

From

**Internet, strategic and practical guide for the
entreprise¹**

by

Jean Haguet

© Reprinted with the authorization of Masson
publishing

¹ © Internet, guide stratégique et pratique pour l'entreprise, Paris, June 1996, 352 pp

Chapter 15

Transactions

The Internet represents a challenge for both commercial online transactions and security. To date, the Net is principally used as a support for promotion and advertising: once consumers are hooked, they order the goods via the usual channels. Most commercial servers still follow this approach; nevertheless, the real interest in using the Internet is to allow to carry out online transactions from one point to another, notably, instantaneously and automatically.

This constitutes a triple challenge:

- If Internet is not secure, how to guarantee the confidentiality of the transactions?
- How can consumers and Merchants authenticate each other?
- How can the management of a company integrate these new forms of transactions?

The number and diversity of systems already existing to solve these problems is surprising. Three models arise: the electronic currency (or Ecash) that is transmitted from one hard disk to another via the Internet under the form of encrypted unique codes; the second model relies on a direct link between the consumer and the merchant; and the third one tries to avoid sending sensitive data over the network through the use of an intermediary.

All models are faced with characteristic constraints that affect open networks such as Internet. First these constraints will be identified. Then, the various payment systems implemented to date will be described and classified.

15.1. ELECTRONIC COMMERCE ON OPEN NETWORKS

Five basic constraints can be identified: blending the new and the old, integrating the transactions within the banking system, ensuring the intermediation, encrypting and authenticating, and managing the online transactions. These restrictions will be examined one by one.

15.1.1. Blending the new and the old

The Internet will undoubtedly provoke a revolution in the commercial praxis –at least in the long term. However, this revolution will evolve slower than has been proclaimed by some publications. Furthermore, commerce conforms to constant parameters. Therefore, the first characteristic of a transaction on the Internet is a blending of new and old, and it is necessary to decide on where to establish the boundary:

- Which procedures resemble the real world ones, and how can this be reflected ?
- Which procedures are actually new, and how can these be managed ?

The Internet creates a new risk: online transactions may not leave any trace if performed as an electronic-only operation. Unscrupulous business people could be tempted to avoid taxation or the regulations pertaining to their legal status, customs and administrative controls. They could also try to perpetrate frauds, using fake identities and addresses, or even stolen instruments of payment (namely, bank card numbers).

Therefore, applying the usual government controls to network transactions is desirable, as trust is the essential condition for the development of Internet-based commerce. Merchants and consumers will not participate in this new market, if they do not feel protected against fraud. Therefore, a payment system has to include some checking devices to allow for control: for example, stubs with time and date as a proof of transaction; or a system to authenticate the transaction participants. The existing control structures will face a new challenge that comes from the Internet. Unprecedented means will be necessary to cope with it.

For these reasons, control mechanisms should not become an obstacle to the development of electronic commerce through Internet. From now on, the current regulations should show enough flexibility to accept these transactions. On the other hand, trying to regulate wherever a possible breach could show up would be wrong. It is recommended to first observe the development of this sector, before nipping it in the bud. This is the position adopted by the American authorities. The US Congress has already summoned a number of expert hearings to identify possible flaws of Internet, so as to be prepared for a rapid intervention. While awaiting possible new regulations, the current ones could satisfy present needs.

Furthermore, Internet relies on the current distribution channels for sending "physical" goods. Nobody has found how wine or cars may be sent through the "pipes" of the Network: resorting to a retailer or a concessioner is still necessary, even if they are several thousands of miles away. Goods are then delivered through traditional channels. Internet is only used for communication and payment. In return, Internet consists of a distribution network for digital goods (information, software, books, videos, services, technical papers, etc.). Therefore, the distribution channels will follow old or new patterns, depending on the type of goods being transferred.

For the sake of security, everything can be safely transmitted online, except sensitive data (e.g., bank card numbers). Traditional communication means (telephone, fax, and mail) could be envisaged for these. Some American companies even ask consumers who wish to use E-mail to send two separate messages: one containing the credit card number, and the other indicating the expiration date. This attempts to elude 'sniffing'¹ programs so that the information cannot be intercepted. Even if one message out of the two is captured, the information is not

¹'Sniffing' is defined as the interception of data circulating through Internet. The hacker sets a program that systematically identifies and traps certain types of data.

complete and, therefore, not exploitable. For the company, this obviously implies a dedicated E-mail management system for rebuilding the fragmented information.

Sensitive data is usually encrypted to process online transactions from point to point. Asymmetric cryptography, thanks to electronic signatures, can also be used to authenticate the transaction partners and ensure the integrity and acceptability of messages. These techniques – or at least their intensive application – represent an innovation in the commercial world.

Last but not least, a transaction entails a payment. Many intermediaries offering specific services (transaction certification, clearing, mutual authentication of consumer and merchant, provision of account statements, EDI integration, etc...) have appeared on the Internet environment, but for the payment itself the Net has to rely on the banking system.

15.1.2. Integrating transactions within the banking system

Contrary to what may appear, the Internet does not represent a threat but rather an opportunity for banks and other financial institutions. In the first place, there is practically no advocate of Internet online transactions who would contemplate developing a system parallel to that of the banks. Even Digicash, the leader of Ecash, has no intention of emitting money by itself, but rather sell a licence of its system to banks.

This is due to a preeminent requirement: confidence. These transactions should inspire confidence among consumers and merchants in order to develop a transaction system on Internet. These consumers and merchants are unlikely to trust new parties with an unknown origin who will ask them to disclose their bank card numbers or other sensitive information. However, if consumers and companies know that well-established banks guarantee the validity of a payment system, they will be more inclined to sell and buy using Internet. Furthermore, there is a geographical criterion: the better known a bank (e.g., locally implanted), the greater the confidence. There is a limit of acceptance to virtual environments.

On the other hand, creating new structures would be too expensive. Relying on the local banking system is more simple and easier for virtual malls. Moreover, banks can bring their own consumers and contribute to an increase in the number of potential consumers. Additionally, legal aspects and regulations can also be a motivation. Banks know how to deal with administrative and litigious problems, and with commercial ventures (coverage, insurance, etc.). Furthermore, they can cover the financial risk associated with the use of bank cards (fraud, stealing) that might be greater today when using Internet rather than telephone as far as transmitting the card identification number is concerned. However, the perception of this risk is greater than its reality: Internet has still to attract a large number of users.

Finally, a number of online transactions rely on the use of bank and credit cards, thus implicitly on the banking system. This is true for systems based on the transmission of bank card numbers, but also for those using virtual wallets. In these cases, there

is no better partner than a bank. Visa, MasterCard, and Microsoft have set up a payment system for Internet, that specifically demands the integration into the banking network.

Banks must try to introduce innovations, and implement (at least) one payment system aimed at integrating Internet into their clearing scheme, or to contract new alliances with partners having a greater expertise on the Internet. To begin with, the banks should acknowledge the significance of Internet; they cannot allow themselves, in the long or short term, to ignore it. The Internet is at least a paradigmatic laboratory for the future information society.

15.1.3. Ensuring the intermediation

Intermediation consists in easing the transaction, by placing an instrument between the customer, the merchant, and the banking system. This is a typical role for this third type of system; either a specialized company or a bank can play it. Nevertheless, banks are at best partners in all the already existing systems.

