(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 January 2002 (03.01.2002)

PCT

(10) International Publication Number
WO 02/01515 A2

(51) International Patent Classification[7]: G07F 7/00

(21) International Application Number: PCT/GB01/02820

(22) International Filing Date: 26 June 2001 (26.06.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0015713.1 27 June 2000 (27.06.2000) GB

(71) Applicant *(for all designated States except US)*: **PURSEUS LTD.** [GB/GB]; 1 Finsbury Square, London EC2A 1AA (GB).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **EVERETT, David, Barrington** [GB/GB]; 31 Ashdown Avenue, Saltdean, Brighton, East Sussex BN2 8AH (GB). **BARKER, Richard, David** [GB/GB]; 52 Woodstock Road, London W4 1UF (GB). **JONES, Timothy, Lloyd** [GB/GB]; 14 Withdean Road, Brighton BN1 5BL (GB). **FERGUSON, Keith, Martin** [GB/GB]; Lona, North Hill, Little Baddow CM3 4TB (GB).

(74) Agent: **BOYDELL, John, Christopher**; Stevens Hewlett & Perkins, Halton House, 20/23 Holborn, London EC1N 2JD (GB).

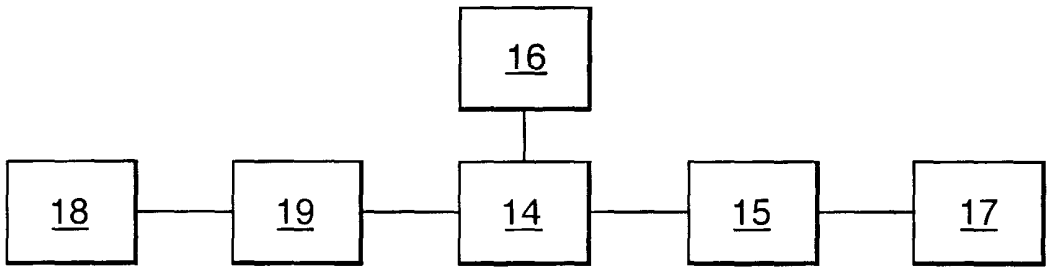
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: PAYMENT PROCESS AND SYSTEM FOR TRANSFERRING VALUE



(57) Abstract: A method of transferring value from a payer to a payee via an intermediary. In one example, value is transferred from a payer smart card (18), associated with a payer terminal (19), to a payee smart card (17), associated with a payer terminal (15), via an intermediary (14) having an intermediary smart card (16), by means of two separate card to card transfers. To initiate the transfer, the payer sends payer transaction data, including the identity of the payee, and signed with the payer's digital signature, to the intermediary (14). The intermediary derives the payer transaction data, checks the authenticity of the data and, if all is well, receives the value to be transferred from the payer. The intermediary (14) now repeats the process with the payee, but utilising the intermediary's digital signature. The payee checks the authenticity of the transaction data and, if all is well, receives the value to be transferred from the intermediary. In alternative embodiments some or all of the smart cards (16, 17 and 18) are replaced by hardware situated in a tamper resistant enclosure.

WO 02/01515 A2

PAYMENT PROCESS AND SYSTEM FOR TRANSFERRING VALUE

This invention relates to a payment process and system by which value may be transferred from a payer to a payee via an intermediary.

As part of a financial transaction between two parties it is often necessary to use an intermediary who accepts instructions from the payer and effects the payment to the payee using one of the available payment systems. Such payment systems are provided by financial institutions such as the banks or other approved organisations, using payment protocols based on the use of credit or debit cards, electronic purses or interbank schemes such as CHAPS or S.W.I.F.T. Smart cards are often used as part of these payment operations, providing a secure environment for the software application used for payment, together with a means of authenticating the payer. Some smart cards may provide both processes.

An example of a smart card payment system is provided by Mondex International Ltd., who have developed a payment protocol for such a system. The basic system provided by Mondex is described in their international patent application No. WO 91/16691. Systems developed to the Mondex specifications allow value to be transferred from an electronic purse on one smart card to an electronic purse on another. In their normal form they allow the payer to transfer funds to a merchant in exchange for goods or services. Such systems also allow person-to-person payments where each party holds a smart card suitably enabled with the Mondex application. When used in this mode it is not normally necessary to authenticate the payer since from a practical point of view such payments may be considered anonymous. Nor is it normally necessary to record the transaction details for audit purposes; the authenticity of the payment instructions are adequately assured by the Mondex payment protocol.

However there are situations where it may nevertheless be necessary to use an intermediary to effect the payment between two parties. This might arise, for example, when the payer has no knowledge

of the payee's purse, which is a necessary condition to effect a payment of the Mondex type. A similar situation can arise when the payer smart card is not authorised to make payments to the payee smart card or when the payee smart card is not authorised to receive a payment from the payer smart card. In both these situations payment can be achieved through the use of an intermediary. It may also be a requirement for the intermediary to record the transaction details for auditing by regulators or other interested parties.

An intermediary is also necessary to effect dvp (delivery versus payment) transactions. In such transactions the intermediary acts as a trusted party who can hold a payment in escrow until a certain condition is met, for example, goods have been delivered. Such transactions are not only involved in the payment for goods, but also in payment for services, or for transactions involving trading exchanges or foreign currency exchanges.

