Internet Banking - An Overview

By Juergen Seitz and Eberhard Stickel
Email: jse@euv-frankfurt-0.de

Juergen Seitz is Assistant Professor of Information Systems at Viadrina European University Frankfurt (Oder). He studied economics and business administration at Hohenheim University, Germany. His main research interest include IT use in banking and electronic payment systems.

Email: stickel@euv-frankfurt-o.de

Eberhard Stickel is Professor of Information Systems at Viadrina European University Frankfurt (Oder). He studied mathematics and computer science at the University of Ulm, Germany and at Syracuse University NY, USA. He is holding a Phd of Ulm University. His main research interests are economics of IT use, virtual banking and electronic payment systems.

1. Introduction

Consumer behavior is changing partly because of more spare time. The way of use of financialservices is characterized by individuality, mobility, independenceof place and time, and flexibility. Financial transactions caused by purchases will more and more be carried out by non- and near-banks. These facts represent big challenges for providers of financialservices. More and more the Internet is considered to be a "strategic weapon".

Financial services companies are using the Internet as a new distribution channel. The goals are:

- complex products may beoffered in an equivalent quality with lower costs to more potentialcustomers;
- there may be contactsfrom each place of earth at any time of day or night.

This means that financial institutions may enlarge their market area without building newoffices or field services,

respectively. Because of its image as an innovative corporation, better interacting possibilities, the usage of rationalization potentials, promotion of self-serviceide as, the improvement of its competitive situation by developmentof core competencies together with the construction of marketentry barriers, it may be possible to increase profits and marketshares.

One way of exploiting rationalizationpotentials is the implementation of the entire transaction (frompurchase to payment) under a common user interface. Information collected in operative databases of financial institutions allowsthem to act as information brokers. Offering special informationin closed user groups may result in more intense customer commitment,as well as customer bonding. Know-how that is built up by Internet presence may be used to facilitate Internet presence of smaller companies. The use of digital coin-based money to completely settle transactions in the Internet is a new service provided by financialinstitutions.

The presentation is organizedas follows. In the next section the properties of the Internet as a distribution channel are explored. In section 3 it is discussed how financial institutions currently use the Internet. It is shown that the possibility to carry out safe transactions is crucial.The focus of the presentation in the fourth chapter lies on thediscussion of electronic payment systems. They may be seen asa prerequisite for more complex safe transactions.

[BACK]

2. Internet as a DistributionChannel

Distribution channels arephysical capacities to build up customer contacts in a systematicway in order to inform, counsel and sell products and services[Aus96]. Like America Online or Compuserve the Internet is a so-calledelectronic distribution channel. Combined with self-service terminals and telecommunication equipment electronic distribution channels are technical channels within the class of media distributionchannels. Another example for a media distribution channel isdirect mail.

Today, media distributionchannels are an important way of distributing information andmanaging standard transactions. Counseling is mostly done in branchoffices or by field workers. Together, personal and media distribution channels are called internal distribution channels. On the otherside there are external distribution channels like salesman or franchising partners. Figure 1 visualizes this classification.

Figure 1:Systematic of distribution channels [Aus96]

The world-wide web (WWW, 3W,W3) is the most well-known and most important Internet service.A standard user interface to be able to address a large numberof users was one of the development goals of the WWW. The WWW is a world-wide network consisting of a large number of various computers. The user interface integrates other Internet serviceslike ftp, telnet, email,... The WWW is based on hypertext and hypermedia principles. Therefore, it is possible to present informationin a well structured manner. Documents are connected via links. Besides text documents it is possible to include pictures, sound and videos.

The client/server-architecture forms the basic implementation platform of the WWW. Data are storedon a WWW-server. The server software responds to inquiries fromWWW-clients and sends files to the clients. The files may be staticon the server or build up dynamically by means of parameters.The client interprets the files and presents the information onits screen. In modern browsers features allowing execution of application modules on client computers are implemented. Corresponding programming languages are e.g. Java, JavaScript or ActiveX.