Intermediating companies acting on the market are usually newcomers, building alliances with one or more banks (e.g., Globe ID™ with Compagnie Bancaire). They provide two main types of items: services and technology. Services encompass an added value of varying amount:

- actors' authentication,
- transaction confirmation,
- record certification,
- operation processing, clearing,
- profits distribution (fees),
- management of virtual wallets,
- provision of account statements, and
- filing.

Furthermore, intermediating companies sometimes offer ad hoc software, for consumers and for merchants. The first ones are always free-of-charge, the second ones are generally billed. These companies also propose encrypting programs embodied into programs and services being offered. The account statements can be transmitted to the merchants via EDI. However, this technology is of lesser importance than the special services provided by intermediating companies. A system such as First Virtual does not rely on any particular technology; it happens to be just a clever orchestration of all events incorporated in a transaction. Globe ID™ provides a little bit more technology – just enough to be better – for enabling real time transactions. [See below.]

15.1.4. Encrypting and authenticating

Online transactions over the Internet use encrypting and authentication procedures. Encrypting programs commonly use RSA technology, sometimes combined with traditional encryption methods. Many people consider cryptography a safe way to transmit bank card numbers. However, the best considered payment systems (Cybercash, First Virtual, Globe ID™) refuse to send sensitive information through the Internet, should they be encrypted or not. Open Market, Cybercash, and Globe ID™ accept it for opening an account, but only as an option. After that – depending on the system – only passwords, identifiers, and other payment orders are encrypted. First Virtual does not use encryption at all.

On the other hand, the Secure Web Norms (S-HTTP - Secure HyperText Transfer Protocol) and SSL (Secure Sockets Layer), and the Netcash system (for buying vouchers) require the transmission of the bank card number simultaneously to passing a purchase order. Ecash procedures rely, by definition, on encryption techniques. The unique codes representing specific currency values can be stolen, as may happen with a bank note. Therefore, they have to be protected (encrypted) while being transferred.

The mutual authentication of consumers and merchants can be endorsed by electronic signatures created by asymmetric encryption, but using more classical methods to authenticate the transaction participants is also possible. First Virtual uses E-mail to ask consumers and merchants for verification messages and specific identifiers.

Nevertheless, electronic signatures have the advantage of ensuring the integrity of the encrypted messages being transmitted. Hackers intercepting messages cannot alter them without vitiating the signatures. Moreover, the sender of a message cannot modify the contents of a sent message, nor can he repudiate it (reject his authorship).

Most transaction systems try to make encrypting procedures transparent to both consumers and merchants. It cannot be expected that the general public and commercial companies become skilled on encryption procedures. Globe ID™, for instance, asks its consumers to enter the information into the fields of an interactive questionnaire; then the program does the necessary.

15.1.5. Managing online transactions

Procedures need to be transparent; ideally they should also be automated. Another essential condition is swiftness, for consumers like transactions being immediately fulfilled. Online transactions will lose a great amount of their appeal if they are not immediately accomplished. An automated payment system gives the consumer the impression of achieving an instantaneous deal, as in a normal store. This is especially true for digital products (software) that can be delivered immediately.

Some payment systems also include management services, so that Merchants can delegate the functions of recording and filing. The intermediating companies can provide receipts and account statements. They can also directly integrate all transactions into the merchant's accounting system (using EDI). This is the

method adopted by Globe ID™. Furthermore, it is possible to conceive transactions based on deferred payments, subject to confirmation. In fact, some transactions have to be fulfilled after a certain delay. For example, a consumer that reserves a plane ticket gives the travel agent a reference of his bank account, but the agent cannot charge the due amount unless he can fulfill the desired travel conditions and get the traveler's approval. In such a case, the payment system would keep during this delay a record of the order passed by the consumer and obtain the necessary confirmations from both, the traveler and the travel agent. Once all confirmations are available, the transaction can be processed.

Based on the five constraints described above, several models of Internet transaction systems have been proposed. In the following section, several schema have been drawn to identify the various participants and summarize each step of the transaction. These schema can be superimposed for ease of comparison. Thick arrows represent the transmission of an encrypted bank card number via Internet. However, this often means just an option, telephone, fax and mail are possible alternatives. This will be described in detail for each model.

15.2. ECASH - ELECTRONIC CURRENCY

In the real world, there are several payment means: cash, cheques, bank transfers, bank and credit cards, travelers' cheques, etc. The same will occur within the cyberspace. Among the instruments envisaged for use on the networks, the most revolutionary one is probably Ecash.

15.2.1. Simple, cheap, anonymous.

Ecash is as easy to use as cash. It appears as a unique set of numbers -validated by a bank - representing a certain amount of cash. Most Ecash systems are based on coins of different value. Each set of digits identifies a coin and carries a serial number that makes it unique. These coins are stored on the customer's hard disk, or on a chip card. Serial numbers are stored in a database available to all banks.

If a consumer wishes to purchase, he transfers coins to the merchant's computer via Internet. The corresponding data is of course encrypted, but it is also validated by the electronic signature of the consumer's bank. The banks are actually the only agents allowed to issue Ecash to the owners of ordinary accounts, and it is up to them to adopt or not the use of Ecash. If they decide to do so, they have to set up a system of issuing and collecting. This system, which relies on a specific software, can be entirely integrated within their usual scope of operations. Ecash is just another instrument of payment.

It is possible to send Ecash to a merchant or any private user. This user can then spend this money or deposit it into his bank account. However, these coins can only be used once: if a person transfers Ecash to a second one, the later cannot forward this Ecash to a third individual without the intervention of his bank, which will exchange his coins with new ones so that these can be finally forwarded. Incidentally, Ecash converts all Internet users into potential merchants: anybody can sell his

literary production or his services as a consultant with a minimum of intermediation and at low cost.

The circulation of Ecash is regulated by ad hoc softwares and the procedures remain transparent to consumers and business people. This concedes the Ecash a great simplicity of use and, additionally, it avoids sending bank card numbers through the Internet. Given the automation due to computer operation, and the reduced number of steps for each transaction, Ecash has a very low cost. Therefore, its use is adequate for dealing with small amounts of money -from a few cents to a couple of hundred US dollars. Moreover, it could be envisaged to deal with smallest amounts, such as a cent fraction. Ecash is very well suited to sell information quantified by page, or even by paragraph.

Specifically, Ecash is potentially anonymous. Digicash has developed an encrypting pattern capable of producing 'blind signatures': the banks deliver their customers the coins, that do not allow to backtrack the consumers. [See below].

15.2.2. A controversial solution

Ecash is still a controversial issue. For many detractors its use is as well unrealistic as dangerous; for the supporters it is the payment instrument of the future, an unavoidable outcome. Ecash is a noteworthy case for it raises the question of anonymity within electronic transactions as a whole. As opposed to metal and paper currency, bits can be easily copied with absolute perfection and for any number of times. In principle, these bits could leave tracks wherever they go through. Therefore, if Ecash becomes common, anybody (neighbors, competitors, tax agencies, evildoers) could do what some legislation forbid: to spy into the private life of a citizen and draw his consumer profile in order to address him systematically personalized advertisements, etc.

