PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : G07F 7/08, 7/10, 19/00 — A1

(11) International Publication Number: WO 00/63854

(43) International Publication Date: 26 October 2000 (26.10.00)

(21) International Application Number: PCT/EP00/02843

(22) International Filing Date: 31 March 2000 (31.03.00)

(30) Priority Data:
99107726.4 19 April 1999 (19.04.99) EP

(71) Applicant: TELEFONAKTIEBOLAGET LM ERICSSON (publ) [SE/SE]; S-126 25 Stockholm (SE).

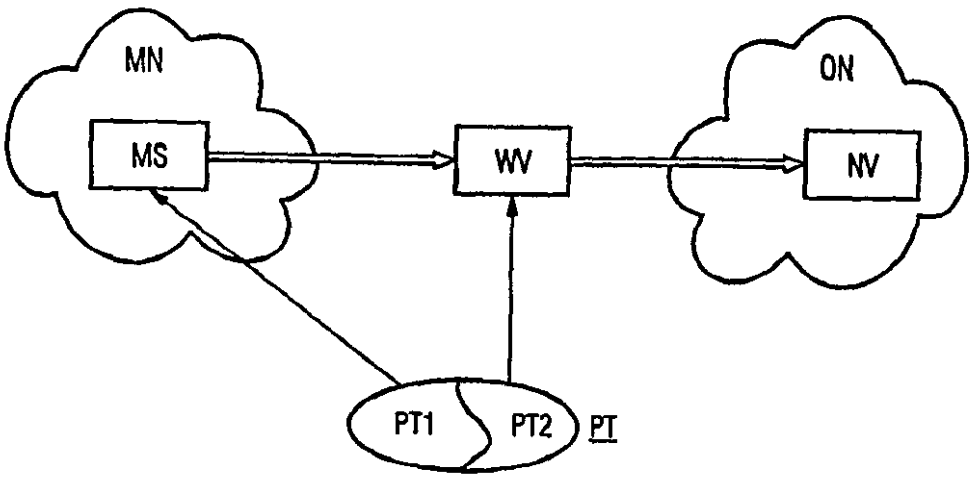
(72) Inventors: WRONA, Konrad; Weikenrather Str. 118B, App. 186, D-52074 Aachen (DE). ZAVAGLI, Guido; Alexanderstr. 37, D-52062 Aachen (DE).

(74) Agent: MOHSLER, Gabriele; Ericsson Eurolab Deutschland GmbH, Ericsson Allee 1, D-52134 Herzogenrath (DE).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, 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, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, 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), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: COMMUNICATION SYSTEM AND METHOD FOR EFFICIENTLY IMPLEMENTING ELECTRONIC TRANSACTIONS IN MOBILE COMMUNICATION NETWORKS



(57) Abstract

The invention relates to a communication system, a method and devices for an efficient implementation of electronic transactions between a mobile subscriber in a mobile communication network and a network facility by exploiting credit card based payment protocols. The protocol, which is used for realizing a secured electronic transaction, such as the SET™, is split over a plurality ofinvolved communication units. For realizing the invention, the first part of the protocol, which is usually contained in the mobile station of a user, is split into two parts. The first part containing the private data of a subscriber, such as the private key or the certificates, is maintained in the mobile station. The second part of the software is shifted to a server being positioned between the mobile station and the merchant. Thus, the invention guarantees on one hand the possibility of integrating complex software for an electronic way of payment in a network, which is characterized by a small transmission capacity and terminals having an insufficient storing capacity, and on the other hand the maintenance of security aspects on the user side. Additionally, the invention guarantees the compatibility with the already existing software.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

FIG. 1

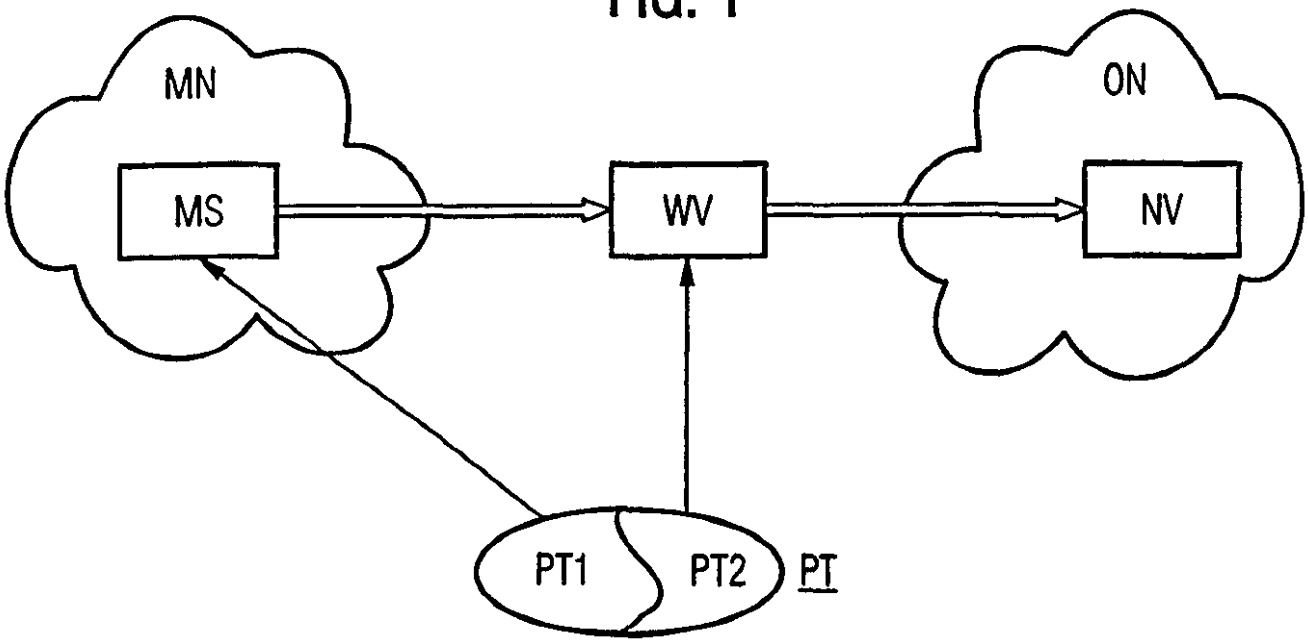

MN
MS
WV
ON
NV
PT1
PT2
PT

FIG. 2

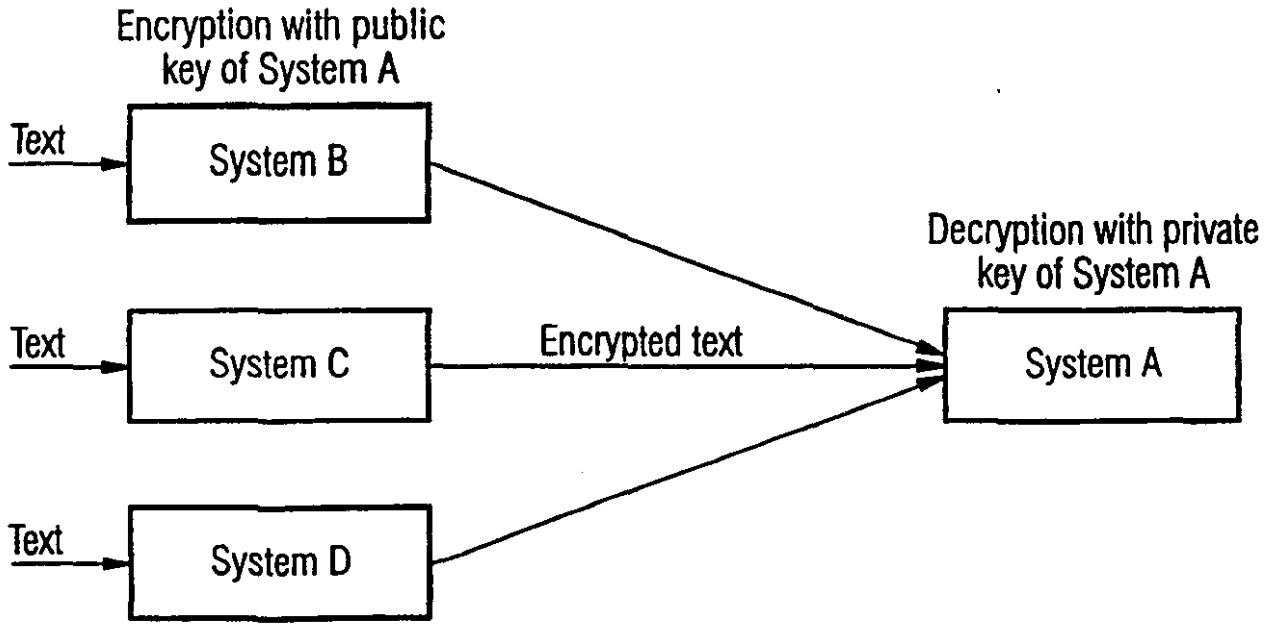

Encryption with public key of System A
Text
System B
Text
System C
Encrypted text
Text
System D
Decryption with private key of System A
System A

FIG. 3

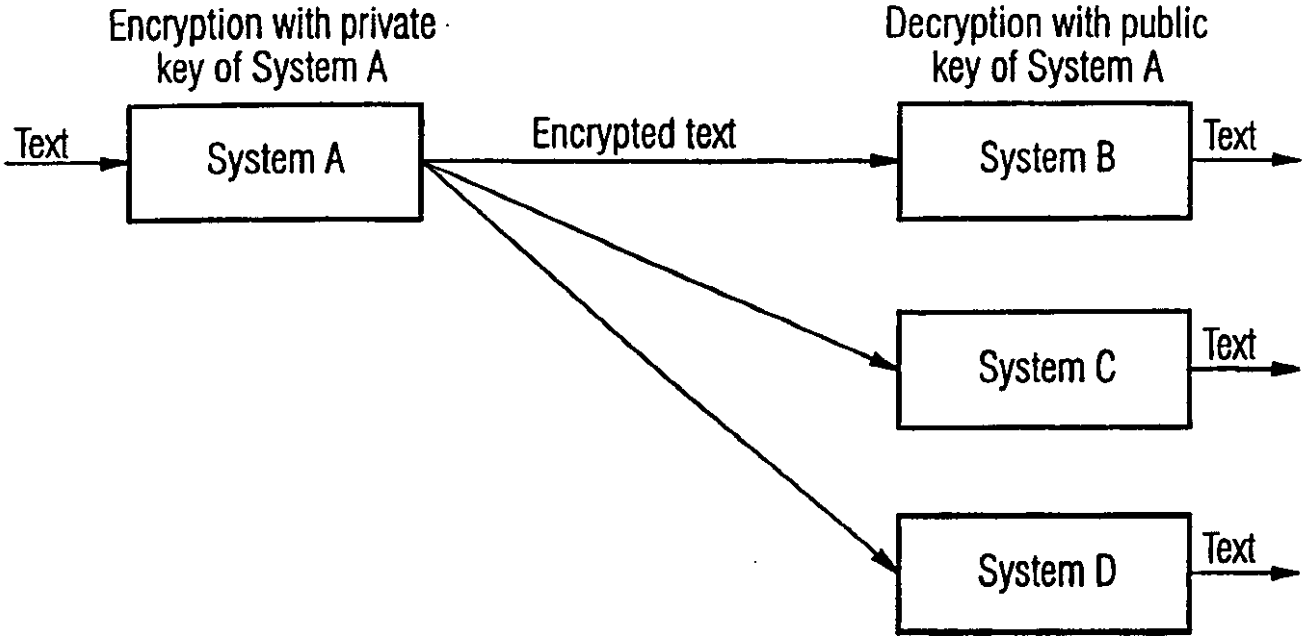

Encryption with private key of System A
Decryption with public key of System A
Text
System A
Encrypted text
System B
Text
System C
Text
System D
Text

