(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number : **0 388 840 B1**

(12) # EUROPEAN PATENT SPECIFICATION

(45) Date of publication of patent specification : **30.11.94 Bulletin 94/48**

(51) Int. Cl.^{5} : **G07B 17/04**

(21) Application number : **90105118.5**

(22) Date of filing : **19.03.90**

(54) **Security extension procedure for electronic remote setting meter.**

(30) Priority : **23.03.89 US 328099**

(43) Date of publication of application : **26.09.90 Bulletin 90/39**

(45) Publication of the grant of the patent : **30.11.94 Bulletin 94/48**

(84) Designated Contracting States : **DE FR GB**

(56) References cited :
EP-A- 0 096 386
GB-A- 2 080 202
GB-A- 2 178 696

(56) References cited :
GB-A- 2 188 874
GB-A- 2 188 878
US-A- 3 792 446
US-A- 4 097 923

(73) Proprietor : **NEOPOST INDUSTRIE**
113 rue Jean-Marin Naudin
F-92220 Bagneux (FR)

(72) Inventor : **Haines, John Gregory**
5341 Golden Gate Ave.
Oakland, California 94618 (US)

(74) Representative : **Weinmiller, Jürgen et al**
Lennéstrasse 9
Postfach 24
D-82336 Feldafing (DE)

EP 0 388 840 B1

Description

This invention relates generally to postage meters, and more particularly, to electronic postage meters capable of being remotely set.

With the advent of electronic postage meters, it has become possible to offer meter customers the feature of remotely adding postage credit (remote setting) to the postage meter. This feature enables the customer to more readily and conveniently remotely set the amount of postage in the meter. Extensive procedures and controls are used to insure that the postage meter amount is remotely set only when authorized. For example, the customer is usually required to enter a long code that varies each time the meter is remotely set. GB-A-2 080 202 discloses a remote postage meter charging system wherein a remote data center computer processes telephone calls from postage meter users, requesting of them information unique to their meter. This information is used to verify the authenticity of the call, and to update the record of the user stored in the computer. Then the computer formulates a combination based upon the identifying information and the amount of postage desired by the user. The combination is transmitted back to the user, who enters it into the postage meter. The postage meter compares the entered combination with an internally generated combination. If the entered combination matches the internally generated combination, the funding registers of the meter are increased by the new postage amount. However, such procedures are not infallible, particularly when the postage meter has been stolen and in the possession of a persistent person.

As a result and of these security concerns, some meters have been designed to detect the entry of an invalid code for remote setting a predetermined consecutive number of times. Once detected, the meter is disabled and must be returned to the factory to be enabled. Although effective for preventing unauthorized remote setting of the meter, this approach also causes problems for authorized users who accidently enter an incorrect remote setting code for the predetermined number of times.

The present invention provides a meter according to claim 1. In a preferred embodiment of the invention, for securely clearing the meter after it has been disabled without returning the meter to the factory, the meter generates a security lock code which is transmitted to a data center computer. The data center computer compares the security lock code with an internally generated security lock code. If the codes agree, the data center computer then generates a security clear code which is transmitted to the meter. The meter then compares this code with an internally generated security clear code. If these codes agree, then the meter clears a security lock flag thereby enabling the meter. As a result, the customer can subsequently remotely set the meter.

A further understanding of the nature and advantages of the present invention can be realized by the reference to the remaining portions of the specification and the attached drawings.

Fig. 1 is a block diagram of a preferred postage meter capable of being remotely set in the field by the customer;

Fig. 2 is a detailed flowchart of the manner in which the security lock flag is set;

Fig. 3 is a high level flowchart of the process for clearing the security lock flag;

Fig. 4 is a detailed flowchart of the procedure for the customer to obtain a security lock code generated by the meter;

Figs. 5a and 5b are detailed flowcharts of the procedure for the customer to confirm the security lock code with the data center computer; and

Fig. 6 is a detailed flowchart of the procedure for the customer to clear the security lock flag.

DESCRIPTION OF THE SPECIFIC EMBODIMENTS

Meter Overview: Structure

Fig. 1 is a block diagram of a preferred postage meter 10 that can be remotely set in the field by the customer. Meter 10 includes a print mechanism 12, accounting registers, and control electronics, all enclosed within a secure meter housing 13. A keyboard 14 and a display 16 provide the user interface. A connector 17 provides an electrical connection with a mailing machine for control of the printing process. The control electronics includes a digital microprocessor 18 which controls the operation of the meter, including the basic functions of printing and accounting for postage, and optional features such as department accounting and remote setting. The microprocessor is connected to a clock 20, a read only memory (ROM) 22, a random access memory (RAM) 24, and a battery augmented memory (BAM) 26.

ROM 22 is primarily used for storing non-volatile information such as software and data/function tables necessary to run the microprocessor. The ROM can only be changed at the factory. RAM 24 is used for intermediate storage of variables and other data during meter operation. BAM 26 is primarily used to store accounting information that must be kept when the meter is powered down. The BAM is also used for storing certain

flags and other information that is necessary to the functioning of the microprocessor. Such information includes meter identifying data such as the meter serial number and BAM initialization date, and a number of parameters relevant to the remote setting of the meter.

How the Security Lock Flag is Set

Fig. 2 is a detailed flowchart of the manner in which the security lock flag is set. Once the customer has a remote setting code for remotely setting the meter (or is attempting to remotely set the meter without the remote setting code), the customer puts the meter in a remote setting mode (step 40) by pressing a certain key sequence. The meter enters the remote setting mode by setting a mode register located in BAM (step 42). This prevents the meter from being used for printing purposes while being remotely set. The meter then determines whether the security lock flag has already been set (step 44). If so, the meter then displays a message and other needed information such as the security lock code and prompts for the security clear code (step 46). The customer is then unable to continue the remote setting process until the security lock flag has been cleared by the procedure shown in Figs. 3-6.

