(12) PATENT **(11)** Application No. **AU 199741180 B2**
(19) AUSTRALIAN PATENT OFFICE **(10)** Patent No. **718123**

(54) Title
Tickets stored in smart cards

(51)7 International Patent Classification(s)
G07F 007/08 **G07B 015/00**

(21) Application No: **199741180** (22) Application Date: **1997.08.07**

(87) WIPO No: **WO98/07120**

(30) Priority Data

(31)	Number	(32)	Date	(33)	Country
	96202240		**1996.08.09**		**EP**

(43) Publication Date : **1998.03.06**
(43) Publication Journal Date : **1998.05.07**
(44) Accepted Journal Date : **2000.04.06**

(71) Applicant(s)
Koninklijke KPN N.V.

(72) Inventor(s)
Frank Muller; Michel Marco Paul Drupsteen

(74) Agent/Attorney
SPRUSON and FERGUSON,GPO Box 3898,SYDNEY NSW 2001

(56) Related Art
AU 48717/90
US 4501958

OPI DATE 06/03/98 APPLN. ID 41180/97
AOJP DATE 07/05/98 PCT NUMBER PCT/EP97/04333

AU9741180

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
G07F 7/08, G07B 15/00
A1

(11) International Publication Number: **WO 98/07120**

(43) International Publication Date: 19 February 1998 (19.02.98)

(21) International Application Number: PCT/EP97/04333

(22) International Filing Date: 7 August 1997 (07.08.97)

(30) Priority Data:
96202240.6 9 August 1996 (09.08.96) EP
(34) Countries for which the regional or international application was filed: NL et al.

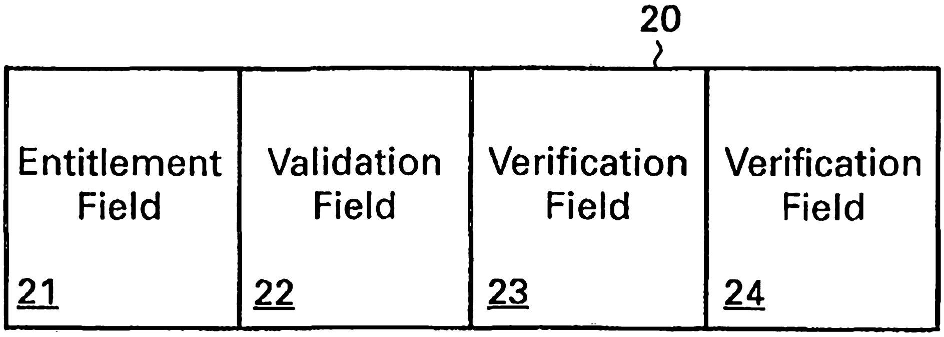
(71) Applicant: KONINKLIJKE ~~PTT NEDERLAND~~ KPN N.V. [NL/NL]; Stationsplein 7, NL-9726 AE Groningen (NL).

(72) Inventors: MULLER, Frank; Meerkoetlaan 24, NL-2623 NJ Delft (NL). DRUPSTEEN, Michel, Marco, Paul; Aert de Gelderlaan 36, NL-1816 NA Alkmaar (NL).

(81) Designated States: AU, CA, CN, CZ, EE, HU, IL, JP, LT, LV, NO, NZ, PL, SG, SI, Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: TICKETS STORED IN SMART CARDS



(57) Abstract

In a smart card (1) electronic tickets (20) are securely stored. Ticket data may be written into the fields (21, 22, 23) of a ticket (20) in a protected manner using a special code. Tickets (20) may comprise several fields: an entitlement field (21), a validation field (22), and preferably also a verification field (23). Preferably, a different key (K1, K2, K3) is used for each type of field. A further protection of the integrity of the tickets is obtained by using a first storage command (UPDATE) to prepare a field when issuing the ticket and using a different, second storage command (WRITE) when validating the ticket. Thus the fraudulent modification of an issued ticket is prevented.

Tickets stored in smart cards.

BACKGROUND OF THE INVENTION

The present invention relates to tickets stored in smart cards, as well as to smart cards for storing tickets and a method of using tickets stored on smart cards. In particular, but not exclusively, the present invention relates to the secure storage of "open" tickets in smart cards, i.e tickets of which the particular date and/or time of use is left open when issuing the ticket. More in particular, the present invention relates to the secure storage, validation and/or verification of tickets stored on smart cards, and to smart cards and a payment system arranged for the same.

Present day smart cards offer a plurality of applications, one of which may be an electronic purse. Other possible applications are identification (user verification), storing important data (e.g. medical data), collecting loyalty credits, and the like. One such application is the storing of tickets, i.e. access rights to goods and/or services.

Various types of tickets may be envisaged. A first type of ticket may be issued containing all relevant data, such as (in the case of e.g. an airline ticket) the company (airline) involved, the price, the day of travel, the place and time of departure and the place and time of arrival. Such a ticket may be ready for use. A second type of ticket is not ready for use, as e.g. the day of travel needs to be filled in after the issuance of the ticket. Such an "open" ticket needs to be validated before it can be used: the ticket is made valid by filling in the day of travel and possibly other data. Such an "open" ticket may be suitable for multiple use if it can be validated more than once.

Examples of tickets stored on smart cards are known from the Prior Art. Dutch patent application NL 93 01902, for example, discloses a method of obtaining a right to a service by means of a smart card (IC card). In this Prior Art method, the card serves both as a payment means and as a registration means. That is, the card is used to store proof of payment of the service paid for, thus replacing paper tickets. The use of multiple tickets, i.e. tickets which may be used more than once, is also mentioned in said patent application.

In the method of the above-mentioned Dutch patent application, a ticket is stored on a card by registering on the card an access code, optionally in combination with a card identification code. At the terminal of e.g. a theatre the access code and (optionally) the identification code are checked, whereupon the access code is erased from the card. The way multiple tickets are implemented or used is not disclosed.

