticate the payer and, adding a checksum, uses the authentication information as signature on the cheque.
3. The "signed" cheque is base64 encoded and sent to the payee via email or online.
4. To deposit a cheque the payee decodes the cheque and needs to obtain a Kerberos ticket ensuring that the cheque can only be paid into the payee's account.
5. The payee opens an encrypted connection issuer accounting server to clears the cheque.

NetCheque cheques may be cleared online or batch processed. Other NetCheque functions allow viewing of balances and transactions.

who / what	Merch.	Cust.	Date	Amount	Item
Merchant	-	Yes	Yes	Yes	Yes
Customer	Yes	-	Yes	Yes	Yes
Bank	Yes	Yes	Yes	Yes	No
Observer	Yes	Yes	Yes	Yes	No

Table 73: NetCheque Visibility Profile

Table 73 shows the NetCheque visibility profile. The NetCheque system is fully identified. As a cheque is not encrypted, an observer can read it. The observer can not trace the item to the payment transaction, if the goods order and delivery is unconnected with the payment.

Table 74 shows the requirements profile of NetCheque. The NetCheque requirements profile is very similar to that traditional paper cheques except that the authors claim it sufficiently economic for micropayments. The NetCheque accounting servers interoperate to clear cheques.

Reference: [NM95]

4.36 NetFare

NetFare is a prepaid fare card, similar to a phone card, meant for use over the Internet. NetFare gains pre- and post-transaction float. Their Web site only contains a very fuzzy description about their system. Currently they are conducting a survey about who might be interested in the system.

Customers need to purchase NetFare "cards", which are identified by a card id and authenticated via a PIN. They correspond to prepaid accounts at the central

Requirement/System	NetCheque
Token System	No
Transaction	
Atomicity	Yes
Consistency	Yes
Isolation	No
Durability	Yes
Security	
No Double Spending	n.a.
No Counterfeiting	Yes
No Overspending	No
Non-Refutability	No
No Unauthorized Use	Yes
Anonymity	No
Untraceability	No
Interoperability	
Divisibility	n.a.
Bidirectionality	Yes
Respendability	No
Acceptability	Yes
Multicurrency Support	Yes
Scalability	
Scalability	Yes
Off-line Operation	No
Economical Issues	
Operational	No, only closed user community
Large User Base	n.a.
Buyer Risk	No
Seller Risk	Yes
Reliability	n.a.
Conservation	Yes
Ease of Use	
Unobstrusiveness	No
Low Latency	No
Micropayments	Yes, limited
Macropayments	Yes, very limited
Low Fixed Costs	n.a.
HW Independence	Yes

Table 74: NetCheque Requirements Profile

Web Resource	[Net96e]
Name	NetFare
Status & Milestones	Under construction, 1997.
Payment Size	Micropayments.
Money Model	Notational.
Payment Model	Indirect push account based.
Validation	Online.
Privacy Control	None.
Security Mechanism	Passphrase (PIN).
Prerequisites	NetFare card (number) and PIN, SW.
Limits	USD only.
Risk	Customer.
Fees	n.a.
Latency/Costs	Fairly high due to online authorization.
User Base	n.a.
Remark	Very simple system.

Table 75: NetFare Feature Profile

NetFare server. Customers can check their balance online with their card number and PIN.

On a payment request by the merchant, the NetFare server requires card number and PIN from the customer and checks the balance of the customer fare card account, if the requested payment is possible. If so, the NetFare server transfers the amount to the merchant account and gives the merchant an indication to release the goods. Merchants accounts are settled once a month.

4.37 Open Market

Web Resource	[Ope96]
Origin	Open Market, Inc.
Payment Model	Electronic business software.
Status & Milestones	Operational, 1994 (as a company).
Genealogy	Going to include SET(see section 4.47) compliant payment facilities.

Table 76: Open Market Feature Profile

Open Market Inc. was founded in February 1994 and aims to provide electronic commerce solutions. Its Internet commerce platform product is Transact, which manages Internet commerce within a corporation's or commerce service provider's operations. The system offers functionality such as order management, online customer service, security, authentication, record-keeping, several purchasing and payment models and secure transaction processing including sales tax and shipping charges.

Open Market participated in the first multivendor SET (see section 4.47) demonstration and is going to include SET compliant payment facilities in their Transact system. Open Market cooperates with MasterCard and Visa.

4.38 PayMe

Web Resource	[Pay96]
Name	PayMe
Origin	M. Peirce and D. O'Mahony of Computer Science Department, Trinity College in Dublin, Ireland.
Status & Milestones	Proposal, 1995.
Payment Size	Micropayments.
Money Model	Token.
Payment Model	Direct cash like.
Validation	Online.
Privacy Control	Not quite anonymous, not quite untraceable, confidential, just like NetCash.
Security Mechanism	Passphrases, signatures, encryption, nonces.
Prerequisites	PayMe wallet software.
Risk	Customer.
Genealogy	Tries to combine features of Ecash (see section 4.16) and NetCash (see section 4.34)

Table 77: PayMe Feature Profile

The PayMe system tries to combine the best features of Ecash (see section 4.16) and NetCash ((see section 4.34). It is a graduate student project by M. Peirce and D. O'Mahony of the Computer Science Department, Trinity College in Dublin, Ireland. A prototype was implemented. The strength of Ecash is seen in its full anonymity and untraceability and its main problem the size of the double spending database. The advantages of NetCash are pointed out as being scalable and secure while not being fully anonymous and untraceable.

The PayMe system aims to be a scalable anonymous electronic cash service, which uses its own proprietary secure communications protocol, the PayMe Transfer Protocol (PMTP), to communicate between the involved parties. The proprietary protocol is seen as out-band security. PayMe uses both symmetric and public-key cryptography. All involved parties have their own public key pair. The protocol is confidential as all messages are encrypted. The use of nonces tries to prevent replay and masquerading. It offers about the same degree of anonymity and untraceability as NetCash.

A PayMe bank mints tokens, maintains a database of all unredeemed tokens to prevent double spending, exchanges tokens on demand and manages accounts of its clients. PayMe clients are customers and merchants, but the system is bidirectional. An interbank clearing network infrastructure is required. Payments must be made exact. No change can be given so as not to compromise anonymity if a merchant colludes with the bank.

A PayMe transaction on the Web is described as follows:

1. To purchase goods, a order URL pointing to a cgi script is selected. This causes the Web server to start the merchant wallet.
2. The merchant wallet receives the goods details and the network address of the requesting Web client.

3. The merchant wallet computes the cost of the goods and contacts the customer wallet asking for payment.
4. The buyer is be notified of the request and will either refuse or accept the payment request. On accepting the customer wallet selects the coins required to make the exact payment and sends them to the merchant wallet.
5. The merchant wallet validates the coins by either exchanging them anonymously for new coins or depositing them into a bank account. An exchange must be performed with the issuer. A deposit can be done with the acquirer and interbank clearing. The issuer performs the double spending check and removes redeemed coins from the database. On an exchange the merchant is given new coins, otherwise the amount is credited with the acquirer on the merchant account.
6. The merchant wallet receives an indication from the bank if the coins were valid. This will be either new coins or a deposit success message.
7. The merchant wallet issues a signed receipt to the customer and releases the goods. The merchant Web server then forwards them to the customer Web client.

The proposal does not elaborate in which way it is superior to NetCash with regards to anonymity and untraceability. It seems to behave in the same way that system does.

4.39 PayNow

Web Resource	[Inc96]
Name	PayNow
Origin	Cyber Cash Inc.
Status & Milestones	Trial, 1997.
Payment Model	Direct account based, cheque like.
Security Mechanism	Integrated into CyberCash wallet.

Table 78: PayNow Feature Profile

Electronic cheque scheme by CyberCash, integrated into their wallet. Behaves just like the secure credit card presentation, only it is going to be bidirectional. Next to no information available.

4.40 PayWord

The proposal by Rivest and Shamir involves chained payments. A detailed description of a chained system is given for NetCard (see section 4.33). Here just some aspects special to PayWord are pointed out.

