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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 September 2003 (04.09.2003)

PCT

(10) International Publication Number
WO 03/073688 A1

(51) International Patent Classification⁷: H04L 9/00, H04K 1/00

(21) International Application Number: PCT/US03/04411

(22) International Filing Date: 14 February 2003 (14.02.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/359,221	22 February 2002 (22.02.2002)	US
10/222,090	15 August 2002 (15.08.2002)	US

(71) Applicant: LEGATO SYSTEMS, INC. [US/US]; 2350 West El Camino Real, Mountain View, CA 94040 (US).

(72) Inventor: JOHNSON, Randall; 252 North 850 East, Pleasant Grove, UT 84062 (US).

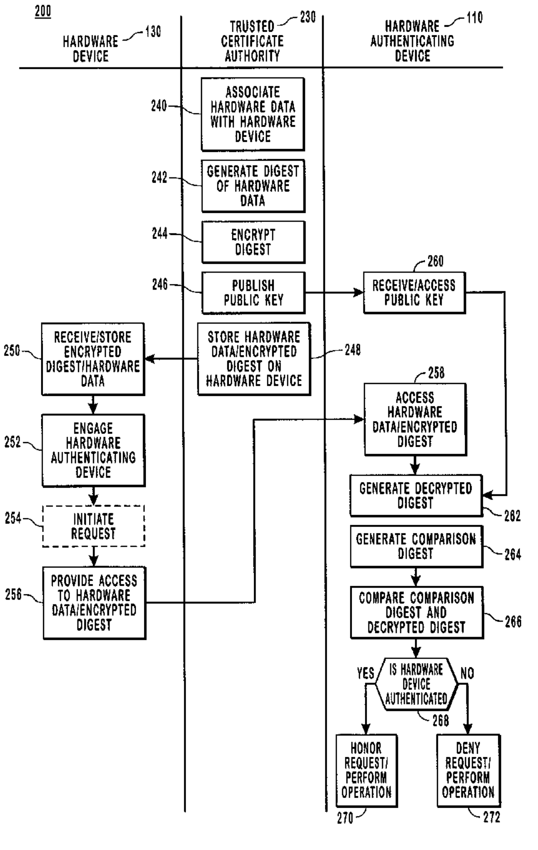
(74) Agents: ISRAELSEN, R., Burns et al.; Workman, Nydegger & Seeley, 1000 Eagle Gate Tower, 60 East South Temple, Salt Lake City, UT 84111 (US).

(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).

[Continued on next page]

(54) Title: AUTHENTICATING HARDWARE DEVICES INCORPORATING DIGITAL CERTIFICATES


200
HARDWARE DEVICE
130
TRUSTED CERTIFICATE AUTHORITY
230
HARDWARE AUTHENTICATING DEVICE
110
ASSOCIATE HARDWARE DATA WITH HARDWARE DEVICE
240
GENERATE DIGEST OF HARDWARE DATA
242
ENCRYPT DIGEST
244
PUBLISH PUBLIC KEY
246
RECEIVE/ACCESS PUBLIC KEY
260
RECEIVE/STORE ENCRYPTED DIGEST/HARDWARE DATA
250
STORE HARDWARE DATA/ENCRYPTED DIGEST ON HARDWARE DEVICE
248
ACCESS HARDWARE DATA/ENCRYPTED DIGEST
258
ENGAGE HARDWARE AUTHENTICATING DEVICE
252
INITIATE REQUEST
254
PROVIDE ACCESS TO HARDWARE DATA/ENCRYPTED DIGEST
256
GENERATE DECRYPTED DIGEST
262
GENERATE COMPARISON DIGEST
264
COMPARE COMPARISON DIGEST AND DECRYPTED DIGEST
266
IS HARDWARE DEVICE AUTHENTICATED
268
YES
NO
HONOR REQUEST/ PERFORM OPERATION
270
DENY REQUEST/ PERFORM OPERATION
272

(57) Abstract: Methods for authenticating hardware devices (130) incorporating digital certificates include a trusted certificate authority (230) assigning hardware data (240) to a hardware device (130). A hash algorithm applied to the hardware data, which generally comprises information identifying or associated with the hardware device (130), generates a digest (242) that is encrypted (244) by the private key of the trusted certificate authority. The encrypted digest and hardware data are stored (248) in a hardware component of the hardware device (130) and are accessed (258) by an authenticating device (110) using the public key of the trusted certificate authority (230) to decipher and create a decrypted digest (262) of the encrypted digest. The decrypted digest is then compared (266) to a comparison digest that is created (264) by applying the hash algorithm to the stored hardware data. The hardware device (130) is finally authenticated when the decrypted digest and the comparison digest are the same (268).

WO 03/073688 A1

Published:

— *with international search report*

AUTHENTICATING HARDWARE DEVICES INCORPORATING DIGITAL CERTIFICATES

BACKGROUND OF THE INVENTION

1. The Field of the Invention

The present invention relates generally to the field of cryptography, and more specifically to the use of digital certificates for authenticating hardware devices and components.