If the security lock flag has not already been set, the customer may then continue the remote setting procedure. The customer enters the remote setting code (step 48). The meter then checks whether the security lock flag has already been set (step 50). If so, then the customer is returned to step 48 as if the remote setting code were incorrect. If the security lock flag has not been set, then the meter determines whether the remote setting code is correct (step 52). If the code is correct, then the meter resets the counter to zero (step 53) and the customer may continue the remote setting procedure (which is not shown as it does not directly relate to the present procedure). If the code is not correct, then the meter checks to see whether the customer has already attempted over a predetermined number of allowed attempts (step 56). If the customer has attempted less than the predetermined number of allowed attempts, then the meter returns the customer to the step of entering the remote setting code. If the customer has attempted over the predetermined number of allowed attempts then the security lock flag in BAM is set and the meter returns the customer to the step of entering the remote setting code.

Method for Clearing the Meter Security Lock Flag

Fig. 3 is a high level flow chart of the process necessary for clearing the security lock flag in the meter. In a first stage 60, the customer obtains a security lock code generated by the meter. This security lock code is essentially a password to the data center computer, and is based upon a combination of factors, the combination of which only the data center computer would know. In a second stage 61, the customer confirms the security lock code with the data center computer. Upon confirmation from the computer, the computer provides a security clear code back to the customer. The security clear code is essentially a password from the data center computer to the meter stating that it is permissible to clear the security lock flag. In a third stage 62, the customer enters the security clear code to the meter. The meter confirms the security clear code and clears the security lock flag.

Fig. 4 is a detailed flowchart of stage 60 as shown in Fig. 3. In a first step 40′ (corresponding to step 40 of Figure 2), the customer presses a certain key sequence, causing the meter to enter a remote setting mode. The meter enters the remote setting mode by setting a mode register located in BAM (step 42′).

The meter then determines whether the security lock flag has been set (step 44′). If so, the meter then displays a message and other needed information and prompts for the security clear code (step 46′). In a first embodiment, the meter displays the meter serial number, the meter BAM initialization date, and the encrypted security lock code. The BAM initialization date is preferably a four digit number wherein the four digits YDDD express the date in which the meter was last initialized. The DDD stands for the number of days since December 31, and Y is the least significant digit of the year in which the meter was initialized. In a second embodiment, the meter displays the above numbers and the Control Register amount or some other meter specific identifying information. The Control Register contains the amount of postage the meter has printed since the meter has been initialized plus the amount the meter is currently authorized to print. The customer should write these numbers down on a separate piece of paper for later use in the method.

Two input numbers used by the meter and the computer to generate encrypted codes are the configuration transaction identifier ("CTID") and the setting transaction identifier ("STID"). They are both specific to the meter and dependent upon the meter serial number. They may also be incremented after each use. The CTID is normally used for reconfiguring the meter functions and clearing the security lock flag and the STID is normally used for resetting the meter postage. Separate numbers are used for the separate procedures in order to maximize security and minimize complexity caused by interdependence. The encryption routine is described in

greater detail.

Figs. 5a and 5b are detailed flowcharts of stage 61 as shown in Fig. 3. The customer establishes communication with the data center computer over a standard telephone. In the first and second embodiments, the customer may communicate to the data center computer on a touch tone telephone by pressing the key. Alternative embodiments may utilize a telephone communications device that includes a user or meter interface and a modem, or by voice recognition over the telephone.

The customer first enters a request code for clearing the security extension flag (step 70). The customer then enters the customer account number (step 72) and the meter serial number which was given above can be found on the exterior of the meter (step 74).

The data center computer then determines whether the serial number is valid given the customer account number (step 76). If the serial number is valid then the customer may continue, otherwise the customer is notified (step 78) and is given the opportunity to decide whether to try again (step 80). If the customer does not decide to try again, the customer should then contact his agent in order to determine how to clear up this problem.

If the serial number is valid, then the customer enters the amount of the Control Register (step 84) obtained earlier in the procedure. The customer then enters the security lock code which was also obtained from the meter in the procedure above (step 86). The computer then generates a security lock code in a like manner (step 88) and compares that code to that entered by the customer (step 90). If the codes are not equal, then the customer is notified (step 92) and is given the opportunity to try again.

If the codes are equal, then the computer determines whether the Control Register amount is valid (step 96). The Control Register amount is valid if the amount is equal to any prior Control Register amounts stored on the computer. The Control Register amount is not valid if it is greater than or equal to the present computer Control Register amount. If the Control Register amount is not valid, then the customer is notified and the occurrence of the invalid Control Register amount is logged in the computer (step 98).

If the Control Register amount is valid, then the customer enters the current remote setting code (step 100). The computer then determines whether it is a valid code (step 102). If the remote setting code is not valid, then the computer passes the customer to a live operator for assistance (step 104). If the remote setting code is valid, then the computer generates a security extension code (step 106), increments the CTID (step 108), flags that this event has occurred (step 110), and displays or returns the security extension code to the customer for use further in this method (step 112).

Fig. 6 is a detailed flowchart of stage 62 shown above in Fig. 3. The customer enters the security clear code obtained from the computer into the meter (step 120). The meter then generates its own security clear code (step 122) and compares the computer generated code with the meter generated code (step 124). If the codes are not equal, then the customer is notified (step 126) and the customer is given an opportunity to try again or contact an agent (step 130). If the codes are equal, then the meter increments the CTID such that it is equal to the CTID stored in the computer (step 132), the meter clears the security lock flag (step 134) and the meter enters the remote setting mode by changing the mode register in BAM (step 136).

Encryption Technique

In order to perform the above procedure in the secure manner and to confirm certain data, the security lock code and the security clear code are generated by an encryption routine, stored both in the meter ROM and in the data center computer. The encryption routine is a nonlinear algorithm that generates a number that is apparently random to an outside person. The encryption routine is performed by an encryption program in combination with a permanent encryption table. In the first and second embodiments, encryption routine uses a 16 digit (or 64 bit) key and a 16 digit input number.

