



(72) CHEN, JAY C., US

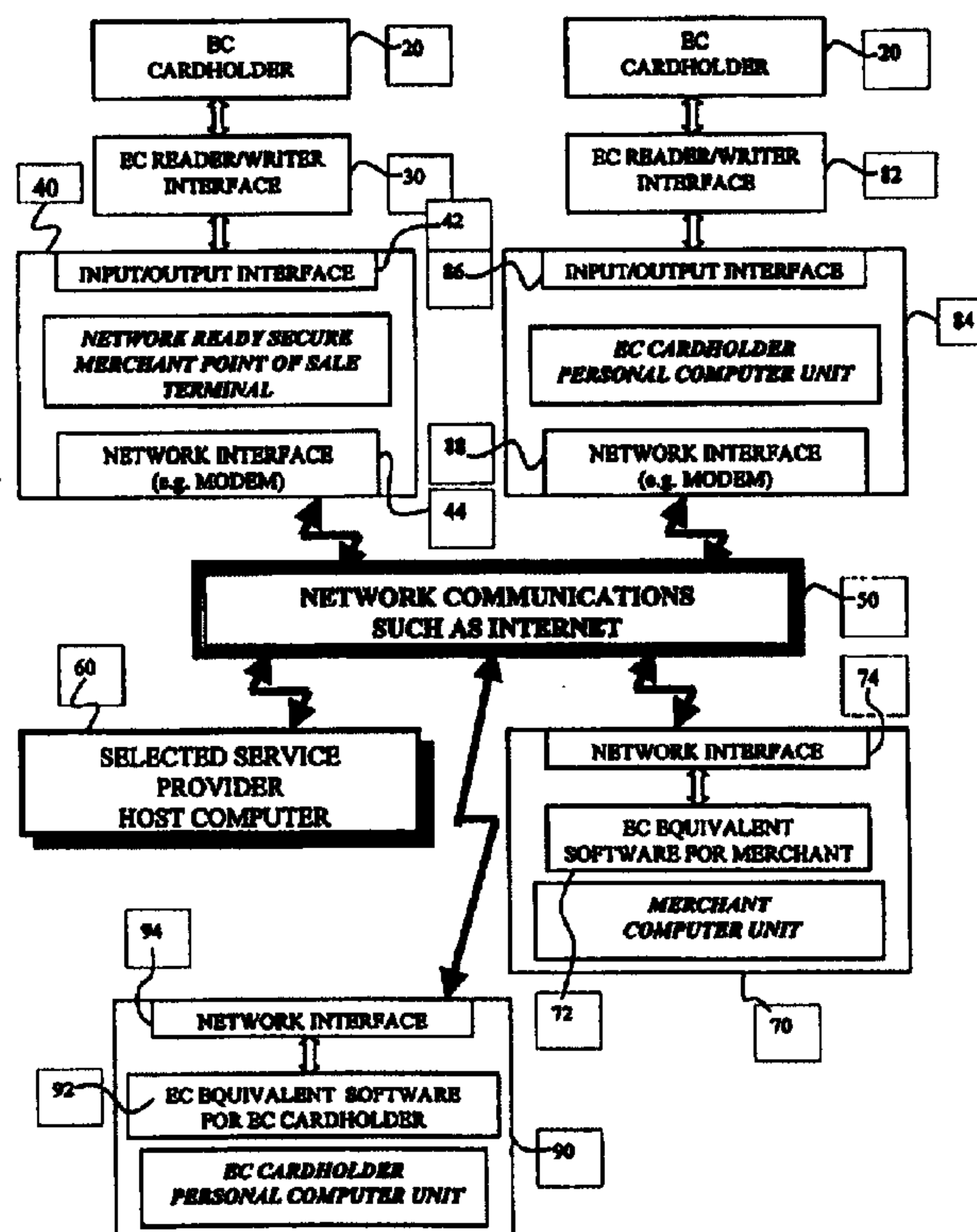
(71) CHEN, JAY C., US

(51) Int.Cl.⁶ H04K 1/00, H04L 9/00

(30) 1998/05/05 (60/084,257) US

(54) **SYSTEME ET PROCEDE CRYPTOGRAPHIQUES POUR
TRANSACTIONS ELECTRONIQUES**

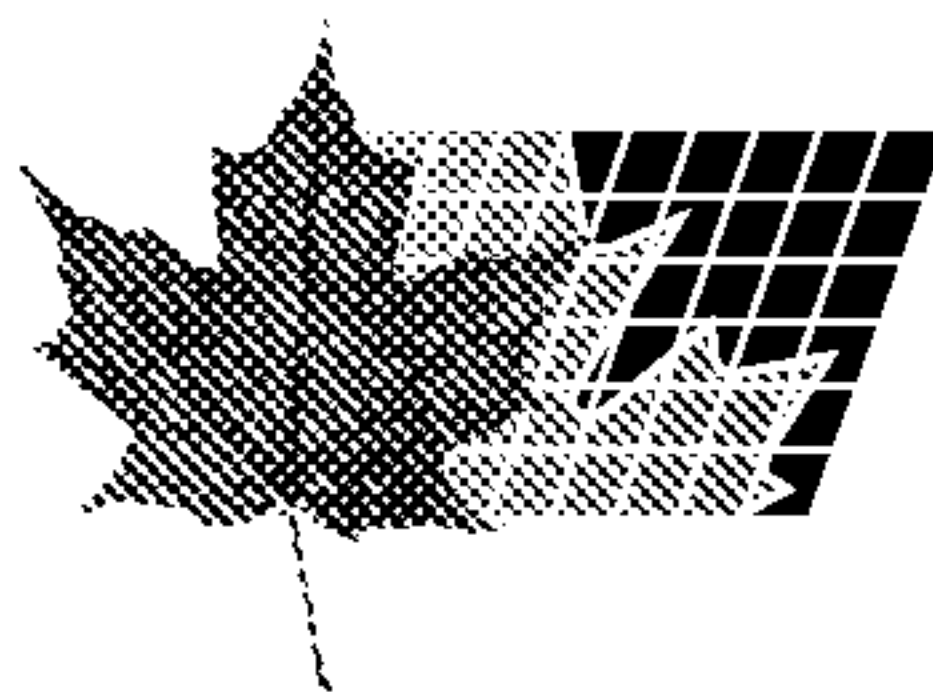
(54) **A CRYPTOGRAPHIC SYSTEM AND METHOD FOR
ELECTRONIC TRANSACTIONS**



(57) L'invention concerne un système de transactions électroniques qui facilite la mise en oeuvre de transactions électroniques sûres entre des parties multiples, notamment des détenteurs (20) de carte, des commerçants (70) et des fournisseurs (60) de services (SP). Le système comporte l'utilisation de cartes

(57) An electronic transaction system, which facilitates secure electronic transactions among multiple parties including cardholders (20), merchants (70), and service providers (SP) (60). The system involves electronic cards, commonly known as smart cards, and their equivalent computer software package. The card mimics





électroniques, appelées généralement cartes intelligentes, et de leur progiciel informatique équivalent. La carte a l'apparence d'un portefeuille réel et contient des instruments financiers ou non financiers ordinaires tels qu'une carte de crédit, un carnet de chèques ou un permis de conduire. Une transaction est protégée par un système cryptographique à clé hybride, et est normalement mise en oeuvre sur un réseau public tel que l'Internet. Des signatures numériques et des nombres aléatoires sont utilisés pour garantir l'intégrité et l'authenticité d'une transaction. La carte utilise des clés secrètes telles que des clés de session attribuées par des fournisseurs de services (SP) pour garantir la confidentialité de chaque transaction. Le SP est seul responsable de la validation d'informations sensibles concernant chaque participant, et de l'attribution des clés de session. La seule relation de confiance nécessaire dans une transaction est celle qui existe entre les participants individuels et le SP.

a real wallet and contains commonly seen financial or non-financial instruments such as a credit card, checkbook, or driver's license. A transaction is protected by a hybrid key cryptographic system and is normally carried out on a public network such as the Internet. Digital signatures and random numbers are used to ensure integrity and authenticity. The card utilizes secret keys such as session keys assigned by service providers (SPs) to ensure privacy for each transaction. The SP is solely responsible for validating each participant's sensitive information and assigning session keys. The only trust relationship needed in a transaction is the one that exists between individual participants and the SP.

**PCT**WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

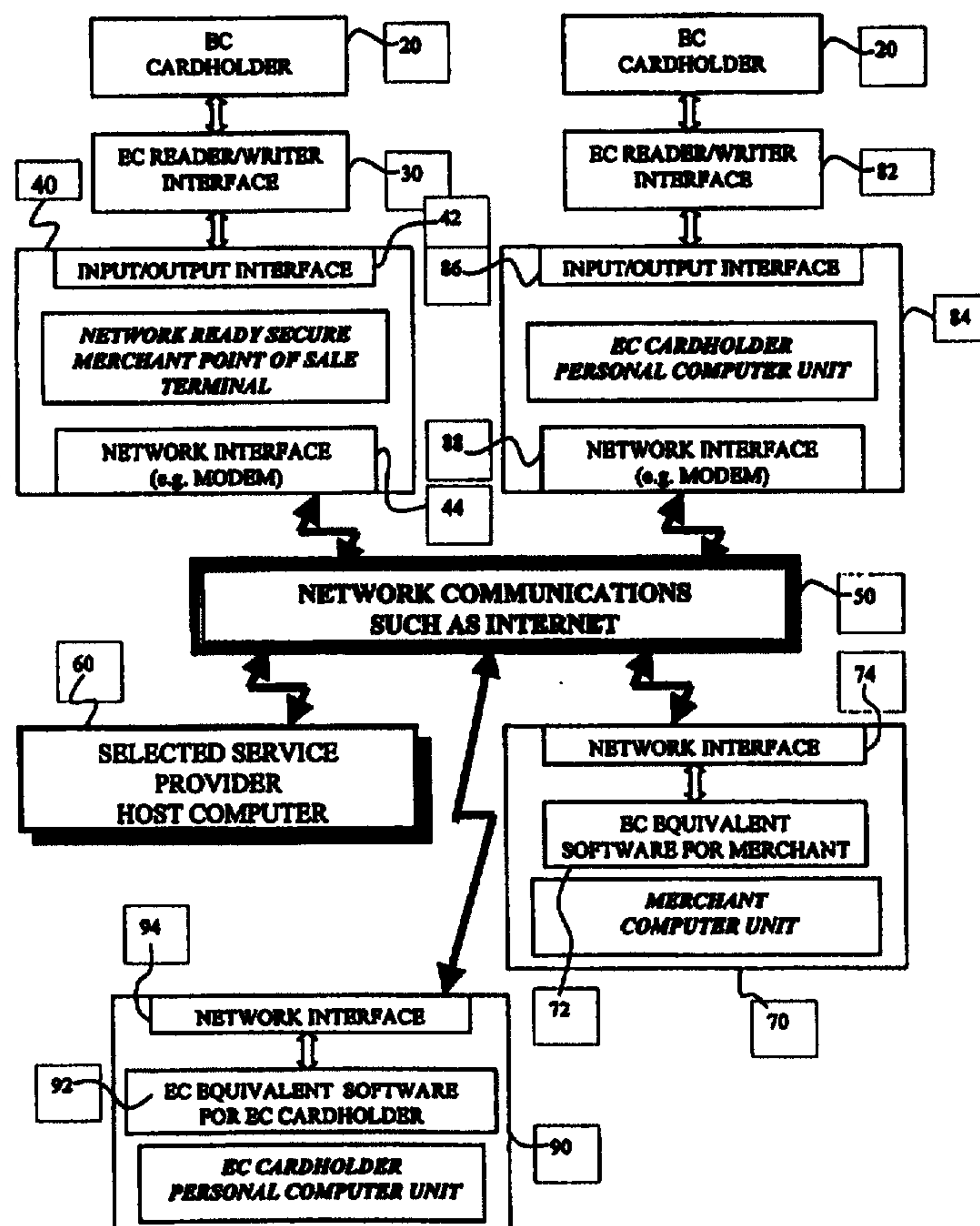
INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁶ : H04K 1/00, H04L 9/00		A1	(11) International Publication Number: WO 99/57835
			(43) International Publication Date: 11 November 1999 (11.11.99)
(21) International Application Number: PCT/US99/09938 (22) International Filing Date: 5 May 1999 (05.05.99) (30) Priority Data: 60/084,257 5 May 1998 (05.05.98) US (71)(72) Applicant and Inventor: CHEN, Jay, C. [-/US]; 1335 Blackstone Road, San Marino, CA 91108 (US). (74) Agent: GELFOUND, Craig, A.; Christie, Parker & Hale, LLP, P.O. Box 7068, Pasadena, CA 91109-7068 (US).		(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, 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, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, 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 <i>With international search report.</i> <i>Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.</i>	

(54) Title: A CRYPTOGRAPHIC SYSTEM AND METHOD FOR ELECTRONIC TRANSACTIONS

(57) Abstract

An electronic transaction system, which facilitates secure electronic transactions among multiple parties including cardholders (20), merchants (70), and service providers (SP) (60). The system involves electronic cards, commonly known as smart cards, and their equivalent computer software package. The card mimics a real wallet and contains commonly seen financial or non-financial instruments such as a credit card, checkbook, or driver's license. A transaction is protected by a hybrid key cryptographic system and is normally carried out on a public network such as the Internet. Digital signatures and random numbers are used to ensure integrity and authenticity. The card utilizes secret keys such as session keys assigned by service providers (SPs) to ensure privacy for each transaction. The SP is solely responsible for validating each participant's sensitive information and assigning session keys. The only trust relationship needed in a transaction is the one that exists between individual participants and the SP.



(SUBSTITUTE)

- 1 -

MICROWAVE POPCORN FORTIFIED WITH CALCIUM
AND METHOD OF PREPARATION

FIELD OF THE INVENTION

5 The present invention relates to packaged food products. More particularly, the present invention relates to microwave popcorn product articles characterized by calcium fortification and to methods for filling such articles.

BACKGROUND

10 Popcorn is a highly popular snack food item. In the past, the at-home preparation of popcorn by the consumer involved adding kernel popcorn plus a cooking oil to a covered pot and heating until the popcorn kernels popped to make popcorn. As used herein, "kernel
15 popcorn" refers to unpopped popcorn. The noun "popcorn" or synonymously "popped popcorn" refers herein to popped kernel popcorn. The adjective "popcorn" can refer to either. Once prepared, common, relatively coarse, table salt is a frequently added flavoring or condiment. The
20 resultant salted popped popcorn is a familiar snack food. The flavorings or condiments can also be added prior to cooking of the popcorn. For example, WO 95/01105 discusses adding salt, color and/or flavors to a popcorn/fat charge placed in a bag. Other flavorings
25 can also be added, such as cheese as disclosed in U.S. Patent No. 4,904,487.

AMENDED SHEET

(SUBSTITUTE)

-2-

More recently, microwave popcorn products have become extremely popular. At present, in the U.S., over 70 different brands of microwave popcorn products are available. In general, the more popular microwave popcorn products comprise an expandable paper bag containing a charge of kernel popcorn, fat and salt. The microwave popcorn article is adapted to be heated in a microwave oven for three to five minutes to produce the popped popcorn. More recently, improved microwave popcorn articles have been fabricated employing a metallized susceptor which facilitates the heating of the kernel popcorn-fat charge and which, in turn, leads desirably to increases in popcorn volume and decreases in unpopped kernels. Microwave popcorn articles of this type are described in detail in, for example, U.S. Pat. No. 4,450,180 (issued May 22, 1984 to J. D. Watkins).

Microwave popcorn articles, of course, comprise a microwave popping bag and a charge of kernel popcorn, fat, and, usually, salt. Certain early patents taught the addition of kernel popcorn, fat and salt in the form of a prefabricated toroid or doughnut shaped piece. The piece was fabricated by mixing the kernel popcorn, salt and melted fat to form a blend and the blend was allowed to cool and harden into the toroid shape desired. These circular pieces were then dropped into the desired chamber of the popcorn bag prior to final sealing. (See for example U.S. 4,450,180, issued May 22, 1984).

Contemporary methods of filling microwave popcorn bags, however, employ a different filling process and

AMENDED SHEET

(SUBSTITUTE)

-3-

technique. (See, for example, U.S. 4,604,854 entitled "Machine For Forming, Filling and Sealing Bags," issued August 12, 1986 to D. W. Andreas). The microwave bags having an unsealed open end are advanced to a first
5 kernel popcorn filling station. While being maintained in an open position, the kernel popcorn is charged to the desired channel. Thereafter, the bags are advanced to a second filling station at which the fat/salt slurry is added to the bag. Typically, the slurry is added in
10 the form of a vertically dispensed pencil jet (i.e., a confined stream) of the slurry. Single station filling methods are also known that involve applying the fat/salt slurry as a spray onto the kernel popcorn as the kernel popcorn falls into the bag. (See, for
15 example WO 95/01105 entitled "Reduced Fat Microwave Popcorn and Method of Preparation" published January 12, 1995, or, equivalently, U.S. 5,690,979 issued November 25, 1997). Such single station filling techniques are especially useful for the preparation of low fat
20 microwave popcorn products.

The bags now containing both kernel popcorn and slurry are then advanced to a sealing station where the bags are provided with a top seal to complete the closure of the bag. The sealed popcorn bags are
25 advanced to subsequent finish packaging operations which complete the folding of the bags, providing the bags with an overwrap, and inserting appropriate numbers of the bags into cartons, etc.

(SUBSTITUTE)

- 4 -

Thus, while microwave popcorn products are popular, it would be desirable if such microwave popcorn products were fortified with supplemental calcium to provide a significantly nutritionally enhanced product. EP

5 781,513 and corresponding U.S. Patent 5,747,080 disclose producing popcorn with added vitamins, minerals and/or trace elements, with calcium being a potential additive. However, the added calcium is fairly low such that the popcorn is not significantly nutritionally enhanced. By
10 significantly nutritionally enhanced is meant a product having at least 10% of the current recommended daily intake ("RDI") or at least 360 mg of calcium (including both the native and supplemental contributions) per 100 grams of unpopped microwave popcorn.

15 One conceivable approach is to merely add the calcium along with the salt to the slurry to facilitate calcium fortification of the food charge. However, a first problem can reside in the slurry viscosity. The slurry viscosity rises rapidly as more particulates are
20 added. If an additional particulate is desired to be added to the slurry such as for flavor or mineral fortification, then addition of requisite amounts of salt to the slurry results in a slurry having a paste consistency and a viscosity too high to pump. This is
25 especially true in the more concentrated slurry typically used for ultra low fat popcorn--usually about 94% fat free.

A second problem is plugging of the orifice of the pencil jet nozzle used to charge the slurry to the bag
30 that can occur when the slurry viscosity is too high. While plugging is a problem when salt alone is added to the slurry, such plugging problems are compounded when

AMENDED SHEET

15-05-2000

:15- 5- 0 :

PCT/US99/02938

763 764 2268→

+49 89 2399 DESC

PCT/US99/02938

(SUBSTITUTE)

-4A-

the slurry contains supplemental particulates such as a calcium mineral.

AMENDED SHEET

1

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a block diagram showing the relationship among the components of a system according to an embodiment of the invention.

5

Figure 2 shows the flow of the two transaction phases via a network.

Figure 3 is the diagrammatic representation of an EC.

Figure 4 shows the format of the service provider data area. Each service provider's information is allocated an entry in the table and is protected by access conditions.

Figure 5 shows how the digital signatures are used in an embodiment of the invention.

10

Figures 6A through 6Q shows the schematic flow chart of the cryptographic system and method used in an embodiment of the invention in order to conduct electronic transactions via an open telecommunication network, such as the Internet.

Figure 7 through Figure 11 depicts the final format and content of the combined request and response messages in the key exchange phase and the transaction phase.

15

Figure 12 shows a service provider conducting a transaction with participants that have been arranged in series.

Figure 13 shows a service provider transaction on a network with participants that have been arranged in a hierarchical organization scheme.

20

DETAILED DESCRIPTION

The preferred embodiment of the invention is a cryptographic system and method for electronic transactions by using an electronic card (EC) in the form of a smart card or equivalent software and communicating over a communications network.

25

In the preferred embodiment of the invention, the network is an open network such as the Internet. In alternative embodiments of the invention, other open networks and/or closed networks may be used to establish communication between a service provider and its members. For example, a service provider may use its own proprietary financial network to communicate with its members.

30

Any Internet protocol may be used for Internet connections. Example protocols, which can be used include TCP/IP, UDP, HTTP, and the like.

35

Communication may also be via a communications network transport service such as the Public Switched Telephone Network (PSTN) using traditional analog telephone service (a.k.a. Plain Old Telephone Service or POTS), or by using a digital communication service such as a T-1, E1 or DS-3 data circuit, Integrated Services Digital Network (ISDN), Digital SubscriberLine (DSL) services, or even using a wireless service, and the like. When implemented using such a service the invention may be implemented independent of a communications protocol (i.e. at an electrical interface layer).