Communication between clientand server is done through the hypertext transfer protocol (HTTP).HTTP is a very simple protocol. It allows short(er) response timesand reduced use of the server. On the other hand, a connection has to be build up for each inquiry. Each document is addressedby a unique key. The uniform resource locator (URL) is formed by the address of the server, the (directory) path and the filename. Sometimes it is useful to append further data, e.g. tocontrol programs that may be executed.

[BACK]

3. Areas of Use of the Internetin Financial Institutions

Generally we may distinguish four classes of Internet use in financial institutions:

- information presentation
- information presentationtogether with two way (asynchronous) communication (e.g. emailto request further

information)
- interaction with user(e.g. execution of programs with individual customer data)
- transaction banking (e.g.electronic payments).

[BACK]

3.1 Information Presentation

Information may be providedin connection with one or two way communication. One way communication means that the institution uses the Internet only as a presentationmedium for its products and services. The simplest way to usetwo way communication is to allow users to send electronic mailsto the server in order to ask for further information or make suggestions with respect to the Internet site.

Interaction with customersrequires quick information exchange. Information provided by theuser controls the information offered by the server. If the customeris identified and authenticated connecting to operative systemsof the financial institution may be possible. Then, often very little information has to be provided by the customer since datastored in the databases of the financial institution may be used.

Presentation of product informationmay be used to initiate new contacts. Implemented product models permit the construction of optimal insurance or financing contracts by using simpler components [Sei97]. Using mathematical models the customer may analyze his portfolios. To do so, he may use simulation techniques, what-if-analysis and other similar techniques.

Most Internet presentationsby financial institutions fall into one of these three categories(actually most of them are within the first two groups). If actualcontracting is desired transaction management is necessary.

[BACK]

3.2 Internet Transactions

There are a large number ofdifferent financial transactions, like e.g. customer payments,securities transactions applications for loans or insurance acquisitions.

Due to the structure and theintention of the Internet to be an open network high securityrisks are involved with financial transactions. Today, various techniques and standards are offered in order to control or evenavoid these risks. Basic requirements are as follows:

- Customer and financial institution have to authenticate each other.
- Private data have to beencoded. Cryptographic algorithms used need to have certain characteristics.No third party should be able to quickly get access to messagesor even to divert financial transactions.
- A digital signature isnecessary to get binding legal contracts. These digital signatures have to secure the integrity of signed documents. It needs tobe guaranteed that sender and receiver have the same intentions.

Base on these requirementsHTTP is extended to S-HTTP. Because the security level of thisprotocol still is not high enough various additional techniquesand standards have been developed. Examples are the home-banking communication interface (HBCI), secure electronic transactions(SET) or secure socket layer (SSL).

Different types of methodsare used or currently tested. These methods may be classifiedinto hardware- and/or software-based solutions. Hardware-based solutions use a chip that is physically located between computerand keyboard. Such a chip is unique. Note, that the system is hardly usable with laptop computers and/or with different financialinstitutions.

More often software-basedmethods are used. Personal identification numbers (PIN) identifythe user. For each transaction a transaction number (TAN) is necessary.Data are encoded using algorithms like IDEA with a 128 bit-keyor RSA with a 1.024 bit-key. A higher level of security maybe reached by means of a so-called electronic

fingerprint. This fingerprint is taken before and after the transmission. Then,both versions are compared. In case of any differences the transactionis aborted.

[BACK]

4. Digital coin-based money

4.1 Basic Requirements

Digital money may only beused for electronic commerce in an efficient and effective wayif an infrastructure on a high technical level exists. A large transmission rate is a prerequisite for simultaneous transmission of product information to potential customers. Access has to besimple and economical. Therefore, private households need PCswith suitable software. If these technical conditions are metsecurity problems have to be addressed. An excellent survey isthe book by O'Mahony et al. [OMa97].

[BACK]

4.2 Actors Involved

New payment systems like digitalcoin-based money are only successful if they are accepted by alarge number of persons. To get this acceptance all actors involvedshould have sufficient benefits that exceed their costs.