In the first embodiment, the security lock code is generated by the encryption routine performed on the CTID as the key and a combination of the STID and Control Register amount as the input number. In the second embodiment, the key is composed of the serial number and the BAM initialization and the input number is composed of the STID and the Control Register.

In the preferred and second embodiments, the security clear flag is generated by the encryption routine performed on the CTID as the key and a combination of the meter serial number and the STID as the input number.

The CTID is a 16 digit number that is stored in BAM. The initial value of the CTID is obtained by performing an algorithm upon the BAM initialization date in combination with the meter serial number. The BAM initialization date is used to prevent starting with the same CTID everytime the meter is initialized. The algorithm is not stored in the meter for security reasons. The initial CTID is stored in BAM during the initialization process at the factory. The CTID is incremented by a non-linear algorithm within the meter after the security lock flag

is cleared.

The codes generated by the encryption routine are 16-digits long. The lower digits of the codes are then communicated to the customer by the meter or the data center computer. The number of lower digits that are communicated is determined by the HSL value (see Appendix A for details).

Conclusion

It can be seen that the present invention provides a secure and efficient technique for allowing the meter to be cleared in the field.

While the above is a complete description of the specific embodiments of the invention, various modifications, alternative constructions, and equivalents may be used. For example, the electronics of the resettable meter may be structured differently. In addition, the security lock flag or another flag can be used to prevent other forms of memory modification when an improper code is entered a predetermined number of times. Furthermore, the encryption key used to generate the request codes could be composed of a meter cycle counter instead of the meter serial number. Other security measures may be implemented such as requiring periodic inspection of the meter.

Therefore, the above description and illustration should not be taken as limiting the scope of the present invention, which is defined by the appended claims.

APPENDIX A

VARIABLE LENGTH SECURITY CODES

An algorithm is used to generate an apparently random code with multiple digits. However, only a selected number of digits (usually the lower digits) of this code needs to be used in most applications. The number of digits needed depends upon the level of security needed. It is preferred to use as few digits as possible to decrease the number of keystrokes that must be entered, thereby increasing convenience and decreasing the potential for error.

As a result, a variable has been created which defines the overall level of security required by the meter or data center computer. This variable is called the high security length (HSL) value.

Each code generated by the meter or data center computer has a variable length of digits used depending upon the HSL value. That is, if the HSL value is 1, then the security lock code should have 6 digits. If the HSL value is higher, then the security lock code should be longer. Other codes may have different lengths for a given HSL value, but each code will increase or decrease in length if the HSL value is increased or decreased.

This predetermined relationship between code length and the HSL value allows the meter manufacturer to increase or decrease security for the meter without having to recover and initialize each meter. Changes in the HSL value are communicated to the meter when performing a remote meter configuration.

In an alternative embodiment, multiple security variables may be used to vary the lengths of individual or groups of codes without affective the length of the remaining codes.

Claims

1. An electronic postage meter having data stored in a memory (26) that can be modified by the by entry

of a remote setting code, the meter comprising:
(a) detection means (18, 52-56) for detecting the entry of an invalid remote setting code a predetermined number of times;
(b) prevention means (18, 50, 58), responsive to the detection means, for selectively preventing the modification of the data in the memory upon the entry of an invalid code the predetermined number of times;
(c) generating means (18, 122) for generating a meter code;
(d) entry means (14, 120) for entering a non-meter code;
(e) comparison means (13, 124), coupled to the generating means and the entry means, for comparing the meter and non-meter codes; characterized by
(f) enabling means (18, 134), responsive to the comparison means, for disabling the prevention means upon the meter and non-meter codes being equal.

2. The electronic postage meter of claim 1 further comprises;
(a) second generating means (18, 60) for generating a second meter code; and
(b) display means (16, 46), coupled to the second generating means, for displaying the second meter code.

3. The electronic postage meter of claims 1 or 2, having a postage amount stored in a memory (26) that can be remotely set by entry of a remote setting code by the meter user,
said prevention means preventing the postage amount from being remotely set upon the entry of an invalid code the predetermined number of times.

4. The electronic postage meter of claim 3 further comprising a print means (12) for printing postage not greater than the postage amount.

5. The electronic postage meter of claim 4 wherein the prevention means further prevents the print means for printing postage upon the entry of an invalid remote setting code the predetermined number of times.

6. The electronic postage meter of claim 3 further comprising enabling means (18, 70) for enabling the postage amount to be remotely set upon the entry of a second non-meter code.

Patentansprüche

1. Elektronische Frankiermaschine, in der Daten in einem Speicher (26) gespeichert sind, die durch Eingabe eines Fernladekodes verändert werden können, wobei die Maschine enthält:
(a) Mittel (18, 52 bis 56) zur Erfassung einer vorbestimmten Anzahl von Wiederholungen der Eingabe eines ungültigen Fernladekodes,
(b) Verhinderungsmittel (18, 50, 58), die aufgrund der Erfassungsmittel selektiv die Veränderung der Daten im Speicher nach einer vorbestimmten Anzahl von Wiederholungen der Eingabe eines ungültigen Kodes zu verhindern,
(c) Mittel (18, 122), um einen Frankiermaschinenkode zu erzeugen,
(d) Mittel (14, 120) zur Eingabe eines nicht von der Frankiermaschine stammenden Kodes,
(e) Vergleichsmittel (13, 124), die an die Mittel zur Erzeugung eines Kodes und an die Eingabemittel gekoppelt sind, um den Kode der Maschine und den Kode von außerhalb der Maschine miteinander zu vergleichen, gekennzeichnet durch
(f) Freigabemittel (18, 134), die von den Vergleichsmitteln gesteuert werden, um die Verhinderungsmittel wirkungslos zu machen, wenn die beiden Kodes gleich sind.