PayWord is credit based. The customer has a standing relation with a broker. The customer is certified monthly by the broker to issue PayWord chains. For an initial

Web Resource	[RS95]
Name	PayWord
Origin	Rivest and Shamir.
Status & Milestones	Proposal, 1995.
Payment Model	Direct cash like (?).
Privacy Control	None.
Security Mechanism	Chained Hashes, signatures.

Table 79: PayWord Feature Profile

commitment to a merchant the customer generates and signs a commitment to a new customer/merchant specific chain of paywords. All paywords of a chain have the same value. Paywords are computed by repeatedly hashing an initial salt. The last has value generated is called the root of the payword chain which has no value itself and is signed by the customer as commitment and given to the merchant in the initial transaction.

Then the customer subsequently trades the paywords in the reverse order generated to the merchant. The merchant can verify the payment by computing the hash of the present payword and checking that it is equal to the prior payword respective the root in the commitment for the first payword tendered. At the end of each day the merchant hands all commitments and paywords to the broker for redemption.

PayWord does not provide any anonymity. Overspending customers can be weeded out after the fact. Merchant and broker share the risk of loss.

For additional security paywords could be sold on a debit basis. PayWord allows for efficient different value payments from a payment chain. If a customer skips some paywords and trades a later one without trading those skipped ones, the customer can pay a higher amount in one transaction. The merchant can still check the validity of the payword by a repeated application of the hash function.

4.41 PC-Pay

Web Resource	[PP96]
Name	PC-Pay
Status & Milestones	?
Payment Model	direct cash like on a smart card.
Privacy Control	Anonymous.
Security Mechanism	Hardware-based encryption.
Prerequisites	A smart card and card reader, interface software.
Fees	595 USD for the prerequisites.

Table 80: PC-Pay Feature Profile

The PC-Pay system developed by Innovonics Inc. relies on tamper-resistant hardware. It uses a smart card, that provides the encryption of the payment information before it reaches the PC. The matching card reader is designed to act as an ATM terminal with additional features. There is no detailed information available on how the system works.

4.42 PhoneTicks

Web Resource	[Ped95]
Status & Milestones	Trial (?), 1995.
Payment Model	Direct cash like (?).
Security Mechanism	Chained hashes.
Genealogy	Similar to PayWord (see section 4.40), Mykro-iKP (see section 4.31) or NetCard (see section 4.33), proposal implemented (?) in CAFE (see section 4.7).

Table 81: PhoneTicks Feature Profile

This proposal by Torbe Pedersen involves chained hashes. It is similar to PayWord (see section 4.40). PhoneTicks supposedly is implemented in CAFE (see section 4.7) and therefore could be termed as in trial.

A detailed description of a chained system is given for NetCard (see section 4.33). The technical details of PhoneTicks are not in great depth and do not seem to contain any new or special ideas to those of the other chained payment proposals.

4.43 Polling

Web Resource	[JO97]
Name	Polling
Origin	A. Odlyzko, AT&T.
Status & Milestones	Proposal, 1997.
Money Model	Notational.
Payment Model	Direct account based.
Payment Size	Micropayment.
Security Mechanism	Probabilistic online validation.
Genealogy	Probabilistic online validation also is proposed in MiniPay (see section 4.28).

Table 82: Polling Feature Profile

Existing payment schemes can be improved in their efficiency and be made suitable for micropayments by using probabilistic polling. This proposal is made by S. Jarecki and A. M. Odlyzko of AT&T.

It allows for control of overspending at the cost of only a modest increase in communication compared to an offline scheme. The proposal elaborates in loving detail on polling parameters and analyzes their impact on risk, delay and communication costs. As the authors are mathematicians it is not surprising that this is a very mathematical paper.

One of their examples proposes the application of Polling on PayWord (see section 4.40). Their proposal also includes the description of a merchant registration and notification scheme, where merchants register each initial transaction with a customer at the broker and in case of an overspending detection the broker notifies the registered merchants as opposed to merchant broadcast notification.

4.44 Redi-Check

Web Resource	[RC96]
Status & Milestones	Operational, April 1995.
Payment Model	Direct account based, electronic cheques.
Privacy Control	Redi-Check keeps customer data confidential.
Security Mechanism	SSL, PGP and eventually SET.
User Base	45,000 customers and 200 merchants

Table 83: Redi-Check Feature Profile

Redi-Check offers a cheque draft service. Customers just need an email address and a cheque bank account. Its security is SSL and PGP based. Involves digital versions of traditional paper cheques.

4.45 Sandia Lab's Electronic Cash

Web Resource	[San96]
Status & Milestones	?
Payment Model	?
Privacy Control	?
Security Mechanism	TTP, mixes

Table 84: Sandia Lab's Electronic Cash Feature Profile

Sandia Lab's Electronic Cash uses trusted third parties to trace payment transactions and at the same time tries to protect customer anonymity. Keywords are trustee-based tracing, electronic trustees and making anonymous change. They claim to have a provably anonymous electronic cash system. Only with the cooperation of several trusted third parties tracing is possible.

4.46 Secure Courier

Web Resource	[Sec96]
Origin	Netscape, T. Elgamal.
Status & Milestones	Operational, July 1995
Payment Model	Secure credit card presentation.
Privacy Control	Confidential.
Security Mechanism	SSL, going to be superseded by SET (see section 4.47).

Table 85: Secure Courier Feature Profile

Secure Courier is a SSL bases secure credit card presentation scheme by Netscape. Going to be superseded by SET (see section 4.47).

Web Resource	[VS96] [MS96]
Name	SET
Origin	Visa, MasterCard, CyberCash, Netscape, IBM, Microsoft, DigiCash and many others.
Status & Milestones	Proposal, 1996, compliance testing, 1998.
Payment Size	Macropayments.
Money Model	Notational.
Payment Model	Secure credit card presentation.
Validation	Online.
Privacy Control	Confidential, non-anonymous, traceable.
Security Mechanism	RSA, DES, encryption, signatures, passphrases, certificates, chain of trust, dual signatures.
Prerequisites	Wallet software, credit card, maybe later a smart card.
Risk	Customer.
Fees	Most probably none, besides the credit card fees.
Latency/Costs	Fairly high due to online authorization and careful encryption and signing schemes.
User Base	Various electronic commerce systems going to be SET compliant.
Limits	?.
Remarks	Refund from credit card transactions is supported.
Genealogy	Besides some obsolete payment protocols mentioned below, SET was strongly influenced by CyberCash (see section 4.12), and iKP (see section 4.22).

Table 86: SET Feature Profile

4.47 SET

IBM & MasterCard & Visa announced an alliance for secure credit card presentation over the Internet, the Secure Electronic Transaction (SET) system. After a few separate efforts to set up their own standard, the major credit card, electronic commerce, software and hardware companies teamed up to develop and support a single unified industrial standard, SET.

The following proprietary standards influenced and were superseded by SET:

SEPP: obsolete secure electronic payment protocol from Mastercard, IBM, Netscape, GTE, and CyberCash.

STT: obsolete secure transactions technology from Visa and Microsoft.

SCC: obsolete secure credit cards scheme from Mastercard and Visa.

iKP: obsolete key payment protocol from IBM.

CyberCash: currently operational secure credit card presentation payment system by CyberCash Inc., going to be SET compliant.

The SET protocol is supported both by VISA and MasterCard and aims to provide a uniform standard for secure transactions in the Internet. SET is a complex protocol set that tries to cover all aspect of online commerce from initial registration of a credit card holder with an online SET agency to actual details of payments themselves.

