HELI SALMI
ERNST & YOUNG FINLAND
FINLAND

SECURITY IN EDI BETWEEN BANK AND IT'S CLIENT *H2*

SECURITY IN EDI BETWEEN BANK AND IT'S CLIENT

Authors: Mr Pauli Vahtera, CPA, CISA
Mrs Heli Salmi, M.Sc.(Econ.)

ERNST & YOUNG

Ernst & Young, Finland

Address: Kaivokatu 8
00100 HELSINKI
FINLAND

Phone: +358-0-172 771
Fax: +358-0-622 1304

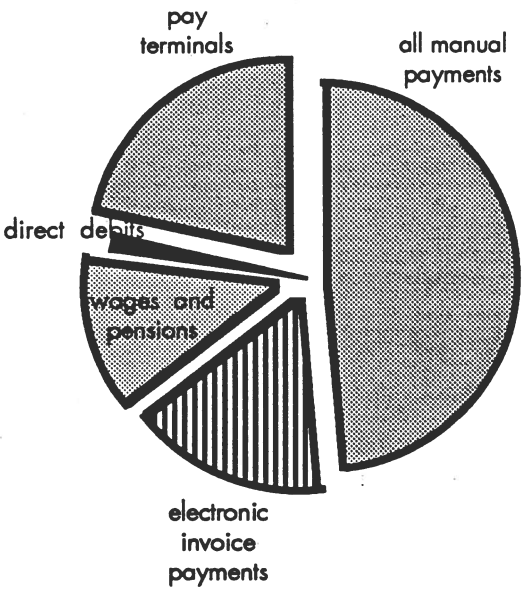
SECURITY IN EDI BETWEEN BANK AND IT'S CLIENT

The speakers will present a nationwide electronic banking system which is unique in the whole world. The system not only covers money transferring but also the bank statements. The information on the balance statement record has been widened in a way that the bank no longer send separate vouchers of the money transactions to the customers. The system saves hundreds of millions every year and simplifies accounting routines of the client company.

The speakers will prove that the electronic controls are better than the traditional paper based controls. Comparison between bank EDI solutions in different countries will be made.

The technique used in the presentation will be multimedia (Macintosh).

The speakers released a book on 'Efficient Money Transfer - Balance Statement without Vouchers' in September1993, 520 pages. The book is unfortunately not available in english.



More than 50 % of the payments are made automatically. In these volumes the security is an essential part and must be planned carefully.

1 History

The computerisation level of accounting has already for a long time been high in our country. But after introducing microcomputers computerised accounting has been available for almost every company and everybody. Computerisation has automatically lead also to widely used client/ bank systems originating already from the 1970'ies.

History of electronic money transfer systems:

1972 automated salary payments
1974 eferenced payments (automated updating of client's sales ledger)
1979 direct debit services
1979 first automated invoice payment via on-line connection
1980 automated foreign payments
1989 automated payment terminal
1992 payments with bar codes on bank giros
1992 bank statements without vouchers.