2. Elektronische Frankiermaschine nach Anspruch 1, die weiter aufweist:
(a) zweite Mittel (18, 60) zur Erzeugung eines zweiten Frankiermaschinenkodes,
(b) und Anzeigemittel (16, 46), die mit den zweiten Mitteln gekoppelt sind, um den zweiten Frankiermaschinenkode anzuzeigen.

3. Elektronische Frankiermaschine nach Anspruch 1 oder Anspruch 2, die einen Frankierkreditbetrag im Speicher (26) enthält, der aus der Ferne durch Eingabe eines Fernladekodes durch den Benutzer der Frankiermaschine gesetzt werden kann, wobei die Verhinderungsmittel das Setzen des Frankierkreditbetrags aus der Ferne verhindern, wenn eine vorbestimmte Anzahl von Wiederholungen der Eingabe ei-

nes ungültigen Kodes erfolgt ist.

4. Elektronische Frankiermaschine nach Anspruch 3, die weiter Druckmittel (12) zum Drucken von Frankierbeträgen aufweist, die den Frankierkreditbetrag nicht überschreiten.

5. Elektronische Frankiermaschine nach Anspruch 4, bei der die Verhinderungsmittel weiter die Druckmittel am Drucken von Frankierbeträgen nach einer vorbestimmten Anzahl von Wiederholungen der Eingabe eines ungültigen Fernladekodes hindern.

6. Elektronische Frankiermaschine nach Anspruch 3, die weiter Freigabemittel (18, 70) aufweist, um den Frankierkreditbetrag aus der Ferne nach Eingabe eines zweiten, nicht von der Maschine kommenden Kodes zu erlauben.

Revendications

1. Machine à timber électronique comportant, mémorisées dans une mémoire (26), des données que l'on peut modifier en entrant un code de télérevalorisation, la machine comprenant:
   (a) des moyens de détection (18, 52-56) pour détecter l'entrée d'un code de télérevalorisation invalide un nombre prédéterminé de fois;
   (b) des moyens d'empêchement (18, 50, 58), sensibles aux moyens de détection, pour empêcher sélectivement la modification des données en mémoire lors de l'entrée d'un code invalide le nombre prédéterminé de fois;
   (c) des moyens de génération (18, 122) pour générer un code fourni par la machine à timbrer;
   (d) des moyens d'entrée (14, 120) pour entrer un code non fourni par la machine à timbrer;
   (e) des moyens de comparaison (13, 124), couplés aux moyens de génération et aux moyens d'entrée, pour comparer le code fourni par la machine et le code non fourni par la machine;
   machine à timber caractérisée par
   (f) des moyens de validation (18, 134), sensibles aux moyens de comparaison, pour invalider les moyens d'empêchement lorsque le code fourni par la machine et le code non fourni par la machine sont égaux.

2. Machine à timbrer électronique selon la revendication 1, comportant en outre:
   (a) des seconds moyens de génération (18, 60) pour générer un second code fourni par la machine; et
   (b) des moyens d'affichage (16, 46), couplés aux seconds moyens de génération, pour afficher le second code fourni par la machine.

3. Machine à timbrer électronique selon les revendications 1 ou 2, comportant une valeur du crédit de timbrage qui est mémorisée dans une mémoire (26) et que l'utilisateur de la machine à timbrer peut télérevaloriser en entrant un code de télérevalorisation, lesdits moyens d'empêchement empêchant la valeur du crédit de timbrage d'être télérevalorisé lors de l'entrée d'un code invalide le nombre prédéterminé de fois.

4. Machine à timbrer électronique selon la revendication 3, comportant en outre des moyens d'impression (12) pour imprimer des timbrages pour une valeur non supérieure à la valeur du crédit de timbrage.

5. Machine à timber électronique selon la revendication 4, dans laquelle les moyens d'empêchement empêchent en outre les moyens d'impression d'imprimer un timbrage lors de l'entrée d'un code invalide de télérevalorisation le nombre prédéterminé de fois.

6. Machine à timbrer électronique selon la revendication 3, comportant en outre des moyens de validation (18, 70) pour valider la valeur du crédit de timbrage à télérevaloriser lors de l'entrée d'un second code non fourni par la machine.