2. Background and Related Art

Technological improvements have had a tremendous impact on how people communicate. For example, it is now commonplace to use a computer device to send and receive email or other communications directly through the Internet. Remote communications over the Internet can be convenient and sometimes practical. However, in today's world of networking and ever increasing convenience of communications, there is a need to improve the security of private communications, particularly electronic communications. Identity fraud boldly underscores this need. Although encryption technologies make it possible to encrypt communications transmitted over an electronic medium, the security provided by encryption is somewhat limited, as described below.

Symmetric cryptography enables a single block cipher key to encrypt a message before it is sent and the same key to decrypt the message once it is received. This technology prevents anyone from deciphering the message without the block cipher key. This also ensures that any message that can be decrypted with the block cipher key came from a party who possesses the same key. In this manner it is theoretically possible to know or at least verify the identity of the party sending a message encrypted with the block cipher key, provided only two parties, the sender and the receiver, possess the block cipher key. However, because it is necessary to send the intended recipient the block cipher key, it is possible that the block cipher key will be intercepted in transit, such as by a computer hacker, thereby compromising the security of the encrypted communications. Accordingly, any communication based on symmetric cryptography is only as secure as the means for transmitting the block cipher key between the communicating parties.

Asymmetric cryptography overcomes some of these problems, which are associated with key transmission, by creating a pair of asymmetric keys, in which one key, known as a public key, is intentionally published and another key, known as a private key, is not published or transmitted, even to the intended recipient. With an asymmetric key pair, data that is encrypted with the private key can only be decrypted with the corresponding public key.

With asymmetric cryptography, data that is encrypted with the public key can also only be decrypted with the corresponding private key. Accordingly, a message encrypted with an asymmetric public key can be securely sent to a party holding the corresponding private key, irrespective of whether or not the public key has fallen into the hands of a hacker or an unintended recipient because the message can only be decrypted with the private key.

One problem with asymmetric cryptography, however, is that it requires substantial computing resources for the encryption and decryption of data, and is therefore impractical and inefficient for the transmission of large quantities of data. Therefore, asymmetric cryptography is often used exclusively to identify parties in communication and to transmit extremely sensitive information, such as a one-time use symmetric block cipher key which can be used for more efficient encryption. Asymmetric cryptography can be used to identify the sender of a message, for example, because only messages encrypted with a private key can be decrypted with the corresponding public key that is publicly known to be associated with a particular person. Therefore, when a message is decrypted with a particular public key, it is known that the message originated from the person who is associated with that public key and who encrypted the message with the corresponding private key. Thus, encryption of a document using a private key is analogous to a digital signature of the document.

One problem with asymmetric cryptography, however, is that if the recipient of the encrypted message does not have access to the sender's public key then the recipient cannot use the public key to authenticate the identity of the sender. Although the party sending the message may include their public key in a transmission sent to the recipient, the recipient is unable to verify the identity of the sender. In particular, the sender may be using a key pair associated with an alias. Therefore, in order to verify the identity of the sender, it is sometimes necessary to first verify that the public key is an authentic public key associated with the identity of the sender. This may be accomplished, for example, using digital certificates.

A digital certificate generally comprises a second layer of asymmetric cryptography that is applied by a trusted certificate authority. Trusted certificate authorities, such as Verisign®, are well known in the art. A trusted certificate authority certifies that a public key belongs to a particular party by digitally signing the public key along with information identifying the party that is assigned to the public key.

To create a digital certificate, the trusted certificate authority first creates a hash number, or digest, of the party's public key and corresponding identification information. This may be accomplished, for example, when the trusted certificate authority applies a hash algorithm to the public key and corresponding identification information. Once the digest is created, the trusted certificate authority uses its own private key to encrypt the digest. The encrypted digest or digital certificate can then be used, as an accompaniment to any message, to certify the identity of the sender and the authenticity of the message. To create a signed message, the sender first creates a digest of the message using the well-known hash algorithm. The digest is then encrypted with the sender's private key.

The identity of the sender and the authenticity of the message can generally be authenticated by any recipient of the message by using the public key of the trusted certificate authority, which is publicly known, to decipher the encrypted certificate digest, thereby creating a decrypted digest of the certificate which contains the sender's public key. The decrypted digest can then be compared to a comparison digest that is created by the recipient applying the aforementioned hash algorithm to the personal identifying information and public key of the party sending the message. The association of the party sending the message and the public key contained in the certificate is verified if the comparison digest and the decrypted digest of the certificate are the same. The authenticity of the message signature is then finally verified by applying the previously verified public key to the digest of the message encrypted with the sender's private key and successfully comparing the decrypted digest to a digest of the message created by the recipient.

Asymmetric cryptography is generally more secure than symmetric cryptography because the private key does not have to be transmitted to the intended recipient of an encrypted message. However, despite this advantage, it is still possible for the security of a private key to be compromised by a hacker with access to the device storing the private key. In particular, the hardware or devices used to store the asymmetric key pair can be stolen, accessed, or misused by an unauthorized party unassociated with the digital certificate or private key stored on the device. By way of example, a device, such as a smart card, containing a personal private key or a digital certificate may be stolen or used by another person without authorization to send an unauthorized message or digitally sign a document under the alias of another.