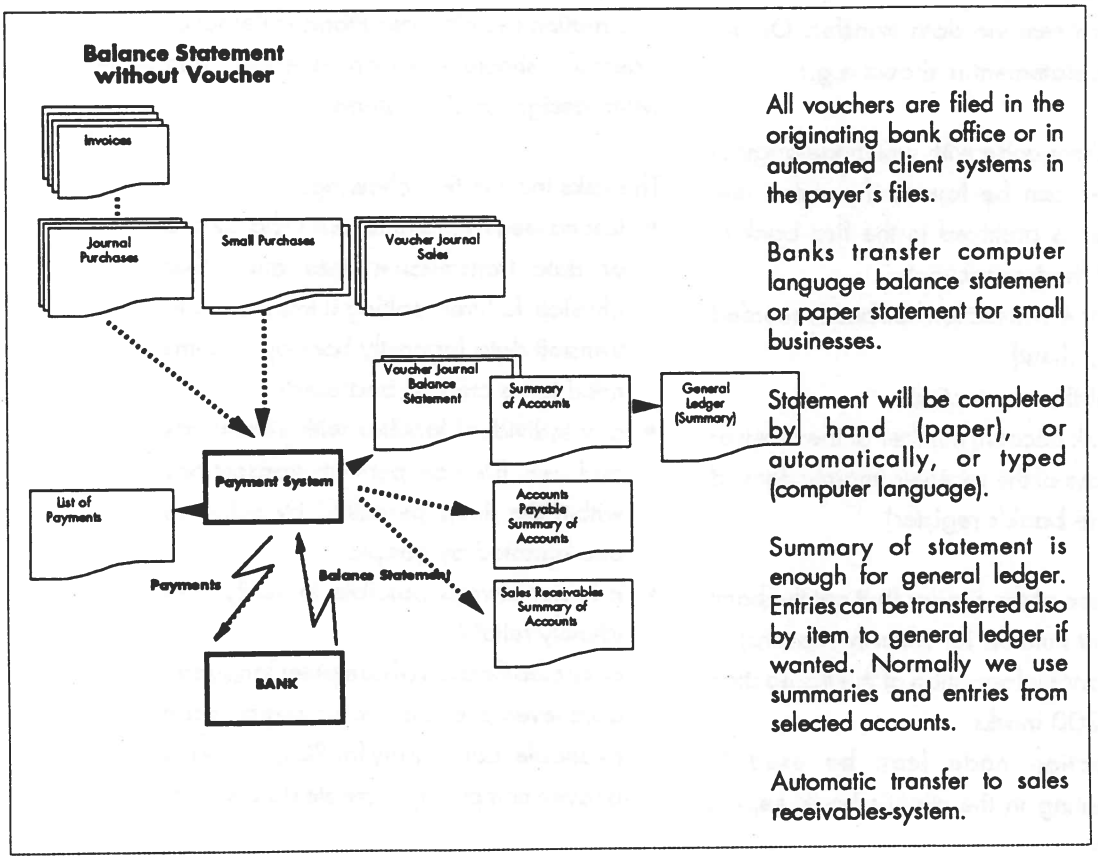
2 Bank Statement without Vouchers

Bank Statement without Vouchers is an example of an EDI system. However, offered by the banks nationwide it will rapidly reach a wide range of companies, as a typical EDI-system still affects normally only two counterparts' business. It has been calculated that the openness and large scale use of the

system will save hundreds of millions of currency yearly on a national basis, both in the banks as well as in the client companies. The information is quicker and the bookkeeping is up to date.

Description of the System

For a long while it has been a very laborious procedure to the banks to send vouchers to their customers. Paper formed voucher has to be transmitted between banks and to the client where the risk of errors is high. A big part of vouchers have already now been only computer output of electronic money transfers which have no more information nor security to the company than the data in the file received or sent. However finding the original paper documents, outputting and sending have cost a lot to the sender bank. In order to resolve this problem the National Bank Association asked permission from the Accounting Board to give up sending the vouchers to companies.



All vouchers are filed in the originating bank office or in automated client systems in the payer's files.

Banks transfer computer language balance statement or paper statement for small businesses.

Statement will be completed by hand (paper), or automatically, or typed (computer language).

Summary of statement is enough for general ledger. Entries can be transferred also by item to general ledger if wanted. Normally we use summaries and entries from selected accounts.

Automatic transfer to sales receivables-system.

In the same time companies had difficulties in organising their bookkeeping because of the bank vouchers often being late or totally missing. The books had to be kept open until all the vouchers were received from the bank. Bigger companies having many bank accounts had complex manual systems to manage the situation.

The National Accounting Board gave the banks permission to give up the sending the vouchers, if they improve the information of bank statements, which already in most cases were sent via data transfer. On the new bank statement is shown e.g.:

- an archive code with which the original voucher can be found, if needed (the voucher is archived in the first bank to record the transaction)
- where the transaction has been recorded (bank /client)
- date of the transaction
- the bank account number of the receiver
- the name of the receiver (mainly derived from the bank's register)

or

- the name of the sender (but not the bank account number for security reasons)
- additional information of the transaction up to 200 marks
- transaction code (can be used in automating in the client's bookkeeping system)

3 Risks in EDI

The speakers certainly accept the fact that EDI systems need good controls in order to verify the integrity of data and the effective functions of EDI.

