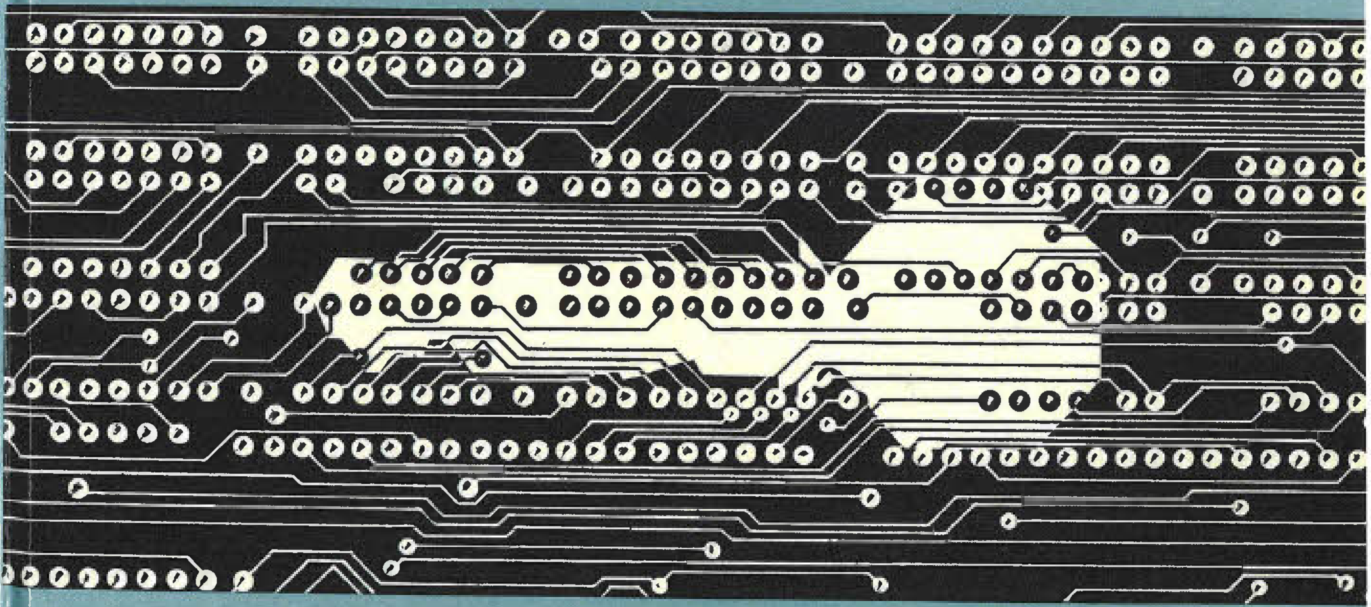
Security for Computer Networks

Second Edition

An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer



D.W. Davies and W.L. Price

EBAY INC.
EXHIBIT 1011

SECURITY FOR COMPUTER NETWORKS

An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer

Second Edition

D.W. Davies
Data Security Consultant

and

W.L. Price
National Physical Laboratory, Teddington, Middlesex

JOHN WILEY & SONS
Chichester · New York · Brisbane · Toronto · Singapore

Wiley Editorial Offices

John Wiley & Sons Ltd, Baffins Lane, Chichester,
West Sussex PO19 1UD, England

John Wiley & Sons, Inc., 605 Third Avenue,
New York, NY 10158-0012, USA

Jacaranda Wiley Ltd, G.P.O. Box 859, Brisbane,
Queensland 4001, Australia

John Wiley & Sons (Canada) Ltd, 22 Worcester Road,
Rexdale, Ontario M9W 1L1, Canada

John Wiley & Sons (SEA) Pte Ltd, 37 Jalan Pemimpin #05-04,
Block B, Union Industrial Building, Singapore 2057

Reprinted August 1992

Library of Congress Cataloging-in-Publication Data:

Davies, Donald Watts.
Security for computer networks : an introduction to data security
in teleprocessing and electronic funds transfer / D.W. Davies and
W.L. Price. — 2nd ed.
p. cm. — (Wiley series in communication and distributed
systems)
Includes bibliographies and index.
ISBN 0 471 92137 8
1. Data transmission systems—Security measures. I. Price, W. L.
II. Title. III. Series.
TK5105.D43 1989
005.8—dc20 89-14760
CIP

British Library Cataloguing in Publication Data:

Davies, D. W. (Donald Watts, *1924–*)
Security for computer networks : an introduction to
data security in teleprocessing and electronic funds
transfer. — 2nd ed — (Wiley series in communications
and distributed systems)
1. Computer systems. Security measures. Cryptograms
I. Title II. Price, W. L.
005.8′2

ISBN 0 471 92137 8

Typeset by MHL Typesetting Ltd, Coventry
Printed and bound in Great Britain by Courier International Limited, East Kilbride

Chapter 10 ELECTRONIC FUNDS TRANSFER AND THE INTELLIGENT TOKEN

10.1. INTRODUCTION

Payments can be made by cash, cheque, credit card and in many other ways. New electronic methods of payment are being introduced to improve the speed and convenience and to reduce costs by eliminating paper vouchers. In addition to these objectives there is the paramount requirement of security against attempts to defraud banks or their customers. The possibility of electronic payment systems depends on the relationship of trust between banks and their customers.

Each payment begins with an instruction by the payer. It must be possible to identify the source of the instruction so that the authority to make the payment can be checked. Traditionally, payments between bank accounts have been initiated by a signed instruction from the customer to his bank, such as a cheque, but there are now other forms of payment using paper documents such as credit-card vouchers and credit transfers. Since the essence of these documents is in their information, they can be replaced by digital messages if the necessary checking of authority is possible. The taking of cash from a cash dispenser, using a plastic card and a personal number, illustrates how far we have come from the concept of a signed authority for each payment, yet this is a type of transaction that has not had serious security problems. On the other hand, credit cards, depending for their authority on a signature, have been the target for fraud on an increasing scale. Each payment mechanism brings with it new security questions.

