OPIC
Office de la propriété intellectuelle du Canada

CIPO
Canadian Intellectual Property Office

(12) (19) (CA) **Brevet-Patent**

(11) (21) (C) **2,193,022**

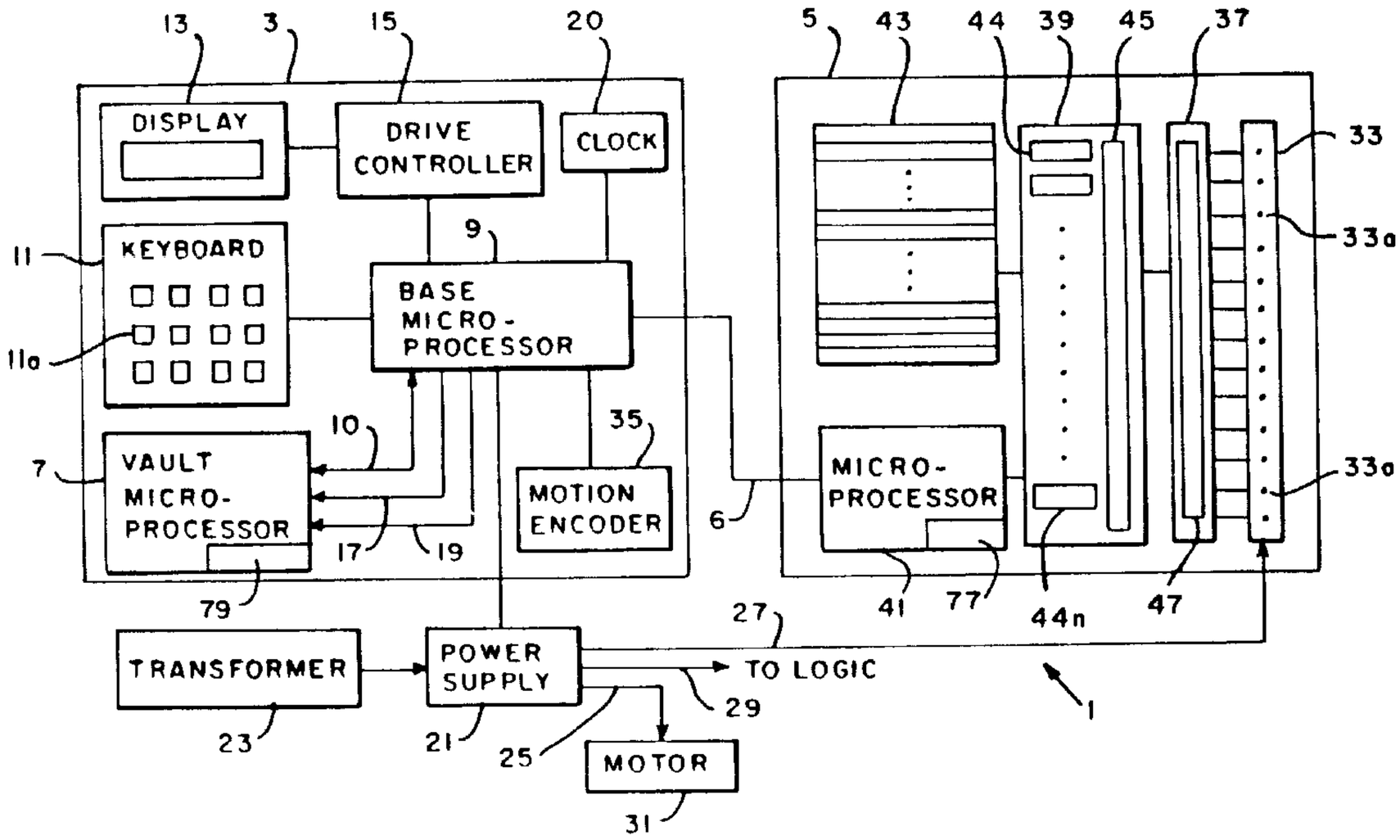
(22) 1996/12/16
(43) 1997/06/28
(45) 2001/07/03

(72) Dolan, Donald T., US
(72) French, Dale A., US
(72) Lawton, Kathryn V., US
(73) PITNEY BOWES INC., US

(51) Int.Cl.[6] G07B 17/02
(30) 1995/12/27 (08/579,506) US

(54) METHODE ET APPAREIL D'AFFRANCHISSEMENT METTANT EN OEUVRE L'OPERATION DE DEBIT AVANT L'IMPRESSION DE L'EMPREINTE D'AFFRANCHISSEMENT

(54) METHOD AND APPARATUS FOR ENSURING DEBITING IN A POSTAGE METER PRIOR TO ITS PRINTING A POSTAL INDICIA



(57) A method for ensuring for each postage transaction in a postage meter having a vault subsystem and a printing subsystem that debiting occurs prior to printing of a postal indicia includes authenticating the postage transaction as being valid, performing debiting within the vault subsytem, sending an encrypted debit certificate from the vault subsystem to the printing subsytem, independently recreating the encrypted debit certificate in the printing subsystem, comparing the encrypted debit certificate to the recreated encrypted debit certificate to ascertain if a predetermined relationship exists therebetween, and initiating printing of the postal indicia only upon determination of the existence of the predetermined relationship. An apparatus incorporates the method.

METHOD AND APPARATUS FOR ENSURING DEBITING IN A POSTAGE METER PRIOR TO ITS PRINTING A POSTAL INDICIA

ABSTRACT OF THE DISCLOSURE

A method for ensuring for each postage transaction in a postage meter having a vault subsystem and a printing subsystem that debiting occurs prior to printing of a postal indicia includes authenticating the postage transaction as being valid, performing debiting within the vault subsytem, sending an encrypted debit certificate from the vault subsystem to the printing subsytem, independently recreating the encrypted debit certificate in the printing subsystem, comparing the encrypted debit certificate to the recreated encrypted debit certificate to ascertain if a predetermined relationship exists therebetween, and initiating printing of the postal indicia only upon determination of the existence of the predetermined relationship. An apparatus incorporates the method.

2193022

METHOD AND APPARATUS FOR ENSURING DEBITING IN A POSTAGE METER PRIOR TO ITS PRINTING A POSTAL INDICIA

BACKGROUND OF THE INVENTION

This invention relates to a method and apparatus for securely authorizing performance of printing in a distributed postage meter system, and more particularly to a method and apparatus for ensuring debiting in a postage meter prior to its printing a postal indicia.