1 Communication may also be via a local area network (LAN) or WideArea Network (WAN) such as Ethernet, Token Ring, FDDI, ATM or the like. Example protocols, which can be used include TCP/IP, IPX, OSI, and the like.

5 Other communication links might include an optical connection, a wireless RF modem connection, a cellular modem connection, a satellite connection, etc.

10 The invention may be employed as long as a communication path can be established between a service provider and its members. The examples above are intended to illustrate several examples of the various communications environments in which the invention may be practiced. As is clear to one ordinarily skilled in the art, the invention is not limited to those environments detailed above.

15 The EC can take the form of a smart card device or a software package running on a computer system such as a personal computer (PC). When the EC is implemented on a smart card, it can be used on a network-ready computer system such as a PC to transact with another member and/or a selected service provider. It will need a read/write interface device to communicate with a computer system and some application software such as an Internet browser to interface with the cardholder and the network. If the EC is a software package loaded into a computer system, then no read/write interface is needed. The exemplary embodiment of the invention is for the EC to act as an electronic wallet (or cyber wallet) which functions similar to real wallet. A real wallet can carry credit cards, debit cards, ATM cards, health provider cards, membership cards, cash, etc. An EC has the digital equivalent of all the above-mentioned financial and non-financial instruments and enables conducting secure transactions over the Internet.

20 A service provider member can be a merchant and/or an EC cardholder. A merchant is a member who is paid by the service provider as a result of a transaction. A member can be both a merchant and an EC cardholder. A merchant may engage in a transaction with other cardholders, which results in the merchant being paid by the service provider. A merchant may also be an EC cardholder and purchase supplies, for example, from a merchant supplier.

25 The cryptographic system may involve communication between a service provider and any number of service provider members. Thus, communication can be between an EC and an SP, between a merchant and an SP, between a first EC, a second EC, and an SP, between a first merchant, a second merchant, and an SP, etc. An EC may communicate directly with a service provider to inquire about an account balance for example. A merchant may communicate with a service provider only on his own behalf and not on behalf of an EC because, for example, the merchant wants to know his own account balance with the service provider. Communication between the SP and its members may follow any permutation of the SP and its members. The organization of the communication links between the SP and its members may be sequential and/or hierarchical. Communication between the SP and its members may also be via routers, which route the messages between the SP and its members.

1 The cryptographic method is a two-phased key-exchange-transaction model. The first
phase is a key exchange phase. The second phase is the transaction phase. In the key exchange
phase, the members exchange keys with the service provider. The members send their keys to
the service provider and the service provider uses the keys to send a session key to the members.
5 The session key protects any further message exchange between the cardholder and the SP or
between the cardholders' themselves. In the transaction phase, either the SP can direct the
transaction or the cardholders themselves may conduct the transaction.

Figure 1 is a block diagram showing the relationship among the components of a system
according to an exemplary embodiment of the invention involving a cardholder, a merchant, and
10 service provider.

An EC cardholder 20 can conduct a transaction over a network 50 and communicate with
a merchant either by using an EC read/write device 82 attached to an originating computer 84
or by using EC equivalent software 92 running on an originating computer unit 90.

A merchant can conduct a transaction over a network by either using a network-ready
15 point-of-sale(s) (POS) terminal 40 or by using EC equivalent software running on a merchant
device 70 to conduct an electronic transaction with a selected service provider 60 via a network
50 such as the Internet.

Once the access conditions to the card have been satisfied, the cardholder can perform
financial or non-financial transactions with other participants of the system through the network
20 50. In Figure 1, there are three different scenarios in which a transaction over a network can be
conducted.

(1) In a POS transaction (Upper left side of figure 1), the cardholder 20 swipes/inserts an
EC through/into a merchant's EC reader/writer 30 at a merchant's premises. The EC
reader/writer is connected to a network-ready merchant POS terminal 40. The network-
25 ready merchant POS terminal 40 is a secure tamper-resistant programmable device
comprising an input means such as a keyboard, a display device, a processing unit, and
an EC read/write device 30 (an EC interface device). It is typically a small computer
unit such as a PC equipped with a communication link to an open network. The POS
terminal communicates to the SP via the network 50.

30 (2) (Right side of figure 1) A cardholder can conduct a transaction with other participants
of the system by inserting the EC 20 into a read/write device 82, which is connected to
the cardholder's personal computer 84 which is the originating computer. The
originating computer connects to a network 50 allowing the EC to communicate with
the merchant computer unit 70. The merchant computer unit 70 has EC equivalent
35 software 72 that enables the merchant to receive the EC generated message and
generates a message combining EC information and merchant information. Then, the
combined message is sent to the SP over a network.

(3) (Bottom side of figure 1) A cardholder can conduct a transaction with other participants

1 of the system by using EC equivalent software 92 on the customer cardholder's personal
computer 90. The transaction begins at the originating computer unit 90, that is, the
cardholder's personal computer. The cardholder conducts the transaction over a
network 50 and communicates with the merchant's computer unit 70, which in turn
5 communicates with the SP 60 over a network 50.

While in the preferred embodiment of the invention, a personal computer is used to hold the
EC equivalent software, in alternative embodiments of the invention other electronic devices can
be used to hold the EC equivalent software.

10 In the preferred embodiment of the invention, the network used to enable the EC to
communicate with the merchant is the same network used to enable the merchant to
communicate with the SP. In another embodiment, the network used to enable the EC to
communicate with the merchant may not be the same network used to enable the merchant to
communicate with the SP. In yet another embodiment, the network used to enable one merchant
to communicate with the SP may not be the same as the network used to enable another merchant
15 to communicate with the SP. In still yet another embodiment, the network used to enable an EC
to communicate to the merchant may not be the same as the network used to enable another EC
to communicate with another merchant. An embodiment may consist of a multiplicity of
networks whereby different parties communicate.

20 In the preferred embodiment of the invention, a transaction is broken down into two phases:
a key exchange phase and a transaction phase. Figure 2 is a specific case, which illustrates the
two-phase key-exchange-transaction model where the SP directs the transaction phase. There is
no direct exchange of sensitive information between participants when the SP directs the
transaction.

25 The key exchange phase is the same where the transaction phase is among the cardholders
themselves and where the SP directs the transaction phase. Where the transaction phase is
among the cardholders themselves, the cardholders use the SP session key to communicate with
each other and conduct a transaction.

30 Figure 2 demonstrates a financial transaction where the SP directs the transaction phase.
The transaction shown involves three parties: an EC (a transaction originator) 102, a merchant
104, and a service provider (SP) 106. The originating party is an EC cardholder who is the
consumer and is represented by the computer unit 102. The computer unit 104 represents the
merchant. The computer unit 106 represents the service provider. An SP is selected by both an
EC and merchant.

35 Figure 2 demonstrates a financial transaction wherein the process flow is from an EC to a
merchant to an SP. The cryptographic method's process flow is not limited to any particular
order between merchants and EC cardholders. Figure 2 is merely an example of a particular
transaction, which flows from EC to merchant to service provider. The process flow can also
go from merchant to EC to service provider. Figure 2 demonstrates how service provider

(SUBSTITUTE)

- 9 -

include any conventionally useful bag for microwave popcorn products.

For example, a suitable bag widely used commercially and preferred for use herein is described in U.S. 4,450,180 patent. A generally similar bag is described in U.S. 4,548,826. Generally, the bag therein described comprises and is fabricated from a flexible sheet material having two collateral tubular sections. The sections are parallel longitudinally extending that communicate with each other at the center of the package.

Referring now briefly initially to Figure 1, there is shown an embodiment of a microwave popcorn article composed of a microwave bag 12 formed from flexible sheet material such as paper and being of collateral tubular configuration, that is to say, being composed of a pair of parallel longitudinally extending tubes 14 and 16 which communicate with one another along a central longitudinal opening. The two parallel tubes 14 and 16 are separated by longitudinally extending side indentations 20 and 22. When the package comprises a paper bag, the bag can be composed of first and second face panels 24 and 26 respectively and the indentations 20 and 22 comprises gussets. When in a vertically aligned orientation, the bag has a bottom seal 28 and initially an open top or orifice 30 but a sealable seal area 31 that transversely extends the open sealable top. The sealable area can include a heat activated adhesive or a "cold seal" adhesive, as is convenient. After

1 for the EC and the merchant and deal with the external system on behalf of the EC and the merchant. A desired result of the invention is to shield all of the participants of a transaction from an external system and therefore reduce the number of trust relationships needed to complete a transaction. If a participant of a transaction has dual membership of this system and
5 an external system, then he has a choice of either acting as a member of this system or as a member of an external system. In the latter case, the SP will interface with the participants using the rules of an external system. For example, to deal with an external public and digital certificate or credential based system, the SP has in its possession all of the required certificate(s) or credential(s) which satisfies the trust relationship demanded by the external system. Such
10 credentials are required in order for the SP and the external system to complete the transaction initiated by the EC and the merchant. In this case, only the SP needs to have a trust relationship with the external system. Based on this trust relationship, individual ECs and merchants are able to complete transactions with the hypothetical external system.

Figure 3 is a diagrammatic representation of a preferred embodiment of an EC. In a
15 preferred embodiment of the invention, an EC is internally composed of the software/hardware components shown in Figure 3. The EC is ISO 7816-based and supports the same kind of communication protocols and commands as defined in ISO 7816.

The EC has a card operating system 550 to manage the EC's internal resources. The on-card cryptographic service 650 can be implemented in software or be provided by a
20 cryptographic co-processor (not shown in figure 3), or other hardware solutions, or a hybrid of software and hardware.

One of the unique features of the EC is the service provider data area (SPDA) in the EC memory, which contains the service providers' account and key information. The service provider data area (SPDA) 700 contains a number of slots. In the preferred embodiment, the
25 SPDA contains a pre-defined number (e.g. ten) of slots -- one for each potential service provider. In another embodiment, the number of slots may be dynamically changed. A record for each service provider can be placed into an empty slot. Each record contains the account number, public key, and other related information for a specific service provider.

Depending on the EC design, the SPDA can optionally allow each SP to include some
30 software (such as an "applet" in the JAVA terminology) to manage its own on-card data and provide an interface between the SP card data and the host application. In other words, the SPDA can contain more than just simple data; it can allow each SP to put a self-contained application program (such as an applet) on the EC to provide its own unique service to the cardholder. The advantage of this type of design is that the EC itself is now detached from the type of service it
35 can provide. Each SP can bring with it its own service capability. When another SP replaces an on-card SP, there will be no change necessary to the EC platform. The new SP applet is simply loaded into the card and it will perform what it is designed to do.

In the SPDA, each service provider is allocated space for public keys. In many transactions,

1 only one key pair is used, but for some online transactions, two or more key pairs are required.
If the SP uses the same public/private key pair for both the incoming and the signing of outgoing
messages, then one public key is enough. If the SP uses a different key pair for signing, then
both SP public keys (one for incoming messages and one for the signing of outgoing messages)
5 are required in the SPDA.

In the preferred embodiment of the invention, two public/private key pairs rather than one
public/private key pair is used to communicate with other applications through a network
because using two public/private key pairs rather than one public/private key pair provides
greater security. One pair is used for decrypting an incoming message, i.e., the sender encrypts
10 the message using the recipient's public key and the recipient decrypts the message using the
corresponding private key. The other pair is for the sender to digitally sign the message he sends
out and the recipient to verify the digital signature using the corresponding sender's public key.

Each service provider is allocated space for the number of public keys used by the service
provider. If the SP uses the same public/private key pair for both incoming messages and
15 signing of outgoing messages, then one public key is enough. If the SP uses different key pairs
for receiving and signing messages, then both of the SP's public keys are required in the SPDA.

In an alternative embodiment of the invention, more than two public/private key pairs may
be required and used by a service provider for even greater security.

When an EC holder is issued a new financial or non-financial instrument, the issuing
20 institution or a trusted third party will load the needed information comprising a record into an
available slot. The information in the slot can be erased when the service provider account is
closed. Some of the information in a slot can be read and modified during a transaction, e.g. an
account balance. Some information such as account number is write protected, but can be read.
Some information such as a private key is both read and write protected. The access conditions
25 600 contain security information such as PINs, biometric data, etc., that an EC user must submit
to open the card for use or to gain access to the information stored on the card.

Traditional Personal Identification Numbers (PINs) or other security measures such as
biometrics data are used to protect the EC. Biometrics involves the measurement of a
cardholder's biological traits, such as physical traits and behavioral traits. A biometric system
30 may measure an individual's fingerprints, hand-geometry, hand writing, facial appearance,
speech, physical movements, keyboard typing rhythms, eye features, breath, body odor, DNA,
or any other physical attribute of the cardholder. The functions provided by an EC can be
activated only after all the access conditions have been satisfied. Each service provider residing
on the card can optionally implement other access conditions.

35 Figure 4 shows the format of the service provider data area of a preferred embodiment of
the invention. Each service provider's information is allocated an entry in the table, which can
be protected by additional access conditions. The PIN 712 and the miscellaneous data field 714
allows the service provider to provide extra protection or data field to the instrument it supports.

1 The name field 702 contains the names of the service providers, which can be used by the
cardholder at the beginning of an online transaction to initially select the applicable service
provider for a transaction. The key type field 704 specifies the type of key the service provider
chooses to use, secret key, public key, etc. The key value 706 and account information fields
5 708 contain information unique to each service provider. The card type field 710 specifies the
type of instrument a service provider supports.

In the preferred embodiment of the invention, the on-card Operating System (COS)
provides some fundamental services for the cardholder. Following is a list of general functions
which can be performed by the COS:

- 10
- (1) Traditional OS functionality such as Memory management, task management, etc
 - (2) External communication-read/write of user data and communication protocol handling.
 - (3) Loading and updating of on-card cardholder information.
 - (4) User PIN changes.
 - 15 (5) Service Provider Data Area management-such as loading and updating of individual service
provider information, SPDA access control, etc.

The COS will also provide support during various stages of a transaction. For example, the
COS can handle the SP selection at the beginning of a transaction and record the transaction into
20 a log file when the transaction has been completed. An embodiment of the invention may
implement one of the following two design approaches to the COS or a hybrid of the two design
approaches:

- (1) Most of the intelligence can be put into the COS whereby the COS supports most of the EC
functionalities. Consequently, each on-card service provider area relies on the COS to carry
25 out the transaction with the merchant and the SP. In this approach, the COS can provide
a uniform interface with the outside world for all on-card SPs and efficiently carries out the
transaction once a SP has been selected.
- (2) Alternatively, the COS can be a pool of general services each on-card SP can utilize. Each
SP data area can contain applets, which have the intelligence to carry out a transaction with
30 the merchant and the SP. In this approach, the SP has more opportunity to implement its
own unique feature when performing a transaction.

Figure 5 shows how digital signatures are used in the preferred embodiment of the
invention. A sender of a message first prepares and sends the data portion of a message M 900
through a one way hash algorithm, H(*) 902. The output from the hash algorithm is called the
35 message digest MD of message M 903. The MD is then encrypted, E(*) 904, i.e. digitally signed,
using the sender's private key (Pri). The result is called the digital signature DS of a message M.
The DS is then combined with the original message M 900 and forms a complete message 906
ready for transmission to a recipient through a network 50.

(SUBSTITUTE)

-13-

In a preferred variation, at least a portion of the fat is supplied by a low moisture butter ingredient. Suitable low moisture butter ingredients and methods of preparing microwave popcorn products therewith are described in co-pending commonly assigned USSN 08/784,850 (filed Jan. 1, 1997) entitled "Shelf-Stable Butter Containing Microwave Popcorn". In general, however, the butter ingredients therein described are low moisture (i.e., less than 3%) butters that are commercially available. The fat/butter blends comprise about 200 ppm antioxidants. To assure shelf stability, the butter content is preferably limited to 10% of the added fat.

Salt

The present microwave popcorn articles additionally essentially include a salt component. Of course, microwave popcorn articles conventionally comprise a salt component. Typically, the salt component is a micro-sized salt, also known as ultrafine salt or pulverized salt or "flour" salt, typically having a mean particle size of about 22 microns. This flour salt is simply physically admixed in with the fat component to form a fat and salt slurry.

In the preferred embodiments, at least a portion of the total salt can be added in the form of a flour sized particulate to the fat slurry. In those embodiments, it is more preferred that the portion of the total salt added as a salt flour to the slurry be at least 60% of

AMENDED SHEET

(SUBSTITUTE)

-14-

the total salt, even preferably more than 75% of the total salt.

In less preferred variations, a coarse salt ingredient can be employed such as described in co-
5 pending commonly assigned USSN 08/998,751, filed December 29, 1997 entitled "Microwave Popcorn With Coarse Salt Crystals and Method of Preparation" (attorney docket 5108). Generally, the coarse salt therein described has a larger particle size of about 250 to 600 μm . Such
10 coarse salt is added to impart an organoleptic attribute in the finished product microwave popcorn to be more reminiscent of the stove-top at-home popped and seasoned popcorn. While in the preferred embodiments herein the salt is in flour form, in other embodiments all or a part
15 of the salt can be in the form of coarse salt added in the third station or in the separate particulates addition step herein.

Calcium Salt

The present microwave popcorn products essentially
20 further comprise a calcium ingredient of defined particle size in an amount effective to provide the desired calcium enrichment. Good results are obtained when the present microwave popcorn products contain about 360 to 3600 mg per 100 grams of the food charge. Better results
25 are obtained when the calcium is present at levels of about 360 to 1800 mg per 100 grams. For best results, the total calcium present ranges from about 930 to 1400 mg per 100 grams of the food charge. Excessive calcium fortification is to be avoided in part because the

AMENDED SHEET

1 transaction phase of a transaction. It can include approval/disapproval data and/or any other relevant data.

RN = Random number.

RN_{EC} = Random number generated by the EC and is sent to SP.

5 RN_{SP-EC} = Random number generated by the SP and is sent to EC.

RN_M = Random number generated by the merchant.

RN_{SP-M} = Random number generated by the SP and is sent to M.

SP = Financial or non-financial service provider

TA = Transaction (currency) amount.

10 Transaction Identification Number $_{SP-EC}$, TID_{SP-EC} (Transaction ID $_{SP-EC}$) = A data field whose value is assigned by the SP during the key exchange phase of a transaction. The EC will use this value to communicate with the SP during the same transaction.

Transaction Identification Number $_{SP-M}$, TID_{SP-M} (Transaction ID $_{SP-M}$) = A data field whose value is assigned by the SP during the key exchange phase of a transaction. The merchant will use this

15 value to communicate with the SP during the same transaction.

* = Combine or concatenation of data within an encryption E or a decryption D.

Figures 6A through 6Q comprise the flowchart for a preferred embodiment of the cryptographic system and method. For the purpose of simplifying the description and symbolism contained in figures 6A through 6Q, the flowchart assumes that each of the parties involved in the transaction uses one key pair. In another embodiment of the invention, two public key pairs may be used, in which case, both public keys need to be exchanged.

The preferred embodiment of the invention consists of two distinct phases: the key exchange phase and the transaction phase.

25 PHASE I: KEY EXCHANGE PHASE (HANDSHAKE PHASE)

The EC cardholder inserts the EC into a card read/write device or starts the EC equivalent software and enters a PIN number and/or satisfies the access conditions 110 to use the EC card. The entered security information conditions is compared 112 with the on-card information 114 to verify that user is authorized to use the EC. If the security information does not match the card security information, then the request to use the card is rejected 116. Otherwise, the card is unlocked 118 for use. Once the card is unlocked, the user can request the list of the on-card SPs available for selection and make a selection 120 by issuing an SP selection command to the EC. Once the SP is selected, the EC proceeds to start the key exchange (KE) with the SP. The public key of the selected SP, represented by the symbols SP-PK and PK_{SP} , is obtained from the EC's SPDA and is used to encrypt messages that will be sent to the SP.

The main purpose of the KE is to securely send the cardholder's public key, PK_{EC} 126 and an EC random number, RN_{EC} 124 to the SP. The SP response to the EC is to assign a session key and a transaction ID to the EC, which will be used by the EC to communicate with the SP for the

rest of the transaction. To format the KE message, the EC generates a random number, RN_{EC} 124, concatenates it with the EC's public key, PK_{EC} 126, and EC sensitive transaction data STD_{EC} 128 relevant to the transaction and/or required by the SP. The EC encrypts them 122 using the SP's public key, PK_{SP} , retrieved from the SPDA 120. The resulting EC cryptogram, $E_{ES-PK}(RN_{EC} * PK_{EC} * STD_{EC})$, is then combined 130 with the plain text portion of the message, $PLAIN\ TEXT_{EC}$ 132, if any, to form an EC combination message, $PLAIN\ TEXT_{EC} * E_{ES-PK}(RN_{EC} * PK_{EC} * STD_{EC})$. The EC's public key PK_{EC} 126 may be placed in the plain text $PLAIN\ TEXT_{EC}$ instead of being encrypted when forming the EC combination message.