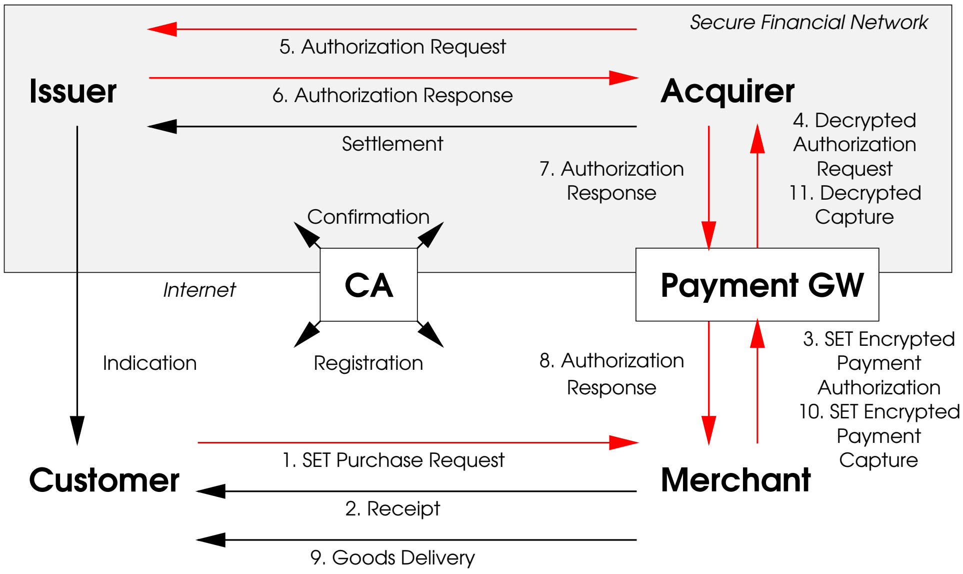

Figure 12: SET Payment Transaction

Picture 12 shows a SET payment transaction. A typical SET purchase scenario is as follows:

1. The customer browses a catalogue and selects items to purchase. The customer then is presented the order details including the total price and selects a payment system, i.e. with SET the particular credit card to use.
2. The customer sends the merchant signed order details and payment instructions.
3. The merchant requests payment authorization from the issuer.
4. The merchant sends confirmation of the order to the customer.
5. The merchant ships the goods to the customer.
6. The merchant requests settlement from the issuer via the acquirer.

Participants in SET transactions are:

Customer/Cardholder: The customer, or cardholder as it is called in SET, uses a credit card that has been issued by its issuer to buy goods at the merchant.

Issuer: The issuer is a bank that keeps an account for the customer and has issued the credit card. The issuer guarantees payment for authorized transactions.

Merchant: The merchant offers goods and receives SET credit card payments. The merchant has a financial relationship with the acquirer.

Acquirer: The acquirer is a bank that keeps an account for the merchant and processes credit card authorizations and payments.

Payment gateway (PG): A payment gateway is a device operated by the acquirer or a designated third party that processes merchant payment messages including payment instructions from customers. In CyberCash (see section 4.12) this payment gateway is represented by the CyberCash server.

Certification authority (CA): All customers and merchants are required to register with a SET certification authority before purchasing can commence. All payment gateways, issuers and acquirers are assumed to be already registered with the certification authority.

SET transactions are non-anonymous and verified online. All involved parties are known and authenticated, all transactions must be online to ensure that authentication and proper authorization.

By using a combination of RSA public key and DES symmetric key operations combined with a chain of trust of digital certificates SET mutually authenticates the identities of the involved parties and ensures confidentiality. All messages passed in SET are signed. All SET certificates can be verified by following their chain of trust to a well known root. All messages containing sensitive data are encrypted, either with a public key or with a symmetric key and signed. Symmetric keys are usually used just once.

SET uses dual signatures which allow to link cryptographically two messages in a way that a third party can verify that a payment request belongs to a certain offer without seeing the details of the offer itself. This is done by creating the a message digest each of both the payment message and the offer text, concatenating the two digests, creating a new digest and signing that. So a party having the digest of the offer and the payment message can recompute and verify the dual signature message.

The main SET transactions being used in registration and purchase are simplified as follows:

Card holder registration: Customers need to register with the CA before they can send SET messages to merchants and they must have a signature key pair. The CA verifies the customer data with the issuer and generates a customer certificate of limited validity which contains a signed hash of the credit card details and sends it to the customer.

Merchant registration: Merchants need to register with CA before they can receive SET payment instructions from customers and they must have a key exchange and a signature key pair. The CA verifies the merchant data with the acquirer and generates a merchant certificate of limited validity, certifies the merchant signature key and sends these certificates to the merchant.

Purchase request: This request is invoked after the customer has completed selection, has approved of the completed order form and selected a credit card for payment. Unlike with traditional credit card transactions, where the initiation starts with the merchant, in SET the customer begins the purchase transaction. The customer creates order information and payment instruction, generates a dual signature for these two messages and transmits them to the merchant. The credit card details can be read only by the PG. The merchant returns an order receipt and processes the order.

Payment authorization: During the processing of an order, merchants need to get payment authorization from the PG. The merchant states the transaction details together with the customer payment instruction to the PG. The PG verifies the cardholder dual signature on the payment instruction and ensures consistency between the merchant transaction details and the customer payment instruction. Then the PG obtains payment authorization via secure financial networks and returns a capture token to the merchant. The merchant then can continue processing the order.

Payment capture: After completing the processing of an order, or several orders for that matter, merchants will request payment. The merchant states the capture request details together with the capture token to the PG. The PG ensures consistency between the capture details and the capture token and then sends the capture request via secure financial networks to the issuer and returns the response to the merchant who uses this response to reconciliate with payments received from the acquirer.

Further SET transactions include:

Certificate query: If the CA is unable to complete a certificate request online, registering customers or merchants can check again later with this message to determine the status of their certificate request.

Purchase inquiry: If a merchant is unable to complete a purchase request online, customers can check again later with this message to determine the status of their payment processing.

Authorization reversal: This transaction allows merchants to correct previous authorization requests. This can apply to the whole or part of the order for which payment authorizion has been requested.

Capture reversal: This transaction allows merchants to correct errors in capture requests.

Credit: This transaction allows merchants to credit a customer credit card account, e.g. if goods have been returned.

Credit reversal: This transaction allows merchants to revoke issued credit.

Payment gateway certificate request: This transaction allows merchants to obtain all current PG certificates and public keys.

Batch administration: This transaction allows merchants to communicate to the PG about their batch processing.

who / what	Merch.	Cust.	Date	Amount	Item
Merchant	-	Partial	Yes	Yes	Yes
Customer	Partial	-	Yes	Yes	Yes
Bank	Yes	Yes	Yes	Yes	No
Observer	No	No	Yes	No	No

Table 87: SET Visibility Profile

Table 87 shows the SET visibility profile. The merchant sees the customer only partially as the account and credit card details are encrypted and only visible to the payment gateway and the bank. The "bank" can be distributed among different entities, but these entities can cooperate to reconstruct transactions if necessary, so they are treated as one unified party in the visibility profile. In SET the participants are not anonymous, but due to the dual signature scheme the transaction goods details are confidential even with respect to the bank.

Table 88 shows the requirements profile of SET. SET does not not define any particular underlaying traditional payment system and could work with debit and credit cards. However, SET demands certain properties of any conforming traditional payment system.

SET is very careful about authentication and authorization. This makes it unsuitable for micropayments, moreover if the underlying traditional payment system is a credit card. SET requires four messages between customer and merchant. These four messages involve four digital signatures, four RSA public key encryption and decryption operations, one DES symmetric key encryption and decryption operation, two certificate validations and one payment authorization by the payment gateway (bank) for the merchant which itself consists of two messages with two digital signatures, three DES symmetric key encryption and decryption operations, five RSA public key encryption and decryption operations and two certificate verifications. The question of scalability is raised by the need for central servers and online verification.

The IBM financial institutions payment system PBS/Europay (http://www.europe.ibm.com/nc/customer/pbseuro.htm) is going to be SET compliant. PBS, Europay, IBM and MasterCard have teamed up to provide this system. A first pilot will be installed in Denmark.

References: [SET97a], [SET97b], [SET97c]

4.48 SubScrip

This proposal by A.Furche and G.Wrightson of Newcastle University, Australia proposes a repeated micropayment system based on temporary customer accounts at the merchant. These accounts are prepaid by a conventional payment system. That conventional payment system must be able to accept refunds as well.

