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

(11) EP 0 845 760 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
03.06.1998 Bulletin 1998/23

(51) Int. Cl.[6]: **G07B 17/00**

(21) Application number: **97120456.5**

(22) Date of filing: **21.11.1997**

(84) Designated Contracting States:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **21.11.1996 US 754570**

(71) Applicant: **PITNEY BOWES INC.**
Stamford Connecticut 06926-0700 (US)

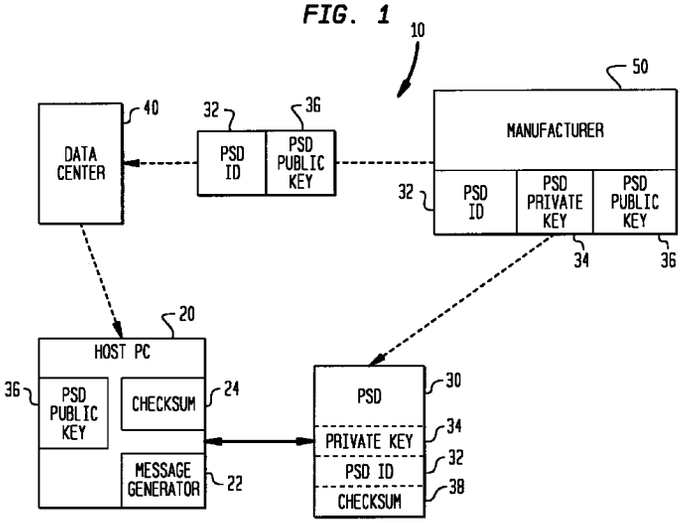
(72) Inventors:
- **Ryan, Frederick W., Jr.**
  Oxford, Connect. 06478 (US)
- **Cordery, Robert A.**
  Danburry, Connect. 06811 (US)

(74) Representative:
Avery, Stephen John et al
Hoffmann Eitle,
Patent- und Rechtsanwälte,
Arabellastrasse 4
81925 München (DE)

(54) Method for verifying the expected postage security device in a host system

(57) A method to verify in a host system that the expected PSD is coupled to the host. The host system generates a message, such as a random number and sends to the PSD. In one embodiment, the random number is signed in the PSD. The signed number is transmitted to the host where the signature is verified. In an alternate embodiment, the PSD encrypts the number and transmits it to the host system. The host system decrypts the encrypted number and ensures it corresponds with the number originally generated and transmitted to the PSD. Methods for verifying in a PSD that the expected host is coupled to the PSD mirrors the two embodiments for verifying the expected PSD. The generated message may include data indicating status of the PSD based, for example a checksum of PSD transaction records stored in the host system.

FIG. 1



EP 0 845 760 A2

Description

The present invention relates generally to a system and method for postage metering security and, more particularly, to systems and methods for verifying authorized postal security devices.

The Information-Based Indicia Program (IBIP) is a distributed trusted system proposed by the United States Postal Service (USPS). The IBIP is expected to support new methods of applying postage in addition to, and eventually in lieu of, the current approach, which typically relies on a postage meter to mechanically print indicia on mailpieces. The IBIP requires printing large, high density, two dimensional (2-D) bar codes on mailpieces. The Postal Service expects the IBIP to provide cost-effective assurance of postage payment for each mailpiece processed.

The USPS has published draft specifications for the IBIP. The INFORMATION BASED INDICIA PROGRAM (IBIP) INDICIUM SPECIFICATION, dated June 13, 1996, defines the proposed requirements for a new indicium that will be applied to mail being processed using the IBIP. The INFORMATION BASED INDICIA PROGRAM POSTAL SECURITY DEVICE SPECIFICATION, dated June 13, 1996, defines the proposed requirements for a Postal Security Device (PSD) that will provide security services to support the creation of a new "information based" postage postmark or indicium that will be applied to mail being processed using the IBIP. The INFORMATION BASED INDICIA PROGRAM HOST SYSTEM SPECIFICATION, dated October 9, 1996, defines the proposed requirements for a host system element of the IBIP. The specifications are collectively referred to herein as the "IBIP Specifications". The IBIP includes interfacing user (customer), postal and vendor infrastructures which are the system elements of the program.

The user infrastructure, which resides at the user's site, comprises a postal security device (PSD) coupled to a host system. The PSD is a secure processor-based accounting device that dispenses and accounts for postal value stored therein. The host system may be a personal computer (PC) or a meter-based host processor. Among the various requirements set forth in the Host System Specification is that the host system verifies that the coupled PSD is "the expected PSD". Conventional postage metering devices and recent digital metering devices, such as PostPerfect and Personal Post Office, both manufactured by the assignee of the present invention, do not include such verification. Thus, a method for achieving such verification is desired.

U.S. Patent No. 5,510,992 discloses a method whereby the host PC verifies that a storage means that is coupled to the host PC and has postal value stored therein, is authorized for use with the host PC. The method comprises the steps of storing a unique identifier, such as a serial number in the storage means when the storage means is filled with postal value, and sending the unique identifier to the host PC when postage value is requested for dispensing. The host PC then verifies that the storage means is authorized for use with the host PC by confirming that the unique identifier retrieved from the storage device is the same as one stored in the host PC. Although such method verifies that the storage means is the expected storage device, the storage means is not a PSD because it is not a processor-based accounting device that dispenses and accounts for postal value stored therein. Furthermore, the verification of the serial number in the host PC is subject to fraud.

