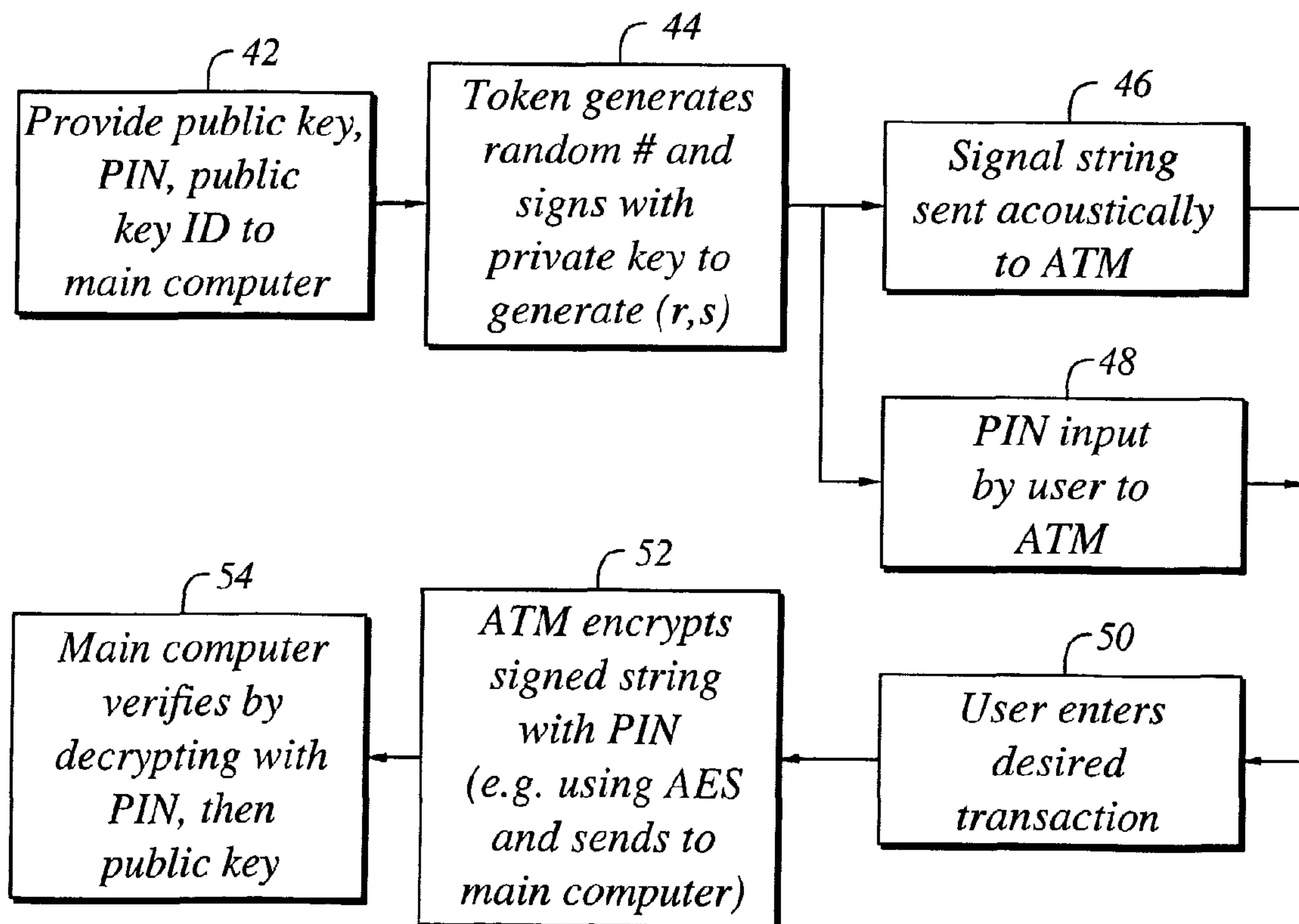




(86) Date de dépôt PCT/PCT Filing Date: 2003/02/12
(87) Date publication PCT/PCT Publication Date: 2003/08/28
(85) Entrée phase nationale/National Entry: 2004/08/16
(86) N° demande PCT/PCT Application No.: US 2003/004387
(87) N° publication PCT/PCT Publication No.: 2003/071770
(30) Priorités/Priorities: 2002/02/15 (10/077,365) US;
2002/05/06 (10/139,873) US

(51) Cl.Int.⁷/Int.Cl.⁷ H04M 3/38, H04M 11/00, H04L 9/00,
H04K 1/00
(71) Demandeur/Applicant:
QUALCOMM INCORPORATED, US
(72) Inventeurs/Inventors:
GANTMAN, ALEXANDER, US;
ROSE, GREGORY G., AU
(74) Agent: SMART & BIGGAR

(54) Titre : SYSTEME ET PROCEDE D'AUTHENTIFICATION ACOUSTIQUE A DEUX FACTEURS
(54) Title: SYSTEM AND METHOD FOR ACOUSTIC TWO FACTOR AUTHENTICATION



(57) Abrégé/Abstract:

A hand-held token can be operated to generate an acoustic or other wireless signal representing a digital signature produced from the private key of a public key pair (44), with the public key being confidential in that it is known only to authorized entities, such as bank computers. The signal from the token can be received by, e.g., a receiver at a bank ATM (46) that also requires a PIN for account access. The user enters the PIN into the ATM (48), and the ATM (52) encrypts the signal from the token with the PIN and sends it on to the bank computer (54) over a link that need not be secure, since even if the PIN is guessed there is no way to verify that it is the correct PIN without also knowing the confidential public key held by the bank computer.