The above-mentioned Dutch patent application therefore does not provide a specific method for securely storing tickets on smart cards, and certainly not for tickets which may be validated after their issuance.

Also, European patent application EP 0 658 862 discloses a method and system for employing multi-functional smart cards by means of a communication system. This prior art method and system allow e.g. airline tickets to be stored on the smart cards. The specific manner in which the tickets are stored is however not disclosed.

In addition, European patent application EP 0 380 377 discloses a system for electronic payment of transport and services by means of smart cards. In the system of said patent application, a ticket is disclosed having fields for stamping the ticket on a certain date at a certain time and fields for storing data indicating that the ticket has been checked. Of the way the ticket data is stored, no further particulars are disclosed.

Conventional electronic tickets are susceptible to fraud in that ticket data can untraceably be altered. Whereas fraudulent manipulations of paper tickets are often visible, or must be carried out very skilfully no to be visible, the alteration of bits on a smart card normally leaves no traces. Especially in the case of open tickets, where various stations "stamp" the ticket in order to perform a validation or verification, the problem of possible fraud exists.

SUMMARY OF THE INVENTION

It is an object of the present invention to overcome the above-mentioned and other disadvantages of the prior art and to provide a smart card which allows tickets to be securely stored.

It is another object of the present invention to provide a smart card which virtually eliminates the possibility of the fraudulent issue or validation of tickets.

It is further object of the present invention to provide a smart card which allows secure "punching", i.e. secure traceable verification, of tickets.

It is a still further object of the present invention to provide a smart card which allows the use of secure open tickets, i.e. tickets which have a non-predetermined validity date or time.

It is a yet further object of the present invention to provide a method for securely storing tickets on smart cards, as well as a system in which the method is applied.

Accordingly, the present invention provides a smart card comprising an integrated circuit having a processor and a memory, the memory being structured so as to comprise tickets, a ticket comprising at least one field for storing data relating to the ticket, the smart card comprising means for storing data using a code containing a fixed number of set bits per group of bits.

By using a code containing a fixed number of set bits, it can be easily verified (by the checking of the number of set bits of the code) if the data is correct, whereby fraud is effectively prevented. Preferably, the code comprises code words having eight bits, the number of set bits in each code word equalling four.

Advantageously, the ticket comprises an entitlement field and a validation field. By providing separate entitlement and validation fields it is possible to issue a ticket in two stages: first the ticket is issued by a first terminal, while e.g. the date of validity is left open, and at a later stage the ticket is validated by a second terminal, e.g. by registering the date of validity in the validation field. In both types of fields, the above-mentioned code is used.

Preferably, a ticket according to the invention further comprises at least one verification field for storing verification data. A verification field offers the opportunity to register verification information, which may be issued by a third terminal. Although the said first, second and third terminals may be separate devices, in some applications they will be identical.

In respect of the coded storage of ticket data, the integrated circuit of the smart card is advantageously arranged for, when issuing the ticket, exclusively storing data in the validation field using a first command only capable of storing a first value (e.g. logical zero), and for, when validating the ticket, exclusively storing data in the validation field using a second command only capable of storing a second, different value (e.g. logical one). In this way, it is impossible to alter the entitlement during the validation or verification, or to alter the validation during verification.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 schematically shows a smart card as may be used in the method of the present invention.

Fig. 2 schematically shows the integrated circuit of the smart card of Fig. 1.

Fig. 3 schematically shows the structure of a ticket as stored in a smart card.

Fig. 4 schematically shows the way a field of a ticket may be coded according to the present invention.

Fig. 5 schematically shows a diagram representing the issuance of a ticket.

Fig. 6 schematically shows a diagram representing the validation of a ticket.

Fig. 7 schematically shows a diagram representing the verification of a ticket.

Fig. 8 schematically shows a system in which the method of the present invention is utilized.

DESCRIPTION OF PREFERRED EMBODIMENTS

The smart card or IC card 1 shown schematically and by way of example in Fig. 1 comprises a substrate 2, in which an integrated circuit is embedded. The integrated circuit, which will further be explained with reference to Fig. 2, is provided with contacts 3 for contacting a card reader or the like. It should be noted that the present invention can also be applied in the case of so-called contactless smart cards.

The integrated circuit 10 shown schematically and by way of example in Fig. 2 comprises a processor 11, a memory 12 and an input/output circuit 13. The memory may comprise a volatile (RAM) memory part for temporarily storing data and a non-volatile (ROM) memory part for permanently or semi-permanently storing data. The latter part is preferably an EEPROM type memory. The data stored in the non-volatile part may contain both programming data (instructions, programs) and payment data, i.e. data relating to monetary transactions. It will be understood that a separate memory (not shown) may be provided to store the instruction set of the processor 11.

An embodiment of a ticket as may be used in the present invention is schematically shown in Fig. 3. The ticket 20 comprises several fields, i.e. an entitlement field 21, a validation field 22, and two verification fields 23 and 24. In practice, a ticket may comprise additional fields which are not shown in Fig. 3. Also, a ticket may comprise only one verification field, or more than two verification fields, e.g. three, five or ten.

It will be understood that the ticket 20 may be implemented by assigning memory locations of the memory 12 to the respective fields, and that in actual implementations the memory locations need not be adjacent.

The entitlement field 21 contains the description of the ticket including e.g. the identity of the ticket issuer, the scope of validity (e.g. an expiry date, the maximum length of a trip), the number of persons the ticket is valid for, and a starting point and destination of a trip, although some of this data may be entered in the validation field after the issuance of the ticket. The entitlement field 21 may comprise e.g. 25 bytes.

The validation field 22 is reserved for information which may be added later to the ticket, such as a starting time and/or date of validity. The entitlement field 21 and the validation field 22 taken together should contain sufficient data for the ticket to be valid while the actual relative allocation of data to these two fields may vary. The validation field 22 may comprise e.g. 12 bytes.