It has been found that the present invention provides a more secure and reliable system and method for verifying the expected PSD is coupled to the host PC. It has further been found that the present invention provides a secure and reliable system and method for verifying the expected host PC is coupled to the PSD.

The present invention provides a secure and reliable method for verifying in the host system that the expected PSD is coupled to the host system. In accordance with the present invention, a message, such as a random number, is generated in the Host system and sent to the PSD. In one embodiment, the PSD encrypts the number and transmits it to the Host system. The Host system decrypts the encrypted number and ensures it corresponds with the number originally generated and transmitted to the PSD. In an alternate embodiment, the random number is signed in the PSD. The signed number is transmitted to the Host where the signature is verified. The generated message may include data indicating status of the PSD based, for example a checksum of PSD transaction records stored in the host system. Methods for verifying in a PSD that the expected host is coupled to the PSD mirrors the two embodiments for verifying the expected PSD.

The above and other objects and advantages of the present invention will be apparent upon consideration of the following detailed description, taken in conjunction with accompanying drawings, in which like reference characters refer to like parts throughout, and in which:

Fig. 1 is a block diagram of a postage metering system in accordance with the present invention showing a process for storing keys in a host system and a PSD coupled thereto;

Fig. 2 is a flow chart showing an alternate process for storing keys in a host system and a PSD coupled thereto;

Fig. 3 is a flow chart of a preferred method for verifying the expected PSD is coupled to the host system;

Fig. 4 is a flow chart of showing a method corresponding to that of Fig. 3 for verifying the expected host system;

Fig. 5 is a flow chart of an alternate method for verifying the expected PSD is coupled to the host sys-

tem; and

Fig. 6 is a flow chart of showing an alternate method corresponding to that of Fig. 5 for verifying the expected host system.

In describing the present invention, reference is made to the drawings, wherein there is seen system and methods for verifying the expected postal security device in a host system and conversely verifying the expected host system. Referring now to Fig. 1, a postage metering system, generally designated 10, includes a Host PC 20 coupled to a PSD 30, a Data Center 40 and a manufacturer 50. The manufacturer 50 initializes PSD 30 with an identification number, such as PSD ID 32, and a cryptographic key, such as PSD private key 34. The manufacturer 50 also sends the PSD ID 32 and a cryptographic key corresponding to the key in the PSD 30, such as PSD public key 36, to the Data Center 40. The Data Center 40 then sends the PSD ID 32 and the public key 36, to the Host PC 20. For the purpose of describing the present invention, the PSD private and public keys are stored in PSD 30 and Host PC 20 respectively. It will be understood that a secret key shared by the Host PC and the PSD may be used in place of such key pair.

The Host PC 20 and PSD 30 each include a microprocessor and memory (not shown). The Host PC 20 further includes a message generator 22 for generating a message. The message may be a random number or may include data indicating status of the PSD, for example a checksum 24 of PSD transaction records stored a log files in Host PC 20. For the following description of the present invention checksums will be used. The PSD records stored in Host PC 20 correspond to PSD records stored in PSD 30 for each transaction by PSD 30. For a more detailed description of such storage of PSD records see European Patent Application Serial Number 0780808, assigned to the assignee of the present invention, and incorporated herein by reference.

Referring now to Fig. 2, an alternate method for initializing the PSD with a cryptographic key is shown. At step 100, Host PC 20 generates a secret key or a key pair. The key or key pair is stored in Host PC 20, at step 105. Host PC 20 the sends the secret key or one of the keys of the key pair to PSD 30, at step 110. PSD 30 stores the key received from Host PC 20, at step 115.

Referring now to Fig. 3, a method is shown for verifying in Host PC 20 that the expected PSD is coupled thereto. At step 200, the Host PC generates a message. In accordance with the present invention, the message may be in the form of a random number or may be a checksum of a PSD transaction log stored in the Host PC. The Host PC, at step 205, sends the message to the PSD. If a checksum has been sent, the at step 210, the PSD compares the message received with a checksum of a PSD transaction log stored in the PSD. If the checksum received is not the same as the checksum of the PSD transaction log, then an error is flagged, at step 215, indicating that there is a discrepancy between the PSD logs stored in the Host PC and the PSD. If the checksums are the same or if the message is a random number, at step 220, the PSD signs the message with the PSD private key. At step 225, the PSD sends the signed message to the Host PC.

At step 230, the Host PC verifies the signature using the PSD public key stored in the Host PC. If the signature is not verified at step 235, the Host PC rejects the PSD from processing any further transactions, at step 240. If the signature is verified, at step 245, the expected PSD has been verified and the Host PC can begin request postal value from the PSD. It will be understood by those skilled in the art that other cryptographic processing, such as encryption or hashing may be used in place of signing.

Referring now to Fig. 4, it may be required that in addition to the Host PC verifying the expected PSD, the PSD verify that the expected Host PC is coupled to the PSD. In the preferred embodiment of the present invention, such verification of the expected Host PC mirrors the process for verifying the expected PSD as set forth above.