(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
28 August 2003 (28.08.2003)

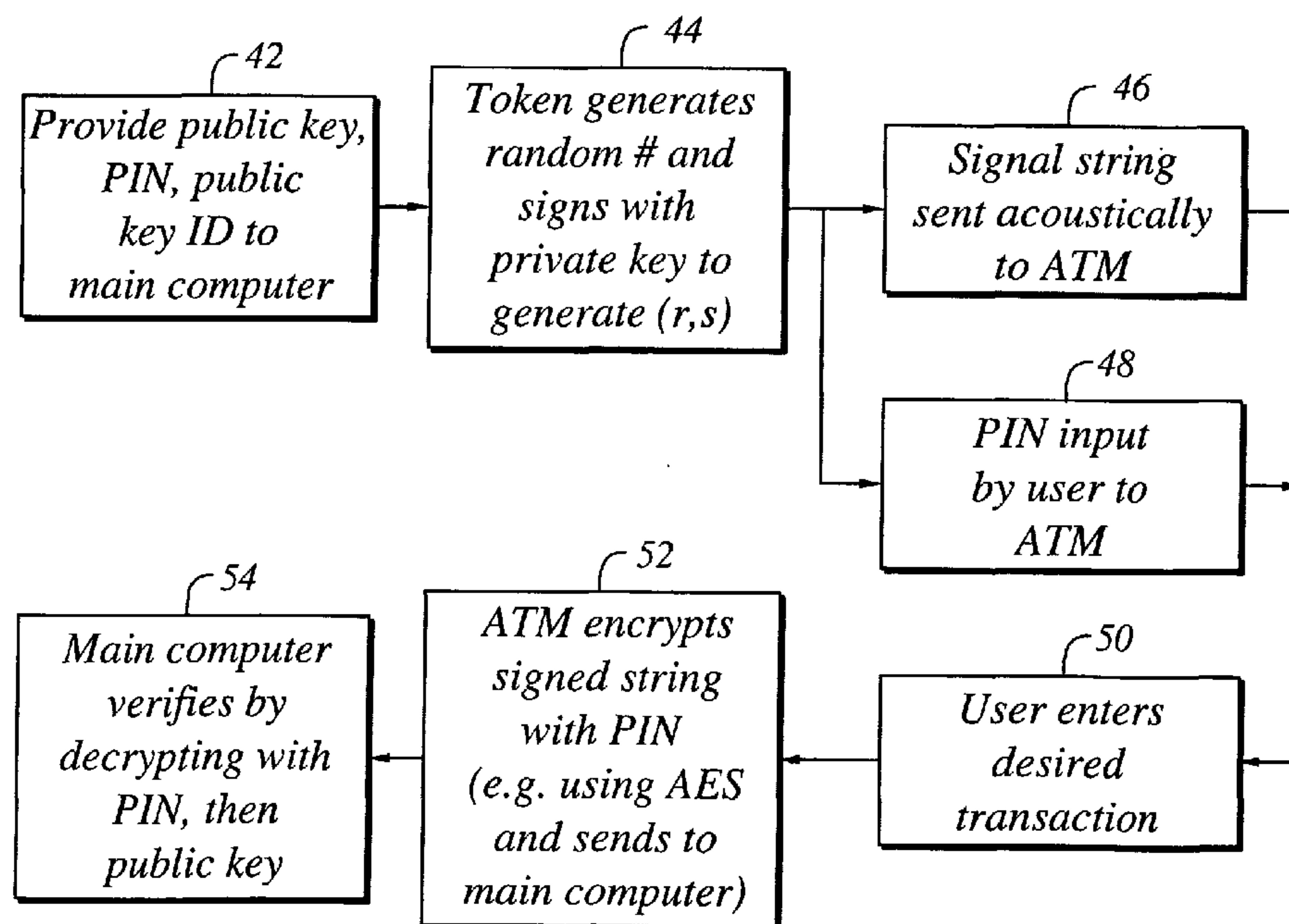
PCT

(10) International Publication Number
WO 03/071770 A1

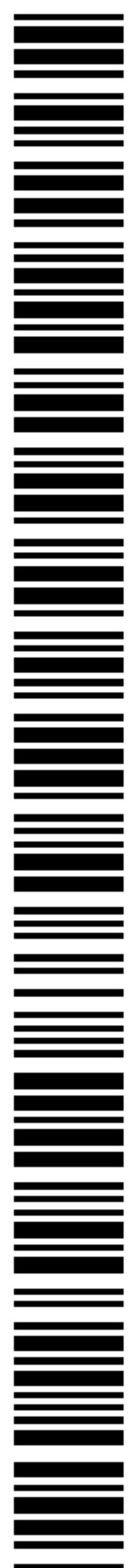
- (51) International Patent Classification⁷: **H04M 3/38**, 11/00, H04K 1/00, H04L 9/00
- (74) Agents: **WADSWORTH, Philip R.** et al.; 5775 Morehouse Drive, San Diego, CA 92121 (US).
- (21) International Application Number: PCT/US03/04387
- (22) International Filing Date: 12 February 2003 (12.02.2003)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
10/077,365 15 February 2002 (15.02.2002) US
10/139,873 6 May 2002 (06.05.2002) US
- (71) Applicant: **QUALCOMM, INCORPORATED**
[US/US]; 5775 Morehouse Drive, San Diego, CA 92121 (US).
- (72) Inventors: **GANTMAN, Alexander**; 8704 Creekwood Lane, San Diego, CA 92129 (US). **ROSE, Gregory G.**; 40 Archer Street, Concord, New South Wales NSW2137 (AU).
- (81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.
- (84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).
- Published:**
— with international search report

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR ACOUSTIC TWO FACTOR AUTHENTICATION



(57) Abstract: A hand-held token can be operated to generate an acoustic or other wireless signal representing a digital signature produced from the private key of a public key pair (44), with the public key being confidential in that it is known only to authorized entities, such as bank computers. The signal from the token can be received by, e.g., a receiver at a bank ATM (46) that also requires a PIN for account access. The user enters the PIN into the ATM (48), and the ATM (52) encrypts the signal from the token with the PIN and sends it on to the bank computer (54) over a link that need not be secure, since even if the PIN is guessed there is no way to verify that it is the correct PIN without also knowing the confidential public key held by the bank computer.



WO 03/071770 A1

WO 03/071770 A1



For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SYSTEM AND METHOD FOR ACOUSTIC TWO FACTOR AUTHENTICATION

RELATED APPLICATIONS

[0001] This application is a continuation-in-part of co-pending U.S. patent application serial no. 10/077,365, filed February 15, 2002, for an invention entitled "Method and Apparatus for Simplified Audio Authentication", which is incorporated herein by reference.

I. Field Of The Invention

[0002] The present invention relates generally to authentication using audio tones.

II. Background Of The Invention

[0003] As Internet use has grown, many types of convenient electronic commerce have been made possible, such as, for example, buying goods and services online, banking online, and using automatic teller machines (ATM) that are linked to remote banks. But the very convenience of electronic commerce has made it easier for thieves to steal valuable information and/or to pose as someone they are not to purchase goods, withdraw money from bank accounts, and so on.