Traditional postage meters imprint an indicia on a mailpiece as evidence that postage has been paid. These traditional postage meters create the indicia using a platen or a rotary drum which are moved into contact with the mailpiece to imprint the indicia thereon. While traditional postage meters have performed admirably over time, they are limited by the fact that if the indicia image significantly changes, a new platen or rotary drum will have to be produced and placed in each meter. Accordingly, newer postage meters now take advantage of modern digital printing technology to overcome the deficiencies of traditional meters. The advantage of digital printing technology is that since the digital printhead is software driven, all that is required to change an indicia image is new software. Thus, the flexibility in changing indicia images or adding customized ad slogans is significantly increased.

Modern digital printing technology includes thermal ink jet (bubble jet), piezoelectric ink jet, thermal printing techniques, and LED and Laser Xerographic printing which all operate to produce images by dot-matrix printing. In dot-matrix ink jet printing individual print elements in the printhead (such as resistors or piezoelectric elements) are either electronically stimulated or not stimulated to expel or not expel, respectively, drops of ink from a reservoir onto a substrate. Thus, by controlling the timing of the energizing of each of the individual print elements in conjunction with

the relative movement between the printhead and the mailpiece, a dot-matrix pattern is produced in the visual form of the desired indicia.

While digital printing technology provides the advantages discussed above, it also permits the size and weight of the meter to be dramatically reduced since the digital printhead is very small in size. Moreover, from an electronics architecture viewpoint the entire meter is now a distributed system having its various functions divided between numerous subsystems such as a vault subsystem and a printer subsystem. Each of the subsystems can communicate with each other but can also have independent processing capabilities permitting parallel processing of information and increased efficiency in operation. However, the downside of the above described distributed system is that when data is transferred over physically unsecured data lines, it is susceptible to interception and analysis utilizing, for example, a logic analyzer. If such interception and analysis occurs, the data signals may be capable of being reproduced. In the case of a postage meter, a vault typically accounts for the postage transaction prior to initiating printing of an indicia by the printer. Thus, if the vault print command signal can be reproduced, it may be possible to generate an indicia without having the associated accounting therefor taking place which would result in reduced revenues for the postal authority.

SUMMARY OF THE INVENTION

It is an aspect of an object of the invention to provide a method and apparatus for securely authorizing the performance of printing in a postage meter only upon verification that debiting has occurred.

The object is met by a method for ensuring for each postage transaction in a postage meter having a vault subsystem and a printing subsystem that debiting occurs prior to printing of a postal indicia which method includes authenticating the postage transaction as being valid, performing debiting within the vault subsystem, sending an encrypted debit certificate from the vault subsystem to the printing subsystem, independently recreating the encrypted debit certificate in the printing subsystem, comparing the encrypted debit certificate to the recreated encrypted debit certificate to

B

ascertain if a predetermined relationship exists therebetween, and initiating printing of the postal indicia only upon determination of the existence of the predetermined relationship.

A postage meter which accomplishes the above object includes a printing subsystem; a vault subsystem having structure for performing debiting within the vault subsystem and for sending an encrypted debit certificate from the vault subsystem to the printing subsystem; and structure for authenticating each postage transaction as being valid. The printing subsystem further includes means for independently recreating the encrypted debit certificate in the printing subsystem, comparing the encrypted debit certificate to the recreated encrypted debit certificate to ascertain if a predetermined relationship exists therebetween, and for initiating printing of a postal indicia only upon determination of the existence of the predetermined relationship.

Therefore, various aspects of the invention are provided as follows: In a postage meter having a vault subsystem and a printing subsystem, a method for ensuring that debiting occurs prior to printing of a postal indicia, the method comprising the steps of: a) separately generating a mutual session key in both the vault subsystem and the printing subsystem; b) using the mutual session key generated in both the vault subsystem and the printing subsystem for authenticating the vault subsystem to the printing subsystem; c) using the mutual session key generated in both the vault subsystem and the printing subsystem for authenticating the printing subsystem to the vault subsystem; d) performing debiting within the vault subsystem only subsequent to steps a), b), and c); e) sending an encrypted debit certificate from the vault subsystem to the printing subsystem; f) independently recreating the encrypted debit certificate in the printing subsystem; g) comparing the encrypted debit certificate to the recreated encrypted debit certificate to ascertain if a predetermined relationship exists therebetween which is indicative that the debiting of step (d) has occurred; and h) initiating printing of the postal indicia only upon determination of the existence of the predetermined relationship.

B

BRIEF DESCRIPTION OF THE DRAWINGS

The accompanying drawings, which are incorporated in and constitute a part of the specification, illustrate a presently preferred embodiment of the invention, and together with the general description given above and the detailed description of the preferred embodiment given below, serve to explain the principles of the invention.

Figure 1 is a schematic diagram of a postage meter incorporating the claimed invention;

Figure 2 is an indicia produced by the inventive apparatus; and

Figure 3 is a flowchart of the inventive authentication procedure.

Figure 4 is a flowchart of the inventive debiting and verification process.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Figure 1 shows a schematic representation of a postage meter 1 implementing the inventive process. Postage meter 1 includes a base 3 and a printhead module 5. Base 3 includes a first functional subsystem referred to as a vault microprocessor 7 and a second functional subsystem referred to as a base microprocessor 9. Vault microprocessor 7 has software and associated memory to perform the accounting functions of postage meter 1. That is, vault microprocessor 7 has the capability to have downloaded therein in a conventional manner a predetermined amount of postage funds. During each postage transaction, vault microprocessor 7 checks to see if sufficient funds are available. If sufficient funds are available, vault microprocessor 7 debits the amount from a descending register, adds the amount of an ascending register, and sends the postage amount to the printhead module 5 via the base microprocessor 9. Base microprocessor 9 also sends the date of submission data to the printhead module 5, via line 6, so that a complete indicia image can be printed.

Vault microprocessor 7 thus manages the postage funds with the ascending register representing the lifetime amount of postage funds spent, the descending register representing the amount of funds currently available, and a control sum register showing the running total amount of funds which have been credited to the vault microprocessor 7. Additional features of vault microprocessor 7 which can be included are a piece counter register, encryption algorithms for generating vendor and postal tokens, and software for requiring a user to input a personal identification number which must be verified by the vault microprocessor 7 prior to its authorizing any vault function for a postage transaction. Alternatively, verification of the PIN can be

A

accomplished by either the base microprocessor 9 or the print module microprocessor 41 (discusssed below).