When using an intermediary in such situations it is necessary that the payment instruction from the payer should be authenticated to ensure payment to the correct payee. Such authentication requires a cryptographic process that can be implemented between the payer smart card and the intermediary. To simplify this operation and to avoid using unnecessary memory in the payer's smart card it is desirable to use existing operations already provided by the smart card or to use very simple applications that can be added to the smart card.

The present invention seeks to provide a payment process and system for enabling the transfer of value from a payer to a payee via an intermediary. Advantageously, if the payer uses a smart card, the transaction details and in particular the data capable of identifying the payee unambiguously, are preferably incorporated into an authentication method that involves the authorisation of the payer by using existing facilities on the smart card or by using an application that can be added to

the smart card to achieve the same effect. Preferably, it should also be possible to record the transaction details for audit purposes.

A knowledge of one of the payment systems, such as the Mondex system, is advantageous for a full understanding of the present invention. However, the present invention is not restricted to any particular payment system. The use of a contact smart card is also assumed in this description but the technique is equally applicable to contactless smart cards or cards containing both types of interfaces.

According to a first aspect of the invention there is provided a payment process enabling the transfer of value from a payer to a payee via an intermediary, said process comprising the following steps:-

the payer sends payer transaction data, including the identity of the payee, and signed with a digital signature, to the intermediary;

the intermediary derives the payer transaction data sent by the payer, checks the authenticity of the data, receives the value sent by the payer and prepares intermediary transaction data, based on the payer transaction data and signed with a digital signature, in respect of the transfer of value from the intermediary to the payee identified in the payer transaction data;

the payee or the intermediary checks the authenticity of the data, and receives the value transferred from the intermediary.

The digital signature is obtained by encrypting the transaction data using a cryptographic key with one of the well known cryptographic algorithms. The key used by the payer – referred to herein as the payer key – is known to, or its complement is known to, the intermediary. Likewise the key used by the intermediary – referred to herein as the intermediary key – it known to, or its complement is known to, the payee. Preferably the payer key is different to the intermediary key.

The security sensitive operations are preferably carried out in a tamper resistant module. A tamper resistant module provides a secure

environment for the sensitive operations, and may comprise a secure hardware enclosure in which the sensitive electronics is housed, or secure software in otherwise physically unprotected circuitry, or a mixture of both. For the purpose of the present invention, the smart card acts as a tamper resistant module and it is quite possible for the different parties in the transaction to have tamper resistant modules of different types: for example, the payer and payee could have smart cards, and the intermediary could have a more sophisticated secure enclosure. The problem with smart cards is that, because of size constraints, their power and functionality is limited. A more sophisticated tamper resistant module can contain high specification microprocessors, memory and hard disks to achieve very fast processing for multiple operations. Whichever type of tamper resistant module is used, it is necessary that it carries the required application software and memory to be able to perform the necessary security checks, and also, of course, to hold the value to be transferred, for example, in an electronic purse carried by the module. For example, where the payer uses a smart card, he or she initiates the process by placing the smart card in a card reader forming part of a terminal which is in communication, temporary or otherwise, with the intermediary. The terminal may be a special dedicated piece of apparatus, or a more general item, like a PC.

Thus, in the preferred embodiment of the invention the process comprises the steps of, at the payer:

entering details of the transaction into a terminal in communication with the intermediary, creating a payer cryptogram of payer transaction data including said transaction details, and including the identity of the payee, using a payer cryptographic key known to or whose complement is known to the intermediary, sending a payer message including at least the payer cryptogram to the intermediary;

at the intermediary:

receiving the payer message, verifying the authenticity of the payer transaction data by checking the correctness of the payer cryptogram, transferring value from the payee to the intermediary, deriving intermediary transaction data from the payer transaction data, creating an intermediary cryptogram of said intermediary transaction data, using an intermediary cryptographic key known to or whose complement is known to the payee; and

at the intermediary or the payee:

verifying the authenticity of the intermediary transaction data by checking the correctness of the intermediary cryptogram, and transferring value from the intermediary to the payee.

According to a second aspect of the invention, there is provided a payment system for enabling the transfer of value from a payer to a payee via an intermediary, said system comprising,

at the payer:

a terminal into which information relating to the transaction may be entered by the payer, means for preparing payer transaction data, including the identity of the payee, means for encrypting said transaction data to produce a payer cryptogram using a payer cryptographic key known to or whose complement is known to the intermediary, and means for sending a payer message including at least the payer cryptogram to the intermediary;

at the intermediary:

means for verifying the authenticity of the payer transaction data by checking the correctness of the payer cryptogram, means for enabling the transfer of the value from the payer to the intermediary, means for deriving intermediary transaction data from the payer transaction data, means for creating an intermediary cryptogram of said intermediary transaction data, using an intermediary cryptographic key known to or whose complement is known to the payee; and

at the intermediary or payee:

means for verifying the authenticity of the intermediary transaction data by checking the correctness of the intermediary cryptogram, and means for transferring the value from the intermediary to the payee.

It will be seen that the transfer of value takes place in two separate stages: first from payer to intermediary and then from intermediary to payee. The second of the stages may take place immediately after the first, as a continuous process, or there may be a delay, possibly a long delay, between the two stages. In the meantime, the value transferred from the payer to the intermediary is held in escrow for the payee, in a storage means at the intermediary. In practice, it is likely that the value transferred from the payer will be passed into a storage means at the intermediary, even if the value is transferred onwards immediately. Also in practice, it is quite possible that the payee may hold an account with the intermediary and therefore it would be the payee's account at the intermediary that would be the recipient of the second stage of the value transfer and, in this case, the intermediately, acting on behalf of the payee, would carry out the authentication of the intermediate transaction data. Thus references herein to sending data from the intermediary to the payee, and the authentication of that data by the payee, should be read in this context.

