PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G07F 7/08, 19/00

A2

(11) International Publication Number: **WO 98/59324**

(43) International Publication Date: 30 December 1998 (30.12.98)

(21) International Application Number: PCT/IB98/01131

(22) International Filing Date: 23 June 1998 (23.06.98)

(30) Priority Data:
08/876,356 25 June 1997 (25.06.97) US

(71) Applicant: SCHLUMBERGER INDUSTRIES, S.A. [FR/FR]; 50, avenue Jean-Jaurès, F-92120 Montrouge (FR).

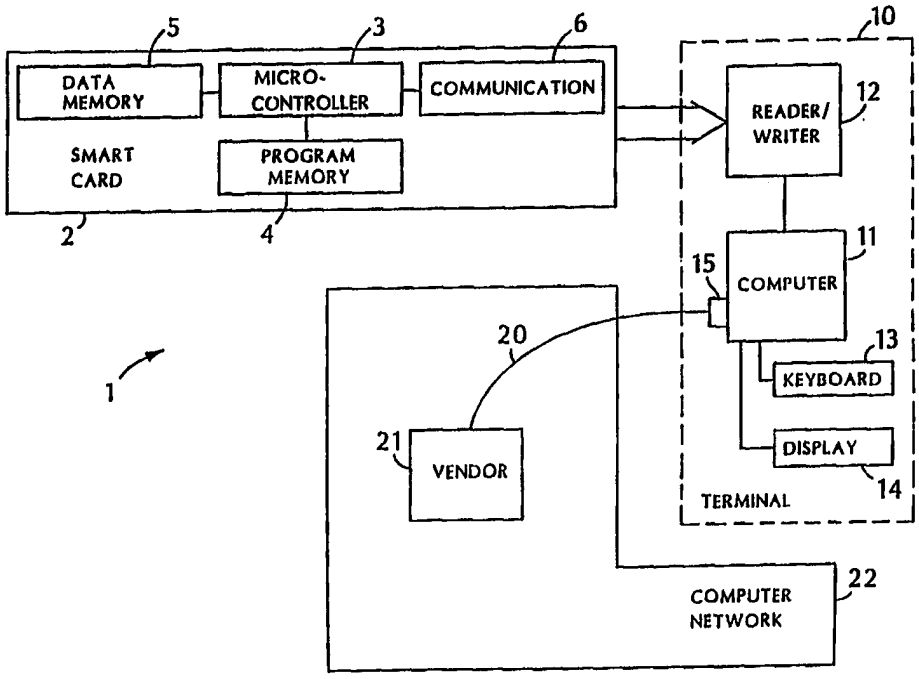
(72) Inventor: GUTHERY, Scott, B.; 19 Foster Road, Belmont, MA 02178-3736 (US).

(74) Agent: AKERS, Noel, J.; Frohwitter Patent- und Rechtsanwälte, Possartstrasse 20, D-81679 München (DE).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, GW, HU, ID, IL, 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, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, 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, ML, MR, NE, SN, TD, TG).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: PERFORMING FIXED-VALUE TRANSACTIONS WITH A SMART CARD



(57) Abstract

A smart card for use with a system capable of receiving a transaction message includes a memory storing a program and data representative of one or more fixed-value units and a microcontroller configured by the program to furnish the transaction and modify the data to reduce the number of fixed-value units by a predetermined amount when the transaction is furnished. A method of performing fixed-value transactions using the smart card is also disclosed.

FOR THE PURPOSES OF INFORMATION ONLY

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

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

PERFORMING FIXED-VALUE TRANSACTIONS WITH A SMART CARD

Background of the Invention

The invention relates generally to performing fixed-value transactions with a smart card.

Smart cards, also known as microprocessor cards or chip-cards, are plastic cards approximately the size of a credit card embedded with an integrated circuit (IC) chip. The chip stores information while protecting it from unauthorized access.

During the past several years, smart cards have become more attractive as the price of micro-computing power and storage have continued to drop. Furthermore, it has been recognized that the use of smart cards can help reduce the high overhead costs associated with transactions involving cash or credit cards. Stored-value cards, for example, lessen transaction costs by carrying monetary value directly instead of acting only as a pointer to an account.

Some smart cards, such as telephone-cards, are designed to allow the purchase of products or services from a specific vendor and are used directly with the vendor's equipment. Such smart cards provide a desirable marketing technique for the vendor and a convenient way for the consumer to gain access to the vendor's products or services.

Summary of the Invention

In general, in one aspect, the invention features a method of performing a fixed-value transaction using a smart card having stored therein initialization data including a count representing a specified number of fixed-value units. The method includes generating a transaction message in the smart card and transmitting the transaction message to a

vendor computer system. The method further includes reducing the count stored in the smart card by a predetermined amount.