On the other hand, the detractors of anonymous Ecash consider it a threat to public law and order. They fear that criminals could use it to make anonymous transfers, build up a black market, to launder money or evade taxation. In the case of Digicash, the sender is anonymous but not the recipient, for the latter has imperatively to involve his bank, either to deposit the money or to spend it again. Tax evasion is therefore impossible, and a black market could only flourish with the complicity of a bank, whereas the consumers can produce receipts to certify their payments. According to Digicash, criminals accepting Ecash could be identified with the backtracking help of one of their consumers.

Ecash is regarded by banks with some kind of distrust. This new technology could question and jeopardize the status of the banks: any new company could distribute Ecash and therefore create money. Digicash insists that it does not intend to issue Ecash and prefers to leave it to the banks, but other companies could decide differently. Banks also express their concern due to anonymity -although no links can be established today between a bank note retired at the counter and the consumer's identity. Nevertheless, the frame of regulations regarding Ecash has yet to be defined. Central banks and governments are just beginning to consider this issue. New laws might be necessary before issuing the first cyberdollar. To master the use of Ecash, it

might be necessary to undergo an experimental phase. This leads many people to think that its use will not become generalized for a long time.

Ecash obviously displays an irresistible charm, although many questions are still waiting to be answered. However, Ecash is too well-suited for online transactions and therefore, it will be used one day.

15.2.3. Digicash

Digicash is an American company with major operations in Amsterdam (Netherlands) created by David Chaum, a cryptography expert. Protection of private life is Chaum's credo. He considers that Ecash implies to choose a type of society for the XXIst century. There are two options: "[...] at one side, unprecedented surveillance and control of the private life; on the other side, the warranty of equality between individuals and organizations." This choice "can be done only once," adds Chaum. His fear is to see all kinds of organizations (companies, administrations, governments, etc.) taking advantage of the 'backtracking-ability' of electronic means of payment, for meddling systematically into the private life of the citizens.

His goal is to give his consumers an elegant electronic payment instrument, as anonymous as a bank note, and not to create the ideal cash for criminals or for the 'underground economy'. Chaum has developed a mathematical method for preserving the anonymity of Ecash owners, given they are not forced to be identified. His method allows at the same time to prove its validity. In other words, this system guarantees to Ecash owners that the bank cannot backtrack them, unless they accept to be identified. However, Ecash would remain under the control of the bank and be legally integrated into the usual commercial patterns. Moreover, the purpose of Chaum is to license to banks the Digicash system (he owns the patents and rights.) He is not seeking to substitute the banks and become a currency emitter, although he has the technical ability to do so.

Digicash Ecash uses 'coins' and allows the participation of the three usual actors: consumers, merchants, and banks. These have to possess the corresponding software and be ready to accept this payment modality. Digicash uses the RSA technology for encryption purposes. All transaction participants own one and only one pair of keys. When a Digicash customer decides to take some Ecash from his bank account, his Digicash computer program sends the bank a code (a random generated number) that is equivalent to a 'blank coin'. This code is hidden inside a digital 'envelope.' The bank first verifies the account's credit and decides then to attach its electronic signature on the digital envelope (not on the 'coin'). In this way, the bank cannot read the code inside. The electronic envelope acts like a sort of carbon paper so that the electronic signature will also be attached to the protected 'coin'.

With this blind signature as a guaranty seal, the bank gives the 'coin' a currency value while, at the same time, debiting the consumer's account. Upon reception of the Ecash by the consumer, his software removes the electronic envelope -in fact, he is the only one who can do that. Removing this envelope does not alter the bank's electronic signature on the 'coin.' The owner has now

anonymous money that, in case of loss (as caused by a computer breakdown) can be reimbursed like traveler's cheques.

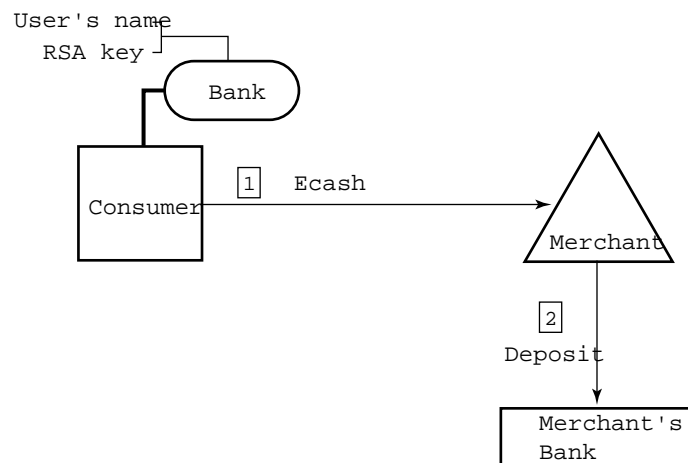


FIGURE 15.1. - Digicash transaction system

Figure 15.1. depicts the simplicity of a purchasing procedure. When the consumer decides to buy, he sends an order to the merchant's server which addresses him a request for payment. Clicking on the button of the Digicash interface (a small window, open at a screen corner), the consumer can transfer the required amount. The Digicash consumer software combines his 'coins' to build the exact sum. In the next step, the merchant's software contacts the bank to check that 1) the 'coins' are valid, and 2) these 'coins' have not yet been compensated by a bank. If somebody tries to use the same 'coins' twice, his identity is revealed. Once the 'coins' have been accepted and transferred, the merchant can keep them in his virtual wallet or place them into his bank account.

The same modus operandi is used for transferring money between individuals. Sending Ecash via E-mail is also possible. The bank checks the validity of each transaction. This is a difference between Ecash and real cash. From the bank's point of view, there is another difference: when a consumer draws cash from the bank, his account is immediately debited. When this consumer draws Ecash from the bank, the amount is recorded under the bank liabilities, and it returns to the assets when it is placed back into a bank account.

In October 1994, Digicash launched a full-size test. Digicash emitted one million 'Cyberbucks' -playing the role of a bank in this occasion. In September 1995, more than a half of this sum had been drawn. This fictitious currency unit could not be exchanged against real currency. However, it was possible to buy real goods through 70 different merchants agreeing to accept it. Each volunteer participating in this test got 100 'Cyberbucks' into his 'bank' account. He could store them into his virtual wallet through a software that could be downloaded free-of-charge.

Since October 23, 1995, the Mark Twain Bancshares (an American bank in St. Louis) issues the Ecash for Digicash. For the time being, the bank has set a top limit or US\$ 200 to Ecash

deposits. The system is currently running under the conditions described hereabove.

15.2.4. Netcash

Netcash was developed by Software Agents Inc. This system does not use 'coins' but vouchers. Customers acquire these vouchers from an ad hoc 'bank' called Netbank. To do this, they transmit their credit card number via Internet or mail. The vouchers are actually made of specific codes similar to the following one:

Netcash US\$ 25.00 M898900Z89032F

For further information, please contact the following address:

netbank-info@agents.com

When a merchant receives a voucher (either by E-mail or through the Web) he sends it to Netbank which will transfer the corresponding amount to his bank account. These vouchers can be used only once and cannot be considered a currency. Netbank is, therefore, not a bank but just a company that proposes vouchers that can be exchanged against goods.

The main flaw of Netcash is the lack of reliability. The security device is still not perfect and potential crooks could fake the vouchers.