Only sensitive data is encrypted. Non-sensitive response data is included in the plain text. Only the SP is able to read the sensitive data. In a multi-party transaction, the SP has full access to the sensitive information of all the participants.

The resulting EC combination message is then sent through a hashing algorithm 134 to form a hash message, which is the EC message digest MD_{EC} . The EC message digest MD_{EC} is digitally signed by the EC 136 using the EC private key 138 to form a digitally signed message $DS_{EC-Private-Key}$. The digitally signed message $DS_{EC-Private-Key}$ is then combined 140 with the EC combination message. The combination of the plain text $PLAIN\ TEXT_{EC}$, cryptogram $CRYPTO_{EC}$ and the digital signature $DS_{EC-Private-Key}$ is the KE message from the EC and is sent to the merchant 158 through a network. Plain text includes all the transaction data fields that are not sensitive in nature and therefore can be transmitted in a clear, discernable form; they do not need to be encrypted. These data fields are different for each message and are defined by the transacting parties.

To communicate with the SP, the merchant goes through essentially the same steps to format its own KE message with the SP as the EC goes through to format the EC's KE message with the merchant. The cardholder and the merchant do not communicate with the SP individually, but through a combined message. Consequently, there will be no need to exchange any confidential financial information between the cardholder and the merchant. The merchant prepares his device for the transaction 142 and selects from his own SPDA, which resides within the merchant's device, the same SP as the EC cardholder has selected for the transaction 144. The public key of the SP, represented by the symbols $SP-PK$ and PK_{SP} , is obtained from the SP's SPDA and is used to encrypt messages that will be sent to the SP.

To format its own KE message, the merchant generates a random number, RN_M 148, concatenates it with the merchant's public key, PK_M 150, and the merchant's sensitive transaction data STD_M . Sensitive transaction data is data that is relevant to the transaction and/or required by the SP 152. The merchant encrypts 146 the combined data using the public key of the service provider, PK_{SP} . The resulting cryptogram is then combined 154 with the plain text portion $PLAIN\ TEXT_M$ 156 of the message, if any, to form a merchant combination message. The merchant's public key PK_M 150 may be placed within the plain text $PLAIN\ TEXT_M$ instead of being encrypted when forming the merchant combination message $PLAIN\ TEXT_M * E_{SP}$.

1 $PK(RN_M * PK_M * STD_M)$.

The merchant combination message $[PLAIN\ TEXT_M * E_{SP-PK}(RN_M * PK_M * STD_M)]$ is further combined 158 with the EC's KE message $\{[PLAIN\ TEXT_{EC} * E_{SP-PK}(RN_{EC} * PK_{EC} * STD_{EC})] * DS_{EC-Private-Key}\}$ to form the data portion of the KE message for both the merchant and the EC, i.e., the EC-merchant combination message $\{[PLAIN\ TEXT_{EC} * E_{SP-PK}(RN_{EC} * PK_{EC} * STD_{EC})] * DS_{EC-Private-Key}\} * [PLAIN\ TEXT_M * E_{SP-PK}(RN_M * PK_M * STD_M)]$. The EC-merchant combination message is sent through a hashing algorithm 160 to form a hash message, which is the merchant message digest MD_M . The merchant message digest MD_M is digitally signed 162 by the merchant using the merchant's private key 164 to form a merchant digitally signed message $DS_{M-Private\ Key}$. The merchant digitally signed message $DS_{M-Private\ Key}$ is then combined 166 with the data portion of the message, i.e., the EC-merchant combination message to form a key exchange request message $\ll \{ [PLAIN\ TEXT_{EC} * E_{SP-PK}(RN_{EC} * PK_{EC} * STD_{EC})] * DS_{EC-Private-Key} \} * [PLAIN\ TEXT_M * E_{SP-PK}(RN_M * PK_M * STD_M)] \gg * DS_{M-Private-Key}$ for both the merchant and EC. This final message is sent to the SP through a network. Figure 7 represents the final format and content of the key exchange request message from a merchant to an SP.

In the preferred embodiment of the invention, the merchant does not check the MD of the EC's request message MD_{EC} because the EC encrypts his public key. However, in an alternate embodiment of the invention, if the EC chooses not to encrypt his public key then the merchant can optionally check the EC's MD before passing it to the SP. In either the case where the EC encrypts his public key or where the EC does not encrypt his public key, for enhanced security and to avoid possible processing errors by the merchant, the SP can still check the EC's MD. When the merchant receives a combination response from the SP for both himself and the EC, the merchant does not have to check the MD for the EC since it is part of the overall message formed by a single originator -- the SP. The merchant only needs to check the MD of the overall message he receives from the SP.

When the SP receives the KE request message, the SP first separates 168 the data portion of the KE request message from the DS and feeds the data portion of the KE request message into a one-way hash algorithm to recalculate the message digest, which becomes MD_M . The SP then separates the merchant's plain text $PLAIN\ TEXT_M$, cryptogram $CRYPTO_M$, digital signature $DS_{M-Private-Key}$ and the EC's KE request message $PLAIN\ TEXT_{EC} * CRYPTO_{EC} * DS_{EC-Private-Key}$. Using its own private key, the SP decrypts merchant's cryptogram 170 and recovers, among other information, the merchant's random number RN_M 148 and the merchant's public key PK_M 150. The SP then uses the recovered PK_M to decrypt the digital signature signed by the merchant $DS_{M-Private-Key}$ and recovers the MD_M for the merchant's KE message. The SP compares 172 the newly hashed $MD^{\wedge}_M$ 168 with the MD_M 170 recovered by decrypting the DS from the original KE message. If there is a discrepancy between $MD^{\wedge}_M$ and MD_M found, then the KE message has been corrupted and is therefore rejected 174. If $MD^{\wedge}_M$ and MD_M match, then the SP separates the data portion of the EC's KE request message from the DS and feeds the data

1 portion of the EC's KE request message into a one-way hash algorithm to recalculate the message digest ($MD_{EC}^{\wedge}$). The SP then separates the EC's plain text $PLAIN\ TEXT_{EC}$, if any, cryptogram $CRYPTO_{EC}$, and digital signature $DS_{EC-Private\ Key}$ in the data portion of the EC's KE request message 176. Using its own private key, the SP decrypts EC's cryptogram and recovers, among other information, EC's random number RN_{EC} and EC's public key PK_{EC} . The SP then uses the recovered PK_{EC} to decrypt the digital signature signed by EC and recovers the MD_{EC} for EC's KE message. In the step 178, SP compares the newly hashed $MD_{EC}^{\wedge}$ 176 with the MD_{EC} recovered by decrypting the DS from the original KE message. If there is any discrepancy found, the KE message has been corrupted and is therefore rejected 180. Otherwise, SP is ready to send a KE response message back to merchant and EC.

To format the KE response message for the EC, the SP generates a random number, RN_{SP-EC} 184, and a session key $Skey_{EC}$ 186 for the EC, combines them with the EC generated random number, 188 RN_{EC} , service provider sensitive transaction data STD_{SP-EC} 190 and encrypts them 192 using the EC's public key PK_{EC} . The resulting cryptogram, $E_{EC-PK}(RN_{EC} * RN_{SP-EC} * Skey_{EC} * STD_{SP-EC})$, is combined 196 with a transaction identification number, TID_{SP-EC} 194 assigned to the EC by the SP and plain text, $PLAIN\ TEXT_{SP-EC}$ 195, if any, to form the data portion of the response message for the EC. The SP runs this data through a hash algorithm to calculate the message digest MD_{SP-EC} 198. Using its own private key 202, the SP creates a digital signature $DS_{SP-Private-Key}$ 200 for the response message by digitally signing the message digest MD_{SP-EC} . After combining 204 the data portion of the message with the newly calculated $DS_{SP-Private-Key}$, the SP's KE response message for the EC is complete, $[TID_{SP-EC} * PLAIN\ TEXT_{SP-EC} * E_{EC-PK}(RN_{SP-EC} * RN_{EC} * Skey_{EC} * STD_{EC})] * DS_{SP-Private-Key}$.

To format the KE response message for the merchant, the SP generates a random number RN_{SP-M} 208 and a session key $Skey_M$ 210 for the merchant and combines them with the merchant generated random number RN_M 212, sensitive transaction data STD_{SP-M} 214 and encrypts them 206 using the merchant's public key PK_M recovered in 170. The resulting cryptogram is combined 216 with a transaction identification number, TID_{SP-M} 218, assigned to the merchant by the SP and plain text, $PLAIN\ TEXT_{SP-M}$ 220, if any, to form the data portion of the response message for merchant. The resulting combination message, $TID_{SP-M} * PLAIN\ TEXT_{SP-M} * E_{M-PK}(RN_{SP-M} * RN_M * Skey_M * STD_{SP-M})$ is further combined 222 with the KE response message for the EC, $[TID_{SP-EC} * PLAIN\ TEXT_{SP-EC} * E_{EC-PK}(RN_{SP-EC} * RN_{EC} * Skey_{EC} * STD_{EC})] * DS_{SP-Private-Key}$, to form the data portion of the SP's final KE response message, $[TID_{SP-EC} * PLAIN\ TEXT_{SP-EC} * E_{EC-PK}(RN_{SP-EC} * RN_{EC} * Skey_{EC} * STD_{EC})] * DS_{SP-Private-Key} * [TID_{SP-M} * PLAIN\ TEXT_{SP-M} * E_{M-PK}(RN_{SP-M} * RN_M * Skey_M * STD_{SP-M})]$. The SP runs the data portion through a hash algorithm to calculate the message digest 224. Using its own private key 228, the SP creates a digital signature, $DS_{SP-Private-Key}$ 226, for the response message by digitally signing the message digest. After combining 230 the data portion of the message with the newly calculated DS 226, the KE response message for both the EC and the merchant is complete. The response message

1 <<{[TID_{SP-EC}*PLAIN TEXT_{SP-EC}*(E_{EC-PK}*RN_{SP-EC}*RN_{EC}*Skey_{EC}*STD_{SP-EC})]*DS_{SP-Private-Key}}[TID_{SP-M}*PLAIN TEXT_{SP-M}*E_{M-PK}(RN_{SP-M}*RN_M*Skey_M*STD_{SP-M})]>>DS_{SP-Private-Key} is sent back to the merchant through a network. Figure 8 depicts the final format and content of the combined KE response message from the SP to the merchant.

5 When the merchant receives the KE response message 232, the merchant first separates the DS_{SP-Private-Key} which was signed by the SP, and then feeds the data portion of the combined KE response message into a one-way hash algorithm to recalculate the message digest MD[^]_{SP-M}. The merchant then separates the data portion of the SP's KE response message, i.e., TID_{SP-M}, PLAIN TEXT_{SP-M}, CRYPTO_{SP-M}, [(TID_{SP-EC}*PLAIN TEXT_{SP-EC}*CRYPTO_{SP-EC})]*DS_{SP-Private-Key}. The
 10 merchant uses SP's public key (selected from 144) to decrypt the digital signature DS_{SP-Private-Key} to recover the message digest MD_{SP-M}. The merchant compares 234 the newly hashed MD[^]_{SP-M} with the MD_{EC}. If there is any discrepancy between MD[^]_{SP-M} and MD_{SP-M}, the KE response message has been corrupted and is therefore rejected 236. If MD[^]_{SP-M} and MD_{SP-M} match, then the merchant identifies the part of the response message which is meant for him and decrypts the
 15 cryptogram CRYPTO_{SP-M} 238 using his own private key. The merchant should be able to recover the original random number RN_M (of 148) that he sent to the SP in the KE request message. The merchant compares 240 the recovered random number RN_M (of the step 238) with the original random number RNM. If they are not equal, then the message has been corrupted and the message is rejected 242. Since the random number RN_M can only be recovered by the
 20 SP using the correct SP private key, it is assured that the sender of the message is indeed the selected SP. The merchant then forwards the EC's KE response message [(TID_{SP-EC}*PLAIN TEXT_{SP-EC}*CRYPTO_{SP-EC})]*DS_{SP-Private-Key} to the EC and prepares for the transaction phase of the transaction.

When the EC receives the KE response message 260, the EC first separates the DS_{SP-Private-Key} which was signed by the SP, and then feeds the data portion of the KE response message for
 25 the EC into a one-way hash algorithm producing a MD[^]_{SP-EC}. The EC then separates the data portion of the message, i.e., TID_{SP-EC}, PLAIN TEXT_{SP-EC}, CRYPTO_{SP-EC}, DS_{SP-Private-key}. The EC uses SP's public key (selected in 120) to decrypt the digital signature DS_{SP-Private-key} message and recovers the message digest MD_{SP}. The EC compares 262 the newly hashed MD[^]_{SP-EC} (in 260) with the MD_{SP-EC} recovered by decrypting the DS_{SP-Private-key} from the KE response message for
 30 EC. If there is any discrepancy between MD[^]_{SP-EC} and MD_{SP-EC} found, the KE response message for the EC has been corrupted and is therefore rejected 264. If MD[^]_{SP-M} and MD_{SP-M} match, the EC identifies the part of the response message which is meant for him and decrypts 266 the cryptogram CRYPTO_{SP-EC}, which is contained in the message, using his own private key. The
 35 EC should be able to recover the original random number RN_{EC} (of 124) that was sent in the EC KE request message. The EC compares 268 the recovered random number RN_{EC} (of 266) with the original random number RN_{EC} (of 124). If the random numbers are not equal, then the message has been corrupted and the message is rejected 270. Since only the SP using the correct

1 SP private key can recover the random number RN_{EC} , this serves to ensure that the sender of the message is indeed the selected SP. The EC prepares for the transaction phase of the transaction.

There will be a predefined timeout period set in the EC and the merchant. During a transaction, if a response message is not received within a timeout period, the EC and the merchant will consider the transaction aborted and will either retry or start the recovery process.

After successful completion of the KE message exchanges, the SP has EC's public key and the merchant's public key. At this point, both the EC and the merchant has a random number, a transaction ID, and a session key from the SP. The EC and the merchant must send the two random numbers recovered from the KE response message back to the SP to complete the key exchange phase of the transaction. This can be done in two ways. The random numbers can be sent back through a confirmation message from both the EC and the merchant. Or the random numbers can be sent back as part of the next message going out from the EC and the merchant to the SP, such as a transaction message. The second method is simpler and is described in phase II below. The random numbers are used only once to ensure the correctness of the key exchange between the SP and merchant, and the SP and EC. Once the session keys and transaction identification number have been established, the random number are no longer be used.

PHASE II: TRANSACTION PHASE

During the transaction phase, the merchant and the EC each sends their own account information such as an account number and other transaction related data such as transaction amount, request for approval or other processing, to the SP. Again, the EC and the merchant talk to the SP individually but through combined messages and the merchant is responsible for combining the messages and sending them as one message to the SP.

The EC first forms the transaction message by concatenating the random number RN_{SP-EC} 274 from the SP and the EC's account information with the selected SP, AI_{EC} 276, transaction amount TA 280 and any other sensitive data 278 relevant to the transaction and/or required by the SP. The EC encrypts 272 them using the session key $Skey_{EC}$ assigned by the SP. The $Skey_{EC}$ is a secret key and uses a cryptographic algorithm different from the cryptographic algorithm used for the public key encryption. The resulting cryptogram $CRYPTO_{EC}$, i.e., $Skey_{EC}(RN_{SP-EC} * STD_{EC} * AI_{EC} * TA)$, is then combined 282 with the transaction ID TID_{SP-EC} 284 and the plain text $PLAIN TEXT_{EC}$ 286, if any, to form the data portion of the EC's transaction message, $TID_{SP-EC} * PLAIN TEXT_{EC} * CRYPTO_{EC}$. The data portion 282 is fed into a one-way hash algorithm 288 to calculate the message digest MD_{EC} and the MD_{EC} is then digitally signed 290 by the EC's private key 292. The resulting digital signature 290 is combined with the data portion of the message (from 282) 294 to form EC's transaction request message and then sent to the merchant, $[TID_{SP-EC} * PLAIN TEXT_{EC} * Skey_{EC}(RN_{SP-EC} * STD_{EC} * AI_{EC} * TA)] * DS_{EC-Private-Key}$.

The merchant goes through essentially the same steps to form his transaction message. The merchant forms his transaction message by concatenating 246 the RN_{SP-M} from the SP and the

1 merchant's account information with the selected SP, AI_M 248, transaction amount TA 252 and
 any other sensitive data STD_M 250 relevant to the transaction and/or required by the SP. The
 merchant encrypts them 244 using the session key $Skey_M$ assigned by the SP. The session key
 $Skey_M$ is a secret key and is created using a different cryptographic algorithm, such as DES, from
 5 the cryptographic algorithm used for public key encryption. The session key $Skey_M$ is used to
 perform the encryption at this point to create the cryptogram $CRYPTO_M$. The resulting
 cryptogram $CRYPTO_M$, i.e., $Skey_M(RN_{SP-M} * STD_M * AI_M * TA)$, is then combined 254 with the
 transaction ID TID_{SP-M} 256 and the plain text $PLAIN TEXT_M$ 258, if any, to form the data portion
 of the merchant's transaction message, $TID_{SP-M} * PLAIN TEXT_M * CRYPTO_M$. This data is
 10 combined 296 with the EC's transaction request to form the data portion of the final transaction
 request message for the SP, $[TID_{SP-EC} * PLAIN TEXT_{EC} * Skey_{EC}(RN_{SP-EC} * STD_{EC} * AI_{EC} * TA)] * DS_{EC-Private-Key} * [TID_{SP-M} * PLAIN TEXT_M * Skey_M(RN_{SP-M} * STD_M * AI_M * TA)]$.
 As before, the merchant feeds his combined data through a one-way hash algorithm 298 to
 calculate the message digest MD_M and the MD_M is then digitally signed 300 by the merchant's
 15 private key 302. The resulting digital signature $DS_{M-Private-Key}$ 300 is combined 304 with the data
 portion of the message (from 296) to form the final transaction request message and is then sent
 to the SP, $\{[TID_{SP-EC} * PLAIN TEXT_{EC} * Skey_{EC}(RN_{SP-EC} * STD_{EC} * AI_{EC} * TA)] * DS_{EC-Private-Key} * [TID_{SP-M} * PLAIN TEXT_M * Skey_M(RN_{SP-M} * STD_M * AI_M * TA)]\} * DS_{M-Private-Key}$. Figure 9 depicts the final
 format of the transaction request message.

20 When the SP receives the transaction request message, the SP first checks 306 the two
 transaction identification numbers, i.e., TID_{SP-EC} and TID_{SP-M} , sent by the EC and the merchant
 and makes sure they are valid. When either TID_{SP-M} (of 210) or TID_{SP-EC} (of 186) is found invalid
 306, then the message is rejected 308. If the transaction identification numbers are both valid,
 then the SP proceeds to separate the $DS_{M-Private-Key}$ from the data portion of the message and feeds
 25 the data portion of the message, $\{[TID_{SP-EC} * PLAIN TEXT_{EC} * Skey_{EC}(RN_{SP-EC} * STD_{EC} * AI_{EC} * TA)] * DS_{EC-Private-Key} * [TID_{SP-M} * PLAIN TEXT_M * Skey_M(RN_{SP-M} * STD_M * AI_M * TA)]\}$ into a one-way hash algorithm to calculate the message digest MD^M of
 this message. The SP separates the data portion of the message, i.e., TID_{SP-M} , $PLAIN TEXT_M$, $CRYPTO_M$, $DS_{M-Private-Key}$, $(TID_{SP-EC} * PLAIN TEXT_{EC} * CRYPTO_{EC}) * DS_{EC-Private-Key}$. The
 30 SP decrypts 310 the $DS_{M-Private-Key}$ using the merchant's public key and compares the newly
 recovered message digest MD_M with the message digest just calculated MD^M (from 306). If
 MD^M and MD_M are not equal, the message has been corrupted and is rejected 314. If MD^M
 and MD_M match, then the SP decrypts 316 the encrypted portion of the message using the session
 key $Skey_M$ (of 210) it assigned to the merchant during the KE phase and recovers the data fields
 35 contained in the encrypted portion. The SP compares 318 the random number RN_{SP-M} the
 merchant sends back in the message with the message the SP sent to the merchant originally,
 RN_{SP-M} (from 208). If the random numbers are not equal, then the merchant has failed the mutual
 authentication test and the message is rejected 320.

1 In addition, the SP will verify the EC's account information AI_{EC} and the transaction data such as the transaction amount TA. The message is rejected 320 if the AI is no longer valid. It is also rejected when the TA from the EC and the TA from the merchant do not match. There may be other conditions for invalidating a message. If the account information AI_{EC} and the transaction are valid, then the SP goes on to verify the EC portion of the message.