FIG. 4

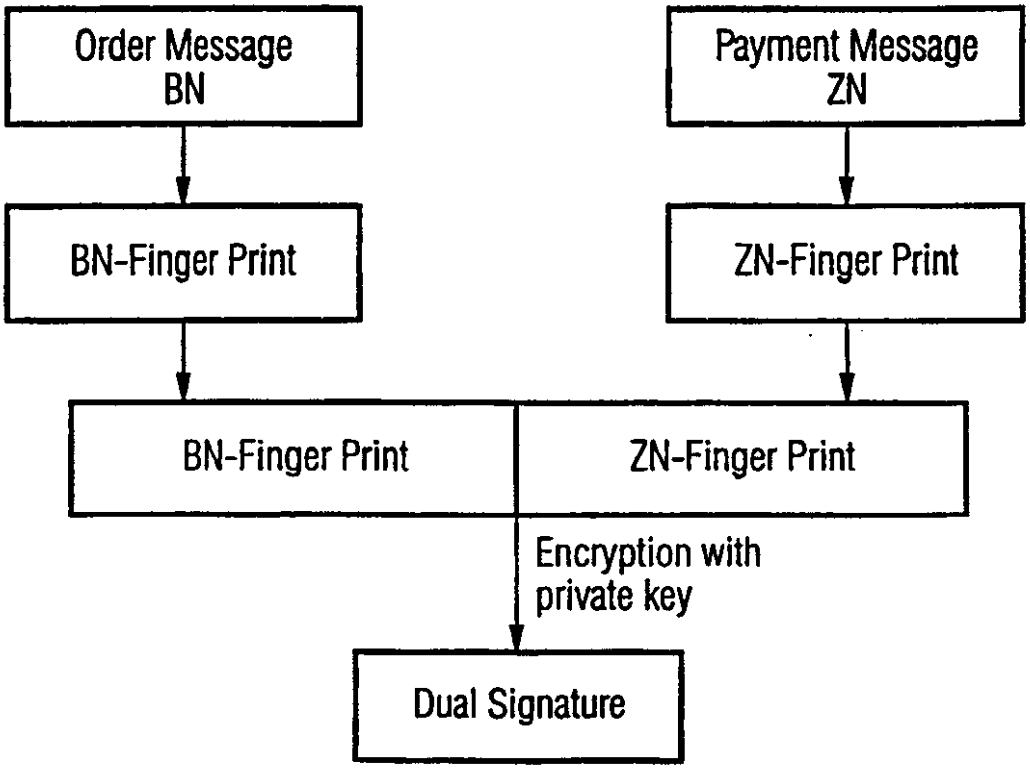

Order Message BN
Payment Message ZN
BN-Finger Print
ZN-Finger Print
BN-Finger Print
ZN-Finger Print
Encryption with private key
Dual Signature

FIG. 5

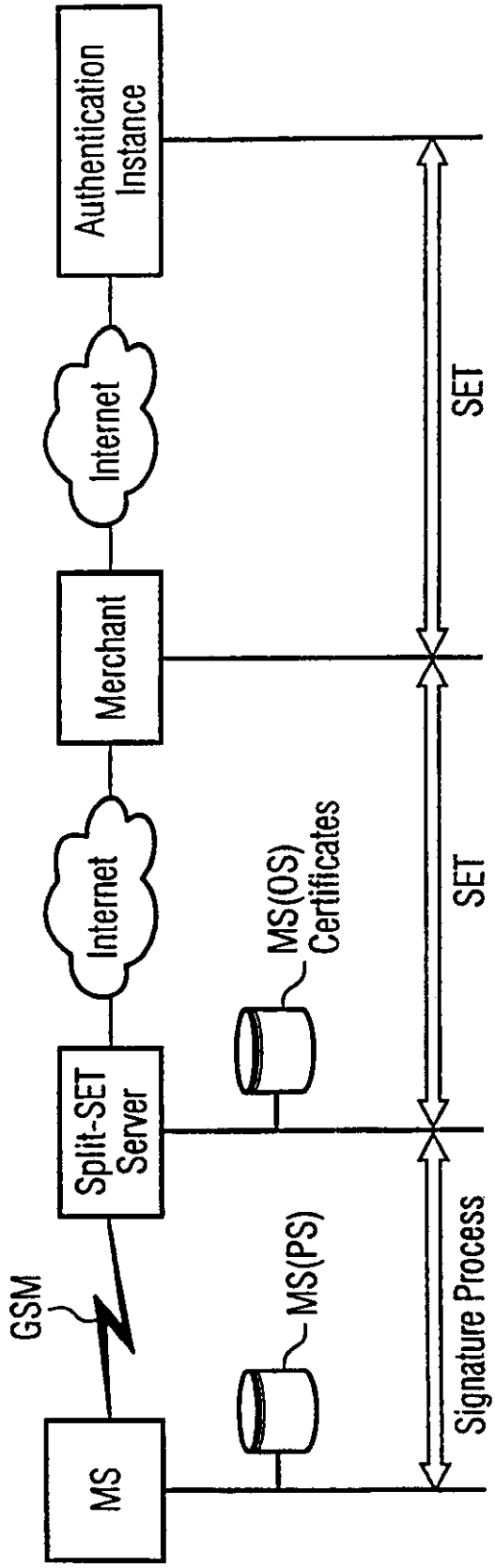
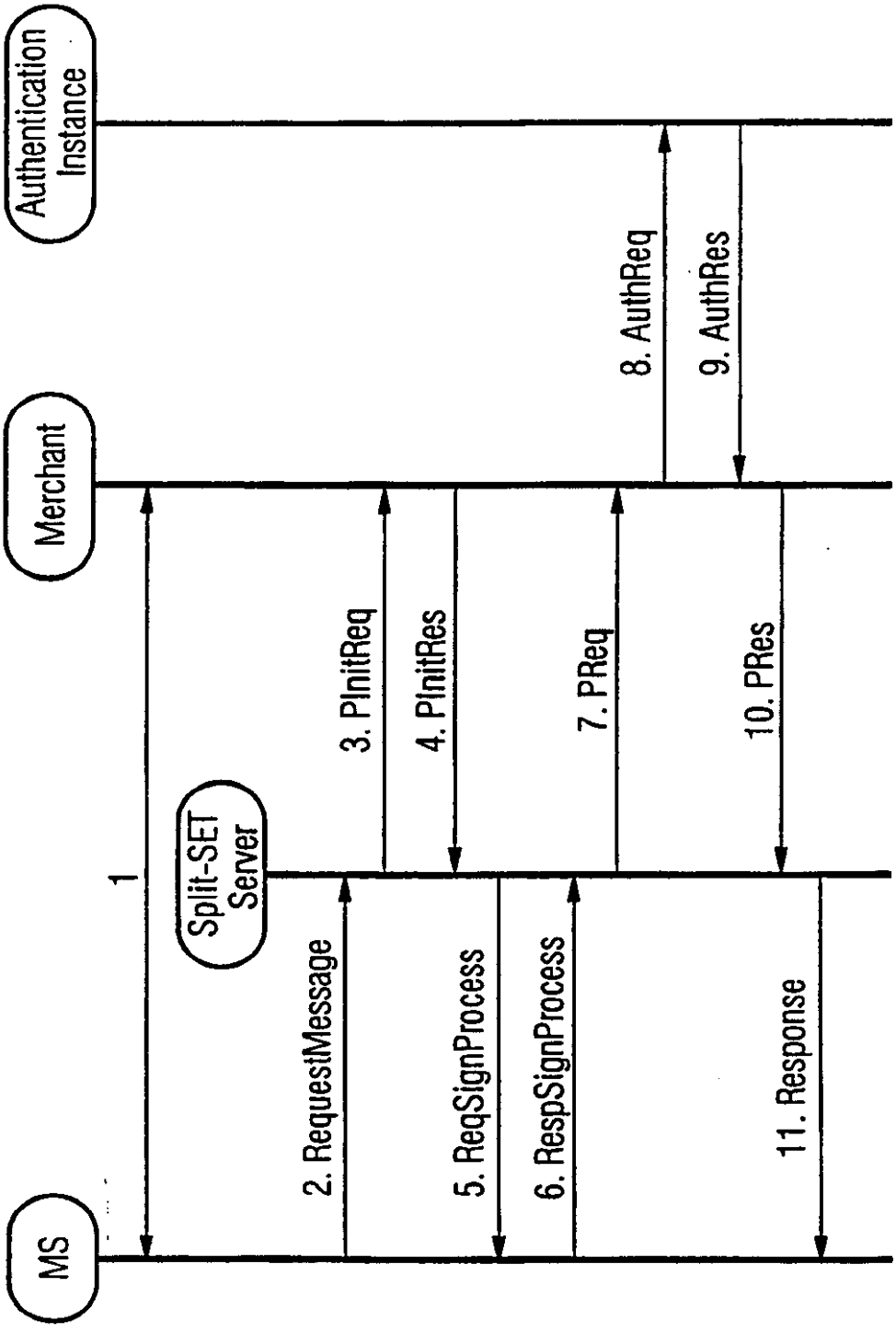

Authentication Instance
Internet
Merchant
Internet
Split-SET Server
GSM
MS
MS(OS) Certificates
MS(PS)
SET
SET
Signature Process

FIG. 6


Authentication Instance
Merchant
Split-SET Server
MS
1
2. RequestMessage
3. PInitReq
4. PInitRes
5. ReqSignProcess
6. RespSignProcess
7. PReq
8. AuthReq
9. AuthRes
10. PRes
11. Response

COMMUNICATION SYSTEM AND METHOD FOR EFFICIENTLY IMPLEMENTING ELECTRONIC TRANSACTIONS IN MOBILE COMMUNICATION NETWORKS

The invention relates to a communication system, a method and devices for efficiently implementing electronic transactions between a mobile subscriber in a mobile communication network and a network facility by exploiting credit card based payment protocols.

The possibility to electronically purchase goods, for example, is part of the various commercial services being available to an internet user. Companies offer their products in the network in the form of electronic catalogues, from which a user can choose, order and acquire goods from a range of products by clicking the mouse. The buying and selling of goods, services and information in the internet has been summarized under the name of the so-called electronic commerce. A request thereby made to the underlying network guarantees a secured implementation of electronic money transactions. The safety is thereby absolutely essential due to the fact that the handling of a payment transaction is done electronically.

For this purpose a plurality of protocols has been developed, which can be used for the realization of electronic payment procedures, such as Cyber-Cash, First Virtual and Secure Electronic Transaction (SET). It is characteristic for the protocols that these have been developed for a credit card based payment by complying with the safety requirements in connection with this form of payment correspondingly. In the following, the Secure Electronic Transaction SET™, SET™ specification version 1.0, of 5/31/97 is used as an example to explain the invention.

The protocols for implementing an electronic payment procedure particularly by means of a credit card were developed for a fixed network having sufficient transmission capabilities and sufficient storing capacities in the terminals. Said requirements are met, for example, by a network architecture, in which an internet user having a personal computer is connected with the internet via a fixed line. Said requirements are, however,

not met, if a user carries out an electronic transaction from a mobile communication network. A mobile communication network is characterized by a low transmission capacity and terminals having a small storing capacity. The terminals used in the mobile network are either mobile phones or devices incorporating an integrated function of a mobile phone as well as the function of a computer, the so-called PDA (Portable Digital Assistant). The size of said devices is kept to a minimum due to the mobility of the user. This merely requires the reduction of the storage capacity and results in that these devices do not have sufficient storage capacity in order to install, for example, the complex Secure Electronic Transaction (SET) protocol. In ServerWallet of Netlife, which is published under http://www.netlife.de/, a solution has been proposed, whereby the entire Secure Electronic Transaction (SET) protocol is shifted to a server specifically installed for this purpose. According to said publication the server is localized between a user and a merchant. The disadvantage of said solution is, however, that a user has no control concerning the safety aspects. The initiation of a transaction is initiated by a user and is transmitted to the server. Said server comprises the total software of the payment protocol including all pertinent data, also the personal data of the user, by means of which the initiated transaction is completely implemented by the server. This particularly means that the control and handling of the electronic transaction to be implemented is completely left to the server.

In accordance therewith it is the object of the invention to provide a method and a device allowing for an efficient implementation of secured payment transactions in a network. It is particularly the object of the invention to reduce the storage space requirement on the user side.