One method for improving security and for preventing the abuse of asymmetric keys described above is to tie the access and operation of the asymmetric keys and digital certificate to an independent identification or verification of the user, such as for example, with a biometric device or another verification device. Biometric devices, such as fingerprint devices and iris scanners, used to detect uniquely identifiable features of a person are well known in the art. A biometric device may be used, for example, to independently verify the identity of an authorized user before enabling access to or operation of a device containing a private key or digital certificate. Therefore, even if the device is stolen, the private key or digital certificate on the device cannot be accessed or utilized until the person using the device is independently verified as an authorized user of the device.

Biometric devices, however, as well as other verification devices, are in and of themselves limited in their ability to protect the user against fraudulent use, as described below, and are therefore correspondingly limited in their ability to provide adequate security. Existing biometric authentication systems consist of multiple components which must work together to authenticate a user. For instance, the biometric authentication system may include a biometric device which copies an image of a particular physical characteristic of a user (e.g. a fingerprint, iris pattern, etc.), an image processor which converts the copied image into data that is easier to work with, an extractor which is configured to recognize key features within the image and to put them into a normalized/listed "feature vector" form, and computer hardware or computer modules that use a matching algorithm to compare the captured feature vector against a specific stored feature vector to authenticate the user. The computer hardware can also use a matching algorithm to compare the captured feature vector against a database of stored feature vector templates for identifying the user.

Typically, the result of using a matching algorithm in biometric systems is a "match" or "no match" verification signal which either validates or invalidates the authentication of the user. However, a hacker can monitor any point of communication between the components of the biometric system, thereby capturing data which can be replayed, or otherwise spoofed to generate a bogus authentication. In addition, biometric scanning devices also transmit biometric information to other devices which extract features and match against stored templates. A hacker monitoring the transmission channel may also be able to capture the biometric data that is transmitted to the other devices and spoof the system at a later time by replaying the previously captured data into the transmission channel.

Once a hacker copies or otherwise obtains the "match" signal from the biometric system, the hacker can operate any device that is conditionally enabled only upon receiving the 'match' signal from the biometric system, thereby enabling the hacker to bypass the security features provided by the biometric system. As a matter of example and not limitation, the hacker could use the spoofed 'match' signal to enable a device storing a private key to execute an unauthorized digital signature with that private key.

Current methods for preventing this undesired void in security is to encrypt the data communicated between the components of the biometric systems and between other devices. Preferably, the encoded data is never repeated, even if the original data is the same. Accordingly, many existing systems are configured so that even if the same data is sent more than once, it is sent with completely different data encodings when it is transmitted between the communicating devices. This can be accomplished, for example, by using symmetric block cipher keys that are used at either end of the communication channel or by encoding an encryption algorithm directly into the communication channel. These methods, however, are unsecure for at least the reasons that have been mentioned above. More particularly, a hacker can collect a sufficient amount of data, over a period of time, to extrapolate the cipher key or encoding algorithm, thereby enabling the hacker to obtain and spoof the verification signal from the authentication device.

Accordingly, any independent verification of a person's identity, such as with a biometric device, can only be considered valid if it can be assured that the verification signal is an authentic signal coming from an authentic verification device, rather than a spoofed signal. Accordingly, there is currently a need in the art to improve the ability to authenticate verification devices and the signals generated by the verification devices to ensure that they have not been spoofed.

The ability to authenticate a piece of hardware, such as a biometric identification device, could also be useful in other industries and applications, such as, for example, manufacturing industries. In manufacturing industries, it is common for a manufacturer seeking to secure revenue associated with selling accessory products to design the base product so that it will only interoperate with or enable the accessory products produced by that manufacturer. However, despite patent law protection and design efforts of manufacturers to ensure that only authentic accessories are compatible with the base product, competitors often succeed in designing, producing, and marketing unauthentic and sometimes infringing accessories that are compatible with the manufacturer's exclusive base product. This is possible, in part, because there are no adequate conventional methods for manufacturers to tie the operability of an accessory product to its authenticity.

Another industry that could benefit from the ability to authenticate a hardware device is the wireless telephone industry. For example, it could be useful to authenticate an authorized telephone device as the source of a telephone signal prior to enabling any telephone communication with that telephone signal, to ensure that the telephone signal is not originating from a fraudulent or unauthorized device using a spoofed telephone signal.

Other industries that could benefit from the ability to authenticate hardware include the automotive and home security industries, among others. For example, it could be useful when a car is started to be able to authenticate that the ignition signal is generated from an authentic key engaging the ignition, rather than from a short circuit that is generated by a thief hotwiring the ignition. It could also be useful to enable the lock of a house or a building to authenticate the key engaging the lock as an authorized key, rather than an unauthorized copy of the key or a picklock device. Although the foregoing uses of authentication processes in association with hardware devices would be useful, there have not previously been adequate authentication techniques that would enable such processes.

Accordingly, because of communications fraud, identity fraud, illegal manufacturing practices, and thievery in general, there is currently a need in the art for improved methods for authenticating hardware devices and systems that can otherwise be infringed or subverted by fraudulent means.