Electronic funds transfer (EFT) operates in 'retail banking' to give the customer a more convenient service, like 24-h service from cash dispensers, to save expense by avoiding the need for capturing data manually from paper vouchers and to improve security as much as possible. When EFT operates between banks and from corporate customers to banks, it serves mainly for convenience and speed of transaction.

Experience shows clearly that, with careful design, EFT can be much better protected against fraud than any method which uses paper documents. New technology such as public key ciphers and digital signatures may be able to offer even greater protection. In this chapter we shall describe some representative EFT systems, giving an indication of their security requirements and the available technology to meet them. We will begin with existing and well-understood systems and move towards those that are still in planning or no more than a future possibility.

When cash dispensers and automatic teller machines (ATM) were introduced, the need to protect them against fraud was obvious and, with a few exceptions, these systems have been reasonably secure. Growing evidence of fraud in other systems with poor protection has made it clear that any new payment method should be very secure in its protection against fraud. No system can be completely secure, so the design should be matched to an assumed level of technology in the way the system may be attacked, with a margin of safety against attacks at a higher level still.

The need for greater care in the design of automated systems is not just a reaction to the growing sophistication of fraudsters. When the protection against fraud is based on human vigilance, the enemy cannot be sure how this is being applied and what rules are in operation at a given time. New precautions can be added where they are needed without upsetting the whole system. In this respect, automated systems are less flexible and the security measures have to be designed and built into the system from the start. These precautions can be studied by the enemy over a long period and an elaborate attack can be prepared if the potential gains are large enough. Because the system is automated there is a danger that the fraud may also be automated in the sense that, once a successful attack has been devised, it can be repeated rapidly to produce a substantial gain to the enemy (and loss to the bank or its customers). Furthermore, the essence of the new systems is their convenience to the user, so any bank which had to withdraw a payment system because of mounting fraud would lose many customers. These are reasons why the design of future electronic banking systems requires a much greater attention to data security than was ever the case in the past, and larger safety margins.

The security of major systems is not preserved primarily by secrecy in their basic design. Discussion of the principles of security in EFT is valuable because it underlines the risks and, in the long run, leads to better methods. But it would be wrong to describe in detail the ways in which working systems can be attacked. In this chapter we shall describe the principles governing the design of various payment mechanisms without describing details which are too close to the potential vulnerabilities of any actual system.

From a cryptographic viewpoint, the attacks on payment systems are active attacks which seek to change data for the benefit of the attacker. Therefore the precautions are primarily those of *authentication* and *integrity* which enable unauthorized changes to be detected, so that payment transactions which are fraudulent can be inhibited before any damage is done. It seems that the need for data security has been understood in banking earlier than in other activities where data security may, in fact, be an equally urgent requirement. Banking provides an excellent example for the application of principles described in the rest of this book. The techniques used in this chapter come from earlier parts of the book, and here it is their application which interests us. We rely heavily on the verification of personal identity, the subject of chapter 7, but the predominant means of identification of payments has been the password. In the form used in banking, the password is usually short because the customer is expected to remember it and it is known as a *personal identification number* with the acronym PIN. When the password includes letters as well as numerals it is sometimes known as a *personal identification code* or PIC, but we will use the name PIN for either kind.

To begin this chapter there is a review of payment methods. Then three general types of payment are introduced and studied from a security viewpoint. We begin with payments between banks where, because of the degree of trust, the security requirements are more easily met, but the risks are great because of the high value of payments. We continue with payments between banks and their customers, such as cash dispenser transactions.

Throughout this chapter we shall be describing payment mechanisms that are implemented by many different kinds of financial instruction such as banks, savings and loans and credit-card issuers. To avoid the expression 'financial institution' at every point we shall refer to them conventionally as 'banks'. When their role in a transaction is specific, they will be denoted by that role, for example 'card issuer'.

An increased complexity appears in the security measures for ATMs when these are shared between a number of banks. The problems are similar to those of 'point-of-sale' payment systems which are the subject of the next section and both have the characteristic that the banks which might lose money from security violations are remote from the point of transaction and dependent on telecommunications. Thus shared ATMs and point-of-sale payment systems usually employ messages between central processors and remote terminals. The possibility of off-line systems for point-of-sale payments is discussed, and this gives a possible role for *intelligent tokens*, sometimes called 'smart cards'.

Having discussed payments from bank to bank and transactions between customer and bank, the final section of this chapter looks at payments between customers in which the bank need not be on-line at the time of payment. These methods depend essentially on the public key signature and there is no current proposal for their widespread introduction, but they are worth studying as a future possibility. They also point to the future value of digital signatures in almost all kinds of payment system.

10.2. ESTABLISHED PAYMENT MECHANISMS

The three main payment systems in operation today are cash, cheques and credit cards. Cash payments are the greatest in number and cheque payments the greatest in value. For example in USA, in the mid 1970s, cash payments formed about 88 per cent of the 300 billion transactions per year.[1] (We use the convention that 1 billion = 10^9.) Of the $7 000 billion transacted in these payments approximately 96 per cent was by cheque even though the survey excluded payments over $10 000. There is some uncertainty about the cost per transaction of these payment methods, but it is clear that cash payments were the least expensive at about 1.5 cents per transaction whereas cheques and credit-card payments each cost about 50 cents at that time. The cost of cash payment lies in the manufacture and replacement of coins and notes and there is a difficult trade-off between the cost of manufacturing notes and their resistance to counterfeiting. Like all anti-forgery measures, this resolves into a technical battle, in this case between the forgers and the legitimate bank-note printers and paper makers.

The bank cheque

The cheque payment mechanism is based on a signed instruction from an account holder to his bank to make the payment. This instruction or cheque is given to the payee as evidence of the payment so that, if the payer can be trusted, the payment can be regarded as complete, enabling the goods or services to be supplied. Figure 10.1 shows the outline of this payment mechanism which is surprisingly complicated and at first sight not a good candidate for automation. The payee or beneficiary, Bill, presents the cheque for payment to his own bank which sends the cheque to the payer's bank since the instructions contained in the cheque are destined for them. The payer's bank debits Ann's account and the payee's bank credits Bill's. The settlement is made between banks in the form of a payment covering all the transactions in a given period, such as those in one day.