[0004] Accordingly, affording security in electronic transactions is crucial. To this end, many electronic transactions are encrypted, to conceal private information being exchanged. But encryption is only one aspect of security, since it is possible for a thief to break the encryption or to come into possession of an otherwise valid item such as a credit card, pose as the owner, and participate in an encrypted transaction.

[0005] With this in mind, it readily may be appreciated that authentication is an important aspect of security. In terms of electronic commerce, the person seeking authentication does so through a computer interface. Consequently, it normally is not feasible to resort to checking a biological feature of the person (appearance, handwritten signature, fingerprint, and so on) to verify that the person is who he says he is, absent the widespread installation of an infrastructure of bio-sensing computer accessories.

[0006] This leaves two authentication factors available, namely, authenticating a person based on something the person has, such as a credit card or key fob, or based on something the person knows, such as a password or personal identification number (PIN). For some particularly sensitive applications such as ATM money withdrawals, both factors might be desirable.

[0007] Currently, a user of an ATM engages an authentication device such as a credit card with the ATM, and then inputs a PIN. In this way, two factor authentication is achieved. However, the ATM must transmit both the secret information on the card and the PIN to a central bank computer for authentication. Consequently, the link between the bank and the ATM must be secure to prevent a thief from eavesdropping on the line and discovering both authentication factors, which otherwise could enable the thief to steal money from the user's account. This places a considerable burden on the link infrastructure.

[0008] The above-identified patent applications disclose hand-held sonic-based "tokens" that a person can manipulate to transmit an acoustic signal representing secret information to a device, referred to as an "authenticator", "verifier", or "receiver", to authenticate the person based on the signal. As recognized in those applications, the advantage of sonic-based tokens is that a large installed infrastructure already exists to receive and transmit sound and electronic signals derived from sound. Specifically, the global telephone system exists to transmit data representative of acoustic information, and apart from telephones many computing devices that are now linked by this same system (as embodied in the Internet) have microphones and speakers (or can easily be modified to have them).