BRIEF SUMMARY OF THE INVENTION

The present invention relates to methods and systems for authenticating hardware devices, and more particularly to methods and systems for certifying the authenticity of hardware devices incorporating digital certificates.

According to one embodiment of the invention, hardware devices store digital certificates certifying the authenticity of the hardware devices and any signals originating therefrom.

A digital certificate is created for a hardware device by a trusted certificate authority that generates and associates hardware data with the hardware device. Hardware data generally comprises information identifying or associated with the hardware device. Hardware data may include, for example, serial numbers, model numbers, manufacturer and part names, public hardware keys, etc.

The trusted certificate authority generates a hash number or a digest of the hardware data, comprising the public hardware key and corresponding information identifying the hardware device, by applying a hash algorithm to the hardware data. Once the digest is created, the digest is encrypted with a private key of the trusted certificate authority. The private key of the trusted certificate authority is an asymmetric key from a key pair that includes a corresponding public key. The encrypted digest and hardware data are stored in a storage component of the hardware device.

During use, the encrypted digest and hardware data are accessed by an authenticating device, which may comprise any device or system interacting with the hardware device. The authenticating device applies the aforementioned hash algorithm to the hardware data, thereby generating a new hash number, or comparison digest, of the hardware data. The authenticating device also generates a decrypted digest by deciphering the encrypted digest with the trusted certificate authority's public key. The decrypted digest and the comparison digest are then compared and the hardware device is finally authenticated when the decrypted digest is the same as the comparison digest. If the decrypted digest differs from the comparison digest then the hardware device is not authenticated.

According to the invention, the authentication of the hardware device may be used as a condition precedent for the operation of the hardware device, the operation of the authenticating device, the operation of any other device, or access to data stored on the hardware device, the authenticating device, or any other device. Authentication of the hardware device can also be required prior to enabling communication between the hardware device and another device or between any combination of other devices.

To ensure that the digital certificate is not stolen from the hardware device and used fraudulently, the invention extends to the use of tamperproof materials, such as ceramics or potting materials, to encapsulate the storage component of the hardware device so that any attempt to remove the storage component will result in fracturing or rendering inoperable the storage component or the hardware device.

In addition, the invention extends to a variety of novel processes that are enabled using the hardware authentication techniques of the invention. Examples of such processes include those in manufacturing industries, wireless telephone industries, home and automotive security systems, and others.

These and other objects and features of the present invention will become more fully apparent from the following description and appended claims, or may be learned by the practice of the invention as set forth hereinafter.

BRIEF DESCRIPTION OF THE DRAWINGS

In order to describe the manner in which the above-recited and other advantages and features of the invention can be obtained, a more particular description of the invention briefly described above will be rendered by reference to specific embodiments thereof which are illustrated in the appended drawings. Understanding that these drawings depict only typical embodiments of the invention and are not therefore to be considered as limiting its scope, the invention will be described and explained with additional specificity and detail through the use of the accompanying drawings in which:

Figure 1 illustrates one suitable environment for practicing the methods of the invention for authenticating a hardware device incorporating digital certificates;

Figure 2 illustrates one exemplary flowchart comprising acts performed by a hardware device, a trusted certificate authority, and an authenticating device according to one embodiment of the methods of the invention for authenticating the hardware device;

Figure 3 illustrates one embodiment of the hardware storage component of the hardware device of the invention that is capable of storing hardware data;

Figure 4 illustrates one embodiment of a system for utilizing the methods of the invention that includes a computer device, a biometric hardware device, and a remote server operating as a hardware authentication device;

Figure 5 illustrates one embodiment of a system for utilizing the methods of the invention that includes a biometric hardware device, a smart card operating as a hardware authenticating device, a computer, and a remote server operating as a third party system;

Figure 5B illustrates one embodiment of a system for utilizing the methods of the invention in which a biometric hardware device is authenticated by a security system that includes a security door with a solenoid that is activated upon receiving an authenticated signal from the iris scanner;

Figure 6 illustrates one embodiment of a system for utilizing the methods of the invention that includes a key operating as a hardware device and a lock operating as a hardware authenticating device;

Figure 7 illustrates one embodiment of a system for utilizing the methods of the invention that includes a wireless telephone operating as a hardware device and a communications tower operating as a hardware authentication device; and

Figure 8 illustrates one embodiment of a system for utilizing the methods of the invention that includes a computer memory chip operating as a hardware device and as an accessory component to a circuit board that operates as a hardware authenticating device.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention relates to methods and systems for authenticating hardware devices, and more particularly to methods and systems for certifying the authenticity of hardware devices incorporating digital certificates.

According to one embodiment of the invention, hardware devices incorporating digital certificates of a trusted certificate authority are authenticated for enabling the hardware device or any other devices or systems to perform a desired operation.

Embodiments of the invention, as described herein, may comprise special purpose or general-purpose computers comprising various computer components and hardware devices. Embodiments may also include computer-readable media having computer-executable instructions or data structures stored thereon. Such computer-readable media can be any available media that can be accessed by a general-purpose or special-purpose computer. By way of example, and not limitation, such computer-readable media can comprise RAM, ROM, EEPROM, CD-ROM, other optical storage medium, magnetic storage medium, digital storage medium, or any other medium which can be used to store the desired data, digital certificates, executable instructions, or other data structures utilized by the invention and which can be accessed by a general-purpose or special-purpose computing device.