- The primary interest of*customers* is to carry out purchases in a comfortable manner.Associated payments should be possible from home in a simple andefficient way.
- The *dealer* usuallyhas to bear the costs of payment transactions. On the other handhe may benefit through an improved image (being innovative) andpossibly higher sales. Also, he may be able to reduce branch officesand sales personnel.
- *System architects*are responsible for the development of payment systems. Their benefits consist of royalties and service fees. Wide acceptanceand usage of their system is an important requirement.
- *System providers*are intermediaries.Dealer's sales are forwarded to the financial institution. Thesystem provider is responsible for transaction clearance. Moreover,he provides supporting services (problem management, user training).Again, revenues consist of fees and service charges.
- *Financial institutions*may promote certainsystems. As was already mentioned, confidence in electronic paymentsystems is a key success factor. Note, however, that a large numberof financial institutions, typically smaller ones in regionalmarkets, may have difficulties to participate due to high costsand know-how required.
- *Trust center*control digital signature keys. They are responsible for the integrityof transmitted data and the authenticity of contractors. Trust centers help to secure confidence in a certain payment system.Their revenues consist of royalties and other service fees.

[BACK]

4.3 SystemRequirements

The following requirementsare implementation independent. They are useful in comparing differentpayment systems.

- Open systems need security features to manage electronic payments. Security may be realizedby cryptographic methods in connection with transaction numbers(TAN).
- A large number of customershave to be able to simultaneously carry out payment transactions.The systems have to work with a large number of customers andshould be easily expandable. Hence, scalability is an importantcriteria.
- Small and smallest payments(micro- and pico-payments) should be possible. The corresponding accounting systems have to be efficient and effective. Therefore,it is necessary that costs per payment are low.
- The system has to be transparent.Customers have to be aware that payment actually takes place.System usage has to be simple.
- Private households should be able to accept digital money (micro-merchants).

Electronic data transfers,as well as electronic payments may be traceable. Then it is possible to analyze e.g. payment information and to construct detailed customer profiles. In most cases customers wish to stay anonymous.

- Digital coins consistof a number of bits. Hence, there is some possibility that copiesof the coins are made and eventually put into circulation. This phenomenon is known as the *double spending problem*. Hence,the payment system needs mechanisms to recognize and/or preventrepeated payments with the same digital coin.
- Digital coin-based payment systems have a nominal value problem. In order that a certainamount may be paid either coins with suitable values are neededor the payment system has to generate change in the form of newcoins. Alternatively, all coins have the same smallest possibleface value (e.g. one cent or even a fraction in the US). The lastalternative requires that a large number of digital coins haveto circulate and to be checked for authenticity.
- Digital money should beconvertible into "real" money, whenever this is desired.
- Confidence in an electroniccurrency means that stable exchange rates between electronic and"real" currencies are necessary. If the exchange ratesare unstable there is a chance of arbitrage profits. This, inturn, would reduce confidence since losses due to value fluctuationsare possible.
- Digital money is storedlocally on hard disks or other media. In case of disk crashesor other problems mechanisms to recover the original state arenecessary.

[BACK]

4.4 BasicPrinciples of Electronic Coin-based Payment Systems

Due to the increasing importanceof electronic commerce via the Internet the importance of digitalmoney increases. Representing "real" money in an electronicworld means that properties and functionalities like anonymity,authenticity, as well as availability of pico-payments are considered.Like "real" money, digital coins have an inherent value.

Depending on the way digitalmoney is implemented there exist different cryptographic methodsand organizational precautions to avoid the usage of forged money.Basically, there are two different types of digital coin-basedmoney:

- Using specific cryptographicmethod the anonymity of digital money may be achieved. Then, neitherthe financial institution nor the dealer may build up a connectionbetween the customer and coins used by him. The financial institutiononly knows to which customer the coins are transferred initially[Cha92, p. 96].
- Coins with customer identifyingcharacteristics allow the financial institution to identify thecustomer and to follow up on payments where the coin has beenused in.

Also, the payment processmay be classified into online and offline transactions. Figure2summarizes the different approaches.

- If an online payment takesplace the coins will be checked immediately for authenticity.This implies that a digital coin is used only once. The financialinstitution needs to check the authenticity by using a list ofall coins that have been issued or a list of all coins that havebeen sent in for credit.
- In case of offline paymentsthe coins may be used more than once. To avoid double spendingit is necessary to store information about the user or the userson the coin in order to be able to perform checks later. Anonymitymay be guaranteed by so-called secret sharing. Then, the financialinstitution only gets information in case of double spending.