15.2.5. Chip cards

Ecash can be stored on a chip that is itself implanted in a plastic card, as on a hard disk. Moreover, Digicash does not exclude this additional possibility. However, the same principle operates differently in the praxis. The chip card needs a special reader, which can be mounted on parking meters, public telephones, vending machines, public transportation systems, computers, etc... Contrary to standard telephone cards, chip cards can be reloaded. When the loaded amount is exhausted, the user just inserts the card into a special device and enters both the data about the corresponding bank account and the new amount that he wishes to store into the chip. Furthermore, chip cards are not limited to certain goods or services but can be used in multiple ways.

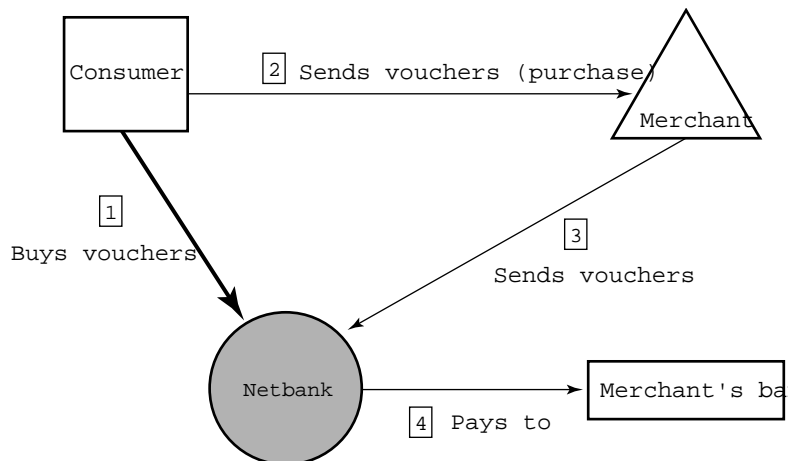


FIGURE 15.2. - The Netcash transaction system

Natwest (National Westminster Bank - a British bank) together with British Telecom and Midland Bank have created the Mondex consortium. Some Canadian and South Asian banks have joined them. They aim at developing a type of Ecash based on 'smart' cards. Mondex cards accept -for the time being - five different currencies. Users can deposit the Ecash contained in the card into their accounts or draw Ecash from these accounts to load the chip. The chip keeps trace of every transaction recording the name of each beneficiary. However, the data stored in the chip is cyphered. Thieves could spend the money contained in the card, but could not reload it, nor could they access the bank information related to the genuine card owner. Mondex Ecash is anonymous. Therefore, the risk of loss is limited to the amount carried within the chip card, as happens for cash. A full-scale test was launched in July 1995 in Swindon, U.K.. This experience involves 40,000 consumers and 1,000 merchants.

On the Internet, Mondex can operate in a similar way as Digicash. One difference is that Mondex needs a specific device connected to the computer instead of the Digicash software. This new peripheral behaves as a sort of virtual wallet. To make a purchase through the Internet, users insert their cards into the device to order (through the interface software provided with the device) the transfer of money from the chip card to the merchant's computer. This device can also play the role of a personal teller machine, at home or in the office. The user inserts his card and can either draw Ecash from his account or make a deposit.

15.3. THE DIRECT LINK CONSUMER- MERCHANT

Some payment systems altogether advocate the online transmission of bank information and protect this, of course, by a foolproof array of measures. The core of these systems consists of encrypting procedures for sensitive information, notably bank card numbers.

15.3.1. Reproducing a standard purchase

These payment systems aim at transferring the usual operations of a purchase to Internet. Other as with Ecash, consumers do not use any form of cash, but credit cards or direct account withdrawals. The consumer reports to the merchant his credit card number or his bank account. The merchant then obtains the transfer from the consumer's bank, and delivers the goods. One main advantage of this procedure is the creation of a direct link between consumers and merchants that avoids the use of intermediaries.

Nevertheless, this procedure carries the danger that the consumer's bank information is exposed on the network. A hacker could possibly set up a program that systematically captures all data looking -for example - like a bank card number. This information is of course encrypted. However, a private code of the exporting version of Netscape's browser was recently broken, which shows that even sophisticated systems have their weak points. On the other hand, the US Government applies restrictions to the exportation of encrypting software, so that the version mentioned above used 40 bits traditional encryption (instead of the customary 56 bits in USA).

15.3.2. Secure Web (SSL and S-HTTP)

Secure Web is a kit of tools that allows to integrate two security protocols within the transactions: SSL (Secure Sockets Layer) and S-HTTP (Secure HTTP²). These two protocols - appearing first as competitors - are technically complementary. SSL was set up by Netscape Communication Corp. in collaboration with MasterCard, Bank of America, MCI and Silicon Graphics. It secures the transactions between Netscape Navigator (the browser) and Netsite Server (the server software sold by the company). S-HTTP is the result of a collaboration between Terisa Systems consortium (established by RSA) and Company Integration Technologies (EIT), and it has been joined by America Online, CompuServe, Prodigy and IBM. S-HTTP is being promoted by CommerceNet (another consortium created by EIT) whose role is to encourage commerce over the Internet.

Actually, these two protocols can be combined. S-HTTP is only used for Web transactions. SSL acts on a higher software layer, so that it can be applied to several protocols, such as Gopher, FTP, Telnet, HTTP and even S-HTTP. S-HTTP can be considered an extension of HTTP that protects the documents. SSL does not only protect the document but also the data transmission channels. Yet, to go through the channel both the start and the endpoint shall comply with the same proprietary norms. SSL works only with Netscape Navigator, at one end, and Netsite Server at the other. However, S-HTTP is compatible with any software.

As it became obvious that both protocols were complementary, Netscape joined Terisa to create Secure Web. With this tool kit, merchants can accept transactions using either protocol (anyhow, merchants are interested in using all possible payment systems, to keep the ability to sell to a maximum number of consumers). This transaction model excludes intermediaries. Customers and merchants rely on technology to authenticate each other, encrypt

² HTTP - HyperText Transfer Protocol is the protocol used to transfer data within the WWW (World Wide Web, or simply Web).

the critical transaction data, ensure its integrity, and confirm the payment. The transaction procedure is therefore very simple, as shown in figure 15.3.

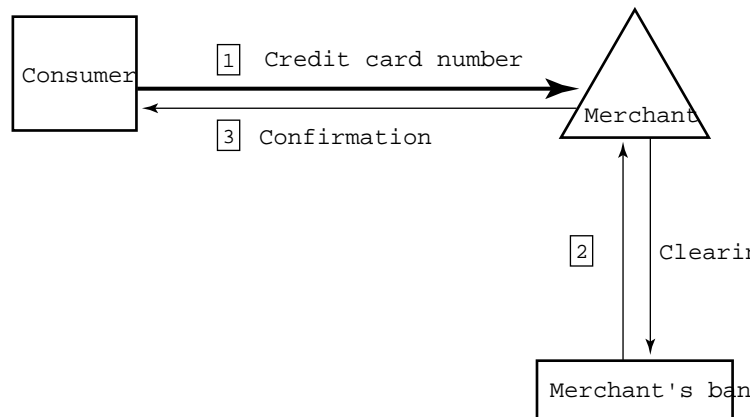


FIGURE 15.3. - Secure Web transaction system (SSL and S-HTTP)

SSL uses an RSA encrypting engine. Data is cyphered and authenticated by electronic signatures. When a consumer using Netscape browser meets a Netsite, the browser gives him two signals: a small key, at the left bottom corner of the screen (in all other cases, this key appears as broken) and a blue line at the top of the display window (below the URL field). The consumer is then supposed to enter his bank account information safely. S-HTTP supporters claim this system is safer than SSL. There is still no evidence for this: contrary to SSL, S-HTTP was not on the market at the time this was written.