Since there are many banks, bilateral arrangements between banks would be clumsy, so both the handling of the cheques and the inter-bank payment is usually provided by a 'clearing system'. As the volume of cheques increases (at about 7 per cent per year) an efficient clearing system has become essential. The big practical disadvantage of the cheque system is its slowness. Even with automation, several days must elapse before Bill's bank can be sure that the cheque has been cleared and allow Bill to use the funds that have been paid to him. The period of uncertainty prevents either Ann or Bill from using the funds for several days. Where very large payments are concerned, this is a serious cost to the customers and it favours the banks, which can use the amounts in transit to gain interest.

The physical sorting of cheques to return them to their payers' banks once threatened to undermine the cheque payment system and it was saved only by the introduction of cheque sorting using magnetic ink characters. In principle, the whole system could work without paper as soon as the essential data have been captured, the cheque itself remaining at the branch of Bill's bank where it was presented for payment. The use of 'cheque truncation' depends on the legal system under which the banks are operating.

The security of the cheque mechanism depends on the manual signature on

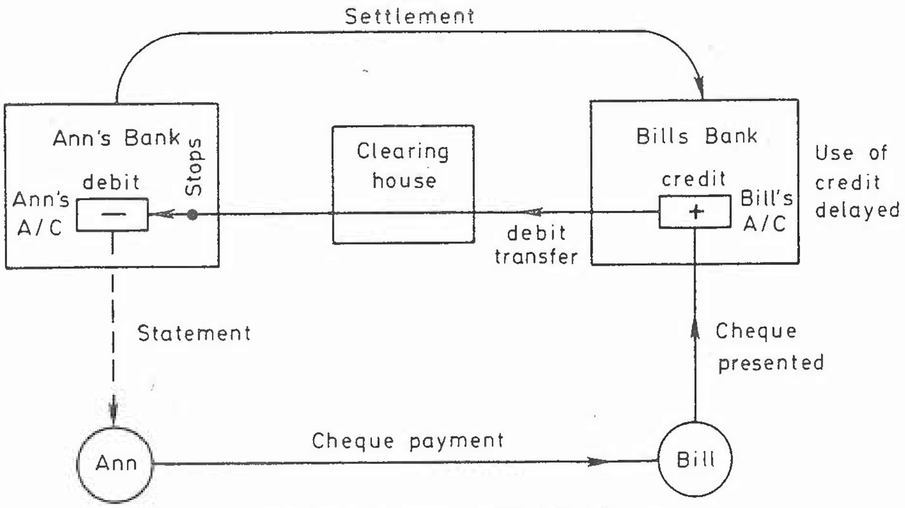


Fig. 10.1 Cheque payment mechanism

the cheque. The weakness of the signature as a security measure is that the enormous volume of cheques which are handled prevents the verification of individual signatures in most cases. Dynamic signature methods which were described in chapter 7 are of no value here, but the automatic verification of signature patterns on paper (the static signature) is showing some promise. Nevertheless, cheque fraud is a considerable problem. Cheque guarantee cards give some protection to shop-keepers, up to a limit set by the banks, in return for checking the signature and copying a number on to the cheque from the cheque guarantee card, but the cost of fraud then falls on the banks.

The paper cheque with its manual signature is not an ideal subject for automation yet it embodies an important principle, which is the authority given by the payer and made apparent to the beneficiary before it threads its way through the clearing system. Changed into a modern form as a message with a digital signature this can be regarded as an 'electronic cheque'. At the end of this chapter we show that this kind of message can be a basis of many different payment systems.

Credit transfer

The cheque is a *debit transfer* when it passes from Bill's bank to Ann's bank because it asks the latter to debit Ann's account. Other transactions are *credit transfers* because they carry the payment with them, for example in the payments between banks which make the settlements for cheques. When an account holder at a bank makes a 'standing order' for regular payments, these payments are carried out by credit transfers. For example, a magnetic tape from the bank of payer Ann may contain among its many transactions a request to credit Bill with a stated sum. The magnetic tape containing this payment also entitles Bill's bank to debit the account it holds for Ann's bank so that the total of the transactions on the tape cancel out. The transport of these magnetic tapes can be replaced by file transfers using data communication.

Figure 10.2 shows the effect of a typical credit transfer from Ann's account in

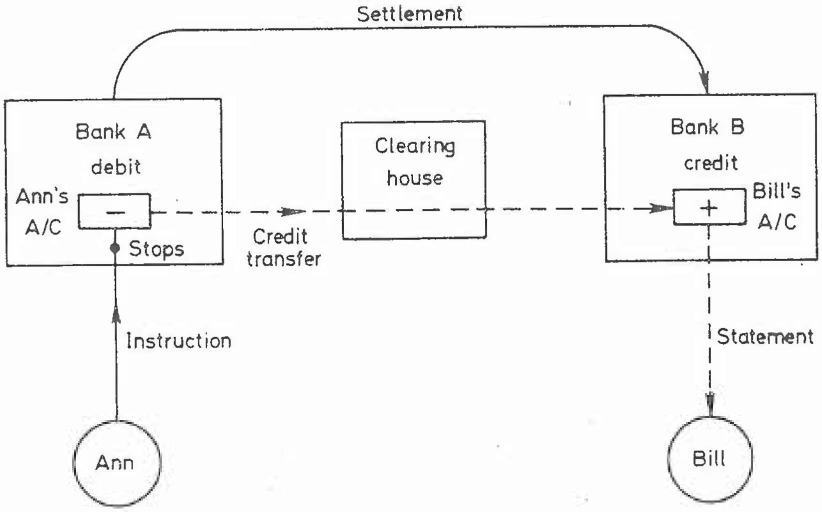


Fig. 10.2 Credit transfer

bank A to Bill's account in bank B. If it starts with a paper document, this can end its journey at A, while the information flows on. The settlement between the banks covers a multitude of individual transactions. Sometimes the credit transfers are initiated by a magnetic tape containing a large number of transactions. In the UK, a bank customer can make an arrangement to send the information directly to the 'Bankers' Automated Clearing Service' where the sorting of entries takes place. For this purpose, tapes or diskettes carry the transactions, or they are sent over a public data network.