As the benefits offered by the EDI methods are substantial, there is a risk that companies introduce the system without being fully aware of how it will affect the implementation of good accounting practices, internal controls and security. The auditors and information security consultants - internal or external - should have an essential role when designing EDI systems.

The risks include the following:

- loss caused by malfunctions in hardware or data transmission lines and other physical failures making it impossible to transmit data (or costly back-up systems need to be created and used)
- any individual familiar with passwords and user IDs can perform transactions within the limits permitted by software and updated by people
- it is not always possible to verify user identity reliably
- easy modification of computer language data (even public domain programs are available, particularly for PCs, to modify or even completely recreate data so that

it looks authentic - easiest way to modify a journal is to print it on a disk, change the data and after that print it on paper)

- problems caused by the destruction of large transaction or accounting files
- any errors in the register or balance information directly affect the final result (an incorrect stock level will result in a purchase order unless this chain of operations is interrupted for checks; or a register entry may be temporarily changed to effect automatic payment without leaving a trace)
- insufficiently processed matching data permitted by the computer language audit trail may result in extra work, unnecessary debt collection action, switching to manual processing, etc. (failure to indicate the payment reference code always leads to manual processing of the accounts, including unnecessary debt collection action, subsequent annoyance and extra reports)
- efficiency requirements make the system too large or too difficult to be managed by one individual
- however, if the potential offered by automation is severely restricted, a number of the rationalisation benefits offered by the system will be lost.

At the same time, the accuracy of the information needs to be controlled using really out-dated procedures. For example,

ERROR IN TYPING IN THE DIGITS, account no 312121-2455205

account no	3	1	2	1	2	1	0	2	4	5	5	2	0	5
factor	2	1	2	1	2	1	2	1	2	1	2	1	2	
result 1	6	1	4	1	4	1	0	2	8	5	10	2	0	
result 2	6	1	4	1	4	1	0	2	8	5	1	2	0	

35
40 subtraction
5 check digit

account no	3	1	2	1	2	1	0	5	4	2	5	2	0	5
factor	2	1	2	1	2	1	2	1	2	1	2	1	2	
result 1	6	1	4	1	4	1	0	5	8	2	10	2	0	
result 2	6	1	4	1	4	1	0	5	8	2	1	2	0	

35
40 subtraction
5 check digit

Check digit controls are not sufficient in the present environment. New security needs cross checking of bank account and the receiver's company code.

hundred of millions of bank transfers are transmitted with no other protection than the bank account's control code, yet two incorrect digits in keying in the information or the shift caused by the storing of the last digit may transfer the funds to a wrong account. Unnecessarily, this represents technology from the 1960s because it would be fully possible to the check the account by matching the official Company Codes stored in the company and bank registers. In fact, such a control system is already being designed. A positive aspect of the risks listed above is that they are easy to manage because most of them can be greatly reduced (if not completely eliminated) at a fairly low cost. Actually, it is a pleasure to note that the biggest risk consists of the limitations imposed by the existing technology and the staff not being experienced enough to make full use of all the benefits offered by EDI.

The risks in EDI from the legal stand point:

- unauthorised changes in transactions
- changing transactions with fraudulent intent
- purporting to be authorised EDI-user or counterpart in business
- loss of confidentiality e.g. personal data
- denial of the transaction's validity
- *accidental or intentional delay of transferring*

4 Controls in the case study: Statement without Vouchers

As the Statement without Vouchers is nationwide and covers all banks in our country, the control issue could not be passed. The best knowledge and best people were used defining the control points in the system (in addition to the statement information):

Reconciliations

Once a month a paper formed reconciliation statement is sent to the companies. This statement covers the transaction sums and transaction counts per every bank day separating debits and credits. This information is available also via data transfer if the company is going to build computerised reconciliations - which is of course the optimal solution.