4.49 TUB

Transactions using bets (TUB) is a simple proposal by Daniel Wheeler. It aims at efficient micropayments by using bets between the merchant and the customer. If the customer wins, the service is free. If the merchant wins, the customer pays the agreed amount which will be much higher that the actual worth of the service.

By the law of large numbers this will work out and instead of a lot of small payments only some of a more substantial value are performed. For these "lost" bets the

Requirement/System	SET
Token System	No
Transaction	
Atomicity	No
Consistency	Yes
Isolation	No
Durability	Yes
Security	
No Double Spending	n.a.
No Counterfeiting	Yes
No Overspending	No
Non-Refutability	Yes
No Unauthorized Use	Yes
Anonymity	No
Untraceability	No
Interoperability	
Divisibility	n.a.
Bidirectionality	No
Respendability	No
Acceptability	Yes
Multicurrency Support	Yes
Scalability	
Scalability	Yes, most probably
Off-line Operation	No
Economical Issues	
Operational	Not quite, but many SET compliant electronic commerce solutions under development
Large User Base	Yes, potentially
Buyer Risk	Yes, limited by credit card liability limit
Seller Risk	No
Reliability	Yes
Conservation	Yes
Ease of Use	
Unobstrusiveness	No, looking at the demonstration prototypes, this is unlikely, as they suggest a direct emulation of traditional print through card slip transactions
Low Latency	No
Micropayments	No
Macropayments	Yes
Low Fixed Costs	?, most probably not exceeding regular credit card costs very far
HW Independence	Yes, unless the integrate a smart card someday

Table 88: SET Requirements Profile

Web Resource	[Sub96]
Status & Milestones	Proposal, 1996
Payment Model	Notational.

Table 89: Subscrip Feature Profile

Web Resource	[Whe96]
Name	TUB
Payment Model	Micropayments.
Origin	D. Wheeler.
Status & Milestones	Proposal, April 1996.
Genealogy	Similar to LotteryTickets (see section 4.24).

Table 90: TUB Feature Profile

customer can pay using a suitable existing small or macropayment system.

The steps proposed are:

- The merchant and the customer both agree on a betting sum, a boolean betting function f and the service that has a cretain value.
- The merchant sends r = hash (R) to the customer.
- The customer sends a random number X to the merchant.
- The merchant unvails R.
- The customer checks that r = hash (R).
- The merchant and the customer both work out f (R, X) and determine whether the charge is the payment agreed or nothing and proceed accordingly.

The protocol is not specified at great detail.

4.50 VeriFone

Web Resource	[Ver96a]
Status & Milestones	Operational, Juni 1996
Payment Model	Secure credit card presentation, claims to support electronic cash and micropayments.
Privacy Control	Confidential, non-anonymous, traceable.
Security Mechanism	RSA public key encryption, a HW solution is aimed at.
Prerequisites	HW later, SW now for customers and merchants, credit card.
Remarks	Going to be SET (see section 4.47) compliant.

Table 91: VeriFone Feature Profile

VeriFone provides secure credit card presentation software and plans to integrate a smart card into this scheme. It is also going to be SET compliant.

Web Resource	[Via96]
Name	ViaCheck
Status & Milestones	Operational, september 1995.
Payment Model	Secure credit card presentation.
Security Mechanism	The software for encryption comes from the merchant server; any customer input will be encrypted.
Prerequisites	Credit card

Table 92: ViaCheck Feature Profile

4.51 ViaCheck

ViaCheck provides software for merchants to allow secure credit card presentation via a Web browser and server.

5 Summary

This section compares some of the major payment protocols presented in the precious sections with regards to their major requirement profile data.

5.1 Profiles

System	Anonymous	Online	Atomicity	Consistency	Isolation	Durability	Economically	Divisibility	Scalability	Interoperability	Conservation
Cash	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	N
CAFE	Y	N	?	Y	Y	Y	Y	Y	Y	?	Y
Ecash	Y	Y	N	N	N	N	Y	Y	?	?	Y
Geldkarte	N	N	Y	Y	Y	Y	Y	-	Y	Y	Y
MilliCent	N	N	?	?	Y	?	Y	Y	Y	Y	?
Mondex	N	N	Y	Y	Y	Y	Y	Y	Y	?	Y
NetCash	N	Y	?	?	?	?	Y	Y	Y	Y	Y

Table 93: Comparison of Token Protocols

Table 93 shows a comparison of token payment protocols. Due to the transmission of information over a insecure network real atomicity is hard to grant for token based systems. It is quite possible to ensure that never both payer and payee think to have legitimate access to a token, but it is not possible to prevent that neither payer nor payee considers itself to be the owner of a token, i.e. there is always a certain probability for to lose monetary value.

Table 94 shows a comparison of notational payment protocols. Notational systems

System	Anonymous	Online	Atomicity	Consistency	Isolation	Durability	Economically	Divisibility	Scalability	Interoperability	Conservation
Cheque	N	N	Y	Y	N	Y	N	-	Y	N	Y
Credit	N	Y	N	Y	N	Y	N	-	Y	N	Y
CyberCash	N	Y	N	Y	N	Y	N	-	?	Y	Y
FSTC	N	Y	Y	Y	N	Y	Y	-	Y	?	Y
FV	Y	Y	N	Y	N	Y	N	-	Y	Y	Y
Mini-Pay	N	N	N	Y	N	Y	Y	-	Y	Y	Y
NetBill	N	Y	Y	Y	Y	Y	?	-	?	?	Y
NetCheque	N	Y	Y	Y	N	Y	Y	-	Y	Y	Y
SET	N	Y	N	Y	N	Y	N	-	?	Y	Y

Table 94: Comparison of Notational Protocols

are generally tied to traditional payment systems and tend to inherit the properties of those systems.

5.2 Discussion

At the moment there are a lot of different competing systems. It is likely that not one single system will dominate the market as there are conflicting requirements for different forms of commercial transactions. With micropayments, efficiency and speed are dominant factors and security issues can be teated with less priority, because gain from fraud would be very small. With macropayments, security is most important and strong encryption systems are required to protect both the details of the transaction and the involved parties.

5.2.1 Macropayments

The field of macropayments (from about 10 USD) appears to be straightforward. The issues here are clearly defined and can to a great extent be derived from existing traditional payment systems like credit cards and cheques. The parties involved will mostly be interested in being authenticated in order to protect themselves from fraud or error. The information exchange must be secure and confidential to avoid eavesdroppers gaining access to details of the transaction. Payment of the money must be ensured via online verification.

The SET (see section 4.47) protocol by MasterCard and VISA is most likely to be the dominating protocol. Microsoft, Netscape, CyberCash, IBM and most other major players are supporting the protocol and are currently developing new or re-engeneering existing payment systems in a SET compliant way. Currently used systems for secure credit card presentation like SSL or SHTTP will recede before these SET compliant payment systems.

5.2.2 Small Payments

One point of view is, that small payments (from at least 0.1 USD) are best performed in a cash like manner, cash like properties such as customer anonymity and untraceability are to be guaranteed and forgery must be prevented. Also multicurrency solutions are required to enable world wide acceptance.

Chipcard based systems like Geldkarte (see section 4.20) are most likely to dominate in this area due to their increased security, offline and scalability properties. Other examples of major cash like payment systems that support small, but not especially micropayments are CAFE (see section 4.7), Digicash Ecash (see section 4.16), Mondex (see section 4.29 or NetCash (see section 4.34).

The other point of view to small payments is, that small change payments transactions are to be viewed as notational just like macropayments. Here forgery becomes harder, but anonymity is less easy to secure. Example for a major notational micropayment system is CyberCoin (see section 4.14).

Which small payment system or systems will become dominant depends not only on user requirements, i.e. how important anonymity and untraceability are rated by the customers, but also on the legal context, i.e. what attitude governments are taking towards these issues. If legislation considers anonymous and untraceable digital payments undesirable, such payment systems will not be able to gain a major market position.