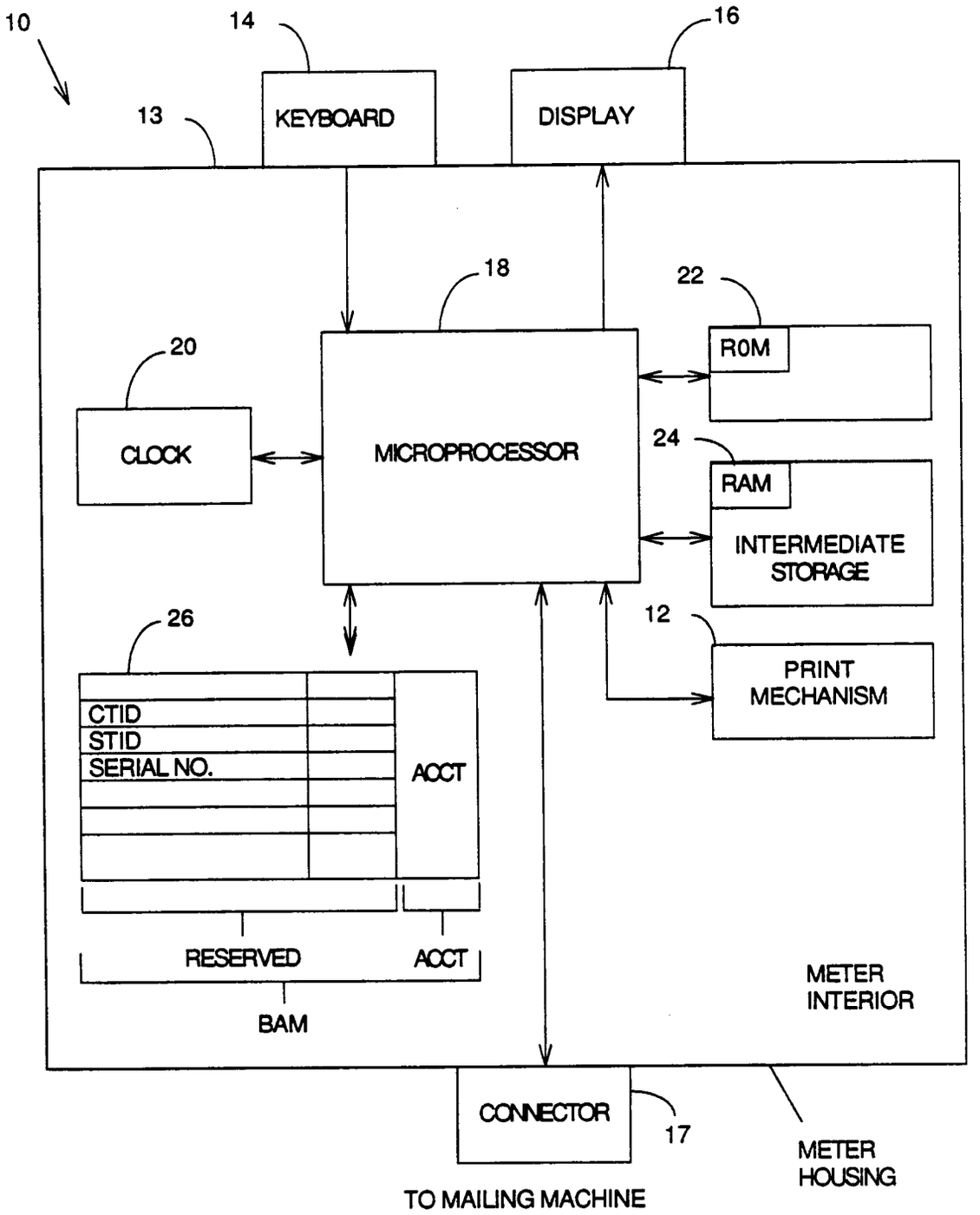
10
14
16
13
KEYBOARD
DISPLAY
18
22
20
ROM
CLOCK
MICROPROCESSOR
24
RAM
INTERMEDIATE STORAGE
12
PRINT MECHANISM
26
CTID
STID
SERIAL NO.
ACCT
RESERVED
ACCT
BAM
METER INTERIOR
CONNECTOR
17
METER HOUSING
TO MAILING MACHINE

FIG. 1

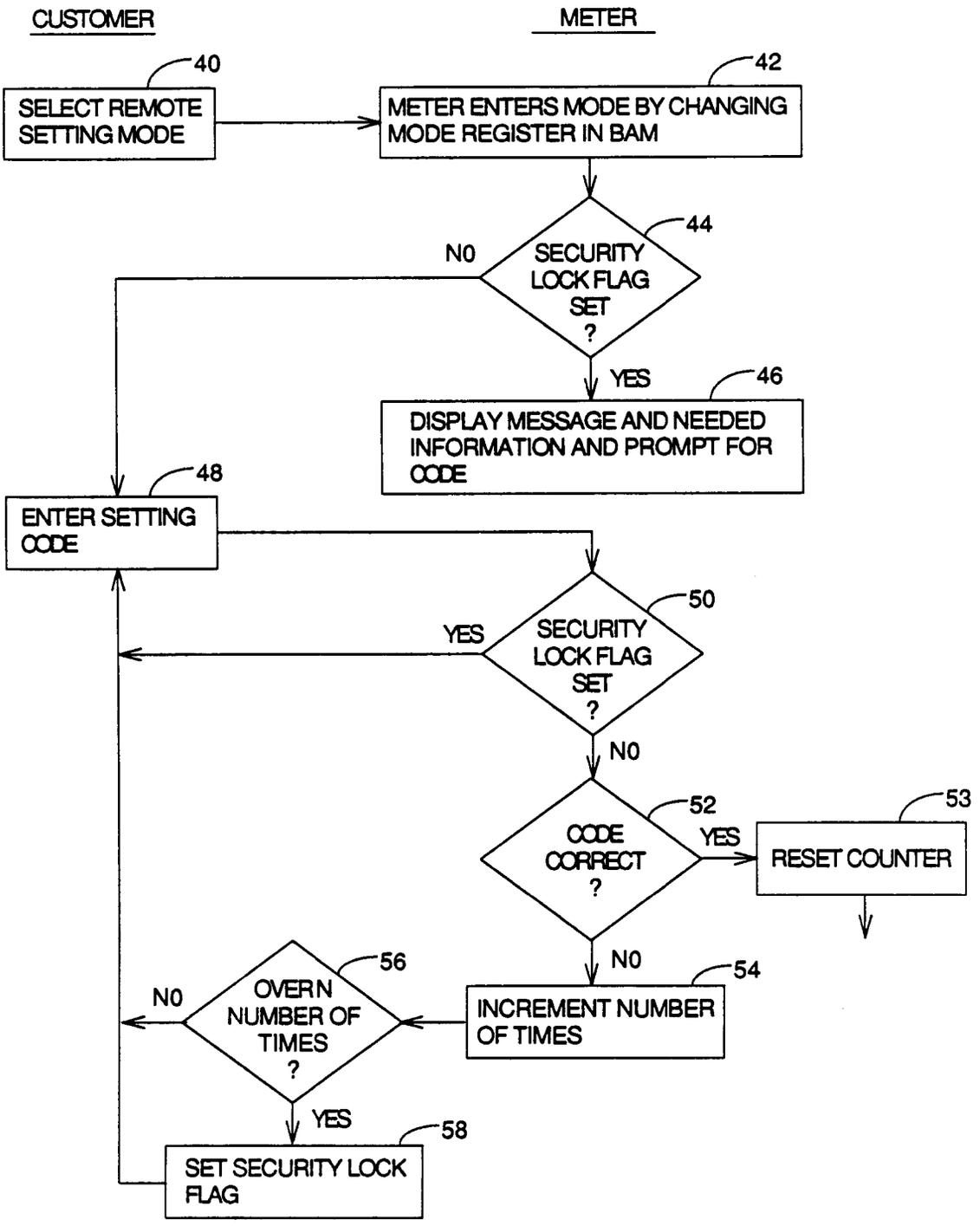
CUSTOMER
METER
40
SELECT REMOTE SETTING MODE
42
METER ENTERS MODE BY CHANGING MODE REGISTER IN BAM
44
SECURITY LOCK FLAG SET ?
NO
YES
46
DISPLAY MESSAGE AND NEEDED INFORMATION AND PROMPT FOR CODE
48
ENTER SETTING CODE
50
SECURITY LOCK FLAG SET ?
YES
NO
52
CODE CORRECT ?
YES
53
RESET COUNTER
NO
54
INCREMENT NUMBER OF TIMES
56
OVER N NUMBER OF TIMES ?
NO
YES
58
SET SECURITY LOCK FLAG