When information is transferred or provided over a network or another communications connection to a computing device, the computing device properly views the connection as a computer-readable medium. Thus, such a connection is also properly termed a computer-readable medium. Combinations of the above should also be included within the scope of computer-readable media. Computer-executable instructions comprise, for example, instructions and data which cause a general-purpose computer, special-purpose computer, or special-purpose processing device to perform a certain function or group of functions. The computer-executable instructions and associated data structures represent an example of program code means for executing the acts of the invention disclosed herein.

Elements of the invention will be described in the general context of computer-executable instructions, such as program modules, being executed by a computer. Generally, program modules include routines, programs, objects, components, data structures, or the like that perform particular tasks or implement particular abstract data types. Moreover, those skilled in the art will appreciate that the invention may be practiced with any type of computing system or device, including embedded LSI, VLSI, and ASIC devices, smartcards, hand-held devices, multi-processor systems, microprocessor-based or programmable consumer electronics, network PCs, minicomputers, mainframe computers, and the like. The invention may also be practiced in distributed computing environments where tasks are performed by remote processing devices that are linked through a communications network. In a distributed computing environment, program modules may be located in both local and remote memory storage devices.

Turning now to Figure 1, one suitable environment 100 for practicing the methods of the invention for authenticating hardware devices incorporating digital certificates is illustrated. As shown, a hardware authenticating device 110 is provided. Hardware authenticating device 110 includes any computing system or device that is capable of communicating with other computing systems and device, such as hardware device 130 and third party system 140. Accordingly, the hardware authenticating device 110 preferably includes a communications module 144 for communicating with other computing systems and devices, such as hardware device 130, and third party system 140, which also each preferably includes a communications module 144 for enabling communication.

Hardware authenticating device 110 also preferably includes a hardware authenticating module 146 that is capable of authenticating any hardware device 130 according to the methods of the invention. In particular, hardware authenticating module 146 is capable of executing computer-executable instructions for performing any necessary acts of the methods of the invention, which are described in more detail below in general reference to acts 258-272 of Figure 2.

Hardware device 130 includes any component or device that may benefit from being authenticated according to the methods of the invention. For example, and not limitation, hardware device 130 may include biometric identification devices, other identification devices, electrical keys, magnetic keys, electro-mechanical keys, other keys and security devices, wireless telephones, other communications devices, computer hardware components, computer cards, and any accessory products.

Third party system 140 includes any computing device or system that is capable of communicating with the hardware authenticating device 110 for receiving or providing data or for performing a desired transaction upon receiving an authorized request from the hardware authenticating device 110 or any hardware device 130 authenticated according to the invention.

Although the hardware authenticating device 110 is shown to be linked to two hardware devices 130 and one third party system 140, it will be appreciated that hardware authenticating device 110 may be linked to any number or combination of hardware devices 130 and/or third party systems 140.

As shown in Figure 1, hardware authenticating device 110 may be linked to hardware device 130 and third party system 140 with a direct communication link 150, which may include a USB port connection, a COM port connection, or any other type of cabling, coupling, adapter, or physical connection, as well as any wireless connection incorporating analog or digital technology, such as, but not limited to Bluetooth and 802.11 wireless technologies.

Even though Figure 1 shows the hardware device 130 are connected directly to the hardware authenticating device 110, it will be appreciated that the hardware device 130 may be indirectly connected to authenticating device 110 through other devices or network connections. For example, the connection between the hardware authenticating device 110, hardware device 130 and any third party system 140 may also include a network connection 160, such as an Internet connection, another type of wide area network (WAN) connection, or any local access network (LAN) connection.

Methods for authenticating hardware devices incorporating digital certificates, according to one embodiment of the invention, include the acts that are illustrated in the flowchart 200 of Figure 2, and which are generally performed by a hardware device 130, a hardware authenticating device 110, and a trusted certificate authority 230.

The terms "hardware device" and "hardware authenticating device," which are generally defined above, may include a variety of devices and systems. The term "trusted certificate authority" should generally be construed to include any entity, organization, corporation, person, business, system, or device that is authorized or trusted to create digital certificates for certifying the authenticity of a hardware device according to the invention. The term "trusted certificate authority" may also refer to any sublicensee or agent of the trusted certificate authority 230 that is authorized by the trusted certificate authority 230 to generate and assign digital certificates to hardware devices. By way of example, and not limitation, the trusted certificate authority 230 may include a manufacturer of the hardware device 130.

Figure 2 illustrates various acts 240-272 that may be performed according to the methods of the invention for authenticating hardware devices. It will be appreciated that although the acts 240-272 are shown in a particular sequence, they may be performed, according to the invention, in any logical or desired sequence.