5.2.3 Micropayments

With micropayments (until fractions of a Cent) the situation is unclear at the moment. Which system or systems will gain a wider acceptance cannot be determined at the present time.

Most of the micropayment systems support just repeated payments at the same merchant really efficient. Token systems, that work well with repeated shopping are localized schemes like MilliCent (see section 4.27), which is currently in public trial, or chained hash systems like PayWord (see section 4.40). A repeated payments account based system is SubScrip (see section 4.48). These systems usually depend on some macropayment system or other expensive operation for the initial transaction.

Example for a major notational micropayment system, that could support unrelated occasional payments in a practical manner, is Mini-Pay (see section 4.28), which is currently going into a trial phase. It is not quite clear if the risk for merchants and customers is acceptable with this system.

Several highly complex theoretical schemes are plain unpractical. E.g. LotteryTickets (see section 4.24), a specialized proposal for high frequency non-repeated micropayments, which due to its unpredictability most probably will not gain any user acceptance. E.g. MicroMint (see section 4.26), a specialized proposal for occasional non-repeated micropayments, who claims enormous investment effort requirements from potential issuers.

6 Certification Authorities

6.1 VeriSign

Web Resource	[Ver96b]
Name	VeriSign
Origin	VeriSign Inc.
Aim	Certification authority.
Status & Milestones	Operational, ?
Prerequisites	Smart card

Table 95: VeriSign Feature Profile

VeriSign is a digital certification service provider. It uses smart cards on which can be issued online a VeriSign Class 1 Digital IDsSM certificate. This portable authentication enables users to access their business and personal information in an authenticated manner anywhere.

VeriSign cooperates with smart card producer Schlumberger, smart card reader producer Litronic and Microsoft. These cards can be used with MS Internet Explorer at all merchants accepting VeriSign Digital IDs.

6.2 GTE Cybertrust

Web Resource	[GTE96]
Name	GTE Cybertrust
Origin	GTE CyberTrust Solutions Inc.
Aim	Certification authority.
Status & Milestones	Operational, ?
Payment Model	Certification authority

Table 96: GTE Cybertrust Feature Profile

GTE CyberTrust Solutions Inc. claims to be of the largest publicly held telecommunications companies in the world, their annual revenues and sales exceeding 21 billion USD.

GTE provides certification authority (CA) products and services for use by financial institutions, corporate enterprises and government agencies to secure a wide range of network-based applications. GTE acts as CA for Secure Electronic Transactions (SET) and Secure Sockets Layer (SSL)

Web Resource	[BIP96]
Name	BIPS
Origin	FSTC.
Aim	Electronic banking infrastructure.
Status & Milestones	Research project since 1996.
Prerequisites	Special SW and HW.

Table 97: BIPS Feature Profile

7 Payment Interface Projects

7.1 BIPS

The Bank Internet Payment System (BIPS) aims to support merchants and customers to process electronic payments over the Internet by developing several components that are necessary to support secure electronic transactions:

- An architecture
- An open specification
- A secure methodology for spontaneous payment instructions to be initiated over open public networks.
- A standard interface to existing bank payments systems.

BIPS is sponsored by a consortium of leading technology banks and will focus on encouraging companies to initiate a variety of payment transactions via the Internet through increased system security.

BIPS project participants to date are among others Citibank, Concept Five Technologies, Inc., Fujitsu Research Institute, Glenview State Bank, GlobeSet Inc., Mellon Bank , NCR, Tandem Computers Inc., CommerceNet, the Retail Payments Office of the Federal Reserve System and SWIFT.

The BIPS project aims to demonstrate the feasibility of a secure, reliable, comprehensive and widely available infrastructure by designing, developing and integrating the components necessary for protecting and linking existing back-end payments systems with banking corporate customers over open public networks. It targets to produce a specification for a secure server that banks will use to provide payment transaction services on the Internet. Goals are:

- Allow payers and payees to agree on payment terms and mechanisms.
- Be able to access multiple bank payments systems, enabling customers and banks to choose the most cost-effective way to make a payment.
- Provide the intelligence to select the appropriate payment mechanism for the payer based on the payer requirements for cost and

- Provide online authentication of payers and payees and authorization for the transaction.

Goal of the Electronic Payments project of FSTC (see section 4.19 is to design and demonstrate feasibility of an infrastructure which will support electronic commerce and other online business and personal financial transactions by providing a secure, reliable, comprehensive and widely available infrastructure for making payments via the existing banking system.

Such an infrastructure benefits banks by allowing them a consistent, secure, trusted way offering the full range of banking products to consumer and corporate customer base. It also allows for the offering of innovative new products which take advantage of new developments in telecommunications technology and enhancements to the existing banking payments system.

7.2 InterPay/UPAI

Web Resource	[Ket96]
Name	Interpay/UPAI
Origin	H. Garcia-Moulina, S. Ketchpel, et.al., Stanford digital libraries project.
Aim	Protocol for payment system integration.
Status & Milestones	Research project since 1995, claim to have implemented a prototype.
Prerequisites	Special SW.

Table 98: InterPay/UPAI Feature Profile

InterPay and UPAI unifying access to payment systems. Layered architecture. Stanford digital libraries project.

References: [CKP$^+$95] [KHGMP$^+$96] [C$^+$95] [Ket95]

7.3 IPAY

Web Resource	[IPA96]
Name	IPAY
Origin	IMC
Aim	Protocol for for automated payment negotiation between computers and merchant offer structures.
Status & Milestones	Research project since April, 1997.
Prerequisites	Special SW.

Table 99: IPAY Feature Profile

Draft from the IETF Payment Working Group. The working group shall have three deliverables:

1. Negotiation of payment scheme and protocol.
2. Transport of the payment messages.
3. Methods for merchant offer of goods and prices.

Proposal to submit offer specification protocol for proposed standard in April 1997, but no published results yet.

7.4 JECF

Web Resource	[JEC97]
Name	JECF
Origin	Sun, Javasoft.
Aim	Protocol for payment system integration.
Status & Milestones	Development project since 1996.
Prerequisites	Special SW.

Table 100: JECF Feature Profile

Sun Javasoft unifying access to payment systems.

7.5 JEPI

Web Resource	[JEP97]
Name	JEPI
Origin	W3 consortium, CommerceNet, CyberCash, Microsoft, NetBill, OSF, and OpenMarket, et.al.
Aim	Protocol for automated payment negotiation between computers, determining the most appropriate payment mechanism for the transaction on hand.
Status & Milestones	Research project since December 1995.
Prerequisites	Most probably smart cards and SW.

Table 101: JEPI Feature Profile

The Joint Electronic Payments Initiative (JEPI) is designed to enable automated payment negotiation between computers.

It is a project from the W3C consortium to design a protocol to enable systems to negotiate payment capabilities automatically. They aim at the following two main issues:

1. A general purpose negotiation protocol based on PEP (Protocol Extension Protocol). This allows a Web client and server to ask one another what extension modules they support, negotiate parameters for these extensions, and ask the other end to commence using an extension if possible. This work is being folded into the specifications of HTTP 1.2 through the IETF processes.

2. A specific extension module, UPP (Universal Payment Preamble), used to negotiate over the payment instrument (cheque, credit card, debit card, electronic cash, etc.), brand (Visa, MasterCard, American Express, etc.), and payment protocol (SET, CyberCash, GlobeID, etc.).

Participants include:

- Browser vendors: Microsoft.
- Server vendors: IBM and Open Market.
- Payment systems: CyberCash and GCTech
- Merchants: Xerox and British Telecom.
- Additional Design Input: Digital Equipment Corporation and VeriFone.

JEPI will be designed to act as a general system into which payment mechanisms can be embedded and will therefore contain minimal payment properties of its own. However properties of the JEPI protocol could maybe restrict the use of certain payment mechanisms, e.g. with respect to anonymity. Several Internet drafts have been put together detailing these protocols.