According to the invention this object is provided by the teaching of patent claim 1, by the teaching of patent claim 19 and by the teaching of patent claims 24 and 26.

It has thereby shown to be advantageous that by shifting part of the software to the server, fewer transactions are implemented via the air interface thereby improving the efficiency of the entire payment procedure via a mobile network. For this reason it is an advantage that the resources of the air interface are exploited in a more profitable manner.

Another advantage is seen in a minimum exploitation of the storage capacity available in terminals. This is obtained by storing only the private data of a user in a terminal.

It also an advantage that the invention is based on the standardized software. For this reason the compatibility with the available software is guaranteed, and a transparency of the implementation of a transaction is obtained for the merchant, i.e. the merchant cannot see whether a mobile user is concerned, or a user who is directly connected to a fixed network.

Additional advantageous developments of the invention result from claims 2 to 19, 20 to 23 and patent claim 25.

The invention is hereinafter explained by means of embodiments and figures, whereby

Fig. 1 shows a schematic illustration of the invention,
Fig. 2 shows an illustration of an asymmetric code,
Fig. 3 shows an scheme of an authentication ,
Fig. 4 shows an scheme of a dual signature,
Fig. 5 shows a network architecture with the logic representation of the used protocols,
Fig. 6 shows an information stream during a payment procedure.

The invention is hereinafter explained by means of patent claim 1 and figure 1.

According to the invention a protocol PT for the implementation of secured electronic transactions is split between a mobile station MS in a mobile communication network MN and an additional device WV being localized between the mobile station MS and a network facility in an open network ON. The splitting of the functionality of the protocol PT is effected in a first part PT1 and in an additional part PT2. The protocol PT realizes the implementation of an electronic transaction between the mobile station MS and the network facility NV via the additional device WV.

When splitting the protocol for implementing secured electronic transactions attention is paid that the mobile device receives the private data of the users and that the administration of the generally accessible data, such as the public key or the certificates, are taken over by another device. Thus, the implementation of the total transaction is controlled by the user, for the transaction is initiated by the user of the mobile station, which implements the signature process due to the available personal data, and the control of the results of the handled transaction is left to the mobile station. The handling of the remaining processes with the network facility relating to orders and payment instructions is controlled by the additional device. In this connection the additional device meets the complex security aspects, such as forming the dual signature.

In the following, the invention is explained in more detail by means of the Secure Electronic Transaction protocol SET™.

The Secure Electronic Transaction (SET) protocol is a complex protocol guaranteeing a secured payment via credit cards in an open network, such as the internet, by using distinct cryptographic techniques. During payment, signaling messages are exchanged in the network. Said messages are transmitted in an encrypted manner. The purpose of encryption is to protect the contents of the message to be transmitted against unauthorized access in order to thereby guarantee the confidentiality of the transaction. The transmitter encrypts the data with a secret information, the so-called key, and the receiver decrypts the data by using another key. In this respect it is not necessary that both keys are identical, which varies in response to the used cryptographic process. The so-called asymmetric coding process, for instance, uses two types of keys. This method provides a public key being generally accessible, and a private key being known exclusively to one communication instance. One key is used for encryption, and the other one is used for decrypting. With respect thereto it is important that the two keys must relate to each other, such that a message encrypted with a key can only be decrypted again with the other key. In general, the method of asymmetric encryption provides that the public key is used by a transmitter for encrypting a message to a receiver. The decryption is done by using the private key of the receiver.

This fact is explained in more detail by means of figure 2. Said figure shows three systems, system B, System C, system D, which plan to transmit a text to system A in an encrypted manner. According to figure 2, the public key of system A is used for encrypting the text. The public key of one unit is generally known and accessible by each system. The encrypted text is transmitted to system A. System A has the private key of A by means of which the received text is decrypted.

In addition to the asymmetric encryption there is the symmetric encryption process. In this method both communicating facilities have the same key with the result that a message is encrypted by a transmitter with the same key as is used for decrypting it by the receiver.

Apart from encryption messages to be implemented, an authentication of the communicating facilities is simultaneously implemented. The authentication guarantees that only persons can have access to certain data, who are authorized. In this context is it necessary to verify the identity of the communicating facilities. A number of different authentication methods can thereby be used. The best known method meeting particularly fully developed security requirements is known by the name of strong authentication. The strong authentication works according to the principle of the asymmetric encryption method. In contrast to the encryption, the authentication provides that the public key is used for decrypting a message encrypted with a private key. This fact can be inferred from figure 3. According to figure 3, the transmitter, system A, encrypts a text with his private key, which in figure 3 is called the private key of system A, and transmits it to systems B, C and D. Said systems decrypt the received message with the public key of system A.

By means of this method each facility is capable of decrypting the message, as the public key of the transmitter used for decrypting is generally known. Thus, it is obtained that a subscriber is able to authenticate himself towards each system. The systems request the authentication to be successful, as the message could only be encrypted by means of the private key on the transmitter side, which leaves to assume that this side only has knowledge of the private key.

The method of "strong authentication" is used with digital signatures. The digital signature is used for determining the authenticity of electronically transmitted messages and constitutes the electronic equivalence to the hand-written signature. By checking digital signature it can be established whether the pertinent message has been altered. A digital signature has the property that it can be produced correctly by only one single person, but that it can be verified by all receivers of the message. The asymmetric encryption methods are suited for this purpose. However, due to the long processing times not the entire document is encrypted, but a so-called cryptographic finger print also called "hash" is computed from the document, which is attached to the document in an encrypted manner. The encrypted cryptographic finger print corresponds to the digital signature. The receiver makes sure that the message received really comes from the transmitter by producing a control finger print from the received document and by comparing the same with the finger print of the transmitter decrypted with a public key.

Due to the required security, Secure Electronic Transaction (SET) uses an expanded form of digital signature, the so-called dual or double signature. The dual signature allows two split messages to be connected by a common signature such that they cannot be decrypted when being connected. The scheme of the dual signature is illustrated in figure 4. Two cryptographic finger prints, BN finger print and ZN finger print, are formed from the order message BN and payment messages ZN, and are concatenated to each other. A new finger print is formed from the concatenation and is encrypted with the private key of the transmitter. Thus, the dual signature is formed from order message BN and payment message ZN.

When forming the finger prints, a different value is used for each finger print. Said values are agreed upon with the corresponding receivers of a message during the initiating phase of the communication, such that a receiver can only decrypt that part of the message which is exclusively meant for him. Even though said receiver has access to the finger print of the other message, he cannot decrypt the actual contents of this message without knowing the pertinent value which was used for forming the finger print. Thus, the facilities involved in a communication become certain that the transmitted messages relate to each other without actually having access to the information contained in a message. The

Secure Electronic Transaction (SET) allows, for example, that a merchant cannot obtain any information concerning the payment, for instance the credit card number, and that the bank vice versa does not receive any information on the order made. By means of this method, however, both facilities gain certainty that the procedures to be implemented relate to each other.

The problem resulting from cryptographic methods is due to the splitting of the keys to the communication partners. An underlying system has to guarantee that a public key is transmitted to a communication partner, which key is guaranteed to be associated with the other communication partner. This is obtained, for instance, by using so-called certificates. A central facility, the so-called certification site, has the information concerning the true identity of a person and its public key. Upon request said site transmits the public key to the communication partner. The transmission of the key is done in an encrypted form. The certification site encrypts the public key of a subscriber with the own private key. The receiver decrypts said message by using the public key of the certification site.

The invention is hereinafter explained in more detail by means of figure 5, which schematically shows the implementation of a transaction between a mobile subscriber, for example, between a mobile station MS and a merchant's bank integrated in the internet. The identity check of a user for the banks is in some countries carried out by a central institution, hereinafter called authentication instance. In Germany, for example, the task of the authentication instance is carried out by the Gesellschaft für Zahlungssysteme (GZS) (company for payment systems). In certain countries, however, the tasks of an authentication instance are carried out by a bank.

The upper part of figure 5 shows the physical connection with the corresponding communication units, and the lower part shows the logical connection with the involved protocols. The mobile station MS can, for instance, be a laptop computer having a card reading device. The laptop is connected with a mobile phone via a Terminal Adaptation Function (TAF), the task of which is fulfilled, for example, by the PCMCIA card (Personal Computer Memory Card International Association). The mobile station MS communicates with a so-called Split-SET server. This additional terminal is introduced for

realizing the invention. The localization of the Split-SET server either takes place in the GSM (Global System for Mobile Communication) or in an external network node, the so-called ESN (External Service Node). The introduction of the Split-SET server allows the splitting of the SET™ software between said unit and the mobile station MS. The administration of the software, particularly the keys, is obtained by means of the available storage devices. According to figure 5 the localization of the private keys of the user, designated by MS(PS) in figure 5, is effected in mobile station MS. The administration of the remaining keys, for instance, the public key, designated by MS(OS) in figure 5, or the certificates takes place in the storage device of the Split-SET server. The communication of the Split-SET server with a merchant is implemented through the internet. The merchant offers his products or services via a WWW server. The WWW pages supply information or precise descriptions, respectively, on the range of products to be offered. Each user calling said page receives the same information, also in view of cash-free money transactions. All possible alternatives of the object of the payment are thereby considered. An object of a payment can either represent a certain money value, for instance, anonymous or digital cash, or it can contain information concerning the customer's bank account, such as the power to collect money.

From the merchant the connection goes on via the internet to the merchant's bank. The bank of the merchant handles all money transactions for the merchant, such as the settlement between the merchant and the customer's bank. For the sake of control, not all facilities involved in a connection via the GSM and the internet have been shown in figure 5 in detail. Figure 5 includes the authentication instance checking the user on behalf of the merchant's bank.

The lower part of figure 5 logically shows the use of different protocols between the respective communication units. The introduction of the Split-SET server allows the splitting of the SET™ software between said unit and the mobile station, wherein the private keys are maintained in the mobile station. The public key and the certificates are shifted to the Split-SET server thereby obtaining that the signature process is controlled by the mobile station MS, whereas the realization of the remaining processes, such as the initialization of the payment, is subject to the control by the Split-SET server. The

communication between the Split-SET server and the merchant as well as between the merchant and his bank is entirely based on the already existing SET™ protocol.
For safety reasons it is important that not all existing keys are available to each unit integrated in a payment system. On one hand, this is guaranteed by splitting the user keys between its mobile station and the Split-SET Server, on the other hand, additional mechanisms are used during the handling of the procedures in connection with the SET™ protocol. In the case of payments according to SET™, for example, also encrypted credit card information are transmitted to the merchant when an order takes place, which, however, are not meant to be read by the merchant, but are to be transmitted by him to an authentication instance upon reviewing them. In order to guarantee the merchant despite the transparent payment instruction that said instruction relates to the effected order process, and in order to protect the customer against misuse at the same time, SET™ uses here the dual signature, whereby it is obtained that the order and the payment instruction can clearly be associated with each other without enabling the merchant to look into the payment instructions or the authentication instance to look into the order.

In the following, the invention is explained in more detail by means of patent claim 19.

According to patent claim 19 an electronic transaction between a mobile station and a network facility in an open network is realized by using a protocol for implementing secured electronic transactions. An electronic transaction involves a mobile station, a network facility and an additional device being localized between the two units. The implementation of the transaction between the mobile station and the network facility takes place by using a protocol for implementing secured electronic transactions, by splitting said protocol into a first and a second part. The first part of the protocol is allocated to the mobile station and serves the control of the implementation of the electronic transaction between the mobile station and the additional device. An electronic transaction is initiated by the mobile station, and the result of an implemented step contributing to the realization of a complete transaction, is re-supplied to the mobile station where it is evaluated. Thus, the mobile station takes over the control over the progress of the initiated transaction. The mobile station also takes over the administration

of private data of the user, by means of which a signature process is carried out. Thus, control over a transaction to be implemented is obtained.