The verification fields 23 and 24 are reserved for information which may be added during the use of the ticket, such as the date, the time, and a terminal identification. A code identifying a particular means of transportation (e.g. a train code) may also be added. The verification fields 23 and 24 may comprise e.g. 22 bytes each.

The validation field 22 thus makes it possible to issue an "open" ticket which is completed at a later point in time. At the moment of issuance, only the essential data may be entered in the entitlement field 21. At the moment of validation, the ticket is completed by entering the remaining data (such as a date of validity) in the validation field 22. The verification fields 23 and 24 allow a proof of verification to be entered in the ticket (verification stamp). Such a proof of verification may provide proof of use of the ticket, proof of presence of the card (holder) at a certain location and at a certain point in time, etc.

In order to provide a secure storage and to virtually eliminate the possibility of fraudulent alteration of tickets, data is advantageously stored in the fields of a ticket using one or more of the following protective measures:

a. using a special code to store data,

b. using different commands to store data, depending on the particular stage of providing a ticket (issuance, verification or validation),

c. using different keys to store data in different fields, depending on the particular stage.

The special code will first be explained with reference to Fig. 4.

Fig. 4 shows an example of a preferred representation of data in the fields 21-24 of the ticket 20 of Fig. 3. Data word 31 comprises eight bits, all of which are (logical) zero. Accordingly, the sum S of the bits is zero. Data word 32 also comprises eight bits, four of which are (logical) one (a so-called eight over four code). The sum S of the bits accordingly equals four. In the tickets of the present invention, the data in the fields 21-24 is stored using a code in which a fixed number of bits equals one. In other words, a code is used as e.g. contained in data word 32, of which the sum of the bits is fixed (e.g. S = 4). This allows an easy detection of alterations of the stored data. Data word 33, for example, is equal to data word 32 exept for one bit. The sum (S) of the bits of data word 33 equals five rather than four. If a code is used in which all data words have a sum S equal to four, the aberration in data word 33 can readily be detected by determining the sum of the bits of each data word.

Accordingly, in the example of Fig. 4 three types of data words may be distinguished, based on the sum S of their bits. For a first type, S equals zero: these words are empty. For a second type, S equals four: these words contain valid data. For a second type, S equals neither zero nor four: these words contain invalid data.

It should be noted that the number of ones and zeros shown in Fig. 4 are by way of example only and that data words may be used which e.g. contain eight or ten bits, three or five of which are equal to one.

Advantageously, use is made of different commands to store data at different stages of providing a ticket. A smart card preferably supports a first write command (called UPDATE) to store ones and zeros in a memory location, and a second write command (called WRITE) to store only ones. During the issuing stage of providing a ticket, the fields of the ticket are provided with data using the first command (UPDATE). In this stage, in the entitlement field 21 relevant data is stored, while in the validation field 22 and the verification fields 23 and 24 zero-only words are written (as data word 31 in Fig. 4). During the validation and verification stages, only the second command (WRITE) may be used, and therefore only ones can be written. This means that the valid code words which have already been written cannot be altered during the validation and verification stages, as this would require a zero to be written. Thus, by allowing only the second command (WRITE) to be used during validation and verification, the tampering of ticket data is prevented.

It should be noted that an empty (i.e. non-issued) ticket should contain invalid data, i.e. data containing more than four ones per word if an eight over four code is used, in order to prevent an empty ticket to be "issued" using the second write command (WRITE). Advantageously, an empty ticket contains only ones.

In order to provide a further protection, preferably different keys are used to store data in different fields, depending on the particular stage of providing a ticket. Thus the issuance of a ticket (use of the first write command UPDATE) requires a first key K1, the validation requires a second key K2, and the verification requires a third key K3. A smart card according to the present invention is preferably arranged so as to provide access to all fields 21-24 of a ticket 20 when the first key K1 is used, while only providing write access to the validation field 22 when the second key K2 is used. Similarly, the third key K3 only provides store access to the verification fields 23 and 24. Optionally, the third key K3 only provides store access to the first verification field 23, while a fourth key K4 exclusively provides write access to the second verification field 24. It will be understood that all keys provide read access to all fields of the ticket 20.

The use of at least three keys thus makes it possible to provide limited access to the various fields and to restrict the use of the first write command (UPDATE) by requiring the key K1.

The method of the invention, as depicted schematically and by way of example in Figs. 5, 6 and 7, involves providing a ticket according to the present invention. The method comprises three stages: a first stage (issuance) shown in Fig. 5, a second stage (validation) shown in Fig. 6 and a third stage (verification) shown in Fig. 7. Subsequent events are shown from top to bottom in Figs. 5-7. It will be assumed that the memory of the smart card is initialized beforehand, e.g. by providing empty tickets containing all-ones code words.

As shown in Fig. 5, the issuance stage begins with a first (start) step 50 in which the issuing terminal is activated, e.g. by the insertion of the card. In the subsequent step 51 the ticket count is checked, i.e. is the terminal permitted to issue another ticket? The ticket count may be limited by e.g. a maximum number of tickets per day and may be reset daily.

If the ticket count is not exceeded, the method continues with step 52, in which the terminal asks the card for a random number. In response, the card produces in step 53 a random number (R) by means of a built-in random number generator, preferably implemented in software. The random number is transferred to the terminal.

In step 54, the terminal provides entitlement data (ED) as well as a first message authentication code (MAC1) derived from the entitlement data ED and the random numer R using the first key K1. This authentication code MAC1 is checked by the card in step 55, e.g. by also deriving MAC1 from the entitlement data ED and the random number R and comparing the received and derived authentication codes. If the code MAC1 is found to be invalid, the procedure may be terminated and an error message may be sent to the terminal. Note that the verification of the authentication code MAC1 implicitly involves the verification of the first key K1. A failed verification thus inhibits the use of the first write command (UPDATE).