5 As with the merchant's message, the SP first separates 322 the $DS_{EC-Private-Key}$ from the EC's message and feeds the data portion of the EC's message, $(TID_{SP-EC} * PLAIN TEXT_{EC} * CRYPTO_{EC})$ into a one-way hash algorithm to calculate the message digest $MD^{\wedge}_{EC}$ of the EC message. The SP separates the data portion of EC's transaction request, TID_{SP-EC} , $PLAIN TEXT_{EC}$, $CRYPTO_{EC}$, $DS_{EC-Private-Key}$. The SP decrypts 324 $DS_{EC-Private-Key}$ using EC's public key PK_{EC} and recovers MD_{EC} . The SP compares 326 the recovered MD_{EC} with $MD^{\wedge}_{EC}$. If $MD^{\wedge}_{EC}$ and MD_{EC} are not equal, the message has been corrupted and is rejected 328. If $MD^{\wedge}_{EC}$ and MD_{EC} match, then the SP decrypts 330 the encrypted portion of the EC message using the session key $Skey_{EC}$ (of 186) it assigned to the EC during the KE phase and recovers the data fields contained in it. The SP compares 332 the random number RN_{SP-EC} the EC sends back in the message with the random number RN_{SP-EC} it sent out to the EC originally (in 184). If the random numbers are not equal, then the EC has failed the mutual authentication test and the message is rejected 334. The SP will verify the merchant's account information AI_M and the transaction data such as the transaction amount TA and will reject the message when the account information is invalid or when the transaction data does not meet the SP's criterion 334. Once the integrity and authenticity of the overall message has been established, the SP can process the data contained in the message and send a response message back. The random number that is sent back in this message completes the mutual authentication between the SP and the merchant, and between the SP and the EC. After this message, no exchange of random numbers will be necessary. The SP can chooses to use the random number as the transaction identification number which the merchant and the EC will use in all subsequent messages that they send to the SP.

20 As before, the response message contains information for both the EC and the merchant. To format the transaction response message for the EC, the SP generates the response data for the EC, $Response Data_{SP-EC}$ 338, and encrypts 336 it using the session key $Skey_{EC}$ assigned to the EC. Only sensitive data is encrypted. Non-sensitive response data is included in the plain text. The cryptogram $CRYPTO_{SP-EC}$, i.e., $E_{Skey-EC}(Response Data_{SP-EC})$, is combined 340 with the transaction identification number TID_{SP-EC} 342 that the SP assigned to the EC (from 194) and the plain text that the SP has for EC 344, if any, to form the data portion of the response message for the EC, i.e., $TID_{SP-EC} * PLAIN TEXT_{SP-EC} * E_{Skey-EC}(Response Data_{SP-EC})$. The data portion of the message is fed into a hash algorithm 346 to generate a MD_{SP-EC} which is digitally signed 348 by the SP using the SP's private key 350. The $DS_{SP-Private-Key}$ is combined 352 with the data portion of the response message (from 340) to form the complete response message for the EC, $[TID_{SP-EC} * PLAIN TEXT_{SP-EC} * E_{Skey-EC}(Response Data_{SP-EC})] * DS_{SP-Private-Key}$.

(SUBSTITUTE)

-23-

If the slurry viscosity is too high, then the slurry becomes unpumpable. The concentrations of salt and calcium ingredients are selected such that the slurry has a viscosity of less than 10,000 cps (10 kg/m.s), preferably less than about 4,000 cps (4 kg/m.s), and, for best results, less than 1,000 cps (1 kg/m.s).

The slurry can be added at temperatures ranging from about 15.5° to 65.5°C (60° to 150°F), preferably about 21.1° to 54.4°C (70 to 130°F).

While a pencil jet spray is preferred for use herein, equivalents thereof in terms of dispensing the slurry can also be used. For example, a multiplicity of very fine jet streams, (e.g., 3-12), or a sparge can be used to achieve the desired dispersion hereunder. Also, other spray types, (e.g., a cone spray, a mist spray, or a fan spray) are useful herein. However, great care must be taken in selecting such useful alternatives so as to avoid getting slurry in the bag seal area. In other embodiments, the spray can be gas assisted, e.g., air, steam, or inert gas.

In preferred embodiments, the bag 12 has a microwave chamber (i.e., wherein one major face panel has an intermediate microwave susceptor layer between the inner and outer bag layers) and, for cost considerations, a microwave susceptor-free chamber. In the preferred practice, the kernel popcorn, fat slurry and particulate(s) are charged to the microwave channel. Conventionally, the microwave channel is the lesser channel (i.e., being formed by the smaller major face 24) and the greater channel is the microwave free

AMENDED SHEET

1 identification number is valid, then the merchant separates the $DS_{SP-Private-Key}$ which was signed
by the SP, from the data portion of the transaction response message, and then feeds the data
portion of the EC transaction response message $TID_{SP-EC} * PLAIN TEXT_{SP-EC} * E_{Skey-EC}(Response$
5 $Data_{SP-EC})$ into a one-way hash algorithm producing $MD^{\wedge}_{SP-EC}$. The EC separates the message
into different parts, TID_{SP-EC} , $PLAIN TEXT_{SP-EC}$, $CRYPTO_{SP-EC}$, $DS_{SP-Private-Key}$. The EC decrypts 398
the encrypted portion of SP's message using the session key $Skey$ assigned by the SP during the
KE phase and recovers the data fields contained within it. The EC uses SP's public key (from
120) to decrypt the digital signature $DS_{SP-Private-Key}$ and recovers the message digest MD_{SP-EC} . The
merchant compares 400 the newly hashed $MD^{\wedge}_{SP-EC}$ 394 with the recovered MD_{SP-EC} . If $MD^{\wedge}_{SP-EC}$
10 and MD_{SP-EC} do not match, then the transaction response message has been corrupted and is
therefore rejected 402. If the message digests match, then the EC starts processing the message.

At the end of the transaction, the EC and the merchant can, if required by the SP, send an
acknowledgement message to the SP to signal that the response message has been correctly
received and processed. This acknowledgement data can be included as a part of the next
15 message to be sent to the SP, if there are more messages to be exchanged between the SP and the
merchant and the EC before the transaction ends. Or the acknowledgement data can be a
message by itself.

To format the acknowledgement message, the EC first encrypts 404 the sensitive part of the
acknowledgement data, Acknowledgement Data_{EC}, 406, if any, using the session key, $Skey_{EC}$
20 thus creating $Skey_{EC}(Acknowledgement Data_{EC})$. The EC combines 408 the resulting cryptogram
with the transaction identification number TID_{SP-EC} 410 assigned by the SP and the plain text
 $PLAIN TEXT_{EC}$ 412, if any. This forms the data portion of EC's acknowledgement message,
 $TID_{SP-EC} * PLAIN TEXT_{EC} * Skey_{EC}(Acknowledgement Data_{EC})$. This combined data is then fed
into a one-way hash algorithm 414 to generate the MD_{EC} . The resulting MD_{EC} is then digitally
25 signed 416 by the EC using the EC's private key 418 to generate a $DS_{EC-Private-Key}$. The $DS_{EC-Private-}$
 Key is combined 420 with the data portion of the message (from 408) to form the complete
acknowledgement message for the EC, $[TID_{SP-EC} * PLAIN TEXT_{EC} * Skey_{EC}(Acknowledgement$
 $Data_{EC})] * DS_{EC-Private-Key}$. The acknowledgement message is then sent to the merchant.

The merchant goes through the same steps to form his own acknowledgement message. To
30 format the acknowledgement message, the merchant first encrypts the sensitive parts of the
acknowledgement data, Acknowledgement Data_M 386, if any using the session key $Skey_M$
assigned by the SP to merchant, thus creating $Skey_M(RN_{SP-M} * Acknowledgement Data_M)$. The
merchant combines 388 the resulting cryptogram with the transaction identification number
 TID_{SP-M} 390 assigned by the SP, and the plain text $PLAIN TEXT_M$ (from 392), if any. This forms
35 the data portion of the merchant's acknowledgement message, $TID_{SP-M} * PLAIN TEXT_M *$
 $Skey_M(RN_{SP-M} * Acknowledgement Data_M)$. This data portion is further combined 422 with the
acknowledgement message received from the EC to form the data portion of the combined
acknowledgement message for the SP, $\{[TID_{SP-EC} * PLAIN TEXT_{EC} * Skey_{EC}(Acknowledgement$

1 Data_{EC})]*DS_{EC-Private-Key}}[TID_{SP-M}*PLAIN TEXT_M*Skey_M(Acknowledgement Data_M)]. The merchant feeds the data portion of the combined acknowledgement message for the SP into a one-way hash algorithm to generate the message digest MD_M. The resulting MD_M is then digitally signed by the merchant using the merchant's private key 428 to generate DS_{M-Private-Key} 426. The DS_{M-Private-Key} is combined 430 with the data portion of the message (from 422) to form the final combined acknowledgement message of the EC and the merchant designated for the SP, <<{[TID_{SP-EC}*PLAIN TEXT_{EC}*Skey_{EC}(Acknowledgement Data_{EC})]*DS_{EC-Private-Key}}[TID_{SP-M}*PLAIN TEXT_M*Skey_M(Acknowledgement Data_M)]>>*DS_{M-Private-Key}. This message is then sent to the SP. Figure 11 depicts the final format of the transaction acknowledgement message.

10 TID_{SP-M} is the transaction identification number assigned by the SP to the merchant (from 218) and TID_{SP-EC} is the transaction identification number assigned by the SP to the EC (from 194). Upon receiving the transaction acknowledgement message, the SP checks 432 the two transaction identification numbers, TID_{SP-M} and TID_{SP-EC}, sent by the EC and the merchant and makes sure they are valid. When either TID_{SP-M} or TID_{SP-EC} is found invalid, then the message is rejected 434. If the transaction identification numbers are both valid, then the SP proceeds to separate the DS_{M-Private-Key} from the combined acknowledgement message and feeds the data portion of the combined acknowledgement message <<{[TID_{SP-EC}*PLAIN TEXT_{EC}*Skey_{EC}(Acknowledgement Data_{EC})]*DS_{EC-Private-Key}}[TID_{SP-M}*PLAIN TEXT_M*Skey_M(Acknowledgement Data_M)]>> into a one-way hash algorithm to calculate the message digest MD[^]_M of this message. The SP separates the data portion of the message, TID_{SP-M}, PLAIN TEXT_M, CRYPTO_M, DS_{M-Private-Key}, (TID_{SP-EC}*PLAIN TEXT_{EC}*CRYPTO_{EC})*DS_{EC-Private-Key}. The SP decrypts 436 the DS_{M-Private-Key} using the merchant's public key PK_M and compares the recovered message digest MD_M 432 with the message digest just calculated MD[^]_M 436. If MD[^]_M and MD_M are not equal, then the message has been corrupted and is rejected 440. 25 If MD[^]_M and MD_M match, then the SP decrypts 442 the encrypted portion of the merchant's acknowledgement message using the session key Skey_M (from 210) that it assigned to the merchant during the KE phase and recovers the acknowledgement data contained within it.

The SP separates 444 the DS_{EC-Private-Key} from the EC's acknowledgement message and feeds the data portion of the EC's acknowledgement message, TID_{SP-EC}*PLAIN TEXT_{EC}*CRYPTO_{EC}, 30 into a one-way hash algorithm to calculate the message digest MD[^]_{EC} of this message. The SP separates the data portion of the EC's acknowledgement message, TID_{SP-EC}, PLAIN TEXT_{EC}, CRYPTO_{EC}, DS_{EC-Private-Key}. The SP decrypts 446 the DS_{EC-Private-Key} using the EC's public key PK_{EC} and compares 448 the recovered MD_{EC} with the message digest just calculated MD[^]_{EC} 444. If the message digests are not equal, then the message has been corrupted and is rejected 450. 35 If MD[^]_{EC} and MD_{EC} match, then the SP decrypts 452 the encrypted portion of the message using the session key Skey_{EC} (from 186) that it assigned to the EC during the KE phase and recovers the acknowledgement data contained within it. This completes the processing of the transaction phase of the transaction 454.

(SUBSTITUTE)

-26-

Without further elaboration, it is believed that one skilled in the art can, using the preceding description, utilize the present invention to its fullest extent. The following preferred specific
5 embodiments are, therefore, to be construed as merely illustrative and not limitative of the remainder of the disclosure. It will be appreciated that other
modifications of the present invention, within the skill of the microwave popcorn art, can be undertaken without
10 departing from the invention.

Example 1

An improved microwave popcorn article of the present invention comprising a microwave popcorn bag is prepared having the popcorn/fat charge of the
15 composition indicated below. The microwave popcorn bag is fabricated substantially in accordance with the teachings of U.S. Pat. No. 4,450,180. Microwave popcorn articles comprising microwave popcorn bags of this type are available under the brand name Betty Crocker™/Pop
20 Secret™. The popcorn fat charge has the following composition:

	<u>Ingredients</u>	<u>Weight %</u>
	Popcorn	92.1
	Fat ¹	2.4
25	Salt	2.7
	CaCO ₂ ² 2.5	
	Artificial butter flavor	<u>0.3</u>
		100.0

- 30 1. A hydrogenated soybean oil available from Cargill Foods under the trade name 600S.

AMENDED SHEET

(SUBSTITUTE)

-27-

2. Pure calcium carbonate available from Specialty Minerals Inc. having a mean particle size of 3 μm .

5 A supply of the fat, butter, salt and CaCO_2 is prepared to form a warm slurry (about 122°F; 50°C). The slurry has a viscosity of 3500 cps (3.5 kg/m.s).

The fat slurry comprises:

	Fat	44.5%
	Salt	25.7%
10	CaCO_2	6.2%
	Butter	23.6%

Thus, the slurry has about 50% of the total salt and about 50% of the calcium carbonate. The calcium carbonate had a particle size of less than 25 μm .

15 The salt added to the slurry was a flour salt having a mean particle size of about 22 μm .

A quantity of microwave popcorn bags were filled as follows:

20 About 82g of popcorn was dispensed by the dispensing wheel into the funnel.

The popcorn filled bag was then advanced to a second filling station. A fat slurry applicator was timed to dispense about 4.7g of the slurry in the form of a downwardly projecting vertically aligned pencil jet spray. The duration of the spray was about 0.5 seconds. The slurry charged the fat slurry within the microwave popcorn bag below the seal area.

25 The popcorn and fat filled bags were then advanced to a third filling station. About 1.2g of salt were dropped by gravity into the open end of the bag. At the

1 request messages and the transaction response message include plain text, if any, a cryptogram,
and a digital signature of the sending party.

In the case when the SP needs to act as the surrogate-certificate for the EC and/or the
merchant in order to deal with a certificate-based external system, the SP shields the EC and/or
5 the merchant from the operation of the external interface. The SP only returns to the EC and/or
the merchant, the information needed to complete the transaction with the EC and/or the
merchant.

While there have been described herein what are considered to be preferred and exemplary
embodiments of the present invention, other modifications of the invention shall be apparent to
10 those with ordinary skill in the art. Therefore, it is desired to be secured in the appended claims
all such modifications and extensions as fall within the true spirit and scope of the
invention. The invention is to be construed as including all embodiments thereof that fall within
the scope of the appended claims and the invention should only be limited by the appended
claims below. In addition, one with ordinary skill in the art will readily appreciate that other
15 applications may be substituted for those set forth herein without departing from the spirit and
scope of the present invention.

20

25

30

35

(SUBSTITUTE)

- 29 -

WHAT IS CLAIMED IS:

1. A method for filling a microwave popcorn bag with a food charge of popcorn kernels, a fat slurry, and a particulate, comprising the steps of:
 - 5 A. providing a microwave popcorn bag having a sealed portion, an open sealable top portion defining an orifice and a seal area extending across the orifice in an open configuration and in a vertically aligned orientation;
 - 10 B. filling the bag through the upper orifice with a quantity of popcorn kernels and the fat slurry;
 - 15 C. filling the bag through the upper orifice with a quantity of a particulate after the bag is filled with the popcorn kernels and the fat slurry, wherein at least one of the fat slurry and the particulate includes a calcium ingredient; and
 - 20 D. sealing the open top end of the popcorn bag after the bag has been filled with the quantity of popcorn kernels, the fat slurry, and the quantity of particulate.
- 25 2. The method of claim 1 wherein the step of filling the bag with the quantity of popcorn kernels and the fat slurry comprises the substeps of:
 1. dispensing the quantity of popcorn kernels in an airborne stream; and concurrently,
 2. spraying a quantity of the fat slurry into the airborne popcorn stream to coat the popcorn with
 - 30 the slurry.

(SUBSTITUTE)

-30-

3. The method of claim 1 wherein the step of filling the bag with the quantity of popcorn kernels and the fat slurry comprises the substeps of:
 1. dispensing the quantity of popcorn kernels through the upper orifice; and
 2. spraying a quantity of fat slurry through the upper orifice defined by the open top end.
4. The method of claim 3 wherein the spraying step is after the dispensing step.
5. The method of claim 4 wherein in step C the particulate includes the calcium ingredient which has a mean particle of less than 25 microns.
6. The method of claim 4 wherein the fat slurry includes the calcium ingredient which has a particle size of less than 25 microns.
7. The method of claim 5 wherein the particulate further includes a salt in flour form having a particle size of less than 90 microns.
8. The method of claim 7 wherein the food charge comprises 50 to 97% popcorn, 2 to 40% fat and 1 to 4% salt, sufficient amounts of the calcium ingredient to provide the food charge with a total calcium content of 360 to 3600 grams per 100 grams of unpopped popcorn.
9. The method of claim 8 wherein the fat includes at least 50% of the calcium ingredient in flour form having a mean particle size of less than 15 microns.
10. The method of claim 9 wherein at least a portion of the fat is supplied by a low moisture butter.

AMENDED SHEET

(SUBSTITUTE)

-31-

11. The method of claim 10 wherein the fat includes approximately 200 ppm of antioxidant.
12. The method of claim 11 wherein the particulate includes at least a portion of the salt in coarse form having a particle size of 250 to 600 microns.
13. The method of claim 11 wherein the food charge is free of a cheese ingredient.
14. The method of claim 13 wherein the fat or slurry has a spray temperature of between 70° to 130°F (21° to 54.5°C) and the fat is a material selected from the group consisting of low melting point fats, partially hydrogenated oils, fluid fats, and mixtures thereof.
15. The method of claim 14 wherein the food charge is free of added sugar(s).
16. The method of claim wherein the food charge contains sufficient amounts of the calcium ingredient to provide 360 to 1800 mg per 100 grams of unpopped popcorn.
17. The method of claim 16 wherein the calcium ingredient is selected from the group consisting of pure calcium carbonate, ground limestone, calcium phosphate salts, and mixtures thereof.
18. The method of claim 17 wherein at least a portion of the calcium ingredient is ground limestone.
19. The method of claim 15 wherein the popcorn quantity ranges from 59 to 79% and the fat quantity ranges from 20 to 40%.

AMENDED SHEET

(SUBSTITUTE)

-32-

20. A microwave popcorn article exhibiting desirable organoleptic attributes comprising:

a continuously sealed microwave popcorn bag,
and

5 a food charge disposed therein of popcorn and fat uniformly dispersed upon the popcorn, said charge comprising:

A. 50 to 98% of the product of unpopped popcorn kernels,

10 B. 2 to 40% of the product of an edible fat uniformly dispersed upon the popcorn kernels,

C. 1 to 4% of the product of salt at least 60% of which having a mean particle size of less than 25 microns, and

15 D. sufficient amounts of a calcium ingredient to provide a total calcium content of 360 to 3600 mg per 100 grams of unpopped popcorn.

21. The article of claim 20 wherein the calcium ingredient has a mean particle size of less than 25
20 microns.

22. The article of claim 21 wherein at least a portion of the calcium ingredient is supplied by a member selected from the group consisting of pure calcium carbonate, ground limestone, calcium phosphate
25 salts, and mixtures thereof.

23. The article of claim 22 wherein at least 60% of the salt is supplied by a flour salt having an average particle size of less than 50 microns.

24. The article of claim 23 wherein the food charge is
30 free of a cheese ingredient.

AMENDED SHEET

(SUBSTITUTE)

-33-

25. The article of claim 24 wherein the food charge is free of sugar.
26. The article of claim 25 wherein the edible fat is a material selected from the group consisting of low melting point fats, partially hydrogenated oils, fluid fats, and mixtures thereof.
27. The article of claim 26 wherein at least a portion of the calcium ingredient has a mean particle size of less than 15 microns.
28. The article of claim 26 wherein at least a portion of the calcium ingredient is pure calcium carbonate or ground limestone.
29. The article of claim 28 wherein at least a portion of the calcium ingredient is supplied by ground limestone.
30. The article of claim 29 having 70 to 85g popcorn.
31. The product prepared by the process of claim 1.
32. The product prepared by the process of claim 2.
33. The product prepared by the process of claim 3.
34. The product prepared by the process of claim 5, and wherein the popcorn has a kernel count of 40 to 80 per 10g.
35. In a microwave popcorn article comprising a sealed microwave popcorn bag and a food charge disposed within the bag comprising popcorn, fat and salt, the improvement comprising: fortifying the food charge with a calcium ingredient in amounts sufficient to provide 360 to 3600 mg per 100 grams of unpopped popcorn, and

AMENDED SHEET

1 message digest;
digitally signing by the merchant device, the merchant message digest using the merchant's
private key to form a merchant digitally signed message;
combining by the merchant, the EC-merchant combination message with the merchant
5 digitally signed message to form a merchant key exchange request message from the merchant;
and
sending the merchant key exchange request message from the merchant to a service provider
through a network.