[0009] As recognized herein, when used in the context of ATMs, sonic tokens have the advantage of transmitting the private information on the token to the ATM in a fashion that prevents the ATM from being able to forge the private information without a confidential key. The ATM simply sends the private information to the central bank computer for authentication. Thus, neither the ATM nor the link between the ATM and the bank need be secure to protect this authentication factor. However, the present invention further recognizes that the second authentication factor - the PIN - still requires link security. This is because PINs generally consist of only 4-6 digits, and an attacker could snoop the line between the ATM and bank, and if the communication allowed a guessed PIN to be verified, the attacker

could simply try out the million or so possible PIN values and remember the one that worked until such time as the attacker could steal the token and gain access to the account. Consequently, secure communication between the bank and ATM, unfortunately, would still be required.

[0010] Having recognized the above problem, the invention disclosed herein is provided.

[00010]

SUMMARY OF THE INVENTION

[0011] A method for authentication includes initially providing a PIN and a confidential public key to an authorizing computer, e.g., a bank computer, and establishing a communication link between the authorizing computer and a receiver, e.g., an ATM, that is remote from the computer. The communication link is not constrained to be secure. Subsequently, a user's acoustic signal can be received at the receiver (e.g., ATM), with the signal being representative of a private key-generated digital signature, and with the receiver transforming the acoustic signal to a signature signal. The PIN is also received by the receiver by, e.g., a user typing it in on a data entry device associated with the receiver, so that the PIN is received separately from the acoustic signal. The signature signal is encrypted with the PIN to render an encrypted signature signal, which is then sent to the authorizing computer for verification of the signature using the PIN and confidential public key.

[0012] Preferably, the signature signal is encrypted with the PIN by the receiver. The acoustic signal, on the other hand, preferably is transmitted using a hand-held token. A desired transaction can be input to the receiver, with the authorizing computer authorizing the receiver to execute the transaction only if the signature is verified.

[0013] The signature is verified by the authorization computer by decrypting the encrypted signature signal using the PIN to render the signature signal. Then, the resulting signature signal is verified using the confidential public key.

[0014] In a preferred embodiment, the token generates a signature signal by combining a message with the private key. The message can include at least a portion of a timestamp, e.g., a predetermined number of least significant bits of a timestamp having more bits than the predetermined number.

[00011]

[0015] In another aspect, a system is disclosed for two-factor authentication over a link that is not constrained to be secure. The system includes a portable token that generates a wireless signal representing a digitally signed message. A receiver receives the wireless signal and a PIN, with the PIN being received separately from the wireless signal. The receiver encrypts the signed message with the PIN to render an encrypted signed message. An authorizing computer receives the encrypted signed message over the link and accesses the PIN and a confidential public key to attempt to verify the signed message.

[0016] In still another aspect, a system for authentication includes an authorizing computer accessing at least a PIN and a confidential public key and communicating over a link with at least one receiver remote from the computer. The communication link is not constrained to be secure. The system includes means for receiving, at the receiver, a wireless signal that represents a digital signature generated by combining a message with a private key. The receiver transforms the wireless signal to a signature signal. Means at the receiver also receive the PIN. Means are provided for encrypting the signature signal with the PIN to render an encrypted signature signal. The encrypted signature signal is sent to the authorizing computer over the link for verification of the signature using the PIN and confidential public key.

[0017] The details of the present invention, both as to its structure and operation, can best be understood in reference to the accompanying drawings, in which like reference numerals refer to like parts, and in which:

BRIEF DESCRIPTION OF THE DRAWINGS

[0018] Figure 1 is a block diagram of the present system for audio-based authentication; and

[0019] Figure 2 is a flow chart of the present logic.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

[0020] Referring initially to Figure 1, a system is shown, generally designated 10, that includes a portable hand-held token 12 that can be configured as a key fob or other small device. The present invention, however, applies to other token configurations, such as mobile communication stations including laptop computers, wireless handsets or telephones, data transceivers, or paging and position determination receivers that can be hand-held or portable as in vehicle-mounted (including cars, trucks, boats, planes, trains), as desired. Wireless

communication devices are also sometimes referred to as user terminals, mobile stations, mobile units, subscriber units, mobile radios or radiotelephones, wireless units, or simply as "users" and "mobiles" in some communication systems.

[0021] In any case, the token 12 can generate an acoustic signal, represented schematically by the lines 14, that can be received by a receiver 16. The receiver 16 is associated with authorizing computer 18. In an illustrative embodiment, the receiver 16 is an automatic teller machine (ATM) and the authorizing computer 18 is a bank main computer, although it is to be understood that the receiver 16 may be a receiving device associated with, e.g., a building, a home, a vehicle, or any other component to which it is desired to limit access to pre-authorized users using two factor authentication. It is to be further understood that while the preferred token 12 is a sonic token that generates an acoustic signal, the present principles apply to other wireless signal-generating tokens including those that might use electromagnetic wave wireless communication principles, e.g., radiofrequency (rf) such as Bluetooth and infrared, to transmit the below-disclosed digital signature to the receiver 16.