By payer transaction data is meant data relating to the transaction and includes transaction details entered by the payer, such as the identity of the payee and the size of the value to be transferred, and some information generated internally by the payer's terminal, such as the transaction date, the identity of the smart card (if used), and the identity of the payer (if the payer uses a smart card, it is likely that his or her identity will be recorded within the card's memory).

Preferably the security sensitive operations at the payer, the intermediary and the payee, are carried out in a secure environment. To

this end, each of the payer, intermediary and payee is provided with a tamper resistant module, as discussed above. Thus, the tamper resistant module may, in each case, comprise a smart card, or advantageously may comprise more conventional hardware situated in a tamper resistant enclosure. The use of conventional hardware enables the functions of the smart card to be realised, but with higher capacity and higher speed. Smart cards need only be used if the value transfer protocol in use only allows card to card transfers (such as Mondex). In addition to the smart card functions, the tamper resistant enclosure may contain hardware, such as hard disk storage, capable of realising additional functions.

If, for example, the payer is using a tamper resistant module in the form of a smart card, then this will be inserted into a card reader associated with the payer terminal at the commencement of the transaction, and the secure operations at the payer will be carried out by the card. In order to commence the transfer of value, the payer first enters certain transaction details, including the identity of the payee and details of the value to be transferred, via a keyboard or keypad associated with the payer terminal, or its card reader (if used), or even the card itself, if it includes its own keypad. Preferably the payer also enters a personal code, such as a PIN so that a software application on the payer's smart card can check its validity and thus securely link the payer with his or her smart card. A software application on the payer's smart card next encrypts the payer transaction data using a secret payer cryptographic key to produce the payer cryptogram which forms at least a part of the message which is sent to the intermediary. The payer cryptographic key will be held by the payer, for example in the memory of his smart card, and will be known to, or derivable by, the intermediary.

Encryption can be by way of any of the known methods, such as DES or RSA. In both DES and RSA, there is a limit to the amount of data that can be handled at once and, in this event a reduced-size version of

the payer transaction details is taken. This reduced-size version may be created by a hashing operation which is a cryptographic operation whose purpose is to reduce the size of the transaction data to manageable proportions to enable it to be encrypted.

In the DES system, the maximum block size which can be handled is 64 bits. In this case, therefore, the reduced-size version may be produced by a combined hashing and encrypting operation in which the payer transaction data is divided into small units, say of 8 bytes length. The units are then operated on one at a time starting, for example, at the beginning, and working through all of the units sequentially. To do this, each unit is encrypted, using the same key and the same function and the encrypted output of each unit is added to the next prior to encryption. When all of the units have been cycled through, the resultant output will be derived from all of the units.

In the RSA system, the maximum block of data that can be handled is related to the key size and is typically 1024 bits, but even this can be exceeded by the size of the payer transaction data. If this is the case, then, prior to encryption, the transaction data can be reduced in size by one of the known hashing functions. One such function is known as SHA-1 and is defined by the US National Institute Standards Technology (NIST) body. It is also possible to utilise the above-described combined hashing and encrypting operation, using a symmetric algorithm such as DES to reduce the size of the transaction data prior to encryption by RSA.

A hashing function is capable of reducing the original payer transaction data down to typically 20 bytes in length, which can be comfortably handled by the RSA system. However, the hash operation is normally a one-way process. In other words, the original data cannot be recreated from the hashed data. In this event, the message sent from the payer to the intermediary will additionally need to contain a copy of the transaction data which is in the clear (i.e. not hashed or encrypted) so that

the intermediary, by carrying out the same hashing and/or cryptographic operation on this additional data, can compare it with the cryptogram sent by the payer, thus confirming the authenticity of the payer transaction data.

The output of the hash operation may still be too large for the system in use to handle, in which case the reduced-size version of the transaction data may consist of just a selection of the hashed output bytes. For example, if the output of the hash operation is 20 bytes in length, just 10 bytes, chosen at random could be taken. As a matter of practice, it is preferred to take a concatenation of the first few and last few bytes in the hash – for example, the first 3 and the last 4 to make a 7-byte resultant. Provided that the intermediary knows what the payer is doing to the transaction data, the necessary action can be taken to authenticate the data by replicating the payer's actions.

The message sent by the payer, and subsequently received by the intermediary thus contains two elements: the original payer transaction data, in the clear, and the payer cryptogram of that data, digitally signed using the payer's secret key. When the intermediary receives the message it is passed to the intermediaries' tamper resistant module where the security sensitive operations are carried out. In outline, these operations comprise the authentication of the payer transaction data by comparing the two elements of the message: that sent in the clear, and that which is encrypted. To properly carry out this comparison, some preliminary actions must be taken on the received data, as will be explained below. If the result of the comparison is favourable, then intermediate transaction data based on the payer transaction data sent in the clear is made and is digitally signed by the intermediaries' secret cryptographic key in the same way as is described above in relation to the payer. A second message is now prepared, containing two elements: the intermediary transaction data, sent in the clear and a cryptogram of that data – the intermediary cryptogram signed by the intermediaries' secret cryptographic key. It will

be understood that the preparation of the second message, at the intermediary, proceeds in the same way as has already been described above in relation to the payer and will not therefore be repeated; however, it is not necessary for the exact same operations to be used in the preparation of the second message – for example, a different hashing method could be used.