References: [Eas97], [EKM97], [Kha97]

7.6 SEMPER/iKP

Web Resource	[SEM97]
Name	Semper/iKP
Origin	Waidner, M. et.al. from IBM, Zuerich
Aim	Protocol for automated payment negotiation and payment system integration. Generic payment system.
Status & Milestones	Research project since 1996.
Prerequisites	Special SW.

Table 102: SEMPER/iKP Feature Profile

IBM Swizerland SEMPER and iKP unifying access and payment system selection generic payment service project.

References

[ACC97] ACC. Home page, 1997. http://portal.research.bell-labs.com/lateinfo/projects/ecom.html.

[Ago97] Agora. Home page, 1997. http://www.bell-labs.com/user/eran/agora.html.

[AIM97] AIMP. Home page, 1997. http://portal.research.bell-labs.com/lateinfo/projects/ecom.html.

[AJSM97] N. Asokan, P. Janson, M. Steiner, and Waidner M. Electronic payment systems. Technical Report 211ZR019, IBM Zurich Research Laboratory, April 1997. http://www.semper.org/info/211ZR019.ps.gz.

[AMS96] R. Anderson, C. Manifavas, and C. Sutherland. Netcard - a practical electronic cash scheme,. In *Cambridge Workshop on Security Protocols*, 1996. http://www.cl.cam.ac.uk/users/cm213/Publications/netcard.ps.

[Ano97] Anonymous. Mondex's pilot system broken. Web Page, September 1997. http://jya.com/mondex-hack.htm.

[APASW96] J.L. Abad-Peiro, N. Asokan, M. Steiner, and M. Waidner. Designing a generic payment service. Technical Report 212ZR055, IBM Zurich Research Laboratory, November 1996. http://www.semper.org/info/212ZR055.ps.gz.

[ATS97] ATS. Home page, 1997. http://www.atsbank.com.

[Ban97] BankNet. Home page, 1997. http://mkn.co.uk/bank.

[Bar97] D. Barnes. Identity agnostic online cash. Web Page, 1997. http://www.c2.net/~cman/agnostic.html.

[BBC+94] J-P. Boly, A. Bosselaers, R. Cramer, R. Michelsen, S. Mjlsnes, F. Muller, T. Pedersen, B. Pfitzman, P. de Rooij, B. Schoenmaers, M. Schunter, L. Valle, and M. Waidner. The esprit project cafe - high security digital payment systems. In *Sicherheit in netzgestützten Informationssystemen, LNCS 875*. ESORICS'94, Third European Symposium on Research in Computer Security, Brighton, Springer-Verlag, Berlin-Heidelberg, 1994. http://www.informatik.uni-hildesheim.de/FB4/Projekte/sirene/publ/BBCM1_94CafeEsorics.ps.gz.

[BGW+95] T.J Bellare, J.A. Garay, M. Waidner, et al. ikp – a family of secure electronic payment protocols. In *1st USENIX workshop on Electronic Commerce*, July 1995. http://www.zurich.ibm.ch/Technology/Security/publications/1995/ikp.ps.

[BIP96] BIPS. Home page, 1996. http://www.fstc.org/projects/bips.

[Bra93] S. Brands. Untraceable off-line cash in wallet with observers. In *LNCS 773*, pages 302–318. Advances in Cryptology - CRYPTO '93, Springer Verlag, 1993. http://www.cwi.nl/ftp/brands/crypto93.ps.Z.

[Bra94] S. Brands. Off-line cash transfer by smart cards. In *First Smart Card Research and Advanced Application Conference*, pages 101–117, Lille (France), 1994. http://www.cwi.nl/ftp/brands/CS-R9455.ps.Z.

[Bra95a] S. Brands. Off-line electronic cash based on secret-key certificates. In *LATIN'95*, Valpara'iso, Chile, April 1995. http://www.cwi.nl/ftp/brands/latin95.ps.Z.

[Bra95b] S. Brands. Publications on electronic cash. Web Page, 1995. http://www.cwi.nl/˜brands/cash.html.

[Bra95c] S. Brands. Restrictive blinding of secret-key certificates. In *LNCS 921*, pages 231–247. Advances in Cryptology - EUROCRYPT '95, Springer Verlag, 1995. http://www.cwi.nl/ftp/brands/CS-R9509.ps.Z.

[BSK89] B. Bryant, J. Steiner, and J. Kohl. *Kerberos Installation Notes, DRAFT Initial Release, patch level 7*, January 1989. ftp://aeneas.mit.edu/pub/kerberos/doc.split/installation.ps.

[C+95] S. Cousins et al. InterPay: Managing multiple payment mechanisms in digital libraries. In *DL '95 proceedings*, 1995. http://csdl.tamu.edu/DL95/papers/cousins/cousins.html.

[CB97] D. Chaum and S. Brands. Minting electronic cash. *IEEE Spectrum*, pages 30–34, February 1997.

[CDS+96a] CWI, DigiCash, Siemens, et al. The cafe project, 1996. http://www.cwi.nl/cwi/projects/cafe.html.

[CDS+96b] CWI, DigiCash, Siemens, et al. The opera project, 1996. http://www.cwi.nl/cwi/projects/opera.html.

[Cen96] Digital Equipment Research Center. Millicent. Web Page, 1996. http://www.research.digital.com/SRC/millicent/.

[Cen97] Digital Equipment Research Center. Millicent frequently asked questions. Web Page, 1997. http://www.research.digital.com/SRC/millicent/pages/faq.html.

[CFN88] D. Chaum, A. Fiat, and M. Naor. Untraceable electronic cash. In S. Goldwasser, editor, *Advances in Cryptology*, pages 319–327. Crypto '88, Springer-Verlag, 1988.

[Cha82] D. Chaum. Blind signatures for untraceable payments. In D. Chaum, Rivest R.L., and A.T. Sherman, editors, *Advances in Cryptology*, pages 199–203. Crypto '82, 1982.

[Cha89] D. Chaum. Online cash checks. In J.J. Quisquater and J. Vandewalle, editors, *Advances in Cryptology*, pages 288–293. EUROCRYPT '89, Springer-Verlag, 1989. http://www.digicash.com/publish/online.html.

[Cha92] D. Chaum. Achieving electronic privacy. *Scientific American*, pages 96–101, August 1992. http://www.digicash.com/publish/sciam.html.

[Cha94] D. Chaum. Prepaid smart card techniques: A brief introduction and comparison. Web Page, 1994. http://www.digicash.com/publish/cardcom.html.

[Cha95] D. Chaum. Security without identification: Card computers to make big brother obsolete. Web Page, 1995. http://www.digicash.com/publish/.

[Che97] CheckFree. Home page, 1997. http://www.checkfree.com.

[CKP+95] S.B. Cousins, S.P. Ketchpel, A. Paepke, H. Garcia-Moulina, et al. Interpay: Managing multiple payment mechanisms in digital libraries. In *The Second Annual Conference on the Theory and Practice of Digital Libraries*. Digital Libraries 95, June 1995. http://www.csdl.tamu.edu/DL95/papers/cousins/cousins.html.

[Cli97] ClickShare. Home page, 1997. http://www.clickshare.com.

[Com97] CommercePOINT. Home page, 1997. http://www.internet.ibm.com/commercepoint/payment.

[Con97] World Wide Web Consortium. W3c electronic payments area, 1997. http://www.w3.org/pub/WWW/Payments.

[CPS95] J. Camenisch, J.-M. Piveteau, and M. Stadler. Faire anonyme zahlungssysteme. In *Herausforderungen eines globalen Informationsverbundes für die Informatik*, pages 254–265. GISI 95, Springer Verlag, 1995.

[CST95a] L.J. Camp, M. Sirbu, and J.D. Tygar. Token and notational money in electronic commerce. In *Usenix Workshop on Electronic Commerce*, July 1995. http://almond.srv.cs.cmu.edu/afs/cs/user/jeanc/www/usenix.html.

[CST95b] L.J. Camp, M. Sirbu, and J.D. Tygar. Token and notational money in electronic commerce. In *Usenix 1995*, 1995. http://www/cs/cmu.edu/afs/cs.cmu.edu/user/jeanc/www/usenix.html.