Various implementations of the invention include one or more of the following features. The transaction message can be transmitted over a computer network. Also, the initialization data can further include a predetermined number of fixed-value units required for each smart card transaction, and the method can include reducing the count stored in the smart card by the predetermined number of fixed-value units. The method can include incrementing in the smart card a count indicative of a total number of transactions generated by the smart card.

The initialization data can further include an encryption key, and the transaction message can be encrypted with the encryption key. The method can also include receiving the transaction message in the vendor computer system and decrypting the transaction message with a decryption key.

The transaction message can include a transaction identifier indicative of goods or services associated with the transaction. The smart card can generate the transaction identifier based on parameters stored in the smart card as part of the initialization data. The transaction message can further include the predetermined number of fixed-value units required for each transaction. Also, the transaction message can include a smart card identifier and a count indicative of a total number of transactions generated by the smart card.

The transaction message can be received in the vendor computer system which can verify that the predetermined number of fixed-value units corresponds to the transaction identifier. The count indicative of the total

number of transactions for the smart card can also be verified.

In another aspect, the invention features a smart card including a memory storing a program and data representative of one or more fixed-value units and a microcontroller configured by the program to furnish the transaction and modify the data to reduce the number of fixed-value units by a predetermined amount when the transaction is furnished.

In various implementations, the smart card includes one or more of the following features. The data stored in the memory can include a predetermined number of fixed-value units required for each smart card transaction, and the microcontroller can be configured by the program to modify and reduce the number of fixed-value units according to the predetermined number stored in the memory.

The data stored in the memory can include an encryption key, and the microcontroller can be configured by the program to encrypt each transaction message generated by the smart card with the encryption key.

The microcontroller also can be configured by the program to include a transaction identifier as part of each transaction message generated by the smart card. In addition, the microcontroller can be configured by the program to include the predetermined number of fixed-value units as part of each transaction message generated by the smart card. Furthermore, a count, indicative of a total number of transactions generated by the smart card, can be stored in the memory. The microcontroller can also be configured by the program to increment the count by one each time a transaction message is generated by the smart card. Moreover, the microcontroller can be configured by the

program to include, as part of the transaction message, the total number of transactions generated by the smart card.

In various implementations, a multi-parameter algorithm can be permanently stored in the memory and vendor-specific parameters can be stored in the memory. The microcontroller can be configured by the program to include a transaction identifier, based on the multi-parameter algorithm and the vendor-specific parameters, as part of each transaction message generated by the smart card.

In various implementations, the invention provides one or more of the following advantages. Various implementations of the invention provide a convenient, robust and tamper-proof technique for the marketing and sale of access to a particular vendor's goods or services. Furthermore, the invention provides for secure, non-reputable transactions without the need for using third parties to facilitate or implement the transfer of goods or services. Moreover, the transactions can occur with relatively small transaction costs. Minimizing transaction costs is particularly important with respect to micro-transactions, in which the cost of the goods or services is of the same order of magnitude as the transaction costs.

In addition, various implementations of the invention allow a smart card holder to initiate a secure transaction for goods or services without requiring the smart card to interact directly with the vendor's equipment. Specifically, the smart card need not be read by a smart card reader/writer attached to the vendor's equipment. For example, the smart card can be used to initiate a transaction over a general-purpose computer network.

Moreover, since the smart card is intended for fixed-value transactions with a specific vendor, only a single communication from the card to the vendor's system is

needed to conclude the transaction. The smart card provides all the information required, including an indication of the goods or services, as well as the cost. Thus, the vendor's system receives all the information needed to conclude the transaction without having to transmit any information or instructions to the smart card. Thus, for example, the vendor's system need not instruct the smart card to reduce the number of stored monetary units on the card according to the cost of the goods or services. Since the cost of the goods or services in fixed in advance, the smart card itself automatically performs this function.

The invention is particularly advantageous, for example, in the context of obtaining services for which a consumer would otherwise have to pay a high subscription price. For example, a consumer may desire access to a vendor's on-line services available over the Internet, but expect to access the on-line services only a limited number of times. Naturally, the consumer does not wish to pay the full subscription price which the vendor would otherwise charge. The invention facilitates such a transaction by allowing the consumer to purchase the opportunity to access the on-line services a limited number of times through the use of the smart card. Once the services have been accessed the predetermined number of times, the card holder can no longer access the vendor's on-line services. The invention has applications to transactions involving other goods and services as well.

Brief Description of the Drawings

FIG. 1 is an exemplary system in which the invention can be practiced.

FIG. 2 shows initialization data stored on a smart card according to the invention.

FIG. 3 is a flow chart of a method of providing a transaction using a smart card according to the invention.

FIG. 4 shows an exemplary transaction message according to the invention.