Base microprocessor 9 acts as a traffic cop in coordinating and assisting in the transfer of information along data line 10 between the vault microprocessor 7 and the printhead module 5, as well as coordinating various support functions necessary to complete the metering function. Base microprocessor 9 interacts with keyboard 11 to transfer user information input through keyboard keys 11a (such as postage amount or date of submission) to the vault microprocessor 7. Additionally, base microprocessor 9 sends data to a liquid crystal display 13 via a driver/controller 15 for the purpose of displaying user inputs or for prompting the user for additional inputs. Moreover, base microprocessor 9 provides power and a reset signal to vault microprocessor 7 via respective lines 17, 19. A clock 20 provides date and time information to base microprocessor 9. Alternatively, clock 20 can be eliminated and the clock function can be accomplished by the base microprocessor 9. Base microprocessor 9 also provides a clock signal to vault microprocessor 7.

Postage meter 1 also includes a conventional power supply 21 which conditions raw A.C. voltages from a wall mounted transformer 23 to provide the required regulated and unregulated D.C. voltages for the postage meter 1. Voltages are output via lines 25, 27, and 29 to a printhead motor 31, printhead 33 and all logic circuits. Motor 31 is used to control the movement of the printhead 33 relative to the mailpiece upon which an indicia image is to be printed. Base microprocessor 9 controls the supply of power to motor 31 to ensure the proper starting and stopping of printhead 33 movement after vault microprocessor 7 authorizes a postage transaction.

Base 3 also includes a motion encoder 35 that senses the movement of the printhead motor 31 so that the exact position of printhead 33 can be determined. Signals from motion encoder 35 are sent to printhead module 5 to coordinate the energizing of individual

printhead elements 33a in printhead 33 with the positioning of printhead 33. Alternatively, motion encoder 35 can be eliminated and the pulses applied to stepper motor 31 can be counted to determine the location of printhead 33 and to coordinate energizing of printhead elements 33a. While only one motor 31 is shown, base microprocessor 9 can control various other motors such as a motor for moving printhead 33 in a second direction and a motor for moving a clamping mechanism (not shown) into engagement with the mailpiece.

Printhead module 5 includes printhead 33, a printhead driver 37, a drawing engine 39 (which can be a microprocessor or an Application Specific Integrated Circuit (ASIC)), a microprocessor 41 and a non-volatile memory 43. NVM 43 has stored therein indicia image data which can be printed on a mailpiece. Microprocessor 41 receives a print command, the postage amount, and date of submission via the base microprocessor 9. The postage amount and date of submission are sent from microprocessor 41 to the drawing engine 39 which then accesses non-volatile memory 43 to obtain the required indicia image data therefrom which is stored in registers 44 to 44n. The stored image data is then downloaded on a column-by column basis by the drawing engine 39 to the printhead driver 37, via column buffers 45,47 in order to energize individual printhead elements 33a to print the indicia image on the mailpiece. The individual column-by-column generation of the indicia image is synchronized with movement of printhead 33 until the full indicia is produced. Specific details of the generation of the indicia image is set forth in copending application U. S. serial number 08/554,179 filed November 6, 1995, which is incorporated herein by reference.

Figure 2 shows an enlarged representative example of a typical postage indicia which can be printed by postage meter 1 for use in the United States. The postage indicia 51 includes a graphical image 53 including the 3 stars in the upper left hand corner, the verbiage "UNITED STATES POSTAGE", and the eagle image; an indicia

identification number 55; a date of submission 57; the originating zip code 59; the words “mailed from zipcode 61, which for the ease of simplicity is just being shown with the words "SPECIMEN SPECIMEN"; the postage amount 63; a piece count 65; a check digits number 67; a vendor I.D. number 69; a vendor token 71; a postal token 73; and a multipass check digit 75. While most of the portions of the indicia image 51 are self explanatory, a few require a brief explanation. The vendor I.D. number identifies who the manufacturer of the meter is, and the vendor token and postal token numbers are encrypted numbers which can be used by the manufacturer and post office, respectively, to verify if a valid indicia has been produced.

The Figure 2 indicia is simply a representative example and the information contained therein will vary from country to country. In the context of this application the terms indicia and indicia image are being used to include any specific requirements of any country.

A benefit of the above-described distributed postage meter system is that because of the divided functionality less, expensive microprocessors can be utilized resulting in a lower cost postage meter. Moreover, the modularity of the system allows for easy replacement of the vault and printing modules in the event of failure of either of these modules. However, as previously discussed, the use of a distributed digital system where data is transferred over physically unsecured data lines (for example, data lines 10, 6) results in the system being susceptible to having its data intercepted and reproduced. If such interception and reproduction is accomplished, it is possible that printing module 5 could be driven to print an indicia image without the necessary accounting taking place.

In order to overcome the security problem discussed above, a secure electronic link is provided between vault microprocessor 7 and print module microprocessor 41. The secure electronic link is accomplished through an encryption process which provides for a mutual authentication between the printhead module 5 and the vault

microprocessor 7 prior to authorizing printing of the indicia image, debiting of postage, and updates to certain vault data areas such as PIN location and account numbers. The inventive encryption process significantly decreases the possibility of data interception and reproduction. In the preferred embodiment the base microprocessor 9 acts as a non-secure communications channel between the vault microprocessor 7 and print module microprocessor 41. However, the secure link discussed above and described in detail below can be applied bewteen any subsystems within the postage meter 1.

The inventive method is described in Figure 3. In step S1 an operator enters a desired postage amount for a postage transaction via the keyboard 11. Upon insertion of the mailpiece into the postage meter 1 and its being clamped in place, base microprocessor 9 sends a signal to vault microprocessor 7 and print module microprocessor 41 requesting that a session key (SK) be established as shown in step S2. In order to establish the session key, vault microprocessor 7 and printhead module microprocessor 41 each have an identical set of "M" authentication keys (AK) stored in memory, with each authentication key having a particular index (1 to M) associated therewith. In addition, print module microprocessor 41 also has a set of numbers "0 to N" stored therein which are used to select a particular one of the authentication keys. That is, print module microprocessor 41 is programmed for each postage transaction to select one of the set of numbers "0 to N" either on a sequential or random basis (step S3). Assuming for example that the number "N" is selected, print module microprocessor 41 determines the particular authentication key index AKI (step S4) utilizing a conventional translation function that creates the index within the range 1 to M. Since the authentication keys AK1 to AKM are stored in a look-up table in both the vault and print module microprocessors 7, 41, the index AKI can be associated with a particular key, such as for example, AK1 (step S5). It is important to note that the set of numbers 0 to N can be very large as compared to

the number of keys 1 to M. Thus, the combination of a large set of numbers 0 to N combined with the random selection of one of those numbers to determine a key index provides for increased security.