Backups and voucher archives

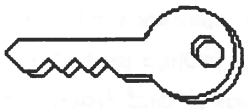
The bank saves the files not collected by the customer for two months ready for transmittal. This is important because smaller companies are totally closed during the holiday month. After that the bank statement transaction is on the bank's backup media and the collection will be more difficult - but possible.

The original paper vouchers are saved in the bank's archives. It is possible to have copies of them on request (e.g. tax or police officials have sometimes need for original vouchers)

User stamps and log

There is a requirement in keeping clear log on transfers in EDI systems. This log has to be printed out and saved as bookkeeping material, and it has to show the date, time and the user initiating the transfer.

Cryptography



All banks will provide a new system in client data transfer security. It is based on Message Authentication Code (MAC) following the ISO 8730 and ISO 8731-1 standards. MAC is based on cryptography using public and private keys. This security module has been designed in a way that in the future it will be possible to add in it security controls, to ensure the integrity of data (encryption of whole data) and user authentication as well as the non-repudiation of data.

The method will provide the following:

- identification of both the client and the bank
- protection of data against tampering
- proof of receipt of data.

Software vendors will provide the MAC module in their applications for banks' customers. The company installs the security feature by making a contract with the bank.

Bar codes in payments

In the same time banks introduced new payment method, where payment information can be read from a bar code on bank's automate. The bar code is printed on the invoice or giro where it can be used making payment information much more reliable and accurate. And if the bar code is there - why not use in the company's ledger systems?

The advantages of the bar code are:

- the input is four times faster compared to typing
- accuracy (risk of read failure is 1:2.000.000)

Security can be improved by using bar codes, because

- no typing errors occur
- user routine is simplified, that also reduces errors
- limiting errors makes the data more reliable
- falsifying of data is made more difficult

- dictionaries are simplified (business code of the seller expressed as a bar code will always refer the invoice to the correct account in the accounts payable system)
- the archive systems can be automated because of the dictionaries created by bar codes.

5 Traditional versus computerised controls

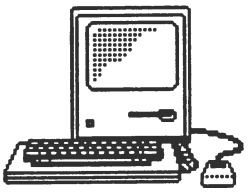
Approvals: a person or a computer?

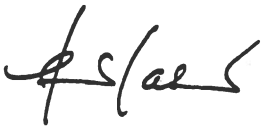
Traditionally one of the most important methods in internal control is built on different kinds of approvals. These approvals have been documented by signatures or initials. Until now it has believed that a list of these individuals who have been given the right to approve certain or all documents constitutes a basis in controlling business transactions. In addition, many companies have taken these people's signature samples on the list to make it possible later check the approvals against receipts and other documents.

When performing audits, these marks and their documentation are of significant weight, without considering the content, significance and the structure of the approved action. But has this kind of audit any significance in practice? It should be noted, that a person's signature changes over the years.

Approvals are often multiplied: the order form is approved before sending, the acceptance of goods is physically checked against documents and approved by stock personnel, the purchase invoice is recalculated and separately approved at the right level in organisation and the payment can be performed only by check or money transfer signed by two authorised persons in the company. Are there too many layers and duplications in this routine? Will this approval routine protect the company against mistakes and fraudulent actions; e.g. a situation where a person in a leading position makes a mistake? How should the control work in an automated environment?

Two signatures, one or none - the computer only?





In many countries, auditors insist old controls be applied to new system. Auditors require manual approvals and paper generated receipts, even in EDI-system. This is a common problem behind introducing new edp technology: a

new system is installed in the old environment without functional changes in work routines. Worst of all, it is still auditor's belief that, in doing business in a new way with old manual controls, the process is reliable and secure. Similarly, they assure the client that the controls are satisfactory, and thus lure him into a false state of security.

Let us next compare the handling of payments. Methods of paying vary to some extent from country to country. The classical solution in a manual environment has been to write first, the separate payment transfer documents and second, one money transfer or cheque covering all the payments. This money transfer or cheque is approved by two authorised persons, by signing. However, it is not usually possible for both the approving persons to actually check all the separate payments following the one money transfer, as the volume of payments is often tens or hundreds per day. Even if it could be done, it means too much extra manual work to be performed daily. After understanding this, the two signatures loose their original purpose! And there is one important fact also to be noticed: the second signature is already documented on the purchase invoice, which creates the payment itself.