Description of the Preferred Embodiments

FIG. 1 shows an exemplary system 1 which includes a microprocessor card, or smart card 2, with a microcontroller 3. Software which controls the operations of the smart card 2 is stored in program memory 4 such as nonvolatile read-only memory (ROM). The software includes an encryption program to encrypt data or other information using a secure data encryption technique. The software also includes a general multi-parameter algorithm for use as explained below. Data is stored in a data memory 5. The data memory 5 includes alterable nonvolatile memory 5, such as electrically erasable programmable read-only memory (EEPROM). The data memory 5 also includes random access memory (RAM).

The system 1 further includes a terminal 10. The terminal 10 includes, for example, a personal computer 11 which is connected to a larger general-purpose computer network 22. A smart card reader or reader/writer 12 is attached and communicates with the computer 11. The terminal 10 also includes means for entering information into the computer or indicating a selection, such as a keyboard 13, as well as a display screen 14. A mouse or a vocal input device (not shown) can be used in addition to or in place of the keyboard 13.

The computer 11 can transmit and receive information to and from other entities in the network 22, for example, via a modem 15 and communication lines 20. As shown in FIG. 1, the network 22 includes one or more vendor computer

systems, such as the vendor computer system 21, which offer goods or services to customers who have access to the network 22. The computer system 21 can be, for example, a server.

The smart card 2 also has a device for communicating 6 with the smart card reader or reader/writer 12. In certain implementations, the device for communicating 6 is electrical circuitry which requires physical contact with pins in the smart card reader/writer 12. Alternatively, electrical circuitry on the smart card 2 can use inductive coupling, capacitive coupling or radio signals to communicate with the reader/writer 12. Communication may be performed by a local area or wide area network, for example, by way of the Internet or by a satellite communication link.

In various implementations, the smart card 2 is issued by a particular vendor associated with the vendor computer system 21 and is intended to be used to purchase goods or services from that particular vendor. The smart card 2 is also intended to be used in fixed-value transactions. In other words, each transaction generated by the smart card 2 has the same predetermined monetary value and requires a previously established number of fixed-value monetary units.

As shown in FIG. 2, when the smart card 2 is purchased from the vendor, the smart card is initialized by the vendor with certain initialization data. This initialization data is stored securely in the data memory 5 to prevent its being tampered with by the purchaser or some other third party. The initialization data includes a unique smart card identifier which can represent, for example, a combination of alphanumeric characters. The initialization data further includes the encryption key of the vendor. A count corresponding to the number of fixed-

value monetary units is also stored on the card in the data memory 5. During initialization of the smart card 2, the vendor sets this count equal to the number of fixed-value monetary units purchased by the consumer. Alternatively, the number of fixed-value monetary units can be stored in hardware, such as a counter. In addition, a predetermined number representing the number of fixed-value units required for each smart card transaction is stored in the data memory 5.

The vendor also initializes the smart card 2 by storing specific parameters to be used in conjunction with the general multi-parameter algorithm stored in the program memory 4. The general multi-parameter algorithm allows each vendor to select parameters which are tailored to its application and security requirements. The parameters are stored in the data memory 5. The microcontroller 3 on the smart card 2 uses the multi-parameter algorithm to generate a transaction identifier which can be used, as discussed above, to identify the particular products or services for which the smart card 2 was issued.

Finally, the initialization data includes a count of the total number of transactions generated by the smart card 2 from the time the smart card is issued until the present. This count is initially set by the vendor to zero.

FIG. 3 is a flow chart illustrating the operation and use of the smart card 2. For purposes of illustration, it is assumed that the vendor is the provider of certain on-line services available to the consumer through the personal computer 11 attached to the network 22. As indicated by 30, a person purchases the smart card 2 which is initialized by the vendor as explained above. When the card holder wishes to gain access to the vendor's on-line services for which the smart card was issued, the card holder accesses an

appropriate program over the computer network and inserts the smart card 2 into the card reader 12, as indicated by 31. The computer 11 prompts the card holder to indicate whether he wishes to access the vendor's on-line services, for example, by pressing a particular key on the keyboard 13. If the card holder makes the appropriate selection, as indicated by 32, then the computer 11 instructs the smart card 2 to generate an encrypted transaction message corresponding to the selected goods or services from the appropriate vendor. The smart card 2 determines whether there are a sufficient number of fixed-value monetary units remaining on the card to allow the transaction, as indicated by 33. If there are a sufficient number of units, then the smart card 2 generates the encrypted transaction message, as indicated by 34. If a sufficient number of monetary units do not remain, then the smart card 2 does not generate the transaction message, as indicated by 35. In this case, a message may appear on the user's display screen 14 indicating that the transaction cannot be performed because there are an insufficient number of monetary units.