After print module microprocessor 41 selects one of the numbers 0 to N, that number is sent to vault microprocessor 7 together with a first piece of data VD1 that varies with each postage transaction and is stored in register 77 in print module microprocessor 41 (step S6). Upon receipt, the vault microprocessor 7, which has stored therein an identical authentication key look-up table and the AKI translation function used by the print module microprocessor 41, independently uses the selected number 0 to N to generate AKI and identify the same authentication key AK (step S7) being utilized by the print module microprocessor 41. The vault microprocessor 7 also has a register 79 whose contents VD2 are variable for each postage transaction and are used together with the authentication key AK to create the session key SK (step S8). That is, a conventional encryption algorithm is applied to VD2 and the authentication key to produce the session key:

$$SK = ENCRYPT(VD2, AK).$$

Once vault microprocessor 7 determines the session key, it generates a first authentication certificate (AUC1) (step S9) as follows:

$$AUC1 = ENCRYPT(VD1, SK)$$

Subsequent to generation of the first authentication certificate, vault microprocessor 7 sends all or part of the first authentication certificate and VD2 to the print module microprocessor 41 (step S10). That is, if AUCI is, for example, eight bytes of data, it can be sent in total or a truncation algorithm can be applied to it to only send a predetermined number of bytes of AUC1. The print module

microprocessor 41, upon receipt of AUC1, independently determines SK (step S11) in the same manner as vault microprocessor 7 since print module microprocessor 41 has stored therein the DES algorithm, has itself generated AK, and has VD2 from vault microprocessor 7.

Subsequent to its generation of SK, print module microprocessor 41 generates a second authentication certificate:

$$AUC2 = ENCRYPT(VD1, SK)$$

which should be the same as AUC1 (step S12). In the event that print module microprocessor compares AUC1 to AUC2 (step S13) and they are not the same, the print module microprocessor 41 will initiate cancellation of the postage transaction (step S14). On the other hand, if AUC1 and AUC2 are the same, print module microprocessor 41 has authenticated that vault microprocessor 7 is a valid vault. It is to be noted that if a truncated portion of AUC1 is sent from vault microprocessor 7 to base microprocessor 41, then print module microprocessor 41 must apply the same truncation algorithm to AUC2 prior to the comparison step.

Subsequent to vault microprocessor 7 authentication, print module microprocessor 41 generates a first ciphered data certificate "CD1" where:

$$CD1 = ENCRYPT(VD3, SK)$$

and VD3 represents a variable piece of data within the postage meter 1 such as piece count or date of submission, which data is made available to both the vault microprocessor 7 and print module microprocessor 41 (step S15). Upon generation of CD1, it is sent in whole or in part (as discussed in connection with AUC1, AUC2) to vault microprocessor 7 (step S16). Vault microprocessor 7 then generates its own ciphered certificate of data "CD2" by applying the

encryption algorithm to VD3 and the session key SK generated by vault microprocessor 7 (step S17). Vault microprocessor 7 then compares CD1 to CD2 (step S18) and if they do not match, vault microprocessor 7 initiates cancellation of the postage transaction (step S19). In the event that CD1 and CD2 are the same, the vault microprocessor 7 has authenticated that print module microprocessor 41 and mutual authentication between vault microprocessor 7 and print module microprocessor 41 has been completed.

Subsequent to the mutual authentication, debiting in vault microprocessor is initiated (Step S20). The debiting procedure and its verification is shown in Figure 4. In step S21 the vault microprocessor 7 determines if the registers are correct. That is, does the control sum register "CR" minus the ascending register "AR" equal the descending register "DR". If it does not, the transaction is rejected for inconsistent data (Step S22) . If it is, the vault microprocessor 7 determines if the requested postage value "PV" is less than or equal to DR (Step S23). If the answer is no, the transaction is rejected for lack of sufficient funds (Step S24). If the answer is yes, vault microprocessor 7 computes a new ascending register value AR' = AR + PV (Step S25), a new descending register value DR' = DR-PV (Step S26), and a new control sum CS' = AR' + DR' (Step S27). Once the above accounting has been completed, vault microprocessor 7 generates a first Card Debit Certificate "CDC1" (Step S28) as follows:

$$CDC1 = ENCRYPT(R', SK)$$

where R' is determined as a function of a variable piece of data such as the postage value or date of submission. CDC1 is then sent from vault microprocessor 7 to print module microprocessor 41 in total or in a truncated manner (Step S29). The print module microprocessor 41 then generates a second Card Debit Certificate "CDC2" (Step S30) in the same manner as vault microprocessor 7 generated CDC1 except

that print module microprocessor utilizes the session key it generated. Print module microprocessor 41 then compares CDC1 to CDC2 (Step S31). If CD1 and CD2 are not the same the transaction is canceled (Step S32). However, if they are the same, the print module microprocessor 41 has verified that a proper debit has occurred. Subsequently, the vault microprocessor 7 sends the vendor and postal tokens in clear text to the print module microprocessor 41 (Step S33) and the print module microprocessor 41 initiates printing of the indicia image including the tokens (Step S34).

The above process provides an extremely secure electronic link between subsystems because all data which is transmitted between the subsytems is variable for each postage base. While this does not necessarily have to be the case, it provides increased security by reducing the predictability of the data being transferred. The use of the variable data (VD1, VD2, VD3) ensures the uniqueness of the ciphered values (SK, AUC1, AUC2, CD1, CD2) for each postage transaction. Moreover, the session key, which is required to initiate the whole mutual authentication procedure and to generate AUC1, AUC2, CD1 and CD2, is never transmitted between the individual subsystems thereby guaranteeing the secure knowledge of the session key among the subsystems. Furthermore, if a truncation algorithm is used in connection with any or all of the generated certificates, security is further enhanced since the truncation algorithm must be known in order to complete the postage transaction. Finally, use of the Card Debit Certificates ensures that a proper debit occurs prior to printing.