Similarly, in using computerised payments, auditors insist on the same arrangement of two signatures, though in the case: using computers. As hand written signatures are impossible in the computerised environment, it has been suggested to use two different passwords or even divide the password into two parts, which are known to two different individuals. This will not be effective in practise, because during holidays and absences due to illness, there will be a need for a third person to know the password. What often happens, is that these two individuals know each others password. And even if the password would remain secret, these two people will never sit next to each other monitoring each other's work. A fraudulent cashier can, if needed, do what ever he wants without worrying that the divided password affects his actions.

In practise, this control will work and is sensible only when transferring millions of currency from one country to another and if the sending person has access to the already prepared transfer data. In this situation, strict password security is justified.

But what about the greatest part of companies: small and the medium sized. They simply cannot afford to establish a two person control system. We definitely need

to find an solution to secure the paying process in a reasonable and reliable way.

A functional security is achieved only in a situation where person A enters purchase invoices using input function in the application restricted by his own password. Person B, accordingly uses his password restricted checking function to check every transaction recorded by A separately. For this checking, person B must have available all the documents the approving individual normally has. Person B is naturally not allowed to enter invoice data. Cashier C can pay only person B's approved invoices, but he cannot input, change or delete invoice data, except the due date, when needed. It sounds complicated and laborious, and that what it is. Good solution, but only for big companies.

The automatised security, in a flexible work environment, can be designed as follows:

1 Paper formed purchase invoices are approved by one person after formal checking

2 Paper formed purchase invoices that already are in the order data base, are approved against data base and delivery notes on the screen

3 EDI purchase invoices are accepted by the application of order and delivery note data base

4 Purchase invoices are transferred to the payment system

5 Salaries and wages from the payroll system are transferred to the payment system

6 The invoices that are for some reason, time limited or other exceptions, are directly entered into the payment system are listed separately. The report, with the original invoice documents, requires special consideration when performing an audit

7 All transactions are printed with a user stamp, which tells the reader who has accepted the transaction and when the action has been made according to the computer's clock

8 Purchases, payroll, bank accounts and main ledger have been balanced regularly

9 All transfers between the company and the bank are automatically stored in a journal log file

When applying this procedure, one person can perform the payment alone and the possibility for him to act fraudulently is minimised.

Segregation of duties

Traditionally, the segregation of duties in accounting has been an essential part of the internal control system. This situation has changed radically in computerised accounting. Now, because of EDI, we are able to implement more reliable and effective controls.

In a traditional example: the person writing invoices does not have access to accounts receivable. The person who handles accounts receivable does not have access to cash or bank accounts.

New applications are designed in a way that an unpaid invoice is a part of the invoice data base. The segregation of duties can be arranged, when needed, by using different passwords for different functions. However, most companies are so small that these kind of controls are impossible to implement effectively. What can be done?

Banks can transfer the incoming payments by using reference code, by which invoices can be updated and payments booked fully automatically. In best case payments using reference code cover over 90% of all payment transactions. As a result, the bookkeeper´s only remaining task is the posting of payments, together with automatic invoicing of late payment interest and automated collection routines.

If one person handles invoicing, accounts receivable and bank accounts, the possibilities for him or her to commit a crime are:

I) - part of the sales is directed to a separate bank account, which is not included in the company´s bookkeeping. This can be done by using special invoice documents. In practice, however, invoices are printed automatically from the order data base, and this kind of procedure would require special modifications in the order data base as well as in the invoicing procedure.

II) part of the incoming payments is directed to a separate bank account and credit notes are added in the accounts receivable system. Payments with reference codes are booked automatically, so these funds cannot be manipulated in this way. This can be done by manipulating the payments

without a reference code. In these cases the electronic bank statement must be falsified after receipt. With application programs, data manipulation and deletion have been prevented. Thus, falsifying accounts require the use of special tool programs to manipulate the data or the output. Even that is not enough because additional credit notes covering the funds must be written. The auditor can find this by checking the credit notes and the procedure involved.