The second part of the software is implemented in the additional device. By means of this step the additional device takes over control over the implementation of the transaction initiated in the mobile station between said unit and the network facility. The additional device has the public data of a user, i.e. the remaining data being required to implement a transaction, which are not contained in the mobile station, however. Upon receipt of an initializing message from the mobile station, the additional device takes over the completion of the electronic transaction by transmitting the necessary signaling messages to the corresponding units, thereby obtaining the control over the electronic transactions.

The exact progress including the required exchange of messages is hereinafter explained by means of an embodiment and figure 6. For this purpose the process of the payment transaction is used, as the acquisition of goods requires a number of transactions. The most important and simultaneously the most critical one, however, is the payment transaction.

Figure 6 schematically shows a communication between a mobile subscriber, a merchant, and an authentication instance. The progress in terms of time is characterized by the increasing sequence of the numbers of the required steps.

Step 1 schematically shows the example of the phase when the shopping is carried out. Upon the termination of this phase the mobile station transmits a message, in figure 6 being designated by Request Message, to the Split-SET server in order to imply the initialization of the transactions, step 2. To the Split-SET server the receipt of this message means that the initialization message can be transmitted to the merchant, step 3, which is responded to by the merchant with a signed message PInitRes, step 4. Said response contains the signature certificate of the merchant. In the next phase, the payment instruction is implemented. This requires the authentication of the user towards the payment system by means of a dual signature. As was already mentioned above, said signature is produced by using the private key of the user. For this reason, the Split-SET server transmits the message ReqSignProcess to the mobile station in step 5. The mobile

station signs the received message with its own private key and re-sends it to the Split-SET server in form of message RespSignProcess, step 6.

The Split-SET server infers from this message the signature of the mobile station, on the basis of which it forms the so-called PReq (Purchase Request) message which is transmitted to the payment system Said message contains the order information sent to the merchant and the payment information supplied by the merchant to the authentication instance in a transparent manner. The order information being used in said phase corresponds with the finger print of the already effected order. The complete description of the effected order, for example, the number of ordered products or the shapes thereof, is generated during the order phase, and upon completion of the ordering phase a finger print is produced from the complete description, which is used as order information during the payment phase.

The order and the payment information are transmitted to the relevant institutions in the system in an encrypted manner. The encryption of said messages is done by using the dual signature. For this purpose, two finger prints are produced from the order and the payment information, which are consequently concatenated to each other for again producing a finger print from said message, which is coded to form a dual signature by using the private keys of the mobile station.

The payment instruction is encrypted by using the symmetric coding. For this reason, the Split-SET server generates a symmetric key by means of a random sequence generator. The payment instruction is encrypted by means of said key. On a separate basis, for instance, during a registration, the credit card information and the generated symmetric key are encrypted by using the public key of the authentication instance, which was sent with the message PInitRes. In this way it is guaranteed that the credit card information are transmitted from the merchant to the authentication instance in a transparent manner without giving him the opportunity to have access to the information.
The encrypted order information, payment information, credit card information and in addition the dual signature are transmitted to the merchant in the PReq message, step 7. The merchant verifies the customer and the pertinent order from the received information.

For this purpose, the merchant uses the dual signature. At first, the own finger print is produced from the order information. Upon using the public key, the merchant infers from the received dual signature the finger print of the payment information. In a next step the merchant concatenates the two finger prints and compares them with the concatenation of said two finger prints decrypted from the dual signature. By means of this process the merchant gains the certainty that the received message really stems from the customer and that the already effected order and payment procedure to be implemented correspond with each other. The credit card information are transmitted by the merchant to the authentication instance in a transparent manner. In the next step, the merchant initiates an authorization of the payment towards the authentication instance. This operation firstly verifies the solvency of the credit owner, and in case of solvency the authorization for debiting is granted. In accordance with figure 6 this is done in step 8 by transmitting the authentication message AuthReq. Said message contains both the merchant's request concerning the acceptance of the customer's payment instruction as well as the encrypted payment instruction from the customer. The merchant's request is equally encrypted by using a symmetric process. Upon using an asymmetric coding process, the symmetric key is transmitted to the authentication instance. The request includes, among others, the finger print of the order. The merchant detects the finger print from the complete description of the order and transmits it together with the dual signature of the customer and the payment instruction to the authentication instance. The authentication instance decrypts the payment instruction by means of the private key. In order to implement the verification of the correspondence of the merchant and the customer concerning the effected order, a finger print is formed from the payment instruction, which is consequently concatenated to the finger print received from the order instruction, in order to form a dual signature from this concatenation and to compare it with the received dual signature. Thus, it is guaranteed that the description of the customer's order and the merchant correspond.

After the successfully implemented verification of the order, the authentication of the payment instruction from the customer is implemented in a next step. For this purpose, the credit card related information are inferred from the payment instruction of the customer, whereupon an inquiry is made with the customer's bank by means of the underlying banking network. The results of the authorization are packaged into a message AuthRes,

encrypted and transmitted to the merchant, step 9. Said data are encrypted with a symmetric key by the authentication instance, which is transmitted to the merchant after having been encrypted with an asymmetric key, i.e. with the public key of the merchant. The merchant uses his private key for decrypting the symmetric key in order to decrypt the received message AuthRes.

Upon their verification said data are transmitted to the Split-SET server in an encrypted manner in step 10. The Split-SET server also implements the necessary verifying operations, and in a step 11 said data are transmitted to the mobile station by means of the message Response.

According to patent claims 24 and 26 the invention is realized by using a device in a mobile station. Said device (not shown) includes means for storing the first part of the protocol, which is used for administering private data of a subscriber in the mobile station. An initiation of an electronic transaction is implemented in the mobile station with means for initiating an electronic transaction in a mobile station. The transmission of a message generated in a mobile station is done by using means for transmitting data. The initiated electronic transactions are controlled with means for controlling an electronic transaction between the mobile station and the additional device. The means for receiving data in the mobile station serve the receipt of messages containing the result of the implemented electronic transaction.

An electronic transaction is implemented by the mobile station to a device being positioned between a mobile station and a network facility. Said device comprises means for storing the additional part of the protocol and means for administering a subscriber's data which are accessible to the public. The transmission of data takes place to both the mobile station and the network facility and is obtained by using means for transmitting data. The results of an implemented transaction are supplied to the mobile station, and the messages in connection with the implementation of an order and payment process are supplied to the network facility. Said facility is responsible for controlling a process in which the network facility is involved. This is obtained with means for controlling the

electronic transaction between the device and the network facility. The receipt of a message from the network facility takes place by using means for receiving data.

Patent Claims

1. Communication system for implementing electronic transactions between a mobile station (MS) in a mobile communication network (MN) and a network facility (NV) in an open network (ON), comprising an additional device (WV) between the mobile station and the network facility, and a protocol (PT) for implementing secured electronic transactions being split into a first part (PT1) for controlling private data of a subscriber and into an additional part (PT2), wherein the first part (PT1) is implemented in the mobile station (MS) and the additional part (PT2) in the additional device (WV), and wherein an electronic transaction is implemented from the mobile station via the additional device to the network facility.

2. Communication system according to claim 1, wherein the mobile station (MS) is given the administration of a private key of a mobile subscriber.

3. Communication system according to claim 1 or 2, wherein the additional device (WV) takes over the administration of certificates and of public keys.

4. Communication system according to one of claims 1 to 3, wherein the implementation of a signature process of the mobile subscriber is effected in the mobile station.

5. Communication system according to one of claims 1 to 4, wherein the additional device (WV) controls the entire process of the electronic transactions.

6. Communication system according to one of claims 1, 3 or 5, wherein the additional device (WV) is installed either in a mobile network or in an external network node.

7. Communication system according to one of claims 1, 2 or 4, wherein the mobile station comprises a function of a personal computer and a function of a mobile phone providing for a communication with a mobile communication network.

8. Communication system according to one of claims 1 to 7, wherein electronic transactions are realized by exchanging signaling information.

9. Communication system according to one of claims 1 to 8, wherein an order and a payment instruction form part of the electronic transactions.

10. Communication system according to one of claims 8 to 9, wherein the signaling information is transmitted in an encrypted manner.

11. Communication system according to claim 10, wherein an asymmetric and symmetric encryption method is used for encrypting and decrypting the signaling information.

12. Communication system according to claim 11, wherein keys used in an encryption method are either identical or related to each other such that a message encrypted with one key is decrypted again with the other key.

13. Communication system according to claims 10 to 12, wherein the key is either a symmetric key or a private and a public key.

14. Communication system according to one of claims 4 to 13, wherein the signature process is effected with the implementation of an authentication based on an asymmetric encryption method.

15. Communication system according to one of claims 4 to 14, wherein a message is transmitted from the additional device to the mobile station during the signature process, the mobile station signing the received message with the own private key and transmitting it to the server for informing the server about the signature of the mobile station.

16. Communication system according to one of claims 1 to 15, wherein the electronic transactions are realized by using electronic transaction protocols.

17. Communication system according to claim 16, wherein the transaction protocols are Cyber-Cash, First Virtual or Secure Electronic Transaction™ (SET™).

18. Communication system according to claim 1, wherein the mobile network is a Global System for Mobile Communication (GSM), a General Packet Radio Service (GPRS), a Universal Mobile Telecommunication System (UMTS) network.

19. Method of implementing electronic transactions between a mobile station (MS) in a mobile communication network (MN) and a network facility (NV) in an open network (ON), and an additional device (WV) between the mobile station and the network facility, and a protocol (PT) for implementing secured electronic transactions, wherein said protocol is split into a first part (PT1) for controlling private data of a subscriber and into an additional part (PT2), wherein a transaction from the mobile station (MS) to an additional device (WV) is controlled by the first part (PT1) and wherein the transaction to the network facility (NV) in the open network (ON) is controlled by the second part (PT2), which is included in the additional device (WV).

20. Method according to claim 19, wherein the private data are a private key of a subscriber.

21. Method according to claim 19, wherein the second part of the software comprises public data of the subscriber.

22. Method according to claim 21, wherein the public data are a public key of the subscriber and at least one certificate.

23. Method according to one of claims 19 to 22, wherein a signature process is initiated by the mobile device by transmitting an initializing signaling message (Request_Message) and the termination of the initiating phase is supplied to the mobile device with a signaling message (RequestSignProcess) carrying the result, and wherein upon the successful implementation of the signature process a payment

process of the additional device is initiated by transmitting a message (ResponseSignProcess) and the result of the implemented payment process is supplied to the mobile device by means of a message (Response).

24. Device in a mobile station for implementing a method according to claim 19, comprising
- means for storing the first part for the administration of private data of a subscriber in the mobile station,
- means for transmitting data,
- means for initiating an electronic transaction in a mobile station,
- means for controlling an electronic transaction between the mobile station and the additional device, and
- means for receiving data.