If the code MAC1 is found to be valid, the entitlement data ED is stored in the card in step 56 using the first write command (UPDATE). Also, the remaining fields of the ticket (validation and verification fields) are reset using said command. An acknowledge message (ACK) is sent to the terminal. Also, proper codes (e.g. all ones) may be written into the validation and entitlement fields.

The issuance stage ends in step 57. A suitable message may be displayed on the terminal.

As shown in Fig. 6, the second or validation stage begins in step 60, in which the validation terminal is activated, e.g. by insertion of the card. The terminal sends a read command to the card. The read command may contain data specifying a certain ticket or a certain type of ticket. The card subsequently reads the specified ticket(s), or alternatively all non-empty tickets, in step 61 and sends the entitlement data ED to the terminal. In step 62 the terminal checks the entitlement data for validity (e.g. by determining the number of set bits per code word). Possibly in step 61 the validation data (VD) of the ticket was sent also. As these validation data is still "empty" (i.e. all zeros) at this stage, it follows that the ticket in question needs to be validated.

If the entitlement data ED received by the terminal in step 62 identifies a ticket which is to be validated, the terminal produces in step 63 a second message authentication code MAC2 using the validation data VD and the second key K2, and sends the data VD and the code MAC2 to the card. In step 64, the card checks the received authentication code MAC2 as in step 55. If the authentication code MAC2 is found to be invalid, an error message may be sent to the terminal. If the code MAC2 is found to be valid, the validation data VD is stored in the ticket in question in step 65, using the second write command (WRITE) and an acknowledge signal is sent to the terminal. Step 66 concludes the validation stage. Note that if the validation (second) terminal does not possess the second key K2, it is not possible to use the first write command (UPDATE) at this stage.

The verification stage shown in Fig. 7 begins in step 70 when the terminal, upon being activated, produces a read command. Again, this read command (which need not be identical to the read command of step 60) may indicate a certain ticket or type of ticket. In step 71, the card reads the relevant entitlement data ED and validation data VD from memory in response to the read command and sends this data to the terminal. The terminal subsequently verifies this data in step 72, based upon verification or check data CD indicating which tickets are to be found valid (e.g. depending on the particular time and date). If the ticket in question is found valid, in step 73 a third message identification code MAC3 is produced using the verification data CD and the third key K3. This data is sent to the card and are checked in step 74. Finally, the verification data CD is stored in a verification field of the card in step 75, upon which the card sends an acknowledge message to the terminal. Step 76, in which the verification terminal may be deactivated, concludes the verification stage.

The system schematically represented in Fig. 8 comprises a first terminal 81, a second terminal 82 and a third terminal 83, as well as a smart card 1. The first terminal 81 is equipped for issuing tickets. To this end, the first key K1 is stored in the first terminal 81. The first terminal 81 also comprises a ticket counter for limiting the number of issued tickets to a predetermined amount.

The second terminal 82 is equipped for validating tickets, while the third terminal 83 is equipped for verifying tickets. The terminals 82 and 83 contain the second key K2 and the third key K3 respectively. The terminals receive input from users and/or operators.

It will be understood by those skilled in the art that the embodiments described above are given by way of example only and that many modifications and additions are possible without departing from the scope of the present invention.

The claims defining the invention are as follows:

1. A smart card comprising an integrated circuit having a processor and a memory, the memory being organized so as to comprise tickets, a ticket comprising at least one field for storing data relating to the ticket, characterized by means for storing data using a code containing a fixed number of set bits per group of bits.

2. A smart card according to claim 1, wherein the code comprises code words having eight bits, the number of set bits in each valid code word equalling four.

3. A smart card according to claim 1 or 2, the processor being provided with a first command for setting and resetting bits and a second command for only setting bits, the first command exclusively being operational in response to an identification of a first type of terminal.

4. A smart card according to any of the preceding claims, a ticket stored in the smart card comprising an entitlement field for storing data relating to the entitlement of the ticket and a validation field for storing data relating to the validity of the ticket.

5. A smart card according to claim 4, wherein a ticket further comprises at least one verification field for storing data relating to a check of the validity of the ticket.

6. A smart card according to claim 4 or 5, the integrated circuit comprising a first key for authenticating entitlement data and a second key for authenticating validation data.

7. A smart card according to claim 6, wherein the integrated circuit further comprises a third key for authenticating verification data.

8. A smart card according to claim 7, wherein the second key and the third key are equal.

9. A smart card according to claim 6, 7, or 8, wherein the identification of a first type of terminal comprises the first key.

10. A method of registering tickets on a smart card comprising a memory, the method comprising the steps of:

creating a ticket in the memory, the ticket comprising at least one field,

issuing the ticket by storing in the field data identifying a right to be conveyed by the ticket using a code containing a fixed number of set bits per group of bits.

11. A method according to claim 10, wherein the code comprises code words having eight bits, the number of set bits in each valid code word equalling four.

12. A method according to claim 10 or 11, wherein the step of issuing the ticket involves the use of a first command for setting and resetting bits and a second command for only setting bits, the first command exclusively being operational in response to an identification of a first type of terminal.

13. A method according to claim 10, 11 or 12, wherein data identifying a right to be conveyed by the ticket is stored in an entitlement field, the method comprising the additional steps of:

validating the ticket by storing in a validation field data relating to the validity of the ticket, and

verifying the ticket by storing in a verification field data relating to a verification of the ticket.

14. A method according to claim 13, wherein the step of verifying the ticket comprises the checking of the number of set bits of the code.

15. A method according to claim 13 or 14, wherein the data stored in the entitlement field comprises an identification of the issuer of the ticket.

16. A method according to claim 13, 14 or 15, wherein the data stored in the validation field comprises the date of validity of the ticket and/or a terminal identification.