FIG. 2

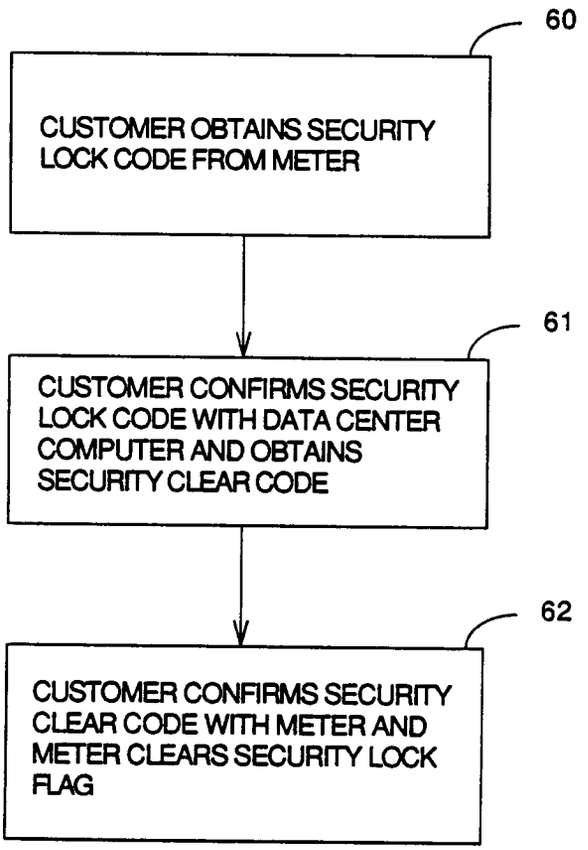
60
CUSTOMER OBTAINS SECURITY LOCK CODE FROM METER
61
CUSTOMER CONFIRMS SECURITY LOCK CODE WITH DATA CENTER COMPUTER AND OBTAINS SECURITY CLEAR CODE
62
CUSTOMER CONFIRMS SECURITY CLEAR CODE WITH METER AND METER CLEARS SECURITY LOCK FLAG

FIG. 3

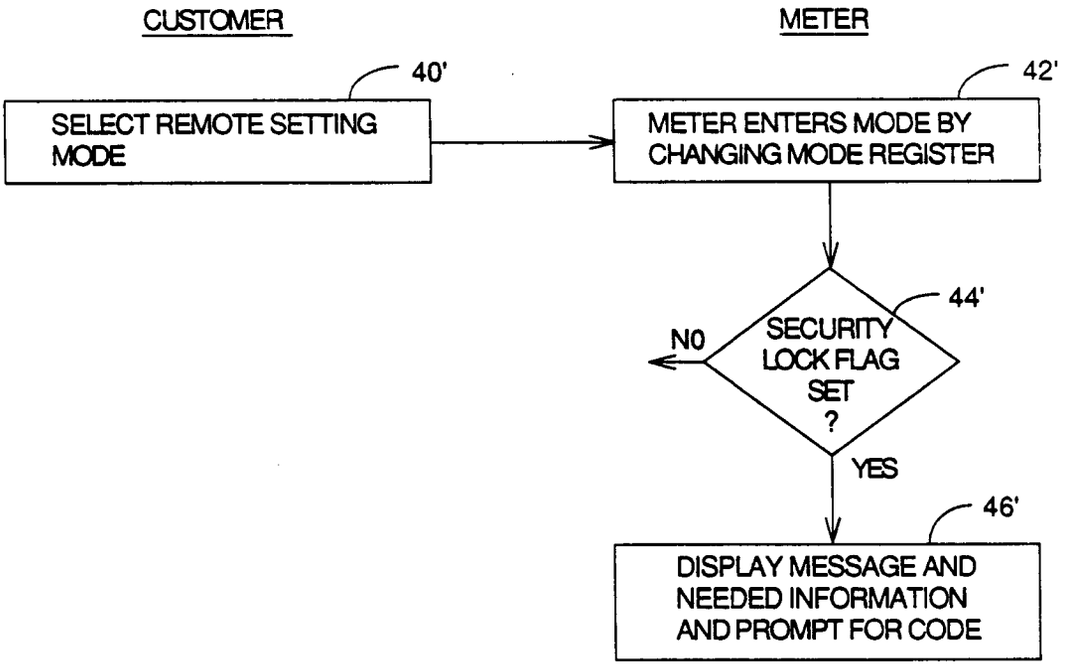
CUSTOMER
METER
40'
SELECT REMOTE SETTING MODE
42'
METER ENTERS MODE BY CHANGING MODE REGISTER
44'
SECURITY LOCK FLAG SET ?
NO
YES
46'
DISPLAY MESSAGE AND NEEDED INFORMATION AND PROMPT FOR CODE