A form of banking, named a Giro, which favours credit transfers, is common in European countries. This is a single 'bank' which can very easily make credit transfers between accounts held by its own customers — the two banks and the clearing house of Figure 10.2 are merged into one organization. Because of the need to let Bill know he has been paid, a short statement of account is made whenever a credit arrives and (since the paper is all in one place) the credit transfer form itself goes with that statement as confirmation of the payment and its source.

The Giro has a long history in Europe where Post Offices operate the systems using the postal service to carry the paper work. Typically, Ann sends a credit transfer to the Giro centre by post, which then makes the transaction by adjusting the accounts of both Ann and Bill, then sends an advice to Bill that the payment has been made. Since the two accounts are adjusted simultaneously, there is no 'float' on which the Giro obtains interest. The first notice to Bill of the completion of the payment comes with the advice, so the completion of the deal in goods or services may have to wait on the two transits through the postal system, and posts are not getting any faster. The Postal Giro has an extra convenience that the document can also contain the order for goods or services, making one letter complete the deal. Since Bill receives the payment with the order, there must be some trust, so this simple and convenient device is used for small payments. Giro payments and credit transfers generally are particularly useful for regular payments that are not constant in value such as for telephone service, utilities, tax and insurance.

The simplicity of the postal Giro is due to the monopoly position of national Giro services, which means that the whole transaction between customers' accounts takes place in one centre. There is no problem of paper-sorting or settlement between clearing banks. It follows that Giro services can be automated easily, except for the postal part. Eventually the cost of the post will make this less economic than on-line electronic payments. Bank credit transfers enable many payments to be covered by one cheque and the credit transfers, once their data have been captured, are easily automated because the instruction on paper stays at the customer's own bank. At present, the credit transfer seems better able to fit in with information processing than the debit transfer or cheque, but if paper documents do not have to be moved around (for example if they stay at the point-of-sale in an on-line system) the distinction is less clear. The route taken by messages in point-of-sale EFT is, in fact, closer to that of the cheque.

Summary of the properties of payment methods

Returning to the three principal methods of payment used today, their advantages and disadvantages can be summarized. Cash is the cheapest to operate and loses very little by fraud. The payment is quick and there is no 'clearing delay'. It is not surprising that cash is the most frequent payment method. The main objection is that cash can be stolen. Its disadvantages are found in collecting large quantities of small payments (public transport, payphones and parking meters) and in large payments when violent crime is a danger. Cheques are best for large amounts when the cheque can be cleared in time or the payer can be trusted (or brought to court successfully). For small payments in shops they are too easily used for fraud, too expensive and payment is slow. For very large payments, the clearing delay loses interest to the customers and favours the bank. Credit transfers are best for multiple and large payments. Credit cards have characteristics similar to cheques, except those concerning payment delay, where the customer has more choice. Considering their disadvantages, cheques and credit cards should be overtaken by more automated payment mechanisms as soon as the economics of on-line operation are favourable and the security of electronic methods is assured. Cash will remain the most frequent payment method.

10.3. INTER-BANK PAYMENTS

A large customer of a bank may present a magnetic tape containing thousands of credit transfers. In the UK these can be handled directly by Bankers Automated Clearing Services (BACS) where the items are sorted according to the destination banks and passed on to them also in batch form on magnetic tape. In the future, most of these batches will be handled by file transfer through a data network. The security requirements are principally the authentication of the files to prevent unauthorized changes and it was for this purpose that MAA was designed. Electronic funds transfer based on the batch handling of credit transactions has been in operation for a long time. This service is provided by BACS for large- and medium-sized bank customers and is the world's largest clearing house in terms of transaction volume.

When very large sums are paid between bank customers a cheque is not used because it puts the funds out of use for too long. In its place, telephone or Telex messages can be sent by one bank to give an immediate request to another bank to make a payment on its behalf. The payer makes the request to his bank. That bank validates the request, making sure that it is genuine and that the individual has sufficient funds, then passes on the request to the beneficiary's bank which makes the payment, debiting the account which the payer's bank holds with it. In this way the payment is completed within minutes or hours instead of days. Because telephone or Telex messages are vulnerable to fraud by impersonation it has become normal to add to each message an authenticator using secret keys established between correspondent banks for this purpose. Traditionally, the name given to this authenticator is a 'test key'. The secret keys employed were often in a form of tables, typically two sets of tables held by different individuals. The calculation of test keys was necessarily rather simple because it was carried out by a clerk.

The volume of these payments increased and so did their complexity. Errors due to misunderstanding of the complex transactions had to be resolved by telephone calls and their resolution depended on a degree of trust betwen correspondent banks. These semi-automatic payments continue but are increasingly being replaced by use of custom-built, message-handling systems of which the prime example is the international Society for Worldwide Interbank Financial Telecommunications (S.W.I.F.T.) system. Following on the introduction of S.W.I.F.T. national systems have been introduced such as clearing houses interbank payment system (CHIPS) in USA and clearing houses automated payments system (CHAPS) in UK. After describing the S.W.I.F.T. system, we shall compare its service, and the method of providing it, with CHAPS.

The Society for Worldwide Inter-bank Financial Telecommunication S.C.

The society is a bank-owned, non-profit cooperative society, directed by more than 1400 shareholding member banks which are located in more than 60 member countries. It began as a result of a study by European banks in the late 1960s which led to the formation of the company in 1973 and the first operation of its network in 1977. It has members in North, Central and South America, Europe, Africa, Australasia and the Far East. The costs of its message transfer service are paid for by members using a tariff designed to recover the costs according to numbers of connections, addresses and volume of message traffic. In addition to providing the service and the associated information and training it acts as the forum for agreement on standards.