At step 300, the PSD generates a message. In accordance with the present invention, the message may be in the form of a random number or may be a checksum of a PSD transaction log stored in the PSD. The PSD, at step 305, sends the message to the Host PC. If a checksum has been sent, the at step 310, the Host PC compares the message received with a checksum of a PSD transaction log stored in the Host PC. If the checksum received is not the same as the checksum of the PSD transaction log, then an error is flagged, at step 315, indicating that there is a discrepancy between the PSD logs stored in the PSD and the Host PC. If the checksums are the same or if the message is a random number, at step 320, the Host PC signs the message with the Host PC private key. At step 325, the Host PC sends the signed message to the PSD.

At step 330, the PSD verifies the signature using the Host PC public key stored in the PSD. If the signature is not verified at step 335, the PSD rejects the Host PC from processing any further transactions, at step 340. If the signature is verified, at step 345, the expected Host PC has been verified and the PSD is ready to accept transaction requests from the Host PC.

Referring now to Fig. 5, an alternate method for verifying the expected PSD is shown. At step 400, the Host PC generates a message, such as a random number or a checksum of a PSD transaction log stored in the Host PC. The Host PC encrypts the message with the PSD public Key, at step 405, and sends the message to the PSD, at step 410. At step 415, the PSD decrypts the encrypted message received. If a checksum has been sent then, at step 420, the PSD compares the message received with a checksum of a PSD transaction log stored in the PSD. If the checksum received is not the

same as the checksum of the PSD transaction log, then an error is flagged, at step 425 indicating that there is a discrepancy between the PSD logs stored in the Host PC and the PSD. If the checksums are the same or if the message is a random number, at step 430, the PSD sends the decrypted message to the Host PC.

At step 435, the Host PC verifies that the message received from the PSD is the same as the message generated in the Host PC. If not the same at step 440, the Host PC rejects the PSD from processing any further transactions, at step 445. If the message received from the PSD is the same as the message generated in the Host PC, at step 450, the expected PSD has been verified and the Host PC can begin request postal value from the PSD.

Referring now to Fig. 6, an alternate method for the PSD verifying that the expected Host PC is coupled to the PSD is shown which mirrors the process for verifying the expected PSD as shown in Fig. 5.

At step 500, the PSD generates a message, such as a random number or a checksum of a PSD transaction log stored in the PSD. The PSD encrypts the message with the Host PC public Key, at step 505, and sends the message to the Host PC, at step 510. At step 515, the Host PC decrypts the encrypted message received. If a checksum has been sent then, at step 520, the Host PC compares the message received with a checksum of a PSD transaction log stored in the Host PC. If the checksum received is not the same as the checksum of the PSD transaction log, then an error is flagged, at step 525, indicating that there is a discrepancy between the PSD logs stored in the PSD and the Host PC. If the checksums are the same or if the message is a random number, at step 530, the Host PC sends the decrypted message to the PSD.

At step 535, the PSD verifies that the message received from the Host PC is the same as the message generated in the PSD. If not the same at step 540, the PSD rejects the Host PC from processing any further transactions, at step 545. If the message received from the Host PC is the same as the message generated in the PSD, at step 550, the expected Host PC has been verified and the PSD can begin to accept requests for postal value from the Host PC.

It has been found that the present invention is suitable for use with any security device that is coupled to a host system in an unsecured manner. For example, the present invention could be used for a certificate metering system such as disclosed in European Patent Application Serial No. 0762692, filed August 21, 1996, assigned to the assignee of the present invention, and incorporated herein by reference.

While the present invention has been disclosed and described with reference to specific embodiments thereof, it will be apparent, as noted above, that variations and modifcations may be made therein. It is, thus, intended in the following claims to cover each variation and modification, including a certificate metering system, that falls within the true spirit and scope of the present invention.

Claims

1. A method for verifying in a host system that a postal security device (PSD) is the expected PSD, the method comprising the steps of:

   storing in the PSD a signing key;
   storing in the host system a verifying key;
   generating a first message in the host system;
   sending the first message to the PSD;
   signing the first message with the signing key;
   sending the signed first message to the host system; and
   verifying the signed first message in the host system using the verifying key.

2. The method of claim 1 wherein the message generated is a checksum of PSD transaction records.

3. The method of claim 1 wherein the signing key and verifying key are identical.

4. The method of claim 1 wherein the signing key and the verifying key are different.

5. The method of claim 1 wherein the signing key is a private key of a key pair and the verifying key is a public key of the key pair.

6. A postage metering system comprising:

   a host system including message generating means;
   a postal security device (PSD) coupled to said host system, wherein said PSD has stored therein a signing key and the host system has stored therein a verifying key; and
   wherein said PSD includes means for signing a message received from said host system using said signing key, and said host system includes means for verifying a signed message received from said PSD using said verifying key.

7. The system of claim 6 wherein the signing key and verifying key are identical.

8. The system of claim 6 wherein the signing key and the verifying key are different.

9. The system of claim 6 wherein the signing key is a private key of a key pair and the verifying key is a public key of the key pair.

10. A method for verifying in a host system that a postal

security device (PSD) is the expected PSD, the method comprising the steps of:

storing in the PSD a decryption key;
storing in the host system an encryption key;
generating a first message in the host system;
encrypting the first message with the encryption key;
sending the encrypted first message to the PSD;
decrypting the encrypted first message with the decryption key;
sending to the host system a second message that is based on the decrypted first message; and
verifying in the host system that the second message is the corresponds to the first message.