CLAIMS:

2193022

1. In a postage meter having a vault subsystem and a printing subsystem, a method for ensuring that debiting occurs prior to printing of a postal indicia, the method comprising the steps of:

a) separately generating a mutual session key in both the vault subsystem and the printing subsystem;

b) using the mutual session key generated in both the vault subsystem and the printing subsystem for authenticating the vault subsystem to the printing subsystem;

c) using the mutual session key generated in both the vault subsystem and the printing subsystem for authenticating the printing subsystem to the vault subsystem;

d) performing debiting within the vault subsystem only subsequent to steps a), b), and c);

e) sending an encrypted debit certificate from the vault subsystem to the printing subsystem;

f) independently recreating the encrypted debit certificate in the printing subsystem;

g) comparing the encrypted debit certificate to the recreated encrypted debit certificate to ascertain if a predetermined relationship exists therebetween which is indicative that the debiting of step (d) has occurred; and

h) initiating printing of the postal indicia only upon determination of the existence of the predetermined relationship.

B

2. A method as recited in claim 1, wherein the encrypted debit certificate is created by applying an encryption algorithm to a variable piece of data associated with the postage transaction.

3. A method as recited in claim 2, further comprising authenticating the vault and printing subsystems without transmitting the mutual session key between the vault and printing subsystems.

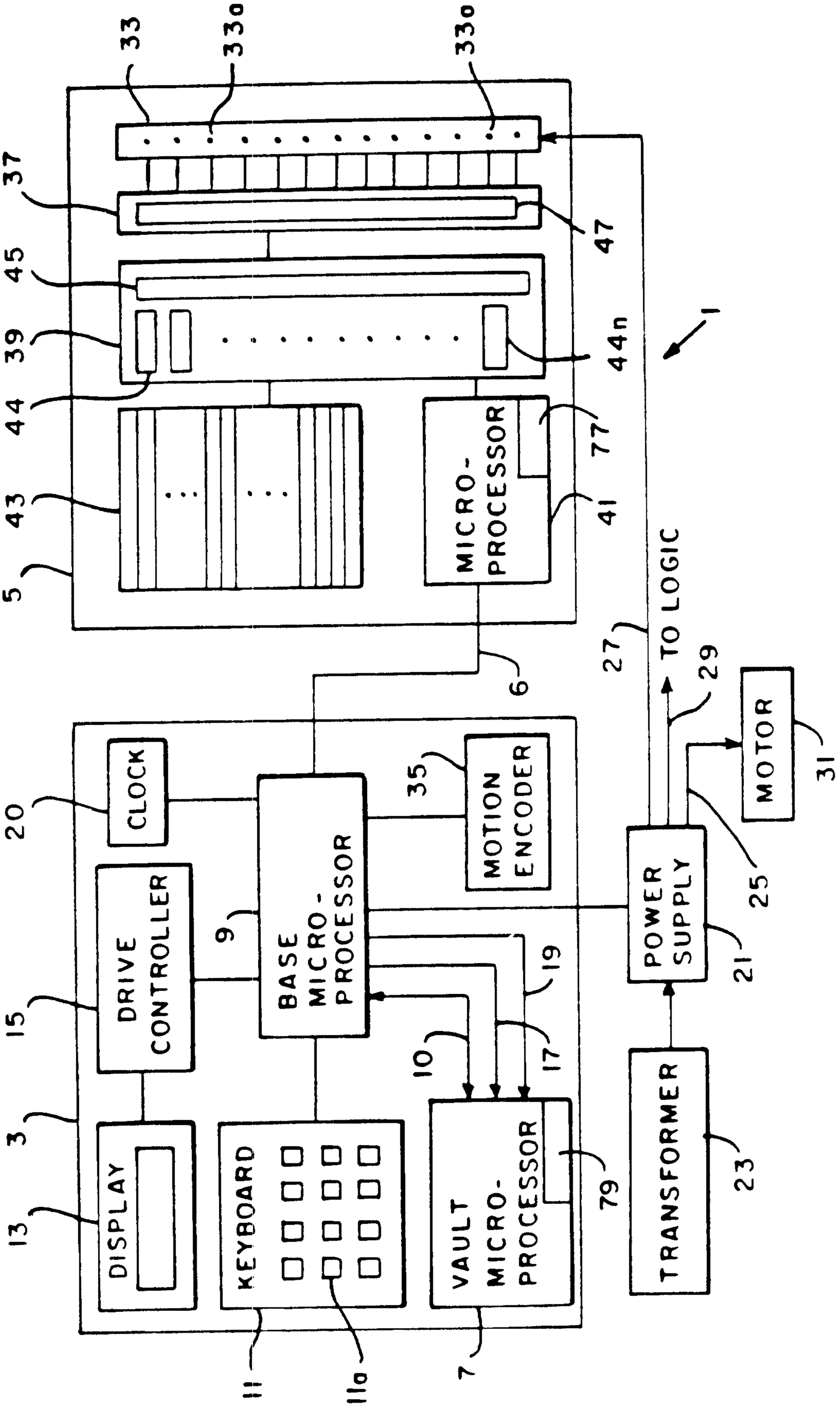
4. A method as recited in claim 2, further comprising separately selecting a common one of a plurality of authentication keys within the vault and printing subsystems and respectively using the common one of the plurality of authentication keys selected within each of the vault and printing subsystems to generate the mutual session key within the vault and printing subsystems.

5. A method as recited in claim 4, wherein generating of the mutual session key within the first and second subsystems is accomplished without transmitting the common one of the plurality of authentication keys between the vault and printing subsystems.

6. A method as recited in claim 5, further comprising randomly selecting a number, applying within each of the vault and printing subsystems a translation function to the randomly selected number to generate an authentication key index, and utilizing the authentication key index to select the common one of the plurality of authentication keys within each of the vault and printing subsystems.

7. A method as recited in claim 6, wherein the mutual session key is generated in the vault and printing subsystems by applying an encryption algorithm to the common one of the plurality of authentication keys and to a first data element that varies with the printing of each postal indicia.