All messages are handled by store and forward procedures through one or both of the 'operating centres' located in Belgium and USA. The society installs, in member countries, its 'regional processors' which are connected by leased lines to the operating centres with some extra connections so that single line failures do not disconnect any country. Countries with heavy traffic such as USA, UK, Germany and Italy have multiple regional processors and each regional processor has duplicate CPUs for reliability. All connections to the network go through the regional processors which act as concentrators. The operating centres contain duplicate equipment and customers can fall back to an alternative regional processor so that the worst effect of an equipment failure is a short delay. Figure 10.3 shows part of the network as it was in 1984. Since then, the communications system has been redesigned for SWIFTII.

A S.W.I.F.T. terminal is generally a small computer which can 'stand alone' or be used as a front end to the bank's payment system computer. The majority of connections use a 'S.W.I.F.T. Interface Device' (SID) with software supported by S.W.I.F.T. but about 30 per cent use other methods, principally the 'Direct S.W.I.F.T. Link' (DSL) software running on International Business Machines (IBM) main frames. For small users, and as a fall back for others, Telex was used but this has not proved convenient and a microprocessor-based terminal offered by a S.W.I.F.T. subsidiary company has taken over this function.

The S.W.I.F.T. system can report the number of messages sent and received and stores the messages it has transmitted so that they can be retrieved until 14 days have elapsed. This helps banks to resolve any difficulties about the content of messages or the completeness of their traffic.

Message format standards

Strict standards for message format can be imposed because the composition of messages is assisted by the SID in nearly all cases. The agreement on standards has been one of the major advances brought by the S.W.I.F.T. system because

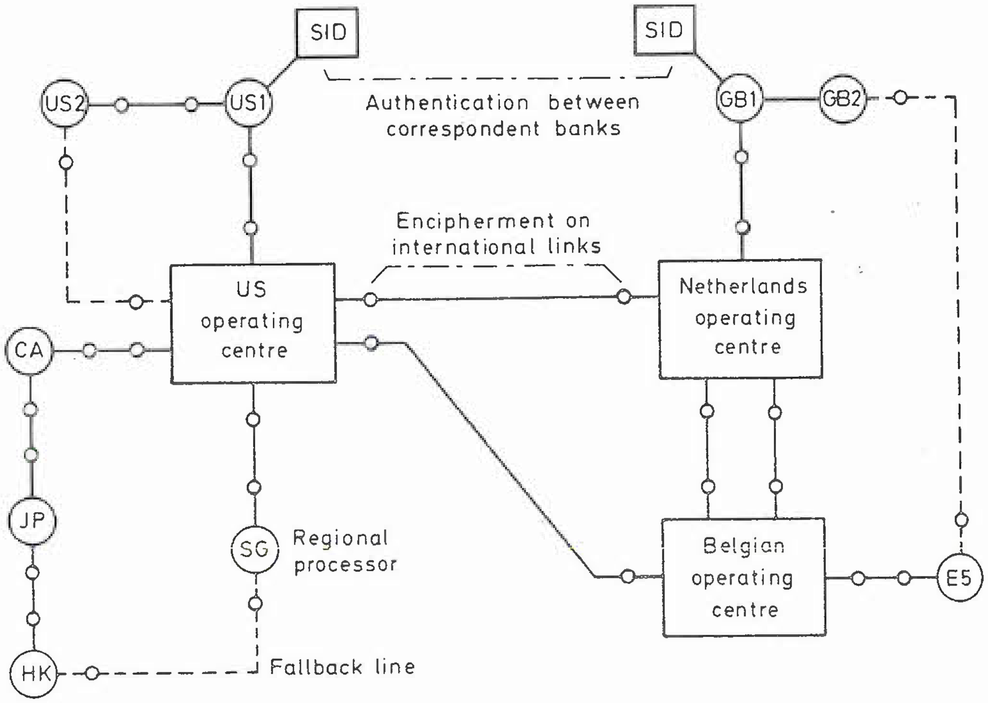

SID
SID
Authentication between correspondent banks
US2
US1
GB1
GB2
Encipherment on international links
US operating centre
Netherlands operating centre
CA
JP
SG
Regional processor
Belgian operating centre
E5
HK
Fallback line

Fig. 10.3 Part of the S.W.I.F.T. network (1984)

its uniform terminology and notation prevent some of the misunderstandings that might otherwise occur in complex interactions. The nature of this complexity will appear later. Working groups of S.W.I.F.T. members derive these standards by discussion and agreement and continually review and update the standards for new applications of the system.

Each message format is denoted by a message type (MT), for example MT 100 is the type known as *customer transfer* which is an inter-bank payment order originated by a bank's customer in favour of another bank's customer. Message types are divided into categories according to their first digit and there are at present eight categories (number 6 is not defined) which are listed in Figure 10.4. In each category n, the groups numberd n90 to n99 are for purposes common to all categories, for example group MT 499 is a free format message concerning documentary collection. The names of categories are self evident except perhaps for categories 4 and 7.

'Documentary collection' is a service provided to an exporter of goods to enable him to receive payment at the place of delivery in return for the shipping documents which give title to the goods. The exporter's bank instructs a bank at the place of delivery, which collects the payment for him. This avoids payment in advance, where the buyer is exposed, or billing the buyer after delivery (open account) where the exporter is exposed. An alternative way to handle the situation is 'documentary credit', for which category 7 messages are designed. The buyer instructs his bank which provides credit (up to a certain sum and time limit) enabling a bank in touch with the exporter to make payment on receipt of stipulated documents. The buyer receives the documents in return for the money, as before, the difference being that the exporter has already been paid.

A message contains a number of fields some of which are mandatory and others

Category	*Example groups*
1. Customer transfers	100 Customer transfer
2. Bank transfers	202 Bank transfer in favour of third bank
3. Foreign exchange, loans/deposits	300 Foreign exchange confirmation 350 Advice of loan/deposit interest payment
4. Documentary collections	400 Advice of payment
5. Securities	50n Orders and offers
6. Reserved for future use	
7. Documentary credits	71n Issue and amendment
8. Special payment mechanisms	88n Bank card authorization
9. Special messages	900 Confirmation of debit

Some of the message groups have standards that are agreed but are not yet implemented.