An exemplary transaction message is illustrated in FIG. 4. The transaction message includes the unique smart card identifier and the number of fixed-value units represented by the transaction. In addition, the transaction identifier, which is generated by the smart card 2 and is based on the multi-parameter algorithm and the parameters entered by the vendor, is included in the transaction message. The transaction identifier can be, for example, a sequence of numbers. The transaction message further includes the number of fixed-value units remaining after the transaction. Finally, the total number of transactions generated by the smart card 2 is included as part of the transaction message. The transaction message is

encrypted by the smart card 2 using the vendor's encryption key which, as previously explained, is stored in the data memory 5.

The computer 11 then sends a request for the vendor's goods or services together with the encrypted transaction message over the network, as indicated by 36. As indicated by 38, the smart card 2 is programmed to reduce automatically the count corresponding to the number of fixed-value monetary units by the number of fixed-value monetary units represented by the transaction. Thus, the count of fixed-value monetary units reflects the current number of fixed-value monetary units remaining on the smart card 2. The smart card 2 is also programmed to increase the count of the total number of transaction generated by the card by one, as indicated by 40.

As indicated by 42, the request for the vendor's goods or services and the encrypted transaction message are received by the vendor's computer system 21. The vendor's computer system 21 decrypts the transaction message using the vendor's decryption key, as indicated by 44 (FIG. 3B). The computer system 21 then verifies the transaction identifier and the number of fixed-value units, as indicated by 46, to confirm that the transaction identifier is valid and that the number of fixed-value units corresponds to the transaction identifier and to the goods or services purchased. If the data received in the transaction message is verified, then the vendor delivers the goods or services, as indicated by 48. In the present example, the card holder would be permitted access to the vendor's on-line services by using the computer 11. If the data received in the transaction message is not verified, then the goods or services are not delivered, as indicated by 50. Moreover,

subsequent requests for goods or services associated with the particular smart card identifier can be denied.

In certain implementations, any or all of the following additional verification checks can be performed, in either real-time or off-line depending on the security requirements of the system. As indicated by 52, the vendor's computer system 21 can verify whether the smart card identifier received in the transaction message is valid, whether the current count of transactions associated with the card identifier is correct, or whether the transaction identifier and the number of transactions generated by the smart card correlate correctly. If one or more of the verification checks fails, subsequent transaction requests associated with the smart card identifier can be rejected, as indicated by 54.

Once the fixed-value monetary units on the smart card 2 are depleted or are insufficient to allow further transactions for the goods or services for which it was issued, the card-holder can either dispose of the card 2 or return it to the vendor for re-initialization and the purchase of additional monetary units.

Although the invention has been described above with reference to a smart card 2 containing initialization data corresponding to a single vendor and a count corresponding to monetary units for a single type of goods or services, it should be understood that, in some implementations of the invention, the smart card 2 can be used with multiple types of transactions, each of which corresponds to a different predetermined monetary value and which requires a corresponding reduction in the number of predetermined fixed-value units on the smart card. The smart card would include a separate count corresponding to each type of goods or services. Furthermore, in such implementations,

initialization data from more than one vendor can be stored on the smart card 2 in a secure manner. For this purpose, the smart card can include an index of identifiers corresponding to the vendors and the products available from each vendor. Once the smart card 2 is inserted into the reader/writer 12 and an appropriate program on the computer 11 is accessed by the user, the computer 11 prompts the card holder to make a selection using, for example, the keyboard 13. The selection indicates the particular transaction which the card holder wishes to initiate with the smart card 2. Once the card holder makes a selection, the computer 11 instructs the smart card 2 to generate an encrypted transaction message based upon the initialization data corresponding to the selected goods or services from the appropriate vendor. The transaction message would then be transmitted to the appropriate vendor's computer system, as discussed above. Additionally, the particular count which resides in the smart card and which corresponds to the selected goods or services would be reduced in the manner discussed above.

Other implementations are contemplated within the scope of the following claims.

What is claimed is:

1. A method of performing a fixed-value transaction using a smart card having stored therein initialization data comprising a count representing a specified number of fixed-value units, the method comprising:

generating a transaction message in the smart card;

transmitting the transaction message to a vendor computer system; and

reducing the count stored in the smart card by a predetermined amount.

2. The method of claim 1 wherein the transmitting comprises transmitting the transaction message over a computer network.

3. The method of claim 1 wherein the initialization data further comprises a predetermined number of fixed-value units required for each smart card transaction, and wherein the reducing comprises reducing the count stored in the smart card by the predetermined number of fixed-value units.

4. The method of claim 1 wherein the initialization data further comprises an encryption key, and generating a transaction message comprises encrypting the transaction message with the encryption key.

5. The method of claim 4 further comprising receiving the transaction message in the vendor computer system and decrypting the transaction message with a decryption key.

6. The method of claim 1 wherein the transaction message comprises a transaction identifier indicative of goods or services associated with the transaction.

7. The method of claim 6 further comprising generating in the smart card a transaction identifier based on parameters stored in the smart card as part of the initialization data.