FIG. 1


33
330
330
37
47
45
39
44
44n
43
5
MICRO-
PROCESSOR
77
41
1
TO LOGIC
27
29
MOTOR
31
25
20
CLOCK
35
MOTION
ENCODER
DRIVE
CONTROLLER
9
BASE
MICRO-
PROCESSOR
POWER
SUPPLY
21
15
19
10
17
3
DISPLAY
KEYBOARD
VAULT
MICRO-
PROCESSOR
79
TRANSFORMER
23
13
11
11a
7
6

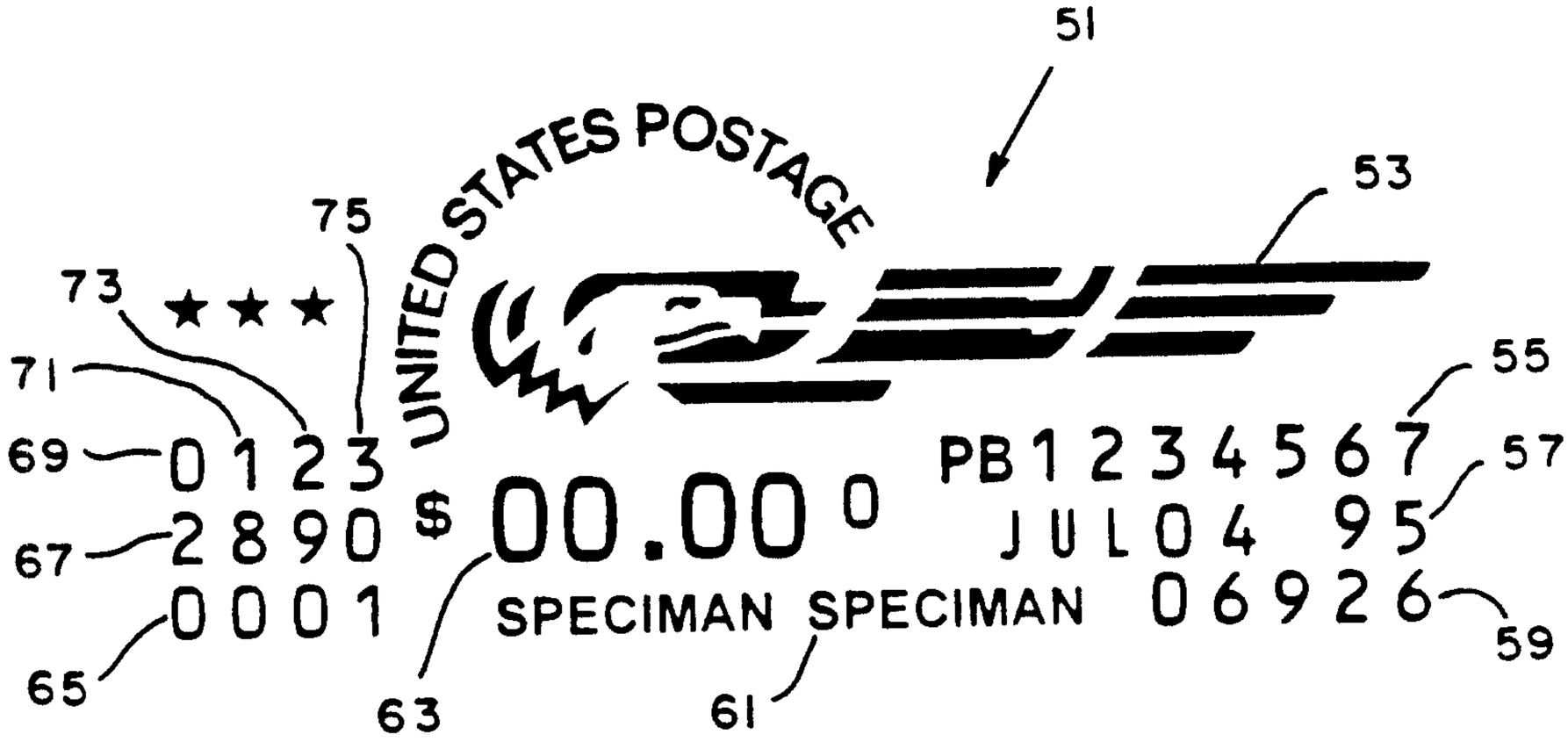

51
53
75
UNITED STATES POSTAGE
73
★ ★ ★
71
55
69
0 1 2 3
PB 1 2 3 4 5 6 7
57
67
2 8 9 0
$ 00.00 0
J U L 0 4 9 5
0 0 0 1
SPECIMAN SPECIMAN
0 6 9 2 6
59
65
63
61