FIG. 4

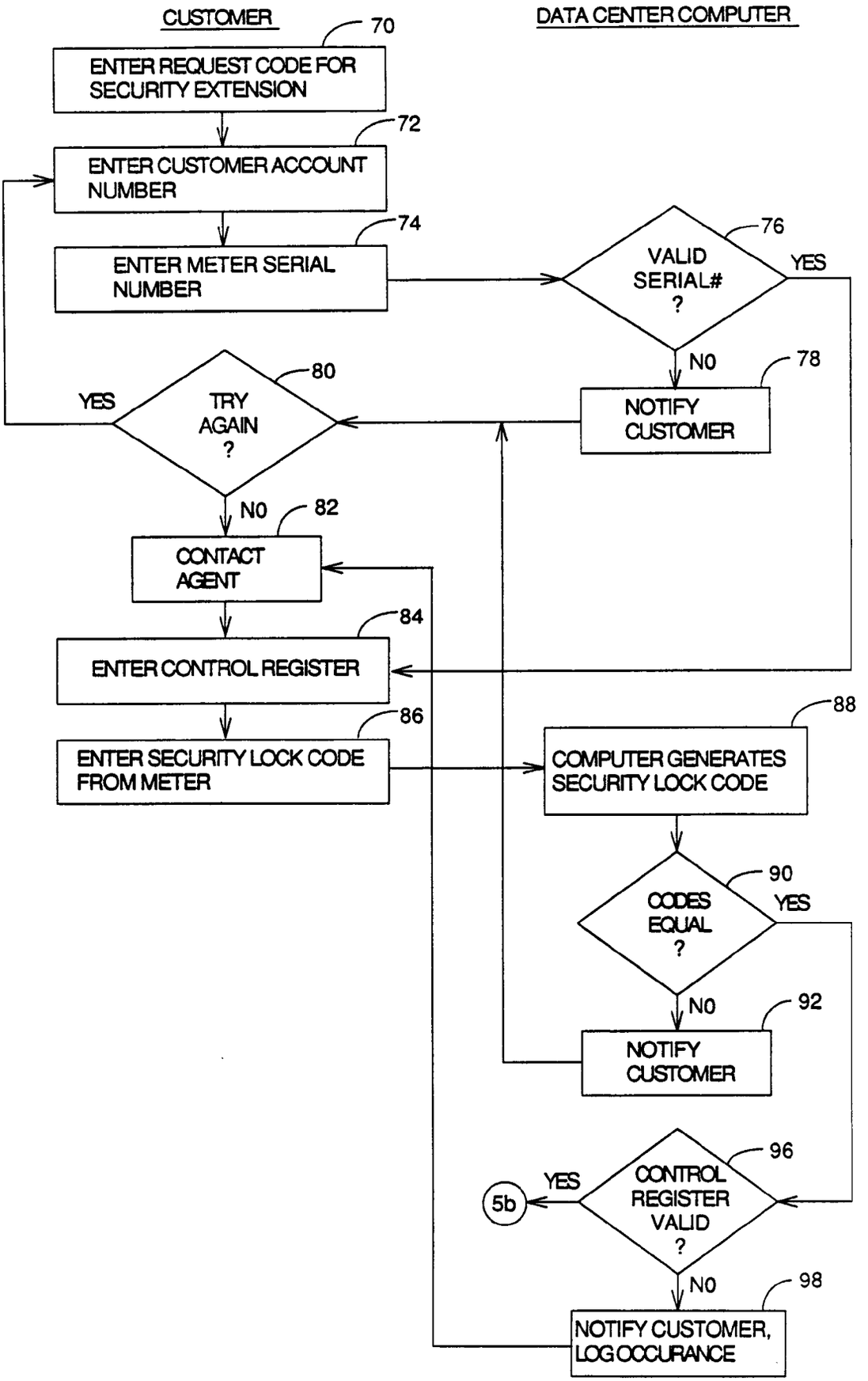
CUSTOMER
DATA CENTER COMPUTER
70
ENTER REQUEST CODE FOR SECURITY EXTENSION
72
ENTER CUSTOMER ACCOUNT NUMBER
74
ENTER METER SERIAL NUMBER
76
VALID SERIAL# ?
YES
NO
78
NOTIFY CUSTOMER
80
TRY AGAIN ?
YES
NO
82
CONTACT AGENT
84
ENTER CONTROL REGISTER
86
ENTER SECURITY LOCK CODE FROM METER
88
COMPUTER GENERATES SECURITY LOCK CODE
90
CODES EQUAL ?
YES
NO
92
NOTIFY CUSTOMER
96
CONTROL REGISTER VALID ?
YES
5b
NO
98
NOTIFY CUSTOMER, LOG OCCURANCE