[Cyb96a] CyberCash. Corporate profile, May 1996.

[Cyb96b] CyberCash. Cybercash launches cybercoin[tm] service, press release, September 1996. http://www.cybercash.com/cybercash/news/releases/1996/96sept30.html.

[Cyb97a] Cybank. Home page, 1997. http://www.cybank.net.

[Cyb97b] CyberCash. Acquiring internet transaction (financial services white paper, 1997. http://www.cybercash.com/cybercash/wp/bankwp.html.

[Cyb97c] CyberCash. Cybercash and german banks dresdner bank and sachsen lb form a working group to offer secure internet transactions in germany, press release, March 1997. http://www.cybercash.com/cybercash/news/releases/1997/97mar07dresdner.html.

[Cyb97d] CyberCash. Ensuring secure payment for internet commerce (merchant services white paper, 1997. http://www.cybercash.com/cybercash/wp/merchwp.html.

[Cyb97e] CyberCash. Introducing cybercoin, 1997. http://www.cybercash.com/cybercash/shoppers/coingenpage.html.

[Cyb97f] CyberCash. The six steps in a secure internet credit card payment, 1997. http://www.cybercash.com/cybercash/info/sixsteps.html.

[Cyb97g] CyberCents. Home page, 1997. http://www.outreach.com.

[Dav97] R. Davies. Money - past, present & future. Technical report, Exeter University, 1997. http://www.ex.ac.uk/~RDavies/arian/money.html.

[Die97] C. Dietze. Systembeschreibung geldkarten-internet-haendlerterminal. Technischer Bericht, Giesecke & Devrient, December 1997.

[Die98] C. Dietze. Slides about the geldkarte im internet proposal, January 1998.

[Dig95] DigiCash. Digital signatures and smart cards, 1995. http://www.digicash.com/publish/digsig/digbig.html.

[Dig96a] DigiCash. Ecash issuers. Web Page, 1996. http://www.digicash.com/ecash/ecash-issuers.html.

[Dig96b] DigiCash. Ecash payment mechanism. Web Page, 1996. http://www.digicash.com/ecash/shop/paymethod.html.

[Dig96c] DigiCash. Ecash trial. Web Page, 1996. http://www.digicash.com/ecash/trial.html.

[Dig97a] Digicash. Home page, 1997. http://www.digicash.com.

[Dig97b] Digicash. An introduction to ecash. Web Page, 1997. http://www.digicash.com/publish/ecash_intro/ecash_intro.html.

[Eas97] D. E. Eastlake. Universal payment preamble. Web Page, Work in Progress, 1997. http://www.w3.org/pub/WWW/Payments/specs/upp.txt.

[EBCY95] D. Eastlake, B. Boesch, S. Crocker, and M. Yesil. CyberCash credit card protocol version 0.8. Internet Draft, July 1995. ftp://ds.internic.net/internet-drafts/draft-eastlake-cybercash-v08-00.txt.

[EKM97] D. E. Eastlake, R. Khare, and J. Miller. Selecting payment mechanisms over http. Web Page, Work in Progress, 1997. http://www.w3.org/pub/WWW/Payments/JEPI/UPPFlow.html.

[eVe97] eVend. Home page, 1997. http://www.evend.com.

[Faj96] R. Fajen. Electronic payment schemes on the internet and their influence on electronic commerce. Technical report, TU Dresden, 1996. http://rcs.urz.tu-dresden.de/~marvin.

[Fir96] FirstVirtual. Home page, 1996. http://www.fv.com.

[FST97a] FSTC. Electronic payments infrastructure: Design considerations, 1997. http://www.fstc.org/projects/echeck.

[FST97b] FSTC. Fstc electronic check project, 1997. http://www.fstc.org/projects/echeck/index.html.

[FST97c] FSTC. Home page, 1997. http://www.fstc.org.

[GCT97] GCTech. Home page, 1997. http://www.gctec.com.

[Gie97] Giesecke&Devrient. Home page, 1997. http://www.gdm.de.

[Glo97] GlobeID. Home page, 1997. http://globeid.gctech.fr.

[GMA+95] S. Glassman, M. Manasse, M. Abadi, P. Gauthier, and P. Sobalvarro. The millicent protocol for inexpensive electronic commerce. In *4th International World Wide Web Conference*, December 1995. http://www.research.digital.com/SRC/millicent/papers/millicent-w3c4/millicent.html.

[Gmb98] CyberCash GmbH. Cybercash germany. Web Page, 1998. http://www.cybercash.de.

[Gol96] I. Goldberg. Some thoughts on an api for ecash. Web Page, 1996. http://HTTP.CS.Berkeley.EDU/˜iang/ecashapi.

[GS96] E. Gabber and A. Silberschatz. Agora: A minimal distributed protocol for electronic commerce. In *2nd USENIX workshop of electronic commerce*, November 1996. http://www.bell-labs.com/user/eran/agora-ec96.ps.

[GTE96] GTE. Home page, 1996. http://www.cybertrust.gte.com.

[HB+95] P. Hallam-Baker et al. W3c micro payment transfer protocol - mptp. Web Page, Work in Progress, 1995. http://www.w3.org/pub/WWW/TR/WD-mptp.

[Het97] R. Hettinga. The e$ home page, 1997. http://www.shipwright.com.

[HSW96] R. Hauser, M. Steiner, and M Waidner. Micro-payments based on ikp. Technischer Bericht RZ 2791, IBM Research, T.J. Watson Research Center & Zürich Research Lab, February 1996. http://www.zurich.ibm.ch/Technology/Security/publications/1996/HSW96.ps.gz.

[HT97] N. Hardy and E.D. Tribble. The digital silk road, draft, 1997. http://www.webcom.com/˜agorics/dsr.html.

[HY97] A. Herzberg and H Yochai. Mini-pay : Charging per click on the web. In *6th International World Wide Web Conference*, Network Computing and Security Group, IBM Research - Haifa Research Lab - Tel-Aviv Annex, April 1997. http://www6.nttlabs.com/HyperNews/get/PAPER99.html.

[iKP97] iKP. Home page, 1997. http://www.zurich.ibm.com/Technology/Security/extern/ecommerce/iKP.ht

[Inc96] CyberCash Inc. Home page, 1996. http://www.cybercash.com.

[Int97] InterCoin. Home page, 1997. http://www.intercoin.com.

[IPA96] IPAY. Home page, 1996. http://www.imc.org/ietf-pay/ietf-pay-charter.

[JEC97] JECF. Home page, 1997. http://java.sun.com/products/commerce.

[JEP97] JEPI. Home page, 1997. http://www.w3.org/pub/WWW/Payments/JEPI.html.

[JO97] S. Jarecki and A.M. Odlyzko. An efficient micropayment system based on probabilistic polling. In *Financial Cryptography 1997, Lecture Notes in Computer Science No. 1318*, pages 173–191. AT&T, Springer-Verlag Berlin-Heidelberg, 1997. http://www.research.att.com/˜amo/doc/polling.ps.

[Jon96] T. Jones. Mondex on 'the future of money'. Submission to the US House of Representatives, 1996. http://www.mondex.com/hserep.htm.

[Ket95] S. Ketchpel. Transaction protection for information buyers and sellers. In *DAGS '95 - Electronic Publishing and the Information Superhighway*, 1995. http://robotics.stanford.edu/users/ketchpel/dags4.html.

[Ket96] S.P. Ketchpel. Interpay: A project in the stanford digital library. Web Page, 1996. http://robotics.stanford.edu/~ketchpel/diglib/interpay.html.

[Kha97] R. Khare. Http/1.2 extension protocol (pep). Web Page, Work in Progress, 1997. http://www/w3/org/pub/WWW/TR/WD-http-pep.html.

[KHGMP+96] S. Ketchpel, H. Hector Garcia-Molina, P. Paepcke, S. Hassan, and S. Cousins. Upai: A universal payment application interface. Technischer Bericht - Work in Progress SIDL-WP-1996-0039, Stanford University, September 1996. http://www-diglib.stanford.edu/diglib/WP/PUBLIC/DOC97.ps.