	Offline payments	**Online payments**
Anonymous digital coins	Secret sharing by storing some information on the coin	Blinding and immediate check by the financial institution
Coins with identifying characteristics	Storage of information about the transaction on the coin	Immediate check by the financial institution

Figure 2: Security approaches to avoid copying digital coins[Sch97, p. 59]

[BACK]

4.5 Examples of Digital Coin-based Money

4.5.1 ECash

ECash is anonymous digitalmoney whose validity is checked online by the corresponding financialinstitution. ECash is developed by DigiCash and is offered byMark Twain Bank, St. Louis since 1995. DeutscheBank AG, Frankfurt (Main) offers eCash as a pilot project to itscustomers since October 1997.

The customer withdraws digitalmoney from his eCash-account using the so-called blinding methodand stores it on its harddisk. The blinding method works as follows.The client encodes a serial number and sends it to the financialinstitution. The financial institution certifies the coin andtransfers it back to the customer. The customer then decodes theserial number. Hence, the serial number is not known to the financialinstitution, which guarantees anonymity. In order to avoid doublespending the financial institution has to record the serial numbersof all incoming coins. At each purchase via the Internet the customergives digital coins to the dealer. The dealer immediately transfersthe coins to his bank in order to check for validity. The dealer'sbank registers the numbers of the coins issued without tracingthem back to the customer. Finally, the dealer is credited anddelivers products and services ordered [Pan96]. Figure3shows the payment process.

Figure 3:Payment process with eCash

Digital coins may be usedonly once. ECash may be considered to be a currency of its own.Financial institutions have to use special accounts. They alsoguarantee conversion into "real" money. As a consequencecentral banks like the Bundesbank or the Federal Reserve Bankhave difficulties in controlling money supply (financial institutions may create additional money and thereby increase the amount ofmoney supplied; this is well-known in the case of so-called checkbookor deposit money [Eva92,&bnsp;p. 410])

ECash security is achievedby using an asymmetric cryptographic algorithm. Account accessmay be protected additionally by using personal passwords. Thestorage of a coin's serial numbers does prevent double spending.There may be a problem with scalability, however. The costs ofchecking for authenticity of coins are relatively high becausethe check have to be done online. This means that the suitabilityfor micro- and pico-payments has to be evaluated carefully. Eachperson who has an eCash-account may accept eCash coins. The blindingmethod, as was already indicated, guarantees anonymity.

[BACK]

4.5.2 NetCash

The NetCash method is developedat the University of Southern California. One important goal ofthis project is the use of already existing accounting systemsand procedures in financial institutions. This reduces initialinvestment costs. In contrast to eCash, this method is based ona decentralized approach. Consequently, problems associated witha large number of coins and participants may be solved more easily.Therefore, reduced anonymity is accepted and the cooperation ofall participating financial institutions is required.

The system is based on independentdistributed currency servers. Currency servers are locations toexchange anonymous into non-anonymous money. Each currency serverpossesses an account on an accounting server. Clearing is doneby the currency server. It is necessary that the integrity ofthe servers is certified and that currency servers accept coinsfrom other currency servers. NetCash-coins have a face value anda serial number. Also, the address of the issuing server and anexpiry date is stored.

Figure 4: Payment process using NetCash

Figure4 shows the payment process using NetCash. The customer gets NetCash-coinsfrom a currency server. These coins are encoded with a publickey and send to the dealer. Anonymity of the customer may be guaranteedby using a new session key for each message. The dealer transfersthe coins received immediately to his currency server. From thecurrency server he either receives new coins or the correspondingvalue will be credited to his account. Final clearing is doneby the currency server.

The serial numbers of allcoins that are not send back and are not yet expired are storedon the currency server in order to avoid double spending. Thismeans reduced anonymity. Anonymity may be increased by exchangingthe coins at another server. Security is reached by means of ahybrid cryptographic algorithm. Like eCash we have a method thatrequires a lot of communication. The usage for micro-payments,however, should be more efficient. Each person may accept NetCash-coinsbecause the system allows free exchange of coins.