Others exist for interim use while awaiting finalization of standards.

Fig. 10.4 Examples of S.W.I.F.T. message groups and categories

optional. The demarcation of each field is by a message tag, for example the tag '15:' denotes the test key. Taking as an example the customer transfer (MT 100), the mandatory fields are

20: transaction reference number
32A: value date, currency code, amount
50: ordering customer
59: beneficiary customer

The fields are sufficient for the simplest kind of transaction where the ordering customer — the person making the payment — has an account with the bank which sends the message and the beneficiary customer has an account with the bank which receives the message. The sending and receiving bank do not appear as fields in the message text because they are contained in the header of the message which directs it through the system.

For technical and accounting reasons, not all pairs of banks can usefully exchange messages. Full connectivity would imply a million or more possible links each with an authentication key and account relationship, which is not practical. Therefore, smaller banks specialize in transfers with certain countries, offering this service in competition with other banks. Consequentrly the accounts of the ordering customer and the beneficiary customer may not be in the banks sending and receiving the messages.

As many as four other banks in addition to the sending and receiving bank may be involved in the transaction and it is this kind of complexity which led to errors when payment messages were less formal, before S.W.I.F.T. existed. Figure 10.5 shows the messages and payment in the most complex case. These messages have fields denoting

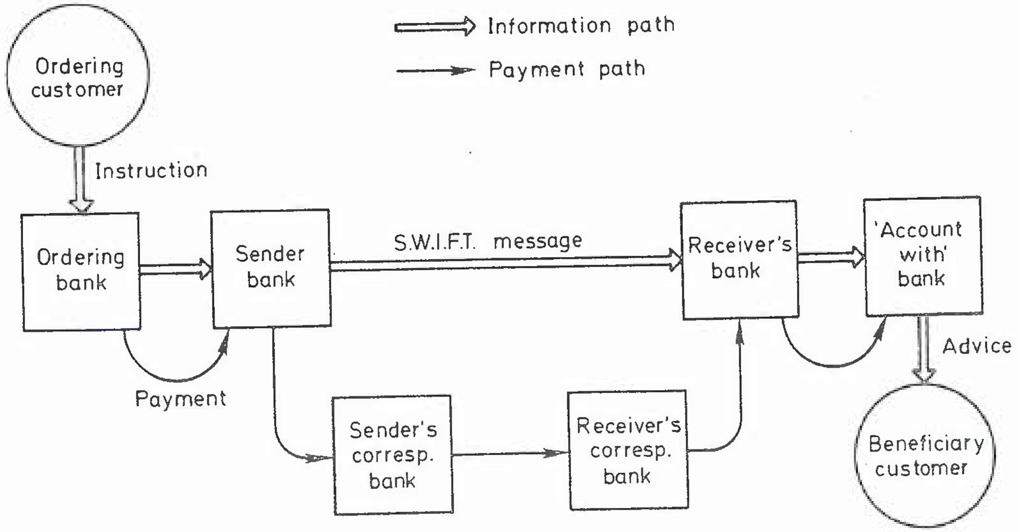


Fig. 10.5 A complex customer transfer by S.W.I.F.T.

52: ordering bank
53: sender's correspondent bank
54: receiver's correspondent bank
57: 'account with' bank.

The ordering bank sends a message to the sending bank (which originates the S.W.I.F.T. message) and also transmits the funds to this bank. The receiving bank makes the payment to the beneficiary via the bank which holds his account, that is the 'account with' bank.

The payment between sending and receiving bank is often made by an account held by one of these banks for the other. Whether this is the sender's account with the receiver bank or the receiver's account with the sender bank depends on the currency in which the transaction is made. If the currency is that of the country of the receiver bank then the receiver debits an account held by the sender in this bank. Alternatively, if the currency is that of the country of the sending bank, the sending bank credits the account of the receiver which it holds for him. Credits and debits for these accounts and statements of account can be sent as special messages in category 9.

In some cases it is necessary for the payment to go through intermediate banks working either on behalf of the sender or receiver. The message says that the payment will be made this way by quoting the correspondent banks in the fields with tags 53: or 54:. Any of the additional four banks referred to in these optional fields can be present or absent in a customer transfer message. Messages to the sender's and receiver's correspondent banks to effect these payments are quite independent of the S.W.I.F.T. message which goes direct from sending to receiving bank.

Formats are defined in a similar way for a large number of message types. New message types are being developed. In each message group there is the possibility to send free format messages for purposes not covered in the standards, using the digits 99 to signify free format, for example 199 in the customer-transfer group.

There is no doubt that the careful definition of these message types and their formats has been an important byproduct of the introduction of the S.W.I.F.T. message service.

Security in the S.W.I.F.T. system

The most important security features are authenticity and integrity. There have been a number of spectacular frauds by generating bogus payment messages between banks under manual systems of operation. In each case the authentication of messages was at fault.

The general properties of an authenticator algorithm were described in chapter 5 with some examples. The details of the S.W.I.F.T. authenticator are not public knowledge. As in any authenticator, the sharing of this key between sender and receiver bank and its secrecy from all others is the basic requirement for secure authentication.

The responsibilities for authentication are clearly defined. The algorithm is provided by S.W.I.F.T. (and in some cases the software in a terminal within which the algorithm is implemented). Keys are exchanged bilaterally between banks and are not known to S.W.I.F.T. or its personnel, but S.W.I.F.T. has issued guidelines about the exchange of authenticated keys suggesting the procedures to be used and the timing of key changes. Members can regard S.W.I.F.T. as a forum to assist their co-operation in the security matters but the responsibility for the safe exchange of keys lies entirely with the members.