The second message, once prepared, is output from the intermediaries' tamper resistant module and is passed to the payee. As explained above, the transmission to the payee may well not happen immediately.

It was stated above that the intermediate transaction data is "based on" the payer transaction data. It is possible that the intermediate transaction data may be identical to the payer transaction data. However, there are circumstances in which the payer transaction data needs to be modified to form the intermediate transaction data. There are various reasons why the transaction data sent on to the payee may be different to that received from the payer. For example, some of the contents of the payer transaction data may not be needed for the second stage, or the payer may have asked for anonymity, in which case all data which could identify the payer would be stripped from the payer transaction data before it is sent to the payee.

The comparison operation as between the two elements of the message received by the intermediary will now be discussed. It will be recalled that the two elements comprise the payer transaction data, in the clear, and the payer cryptogram of that data. If the payer cryptogram has been obtained by a reversible cryptographic operation – such as RSA – then the comparison operation can be effected by first decrypting the cryptogram, using the payer's public key (known to the intermediary), followed by a direct comparison of the payer transaction data with the decrypted cryptogram. However, if a non-reversible cryptographic

operation – such as DES – is used, and/or if a hashing operation is used, then a straight comparison of the decrypted data cannot be made. In this case, the intermediary takes that element of the payer transaction data sent in the clear and, prior to the comparison, carries out the identical hashing or combined hashing/cryptographic operation as was carried out at the payer. Once this has been done, the next stage depends upon the nature of the hashing operation used. If a combined hashing/cryptographic operation, such as DES described above, was used at the payer then, once the same operation has been carried out at the intermediary, the two encrypted versions – that prepared at the payer (i.e. the payer cryptogram) and that prepared at the intermediary – can be directly compared. If, however, the hashing operation at the payer was followed by a RSA encryption operation, to form the payer cryptogram, then the payer cryptogram element of the message received by the intermediary will have to be decrypted before a comparison is made – thus, in this case, the intermediary compares the resultant of an identical hashing operation as was carried out at the payer on the payer transaction data element of the message received by the intermediary was the decrypted payer cryptogram element of the message received by the intermediary.

The cryptographic key used for decryption depends on the system in use: in the DES system, the payer's secret key, which is also known to the intermediary, is used. In variants of DES, for example, triple DES, each individual is allocated two or more secret keys which will be known to the intermediary. In the RSA system, the intermediary uses the payer's public key to decrypt.

It will be seen that the hashing operation provides a convenient way of enabling the authentication of the data sent from the payer to the intermediary. The same comments apply, mutatis mutandis, to the transfer from the intermediary to the payee. If there is no hashing or equivalent operation, there is no need to additionally send the payer

transaction data in the clear. However, other methods of authenticating the sent data would then have to be used. For example, the transaction data can be loaded with redundant information (i.e. information not essential for the transaction) which can be checked at the other end. For this purpose, the receiver of the information – the intermediary or the payee – needs to know what the redundant information is, so that a comparison can be made after decryption by the receiver. Preferably also the redundant information changes periodically or for each transaction. One example of redundant information might be a transaction number which sequences onwards by a known amount for each transaction. As long as the receiver knows what the sender is doing with the transaction data, a comparison can be made.

An additional function which is of importance is the ability for the intermediary to create a log file of all transactions for audit purposes. Such a log file can contain full transaction details of all transactions during both the payer to intermediary stage and during the intermediary to payee stage. Preferably the log file will contain copies of the complete messages that enter and leave the intermediaries' tamper resistant module so that the whole history of the transaction can be studied. Thus the log file stores the payer transaction data (in clear) and its accompanying payer cryptogram, together with the intermediary transaction data (in clear) and its accompanying intermediary cryptogram. It will be seen form this that the contents of the log file can itself later be checked by carrying out similar operations on the data to that described above.

After the intermediary has successfully authenticated the transaction data sent by the payer, a conventional value transfer protocol is used to transfer the value from the payer to the intermediary. Once this has been done, the communication channel between the payer and the intermediary can be closed. The value is stored temporarily at the intermediary either in short term memory such as RAM or, more likely, in long term memory

such as a hard disk. In both cases the memory is located within the tamper resistant enclosure.

The intermediary next establishes a channel of communication with the payee identified in the payer transaction data. For this purpose, the payee may periodically, or as a result of an e-mail or similar notification from the intermediary, make contact with the intermediary. In some cases there may be a permanent connection between the intermediary and the payee, for example, where the payee has an account at the intermediary (see above). Once a connection is made, the method proceeds in substantially the same way as described above in connection with the transfer from the payer to the intermediary.

The transaction data sent by the intermediary is first optionally reduced in size, for example by a hashing operation, and is then encrypted in the same way as described above, but using the intermediary's cryptographic key or keys. There is in fact no need to use the same cryptographic system for the second stage as for the first, although normally the same will be used. Likewise hashing may be used in the first stage and not the second, or vice versa, or it may be used in both stages.

At the payee, the transaction data sent by the intermediary – the intermediary transaction data – is decrypted using the appropriate cryptographic key or keys, as described above. The payee may have a tamper resistant enclosure, as with the intermediary, or they may have a smart card which will be used in a similar manner to the payer's smart card, except to make the above-described decryption and comparison of the intermediary transaction data.

Once the authenticity of the intermediary transaction data has been established by the payee, a payment protocol can be used to effect the actual transfer of value from the intermediary to the payee.