25. Device according to claim 24, comprising means for implementing a signature process.

26. Device between a mobile station and a network facility for implementing a method according to claim 19, comprising
- means for storing an additional part,
- means for transmitting data,
- means for the administration of data of a subscriber accessible by the public,
- means for controlling the electronic transaction between the device and the network facility, and
- means for receiving data.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 00/02843

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	WO 98 37524 A (RITTER RUDOLF ;SWISSCOM AG (CH)) 27 August 1998 (1998-08-27) page 3, line 17 - line 29 page 4, line 18 - line 25 page 6, line 16 - line 29 page 9, line 25 - line 34 page 27 -page 39; figures 1,7-12	1-22, 24-26
A	WO 97 45814 A (VAZVAN BEHRUZ) 4 December 1997 (1997-12-04) page 2, line 10 - line 13 page 4, line 21 - line 26 page 6, line 9 - line 22 page 8, line 7 - line 15; claim 1; figures 1,2,6,7 abstract	1-26
A	WO 96 33476 A (CITIBANK NA) 24 October 1996 (1996-10-24) page 11, line 8 - line 12 page 12, line 9 - line 15; figures 1A,1B,2,3A,3B,5 abstract	1-22, 24-26
A	WO 98 42173 A (LAHTI SEPPO ENSIO ;TELAMA SAMI PEKKA (FI); FD FINANSSIDATA OY (FI)) 1 October 1998 (1998-10-01) page 4, line 31 -page 5, line 5; figure 1	1-22, 24-26

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inte 'onal Application No
PCT/EP 00/02843

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F7/08 G07F7/10 G07F19/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	WO 98 26386 A (MASCHOFF KURT M ;POWAR WILLIAM L (US)) 18 June 1998 (1998-06-18) page 4, line 8 - line 27 page 6, line 9 - line 29 page 10, line 23 -page 11, line 27 page 13, line 3 - line 14; figures 2-6 abstract	1-22, 24-26 23
Y A	WO 96 32700 A (AU SYSTEM ;JONSTROEMER ULF (SE)) 17 October 1996 (1996-10-17) page 1, line 24 -page 2, line 8 page 3, line 11 - line 21 page 7, line 18 - line 27 page 12, line 20 - line 34; figure 2	1-22, 24-26 23

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 June 2000	30/06/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Wauters, J

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter nal Application No
PCT/EP 00/02843

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9826386 A	18-06-1998	AU 5382098 A	03-07-1998
		EP 0961999 A	08-12-1999
WO 9632700 A	17-10-1996	SE 506506 C	22-12-1997
		EP 0958556 A	24-11-1999
		NO 974626 A	13-10-1997
		SE 9501347 A	12-10-1996
WO 9837524 A	27-08-1998	AU 6086898 A	09-09-1998
		AU 8007098 A	19-01-1999
		WO 9900773 A	07-01-1999
		EP 0992025 A	12-04-2000
		EP 0993664 A	19-04-2000
		NO 996147 A	28-02-2000
WO 9745814 A	04-12-1997	FI 962553 A	25-11-1997
		FI 971248 A	26-04-1997
		FI 970767 A	20-10-1997
		EP 0960402 A	01-12-1999
		FI 971009 A	26-04-1997
WO 9633476 A	24-10-1996	US 5799087 A	25-08-1998
		AU 720200 B	25-05-2000
		AU 5561596 A	07-11-1996
		BR 9608187 A	04-05-1999
		CA 2218612 A	24-10-1996
		CN 1185851 A	24-06-1998
		CZ 9703323 A	16-09-1998
		EP 0823105 A	11-02-1998
		HU 9800982 A	28-08-1998
		JP 11504144 T	06-04-1999
		NO 974835 A	19-12-1997
		NZ 306918 A	29-07-1999
		PL 323007 A	02-03-1998
		SI 9620055 A	31-10-1998
		SK 142697 A	04-11-1998
		US 6047067 A	04-04-2000
		US 5963648 A	05-10-1999
		US 5920629 A	06-07-1999
		US 5953423 A	14-09-1999
WO 9842173 A	01-10-1998	FI 971224 A	25-09-1998
		AU 6501998 A	20-10-1998
		EP 0972275 A	19-01-2000

[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]
G07F 7/08
G07F 7/10 G07F 19/00

[12]发明专利申请公开说明书

[21]申请号 00806481.4

[43]公开日 2002年5月1日

[11]公开号 CN 1347539A

[22]申请日 2000.3.31 [21]申请号 00806481.4
[30]优先权
[32]1999.4.19 [33]EP [31]99107726.4
[86]国际申请 PCT/EP00/02843 2000.3.31
[87]国际公布 WO00/63854 英 2000.10.26
[85]进入国家阶段日期 2001.10.19
[71]申请人 艾利森电话股份有限公司
地址 瑞典斯德哥尔摩
[72]发明人 K·弗罗纳 G·扎瓦利

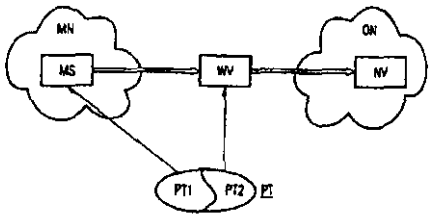
[74]专利代理机构 中国专利代理(香港)有限公司
代理人 吴立明 张志醒

权利要求书3页 说明书10页 附图页数4页

[54]发明名称 移动通信网络中有效实施电子交易的通讯系统和方法

[57]摘要

本发明涉及通过基于付款协议的信用卡来有效实施移动通讯网络 用户与网络设备之间的电子交易的通信系统,方法以及设备。用于实 现电子交易,如安全电子交易(SET™)的协议,被分解并嵌入到多个 通讯单元当中。为实现本发明,通常放置在用户移动站的第一部分协 议被分解成两部分。包含用户私人数据,如私人密码或凭证的第一部 分保存在移动站里。第二部分软件被移植到位于移动站和商家之间的 服务器上。从而,本发明一方面保证了在网路中用于以电子货币形式 付款的复杂软件的综合性,它具有较小的信息发送能力和较小的存储 能力的特点;另一方面保证了对用户安全性方面的维护。此外,本发 明还保证了与其他软件的兼容性。



ISSN1008-4274

01.10.19

权 利 要 求 书

1. 一种用于实现移动通讯网络（MN）中的移动站（MS）和开放式网络（ON）中的网络设备（NV）之间的电子交易的通讯系统，包括一个位于移动站和网络设备之间的辅助设备（WV）和一个用于实现安全电子交易的协议（PT），其中协议被分解成两部分（PT1 和 PT2），第一部分用于控制用户的私人数据，其中，第一部分（PT1）在移动站（MS）中执行，而第二部分（PT2）在辅助设备（WV）中执行，其中，电子交易从移动站经网络设备的辅助设备来实现的。

2. 根据权利要求 1 的通讯系统，其中移动用户的私人密钥由移动站（MS）监管。

3. 根据权利要求 1 或 2 的通讯系统，其中辅助设备（WV）接管公共密钥和身份凭证的监管。

4. 根据权利要求 1 至 3 之一的通讯系统，其中移动用户实施的签名处理在移动站中生效。

5. 根据权利要求 1 至 4 之一的通讯系统，其中辅助设备（WV）控制电子交易的整个过程。

6. 根据权利要求 1，3，或 5 之一的通讯系统，其中辅助设备（WV）安装在移动网络中或者安装在外部网络的节点上。

7. 根据权利要求 1，2 或 4 之一的通讯系统，其中移动站包括个人计算机功能和与移动通讯网络通讯的移动电话功能。

8. 根据权利要求 1 至 7 之一的通讯系统，其中电子交易通过相互交换信号信息来实现。

9. 根据权利要求 1 至 8 之一的通讯系统，其中货物订单和付款单构成电子交易的一部分。

10. 根据权利要求 8 至 9 之一的通讯系统，其中以加密形式发送信号信息。

11. 根据权利要求 10 的通讯系统，其中非对称加密方法和对称加密方法用于对信号信息的加密和解密。

12. 根据权利要求 11 的通讯系统，其中用于加密的密钥或者完全相同，或者互相有关联，这样就使得经一个密钥加密的信息可以由另一个密钥解密。

13. 根据权利要求 10 至 12 之一的通讯系统，其中的密钥或者是非对称密钥，或者是私人和公共密钥。

14. 根据权利要求 4 至 13 之一的通讯系统，其中签名处理是通过实施基于非对称加密方法的身份认证而生效的。

15. 根据权利要求 4 至 14 之一的通讯系统，其中在签名处理过程中一个信息由辅助设备发送给移动站，移动站用自身的私人密钥对接收到的信息进行签署并把它发送给服务器以便把移动站的信号通知给服务器。

16. 根据权利要求 1 至 15 之一的通讯系统，其中使用电子交易协议来实现电子交易。

17. 根据权利要求 16，通讯系统中的交易协议是虚拟货币，第一虚拟或者安全电子交易。

18. 根据权利要求 1 的通讯系统，其中移动网络是一个全球移动通讯系统（GSM），一个通用数据包无线服务（GPRS），一个通用移动远程通讯系统（UMTS）网络。

19. 一种用于来实现移动通讯网络（MN）中的移动站（MS）和开放式网络（ON）中的网络设备（NV）之间的电子交易的方法，包括一个位于移动站和网络设备之间的辅助设备（WV）和一个用于实现安全电子交易的协议（PT），其中协议被分解成两部分，即第一部分（PT1）和第二部分（PT2），第一部分用于控制用户的私人数据以及控制从移动站（MS）到辅助设备（WV）的交易，其中，开放网络（ON）中的网络设备（NV）的交易由第二部分（PT2）控制，而这部分的协议被存放在辅助设备（WV）上。

20. 权利要求 19 中的方法，其中，私人数据是用户的一个私人密钥。

21. 权利要求 19 中的方法，其中，软件的第二部分包括用户的公共数据。

22. 权利要求 21 中的方法，其中，公共数据是用户的一个公共密钥和至少一个身份凭证。

23. 根据权利要求 19 至 22 之一的方法，其中，签名处理是由移动设备通过发送一个初始化信号信息（Request_Message）来启动，初始化阶段的结束通过载有结果的信息（RequestSignProcess）提供给

移动设备，其中，一旦成功实现签名处理，辅助设备的付款过程便通过发送一个信息（ ResponseSignProcess）来启动，付款过程的执行结果通过反馈信息（Response）提供给移动设备。

24. 一种用于实现权利要求 19 中的方法的移动站设备，包括

- 移动站中用于存储对用户私人数据进行监管的第一部分的设备，
- 数据发送设备，
- 在移动站中启动电子交易的设备，
- 用于控制移动站和辅助设备之间的电子交易的设备，和
- 数据接收设备。

25. 根据权利要求 24 的设备，包括用于实施签名处理的设备。

26. 一种用于在移动站和网络装置之间实现权利要求 19 中的方法的设备，包括

- 存储附加部分的设备，
- 数据发送设备，
- 用于监管可供公共访问的用户数据的设备，
- 用于控制设备和网络装置之间的电子交易的设备，和
- 数据接收设备。

01.10.19

说　明　书

移动通信网络中有效实施
电子交易的通讯系统和方法

本发明涉及通过基于付款协议的信用卡来有效实施移动通讯网络用户与网络设备之间的电子交易的通信系统，方法以及设备。

可行的电子购物，举个例子，是因特网用户不同可行商业服务中的一部分。公司把他们的产品以电子清单的形式放在因特网上，用户可以通过点击鼠标来选择，订购和获取电子清单上的货物。网上货物的购买和销售，服务和信息归总在被称作电子商务的栏目里。这就要求网络系统能够保证电子货币交易的安全性。因此，由于这种交易的付款是用电子形式实现的，这使得安全性成为绝对必须的因素。

出于这个目的，开发了多种协议，这些协议可以用来实现电子交易，例如虚拟货币（Cyber-Cash），第一虚拟（First-Virtual）和安全电子交易（SET）。这种协议的特点是他们建立了符合安全性要求的信用卡付款系统。在下文中，安全电子交易（SET），安全电子交易（*SET™*）1.0说明版，5/31/97，作为例子用于解释本发明。

用于实现电子付款手段，尤其是用信用卡付款的协议是为具有足够传输容量和存储能力的固定网络制定的。上述要求会在网络结构中遇到，在这种网络结构中因特网用户拥有一台经由固定线路与因特网相连的个人电脑。然而，如果用户用移动通讯网络进行电子交易就不会遇到上述要求。移动通讯网络的特点是较低的传输速度和较小的存储容量。移动网络中所用的终端要么是移动电话要么是具有完整的既有移动电话功能又兼有计算机功能的设备，如所谓的 PDA（便携式数字助理）。由于用户的移动性，上述装置的体积尽可能地设计成最小。这仅仅通过减少存储容量即可实现，同时它会导致这些装置缺乏足够的用于安装，如，复杂安全电子交易（SET）协议的存储容量。刊登在 http://www.netlife.de/ 的网络生活服务器银行（ServerWallet of Netlife）栏中，提出了一个解决方案，借此完整的安全电子交易协议移植到出于此目的而特定安装的服务器上。根据上述公布，服务器被置于用户和商家之间。然而上述解决方案的缺点是用户在涉及安全方

面时没有自身的控制权。用户通过向服务器传送信息来启动交易。上述服务器包括全部的付款协议软件，包含所有的相关数据以及用户的个人数据，通过这种方法，启动后的交易就完全由服务器来实现。这显然意味着电子交易的控制和处理完全留给了服务器来实施。