17. A method according to any of claims 13 through 16, wherein the data stored in the at least one verification field comprises a date, a time and/or a terminal identification.

18. A method according to any of claims 13 through 17, wherein the storing of data in the entitlement field involves the use of a first key, while the storing of data in the validation field involves the use of a second key.

19. A method according to claim 18, wherein the storing of data in a verification field involves the use of a third key.

20. A method according to claim 19, wherein the second key and third key are equal.

21. A system for providing access to services, the system comprising smart cards and terminals, each smart card being provided with a memory for storing tickets comprising at least one field, an issuing terminal being equipped for storing in the field data representing the right to access a service, whereby data in the at least one field is stored using a code containing a fixed number of set bits per group of bits.

22. A system according to claim 21, wherein the code comprises code words having eight bits, the number of set bits in each valid code word equalling four.

23. A system according to claim 21 or 22, wherein the smart card is provided with a first command for setting and resetting bits and a second command for only setting bits, the first command exclusively being operational in response to an identification of an issuing terminal.

24. A system according to claim 21, 22 or 23, wherein each ticket comprises an entitlement field and a validation field, a validation terminal being equipped for storing in a validation field data validating the respective ticket.

25. A system according to claim 24, wherein a ticket further comprises a verification field, a verification terminal being equipped for storing in a verification field data relating to a verification of the ticket.

26. A system according to any of claims 21 through 25, wherein an issuing terminal comprises a ticket counter for limiting the number of issued tickets.

27. A smart card, substantially as described herein with reference to Figs. 1 and 2 of the accompanying drawings.

28. A method of registering tickets on a smart card, substantially as described herein with reference to the accompanying drawings.

29. A system for providing access to services, substantially as described herein with reference to Fig. 8 of the accompanying drawings.

DATED this Day of 2000

Koninklijke KPN N.V.