15.3.3. Visa and MasterCard

After some isolated attempts, MasterCard and Visa have decided to work together and encourage the use of credit cards within Internet. All over the world, MasterCard and Visa have 300 and 442 million card users, respectively. Both competitors have been joined by prominent partners, such as GTE, Microsoft, IBM, Netscape, SAIC, Terisa Systems, and Verisign. Together, they have set up a common norm called SET (Secure Electronic Transaction) aimed at securing credit card transactions conveyed on open networks like Internet. The specifications were published via Internet in February 1996. Tests were previewed for the Spring 1996 and the product should come to the market during the last quarter of 1996.

Visa et MasterCard had to consider two facts: first, Internet navigators are afraid of sending their bank or credit card data even if these are encrypted; second, Visa and MasterCard have to promote a broader use of their cards for Internet transactions. They have found a simple solution and that is to replace the credit card number with a digital certificate based on asymmetric RSA encryption. Thus, the merchant can simultaneously authenticate the consumer and be sure of his solvency. They selected VisaNet authentication system.

Customers get their keys using a specific program integrated into the Net browser. Within this program, the customer enters a credit card number and the program creates a file that has to

be forwarded to Visa (or MasterCard). This company sends back a digital certificate containing a key which will be definitely embodied into the consumer's program. For every transaction, the consumer asks the program to send the key to the merchant who in turn asks the customer's bank for authentication. The payment occurs then in the usual way. Merchants and banks must equip themselves with the necessary software tools. The goal is that the SET norm becomes as popular as the credit cards themselves. The only way for a hacker to perpetrate a fraud is to get either the consumer's credit card number or to steal his computer.

In principle, the transaction happens in the same conditions as with the SSL and S-HTTP protocols. Besides, Netscape has decided to integrate this program into his own browser. Furthermore, MasterCard envisages making mandatory the use of this program with one of its cards. Certification authorized agents will be the only ones empowered to attribute digital certificates.

15.4. INTERMEDIATION

Ecash is not ready yet, and credit card numbers should not be transmitted over the network. Furthermore, bank cards are not adequate for paying small amounts, for they entail considerable expenses. Finding other solutions is therefore necessary. New companies have appeared to propose new payment systems adapted to open networks like Internet. All these systems require the presence of an intermediary between the consumer and the merchant. They are considered today the most secure. Furthermore, the expertise and services offered by intermediating companies ease the management of online transactions.

15.4.1. A complex intermediation

Speaking of intermediation is possible when consumers or merchants have to open an account in a specialized company before buying or selling. However, this definition is not accurate enough. Internet Shopping Network (ISN), for instance, asks its consumers to reveal their credit card numbers only the first time. ISN then exchanges this number for a personal code which the consumer will use for future purchases, instead of the credit card. Yet, ISN cannot be considered an intermediary. Real intermediaries such as First Virtual or Globe ID™ use an analogous procedure but on behalf of another party (merchants). Most important, they play a much ampler role. Intermediation in the Internet actually consists of:

- managing identifiers,
- ensuring participants identity and data integrity,
- proposing a secure payment system,
- acting as interface to the banking system, and
- bringing a range of value-added services.

Identifiers supplied by intermediaries do not give access to a virtual mall (as with ISN) but to a payment system. Consumers wanting to use First Virtual services, for instance, open an account with this company which takes note of the credit card number and provides them with an identifier. From then on the consumer can purchase in any virtual shop subscribing to First

Virtual payment system. Merchants identify their consumers with their personal codes. However, the intermediary's role goes even further. It allows consumers and merchants to identify each other; it confirms the transaction; it proposes an encrypting system to protect the transaction's sensitive data; it may provide a specific software to manage the payment system; it can operate all transfers to the banks or compensation centers; it can file the transaction records to keep documentary evidence and issue account statements to the merchants, etc... The range of services varies from one intermediary to the other.

15.4.2. Open Market

Open Market, a company based in Cambridge (Massachusetts), presents a global offer. This company aims to offer all necessary tools for doing business through the Internet. First, Open Market provides the software and services required to create a virtual shop. Another program, called Commerce Connection, allows to converse confidentially with the Open Market payment system (Integrated Commerce Service). This service ensures the security of the transactions, proposes adequate payment mechanisms, and also offers a consumer management service (e.g., automated consumers' assistance service, help for managing queries, etc.).

The Open Market payment system has been designed to accept any kind of security operation, including: S-HTTP protocol, various authentication procedures (from passwords to electronic signatures), procedures for entitling transactions (depending on lists of authorized consumers or the agreement of the consumer's bank), auditing services (recording the events), and 'fingerprints' to mark documents avoiding its unauthorized circulation. Merchants have the possibility to adapt the security level, according to the amount of the transaction.

This payment system complies with all types of servers, any amount of money (from one cent to thousands of US dollars), and any payment standard (debit cards, credit cards, account withdrawals, etc...). It also allows to sell goods of multiple formats: either physical goods or information (charged by quantity or by subscription). Open Market accepts payments in foreign currency, owed services, or frequent flyer miles.

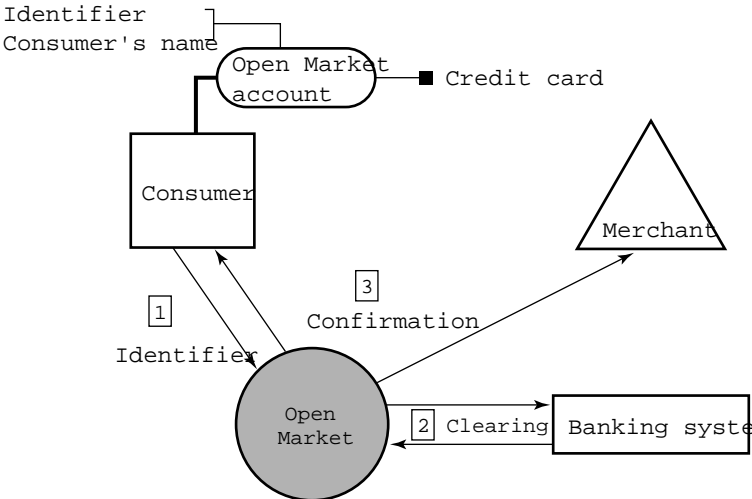


FIGURE 15.4. - Open Market transaction system

Consumers open a unique account which is used for all purchases made on shops equipped with a Commerce Connection server software. Their bank data can be transmitted either online, or by telephone or fax. They can decide about top limits for expenditures, or define some privileges affecting the goods' prices (e.g., subscriptions, membership to clubs etc.). When a consumer makes a purchase through a virtual shop server using Commerce Connection, he transmits his identifier (related to a credit card). The Open Market server performs the payment upon due verification. The credit card validation is a real time procedure. Subsequently, it confirms the transaction to both the consumer and the merchant. Merchants never get information about the consumer's credit card. At the payment level, this is the most simple form of intermediation.