[00012]

[0022] The preferred acoustic signal 14 can represent a digital signature that is generated using a private key stored in an electronic data store 20 of the token 12. A pseudorandom number (PN) generator 21 can also be included on the token 12. Corresponding confidential public keys or confidential public key identifications can also be stored therein for purposes to be shortly disclosed.

[0023] In accordance with private key/public key principles known in the art and set forth in, e.g., the National Institute for Standards and Technology (NIST) Federal Information Processing Standards Publication 186-2, January, 2000, the signature algorithm in the token 12 (executed by a microprocessor 22 within the token 12) receives as input (and thus "combines") the private key and at least a portion of the message to be signed and with a random number "k" from the PN generator 21 to render a digital signature which is a random pair (r,s). Preferably, the microprocessor 22 executes the signature algorithm upon receipt of activation signals from, e.g., one or more activation elements 24 such as toggle switches, voice activation devices, or pushbuttons. The message being signed and the identity of the confidential public key corresponding to the private key also are preferably included in the signal generated by the microprocessor 22. It is to be understood that the microprocessor 22

can include a digital processor proper as well as necessary clocks, analog to digital conversion circuitry, and digital to analog conversion circuitry known in the art.

[0024] The microprocessor 22 accesses the data store 20, such that when multiple activation elements 24 are used, one or more can be associated with a respective private key in the store 22. The electronic signature signals are sent to an audio speaker 26 for transformation of the electronic signature signal to the acoustic signal 14. The acoustic signal may or may not be audible. If desired, a microphone 28 can also be provided on the token 12 to receive acoustic signals and transform them to electronic signals, which are sent to the microprocessor 22 for processing. When EM wave wireless principles are used, the speaker 26 is replaced by, e.g., an rf transmitter or IR transmitter.

[00013]

[0025] The preferred acoustic signal 14 is received by a microphone or other acoustic receiving device 30 at the receiver 16. The acoustic signal is transformed by the microphone 20 back to an electronic signature signal (with accompanying confidential public key ID and original pre-signed message, if desired) and sent to a microprocessor 32, which may access a data store 34 if desirable. If desired, a speaker 36 can also be provided on the receiver 16 to send acoustic signals back to the token 12, which signals are received by the microphone 28 on the token 12.

[0026] When the receiver 16 is an ATM and the authorizing computer 18 is a central bank computer, the authorizing computer 18 can include a processor 38 that accesses a data store 40 to selectively grant authorization by verifying (or not) the digital signature received from the receiver 16. The data store 40 can include a data structure such as a list or database table which stores the confidential public key (and its ID) that is associated with the private key represented by the signal. In any case, the link 41 connecting the bank with the ATM need not be secure, owing to the novel use of cryptography disclosed below.

[0027] Figure 2 shows the logic of the present invention. Commencing at block 42, the confidential public key(s) associated with the token 12, along with the IDs of the public keys, are provided to the authorizing computer 18 (e.g., main bank computer). Also, the user's PIN is provided. This provision is done securely, either in person or over a secure connection. By "confidential public key" is meant a public key in accordance with private key/public key

principles known in the art, except that the confidential public key is not publicly accessible, but rather is provided only to trusted entities, such as a main bank computer.

[00014]

[0028] Moving to block 44, when a user manipulates one of the activation elements 24 the signature algorithm in the token 12 receives as input the private key, a pseudorandom number, and a message, such as all or a portion of a timestamp, to generate an electronic signature, e.g., a random pair (r,s). The user then inputs both factors of authentication into the receiver 16. Specifically, at block 46 the digital signature is wirelessly (e.g., acoustically) sent to the receiver 16, along with the message that was signed and if desired the ID of the corresponding confidential public key, and at block 48 the user inputs the PIN using, e.g., the numeric keypad that is provided on most ATMs. The desired transaction (e.g., withdrawal, funds transfer, etc.) is entered at block 50. It is to be understood that the steps at blocks 46, 48, and 50 can be executed in any order.

[0029] In accordance with the present invention, at block 52 the receiver 16 encrypts the signature (r,s) with the PIN. This encryption can be a symmetric encryption using, e.g., AES encryption principles. The encrypted signature, along with the unencrypted confidential public key ID and unencrypted pre-signed message being signed (e.g., a timestamp or least two significant bits thereof) are sent to the main computer processor 38.

[0030] At block 54, the main processor 38 first decrypts the digital signature using the PIN. Then, using the confidential public key ID and original pre-signed message, the processor retrieves from the data store 40 the appropriate confidential public key and verifies the signature in accordance with public key/private key principles known in the art. If verification is successful, the authorizing computer 18 signals the receiver 16 to allow access. In the case of an ATM verifier 16 and bank computer authorizing computer 18, the bank computer signals the ATM to execute the requested transaction.