本发明的一个目标是提供一种方法和设备，它允许在网络中有效实现安全付款的交易。减少用户端对存储空间的要求是本发明的一个特定的目标。

根据本发明，这个目标可由专利中的权利要求 1，权利要求 19，权利要求 24 和权利要求 26 的示例来实现。

因此，其优点在于通过把部分软件转移到服务器上，很少部分交易是经空气接口来实现的，从而提高了经由移动网络实现完整支付手段的效率。由于这个原因，充分有利地开发空气接口资源是一个优点。另外一个优点是可以最小限度地利用终端存储容量。它可以通过只在用户终端存储个人数据来实现。

本发明的另一个优点是它基于标准化的软件。由于该原因，确保了它与其他软件的兼容性，也为商家的交易提供了一个公开的实现手段，也就是说商家看不到是否有移动用户参与业务，或者用户是否直接连在固定网络上。

本发明的其他一些优点可由权利要求 2 到 19，20 到 23，以及权利要求 25 得出。

下面，将通过图表和实施方案来阐述本发明，其中

图 1 ， 图示了本发明的一个原理图，

图 2 ， 图示了一个非对称加密图，

图 3 ， 图示了一个鉴定方案，

图 4 ， 图示了一个双重签名方案，

图 5 ， 图示了一个具有逻辑协议表示法的网络结构，

图 6 ， 图示了一个付款过程的信息流。

下文中，由权利要求 1 和图 1 来描述本发明。

根据本发明，用于安全电子交易的 PT 协议，分解到移动通信网络 MN 的移动站 MS 和处于移动站 MS 以及开放网络 ON 的网络设备之间的辅加设备 WV 上。通过把协议（PT）分解成第一部分 PT1 和辅加部分 PT2 来实现对 PT 协议功能的分解。协议 PT 实现了移动站 MS 和网络设备 NV

之间经附加设备 WV 的电子交易.

当为实现电子交易而分解协议时，必须注意，移动设备接收用户的私人数据，并对可供普通访问的数据进行管理，例如认证系统的公共密钥有其他的设备接管。因而，由于交易的开始是由移动站用户启动的，整个交易的实现完全由用户来控制，移动站根据用户的个人数据实现对信号的处理，交易的控制也就留给了移动站。而剩余的与订购和付款相关的步骤由其他的附加设备来控制。在这个关系中附加设备遇到了复杂的安全性方面的问题，形成双重签名。

接下来，将用安全电子交易协议 *SET™* 来详细说明本发明。

安全电子交易（SET）协议是一个复杂的协议，它通过使用密钥区分技术来保证开放式网络，如，因特网中，用信用卡付款的安全性。付款过程中，在网络中相互交换信号信息。上述信息经加密后发送。加密的目的是为了保护信息内容免遭未经许可的访问或窃取，从而保证了交易的安全性。信息发送器用加密信息，即所谓的密钥，把数据加密成保密的信息，信息接收器用另一个密钥把数据解密。在这个关系中两个密钥不必完全相同，它（两个密钥是否必须完全相同）取决于不同的加密机制。例如，所谓的非对称密钥机制，用的是两种形式的密钥。这种机制为用户的访问提供了一个公共密钥，而不同的私人密钥提供给不同的通信用户。一个密钥用来加密，另一个用来解密。此外，该关系中有一点很重要，即两个密钥必须具有特定的联系，也就是说，经过一个密钥加密后，能，而且只能由另一个密钥来解密。总之，非对称加密机制向信息发送器提供一个密钥用于加密发送给接收器的信息。接收器通过私人密钥对加密后的信息进行解密。

这个过程将用图 2 进行详细解释。上述图中图示了三个系统，系统 B，系统 C，系统 D，这些系统等候向系统 A 发送一个加密文本。根据图 2，系统 A 的公共密钥用于加密文本。每个单元的公共密钥通常是公开的并可用于各个系统当中。加密文本被发送给系统 A。系统 A 有一个私人密钥，它通过该私人密钥解密接收到的加密文本。

除了非对称加密方式外还有对称加密方式。在对称加密方式中通讯两端的设备具有相同的密钥，其结果是信号发送器对信号的加密以及接收器对信号的解密用的是同一个密钥。

除了需要对信息进行加密外，同时还需对通讯设备进行身份验证。

身份验证确保了只有经授权的用户才有权访问数据，在这种关系下，必须对通讯设备的身份进行验证。因此便采用了一系列不同的身份验证方法。其中，一种叫超强身分认证(strong authentication)的验证方法最为人所知，它经过了充分的发展，安全性方面能满足特定要求。超强身分认证方法是根据非对称加密方法来实现的。同加密系统相比，身份认证系统中公共密钥用于对经私有密钥加密的信息进行解密。这个结论可以在图 3 中得出。根据图 3，信号发送器，系统 A，用在图 3 中称作系统 A 的私有密钥的密钥对文本进行加密，并把它发送给系统 B，C 和 D。系统 B，C 和 D 用系统 A 的公共密钥对接收到的信息进行解密。

由于用于解密的信号发送器的密钥是公开的，通过上述方法使得每个设备都有能力对信息进行解密。因而用户能够针对不同的系统对自身进行鉴别。由于信息只能由信号发送端的私有密钥进行解密，系统要求身份认证系统必须对身份进行成功的验证，它使得发送端紧紧拥有私有密钥方面的信息。

“超强身份认证”方法使用数字签名。数字签名用于判断发送的电子信息的真实性以及构成手写信号的等价电子信息。通过检验数字签名就可以确定相关信号是否已经改变。数字签名的特征是它只能由单个用户正确产生，但可以被所有的信号接收器验证的特征，非对称加密方式能够满足这种要求。然而，考虑到加密处理需要较长时间，系统并不是对所有的文件进行加密，而是从文件中计算出所谓的加密指印，也称杂乱信息，并把这些加密指印放在加密文件中。加密指印与数字签名相一致。通过从接收到的文件生成一个控制指印并且同另一个由公共密钥从发送器处解密得到的指印进行相同性比较，来判断接收到的信息是否确实来自信号发送器。

由于安全性方面的要求，安全电子交易（SET）使用了扩展形式的数字签名，即所谓的双重签名（dual or double signature）。双重签名允许分解后的信息用一个普通信号进行连接，这样在他们的连接过程中就不会泄密。双重签名方案图示在图 4 中．两个加密指印，BN 和 ZN，从订单信息 BN 和付款信息 ZN 中形成，两者相互关联。在两者的相互关联中又形成了另一个新的指印，并且用发送器的私有密钥对其进行加密。这样，就可以从订单信息 BN 和支付信息 ZN 中形成双重签

名。

指印的形成中，不同的指印使用不同的参数。上述不同的参数在通讯初始阶段，对应于不同的信息接收器。这样，信息接收器就只能对专属于它的那部分信息进行解密。即便这样，上述接收器还是有权访问其他信息的指印，但由于它不知道用于形成指印的相关参数，就不可能对这些信号的实际内容进行解密。因此，就确定了涉及通讯的设备，即，涉及每个发送的信息并没有真正访问包含在信息中的资料的权力。安全电子交易（SET）允许，如，商家不能获得任何涉及付款的信息如信用卡号，反之，银行也不能从用户订单中获得任何信息。然而，通过这种方法，两个部门设备都获得了确定，即交易的实现过程涉及到两者。

加密法所导致的问题源于把密钥分解给不同的通讯用户。必须用一个相关的系统来确保把公共密钥发送给通讯用户，而这个公共密钥能保证不同通讯用户之间的联系。它可以通过使用，如，所谓的凭证的方法来实现。所谓的认证站点是一个位于系统中心的设备，它存有个人身份以及公共密钥的相关信息。一旦请求上述站点把公共密钥发送给通讯用户，密钥的发送就以加密的形式来完成。认证站点把用户密钥用自身的私有密钥进行加密。接收器用认证站点的公共密钥对上述信息进行解密。

下文中将以图 5 的形式更加详细地解释本发明，图 5 图示了移动用户之间交易的实现方法的原理图，如，移动站 MS 与商业银行之间在网上的交易。在某些国家，银行系统的用户身份验证由一个中央机构来执行，下文中称作身分认证机构。例如，在德国，身分认证机构任务由 GZS 来执行（付款系统公司）。而在别的某些国家，身分认证机构任务由银行来执行。

图 5 的上面部分图示了对应通讯单元之间的物理连接，下面部分图示了有关协议的逻辑连接。移动站 MS 可以是，如，具有读卡设备的手提电脑。手提电脑通过自适应功能终端（TAF）与移动电话相连接。任务的执行由，如，国际协会个人计算机记忆卡（PCMCIA）。移动站 MS 与所谓的分离安全电子交易服务器（Split-SET server）相通讯。用该辅助终端来实现本发明。分离安全电子交易服务器要么是安置在 GSM 全球移动通讯系统中，或者位于外部网络节点上，即所谓的 ESN 外部

服务节点。分离安全电子交易服务器的引入允许上述单元和移动通讯站之间对安全电子交易（*SET™*）软件进行分解。系统对软件，尤其是密钥的管理，由一个有效的存储设备来实现。根据图 5，由图 5 的 MS（PS）指定的用户私人密钥的存放位置，并在移动通讯站 MS 中生效。其余密钥的管理，如，图 5 指定的公共密钥，或在分离安全电子交易服务器上进行的身份凭证。分离安全电子交易服务器与商家之间的通信是通过因特网来实现的，商家通过 WWW 服务器提供他们的产品。WWW 网页提供了各个不同的待售商品的详细信息。不同的用户可在网页上得到相同的商品信息，同时，进行的是非现金交易。因而考虑了付款方式的所有可能的可选方案。一个付款项既能代表一个特定的价目，如，匿名或数字现金，也可以包含有关用户银行帐号的信息，如聚敛钱财的能力。

商家经因特网同商家银行相联系。商家银行为商家处理所有交易上的钱款问题，如，解决商家银行和用户银行之间的汇兑。出于控制方面的原因，图 5 中没有图示出所有通过 GSM 和因特网连接的有关设备。图 5 包括了用于验证商家银行用户的身分认证机构。

图 5 的下面部分图示了各个不同通讯单元之间不同协议的逻辑关系。分离安全电子交易服务器的引进允许在上述单元和移动通讯站之间对安全电子交易（*SET™*）软件进行分解，其中私有密钥保存在移动通讯站中。公共密钥和身份凭证被移植到分离安全电子交易服务器上，从而使得信号的处理由移动通讯站 MS 来控制，而其他的处理，如，支付的初始化就交给了分离安全电子交易服务器来完成。分离安全电子交易服务器和商家之间以及商家同其银行之间的通信完全基于已存在的安全电子交易（*SET™*）协议的基础上的。出于安全方面的原因，有一点很重要，并不是每个结合在付款系统上的单元对所有密钥都有权访问。一方面，它通过把密钥分解给移动通讯站和分离服务器来得到保证，另一方面，在处理连接安全电子交易协议过程中采用了一个附加机制。根据安全电子交易（SET）协议，付款情况，如，尽管当用户订购时把加密后的信用卡信息发送给商家，然而，这并不意味着商家能够读取信用卡的信息，而是由他把信息发给认证机构以读取信息。为确保商家除了公开的付款单，上述的付款单涉及到已生效的订单处理，同时为保证顾客之间不会同时乱用，安全电子交易（*SET™*）使用

了双重签名系统，从而实现了订单与付款单之间能够很清楚地联系在一起而无需让商家查看付款单或者让认证机构查看订单。

下文中，将以专利权利要求 19 对本发明进行详细解释。

根据权利要求 19，移动站和网络设备在开放网络中进行的电子交易是通过实施一个安全电子交易的协议来实现的。电子交易涉及移动站，网络设备和置于两者之间的辅助设备。移动站和网络设备在开放网络中进行的电子交易是通过实施一个安全电子交易的协议，并把上述的协议分解为第一和第二两部分来实现的，其中，协议的第一部分放置在移动站上它控制着移动站和辅助设备之间的电子交易。电子交易由移动站来初始化，而促成实现完整交易的其他一些实施步骤也是由移动站来完成。这样，移动站监管了电子交易的初始化，同时它通过对信号的处理来实现对私人数据的管理。从而实现了对电子交易的控制。