10 36. A key exchange request message comprising:
electronic card plain text;
electronic card cryptogram, encrypted with a service provider public key, comprising an
electronic card random number, an electronic card public key, and electronic card sensitive
transaction data;
15 an electronic card digital signature of the electronic card plain text and the electronic card
cryptogram;
merchant plain text;
merchant cryptogram, encrypted with the service provider public key, of a merchant random
number, a merchant public key, and merchant sensitive transaction data; and
20 a merchant digital signature of the merchant plain text and the merchant cryptogram.

37. A key exchange response message comprising:
service provider (SP) plain text for the electronic card (EC);
SP transaction identification number for the EC;
25 SP cryptogram for the EC, encrypted with the EC public key, of the EC random number, an
SP random number for the EC, a session key, and SP sensitive transaction data for the EC;
an SP digital signature of the SP plain text for the EC, the SP transaction identification
number for the EC; and the SP cryptogram for the EC;
SP plain text for the merchant;
30 SP transaction identification number for the merchant;
SP cryptogram for the merchant encrypted with the merchant public key, of the merchant
random number, an SP random number for the merchant, a session key, and SP sensitive
transaction data for the merchant; and
an SP digital signature of the SP plain text for the merchant, the SP transaction identification
35 number for the merchant; and the SP cryptogram for the merchant.

38. A method of conducting an electronic transaction among multiple parties arranged in
series comprising the steps of:

1 sending a key exchange request message from an electronic card to a first party where the first party is a message router or participant;

sending the key exchange request message from the first party to a next party if the first party is a router;

5 combining a first party's key exchange request message with the electronic card's key exchange request message and sending the combined key exchange request message to a next party if the first party is a participant;

sending the key exchange request message to a next party if the current party is a message router;

10 combining a current party's key exchange request message with a last party's key exchange request message and sending the combined key exchange request message to a next party, if the current party is a participant;

formatting, by the service provider, into one message, a key exchange response for each participant and sending the message in reverse order of the path for sending the key exchange request message to the service provider; and

15 separating, by every participant, the key exchange response for itself from the key exchange responses for the other participants, and forwarding the remaining key exchange responses to the other participants in reverse order of the path for sending the key exchange request message to the service provider, until the electronic card receives its key exchange response.

20 39. A method of conducting an electronic transaction among multiple parties arranged in series comprising the steps of:

sending a transaction request message from an electronic card to a first party where the first party is a message router or participant;

25 sending the transaction request message from the first party to a next party if the first party is a router;

combining a first party's transaction request message with the electronic card's transaction request message and sending the combined transaction request message to a next party if the first party is a participant;

30 sending the transaction request message to a next party if the current party is a message router;

combining a current party's transaction request message with a last party's transaction request message and sending the combined transaction request message to a next party, if the current party is a participant;

35 formatting, by the service provider, into one message, a transaction response for each participant and sending the message in reverse order of the path for sending the transaction request message to the service provider; and

separating, by every participant, the transaction response for itself from the transaction

1 responses for the other participants, and forwarding the remaining transaction responses to the other participants in reverse order of the path for sending the transaction request message to the service provider, until the electronic card receives its transaction response.

5 ~~40. A method of conducting an electronic transaction among multiple parties arranged in a hierarchical organization comprising the steps of:~~

sending a key exchange request message from an electronic card to a first party where the first party is a message router or participant;

10 sending the key exchange request message to a next party $X_{j,k}$ ($j = 2, 3, 4, \dots; k = 1, 2, 3, \dots, m$; m is a variable of type n ; $n = 1, 2, 3, \dots$; m can be different values for different values of j) if the first party is a message router;

combining a first party's key exchange request message with the electronic card's key exchange request message and sending the combined key exchange request message to a next party $X_{j,k}$ if the first party is a participant;

15 sending the key exchange request message to the next party $X_{j,k}$ if a current party $X_{j,k}$ is a message router;

combining a current party $X_{j,k}$'s key exchange request message with the last party's key exchange request message and sending the combined key exchange request message to the next party $X_{j,k}$ if the current party $X_{j,k}$ is a participant;

20 formatting, by the service provider, into one message, a key exchange response for each participant and sending the message in reverse order of the path for sending the key exchange request message to the service provider; and

25 separating, by every participant, the key exchange response for itself from the key exchange responses for the other participants, and forwarding the remaining key exchange responses to the other participants in reverse order of the path for sending the key exchange request message to the service provider, until the electronic card receives its key exchange response.

41. A method of conducting an electronic transaction among multiple parties arranged in a hierarchical organization comprising the steps of:

30 sending a transaction request message from an electronic card to a first party where the first party is a message router or participant;

sending the transaction request message to a next party $X_{j,k}$ ($j = 2, 3, 4, \dots; k = 1, 2, 3, \dots, m$; m is a variable of type n ; $n = 1, 2, 3, \dots$; m can be different values for different values of j) if the first party is a message router;

35 combining a first party's transaction request message with the electronic card's transaction request message and sending the combined transaction request message to a next party $X_{j,k}$ if the first party is a participant;

~~sending the transaction request message to the next party $X_{j,k}$ if a current party $X_{j,k}$ is a~~

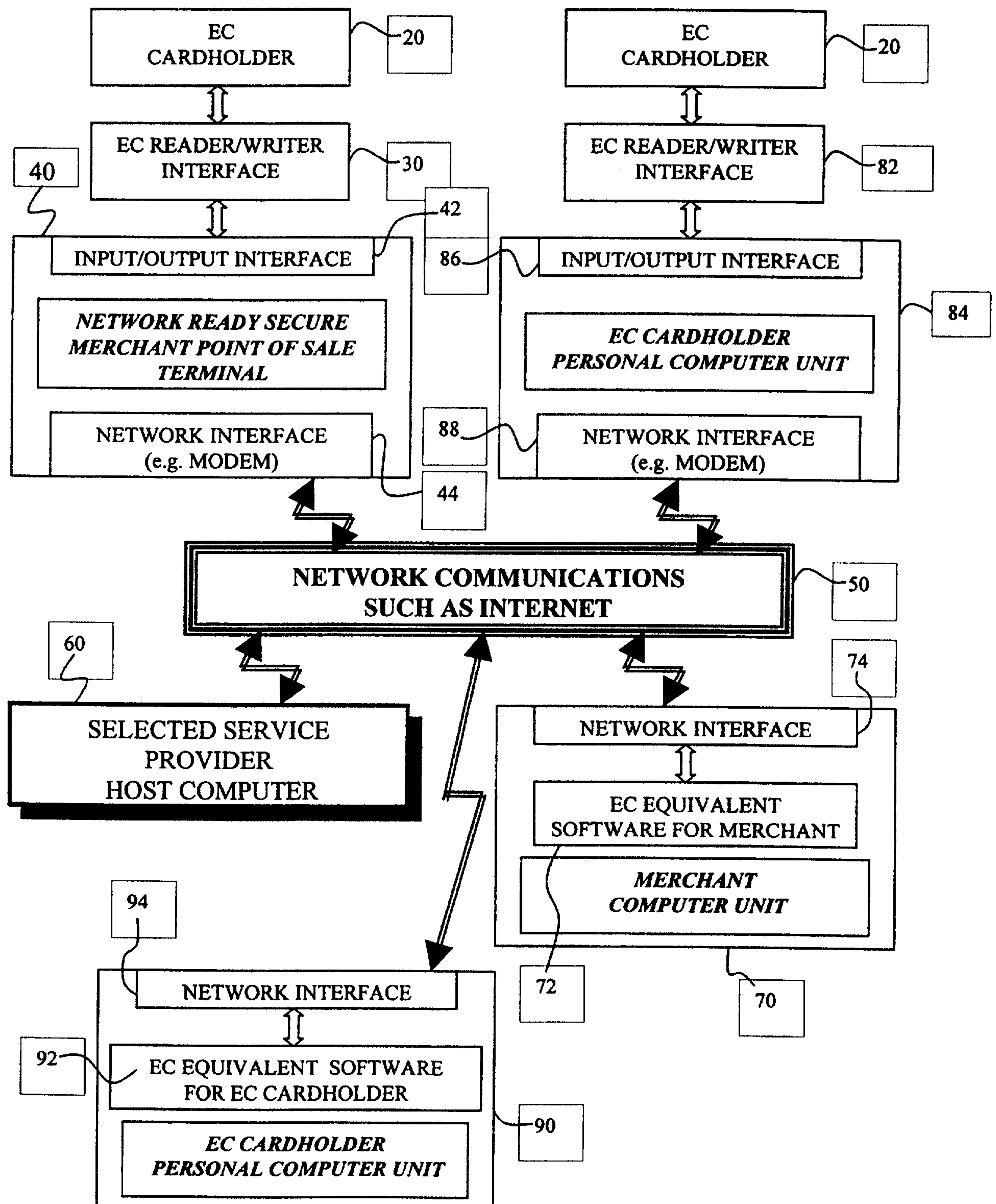
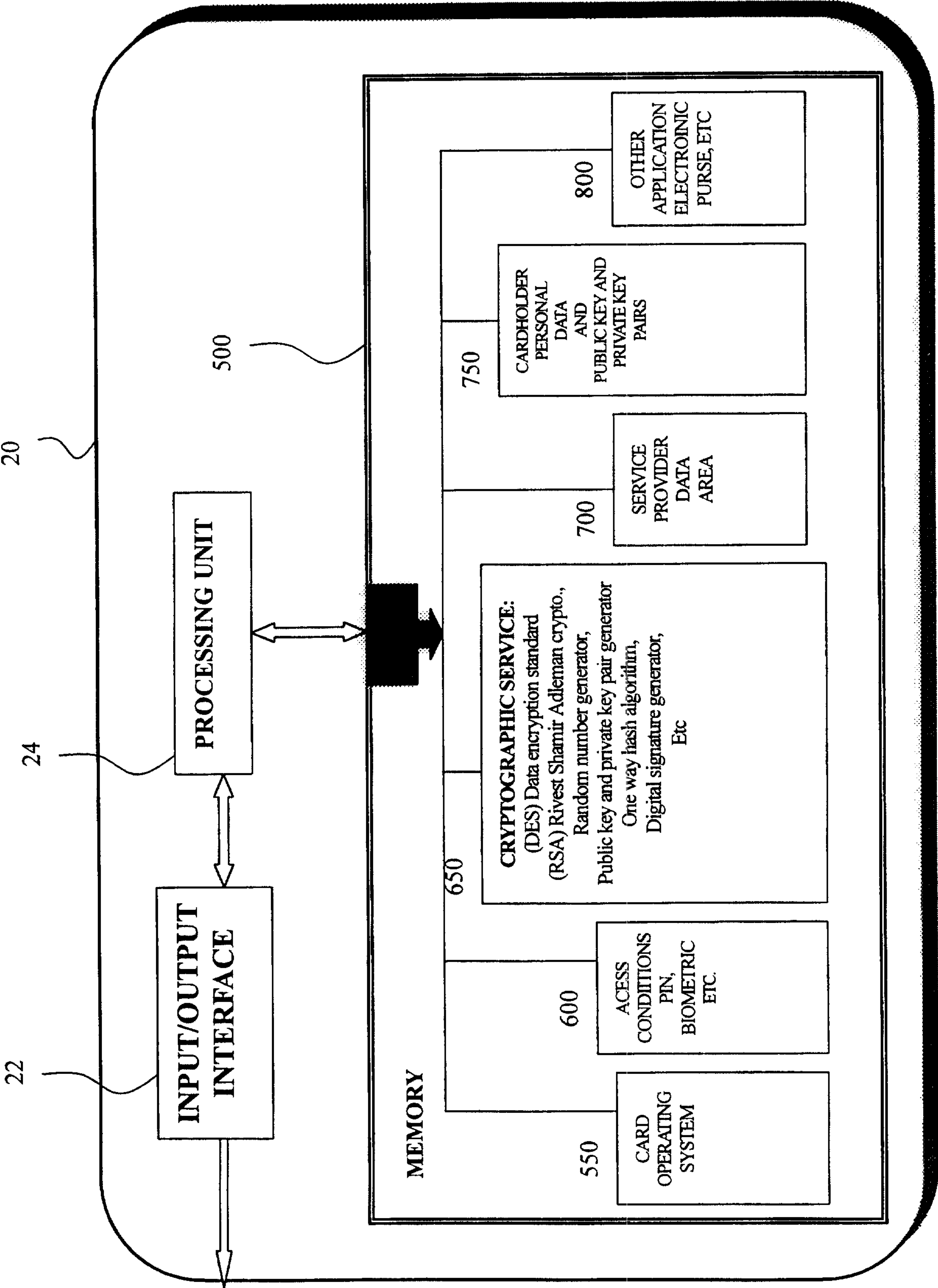
FIG. 1

FIG. 3



ELECTRONIC CARD

FIG. 4

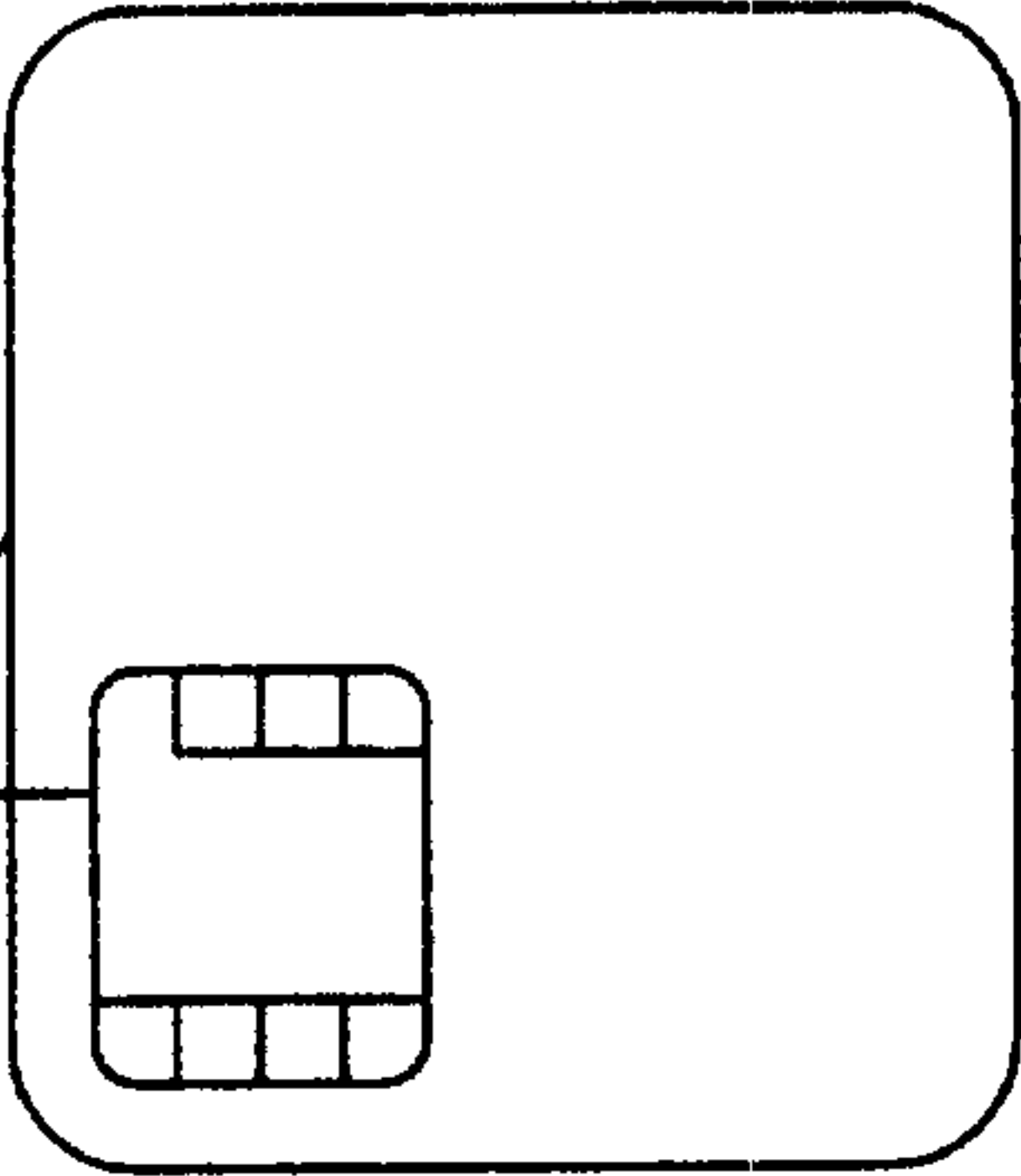
700

↳

SERVICE PROVIDERS' DATA AREA (SPDA)						
702	704	706	708	710	712	714 ←
NAME	KEY TYPE	KEY VALUE	ACCOUNT INFORMATION (Number, expiration date, etc.)	CARD TYPE	PIN (optional)	Miscellaneous Data
				CREDIT CARD		
				DEBIT CARD		
				ATM CARD		
				MEMBER CARD		
				LOYALTY CARD		
				etc.		