[Kle97] Kleline. Home page, 1997. http://www.kleline.com.

[KLM94a] D. Kristol, S. Low, and N. Maxemchuck. Anonymous credit cards. In *Globecom'94*, 1994. ftp://ftp.research.att.com/dist/anoncc/anoncc.ps.Z.

[KLM94b] D. Kristol, S. Low, and N Maxemchuck. Anonymous internet mercantile protocol. Technical report, AT&T Bell Labs, March 1994. ftp://ftp.research.att.com/dist/anoncc/accinet.ps.Z.

[LL96] D.C. Lynch and L. Lundquist. *Digital Money: The New Era of Internet Commerce*. John Wiley & Sons, 1996.

[LMP94] S. Low, N Maxemchuck, and S. Paul. Collusion in a multiparty communication protocol for anonymous credit cards. In *IEEE/ACM Transactions on Networking*, 1994. ftp://ftp.research.att.com/dist/anoncc/collude.ps.Z.

[LSS96] L. Law, S. Sabett, and J. Solinas. How to make a mint: The cryptography of anonymous electronic cash. Technical report, National Security Agency, October 1996. http://jya.com/nsamint.htm.

[Mag97] MagicMoney. Home page, 1997. http://www.unicorn.com/pgp/mm-readme.html.

[Man95] M. Manasse. The millicent protocols for electronic commerce. In *1st USENIX workshop on Electronic Commerce*. USENIX, July 1995. http://www.research.digital.com/SRC/millicent/papers/mcentny.htm.

[Mil97] MilliCent. Home page, 1997. http://www.millicent.digital.com.

[MMW97] J. MacKie-Mason and K. White. Evaluating and selecting digital payment mechanisms. Technical report, School of Information, University of Michigan, November 1997. http://www-personal.umich.edu/~jmm/papers/digidoll.pdf.

[MN93] G. Medvinsky and B.C. 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.

[Mon96] Mondex. Home page, 1996. http://www.mondex.com.

[MP97] Mini-Pay. Home page, 1997. http://www.ibm.net.il/ibm_il/int-lab/mpay.

[MS96] MasterCard-SET. Home page, 1996. http://www.mastercard.com/set.

[Net96a] NetBill. Home page, 1996. http://www.netbill.com/.

[Net96b] NetCard. Home page, 1996. http://www.cl.cam.ac.uk/users/cm213/Project.

[Net96c] NetCash. Home page, 1996. http://nii-server.isi.edu/info/netcash.

[Net96d] NetCheque. Home page, 1996. http://gost.isi.edu/info/netcheque.

[Net96e] NetFare. Home page, 1996. http://www.netfare.com.

[New97] NewShare. Home page, 1997. http://www.newshare.com.

[NM95] B.C. Neuman and G. Medvinsky. Requirements for network payment: The netcheque perspective. In *COMPCON'95*, San Francisco, March 1995. IEEE. ftp://propsero.isi.edu/pub/papers/security/netcheque-requirements-compcon95.ps.

[Ope96] OpenMarket. Home page, 1996. http://www.openmarket.com.

[oPS96] Committee on Payment and Settlement Systems. Security of electronic money. Technical report, G10, 1996. http://www.bis.org/publ/cpss18.htm.

[Owe97] C. A. Owen. Internet micro payment protocols, 1997.

[Pay96] PayMe. Home page, 1996. http://www.w3.org/Conferences/WWW4/Papers/228.

[Ped95] T. Pedersen. Electronic payments of small amounts. Technical Report DAIMI PB-495, Aarhus University, Institut für Informatik, Aarhus, Denmark, August 1995.

[PP96] PC-Pay. Home page, 1996. http://www.innovonics.com/pcpay/pcpayhome.html.

[RB96] M. T. Rose and N. S. Borenstein. The simple mime exchange protocol, 1996. http://www.fv.com/pubdocs/smxp-spec.txt.

[RC96] Redi-Check. Home page, 1996. http://www.redi-check.com.

[Ric96] D. Richards. Requirements analysis for library accounting systems. In *Elektronisches Publizieren und Bibliotheken*. Bibliothek der Universität Bielefeld, February 1996. http://www.ub.uni-bielefeld.de/aktuell/kongress/vortraeg/richard.htm.

[Ric97] S. Richards. The electronic banking resource center. Technical report, Ohio State University, 1997. http://www2.cob.ohio-state.edu/˜richards/banking.htm.

[Riv92] R.L. Rivest. The md5 message digest algorithm. Internet RFC 1321, April 1992. http://theory.lcs.mit.edu/~rivest/Rivest-MD5.txt.

[Riv97] R. Rivest. Electronic lottery tickets as micropayments. In *Proceedings of Financial Cryptography '97*, February 1997. http://theory.lcs.mit.edu/~rivest/lottery.ps.

[RS95] R.L. Rivest and A. Shamir. Payword and micromint–two simple micropayment schemes. To Appear at the RSA '96 Conference, May 1995. http://theory.lcs.mit.edu/~rivest/RivestShamir-mpay.ps.

[San96] Sandia. Home page, 1996. http://www.cs.sandia.gov/HPCCIT/el_cash.html.

[Sch96] B. Schneier. *Applied Cryptography, 2nd Ed.* Wiley, 1996.

[Sec96] SecureCourier. Home page, 1996. http://www.netscape.com/newsref/std/credit.html.

[SEM97] SEMPER. Home page, 1997. http://www.semper.org.

[SET97a] SET. Set business description, 1997. http://www.visa.com/cgi-bin/vee/sf/set/setbus.html.

[SET97b] SET. Set programmers' guide, 1997. http://www.visa.com/cgi-bin/vee/sf/set/setprog.html.

[SET97c] SET. Set protocol description, 1997. http://www.visa.com/cgi-bin/vee/sf/set/setprot.html.

[Sir97] M. Sirbu. Credits and debits on the internet. *IEEE Spectrum*, pages 23–29, February 1997.

[SPC96] M. Stadler, J.-M. Piveteau, and J. Camenisch. An efficient fair payment system. In *CCS'96*, pages 88–94, New Delhi, India, 1996. ACM. ftp://ftp.inf.ethz.ch/pub/publications/papers/ti/isc/acm_ccs.ps.

[SSBR96] L. H. Stein, E. A. Stefferud, N. S. Borenstein, and M. T. Rose. The green commerce model, 1996. http://www.fv.com/pubdocs/green-model.txt.

[ST95] M. Sirbu and J.D. Tygar. Netbill: An internet commerce system optimized for network delivered services. In *COMPCON'95*, San Francisco, March 1995. IEEE. http://www.ini.cmu.edu/netbill/pubs/CompCon_TOC.html.

[Sub96] SubScrip. Home page, 1996. http://www.cs.newcastle.edu.au/Research/afurche/subscrip.ps.

[SW95] M. Schunter and A. Weber. News from cafe – the high security digital payment system, June 1995. http://www.informatik.uni-hildesheim.de/FB4/Projekte/sirene/publ/ScWe_95CafeNews.ps.gz.

[SW97] A. Schoeter and R. Willmer. Digital money online. Technical report, Intertrader Ltd., 1997. http://www.intertrader.com/library/DigitalMoneyOnline/dmo/dmo.htm.

[Ver96a] VeriFone. Home page, 1996. http://www.verifone.com/products/commerce.

[Ver96b] VeriSign. Home page, 1996. http://www.verisign.com.

[Via96] ViaCheck. Home page, 1996. http://theyellowpages.com/Viacheck.

[VS96] VISA-SET. Home page, 1996. http://www.visa.com/cgi-bin/vee/sf/set/intro.html?2+0.

[Whe96] D. Wheeler. Transactions using bets, April 1996. ftp://ftp.cl.cam.ac.uk/users/djw3/tub.ps.

[Zwi96] S. Zwissler. *Methodischer Systementwurf für den elektronischen Handel*. PhD thesis, Universität Karlsruhe, April 1996.