Patent Attorneys for the Applicant

SPRUSON & FERGUSON

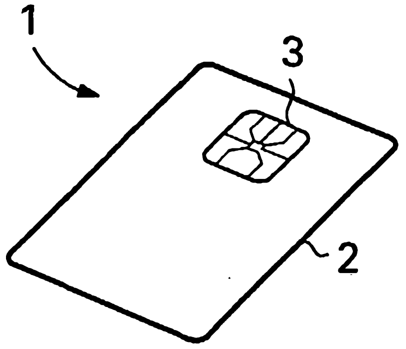


Fig. 1

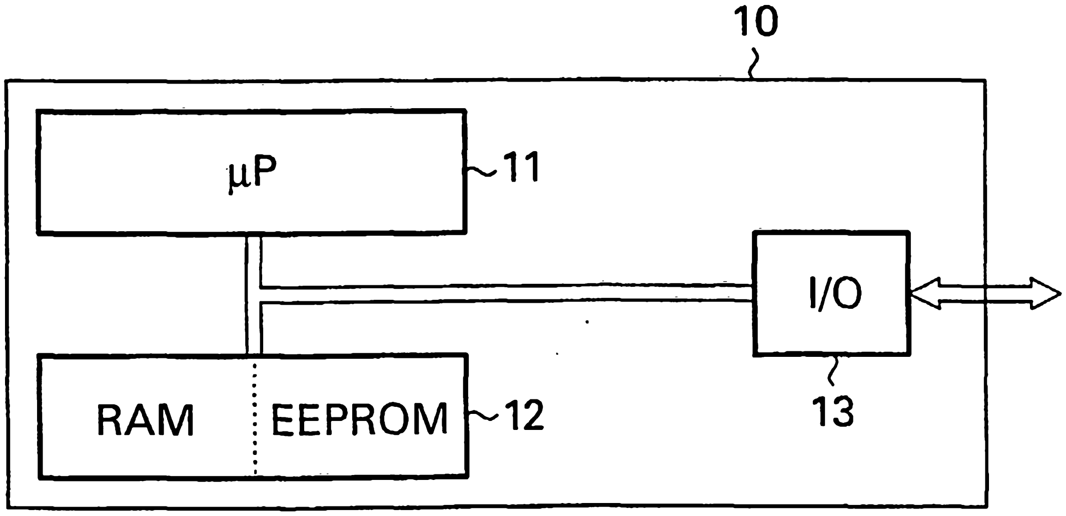


Fig. 2

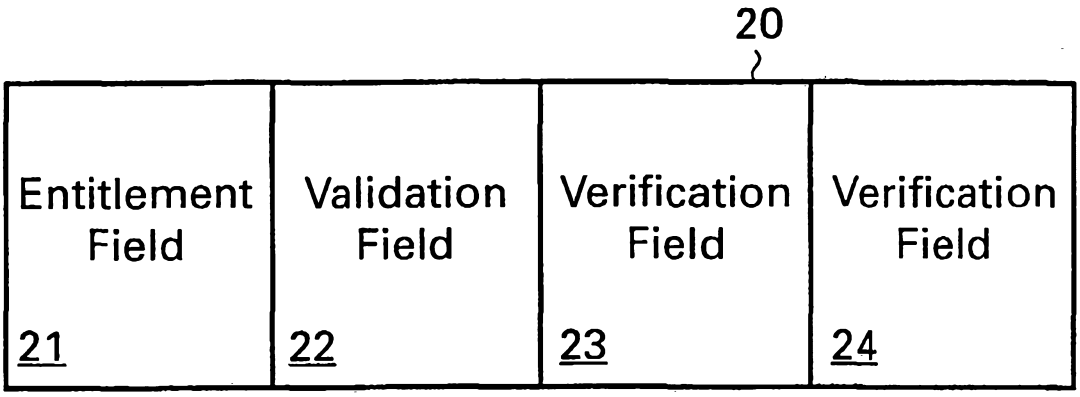

20
Entitlement Field
21
Validation Field
22
Verification Field
23
Verification Field
24

Fig. 3

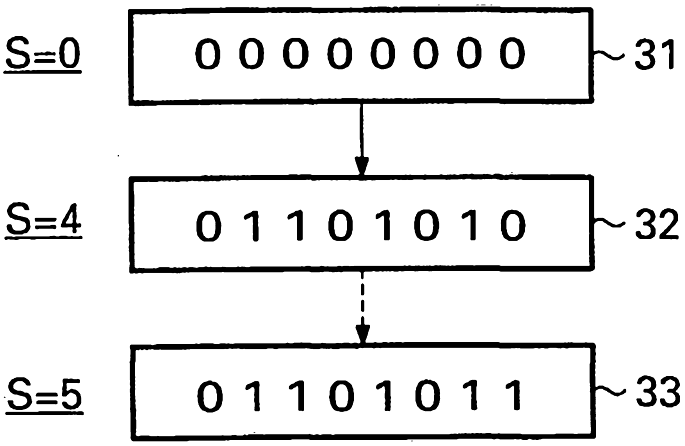

S=0
0 0 0 0 0 0 0 0
31
S=4
0 1 1 0 1 0 1 0
32
S=5
0 1 1 0 1 0 1 1
33

Fig. 4

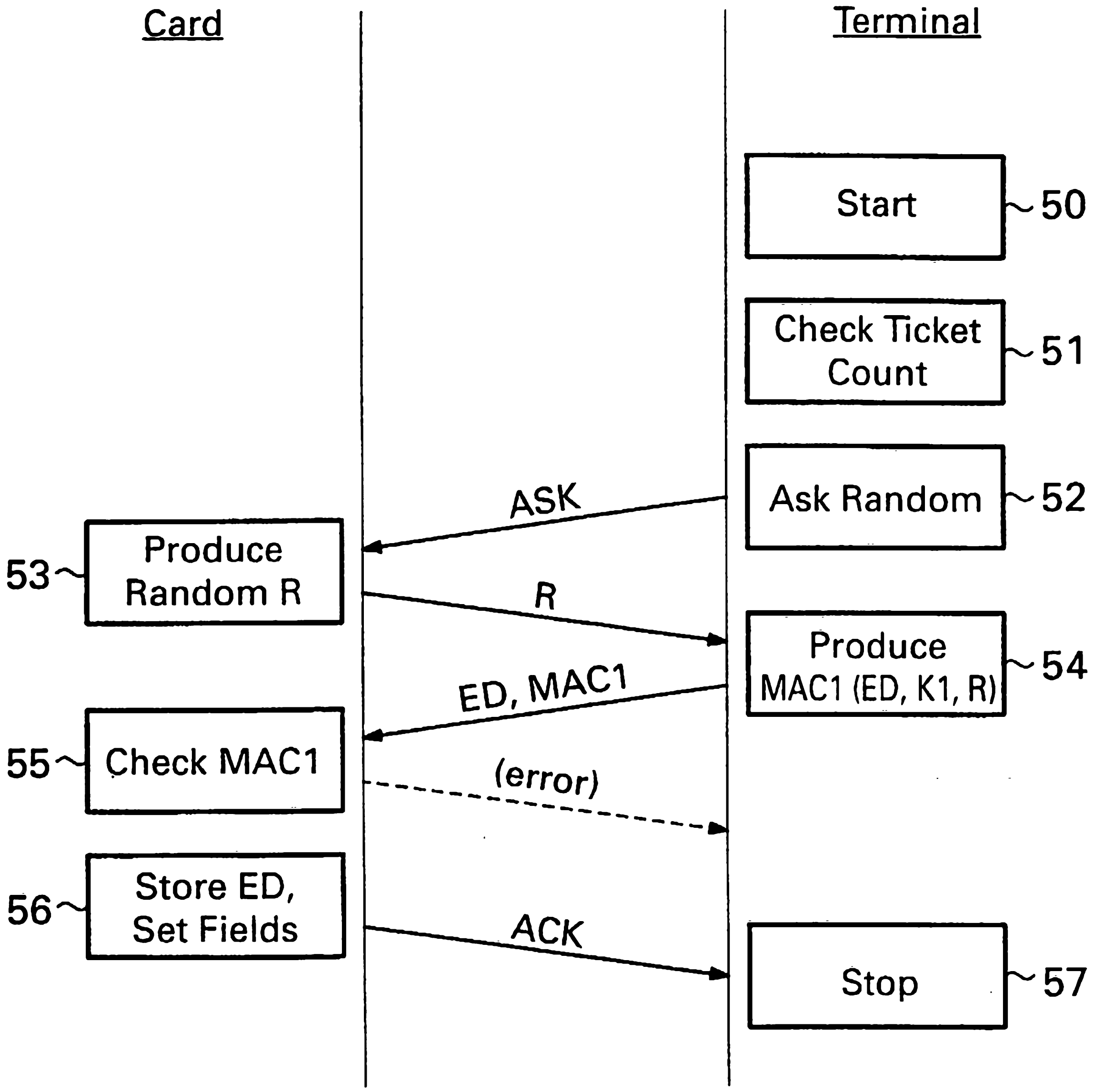

Card
Terminal
Start
50
Check Ticket Count
51
ASK
Ask Random
52
53
Produce Random R
R
Produce MAC1 (ED, K1, R)
54
ED, MAC1
55
Check MAC1
(error)
56
Store ED, Set Fields
ACK
Stop
57