11. The method of claim 1 or 10 wherein the first message generated is a random number.

12. The method of claim 10 wherein the message generated includes data indicating status of the PSD based on PSD transaction records stored in the host system.

13. The method of claim 10 wherein the host system is a personal computer.

14. The system of claim 10 wherein the decryption key and encryption key are identical.

15. The system of claim 10 wherein the decryption key and the encryption key are different.

16. The system of claim 10 wherein the decryption key is a private key of a key pair and the encryption key is a public key of the key pair.

17. The system of claim 10 wherein the second message is the same the decrypted first message.

18. The method of claim 12 wherein the data indicating status of the PSD is a checksum of PSD transaction records.

19. A method for verifying in a host system that a postal security device (PSD) is the expected PSD and in the PSD that the host system is the expected host system, the method comprising the steps of:

storing in the PSD a first signing key and a second verifying key;
storing in the host system a first verifying key and a second signing key;
generating a first message in the host system;
sending the first message to the PSD;
signing the first message with the first signing key;
sending the signed first message to the host system;
verifying the signed first message in the host system using the first verifying key;
generating a second message in the PSD;
sending the second message to the host system;
signing the second message with the second signing key;
sending the signed second message to the PSD; and
verifying the signed second message in the PSD using the second verifying key.

20. A method for verifying in a host system that a postal security device (PSD) is the expected PSD and in the PSD that the host system is the expected host system , the method comprising the steps of:

storing in the PSD a first decryption key and a second encryption key;
storing in the host system a first encryption key and a second decryption key;
generating a first message in the host system;
encrypting the first message with the first encryption key;
sending the encrypted first message to the PSD;
decrypting the encrypted first message with the first decryption key;
sending to the host system a second message that is based on the decrypted first message;
verifying in the host system that the second message corresponds to the generated first message;
generating a third message in the PSD;
encrypting the third message with the second encryption key;
sending the encrypted third message to the host system;
decrypting the third encrypted message with the second decryption key;
sending to the PSD a fourth message that is based on the decrypted third message; and
verifying in the PSD that the fourth message corresponds to the third message.

21. The method of claim 20 wherein the second message is the same as the decrypted first message and the fourth message is the same as the decrypted third message.

FIG. 1

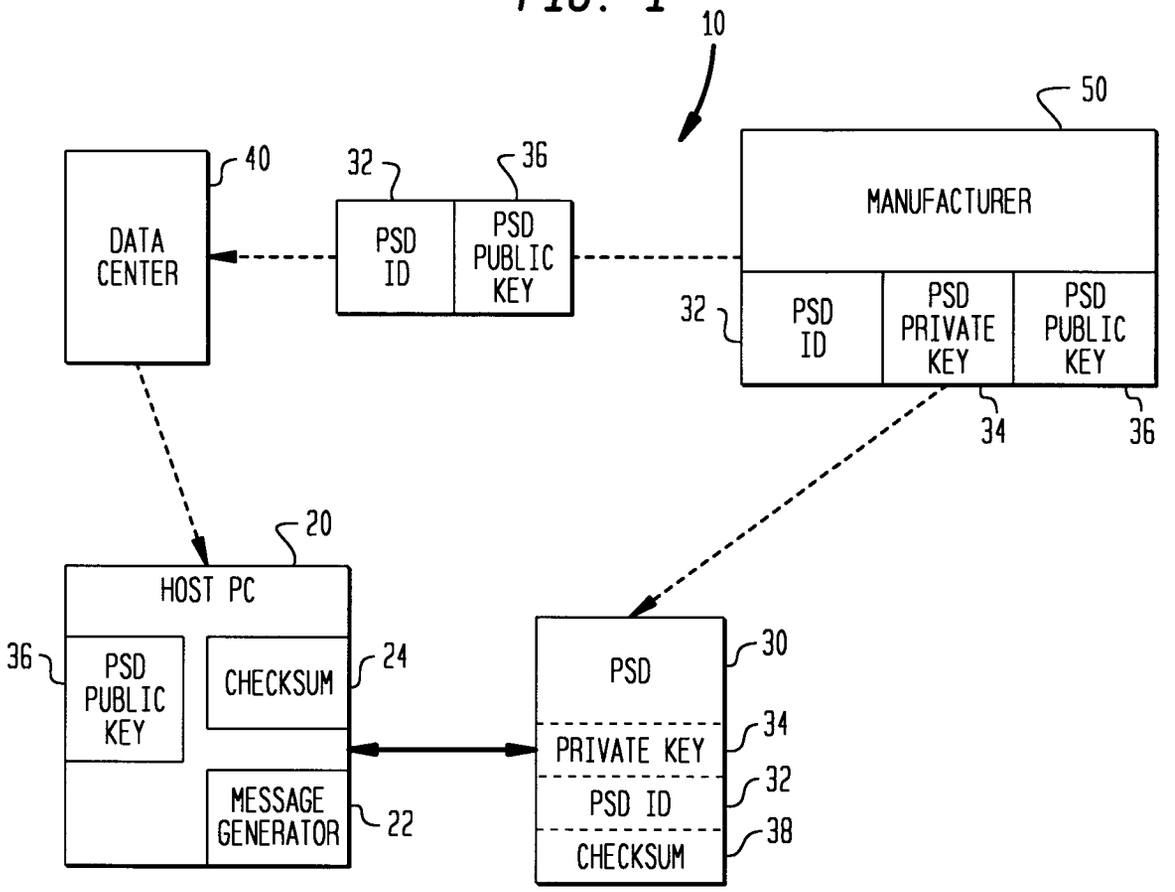

10
50
40
32
36
DATA CENTER
PSD ID
PSD PUBLIC KEY
MANUFACTURER
32
PSD ID
PSD PRIVATE KEY
PSD PUBLIC KEY
34
36
20
HOST PC
36
PSD PUBLIC KEY
CHECKSUM
24
MESSAGE GENERATOR
22
PSD
30
PRIVATE KEY
34
PSD ID
32
CHECKSUM
38