[BACK]

4.5.3 Millicent

The Millicent method is developedby Digital Equipment Corporation (DEC) to manage small and smallestpayments (e.g. payment for getting information from the Internetabout news and stock quotations or payment for small programslike Java-applets)

The customer buys a brokerscrip with a defined value by using his credit card or by debitinga suitable bank or broker account. Such a scrip is like a telephonecard. At the time of purchase the customer exchanges parts ofthe scrip into a dealer's scrip. This scrip is then send to thedealer. The dealer collects all scrips and exchanges them into"real" money. Figure5 shows the payment processusing Millicent.

Figure 5 : Payment process using Millicent

To guarantee the securityof this method one-way-hash-functions that may be evaluated quickly(e.g. MD-5) are used. Furthermore, the costs of illegally decodinga scrip (this means finding the inverse of the hash-function used)are much higher than the scrip's value. A large number of transactionsare possible at low costs compared to the other two methods discussed.In principle, each person may be registered at a broker and maythen accept digital payments. There is no anonymity but thereis the possibility to buy scrips from different brokers. Then,no comprehensive user profile may be built.

[BACK]

5. Conclusion

Currently most financial institutionsuse the Internet as a presentation medium. Often there is a possibilityto request additional information or to perform individual calculations.Business transactions are rather rare at least in most Europeancountries. On the other hand, a lot of effort is devoted to constructsolutions to manage financial routine transactions like moneytransfers, opening and closing of accounts, implementation anddeletion of standing orders and much more. Payment systems aredeveloped to facilitate electronic commerce. In order to realizesignificant rationalization potentials no isolated but integratedsolutions that support existing business processes are required[Sei97]. Collaboration between competing financial institutionsmay be necessary to cut down development costs [Sti97b].

In general, financial institutionshave to decide on their Internet presence. Is it worth to investsignificant sums? It can be shown that there are not necessarilyfirst mover advantages [Sti97a]. On the other hand, fast reactionsto actions of competitors are difficult since significant know-howis required to quickly build up an Internet presence. This impliesthat waiting too long may be extremely harmful and expensive.Consequently, a good strategy should be to build up know-how bymeans of small or medium pilot projects. Actions of competitors,as well as the development of the Internet should be monitoredclosely.

[BACK]

References

[Aus96] Ausfelder, R.(1996): Die Einführung von Telebanking als Vertriebswege-Entscheidungvon Kreditinstituten. Dissertation. Universität Passau. Frankfurt (Main).

[Cha92] Chaum, D. (1992):Achieving Electronic Privacy. In: Scientific American, August,pp. 96 - 101.

[Eva92] Evans, J. (1992):International Finance. A Markets Approach. Orlando.

[OMa97] O'Mahony, D., Peirce,M., Tewari, H. (1997): Electronic Payment Systems. Boston, London.

[Pan96] Panurach, P. (1996):Money in Electronic Commerce: Digital Cash, Electronic Funds Transfer,and Ecash. In: Communications of the ACM, Vol. 39, No. 6, pp.45 - 50.

[Sch97] Schuster, R.; Färber,J.; Eberl, M. (1997): Digital Cash: Zahlungssysteme im Internet.Berlin u. a.

[Sei97] Seitz, J., Stickel,E. (1997): Cooperative Software Development Supporting FinancialProduct Representation and Distribution in the World-wide Web.In: Wojtkowski, G. & Wojtkowski, W. & Wrycza, S. (Eds.):Proceedings of the Sixth International Conference on InformationSystems Development (ISD '97), Boise: Plenum Press, to appear.

[Sti97a] Stickel, E. (1997):Problems Associated with Cost/Benefit Analysis for Strategic InformationSystems. In: In: Wojtkowski, G. & Wojtkowski, W. & Wrycza,S. (Eds.): Proceedings of the Sixth International Conference onInformation Systems Development (ISD '97), Boise: Plenum Press,to appear.

[Sti97b] Stickel, E. (1997):Collaboration among Competitors - A First Economic Analysis.

[BACK]