FIG. 5a

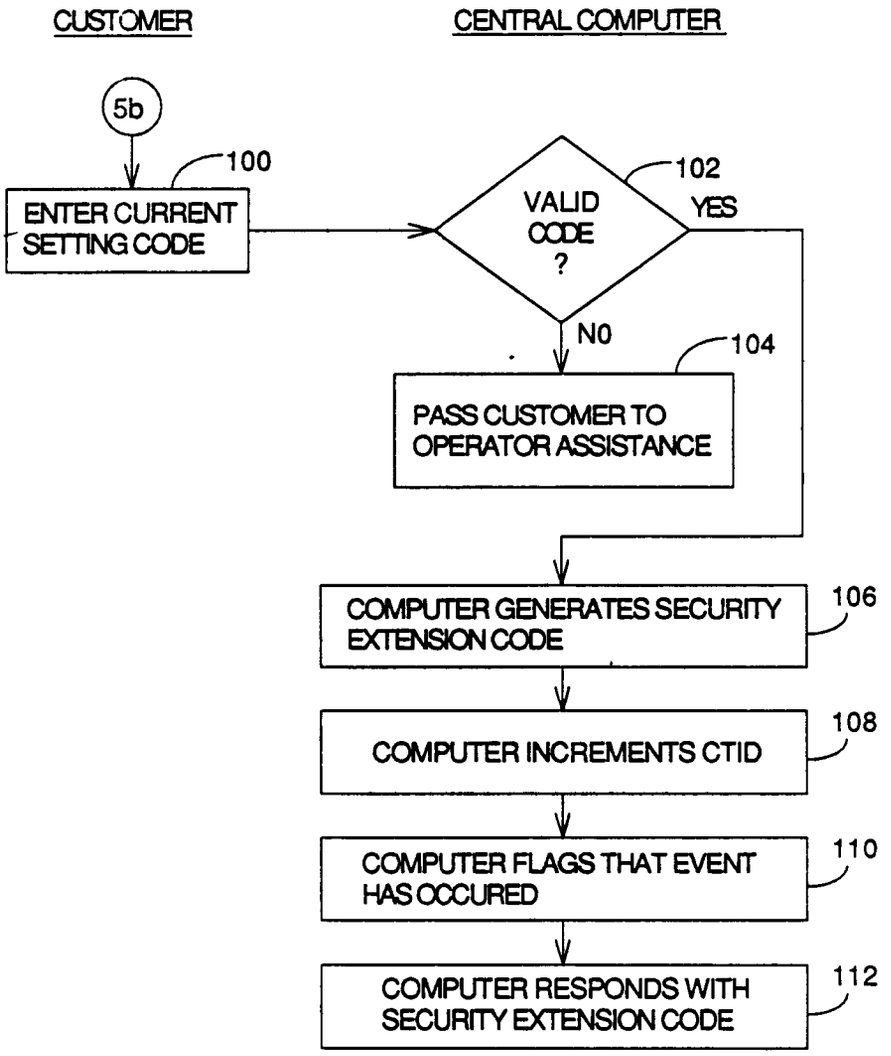
CUSTOMER
CENTRAL COMPUTER
5b
100
ENTER CURRENT SETTING CODE
102
VALID CODE ?
YES
NO
104
PASS CUSTOMER TO OPERATOR ASSISTANCE
COMPUTER GENERATES SECURITY EXTENSION CODE
106
COMPUTER INCREMENTS CTID
108
COMPUTER FLAGS THAT EVENT HAS OCCURED
110
COMPUTER RESPONDS WITH SECURITY EXTENSION CODE
112

FIG. 5b

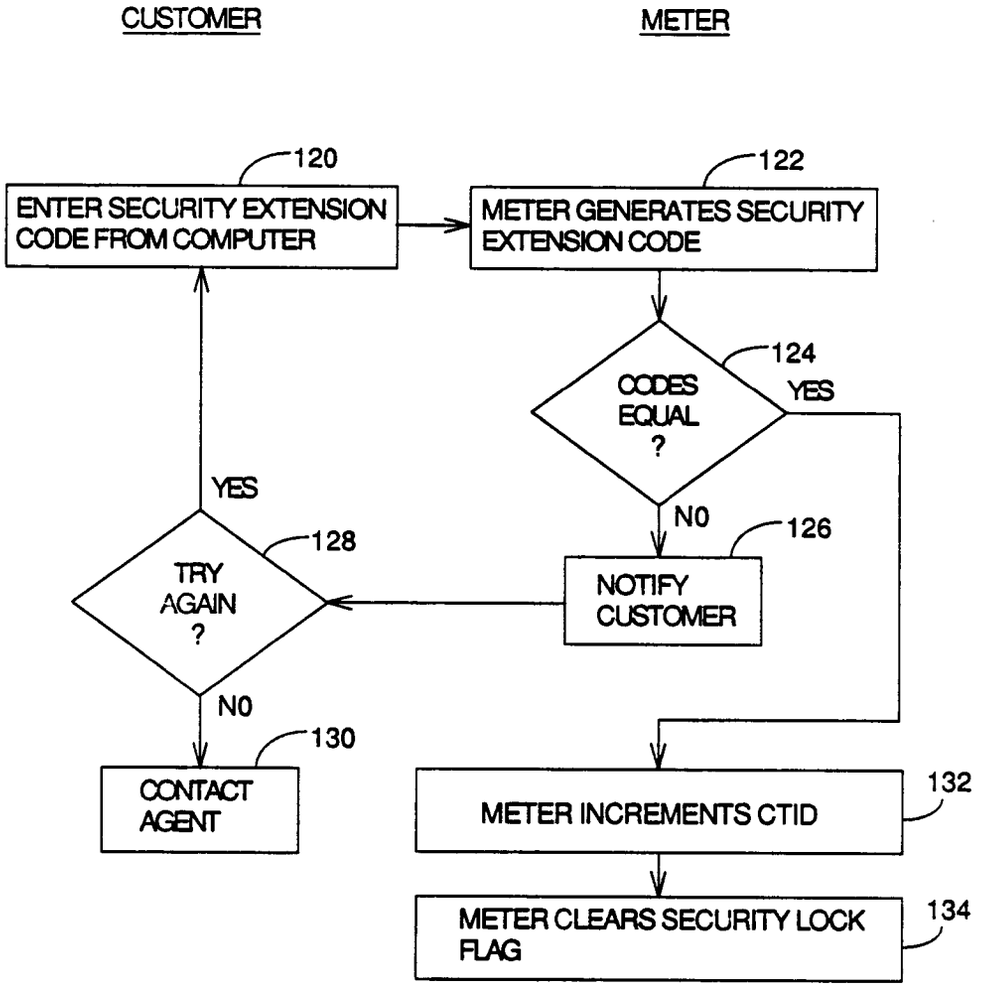
CUSTOMER
METER
120
ENTER SECURITY EXTENSION CODE FROM COMPUTER
122
METER GENERATES SECURITY EXTENSION CODE
124
CODES EQUAL ?
YES
NO
126
NOTIFY CUSTOMER
128
TRY AGAIN ?
YES
NO
130
CONTACT AGENT
132
METER INCREMENTS CTID
134
METER CLEARS SECURITY LOCK FLAG

FIG. 6