8. The method of claim 6 wherein the initialization data further comprises a predetermined number of fixed-value units required for each smart card transaction, and wherein the transaction message further comprises the predetermined number of fixed-value units required for each smart card transaction.

9. The method of claim 8 further comprising receiving the transaction message in the vendor computer system and verifying in the vendor computer system that the predetermined number of fixed-value units required for each smart card transaction corresponds to the transaction identifier.

10. The method of claim 1 wherein the transaction message further comprises a smart card identifier and a count indicative of a total number of transactions generated by the smart card.

11. The method of claim 10 further comprising receiving the transaction message in the vendor computer system and verifying in the vendor computer system that the

count indicative of the total number of transactions for the smart card is correct.

12. The method of claim 1 further comprising incrementing in the smart card a count indicative of a total number of transactions generated by the smart card.

13. A smart card for use with a system capable of receiving a transaction message, comprising:

a memory storing a program and data representative of one or more fixed-value units; and

a microcontroller configured by the program to furnish the transaction and modify the data to reduce the number of fixed-value units by a predetermined amount when the transaction is furnished.

14. The smart card of claim 13 wherein the data stored in said memory includes a predetermined number of fixed-value units required for each smart card transaction, and wherein the microcontroller is configured by the program to modify and reduce the number of fixed-value units according to the predetermined number stored in the memory.

15. The smart card of claim 13 wherein the data stored in the memory further comprises an encryption key, and wherein the microcontroller is further configured by the program to encrypt each transaction message generated by the smart card with the encryption key.

16. The smart card of claim 13 wherein the microcontroller is further configured by the program to

include a transaction identifier as part of each transaction message generated by the smart card.

17. The smart card of claim 13 wherein a multi-parameter algorithm is permanently stored in the memory, vendor-specific parameters are stored in the memory, and the microcontroller is configured by the program to include a transaction identifier, based on the multi-parameter algorithm and the vendor-specific parameters, as part of each transaction message generated by the smart card.

18. The smart card of claim 14 wherein the microcontroller is configured by the program to include the predetermined number of fixed-value units as part of each transaction message generated by the smart card.

19. The smart card of claim 13 wherein a count, indicative of a total number of transactions generated by the smart card, is stored in the memory.

20. The smart card of claim 19 wherein the microcontroller is further configured by the program to increment by one the count, indicative of the total number of transactions, each time a transaction message is generated by the smart card.

21. The smart card of claim 21 wherein the microcontroller is further configured by the program to include, as part of the transaction message, the total number of transactions generated by the smart card.