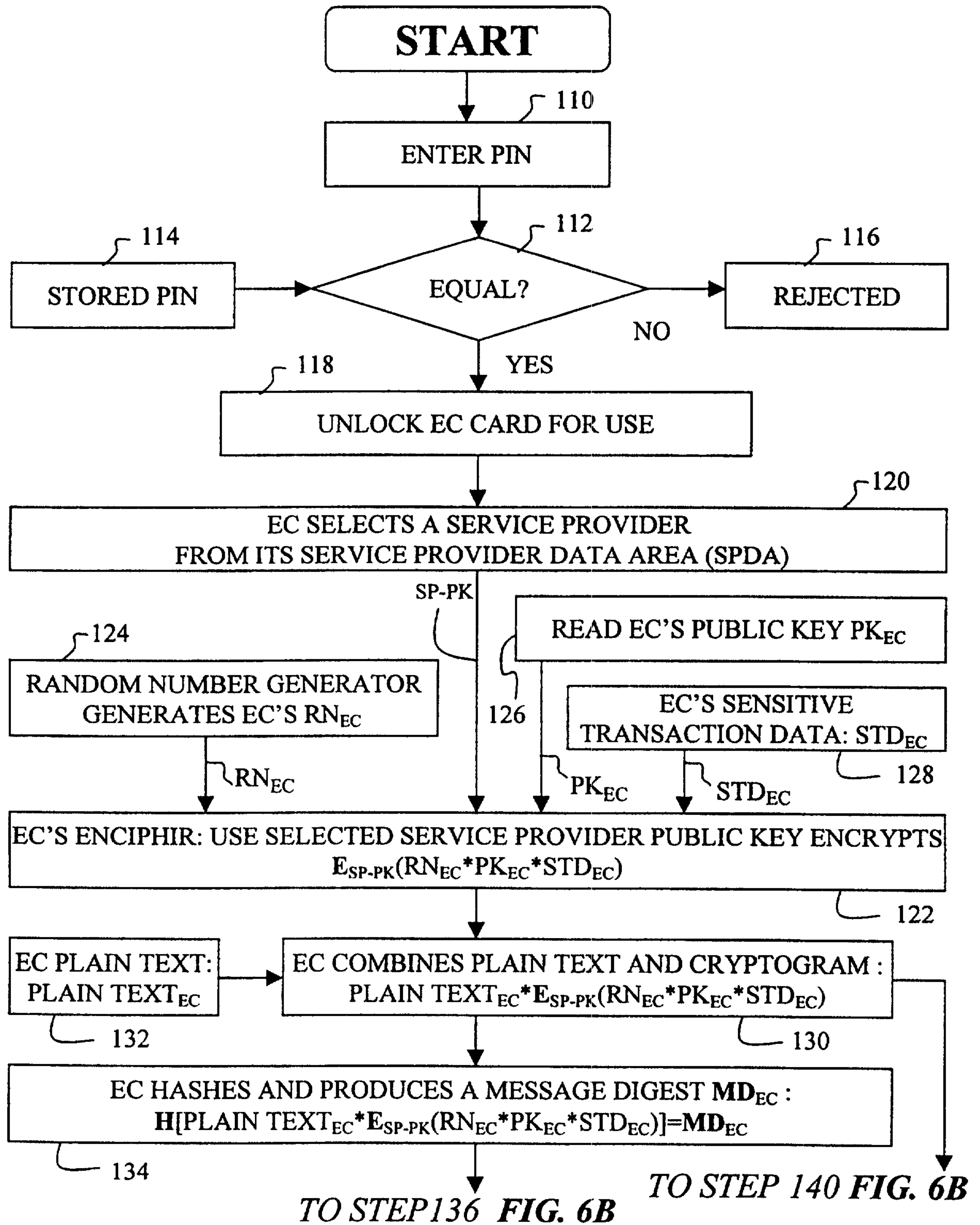
20

↳



ELECTRONIC CARD

6/29

FIG. 6A

8/29

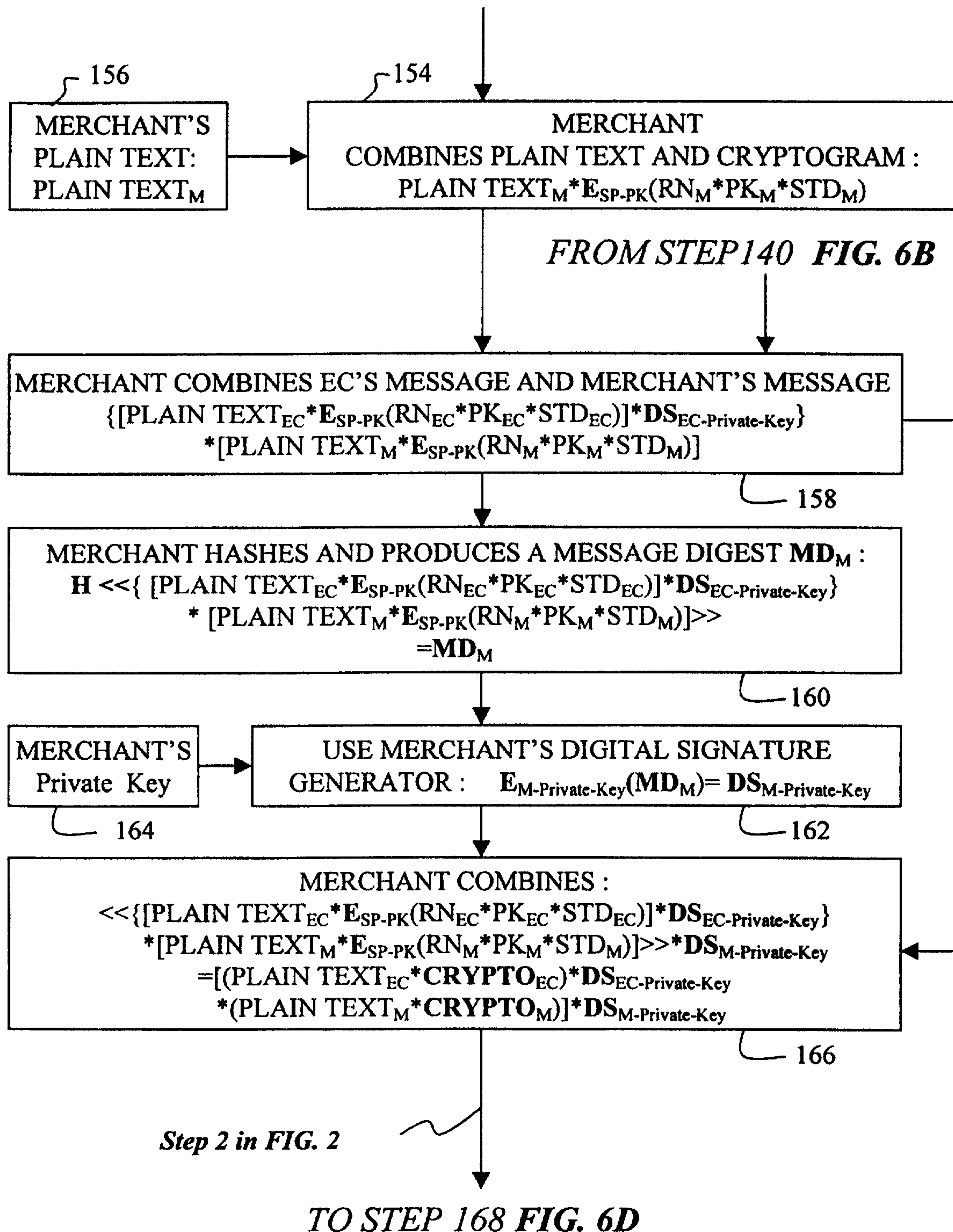
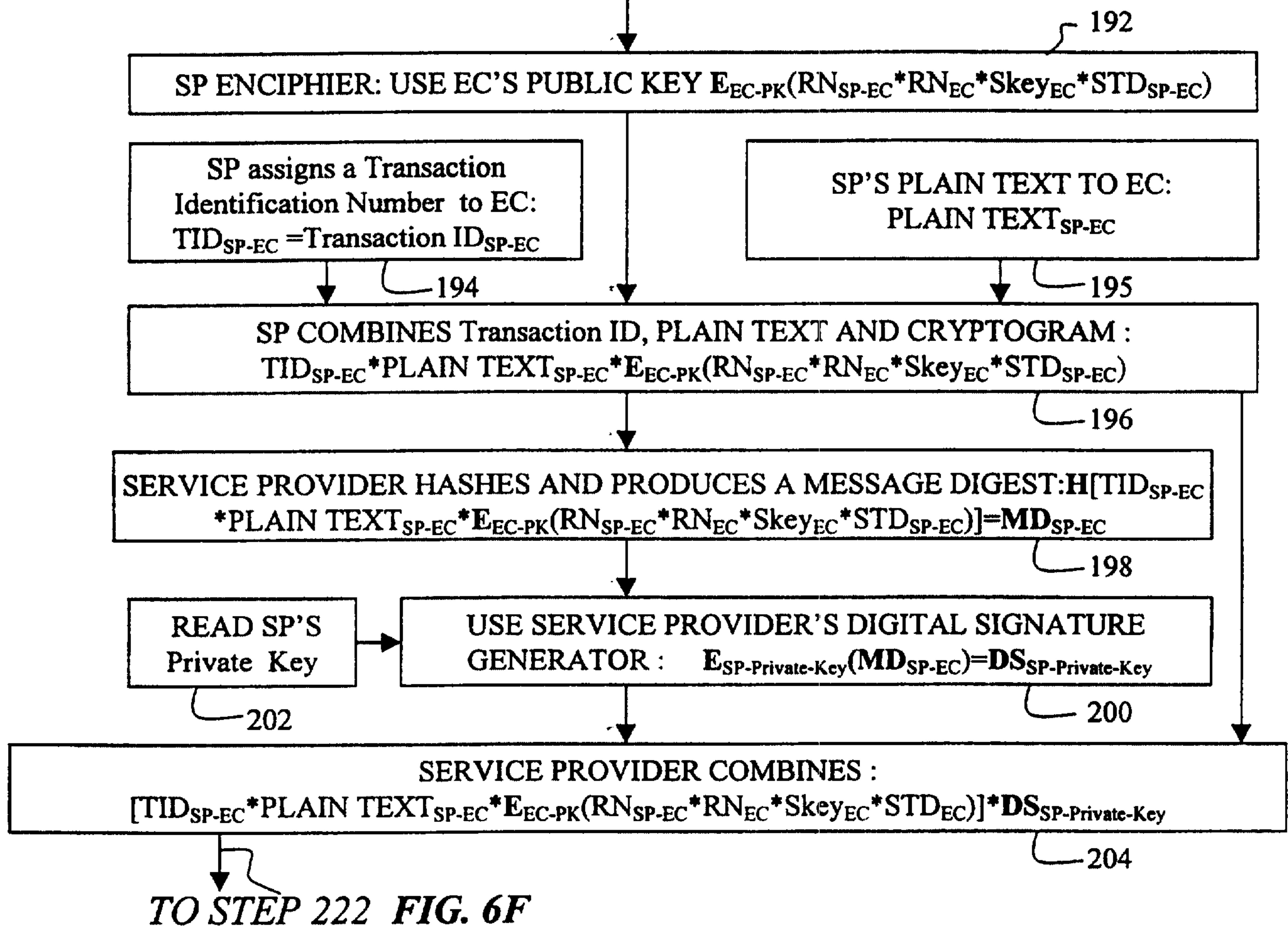
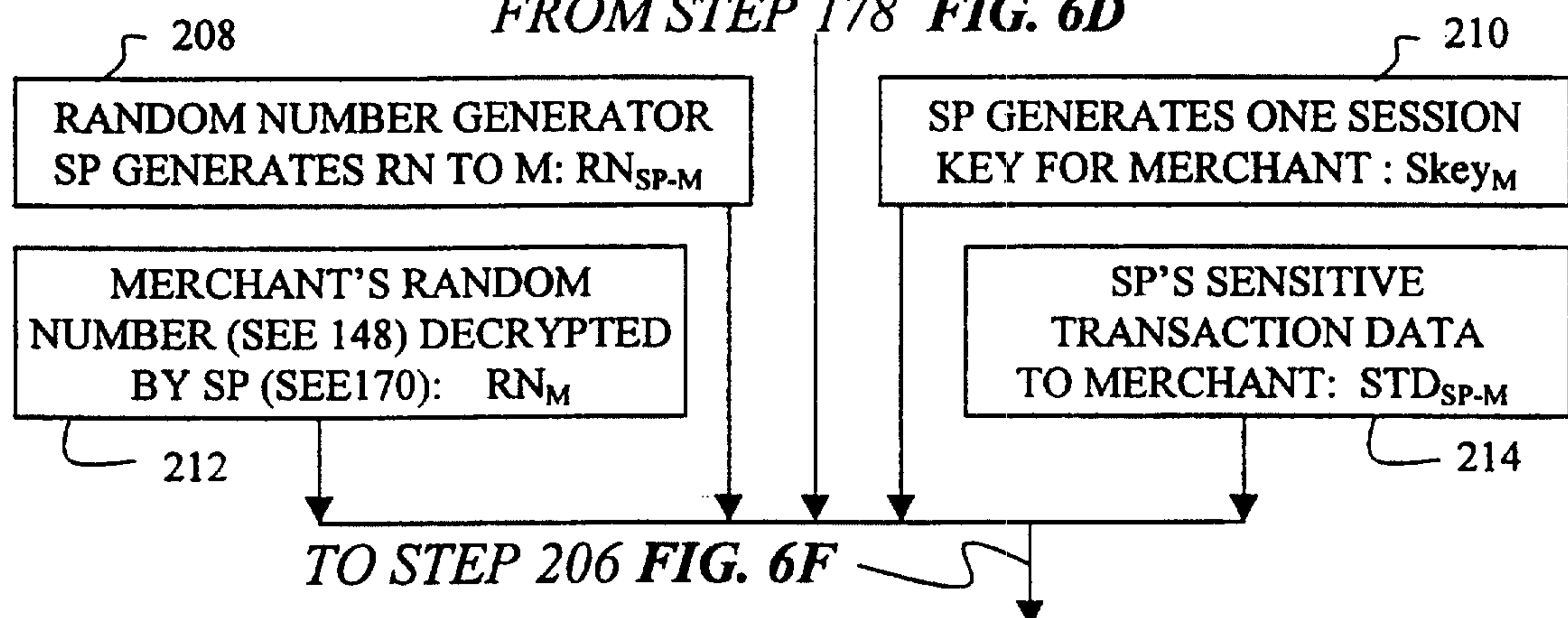
FIG. 6C**FROM STEP 146 FIG. 6B**

FIG. 6E**FROM STEPS 184, 186, 188, 190 FIG. 6D****FROM STEP 178 FIG. 6D**

11/29

FIG. 6F
 FROM STEPS 208, 210, 212, 214 FIG 6E

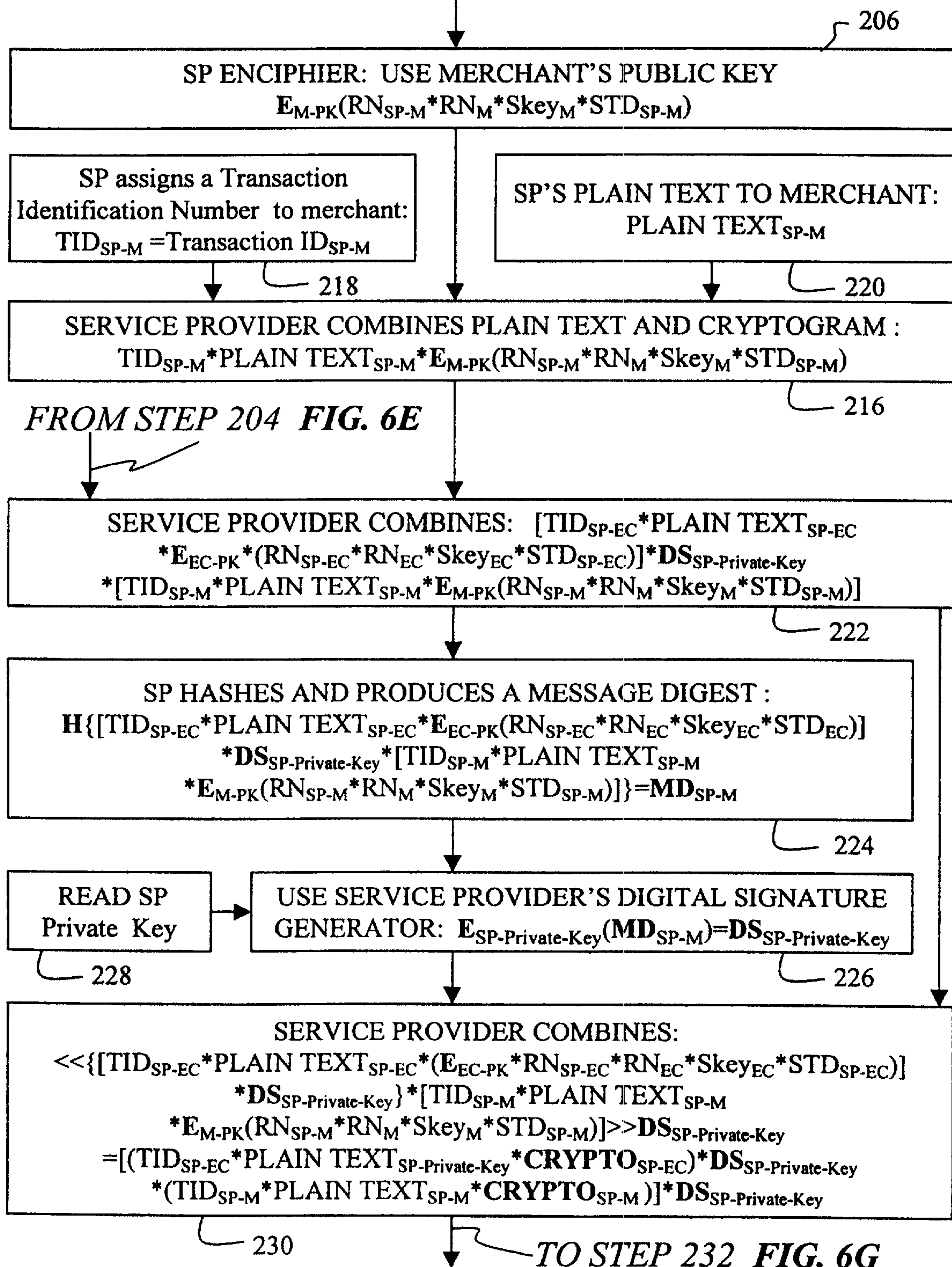
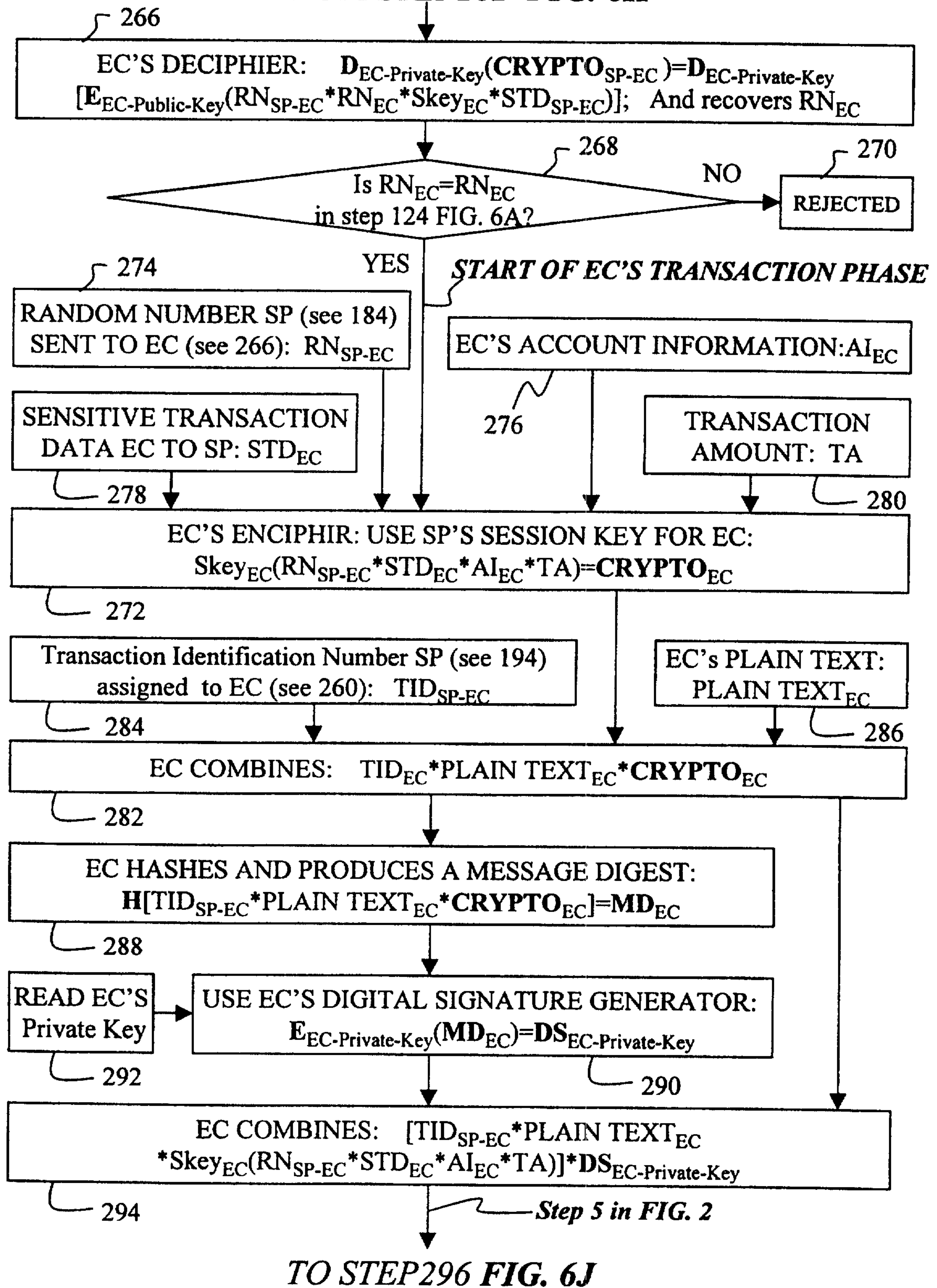
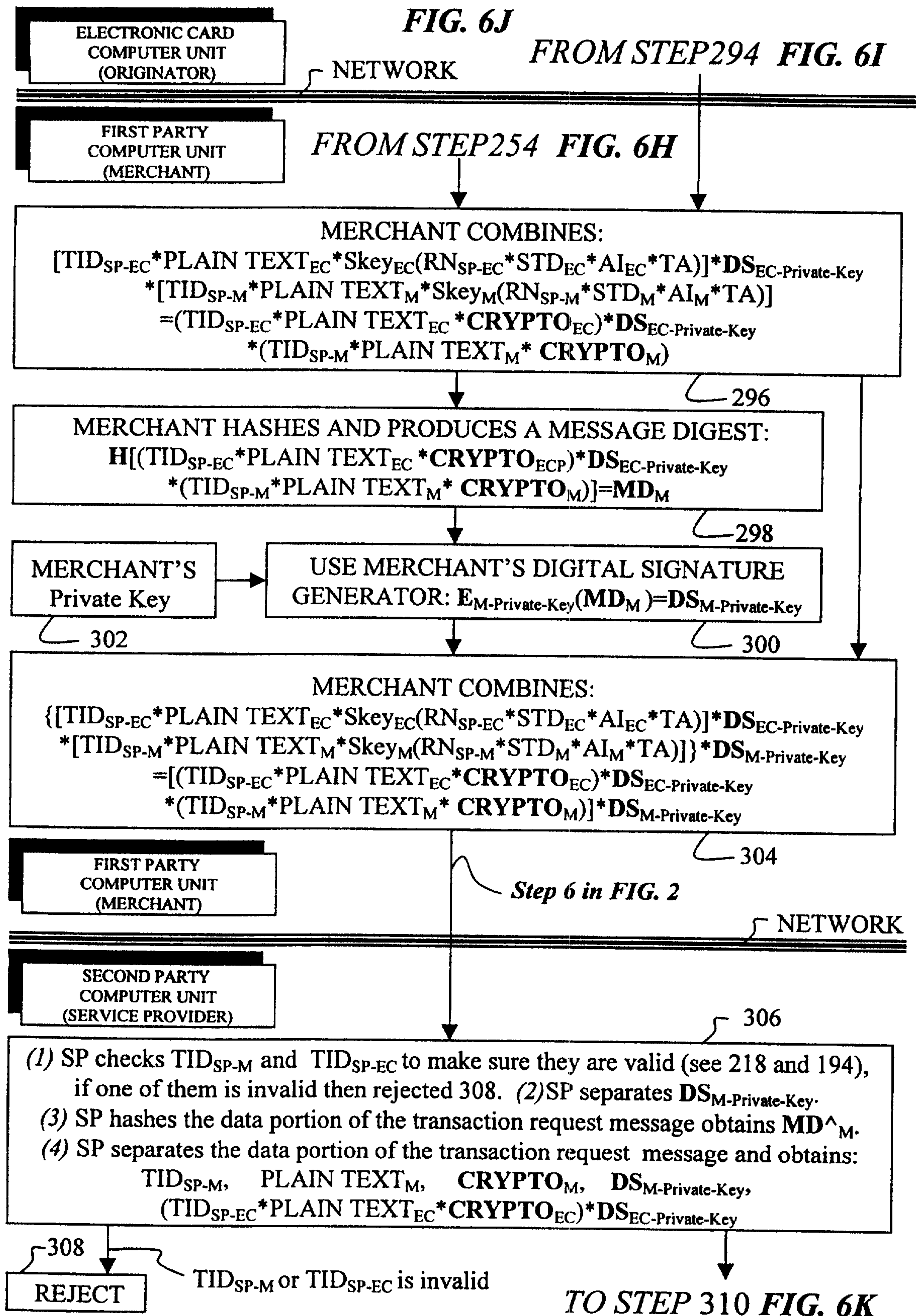
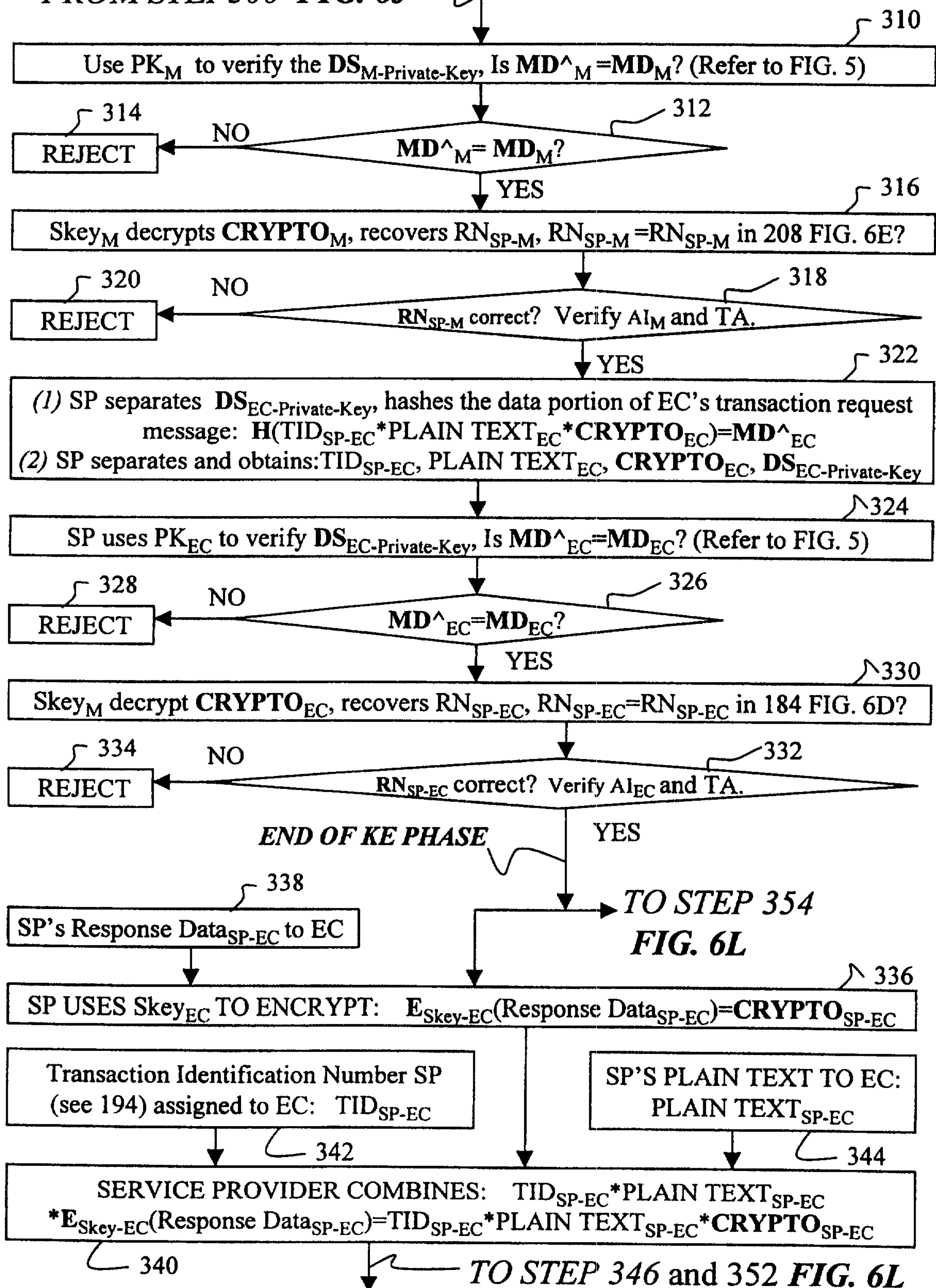