[00015]

[0031] It may now be appreciated that an attacker who might intercept ATM-bank communications on the link 41 could not deduce the PIN. Specifically, decrypting the signature using the "correct" PIN will yield the equivalent of decrypting it using an incorrect PIN, i.e., a random pair that can't be understood without verifying the signature, something that cannot be done without the confidential public key and the data being signed (note that

only the least significant bits of the timestamp are transmitted). This feature removes the final requirement for security on the link 41.

[0032] While the particular SYSTEM AND METHOD FOR ACOUSTIC TWO FACTOR AUTHENTICATION as herein shown and described in detail is fully capable of attaining the above-described objects of the invention, it is to be understood that it is the presently preferred embodiment of the present invention and is thus representative of the subject matter which is broadly contemplated by the present invention, that the scope of the present invention fully encompasses other embodiments which may become obvious to those skilled in the art, and that the scope of the present invention is accordingly to be limited by nothing other than the appended claims, in which reference to an element in the singular is not intended to mean "one and only one" unless explicitly so stated, but rather "one or more". All structural and functional equivalents to the elements of the above-described preferred embodiment that are known or later come to be known to those of ordinary skill in the art are expressly incorporated herein by reference and are intended to be encompassed by the present claims. Moreover, it is not necessary for a device or method to address each and every problem sought to be solved by the present invention, for it to be encompassed by the present claims. Furthermore, no element, component, or method step in the present disclosure is intended to be dedicated to the public regardless of whether the element, component, or method step is explicitly recited in the claims. No claim element herein is to be construed under the provisions of 35 U.S.C. §112, sixth paragraph, unless the element is expressly recited using the phrase "means for" or, in the case of a method claim, the element is recited as a "step" instead of an "act".

WHAT IS CLAIMED IS:

CLAIMS

1. A method for authentication, comprising:
providing at least a PIN and a confidential public key to an authorizing computer;
establishing a communication link between the authorizing computer and at least one receiver remote from the computer, the communication link not being constrained to be secure;
receiving, at the receiver, at least one acoustic signal representative of at least one private key-generated signal, the receiver transforming the acoustic signal to a signature signal;
receiving, at the receiver, the PIN, the PIN being received separately from the acoustic signal;
encrypting the signature signal with the PIN to render an encrypted signature signal;
and
sending the encrypted signature signal to the authorizing computer for verification of the signature using the PIN and confidential public key.
2. The method of Claim 1, wherein the act of encrypting is undertaken at the receiver.
3. The method of Claim 1, comprising transmitting the acoustic signal using a hand-held token.
4. The method of Claim 1, further comprising inputting a desired transaction to the receiver, the authorizing computer authorizing the receiver to execute the transaction only if the signature is verified.
5. The method of Claim 1, wherein the signature is verified by:
decrypting the encrypted signature signal using the PIN to render the signature signal;
then

verifying the signature signal using the confidential public key.

6. The method of Claim 3, wherein the token generates a signature signal by combining at least one message with the private key.

7. The method of Claim 6, wherein the message includes at least a portion of at least one timestamp.

8. The method of Claim 7, wherein the portion of the timestamp is a predetermined number of least significant bits of a timestamp having more bits than the predetermined number.

9. A system for two-factor authentication over a link not constrained to be secure, comprising:

at least one portable token generating at least one wireless signal representing a digitally signed message;

at least one receiver receiving the wireless signal and a PIN, the PIN being received separately from the wireless signal, the receiver encrypting the signed message with the PIN to render an encrypted signed message; and

at least one authorizing computer receiving at least the encrypted signed message over the link, the authorizing computer accessing the PIN and a confidential public key to attempt to verify the signed message.

10. The system of Claim 9, wherein the wireless signal also represents at least an ID of a confidential public key and a message that was signed by a private key corresponding to the public key to render the digitally signed message.

11. The system of Claim 10, wherein the receiver sends the encrypted signed message, ID, and message that was signed to the authorizing computer.

12. The system of Claim 10, wherein the authorizing computer decrypts the

encrypted signed message using the PIN and then verifies the signed message by accessing the confidential public key using the ID and using the confidential public key.

13. A system for authentication including an authorizing computer accessing at least a PIN and a confidential public key and communicating over a link with at least one receiver remote from the computer, the communication link not being constrained to be secure, the system comprising:

means for receiving, at the receiver, at least one wireless signal representative of at least one digital signature produced from a private key, the receiver transforming the wireless signal to a signature signal;

means for receiving, at the receiver, the PIN; and

means for encrypting the signature signal with the PIN to render an encrypted signature signal, wherein the encrypted signature signal is sent to the authorizing computer over the link for verification of the signature using the PIN and confidential public key.

14. The system of Claim 13, wherein the means for encrypting are at the receiver.

15. The system of Claim 13, comprising means for transmitting the wireless signal using a hand-held token.

16. The system of Claim 13, further comprising means for inputting a desired transaction to the receiver, the authorizing computer authorizing the receiver to execute the transaction only if the signature is verified.