An authenticator does not prevent messages being replicated, deleted or stored and retransmitted later. These requirements are handled by the sequence numbering of messages. Sequence numbering within the S.W.I.F.T. network ensures that messages are not lost or duplicated. The connection between S.W.I.F.T. and its users is safeguarded by input and output sequence numbers. The S.W.I.F.T. operating centre checks the format and input sequence number of messages offered to it and refuses those which have format errors or wrong sequence numbers. The output from the S.W.I.F.T. operating centre contains an output sequence number which must be checked by the receiver. The transaction reference number provides an end-to-end sequence control for each pair of banks and is included in the part of the message to which the authenticator is applied.

The interface between S.W.I.F.T. and a member bank must be protected against the introduction of false messages which have correct sequence numbers and authenticators. This is a matter for the individual banks who carry the ultimate responsibility for declaring that a message is valid and should be passed into the S.W.I.F.T. system. For this reason, SIDs and other connection arrangements normally provide for the assembly of a message by one person and the checking of the message and its release for transmission by a second person. The software and hardware of the connection must be protected against unauthorized changes because they administer these precautions and also store the authenticator algorithm and its keys.

Terminals coming on line to the system must verify their identity by a password. The passwords are issued by S.W.I.F.T. in the form of tables which are sent in two parts, A and B. By sending them separately the interception of a complete password set is made less likely. Password tables must be acknowledged to S.W.I.F.T. by an authorized person before they are activated on the system. Each table contains a sequence of passwords listed against a sequence number. Each login employs the next password in the sequence so that interception of passwords by line tapping gives no clue to the next password that will be needed. To avoid the trick of extracting passwords by impersonating the S.W.I.F.T. system to the terminal, each password is given a response number which the user must receive from S.W.I.F.T. and check before beginning transactions. The formalities and procedures for introducing new password tables and the method of fall back when problems occur are carefully defined.

In the central part of the S.W.I.F.T. system which consists of the operating centres, regional processors and connecting lines, the security is the responsibility of the S.W.I.F.T. organization. Access to the system, its software and the users' messages is strictly controlled and so is physical access to the areas containing the computer systems. The international lines which connect operating centres together and join them to regional processors are protected by encryption to preserve the privacy of the banks' messages. It is a matter for the individual bank to decide whether to use encryption on the line between its SID and the regional processor but S.W.I.F.T. will offer help. Privacy, though important to some, is not such a cardinal security factor as authentication. This is why end-to-end encryption is not provided, whereas authentication is end-to-end. The authentication allows the use of keys which are not known to S.W.I.F.T. but end-to-end encryption would prevent the useful role of S.W.I.F.T. in storing, validating and retrieving messages.

The chief inspector's office has overall supervision of security and privacy and performs security audits. Internal and external auditing are carried out at random intervals to make sure that the security of data and of all S.W.I.F.T. operations is being maintained.

The S.W.I.F.T. system provides an excellent lesson in the careful design of system security. Similar systems like CHIPS and CHAPS, though they differ in detail, employ similar principles for authentication, sequence numbering, login and other security features.

The Clearing Houses Automated Payments System

The Clearing Houses Automated Payments System (CHAPS) network carries payment messages between banks, like S.W.I.F.T. The basic security requirements of the two systems are similar, but when they are examined in more detail, differences appear, due to their different institutional framework, geographical coverage and settlement methods. A comparison of the two systems is instructive.

S.W.I.F.T. provides the facility for carrying messages between any of its banks. Any pair of banks which use it make their own arrangements for keys to authenticate messages travelling between them and arrange a route for settlement of debts between them. CHAPS is operated by a small group of 'settlement banks', who all do substantial business with each other, so it is a closer-knit community. These banks offer a means for large payments between about 300 other banks in the UK, most of them branches of foreign banks which use London as a business centre. The attraction of the settlement banks as intermediaries lies in their facility for *same-day* settlement using accounts they hold at the Bank of England. Cheque-clearing settlement in the UK takes place via CHAPS, in addition to its main function of payments between bank customers. The facility of same-day settlement for individual payments is called 'town clearing'. It has been done in the past by carrying paper documents within the compact business centre of 'the City' — a square mile (2.5 km^2) containing the offices of most of the 300 banks involved. In order to let the Bank of England arrange its funds before close of business, the individual payments stop at 15.00 hrs and the settlement between the thirteen banks follows immediately. About 19 000 payments took place per day with a total of £17 000 million. The movement of paper documents in the city is by bank messengers on foot.

The method worked well but had two limitations due to its old-established transport method. It was limited to the city. Banks elsewhere had to correspond with settlement banks by telephone or telex messages which was inconvenient and required careful discipline to keep it secure. The service was expensive per message and, though this cost was small compared with the interest saved by immediate access to funds, it led to a lower limit of £10 000 on individual transactions allowed to use the system. The CHAPS payment system is an automation of town clearing, using a computer-based message system between the settlement banks (of which the Bank of England is one). Some of these banks share gateways into the system, for economy. There is no limitation on where the point of entry to CHAPS is placed, which makes it possible for Scottish banks to have access points placed near to the banks they will serve. Additions to the group of settlement banks are not often made but further access points are feasible whenever they are needed.

The message format has been chosen with the aim of easy conversion to or from S.W.I.F.T. standards because instructions for payments via S.W.I.F.T. will often initiate payments through CHAPS. When a payment has been sent into CHAPS, settlement that day is part of the implied agreement, therefore a bank acting on a S.W.I.F.T. payment message must be sure of the source of the funds. Members of CHAPS compete in providing settlement facilities, balancing the value of the business against the risks they take. If a CHAPS payment has to be cancelled, this can only be done by a contrary payment, which needs the agreement of the payee.