FIG. 2

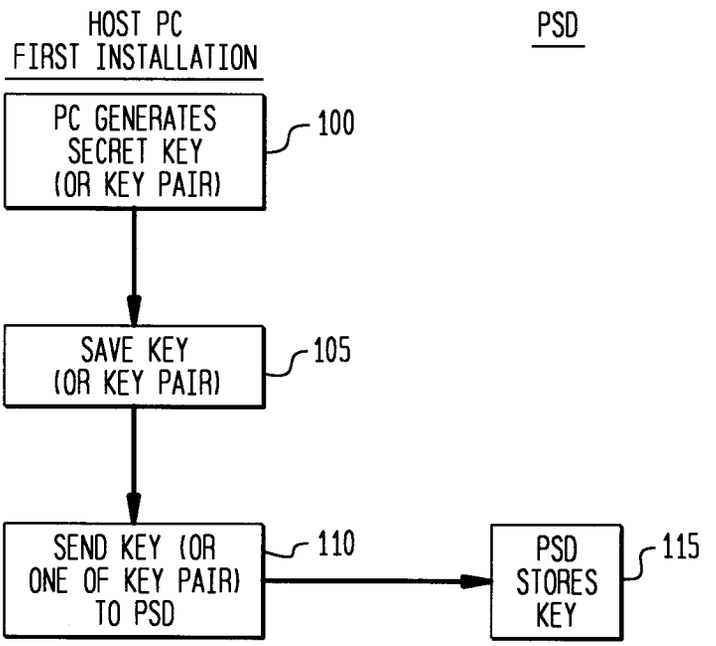

HOST PC
FIRST INSTALLATION
PSD
PC GENERATES SECRET KEY (OR KEY PAIR)
100
SAVE KEY (OR KEY PAIR)
105
SEND KEY (OR ONE OF KEY PAIR) TO PSD
110
PSD STORES KEY
115