According to the presently preferred embodiment, the methods of the invention commence with the generation and assignment of an asymmetric key pair, act 240. The term "hardware data" is generally defined herein to include any identification information, such as, but not limited to the name of the hardware device, the name of the manufacturer of the hardware device, the serial number of the hardware device, the model number of the hardware device, and any other information corresponding to the hardware device. Generally, hardware data includes at least enough information to identify the hardware device.

According to one embodiment, hardware data also includes a public key from an asymmetric key pair that is assigned to the hardware device. Asymmetric key pairs, which are well known in the art, generally include a unique public key and a unique private key, each of which is capable of encrypting data and decrypting the data encrypted with the other key. The private key is theoretically kept secret and private, whereas the public key is published and constructively made available to the public, hence their names. According to this embodiment of the invention, once a key pair is generated, it is assigned to the hardware device 210. Therefore, the public key is hereinafter referred to as the public hardware key and the corresponding private key is hereinafter referred to as a private hardware key.

It is anticipated that the hardware key pairs are used to encrypt data transferred between mutually authenticated hardware devices. For example, but not limitation, once two or more hardware devices have authenticated each other, one device may create a random symmetric block cipher key which it may then encrypt with its hardware private key and transmit to the other devices.

Next, according to act 242 of Figure 2, a digest is generated of the hardware data. A digest of the hardware data is generated, according to the invention, by applying a hash algorithm to the hardware data. Hash algorithms and digests, which are also known as hash numbers, are well known in the art.

Next, according to act 244, the trusted certificate authority 230 encrypts the digest to create an encrypted digest. This may be accomplished, for example, by encrypting the digest with a private key of the trusted certificate authority 230. Because this private key and a corresponding public key, which constitute an asymmetric key pair, are associated with the trusted certificate authority, they are hereinafter referred to respectively as the private certification key and public certification key.

As illustrated in Figure 2, act 246 includes publishing the public certification key so that it is at least made available to the hardware authenticating device 220, such as, for example, through a direct connection or a network connection, which are described above in reference to Figure 1. According to embodiments in which hardware data includes a public hardware key, act 246 may also include publishing the public hardware key.

The final act performed by the trusted certificate authority 230, according to this embodiment, is act 248, which includes storing the hardware data and encrypted digest on the hardware device 130. The hardware data and encrypted digest may be stored, for example, in a storage component of the hardware device 130.

As shown in Figure 3, the hardware storage component 300, which is also illustrated in Figure 1, stores hardware data 310. As described above, hardware data 310 may include a public hardware key 320 and identification information 330. The hardware storage component 300 also stores the encrypted digest 340, and may optionally store a private hardware key 350. In such an embodiment, in which the hardware storage component 300 stores the private hardware key 350, it is preferred that the private hardware key 350 be stored separately from the hardware data 310 and encrypted digest 340. This is desirable so that the hardware device can provide access to the hardware data 310 and encrypted digest 340 without compromising the secrecy of the private hardware key 350.

The storage component 300 may include any type of storage medium, such as, but not limited to optical storage medium, magnetic storage medium, digital storage medium, or any other medium capable of storing the encrypted digest 340, hardware data 310, and optional private hardware key 350.

According to one preferred embodiment of the invention, the storage component 300 is encapsulated within a tamperproof material, such as a ceramic or potting material, so that any attempt to remove the storage component 300 from the hardware device will result in fracturing or rendering inoperable the storage component 300 or any essential component of the hardware device. This may be useful, for example, to generally prevent theft and fraudulent misuse of the encrypted digest 340, hardware data 310, and private hardware key 350.

This process may also be extended to include the electronic distribution of hardware certificates to enable the hardware device manufacturer to store the hardware certificates, created by the trusted certificate authority, within their own storage devices. This may be done, for example, by the trusted certificate authority placing a device or computing system on the premises of the hardware device manufacturer for the purpose of securing transmitting, receiving and accounting of hardware digital certificates created by the trusted certificate authority and transmitted to the hardware device manufacturer for the purpose of storing within the hardware device. It is anticipated that such a device or computer system would incorporate the hardware authentication methods described herein to ensure authorized use.

Returning now to Figure 2, once the encrypted digest and hardware data are stored in the storage component of the hardware device 130, the hardware device 130 can be authenticated by another device or system, such as hardware authenticating device 110. Authentication of the hardware device 130 may occur when the hardware device 130 communicably engages, or is otherwise placed in communication with, the hardware authenticating device 110, act 252, such as through a direct communication link 150 or a network connection 160, as shown and described above in reference to Figure 1.

Upon engaging the hardware authenticating device 110, the hardware device 130 may initiate a request of the hardware authenticating device 110, act 254. The request may include a request to perform a desired operation or a request to enable the functionality of any one of the hardware devices 130, the hardware authenticating device 110, and any third party device or system. It will be appreciated, however, that initiating a request is not a necessary act to be performed by the hardware device 130 according to the invention. For example, the hardware authenticating device 110 can be configured to execute or initiate a desired operation or enable another device to perform a desired operation *sua sponte*, solely upon authenticating the hardware device 130 and without ever receiving a request from the hardware device 130.