Fig. 5

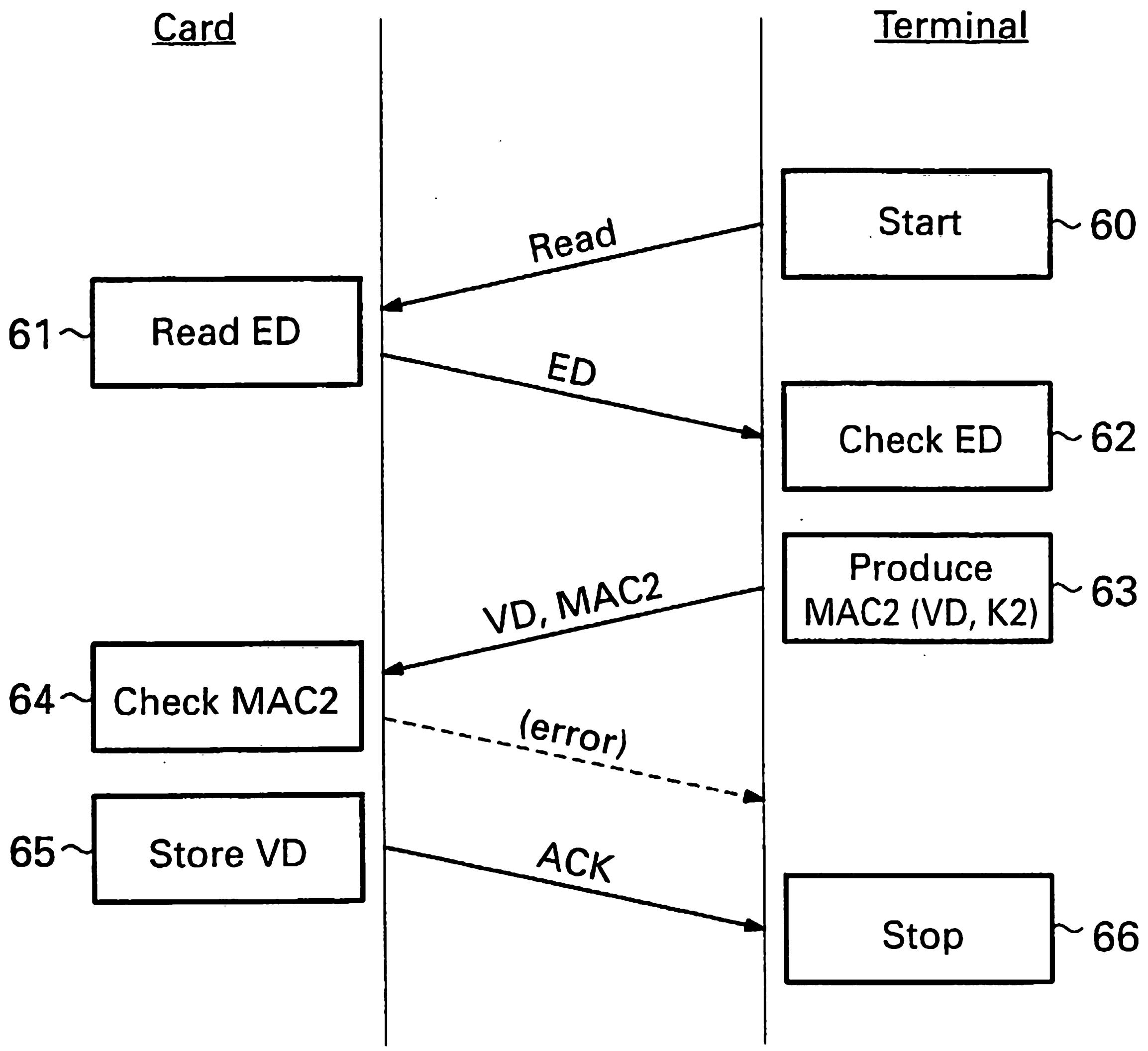

Card
Terminal
Start
60
Read
61
Read ED
ED
Check ED
62
Produce MAC2 (VD, K2)
63
VD, MAC2
64
Check MAC2
(error)
65
Store VD
ACK
Stop
66