17. The system of Claim 13, comprising:

means for decrypting the encrypted signature signal using the PIN to render the signature signal; and

means for verifying the signature signal using the confidential public key.

18. The system of Claim 15, wherein the token generates a signature signal by combining at least one message with the private key.

19. The system of Claim 18, wherein the message includes at least a portion of at least one timestamp.

20. The system of Claim 18, wherein the message is further combined with a pseudorandom number.

21. The system of Claim 13, wherein the wireless signal is an acoustic signal.

22. The system of Claim 9, wherein the wireless signal is an acoustic signal.

23. A computer readable medium containing instructions for controlling a computer system to perform a method, the method comprising:

providing at least a PIN and a confidential public key to an authorizing computer;

establishing a communication link between the authorizing computer and at least one receiver remote from the computer, the communication link not being constrained to be secure;

receiving, at the receiver, at least one acoustic signal representative of at least one private key-generated signal, the receiver transforming the acoustic signal to a signature signal;

receiving, at the receiver, the PIN, the PIN being received separately from the acoustic signal;

encrypting the signature signal with the PIN to render an encrypted signature signal;

and

sending the encrypted signature signal to the authorizing computer for verification of the signature using the PIN and confidential public key.

24. The computer readable medium Claim 23, wherein the act of encrypting is undertaken at the receiver.

25. The computer readable medium Claim 23, comprising transmitting the acoustic

signal using a hand-held token.

26. The computer readable medium Claim 23, further comprising inputting a desired transaction to the receiver, the authorizing computer authorizing the receiver to execute the transaction only if the signature is verified.

27. The computer readable medium Claim 23, wherein the signature is verified by:
decrypting the encrypted signature signal using the PIN to render the signature signal;
then
verifying the signature signal using the confidential public key.

28. The computer readable medium Claim 25, wherein the token generates a signature signal by combining at least one message with the private key.

29. The computer readable medium Claim 28, wherein the message comprises at least a portion of at least one timestamp.

30. The computer readable medium Claim 29, wherein the portion of the timestamp is a predetermined number of least significant bits of a timestamp having more bits than the predetermined number.