15.4.3. Cybercash

Cybercash is an even more interesting solution whose future will depend on the endorsement it will deserve from the banks. This company based in Reston (Virginia) near Washington, D.C., was created by Bill Melton (who founded Verifone, a system for verifying credit cards at the selling points) and Dan Lynch (who founded Interop, the greatest professional international exhibition for computer networking and integration). Cybercash associates a remarkable group: Trusted Information Systems (TIS), software provider (gate keepers, among others), EIT, RSA etc., without mentioning the partnership with Wells Fargo. Cybercash is operational since 1995.

Consumers receive a free software, which allows them to connect directly to Cybercash servers linked to the banking network. These servers are secured for ensuring the impermeability between the banking network and the Internet. First, a consumer uses the software to enter data about one or more credit cards into the Cybercash server. The data will travel only once through the Internet. During this operation, the consumer defines a 'Persona' which encompasses an identifier and a password. The merchant should be able to accept credit card payments. Cybercash does not help merchants to create virtual shops. Most importantly, the merchant's bank must accept requests coming from Cybercash.

Once the computer is connected to a virtual shop using the Cybercash system, the consumer signals the merchant his intention to buy. The merchant sends back a request for payment (see picture 15.5). The consumer transmits the recorded Persona to the merchant, selects one bank card registered at Cybercash and clicks on the button labeled 'Pay.' The merchant adds his own data to this message and forwards it all to the Cybercash payment server. This server validates this transaction or not and processes the links with the banks or compensation centers. In case of approval, the transaction is confirmed to the merchant who concludes the deal with the consumer. The payment occurs automatically and the whole operation requires no more than a minute after pressing the 'Pay' button. According to Cybercash, the money is generally available the day after the transaction on the merchant's account.

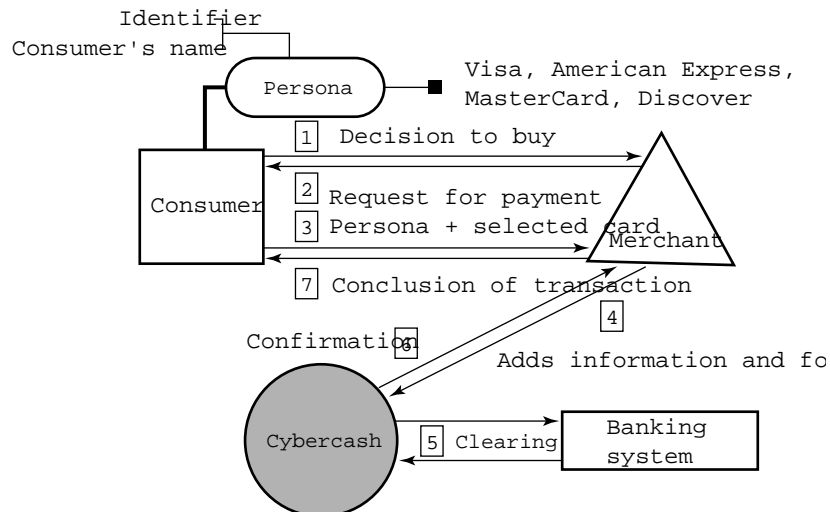


FIGURE 15.5. - Cybercash transaction system

Cybercash data carried on the Internet is very efficiently encrypted: 56 bit DES (Data Encryption Standard) traditional encryption, with 768 bit long RSA keys. Electronic signatures use the MD5 technology and 768 bit long RSA keys. Merchants also receive a free Cybercash software that allows them to instantaneously obtain the authorization for debiting the bank cards, handle the transactions and interact with their banks. This has an anonymous character for no merchant knows the consumer's credit card number (except if the bank imposes this condition). Cybercash servers deal only with information referred to payments and not with the transaction objects. Furthermore, only the banks decide about transferring funds, Cybercash plays only an intermediary's role.

At the end of 1995, Cybercash launched Money Payments Service, a service that allows transferring money via E-mail between two individuals even if only one of them owns a Cybercash account. This service corresponds to a transfer from account to account and does not rely on the use of bank cards. Merchants, of course, can also take advantage of this service. This aims at a double target: to foster commerce with merchants not possessing a Cybercash software and to give the merchant the possibility of being paid in cash instead of a credit card. In addition, a Mini Payments service will introduce a sort of Ecash consisting of a virtual-wallet filled with 'coins' in Digicash style. Merchants could sell information for very small amounts. Allegedly, Cybercash is entitled to obtain interests from the deposits in these virtual wallets.

15.4.4. First Virtual

First Virtual probably proposes the most clever solution. Its system combines simplicity of means with optimal security. This company is based in Washington, D.C.; it associates a business man and three Internet gurus. Lee Stein, a lawyer and accountant, is a consultant for Hollywood-based companies; he is First Virtual CEO. Marshall Rose, an expert in network management, is the coordinator. Nathaniel Borenstein, the main author of the MIME protocol that allows to send binary files via E-mail, manages the technical aspects. Einar Steferud, E-mail expert, is in charge of research and development. The group has built alliances with powerful partners. First USA Bank deals with transactions entailing the use of credit cards. Northern Trust (another bank) takes care of bank account withdrawals. EDS (more precise, its Bank Card Processing Division) manages the financial data and is in charge of compensations. Some big names, such as Reuters or Apple have chosen First Virtual to market their products.

First Virtual has the particularity of using neither cryptography nor software. This simplicity is one of its strengths. How does this miracle happen? As in any other intermediation system, consumers must first open an account with the intermediary. First Virtual has set up a vocal server. Consumers transmit by telephone their bank card number and immediately receive an identifier. Merchants also have to open an account linked to a bank account. All the sensitive data are stored into a stand alone computer, isolated from the Internet. EDS controls this computer from Ohio and it is the only one having access to the bank card numbers. These numbers are never accessible from the Internet.

Transactions go over the E-mail and essentially consist of the mutual authentication of both parties before proceeding to a payment. Figure 15.6 summarizes the procedure. When a customer wants to buy, he transmits the merchant his name and his identifier. The merchant requests the authenticity of this information, sending the data to First Virtual that checks if the consumer has an account. First Virtual then sends the consumer a message 1) to inform him that he is facing an authorized merchant, and 2) to ask him to confirm his order (through a message displaying the options: yes, no or fraud). In this way, the intermediation enables a mutual (consumer-merchant) authentication. First Virtual initiates the payment procedure, once the customer has confirmed the order. The merchant obtains next a confirmation of the transaction. To ease the flow of all these data going back and forth, messages coming from First Virtual display on the screen (in the 'Subject' zone) a unique identifier for each confirmation request. First Virtual debits the bank account of a customer when the expenditure amounts more than US \$ 10 (accumulated or not). Therefore, transactions remain within a fair cost range.