After setting up the transaction authentication value, even the falsified output can be discovered in audit samples. The fund transfer would also create a discrepancy between the bank account and sales receivable. In our country, reconciliations have to be documented, and they have to be filed for seven years.

III) unpaid invoices are booked as bad debts. This means that the employee must act in close cooperation with the payer in order to purport this kind of crime. In our country, bad debts must be approved at the Board meeting and documented in the official minutes. So, in fact, this kind of crime is not likely.

These examples show that electronic data interchange between organisations significantly reduces the need for segregation of duties among personnel.

Electronic Signatures

With the increase in computer language processing, it is necessary to make it possible to use the electronic signature. Several procedures are available but the most common so far is based on the password system in which a password, equivalent to a user identification, is recognised as a personal signature.

To make the signature strictly personal, the password system must be reliable. As it is not possible to achieve complete confidentiality, revised or completely new systems must be introduced.

Several forms of electronic signatures are available. It is sad to see, however, how little enciphering is used for protecting the data and users, although the prices of programmes designed for use on PCs are really low. Another advisable strategy is to route the data and authorisation differently, particularly in payment transfers.

The reliability of user authorisation is, however, determined by human behaviour:

group identifications are still far too common while too many users fail to switch off the unit when leaving the work area. One remedy would be to modify the operating system to make it necessary for the users to sign on again following a predetermined break (such as 15 minutes). The unit could be on stand-by and require the user to enter the authorisation information again. But the best method that will one day be introduced is identification by finger prints. If the unit suspects that the user is not authorised to perform certain functions, it will switch off automatically.

Irrespective of what method is used for recognising the user, it is important that all entries are identified by the user ID and time. In EDI, such information consists of the identity of at least the operator and the individuals by whom the invoice is cleared, checked, and paid. For practical control purposes, it is advisable to print the identification information as part of the accounting data to clearly indicate who fed a specific invoice into the payment transfer system and when such an input was made.

If data is modified after installation, it makes sense to indicate original input and latest modification. With respect to register data, it is advisable to set up a (computer language) log to record all modifications to critical basic data despite the fact that the operator responsible for installation and the latest update are stored in the actual register. In payment transfers, bank account numbers are good examples of such critical data.

To print the electronic signature, or the user identification and other supportive evidence, as part of accounting data is advisable for other reasons as well. For example, with payments, the recipient's bank account number and name appearing on the statement of accounts must be printed in the receipt journal when using the system to clearly identify to whom the payment was made.

Smart Cards

The use of magnetic stripe plastic cards is heavy worldwide. The problems in plastic cards are

- the magnetic stripe on the card can be falsified. The use of the card then seems authentic, in spite of the falsification and the transaction trail cannot be followed
- the cards are used manually, in which case they can be verified only by formal checking of signatures or expiration dates
- the 4-digit PIN code can be fraudulently obtained and not all the machines will 'eat' the card after a number of false trials. One can even steal or falsify the reader automate..

As it has been mentioned above, the falsification of a signature is quite possible because of variations in situations.

Cards are used and will be used in the future more and more and in many different ways:

- to identify the user, which means that the person possessing the card can have access to computers and can act like the authorised person regardless his actual identity
- to access physical entities; offices, factories, laboratories, thus corresponding to a safety lock key
- in reporting working hours in production, replacing manual reports

All these problems caused by verifying signatures and personal authentication can be solved by using microprocessor smart card based security systems. Smart cards can be used to identify an authorised person, but of course, they cannot prevent an authorised person from committing fraudulent actions.