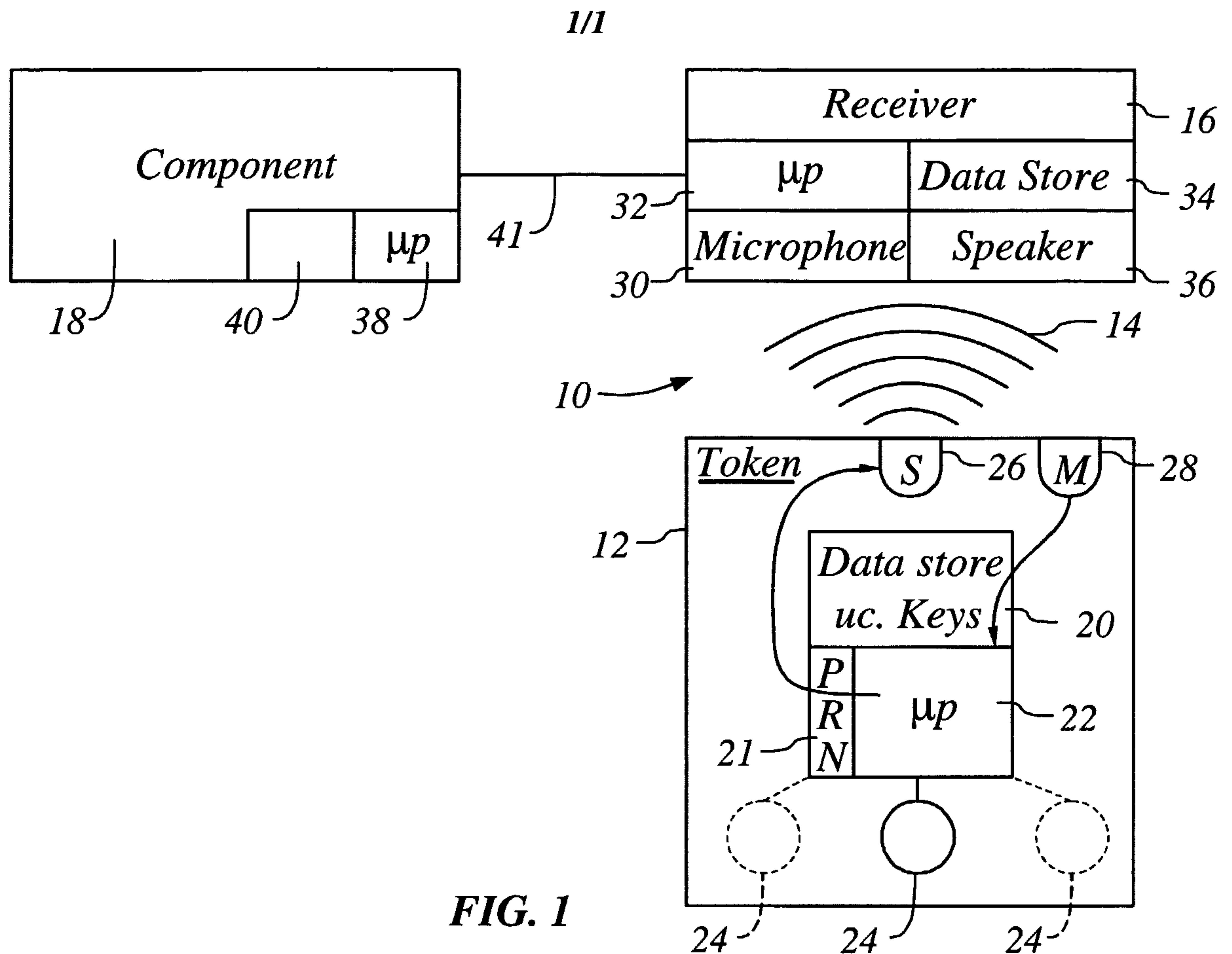


FIG. 1

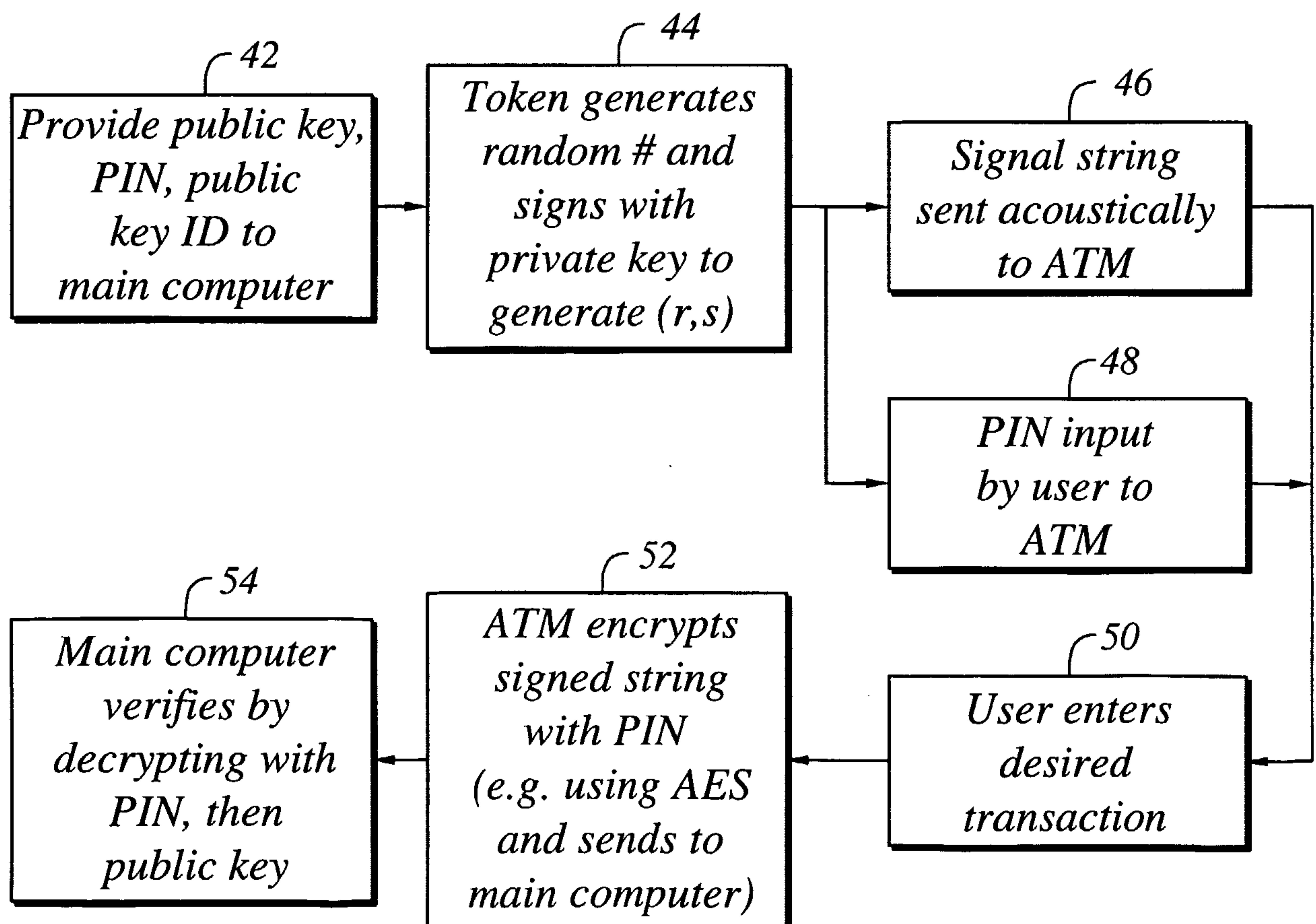


FIG. 2