FIG. 2

FIG. 3

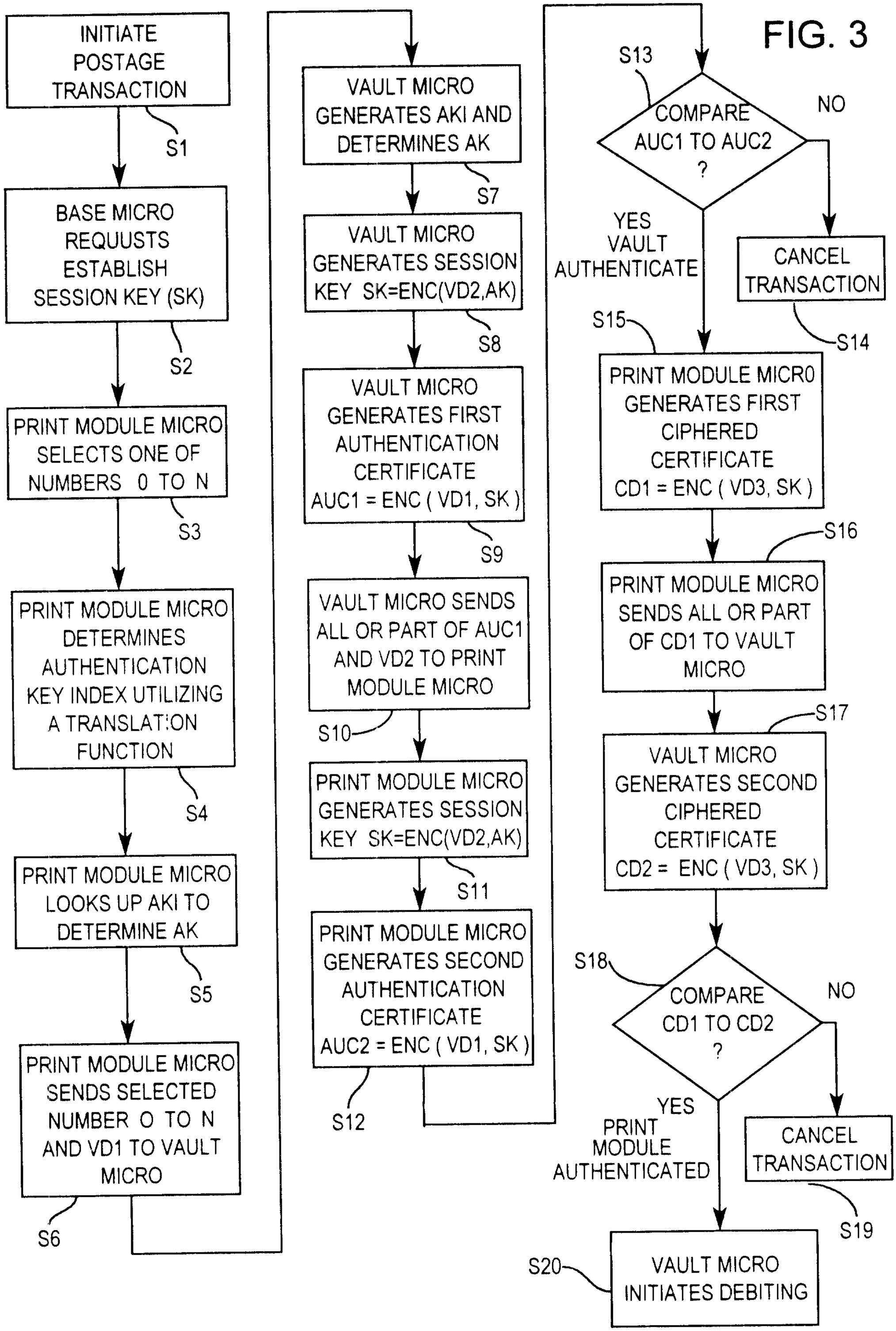
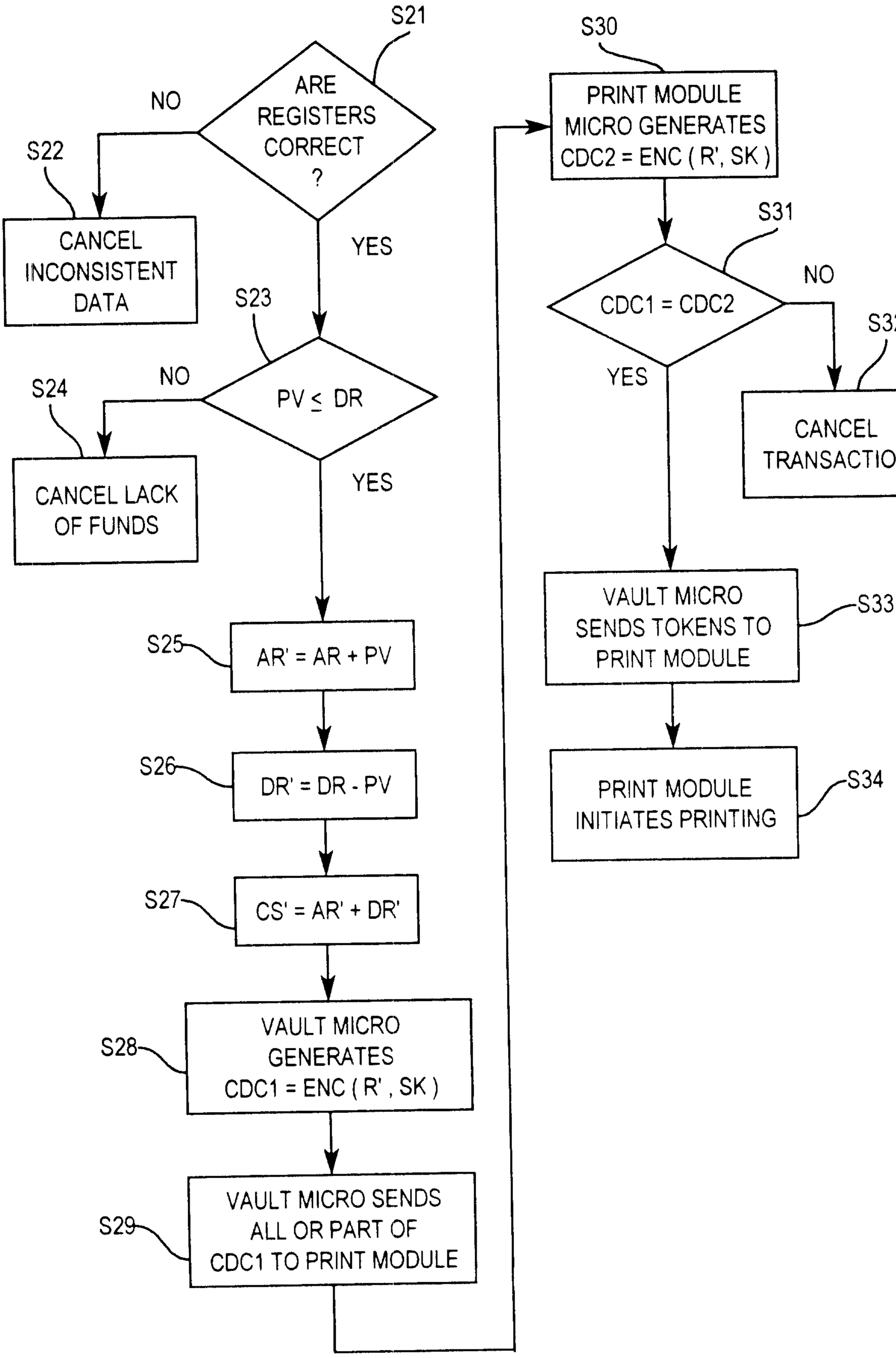
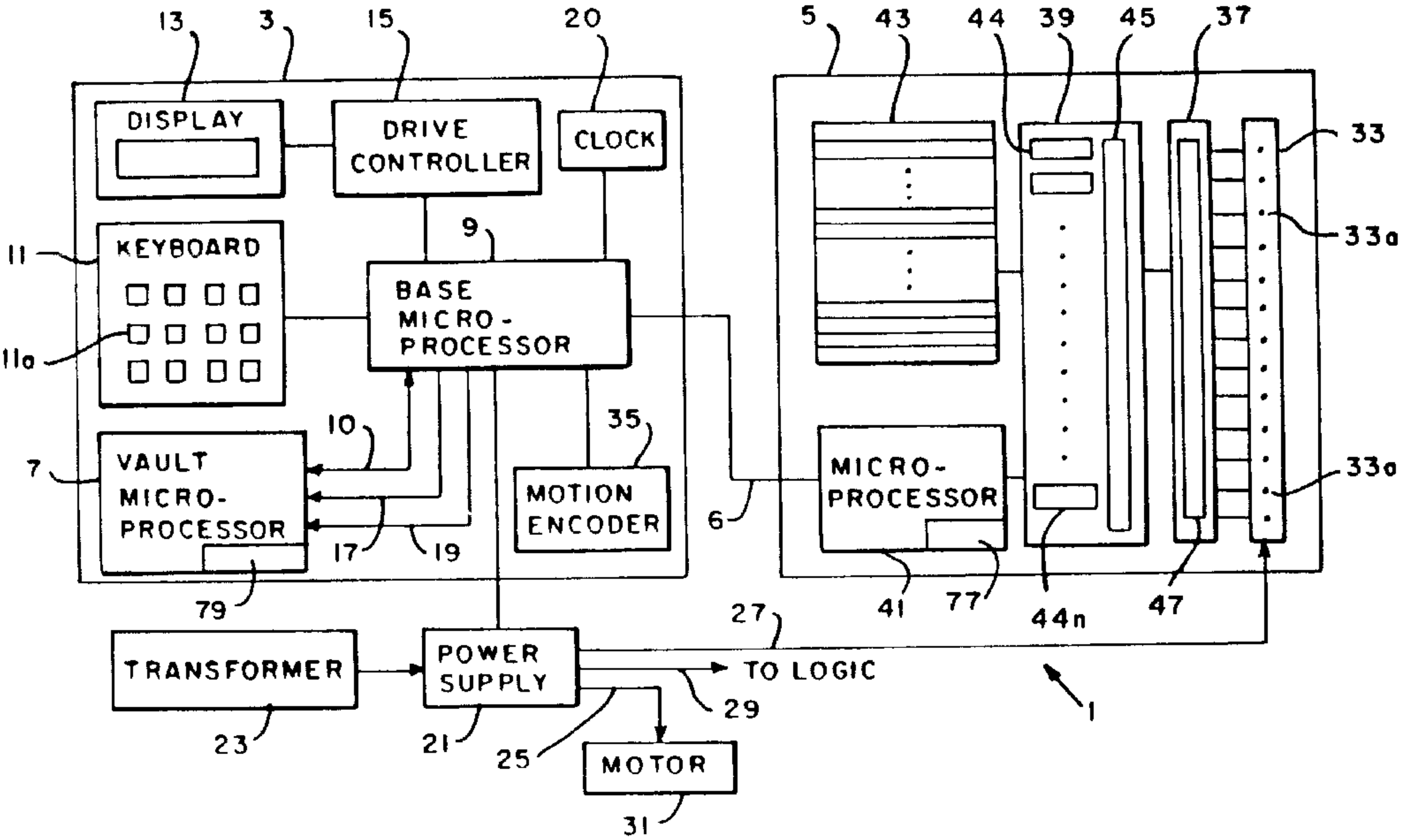