软件的第二部分在辅助设备中执行。通过这个步骤，辅助设备担当起对实现在上述单元和网络设备之间经移动站初始化的电子交易的控制。辅助设备中存有用户的公共数据，以及实施电子交易所需的其他一些没有包含在移动通讯站里的数据。一旦从移动站接收到交易初始化信息，辅助设备通过向相关单元发送所需信息来并完成电子交易，从而实现了对交易的控制。

本发明的一个实施方案以及图 6，在下文中将解释包括所需交换信息的完整程序。由于商品的获取需要一系列的交易过程，出于这个原因，便使用了交易付款的处理程序。然而最为重要，同时也最为决定性的因素是交易的付款系统。

图 6 图示了移动用户，商家和认证处之间通讯的原理图。根据时间的进展的特征是所需步骤顺序号的增加。

步骤 1 图示了购物阶段原理图的一个例子。一旦这个阶段结束，移动通讯站向分离服务器发送一个信息，在图 6 中，该信息由需求信息（ Request Message）指定，来提供步骤 2 中的交易的初始化信息。对于分离安全电子交易服务器来说，接收到的这个信息意味着这些初始化信息能够发送给商家，见步骤 3，这可以由商家反馈一个初始化购物信息（PinitRes）得到确认，见步骤 4。上述反馈信息包含了一个商家的签名验证。在下一阶段中，系统将实现付款单（的填写）。这

要求用双重签名方法向付款系统用户进行身份认证。正如上文提到的，上述信号是由用户的私人密钥产生的。由于这个原因，分离安全电子交易服务器把信号（ReqSignProcess）传送给移动站，见步骤 5。移动站用它本身的私人密钥向收到的信息作了标记并以（RespSignProcess）信号形式返回给分离安全电子交易服务器，见步骤 6。

分离安全电子交易服务器从这些信息中推断出移动站信号，这种推断是基于形成发送给付款系统的所谓的购买需求 Preq（Purchase Request）信息，而上述信息包含了发送给商家的订购信息以及由商家向认证机构以公开方式提供的付款信息。上述阶段中使用的订购信息与已生效订单的指印相一致。生效订单的完整描述，如，订购商品的数量，商品的形状等，产生于订购阶段，订购阶段一旦完成，就从完整的订单信息中产生了一个指印，这个指印将在付款阶段中使用。

订单与付款信息以加密的形式发送给系统的相关机构。上述信息是用双重签名形式进行加密的。出于这种目的，从订单和付款信息中产生了两个指印。这两个指印的连接又产生上述信息的另一个指印。而通过使用移动站的私人密钥对该指印进行编码便形成一个双重签名。

付款单是以对称密钥方式加密的。由于这个原因，分离安全电子交易服务器用一个随机序列发生器产生一个对称密钥。付款单就是用上述的密钥加密的。在分解的基础上，如，注册过程中，信用卡信息和产生的对称密钥用认证机构处的公共密钥对其加密，并以初始化请求信息（PinitRes）形式发送。这样，就确保了信用卡信息以公开的方式从商家发送到认证机构，而不会让其获得任何访问信息的机会。加密后的订单信息，付款信息，信用卡信息，以及双重签名，全部包含在请求（PReq）信息中并发送给商家，见步骤 7。商家从接收到的信息对顾客及相关订单进行核实。出于这个目的，商家使用了双重签名。首先，从订购信息中产生自身的指印。一旦使用公共密钥后，商家从接收到的双重签名推导出付款信息的指印。接下来一步中，商家对两个指印进行连接并把他们同上述两个从双重签名解密得到的指印的连接进行比较。经上述步骤处理后，商家就可以确定，收到的信息确实来自顾客，以及已生效的订单手续和付款手续两者互相对应。商

家以公开的形式把顾客的信用卡信息发送给认证机构。下一步中，商家要求认证机构开始对付款进行认证。该操作首先核实信用卡（拥有者）用户的支付能力，同时，一旦确定其具有支付能力，认证系统就向用户授权。依照图 6，上述操作在步骤 8 中通过发送一个 AuthReq 信息来完成。上述信息中既包含了商家请求接收顾客付款单的信息还包含了来自顾客的经加密的付款单信息。商家的请求信息经对称密钥程序等效加密。一旦使用非对称密钥程序后，就把非对称密钥发送到认证机构。商家的请求信息包括订单信息的指印。商家从订单的完整信息中检测出指印，并把它同顾客的双重签名以及付款单一起发送给认证机构。认证机构通过私有密钥对付款单进行解密。为实现对商家和顾客相关的已生效订单的一致性的确认，从付款单信息中形成一个指印，该指印随后同另一个从订单中接收到的指印相连接，其目的是为了用该连接形成一个双重签名并同接收到的双重签名进行比较。这样，就可以确保顾客和商家两者的订单信息相一致。

成功实现对订单信息的验证后，系统将在下一步中对来自顾客的付款单信息进行验证。为此，从顾客的付款单信息中推导出信用卡相关的信息，因此需要通过相关银行网络对顾客所在银行作一个查询。认证的结果经打包放入 AuthRes 信息中，后经加密发送给商家，具体见步骤 9。上述经非对称密钥以及商家的公共密钥加密后发送给商家的数据在认证处机构用一个对称密钥加密。商家用他的私人密钥解密对称密钥一解密接收的消息 AuthRes。

上述数据一旦验证后经加密发送给分离安全电子交易服务器，详见步骤 10。分离安全电子交易服务器也执行一些必要的验证操作，见步骤 11，上述数据以反馈信息的形式发送给移动站。

根据本发明权利要求 24，26，本发明由一个移动站设备来实现。上述设备（没有图示出）包括用于存储协议的部分装置，这个装置用于管理移动站用户的私人密钥。电子交易的开始是在移动站用电子交易的初始化装置执行的。系统用数据发送设备发送移动站产生的信息。电子交易启动后便交给用于控制移动通讯站和辅助设备之间的电子交易的设备控制。移动通讯站的数据接收装置用于接收包含电子交易实施结果的信息。

电子交易是由安装在移动通讯站和网络设备之间的一个设备来实

现的。上述设备包含用于存储另一部分协议的装置和用于管理可供公共访问的用户数据。移动站和网络设备两者都进行信息的传送，它们通过发送数据来实现。电子交易的执行结果发送给移动站，而与订购及付款操作相关的实施信息则发送给了网络设备。上述装置负责控制涉及网络设备的操作。它通过控制设备与网络装置之间的电子交易来实现。通过使用数据接收装置接收来自网络设备的信息。