In order to authenticate the hardware device 130, the hardware device 130 provides access to the hardware data and encrypted digest that are stored by the hardware device 130, act 256. The hardware authenticating device 110 accesses the hardware data and encrypted digest, act 258, via a direct communication link or network connection, as described above. The hardware authenticating device 110 may also utilize a direct communication link or network connection to receive or access the public certification key of the trusted certificate authority 130, act 260. It will be appreciated, however, that the hardware authenticating device 110 can also receive or access the public certification key through other means, such as during manufacture of the hardware authenticating device 110, or through uploading data from a computer-readable medium at any time.

It is important that the hardware authenticating device 110 have access to the public certification key because that public certification key is used to decipher the encrypted digest. By deciphering the encrypted digest, a decrypted digest is generated, act 262. A comparison digest, which is generated by applying a hash algorithm to the hardware data, act 264, is then compared to the decrypted digest, act 266. If the decrypted digest and the comparison digest are the same then the hardware device 130 is finally authenticated, act 268.

Upon authenticating the hardware device 130, as mentioned above, the hardware authenticating device 110 can perform an operation or enable an operation to be performed, either *sua sponte*, or alternatively, by honoring a request initiated by the hardware device 130, act 270. If the hardware device is not authenticated, any request initiated by the hardware device is denied, act 272.

It should be appreciated that the methods of the invention for authenticating hardware devices incorporating digital certificates may include any combination of the above-identified acts, which may be performed in any desired sequence. For example, as a matter of illustration and not limitation, act 264 involving the generation of a comparison digest may be performed prior to the hardware authenticating device 110 receiving the public certification key and generating the decrypted digest, as specified according to acts 260 and 262.

It should also be appreciated that the acts of authenticating the hardware device 130, as described above, can generally be construed as acts for determining whether the hardware device 130 comprises a valid digital certificate. For example, when the hardware device 130 comprises a valid digital certificate, the hardware authenticating device 110 authorizes the hardware device 130 to operate, but when the hardware device 130 does not comprise a valid digital certificate, the hardware authenticating device 110 does not authorize the hardware device 130 to operate. The term "operate" is broadly defined herein to include the enabling of the hardware device to perform any desired function, and which may include enabling another device, even the authenticating device 110, to perform a desired function in response to communications or operations performed by the hardware device 130, as described below. As a matter of example, and not limitation, authorizing the hardware device 130 to operate can include transmitting and receiving data from the hardware device, whereas not authorizing the hardware device 130 to operate can involve the termination of any communication between the hardware authenticating device 110 and the hardware device 130, when that communication is necessary for the hardware device 130 to perform a desired function.

Specific embodiments of systems that include hardware devices and hardware authenticating devices will now be provided, as a matter of example and not limitation, to further illustrate the utility and benefits of the invention as applied in various industries and applications and to further illustrate a variety of novel processes that are enabled by and encompassed within the invention.

Figure 4 illustrates one embodiment that includes a biometric device 420 that is generally used to verify the identity of an authorized user seeking to use computer 410 to access a remote third party system or server, such as remote server 430. In this embodiment, the biometric device 420 and computer 410 may be collectively considered a hardware device used to initiate requests and verify the identity of a user. The biometric device 420 may also individually be considered a hardware device to be authenticated according to the invention.

Figure 4 also illustrates a remote server 430 that may include any type of server or system that is capable of communicating with computer 420. Remote server 430 may be, for example, a banking network server in direct communication with computer 410 through an Internet connection and in indirect communication with biometric device 420 through computer 410. According to this example, remote server 430 is capable of performing a desired operation, such as executing a financial transaction, only upon verifying the identity of the user requesting the operation be performed.

To verify a user is an authorized user, the remote server may require that the identity of an authorized user be verified by biometric device 420 before access to the remote server is granted to the user. Some identification devices, however, such as biometric device 420, generate "match" / "no match" signals that can be intercepted and spoofed by a hacker. Accordingly, although the remote server may receive a signal that supposedly verifies the identity of an authorized user, it is possible that the signal is not an authentic signal submitted by biometric device 420, but is rather a spoofed "match" signal that is submitted fraudulently by a hacker or unauthorized user using computer 410 or another device.

It will be appreciated that the present invention overcomes this problem by generally providing the remote server 430 with a means for authenticating the source of the biometric signal. According to the invention, the biometric device 420 includes a storage medium 440 that is used to store hardware data and an encrypted digest of the hardware data that are associated with the biometric device 420, and which are generally described above. In review, the hardware data generally includes identification information associated with the biometric device 440 that can be used to authenticate the biometric device 420.

The remote server, operating as a hardware authenticating device according to the invention, accesses the hardware data and the encrypted digest, which are stored in the storage medium of the biometric device 420 and generates a decrypted digest and comparison digest, as generally described above with reference to acts 258-264 of Figure 2. Next, the remote server compares the decrypted digest and comparison digest to determine whether the biometric device is authentic, acts 264-266. If the decrypted digest and the comparison digest are the same, the biometric device is authentic and the verification signal generated by the biometric device can be trusted to be an authentic signal, rather than a spoofed signal. Upon authenticating the biometric device 420, the remote server 430 can then proceed to honor any request generated by the computer 410, act 270. Thus, it can be seen how, according to the invention, a hardware authenticating device can generally condition the performance of an operation on the authentication of a hardware device.