Fig. 6

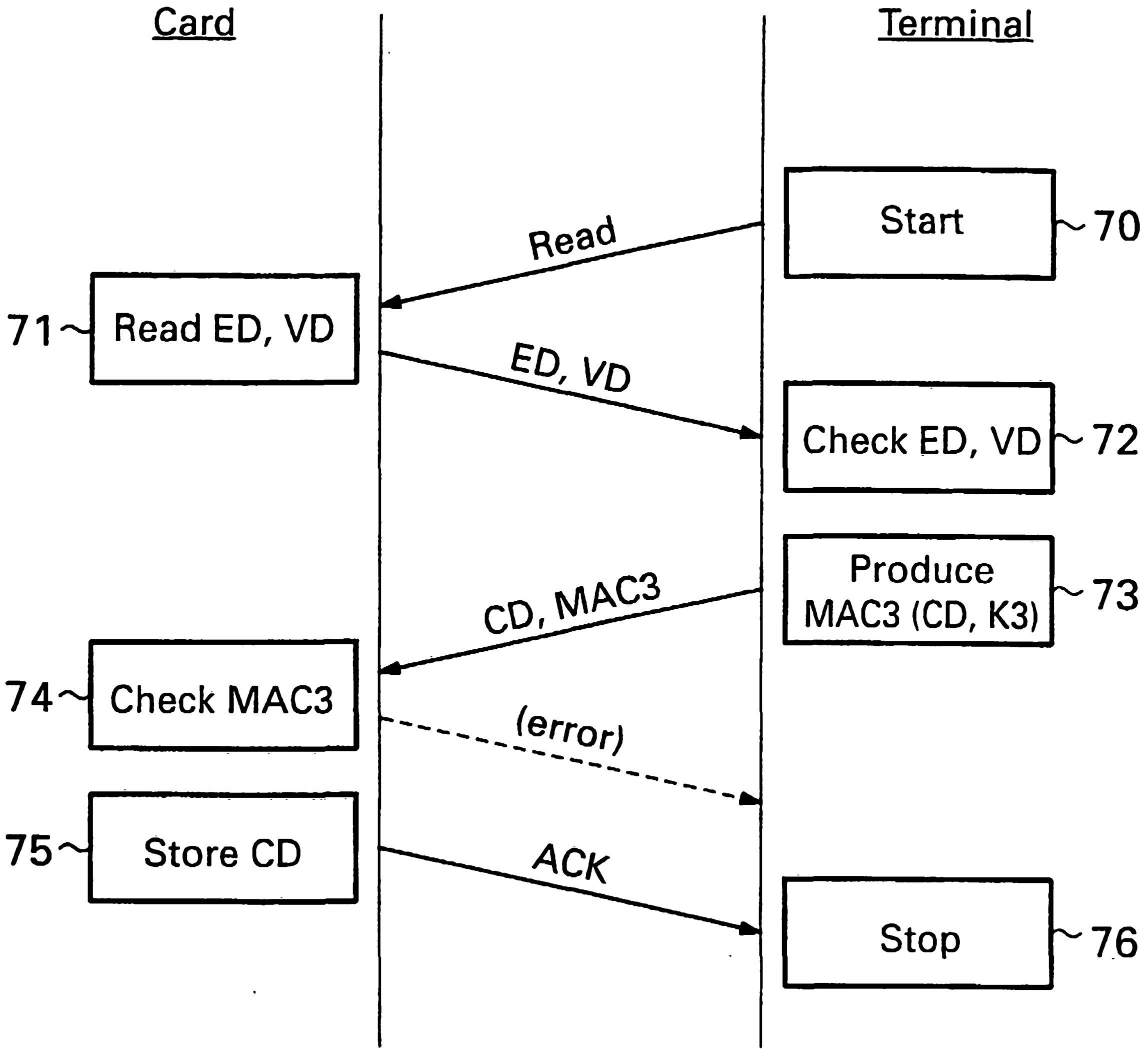

Card
Terminal
Start
70
Read
71
Read ED, VD
ED, VD
Check ED, VD
72
Produce MAC3 (CD, K3)
73
CD, MAC3
74
Check MAC3
(error)
75
Store CD
ACK
Stop
76

Fig. 7

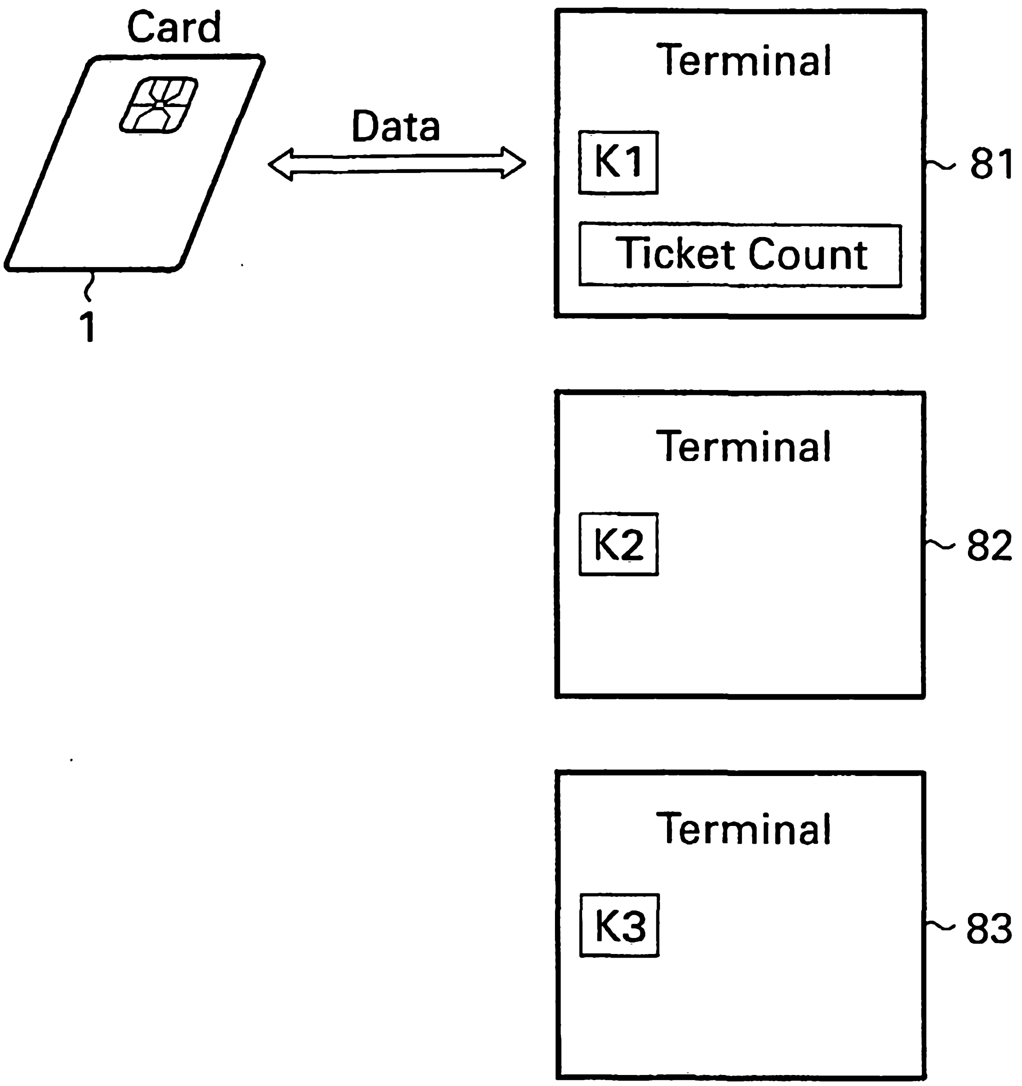

Card
1
Data
Terminal
K1
Ticket Count
81
Terminal
K2
82
Terminal
K3
83

Fig. 8