By checking the correctness of the payer and intermediary cryptograms, the intermediary or payee, as appropriate, is able to ensure

that the correct payment transaction is made to themselves. In this way authenticated payment transactions can be made between a payer and a payee by means of an intermediary where the correct identity of the payee is assured.

In order that the invention may be better understood, several embodiments thereof will now be described by way of example only and with reference to the accompanying drawings in which:

Figure 1 is a schematic drawing of a smart card for use in the transfer process according to the invention;

Figure 2 is a block diagram of a payment terminal suitable for use in the transfer process;

Figure 3 is a block diagram showing the transfer method of the invention, using smart cards at payer, payee and intermediary; and

Figure 4 is a block diagram similar to Figure 3, showing an alternative embodiment using a mixture of smart cards and tamper proof modules.

The basic components of the simplest payment system are a payer, an intermediary and a payee. More complex systems may comprise more than one intermediary between the payer and the ultimate payee and the method of this invention can be applied to all of the steps from the payer to the payee, or only to some of them, as required. The links between the payer and the intermediary and between the intermediary and the payee may be temporary links or permanent links and may be effected by any of the known methods such as direct connection, telephone connection, or internet connection.

As already mentioned, the payer, the payee and the or each of the intermediaries preferably has a tamper resistant module in which to perform the various security sensitive operations and to store security sensitive data such as the cryptographic keys. The nature of the tamper resistant module will depend upon the circumstances, and need not

necessarily be the same as between the various components of the system. One example of a tamper resistant module is a smart card.

An example of a typical smart card will now be described with reference to Figure 1. A more sophisticated tamper resistant module will provide essentially the same, and probably enhanced, functionality due to the use of upgraded (and probably physically larger) components.

Referring to Figure 1 there is shown a smart card 1 having on one surface a contact plate 2 carrying several separate electrical contacts whereby an external power source may be connected and a serial communication channel established with the card. The card further comprises a microprocessor 3, a read only memory 4, a random access memory 5 and a non volatile memory such as EEPROM 6.

The memories 4 or 6 hold one or more software applications which define the operations of the card. The cryptographic key or keys are normally held in the memory 6.

In order to use the card in the authentication process it is inserted into a card reader forming part of a terminal which can communicate with an intermediary. A simplified diagram of a suitable terminal is shown in Figure 2. The terminal 7 comprises a processor 8, memory 9, a display 10, a keypad 11, a smart card reader 12, and communications port 13 for connection to the intermediary by either direct link, telephone lines, or through an existing communications infrastructure such as the Internet.

In Figure 3 a block diagram of a first example of a payment system is shown. A payer smart card 18 is connected to a payer terminal 19, which connects to the intermediary 14, which itself has an intermediary smart card 16. The intermediary 14 also has a connection to a payee terminal 15 which includes a payee smart card 17.

The authenticated payment process operates as follows:

The payer inputs the transaction details at the keypad 11 forming part of the payer terminal 19. The details include such things as the payer

and payee names (32 chars each), the payer and payee identity codes (16 chars each) which are known to the intermediary, the amount of the payment (16 chars), the currency of the payment (4 chars), the payment date and time (12 chars), a payment reference field (16 chars) and a supplementary free format reference field (512 chars). The terminal display 10 presents a form to the payer with default fields such as date, time, payer name and identity codes pre-filled to allow simple data entry. The payer can accept or alter these fields as required.

A program executing in the payer smart card 18 takes these transaction details and reduces their size, using the SHA-1 hashing algorithm, to produce a message digest of 20 bytes length. If the payment system in use is not able to operate with a message digest as long as this, then the transaction details may be reduced in size still further. For example, the Mondex card to card payment protocol can only handle a message of up to 7 bytes, in which case, for example, the first three bytes and the last 4 bytes of the message digest may be concatenated together to form a seed that will be used for the authentication check in the associated software application. The payer also enters their personal code (PIN) at the key pad 11 which enables the smart card to authenticate itself with the payer, using conventional techniques.

If the payer has entered their PIN correctly then the payer smart card 18 will return a cryptogram using the public key algorithm operated by the particular payment system in use. This cryptogram is obtained by encrypting the complete message digest, or the smaller seed, using the payer's public key (stored within the card 18), and is equivalent to a digital signature using the secret key contained within the payer's smart card. The terminal 19 also obtains from the smart card 18 the public key certificate that relates to the use of the key involved in the signature operation.

The terminal 19, using its internet or direct connection, next sends to

the intermediary 14, the transaction details, in clear, the signature cryptogram, and the public key certificate as a "payment request" message. Such a payment request message forms a part of the protocol of all electronic payment systems. When the intermediary 14 receives the payment request message, a software program in the intermediary smart card 16 first checks the authenticity of the payment request message by taking the transaction details, sent in clear from the payer, and calculating a 20 byte message digest and possibly a 7 byte seed of these transaction details, using the SHA-1 hash algorithm in the same way as calculated by the payer's terminal. It will be understood that, for a valid comparison to be made at the intermediary, the intermediary must carry out the same operations on the transaction data as were carried out at the payer. The program operating at the intermediary also sends the received cryptogram to the attached smart card 16 which latter contains an authentication check function. The smart card 16 decrypts the cryptogram to produce what should be the same 20 byte message digest or 7 byte seed value as was calculated at the payer's terminal 19. The card next carries out a comparison to check that the decrypted cryptogram is the same as the 20 byte message digest or 7 byte digest (as appropriate) that was calculated at the intermediary. If it is, then the authenticity of the payment instructions is assured. If it is not, then it is assumed that there has been corruption of the data, deliberate or otherwise, and the transaction is aborted.