FIG. 6I
FROM STEP 262 FIG. 6H





16/29

FIG. 6K**FROM STEP 306 FIG. 6J**

17/29

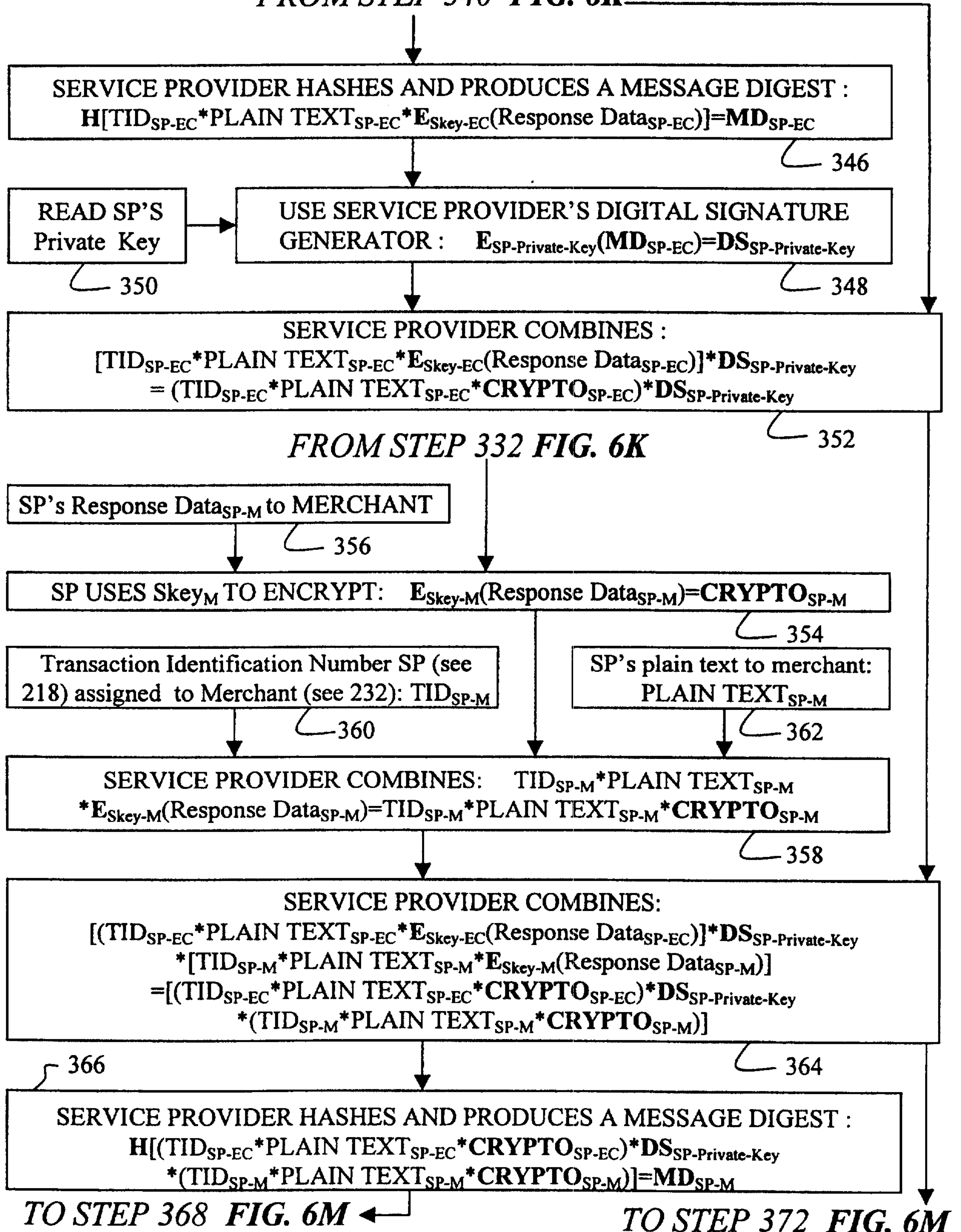
FIG. 6L**FROM STEP 340 FIG. 6K**

FIG. 60

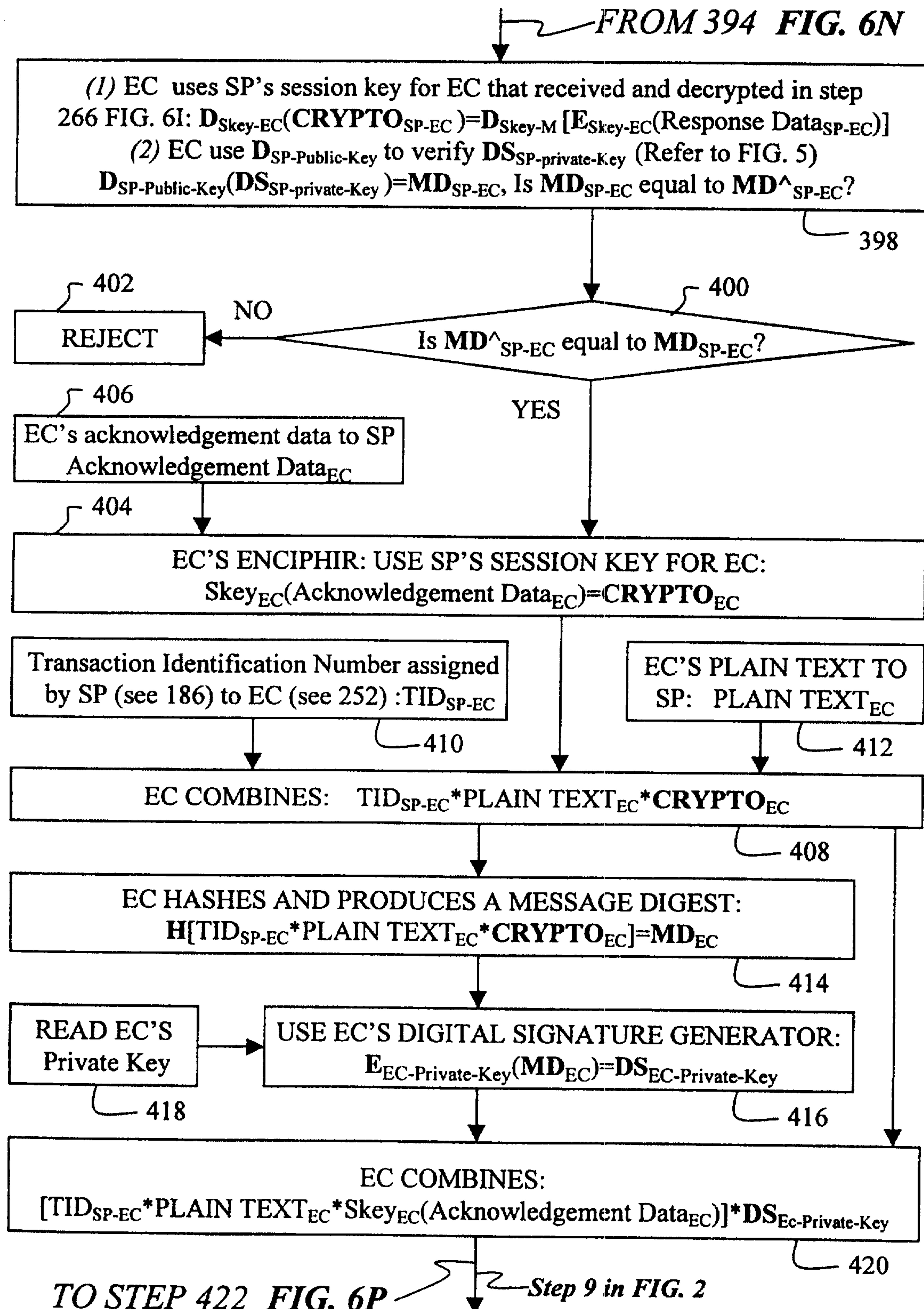


FIG. 6Q

FROM STEP 430 FIG. 6P

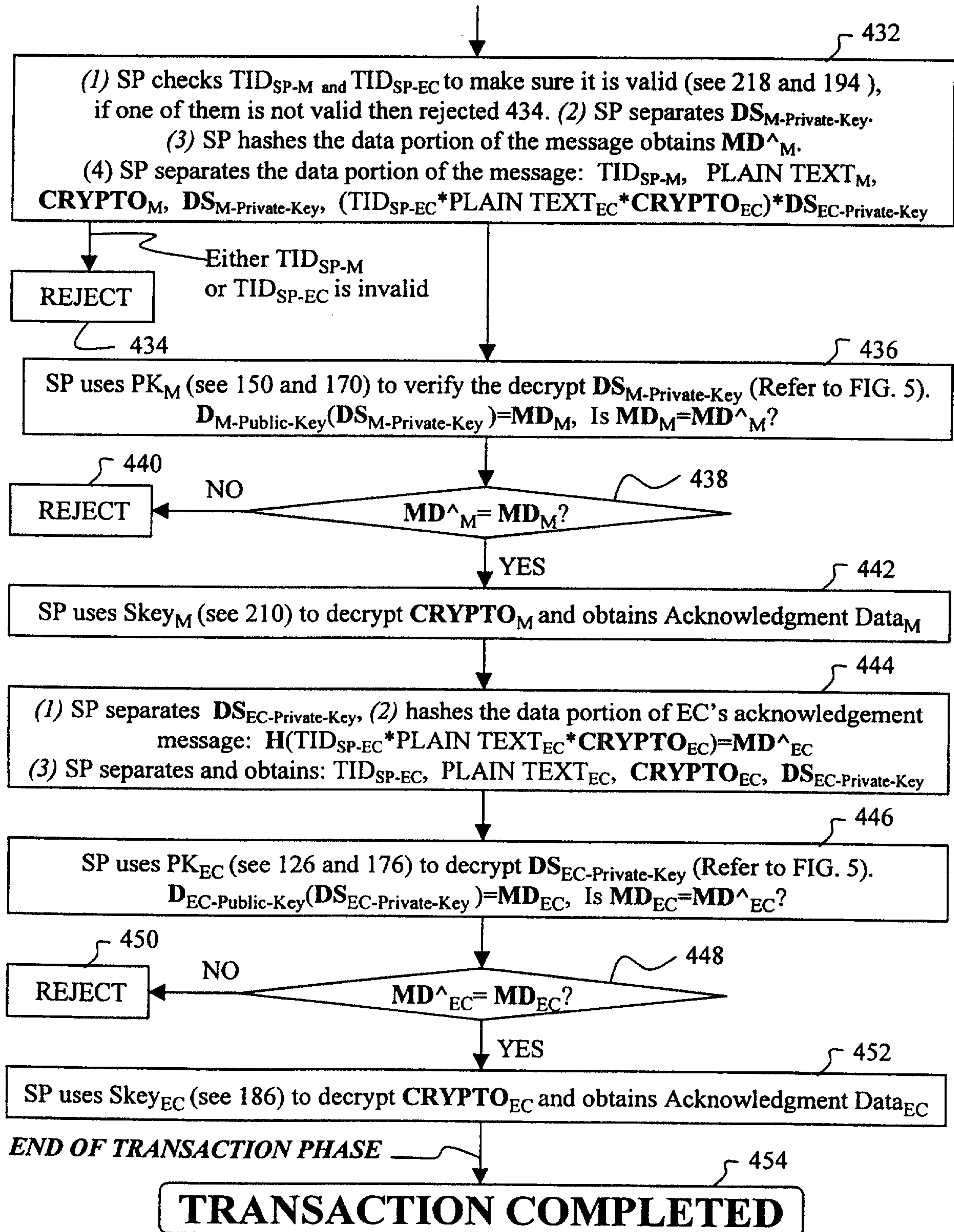


FIG. 7

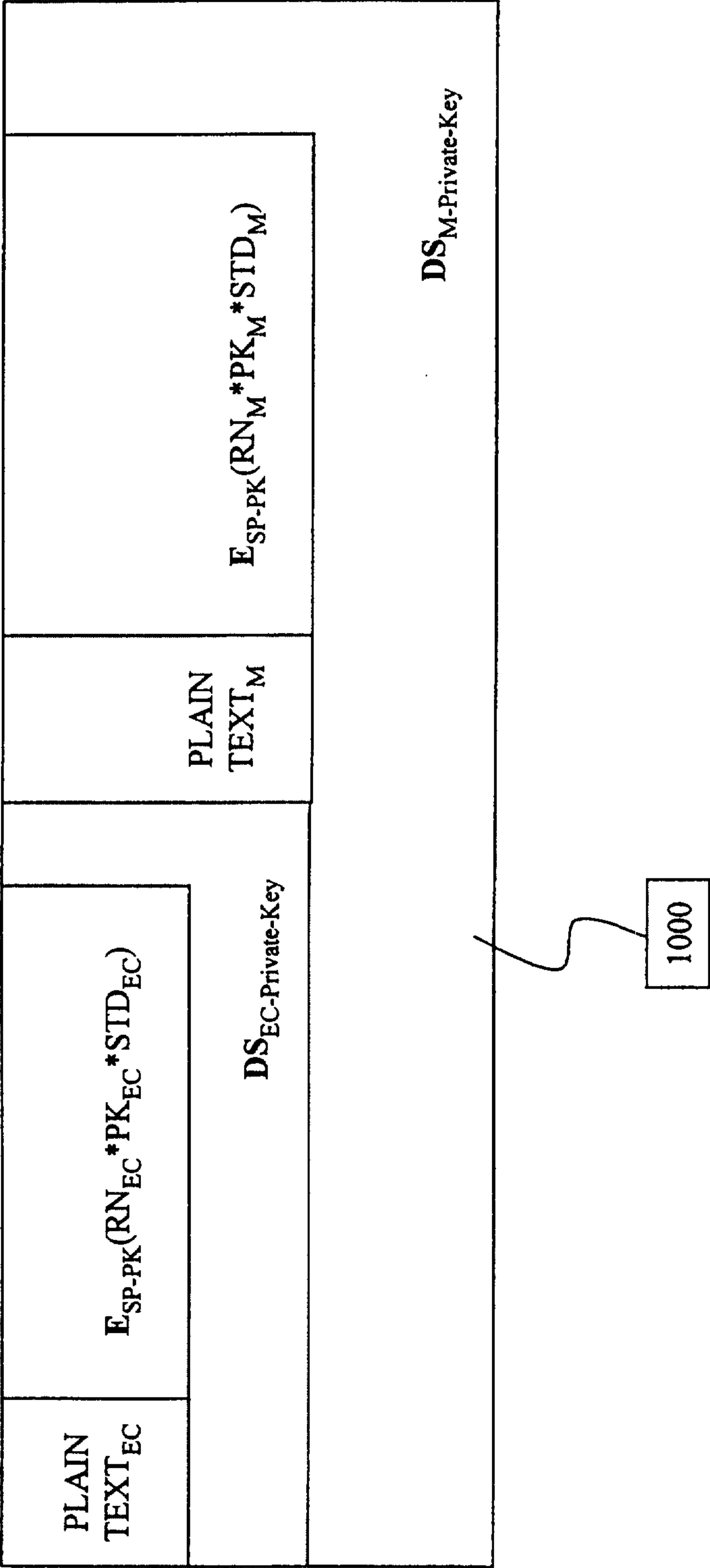


FIG.8

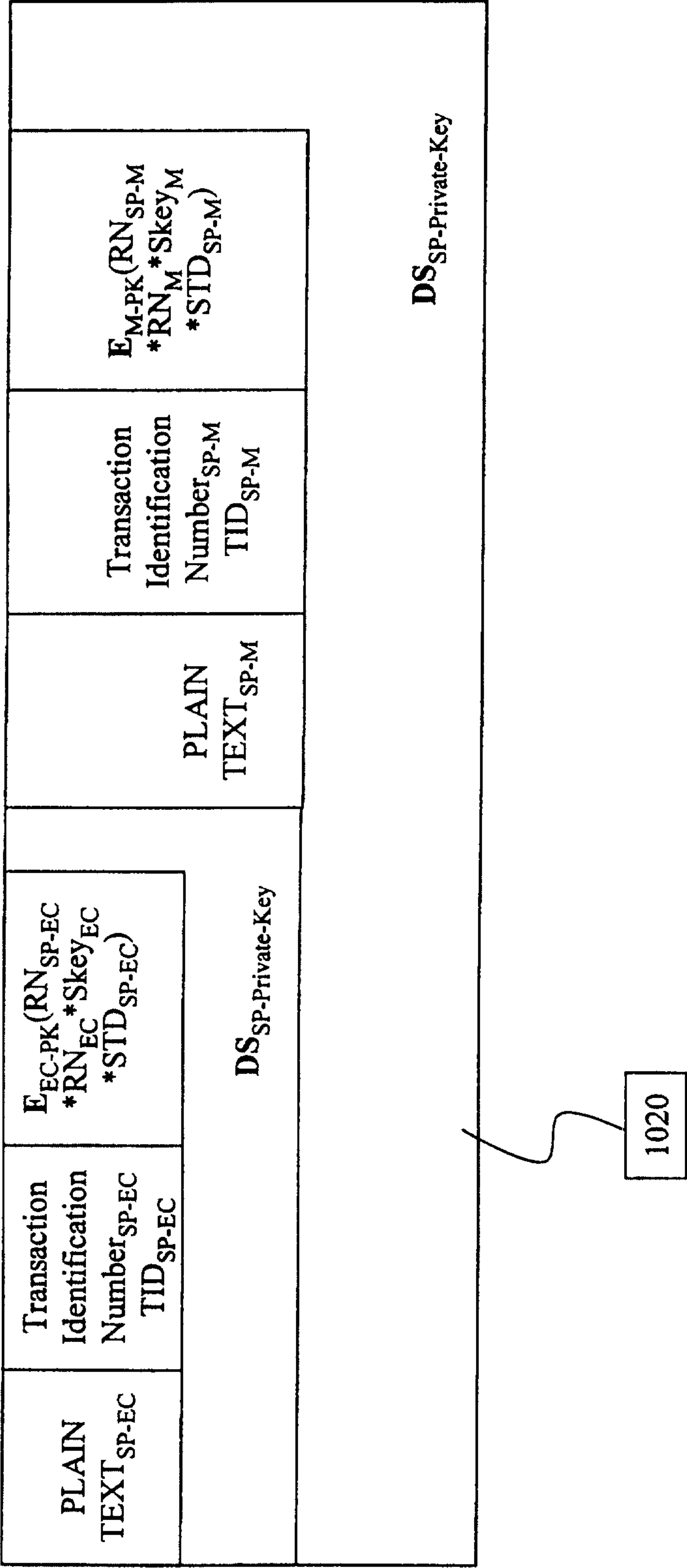


FIG. 9

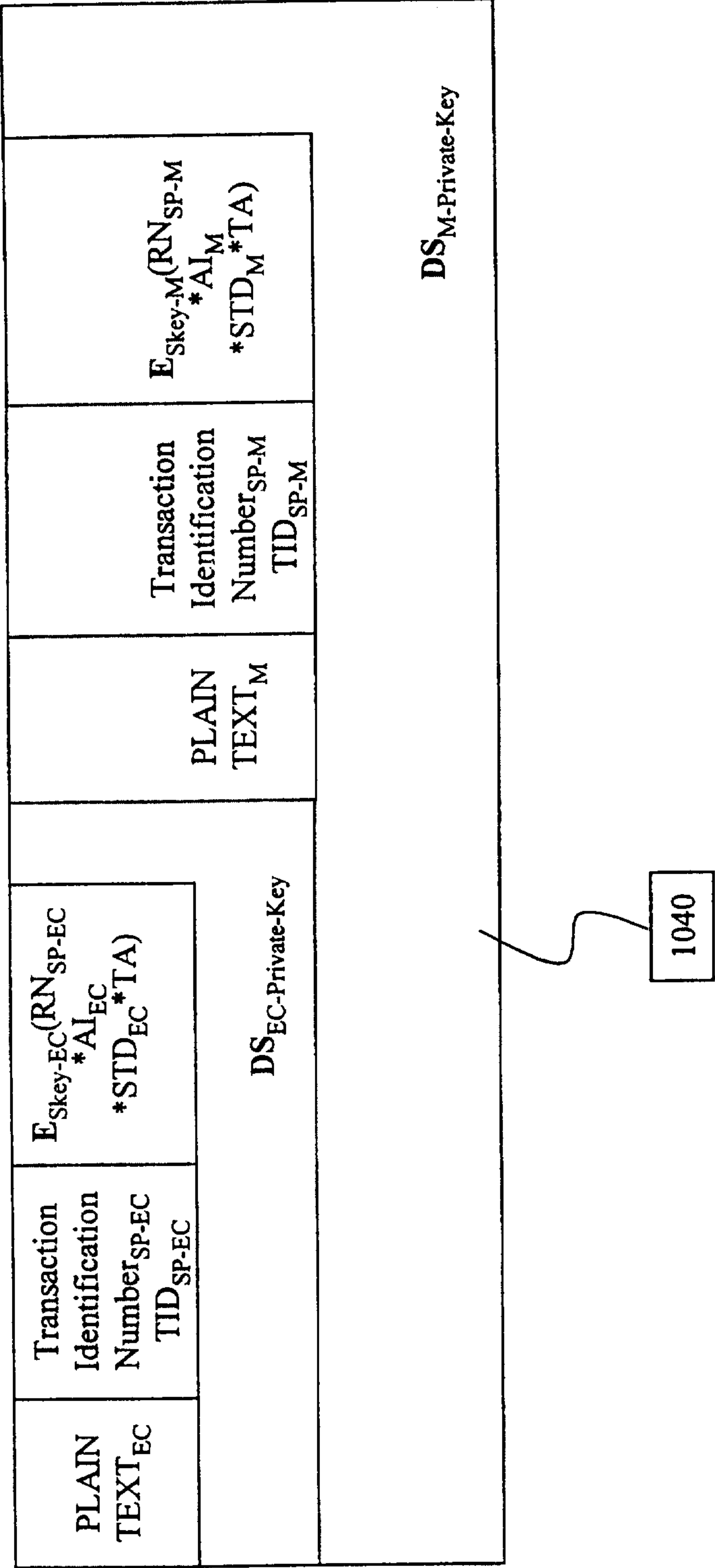


FIG.10