The essential features of smart cards, in securing actions, are:

- access can be limited to one system only or a number of systems restricted by the card, and nothing else
- the unauthorised use of the card can be prevented entirely, because the length of the PIN-code can be up to to 8 characters and the code can be changed. The owner of the card can instruct the card to render itself as unusable, after a number of false trials. When instructing the card e.g. 3 acceptable wrong trials, the guessing rate is 3:99,999,999, if the code cannot be deduced either from the owner's birth day or from some other known or even given data.
- embedded in the card can be a cipher text secret key, which can be used in checking the correctness of transferred data by the receiver using his the public key. Still, a person in possession of the PIN code has all the rights the card gives its user, either though he is not the authorised user.
- internal control can be embedded on the card: a credit card can contain information concerning the account balance or the credit limit, which is updated after every purchase transaction. The card can be loaded only by transferring money to the card. In this case, the card will never allow purchases, that override the limit.
- one card can contain many applications or user rights, and for each their own controls. The rights can be updated also during use. This makes it possible for the card holder to use one application, and not another. For example, exceeding the

credit limit, will not prevent the card owner from opening office doors with the card or vice versa. The employee can be denied access to office doors, even though his personal account has money available for purchasing. Changes in the card holders organisational status can be accommodated in the cards memory(e.g. company's credit card, access to company's data applications), though he still retains rights to use the card for access to his office.

Today the price of a smart card is 3-5 dollars when ordered in quantities. The equivalent price of the holographic magnetic stripe card is 0,25 dollars. Though the difference between the yearly issue of credit cards is hundred million dollars, has the amount of fraud increased so much during the last few years, that it is worth paying the difference for the sake of security.

Biological user identification methods

We already have new security systems technically ready, but the cost of the equipment they would need, is for the time being too high for large volume applications; e.g.

As an actuality:

1 the dynamic signature, which is based on the hand written signature. The computer compares the rapidity, weight and style of the signature. This method has, in practice, proved to be more reliable than the old method of comparing two signatures visually.

2 finger print identification, which is based on the biometrics of the user's fingers

and among others as a curiosity (at least for the time being):

3 identifying the retina of a person's eye

4 identifying the nerve patterns

It is easy to say that security, as described here, cannot be implemented or that all this is pure futurology. However, ten years ago, we did not know anything about micro computers except for having a micro computer at home for children to play computer games with. Today we have 100,000,000 micro computers in the world. The prices of micro computers are today 5% of their price 10 years ago and their capacity has increased dramatically.

6 Public reactions

Though the new Bank Statement without Vouchers was received by the companies with enthusiasm, it also met heavy criticism mainly from - authorised auditors. The companies clearly saw the benefits gained by the voucherless statements and the computerisation. Auditors did not want to see new possibilities offered by computers and stack to the old paper system. Psychologically this is an understandable reaction: people always are afraid of things they don't understand. Thus, the only solutions to this 'problem' is in auditors' own hands: they have to get more acquainted with computer techniques.

Some examples of the criticism and answers to it has been described below:

- "The new Bank Statement without Vouchers is a catastrophe"
  Catastrophe is a very strong word - according to the dictionary: disaster, failure. In accounting we seldom meet catastrophes of that magnitude, they occur elsewhere. If a catastrophe - say a nuclear pollution - meets the country we hardly need any bank statements or vouchers anymore.

- "We have to maintain the principle of two signatures on vouchers"
  Only a small percent of companies have so many employees or so many accountants that this kind of approval method is possible. In our country on an average there are only 10,7 employees in a company. The demand for two signatures is place in a new light when accepting this fact.

  The control function of the signature has been overrated. The signature can be forged in a manner that a normal reader cannot see the difference. And - the second signature is often just a signature - the transactions or voucher seldom are studied carefully one by one.

- "Embezzlement will grow dramatically when the cashiers get the possibility to edit the bank statements"
  We have often met this assumption which is based on the erroneous belief of all cashiers being dishonest. Many auditors believe that cashiers will stay honest only because of the strong control organised by the company management. In the same time it is forgotten that cashiers have got the job just because they are reliable long term employees in the company.

This also proves that people rely much too much on papers. For most people it is easier to forge a paper by using copiers, word processing or both than to edit a file and be aware of the control hidden in the control sums, user stamps, log files and so on.

- "Banks have to send companies besides the electronic file also the same information on paper"
  The principle and the greatest benefit of EDI is giving up sending papers and business running on electronic transactions. Sending both files and papers will become even expensive because the costs of the electronic system will be added to and not replace the old paper based information system.