Having established the authenticity of the payment instructions, the intermediary 14 now proceeds through a standard payment protocol with the payer's terminal 19 between the payer's smart card 18 and the intermediary's smart card 16. The protocol follows that defined in the specification of the particular payment system, for example, Mondex, being used. The payment value and currency are defined in the transaction details, as described previously.

On successful completion of the value transfer the intermediary 14 stores as part of a transaction audit trail log the data received in the payment request message, which includes the identity of the payer and payee and the complete message that forms the payment protocol between the payer and intermediary smart cards. This data also includes the identity of any electronic purses carried by the smart cards.

A second "payment request" message is now prepared within the intermediary smart card 16. This second message contains the intermediate transaction data (in the clear) which is prepared from the received payer transaction data, together with a cryptogram of the intermediate transaction data, prepared at the intermediary. The intermediary cryptogram is prepared in the same or similar way to the payer cryptogram and is digitally signed using the intermediaries' public key.

The intermediary 14, using the payee name field and the payee identity code, checks a database at the intermediary to set up the next stage of the payment transaction, namely from the intermediary smart card 16 to the payee's smart card 17. The intermediary's database includes the identity of any electronic purses, carried by the payee smart card. The intermediary also confirms that the name and code fields correspond. A notification may be sent to the payee by e-mail to advise him of the payment authorisation.

The payee's terminal 15 periodically or as the result of the e-mail notification connects through the Internet to the intermediary 14 to effect the value transfer previously authorised. Before undertaking the value transfer the intermediary checks that the identity of any electronic purse presented by the payee corresponds to a purse held by the payee as stored on the intermediary's database. Once this check is completed satisfactorily, the second payment request message is transmitted from the intermediary to the payee, and the process described in detail above is

carried out as between the intermediary and the payee. The complete payment message between the intermediary 14 and the payee is also stored at the intermediary as part of the transaction audit trail log.

In the case where the payee has an account at the intermediary there is, of course, no need to contact the payee, except by way of information, and no need to set up an external communications link from the intermediary to the payee. Authentication of the intermediary transaction data is carried out, in the same manner as described above, but at the intermediary and, indeed, preferably within the intermediary's tamper resistant module. Once the authentication check has been carried out successfully, the value is transferred from the intermediary's holding account to the payee's account.

The transaction audit trail log is stored in the form of a database at the intermediary which can be queried using standard SQL protocol. This allows the intermediary to prepare reports for each transaction that includes the identity of the payer and payee, the value and currency of the transaction, the date and time, and the identity of any purses carried by the cards.

The intermediary also prepares summary data that shows the value and currency contained in all the electronic purses known to the intermediary and the transactions relating to their current state.

If the purses involved in this example are Mondex purses, then they are preferably personalised in such a way that the purse classes held by the payer and payee can only effect payments between themselves and purse classes held by the intermediary. They are not allowed to make payments directly between the payer and payee class purses. This ensures that the intermediary is aware of all transactions involving these purses.

Although we have assumed the use of smart cards at the intermediary 14 and the payee terminal 15 they may not be necessary

unless the payment system in use requires it – the Mondex system, for example, is a card to card payment system.

In Figure 4 there is shown an alternative example of a payment system in which the intermediary 14 at least, and possibly the payer and payee as well, use a more sophisticated tamper resistant module instead of a smart card, this allowing much faster processing of multiple payment transactions.

In Figure 4, the intermediary is as in Figure 3, except that the security sensitive components are situated in a sophisticated tamper resistant module, which effectively takes the place of the smart card 16 of Figure 3.

The effective payer, shown under reference 20, takes the form of the payer's bank, the actual payer being represented by the box 21. Likewise, the effective payee, shown under the reference 22, takes the form of the payee's bank, the actual payee being represented by the box 23. The actual payer and payee 21,23 may be an individual or a corporate body, and it is assumed that they are each linked to their respective banks, as represented by dotted lines, by any of the conventional methods. Thus the payer, for the purposes of the present invention, can be considered as the combination of the payer bank 20 and its customer 21. Likewise the payee can be considered as the combination of the payee bank 22 and its customer 23. Of course, it is possible that the payer and payee banks 20,22 may actually be the same organisation.

Since banks and similar financial organisations will be handling a large number of transfer requests from their customers, it makes sense to utilise the fastest hardware possible to carry out the authentication processes necessary to carry out the method of the present invention. Thus it is preferred that the payer and payee banks 20,22 each use a sophisticated tamper resistant module to house the security sensitive

hardware, enabling the highest-speed hardware to be used for the authentication and other processing. However there is no reason in principle why a bank smart card could not be used for these functions.

The payment process itself in the arrangement of Figure 4 is very similar to that described above in relation to Figure 3, and will not be repeated in detail. The differences lie in the fact that the actual payer and payee 21,23 may well be physically separated from their respective banks 20,22 at the time they initiate or receive the payment process. It is assumed that each bank will use its own methods to communicate with its customers, and that these methods will be secure. Thus, for example, when the actual payer 21 initiates a payment, the required transaction details, as discussed above with reference to Figure 3, will be transferred up to the payer's bank 20 by a method which is assumed to be secure (the method could, of course, involve authentication techniques similar to those described herein). At the payer bank 20, the same actions are then carried out as described above in relation to the payer in the Figure 3 system prior to the payment request message being communicated to the intermediary 14. The same action operates, only in reverse, at the payee end 22, 23.