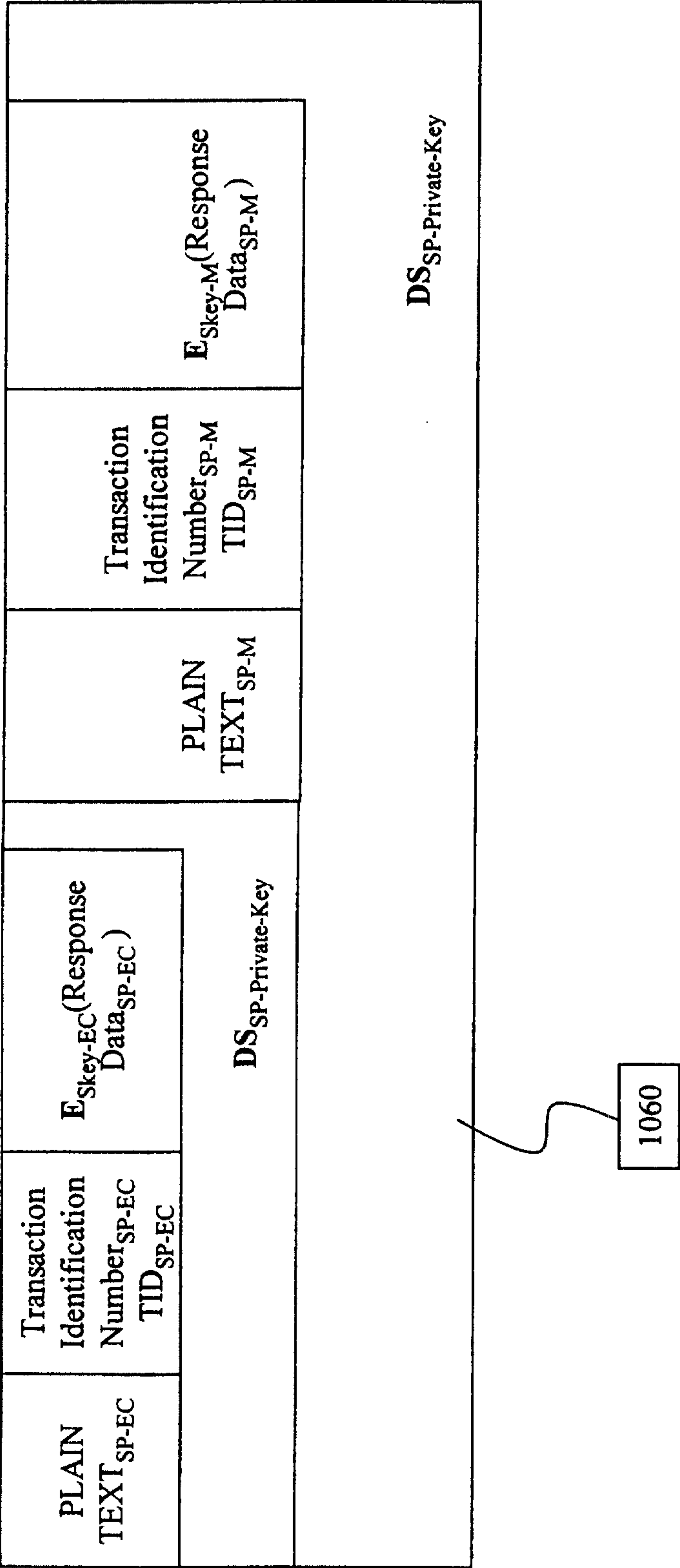


FIG.11

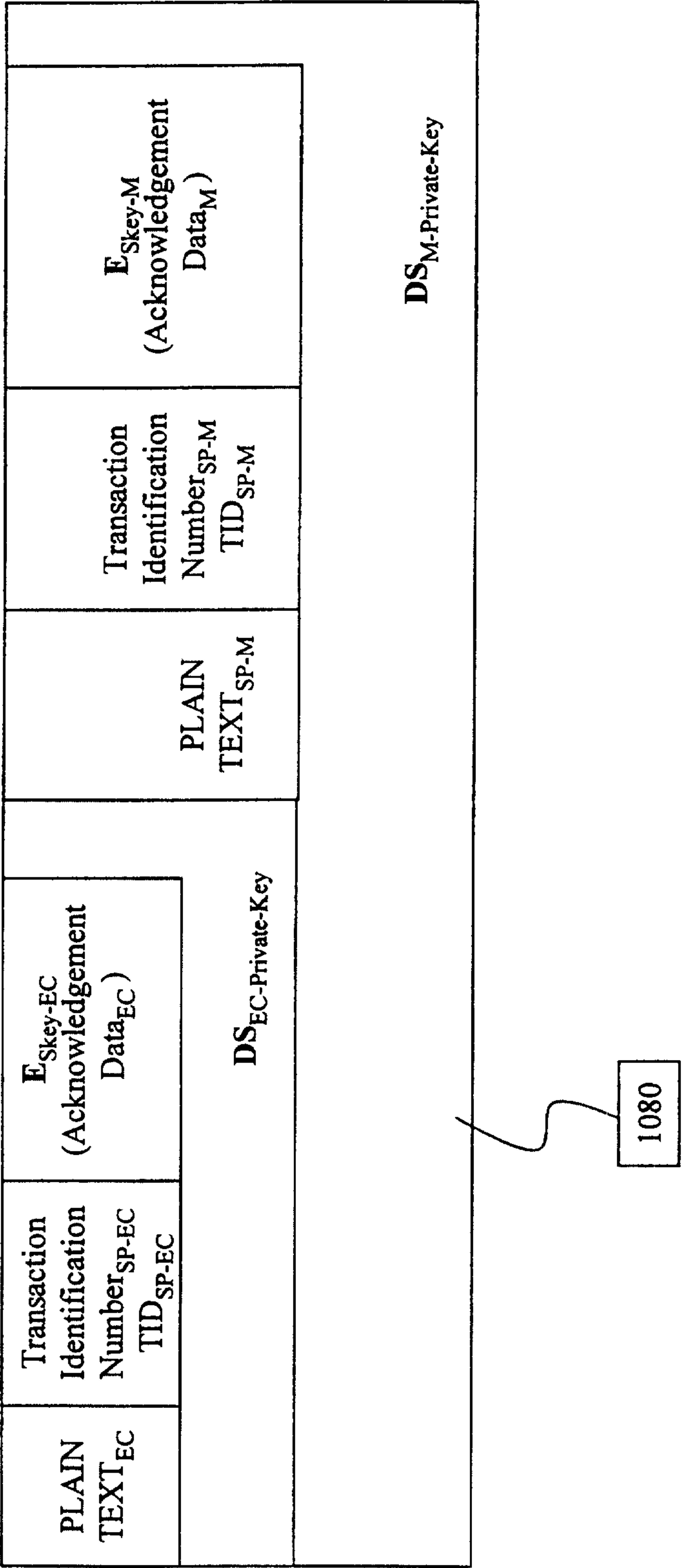
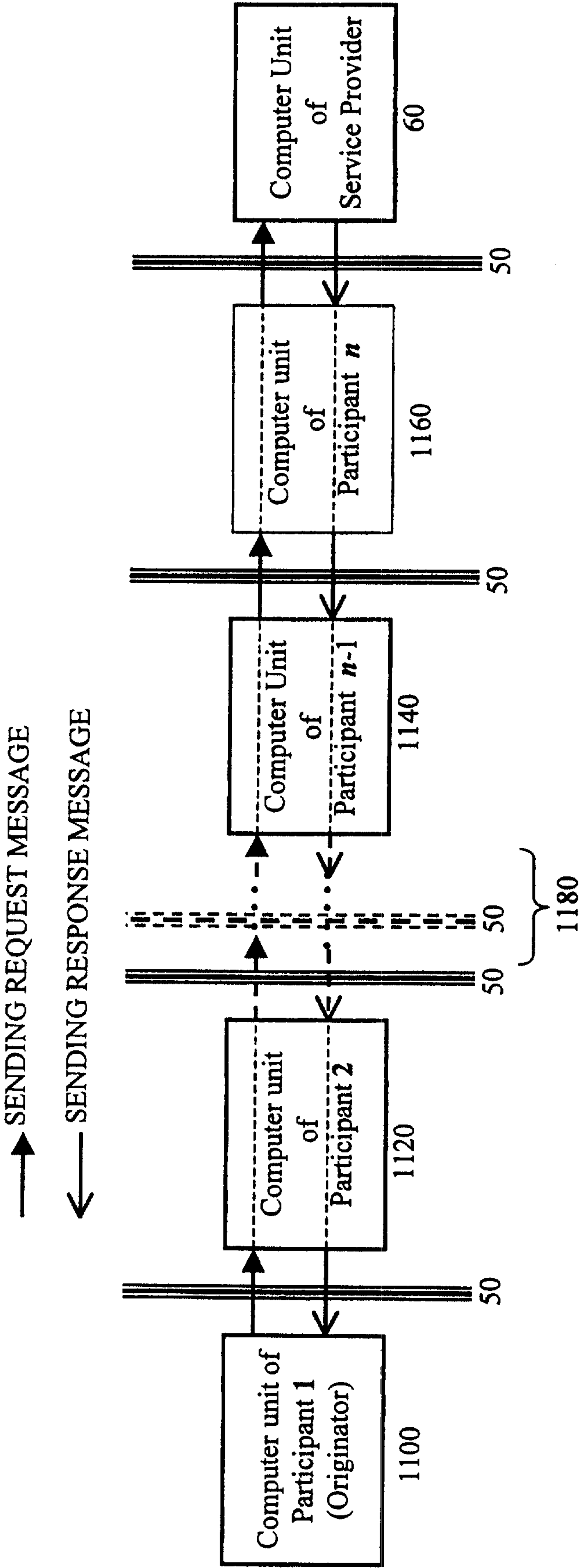
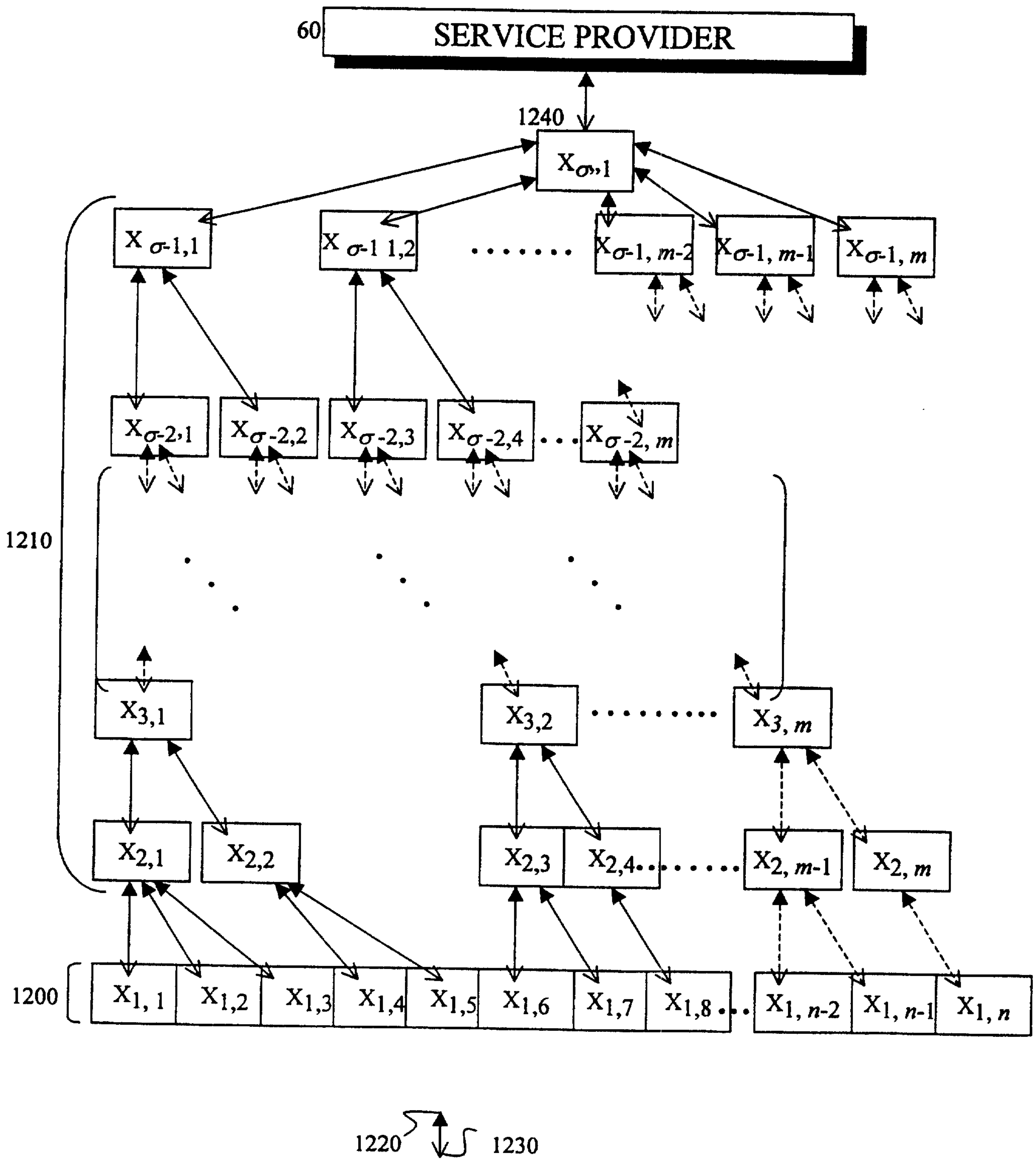


FIG. 12



29/29

FIG. 13

UNSCANNABLE ITEM

RECEIVED WITH THIS APPLICATION

(ITEM ON THE 10TH FLOOR ZONE 5 IN THE FILE PREPARATION SECTION)

DOCUMENT REÇU AVEC CETTE DEMANDE

NE POUVANT ÊTRE BALAYÉ

(DOCUMENT AU 10 IÈME ÉTAGE AIRE 5 DANS LA SECTION DE LA
PRÉPARATION DES DOSSIERS)