Figure 10.6 shows the physical structure of CHAPS. Unlike S.W.I.F.T. it has no central operation, but uses messages transferred through the packet-switched public data network called Packet Switchstream (PSS). The integrity of the system depends on 'gateways' implemented in Tandem non-stop computers with software that has been jointly developed. Each message receives a logical acknowledgement via PSS back to the originating gateway, so that the performance of the system is continually monitored. The high availability of PSS and the Tandem computers is fundamental to the design. The gateways administer time stamps, sequence numbers and running totals for each bank pair. With each message from A to B, the total 'paid' by A to B since the last settlement is reported,

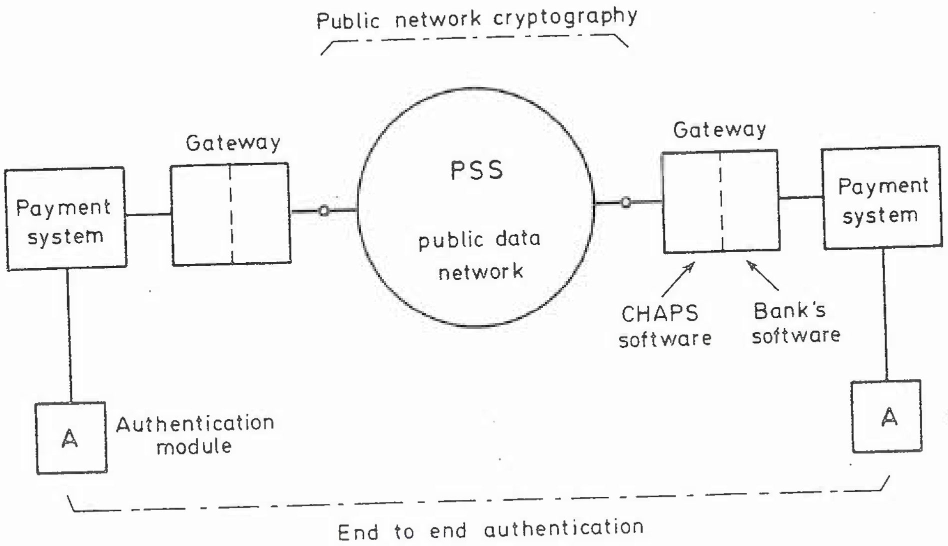


Fig. 10.6 Structure of the CHAPS system

like a bank statement that is always up-to-date. Consequently, at the end of business for the day, agreement on the accounts can be immediate and settlement follows by a message to the Bank of England.

Each bank's arrangements for message processing outside the CHAPS interface are its own concern. The large banks run a payment process in their own main-frames. Smaller banks (those with less CHAPS activity) can run their payment process in the Tandem that holds the gateway.

Clearing houses automated payments system is different from S.W.I.F.T. because same-day settlement through the central bank is an integral feature of its operation. The physical and organizational structure is also different. It is operated by a more centralized group of banks but the network has a more distributed structure. The security requirements are very similar to those of S.W.I.F.T. and are primarily concerned with authentication of messages and less critically with the confidentiality of messages.

The authenticator used in CHAPS is the Data Encryption Standard (DES) in its cipher-block chaining mode. It is implemented in the tamper-resistant hardware modules which hold the keys and perform the tasks of generating and checking authenticator values. The key management reflects the structure of CHAPS in which each pair of banks has an individual relationship. It employs master keys used to protect session keys which are transmitted over the network. Though the method of authentication has been agreed by the settlement banks, authentication is an end-to-end matter and is the responsibility of the two banks concerned. The payment system has been designed to be transparent to the message content, except for its procedure of handling the payment fields.

Confidentiality is provided by encipherment at the point of entry to PSS and decipherment at the exit from PSS. The main security feature is the authentication procedure, implemented in the bank's payment process with the aid of the special hardware module. Because the two processes of generating and checking authenticators are carried out in the physically secure modules, the ability to generate authenticators can be confined to the sender. In this way, some of the useful properties of a signature are obtained in a system which uses a symmetric cipher, the DES.

10.4. AUTOMATIC TELLER MACHINES

Early automatic teller machines (ATMs) were essentially cash dispensers which had only one function, to deliver cash in the form of bank notes and debit a corresponding bank account. To identify the user, tokens were used in the form of cards of various kinds. Some early machines used punched cards that had only one life — they authorized one payment only and were not returned to the user, who had to obtain a supply of cards from his bank. There were also magnetic cards with a limited life, for example twenty withdrawals of cash. These early machines functioned for one bank, dispensing cash only to customers of that bank. To reduce the risk of lost cards being misused it was usual, right from the beginning of cash dispensers, to issue a personal identification number (PIN) to the customer which is entered on a keyboard to complete the identification. Many of these early cash dispensers were off-line; they worked on their own without connection to a central data base. They were located at first inside the bank where they provided an alternative to the human tellers. After some experience had been gained, cash dispensers were installed in the 'through the wall' position in which they were part of the bank building but available from outside it when the bank was closed. In this way banks could provide 24-h cash service — a factor which is becoming even more important with the growing competitiveness of banking organizations.

A third kind of location which was entirely away from the bank developed later. This can provide greater convenience but the cost of installation makes it suitable only in places with a large access to users, for example shopping centres and very large work areas which are remote from banks. The real value of these remotely sited cash dispensers or ATMs arrives when a single ATM can be used by the customers holding 'cash cards' of many different financial institutions.

The increase in remoteness from the bank increases the problems of physical security. One of the earliest crimes against 'through the wall' cash dispensers was to pull them completely out of the building with a heavy machine. Now these dispensers are built like a strong safe and fixed to the concrete foundation.

By adding further facilities, cash dispensers began to deserve the name of 'automatic tellers'. These can be used for enquiries about the status of accounts, for transfers between the customer's own accounts (such as deposit and checking accounts) and possibly for credit transfers from a customer's account to some other person's account. The machines can deliver travellers cheques instead of money and they can accept deposits, though in doing the latter they add little to the facilities of a bank deposit box. The most important function of automatic teller machines is still that of dispensing cash (or travellers cheques in countries where these are needed) and this is the operation requiring the greatest attention to security because any weakness which allowed cash to be withdrawn without authority would quickly render the service untenable to the banks. One of the primary requirements of a cash dispenser or ATM transaction is, therefore, to identify the customer as reliably as possible.