CLAIMS

1. A payment process enabling the transfer of value from a payer to a payee via an intermediary, said process comprising the following steps:-

the payer sends payer transaction data, including the identity of the payee, and signed with a digital signature, to the intermediary;

the intermediary derives the payer transaction data sent by the payer, checks the authenticity of the data, receives the value sent by the payer and prepares intermediary transaction data, based on the payer transaction data and signed with a digital signature, in respect of the transfer of value from the intermediary to the payee identified in the payer transaction data;

the payee or the intermediary checks the authenticity of the intermediary transaction data, and the payee receives the value transferred from the intermediary.

2. A payment process as claimed in claim 1 comprising the steps of,

at the payer:

entering details of the transaction into a terminal in communication with the intermediary, creating a payer cryptogram of payer transaction data including said transaction details, and including the identity of the payee, using a payer cryptographic key known to or whose complement is known to the intermediary, sending a payer message including at least the payer cryptogram to the intermediary;

at the intermediary:

receiving the payer message, verifying the authenticity of the payer transaction data by checking the correctness of the payer cryptogram, transferring value from the payee to the intermediary, deriving intermediary transaction data from the payer transaction data, creating an intermediary cryptogram of said intermediary transaction data, using an intermediary cryptographic key known to or whose complement is known to the payee;

and

at the intermediary or the payee:

verifying the authenticity of the intermediary transaction data by checking the correctness of the intermediary cryptogram, and transferring value from the intermediary to the payee.

3. A payment process as claimed in claim 2 wherein at least the step, at the payer, of creating a payer cryptogram, is carried out in a tamper resistant module.

4. A payment process as claimed in either one of claims 2 or 3 wherein at least the steps, at the intermediary, of verifying the authenticity of the payer transaction data, deriving the intermediary transaction data, and creating an intermediary cryptogram, are carried out in a tamper resistant module.

5. A payment process as claimed in claim 4 wherein the step of verifying the authenticity of the intermediary transaction data is carried out in the tamper resistant module at the intermediary.

6. A payment process as claimed in any one of claims 2 to 4, wherein a least the step of verifying the authenticity of the intermediary transaction data, is carried out in a tamper resistant module at the payee.

7. A payment process as claimed in any one of claims 2 to 6 wherein said payer message further includes the payer transaction data, in clear.

8. A payment process as claimed in any one of claims 2 to 7 wherein said intermediary message further includes the intermediate transaction data, in clear.

9. A payment process as claimed in either one of claims 7 or 8 wherein said payer cryptogram is created by encrypting said payer transaction data using said payer cryptographic key.

10. A payment process as claimed in claim 9 wherein the correctness of the payer cryptogram is checked, at the intermediary, by decrypting the payer cryptogram contained within the message received from the payer,

and comparing the decrypted payer cryptogram with the payer transaction data contained within the message received from the payer.

11. A payment process as claimed in any one of claims 7 to 10 wherein said intermediary cryptogram is created by encrypting said intermediary transaction data using said intermediary cryptographic key.

12. A payment process as claimed in either one of claims 7 or 8 wherein said payer cryptogram is created by encrypting a reduced-size version of said payer transaction data using said payer cryptographic key.

13. A payment process as claimed in either one of claims 7, 8 or 12 wherein said intermediary cryptogram is created by encrypting a reduced-size version of said intermediary transaction data, using said intermediary cryptographic key.

14. A payment process as claimed in either one of claims 12 or 13 wherein said reduced-size version comprises a digest produced by applying a hashing algorithm to said payer transaction data, or said intermediary transaction data, as appropriate.

15. A payment process as claimed in claim 14 wherein said reduced-size version comprises a seed consisting of selected bytes of the digest.

16. A payment process as claimed in any one of claims 12, 14 or 15 wherein the correctness of the payer cryptogram is checked, at the intermediary, by producing a reduced-size version of the payer transaction data contained within the message received from the payer, decrypting the payer cryptogram contained within the message received from the payer, and comparing the decrypted payer cryptogram with the reduced-size version of the received payer transaction data.

17. A payment process as claimed in either one of claims 7 or 8 wherein said payer cryptogram is created by a combined encryption and hashing operation applied to said payer transaction data, and using said payer cryptographic key.

18. A payment process as claimed in claim 17 wherein the correctness

of the payer cryptogram is checked, at the intermediary, by carrying out the same combined encryption and hashing operation on the payer transaction data contained within the message received from the payer, and comparing the resultant of such operation with the payer cryptogram contained within the message received from the payer.

19. A payment process as claimed in any one of claims 2 to 18 wherein the intermediary transaction data is the same as the payer transaction data.

20. A payment process as claimed in any one of claims 2 to 18 wherein the intermediary modifies the payer transaction data to create the intermediary transaction data.

21. A payment process as claimed in any one of claims 2 to 20 wherein the intermediary creates a log of the transaction, including the payer and payee identities.

22. A payment process as claimed in claim 21 wherein the log contains copies of the payer and intermediary messages.

23. A payment process as claimed in either one of claims 21 or 22 wherein said log is stored by the intermediary as a transaction log file for audit purposes.