INITIATE POSTAGE TRANSACTION
S1
BASE MICRO REQUUSTS ESTABLISH SESSION KEY (SK)
S2
PRINT MODULE MICRO SELECTS ONE OF NUMBERS 0 TO N
S3
PRINT MODULE MICRO DETERMINES AUTHENTICATION KEY INDEX UTILIZING A TRANSLAT:ON FUNCTION
S4
PRINT MODULE MICRO LOOKS UP AKI TO DETERMINE AK
S5
PRINT MODULE MICRO SENDS SELECTED NUMBER O TO N AND VD1 TO VAULT MICRO
S6
VAULT MICRO GENERATES AKI AND DETERMINES AK
S7
VAULT MICRO GENERATES SESSION KEY SK=ENC(VD2,AK)
S8
VAULT MICRO GENERATES FIRST AUTHENTICATION CERTIFICATE AUC1 = ENC (VD1, SK)
S9
VAULT MICRO SENDS ALL OR PART OF AUC1 AND VD2 TO PRINT MODULE MICRO
S10
PRINT MODULE MICRO GENERATES SESSION KEY SK=ENC(VD2,AK)
S11
PRINT MODULE MICRO GENERATES SECOND AUTHENTICATION CERTIFICATE AUC2 = ENC (VD1, SK)
S12
S13
COMPARE AUC1 TO AUC2 ?
NO
YES VAULT AUTHENTICATE
CANCEL TRANSACTION
S14
S15
PRINT MODULE MICR0 GENERATES FIRST CIPHERED CERTIFICATE CD1 = ENC (VD3, SK)
S16
PRINT MODULE MICRO SENDS ALL OR PART OF CD1 TO VAULT MICRO
S17
VAULT MICRO GENERATES SECOND CIPHERED CERTIFICATE CD2 = ENC (VD3, SK)
S18
COMPARE CD1 TO CD2 ?
NO
YES PRINT MODULE AUTHENTICATED
CANCEL TRANSACTION
S19
S20
VAULT MICRO INITIATES DEBITING

FIG. 4


S21
ARE REGISTERS CORRECT ?
NO
YES
S22
CANCEL INCONSISTENT DATA
S23
PV ≤ DR
NO
YES
S24
CANCEL LACK OF FUNDS
S25
AR' = AR + PV
S26
DR' = DR - PV
S27
CS' = AR' + DR'
S28
VAULT MICRO GENERATES CDC1 = ENC (R' , SK)
S29
VAULT MICRO SENDS ALL OR PART OF CDC1 TO PRINT MODULE
S30
PRINT MODULE MICRO GENERATES CDC2 = ENC (R', SK)
S31
CDC1 = CDC2
NO
YES
S32
CANCEL TRANSACTION
S33
VAULT MICRO SENDS TOKENS TO PRINT MODULE
S34
PRINT MODULE INITIATES PRINTING


13
3
15
20
DISPLAY
DRIVE CONTROLLER
CLOCK
9
11
KEYBOARD
BASE MICRO-PROCESSOR
11a
10
35
7
VAULT MICRO-PROCESSOR
MOTION ENCODER
17
19
79
TRANSFORMER
POWER SUPPLY
27
TO LOGIC
29
23
21
25
MOTOR
31
5
43
44
39
45
37
33
33a
6
MICRO-PROCESSOR
33a
41
77
44n
47
1