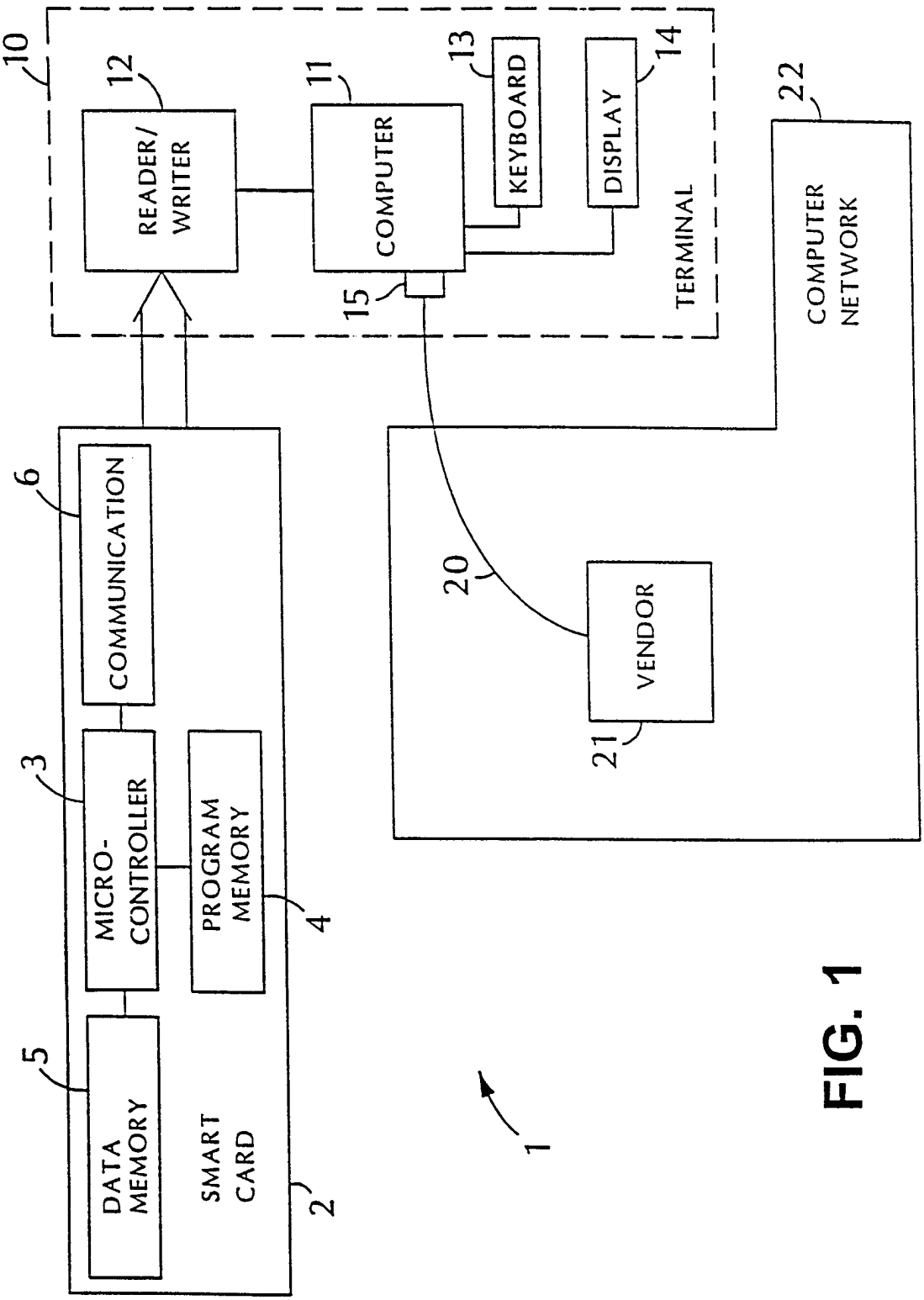

10
12
READER/ WRITER
11
COMPUTER
13
KEYBOARD
14
DISPLAY
TERMINAL
15
22
COMPUTER NETWORK
6
COMMUNICATION
3
MICRO-CONTROLLER
PROGRAM MEMORY
4
5
DATA MEMORY
SMART CARD
2
20
VENDOR
21
1

FIG. 1

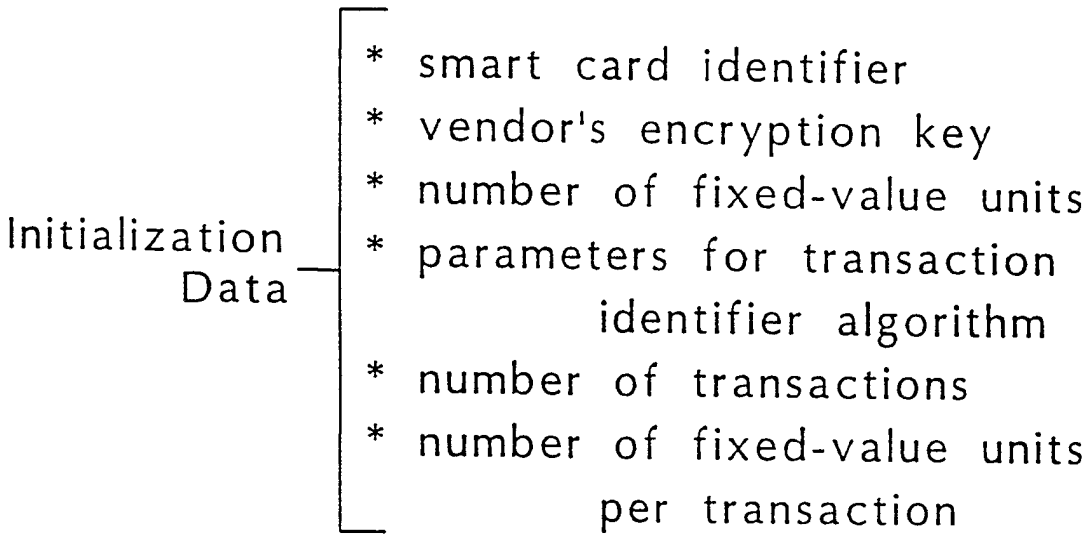

Initialization Data
* smart card identifier
* vendor's encryption key
* number of fixed-value units
* parameters for transaction identifier algorithm
* number of transactions
* number of fixed-value units per transaction