说 明 书 附 图

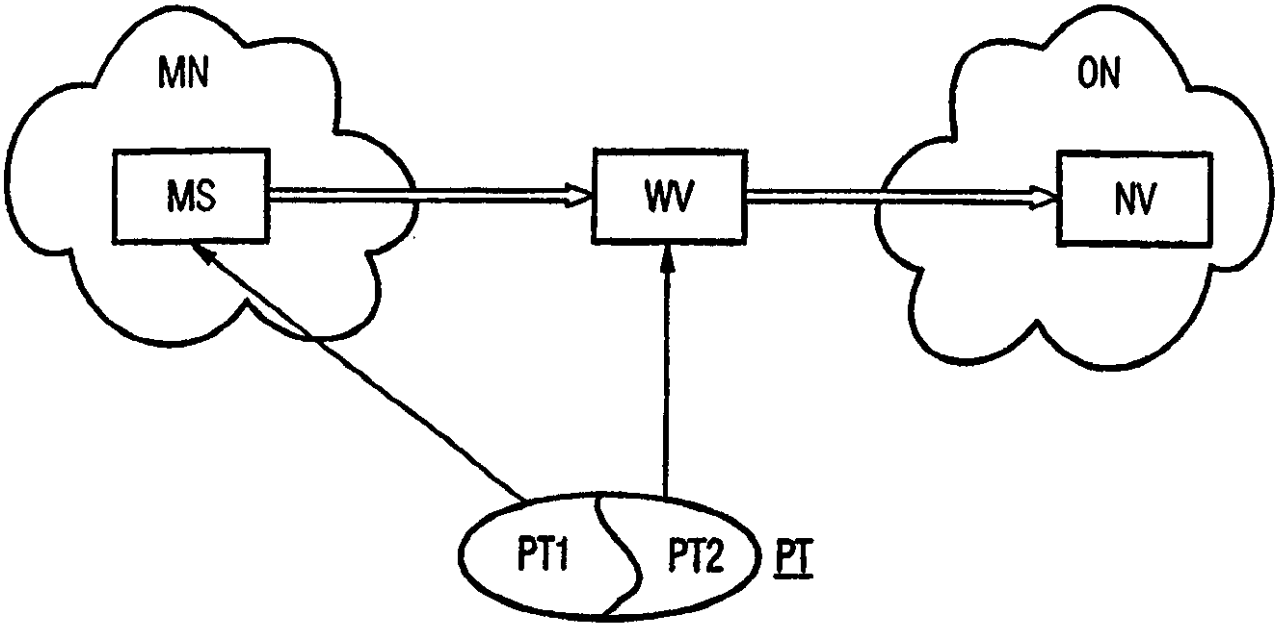

MN
MS
WV
ON
NV
PT1
PT2
PT

图 1

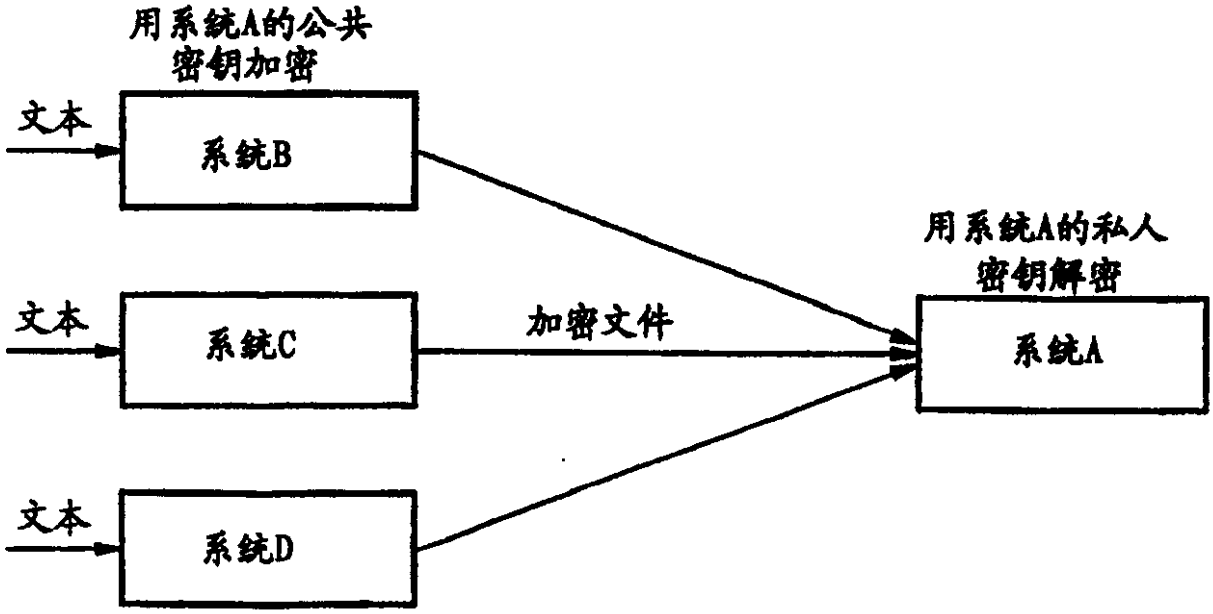

用系统A的公共
密钥加密
文本
系统B
文本
系统C
加密文件
文本
系统D
用系统A的私人
密钥解密
系统A

图 2

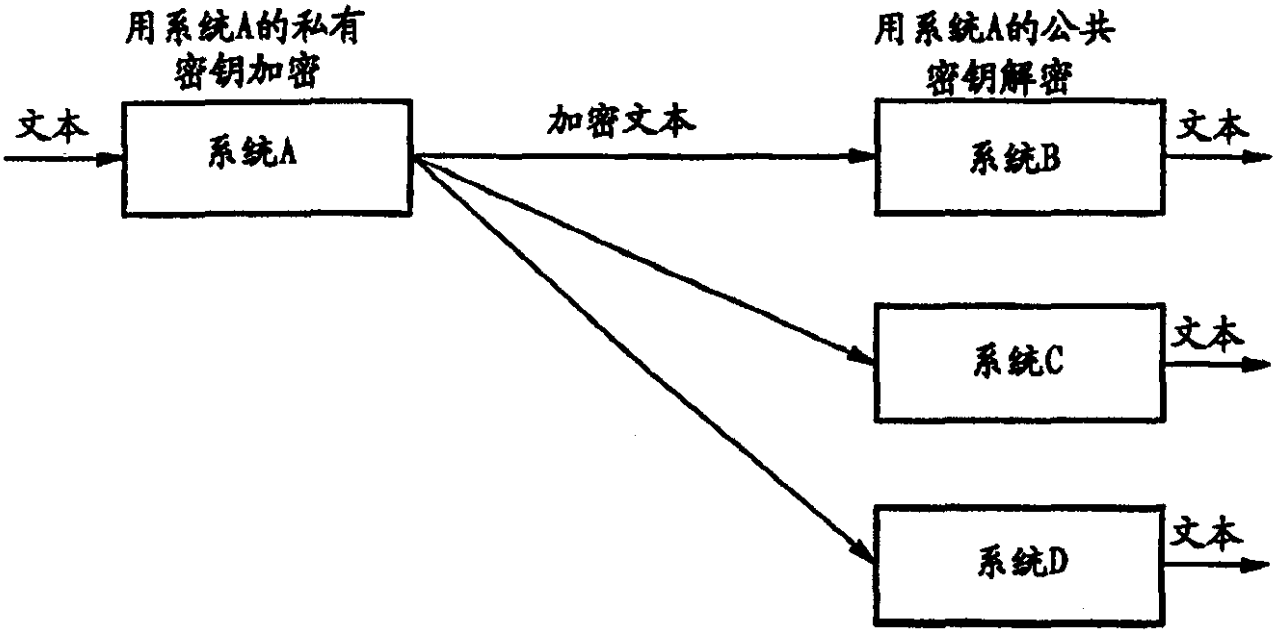

用系统A的私有
密钥加密
用系统A的公共
密钥解密
文本
系统A
加密文本
系统B
文本
系统C
文本
系统D
文本

图 3

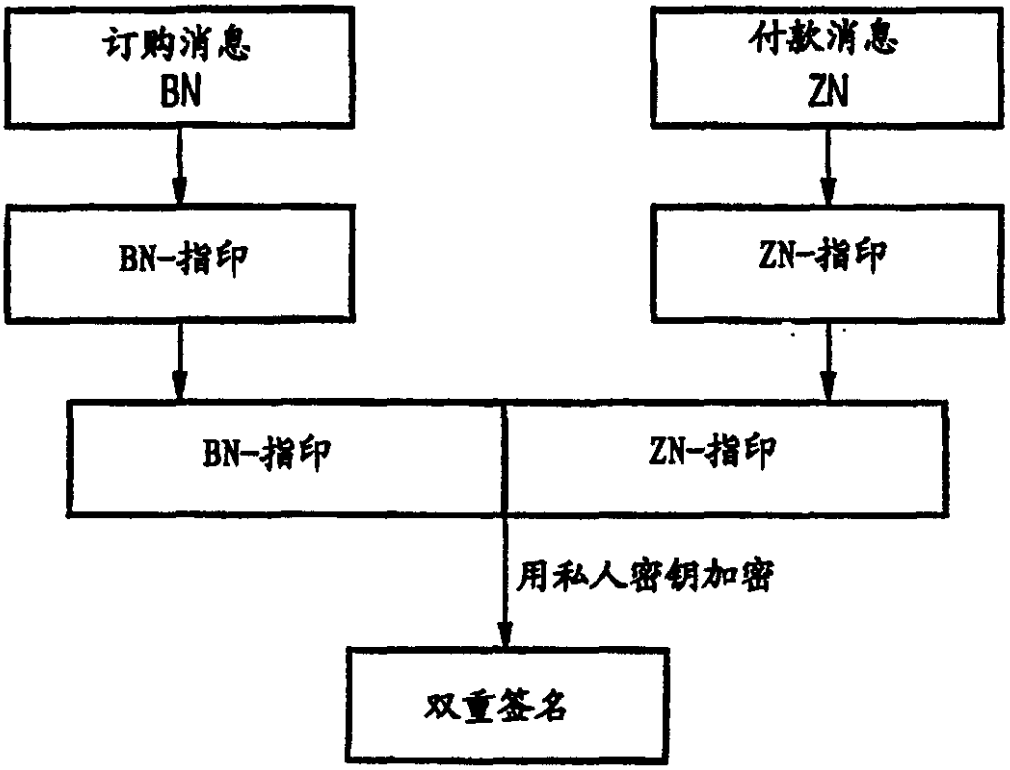

订购消息
BN
付款消息
ZN
BN-指印
ZN-指印
BN-指印
ZN-指印
用私人密钥加密
双重签名

图 4

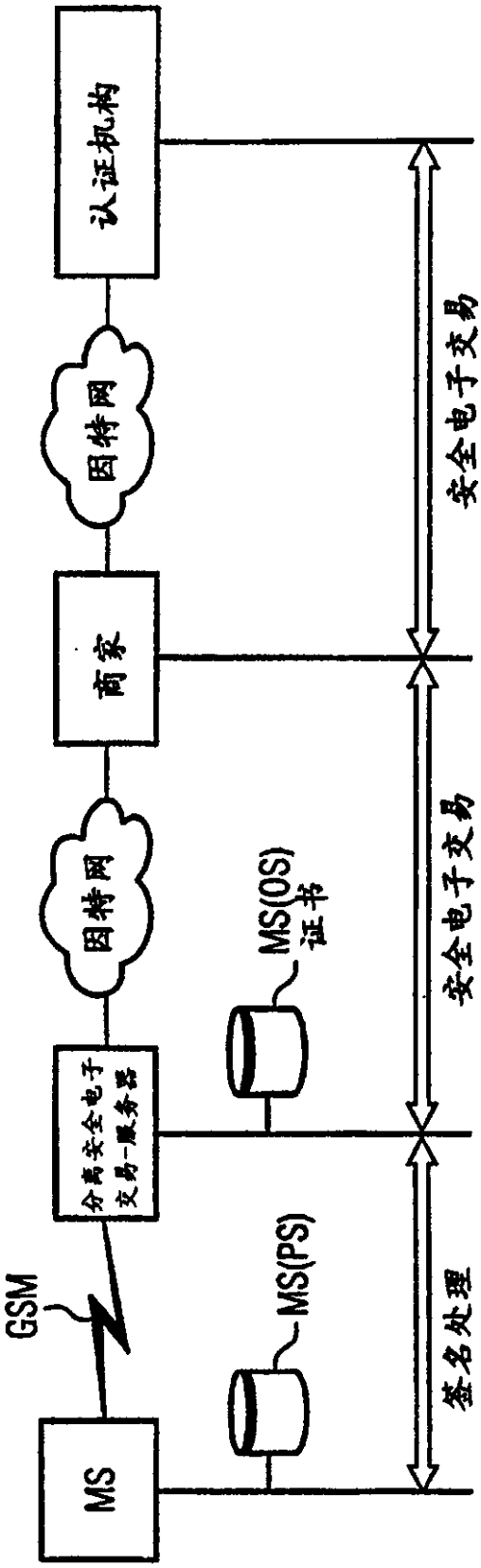

认证机构
因特网
商家
因特网
分离安全电子交易-服务器
MS(OS)证书
MS(PS)
GSM
MS
安全电子交易
安全电子交易
签名处理

图 5

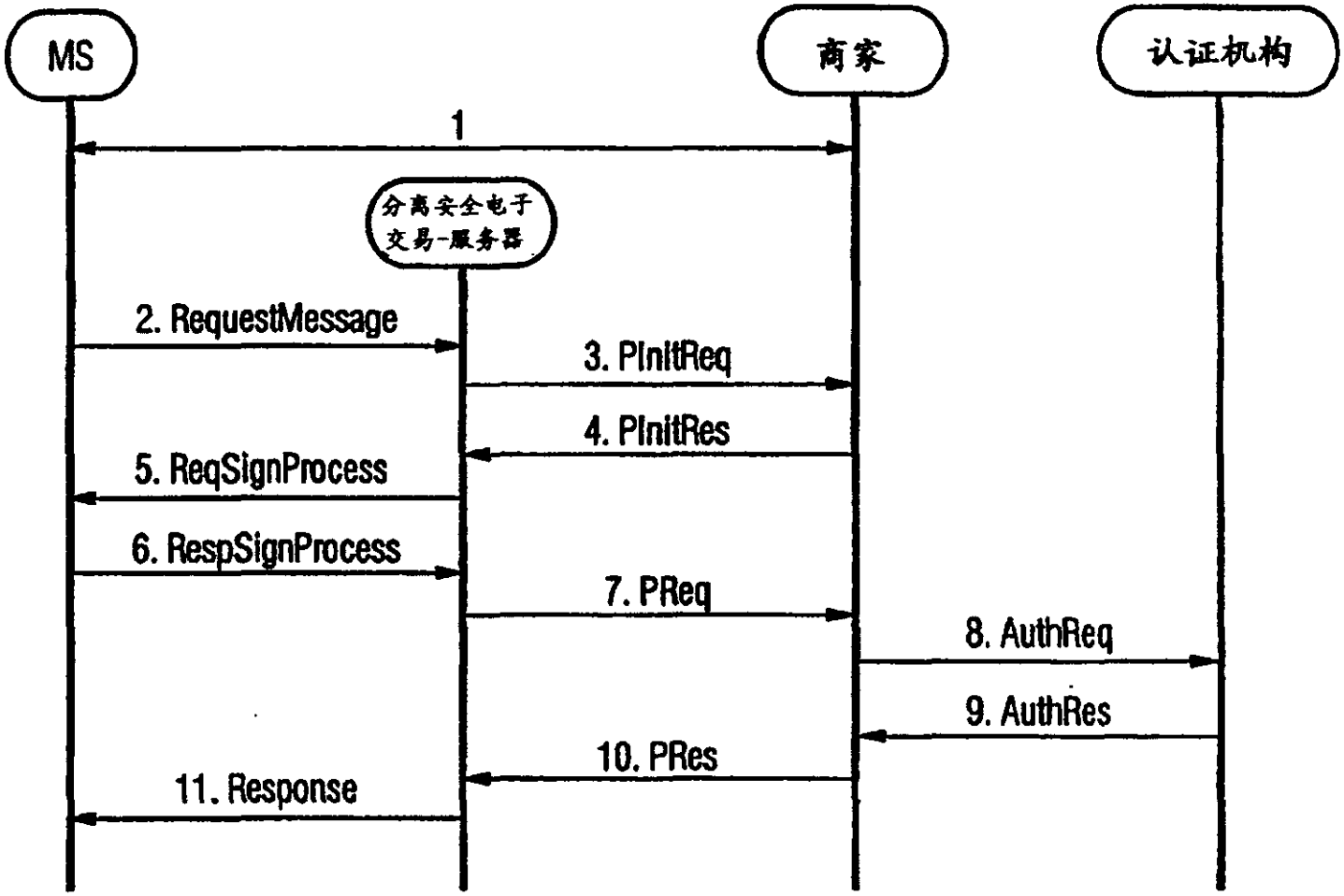

MS
商家
认证机构
1
分离安全电子交易-服务器
2. RequestMessage
3. PInitReq
4. PInitRes
5. ReqSignProcess
6. RespSignProcess
7. PReq
8. AuthReq
9. AuthRes
10. PRes
11. Response

图 6