24. A payment system for enabling the transfer of value from a payer to a payee via an intermediary, said system comprising,

at the payer:

a terminal into which information relating to the transaction may be entered by the payer, means for preparing payer transaction data, including the identity of the payee, means for encrypting said transaction data to produce a payer cryptogram using a payer cryptographic key known to or whose complement is known to the intermediary, and means for sending a payer message including at least the payer cryptogram to the intermediary;

at the intermediary:

means for verifying the authenticity of the payer transaction data by checking the correctness of the payer cryptogram, means for enabling the transfer of the value from the payer to the intermediary, means for deriving intermediary transaction data from the payer transaction data, means for creating an intermediary cryptogram of said intermediary transaction data, using an intermediary cryptographic key known to or whose complement is known to the payee; and

at the intermediary or payee:

means for verifying the authenticity of the intermediary transaction data by checking the correctness of the intermediary cryptogram, and means for transferring the value from the intermediary to the payee.

Fig.1.

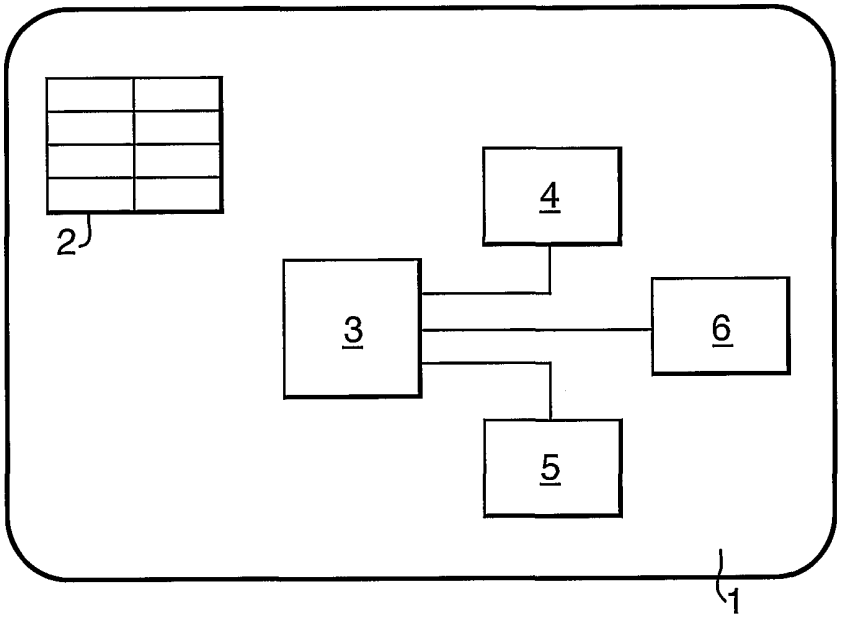


Fig.2.

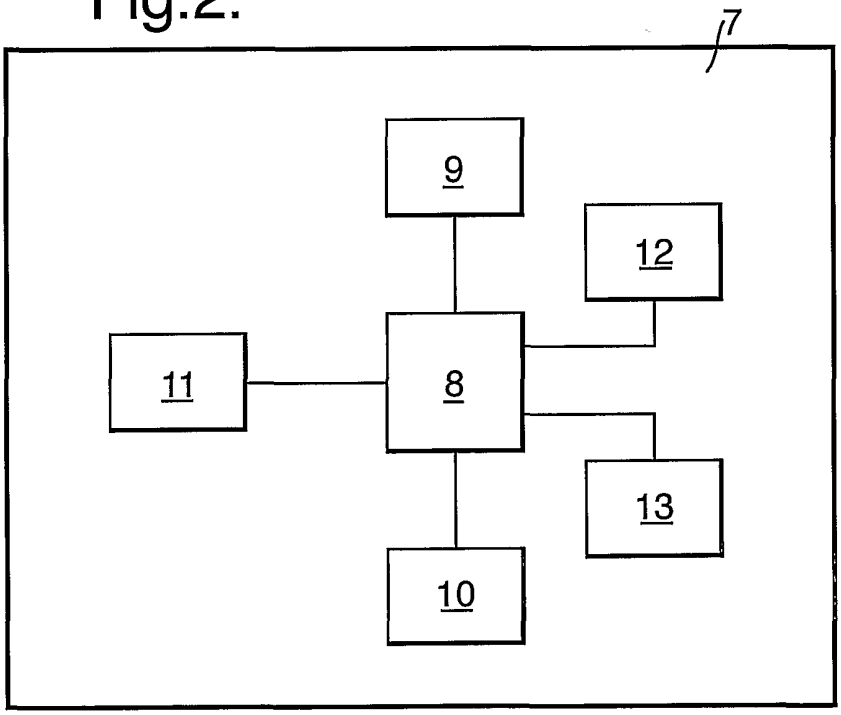


Fig.3.

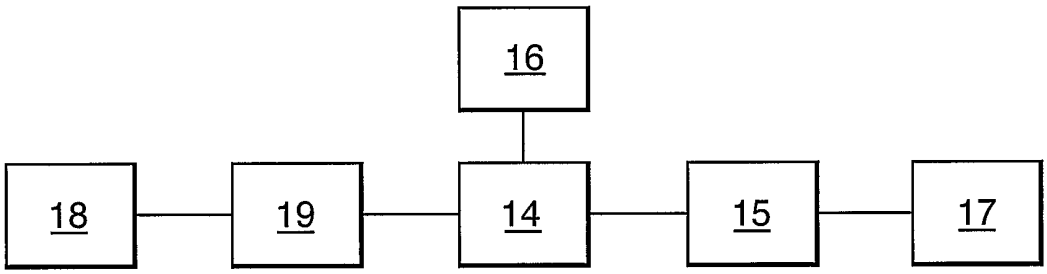


Fig.4.