FIG. 2

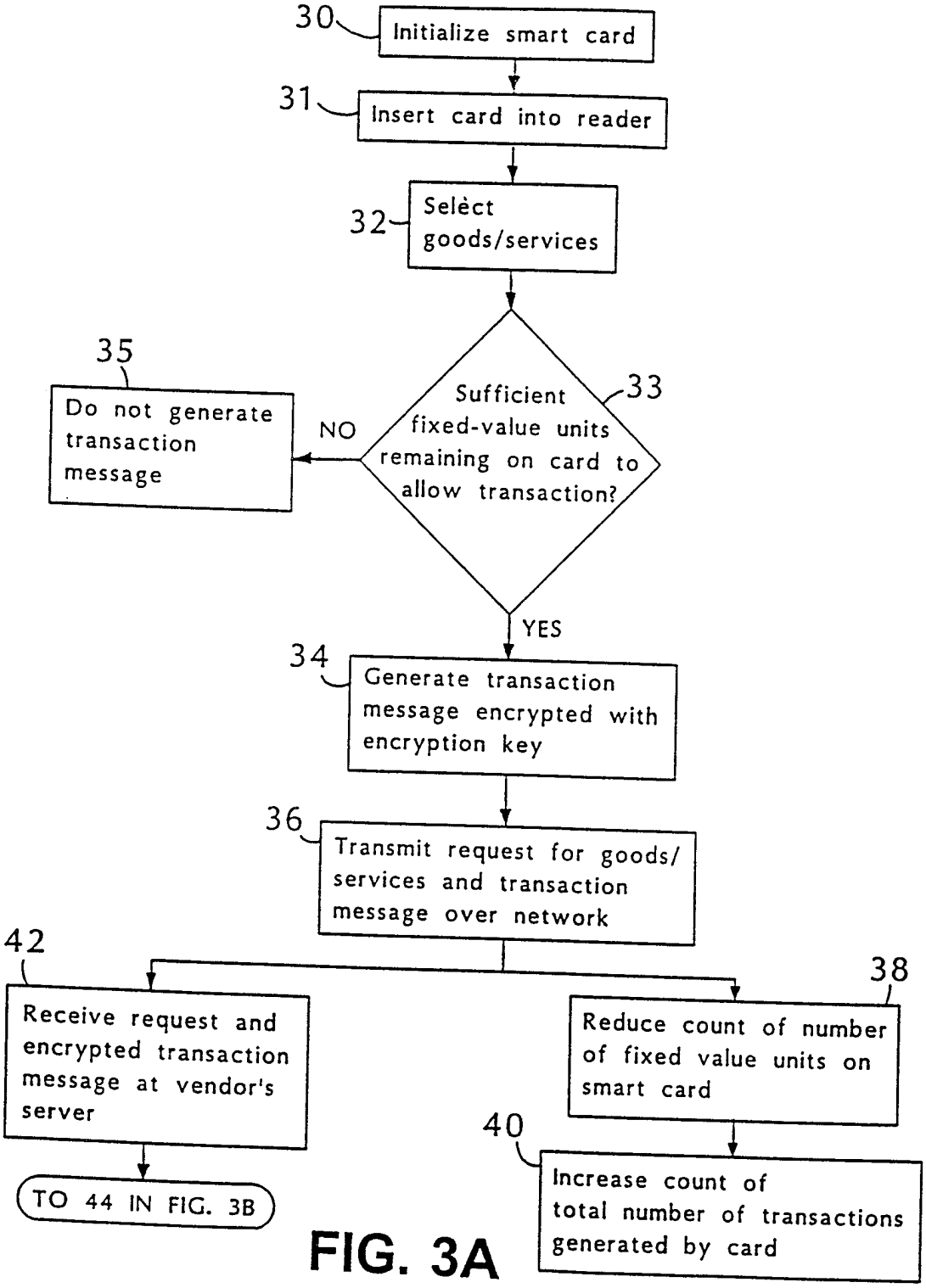

30
Initialize smart card
31
Insert card into reader
32
Select goods/services
33
Sufficient fixed-value units remaining on card to allow transaction?
NO
35
Do not generate transaction message
YES
34
Generate transaction message encrypted with encryption key
36
Transmit request for goods/ services and transaction message over network
42
Receive request and encrypted transaction message at vendor's server
TO 44 IN FIG. 3B
38
Reduce count of number of fixed value units on smart card
40
Increase count of total number of transactions generated by card