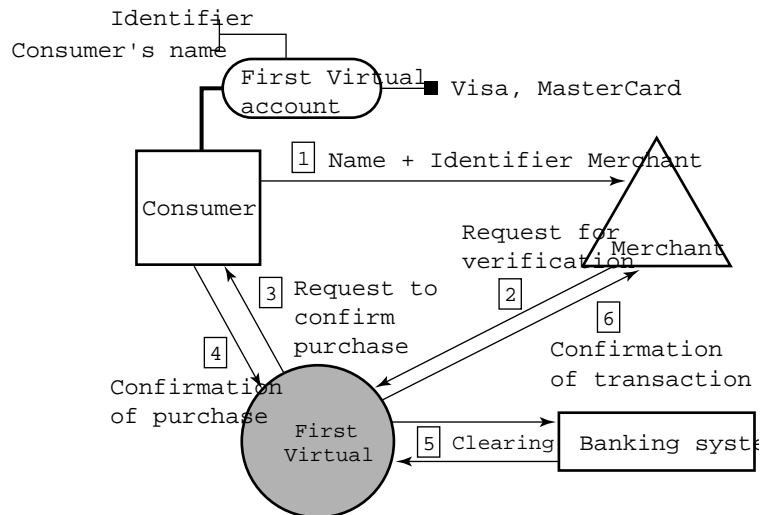


FIGURE 15.6. - First Virtual transaction system

Hackers intercepting a message cannot misuse the identifiers. The only way to relate an identifier to a credit card number is to have access to the computer holding all sensitive data. In other words, the hacker would have to commit a burglary. Somebody trying to use others' identifiers cannot go too far, because the legitimate customer will refuse to acknowledge the transaction when First Virtual asks for confirmation. That the customer has to confirm each order makes up the system's core.

First Virtual follows a « try before buying » policy. However, this involves an additional risk. Consumers can read a document (or part of it) before buying it (a practice similar to that of shareware software). Some consumers could take advantage of this possibility and get the documents without paying for it. However, First Virtual watches all accounts, and would recognize a misuse very soon, therefore closing the corresponding account. Opening a new account using the same credit card is, of course, not possible. Regarding the possibility of photocopying duly purchased documents, the problem is the same as outside Internet. Consumers refusing to settle their credit card bills will have their accounts closed. The company issuing the card will probably invalidate the card.

From a legal point of view, consumers have to accept that a message confirming a purchase is a contract. At the same time, the confirmation messages transmitted by the merchant stand for a proof of purchase. This is a condition they have to accept if they wish to use the system. Beyond this, all parties are free to use any form of encryption.

Customers have to disburse two US dollars for opening an account. For Merchants there are three types of charges:

- US\$ 10 dollars upon the opening of an account,
- US\$ 0.29 plus 2% of the transaction amount (for each transaction), and
- One US dollar for operation expenses (for each payment).

Before gathering these returns, First Virtual waits until banks and associates collect their gain. This is logical since it does not own the circulating money. First Virtual is therefore, the last to gather its profit. On their side, merchants can freely

set their prices. As for the consumers, they can remain anonymous if they decide to. Anyway, the mutual authentication procedures assure to all partners that no impostor is hiding behind an offer.

The First Virtual system shows some unbecoming features. It is not adequate for dealing with physical goods, but it is intended for selling information. Moreover, First Virtual encourages all users to become merchants, so they can sell specialized publications, all kind of guidebooks, poetry, professional advice, etc... First Virtual proposes a virtual shop, called Infohaus, where users can rent a space. By the way, transactions do not happen in real time. The flow of messages needed for the transaction takes some time (often up to 24 hours). Although merchants can automate the interchange of messages, consumers have no means to do so. They have to give specific answers.

15.4.5. Globe ID™

The best payment system on the Internet is French after all. At least, Globe ID™ is the most ambitious and most complex option and simultaneously, one of the closest to everyday praxis. The future will tell if it prevails as expected.

Globe ID™ payment system was set up by GC Tech (managed by Gérard Dahan) in collaboration with Edelweb (a service company established by a group of former INRIA researchers). GC Tech proceeds from Seppia (CD Rom conception), Waldo S.A. (financial advice), and BPA (created by former INRIA researchers, namely Philippe Brun and Paul-André Pays). Globe ID™ is the system used by Globe Online, a virtual mall comprising more than 30 French investors: La Tribune Desfossés (Louis Vuiton Moët Henessy), Le Monde, Libération, Dafsa, Compagnie Bancaire, Encyclopaedia Universalis, Euro RSCG and La Centrale des Particuliers, among others. The pilot server was launched on September 25, 1996 but the main operation was to start during the third quarter of 1996 when the Globe ID™ payment system is fully operational.

Transactions are totally transparent, thus the consumer has the sense of directly dealing with the merchant. In fact, Globe ID™ is the unavoidable intermediary, the system's turntable. It uses a specific transaction model: the Certification in the Middle Transaction Model (CMTM). It is the only one, together with Open Market, that avoids a direct contact between consumers and merchants. Figure 15.7 describes how Globe ID™ intervenes at every step of the transaction.

Globe ID™ relays on the use of electronic wallets called PMV (porte-monnaies virtuels), consisting of a previous amount deposited by the customer. This deposit is debited each time the consumer makes a purchase. Aside from Ecash, two techniques allow debiting small amounts of money, with a minimum of expenses: 1) small amounts may be added on until reaching a pre-established threshold before being debited (as in the technology used by First Virtual), 2) any amount may be immediately debited from the consumer's account. The second is the technique adopted by Globe ID™.

Before opening a PMV, the customer downloads a free software. This software shall be widely distributed among consumers and merchants to ensure the success of Globe ID™ and Globe Online.

The opening of the PMV itself is also free-of-charge. This can be done instantly online. In this case, the customer's bank data is encrypted (using RSA technology) and transmitted via the Internet. However, consumers that do not trust this kind of transmission can use the telephone or mail. A PMV is related to one or more bank cards. The consumer has the possibility to personalize the bank cards assigning them names to avoid confusion. Special techniques ensure that each card corresponds to a single person. For each created PMV (a consumer can have more than one), the consumer receives a virtual wallet number and a confidential code.

Consumers can pay in two different ways: using the card for big amounts or having their accounts debited for small amounts. Upon opening a PMV the consumer accomplishes two operations: he transmits his bank card number and other necessary data and transfers a sum to his PMV (less than US\$ 100). Actually, the consumer has the choice among three modalities of payment depending on the amount of his expenditure:

- less than US\$ 20 : PMV will be debited,
- from US\$ 20 to US\$ 100 : PMV or bank card can be chosen, and
- more than US\$ 100 : bank card will be used.

Thanks to the provided software, the customer is always aware of the status of his PMV account so that he can deposit new sums whenever he wishes to. He can also withdraw a part of or all his money from his PMV. This amount is actually a blocked account at the Compagnie Bancaire which cannot charge its services to this account. On the other hand PMVs may be created within a company. A certain amount could be made available to duly authorized employees.

A consumer equipped with a PMV can 'wander' along virtual malls. When he finds an interesting item he would like to acquire, he clicks on its image. If he expresses his decision to buy, Globe ID™ confirms to him the exact nature of the selected article, its origin (the merchant) and its price. The merchant is thus authenticated. The consumer wishing to buy transmits his PMV number and confidential code. Therefore, he is also authenticated. His PMV is immediately debited with the transaction sum. Globe ID™ instantly processes the transaction with the banking network. Subsequently, it remits the merchant a fixed percentage (80% to 95%) of the bill, depending on the type of items sold. The margin is then shared between Globe Online, if any, Globe ID™ and GC Tech.

Information purchased this way are available for the consumer during two days.