FIG. 3

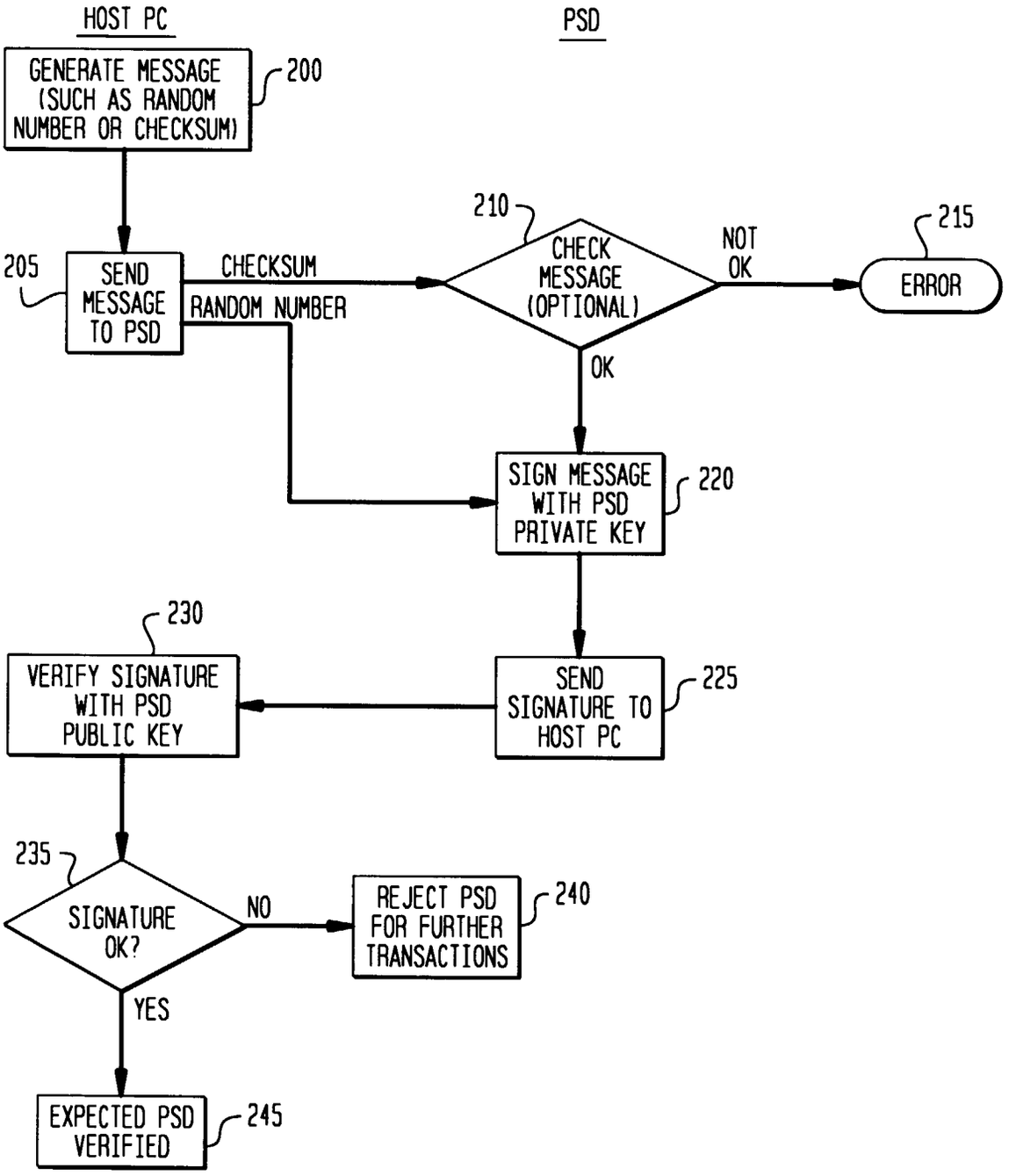

HOST PC
PSD
GENERATE MESSAGE (SUCH AS RANDOM NUMBER OR CHECKSUM)
200
205
SEND MESSAGE TO PSD
CHECKSUM
RANDOM NUMBER
210
CHECK MESSAGE (OPTIONAL)
NOT OK
215
ERROR
OK
SIGN MESSAGE WITH PSD PRIVATE KEY
220
SEND SIGNATURE TO HOST PC
225
230
VERIFY SIGNATURE WITH PSD PUBLIC KEY
235
SIGNATURE OK?
NO
REJECT PSD FOR FURTHER TRANSACTIONS
240
YES
EXPECTED PSD VERIFIED
245