FIG. 3A

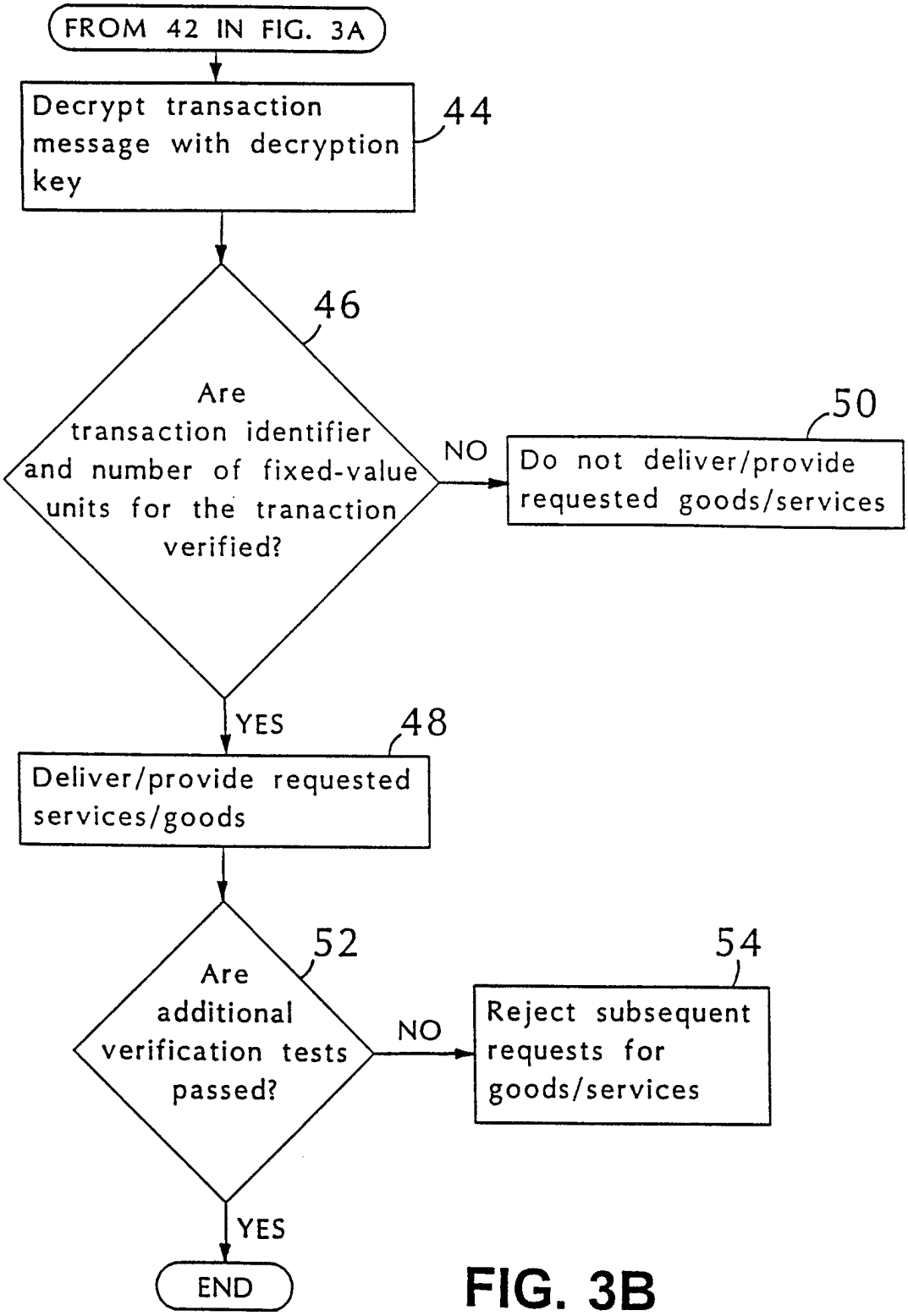

FROM 42 IN FIG. 3A
Decrypt transaction message with decryption key
44
46
Are transaction identifier and number of fixed-value units for the tranaction verified?
NO
50
Do not deliver/provide requested goods/services
YES
48
Deliver/provide requested services/goods
52
Are additional verification tests passed?
NO
54
Reject subsequent requests for goods/services
YES
END

FIG. 3B

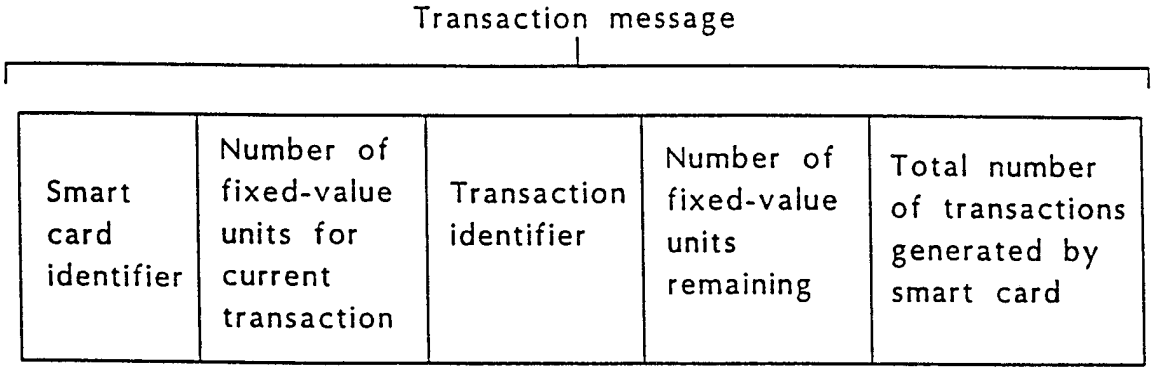

Transaction message
Smart card identifier
Number of fixed-value units for current transaction
Transaction identifier
Number of fixed-value units remaining
Total number of transactions generated by smart card

FIG. 4