<http://www.globeonline.fr>

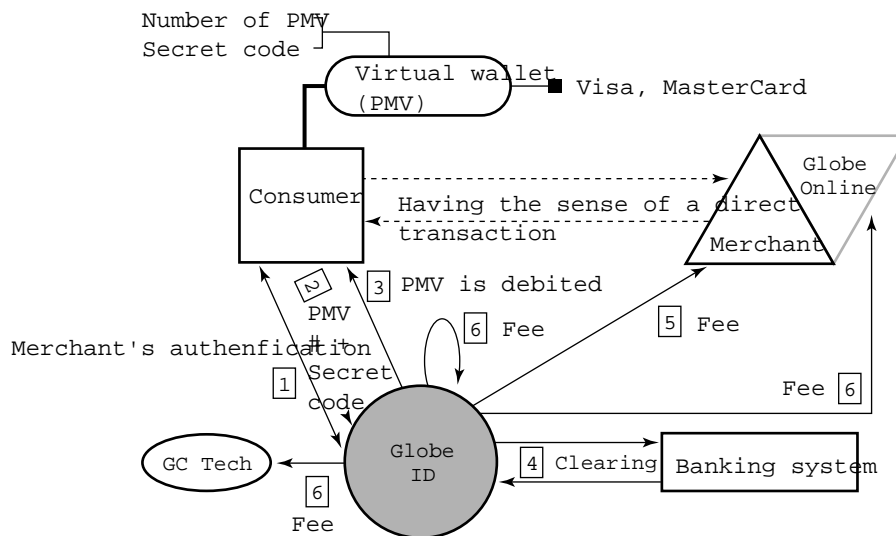


FIGURE 15.7. - Globe ID transaction system

Globe ID™ (as Globe Online) has worldwide ambitions: it deals with all currencies and credit cards. Independently of his residence or nationality, the consumer can choose the currency for his PMV (virtual wallet). Globe ID™ updates its currency exchange board every six hours. During this period such board is used as a reference for currency compensation.

The Compagnie Bancaire promises an interesting exchange rate. On its side, Globe Online uses 5 languages : French, English, German, Spanish, and Japanese. The virtual mall shall be extended to Europe and North America. Contacts have been engaged in Brazil and Japan.

Merchants can freely decide about their marketing strategy and prices. They can even set different prices for the same good, depending on the consumer's residence. For example, a perfume can be billed to different prices to French and to Japanese in order to comply with market conditions. The account statement, evidencing the transactions are transmitted to the Merchants via EDI (Edifact norm) if they wish to. Besides, Compagnie Bancaire is committed to handle 25 transactions simultaneously per second (meaning 0.4 seconds per transaction).

Essentially, Globe ID™ plays a role that reaches further than being an intermediary for the payment procedure: it brings value-added services. At the system's core relies the certification of the transaction. For this purpose, authenticating the participants is more important than encrypting the transmitted data. Moreover, Globe ID™ makes sure that the participants are willing to accomplish the transaction. It also takes care of data integrity and its non-repudiability (participants cannot deny the transmitted data since it cannot be modified after being sent). Only after these control procedures, the Globe ID™ operates the payment in relation with Compagnie Bancaire. But its role goes even further: it files every transaction and keeps these files available to the participants. Therefore, it can produce documentary evidence in case of litigation between consumers and merchants.

15.4.6. Netbill

Last but not least, there is an experimental system proposed by the Carnegie-Mellon University of Pittsburgh, Pennsylvania (the same university that developed the Lycos search engine). This model allows the transfer of small amounts for dealing with information (digital goods), but its real aim is to guarantee that the consumers should not be able to use the acquired products until the payment is accomplished. They cannot read the document without paying for it, as it can happen with First Virtual. To achieve this goal this system makes use of virtual-wallets that the consumer feeds from a bank or a credit card. Netbill maintains a server for payments which is linked to the existing financing institutions.

To start with, consumers and Merchants have to open an account with Netbill. The system uses a transaction protocol that allows the dialog between two software libraries: the customer's 'chequebook' and the merchant's 'cash register'. These libraries hold all rules and procedures necessary for a transaction. They are integrated in two softwares, one for the consumer and one for the merchant. Both programs run within the Web environment.

The diagram below (Figure 15.8.) shows that the first contacts are established between the consumer and the merchant. When the consumer chooses an item he requests a bid. The merchant sends him his bid, and the consumer orders the item if he agrees. The merchant then sends him an encrypted version of the item, so that it cannot be used without the corresponding key. Next, the consumer sends the merchant a formal payment order that engages him to accomplish the transaction. The merchant forwards this payment order to the Netbill server which achieves the payment, charging the consumer's account and crediting the merchant's account. Next, it sends a confirmation to the merchant, so that this can finally send the consumer the key giving access to the acquired item.

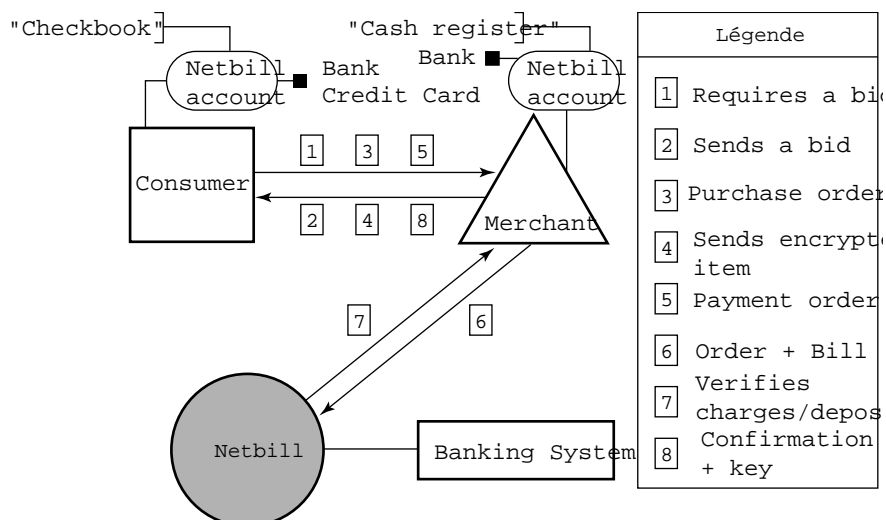


FIGURE 15.8. - Netbill transaction system

The systematic encryption of all data during the whole process ensures the security of the transaction. This system embodies a certain number of refinements such as the price discrimination depending on some privileges (membership to a club,

subscriptions, purchase of large quantities, price-time linkage etc.). The amount indicated in the payment order (step [5]), as calculated by the consumer's 'chequebook' must match the one calculated by the merchant's 'cash register', otherwise the merchant recovers the item or the transaction is cancelled. Nevertheless, the Netbill server keeps control of the transaction and decides about its further development. The number of data interchange operations could weaken the procedure so that technical troubles might bother the transaction. However, the system is conceived in such a way that it can always ensure the transaction consistency. Furthermore, Netbill provides accounting tools to manage the accounts of consumers and merchants. Margin costs are very low, due to the high degree of automation, the reduced financial charges (thanks to the money advanced by consumers and merchants when opening the accounts), the certification of items delivery (reducing the possibility of litigation), etc...

15.5. SUMMARY

Several technical solutions are more or less ready for action, and several payment systems will make a breakthrough in the coming years. Although appearing in a broad variety, they do not always compete against each other. Customers and Merchants can use several payment systems, as they do in the conventional market. However, one thing can be said with certainty: thanks to these systems, Internet commerce can only develop from now on.

The remaining obstacles will be overcome and the market will adapt to the non-tangible constraints. One of the long-term effects of this development will be the increasingly globalization of transactions. Internet, the world network, leads to a world market, and this fact should be taken into account when defining any company strategy.