FIG. 4

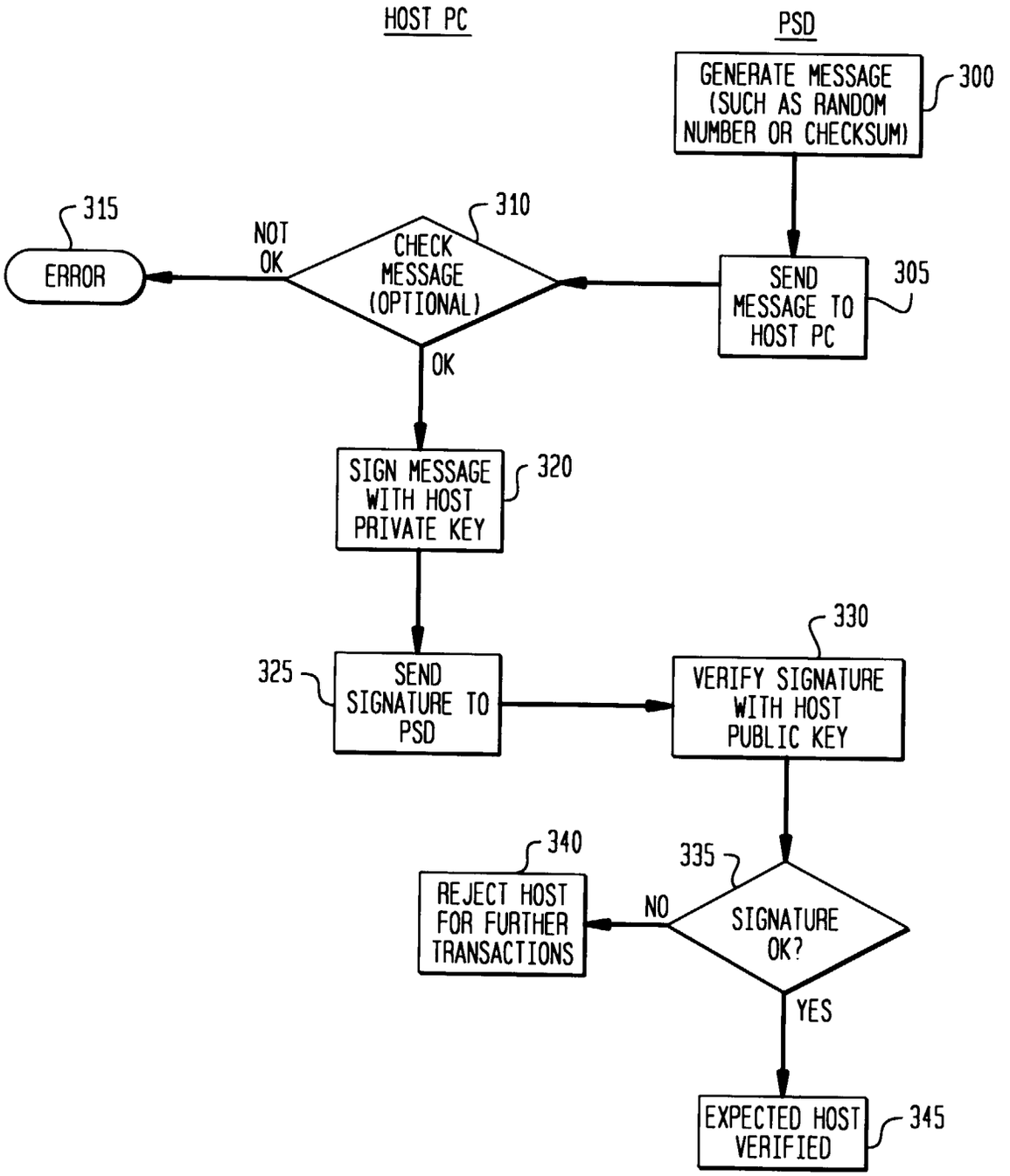

HOST PC
PSD
GENERATE MESSAGE (SUCH AS RANDOM NUMBER OR CHECKSUM)
300
SEND MESSAGE TO HOST PC
305
CHECK MESSAGE (OPTIONAL)
310
NOT OK
ERROR
315
OK
SIGN MESSAGE WITH HOST PRIVATE KEY
320
SEND SIGNATURE TO PSD
325
VERIFY SIGNATURE WITH HOST PUBLIC KEY
330
SIGNATURE OK?
335
NO
REJECT HOST FOR FURTHER TRANSACTIONS
340
YES
EXPECTED HOST VERIFIED
345

FIG. 5

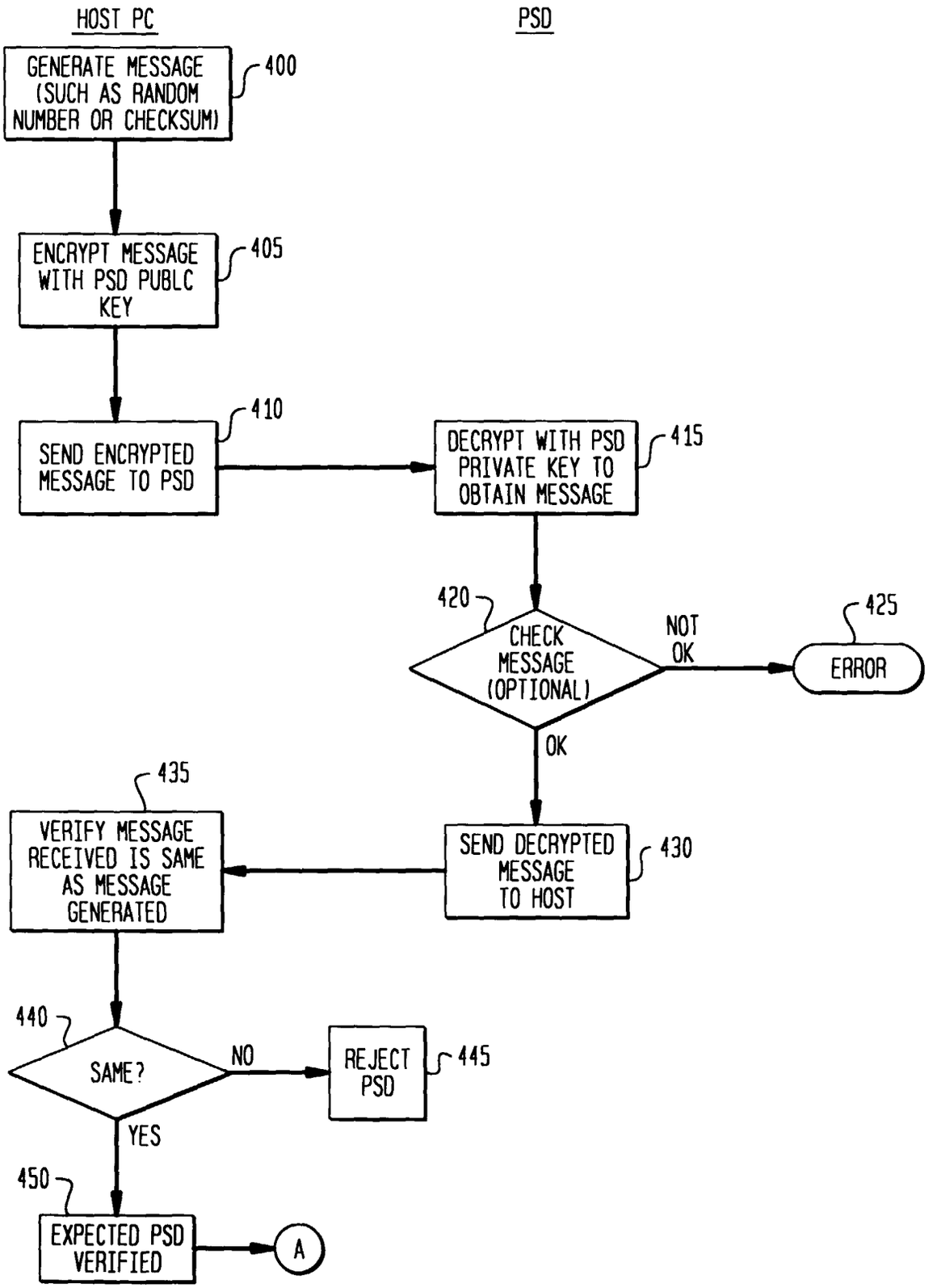
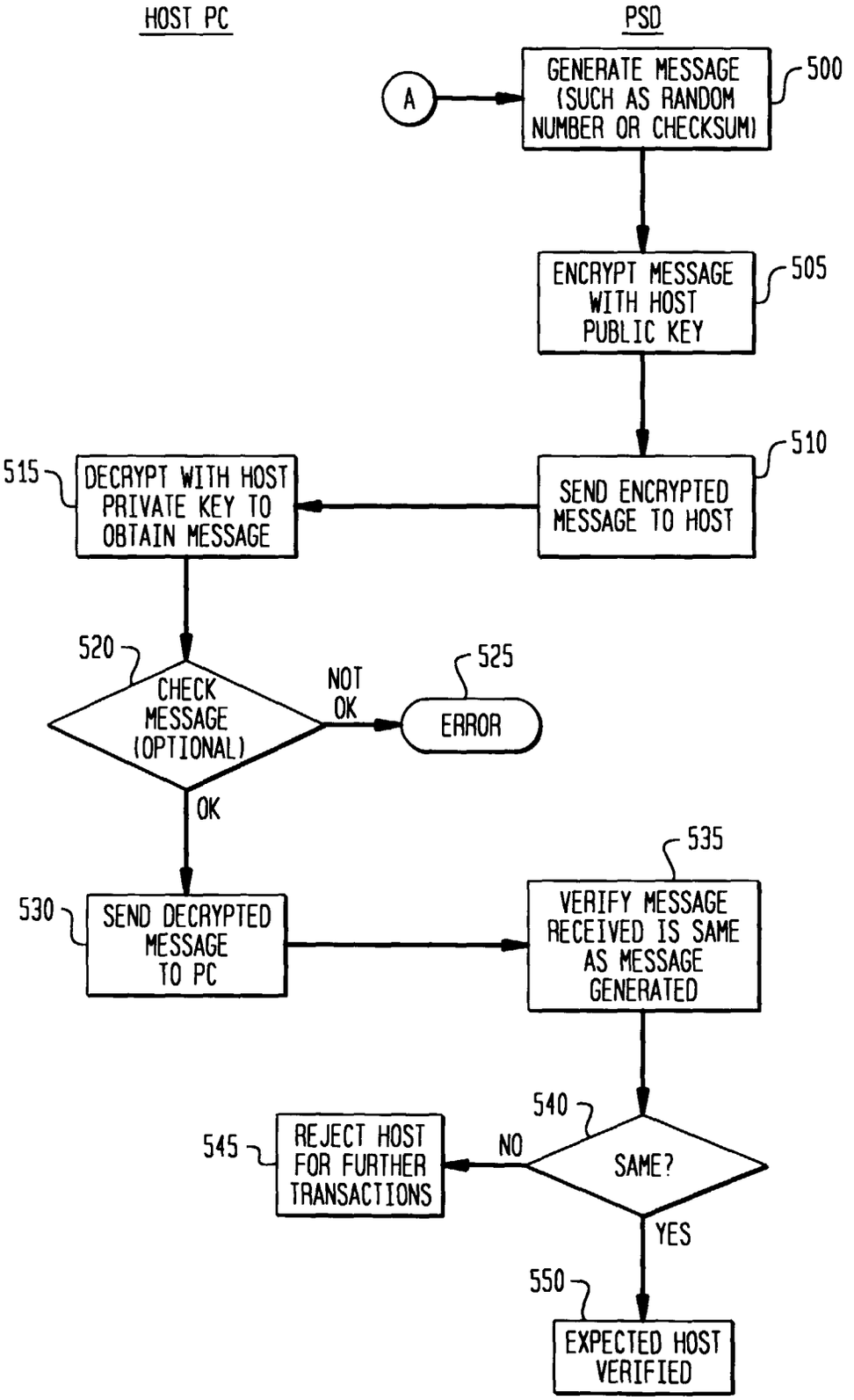

HOST PC
PSD
GENERATE MESSAGE (SUCH AS RANDOM NUMBER OR CHECKSUM)
400
ENCRYPT MESSAGE WITH PSD PUBLC KEY
405
SEND ENCRYPTED MESSAGE TO PSD
410
DECRYPT WITH PSD PRIVATE KEY TO OBTAIN MESSAGE
415
420
CHECK MESSAGE (OPTIONAL)
NOT OK
425
ERROR
OK
435
VERIFY MESSAGE RECEIVED IS SAME AS MESSAGE GENERATED
SEND DECRYPTED MESSAGE TO HOST
430
440
SAME?
NO
REJECT PSD
445
YES
450
EXPECTED PSD VERIFIED
A

FIG. 6


HOST PC
PSD
A
GENERATE MESSAGE (SUCH AS RANDOM NUMBER OR CHECKSUM)
500
ENCRYPT MESSAGE WITH HOST PUBLIC KEY
505
SEND ENCRYPTED MESSAGE TO HOST
510
DECRYPT WITH HOST PRIVATE KEY TO OBTAIN MESSAGE
515
CHECK MESSAGE (OPTIONAL)
520
NOT OK
ERROR
525
OK
SEND DECRYPTED MESSAGE TO PC
530
VERIFY MESSAGE RECEIVED IS SAME AS MESSAGE GENERATED
535
SAME?
540
NO
REJECT HOST FOR FURTHER TRANSACTIONS
545
YES
EXPECTED HOST VERIFIED
550