According to another embodiment, illustrated in Figure 5, it is shown how the performance of a desired operation by a third party system, which is not a hardware authenticating device, can also be generally conditioned on the authentication of a hardware device. For example, in this embodiment, a remote server 510 operates as a third party system that is capable of performing a transaction upon receiving a digitally signed document from computer 520. A smart card 530, operating as a hardware authenticating device, includes a personal private key that is capable of digitally signing the document stored on the computer 520. However, according to this embodiment, the personal private key stored on the smart card 530 can only be accessed and used upon verifying, with an authentic biometric device 540, that the user of the smart card 530 is an authorized user. Because the signal generated by biometric device 540 may be spoofed and misused, it is necessary to authenticate the biometric device 540, otherwise, an unauthorized person with access to the smart card 530 could use a spoofed biometric device 540 signal to access the personal private key on the smart card, such as, for example, to execute an unauthorized digital signature.

To authenticate the biometric device 540, the smart card 530 engages the biometric device 540 through computer 520 and accesses the hardware data and encrypted digest stored in the storage component 550 of the biometric device 540. As generally described above, in reference to acts 260-266 of Figure 2, the biometric device 540 is authenticated upon creating a decrypted digest and a comparison digest and determining that they are the same. Once the biometric device 540 is authenticated, the smart card 530 enables the personal private key stored on the smart card 530 to be accessed and to be used to digitally sign the document on the computer 520, thereby enabling the third party system comprising remote server 510 to perform the desired transaction that was at least partially conditioned on authentication of the biometric device 540, as described.

According to one embodiment, a biometric device is first authenticated according to the methods of the invention, as described above, then the authenticating device, which has obtained the public key of the biometric device during the authentication procedure, uses the public key of the biometric device to encrypt a symmetric block cipher key, such as a random number. This encrypted block cipher key is then sent to the biometric device, whereupon the biometric device decrypts the block cipher key with its own private key. The block cipher key is then used by the biometric device to encrypt all subsequent communication between the authentication device, such as, for example, when transmitting a scanned biometric image to the authentication device. A hacker listening in is thereby thwarted since he cannot ascertain the block cipher key and cannot determine the original data. More particularly, the hacker cannot simply capture the data transmission and replay it later since it is 'married' to the block cipher key which is a random number that will never be used again

It will be appreciated that this method is both an efficient and a secure method for communicating between devices. In particular, the use of block cipher keys to encrypt large amounts of data is much more efficient than encrypting large amounts of data with asymmetric key algorithms. Nevertheless, security is not compromised inasmuch as the block cipher is initially transmitted between the devices with asymmetric encryption according to the methods of the invention. Accordingly, asymmetric encryption is used to protect and safely share the symmetric block cipher key between the devices and thereafter block cipher encryption is used to enable efficient communication between the devices.

Figure 5B illustrates one useful embodiment for implementing of secure communication between devices, as described above. In this embodiment, a biometric security system 560 is configured with a security door 570 that limits access to a physical location to only authorized personnel. As shown, the security system 560 includes a smart card reader 575, and a biometric device comprising an iris scanner 580. Upon authenticating the identity of the authorized personnel with the iris scanner 580 and smart card device 575, according to the methods of the invention, as generally described above, the security system 560 energizes a solenoid 590 within the door 590 which unlocks the door and permits access.

One problem with existing security systems of this type is that an unauthorized intruder can bypass the biometric system altogether by energizing the solenoid with an external power source. To overcome this weakness, existing systems protect the electrical wiring leading to the solenoid with steel conduit and large physical barriers, which can be both expensive and inconvenient.

The present invention overcomes the limitations of the prior art security systems by providing a means for preventing the solenoid 590 from being activated without first receiving an authentication signal from the iris scanner 580. For example, the solenoid 590 can be configured to be activated only upon receiving a digital certificate (e.g. hardware data and an encrypted digest) from the iris scanner 580. Accordingly, the solenoid 590 can then authenticate the iris scanner 580, upon receiving the digital certificate, by creating a decrypted digest and a comparison digest and by determining that they are the same, as generally described above. Once the solenoid 590 authenticates the iris scanner 580 then the solenoid 590 awaits a 'match' signal from the iris scanner 580. As described above, the 'match' signal and any other communication can be communicated both efficiently and securely with the use of random block cipher keys. Upon receiving the 'match' signal from the iris scanner 580, indicating an authorized person has been identified; the solenoid 590 activates and allows the door 570 to be opened. The security system 560 may also be configured to only generate a 'match' signal only when the smart card reader 575 has also generated an appropriate authorization signal.

It will be appreciated that according to this embodiment, the use of steel conduit and other barriers, as used in the prior art, are not necessary to prevent an intruder from bypassing the security system 560 inasmuch as the solenoid 590 will not activate until it first authenticates the source of the activation signal, namely, the iris scanner 580. As generally described above, this is done by determining that the iris scanner 580 comprises a digital certificate that includes encrypted hardware data that identifies the biometric device as an authentic biometric device of the security system 560.

It will be appreciated the advantages and benefits of the invention can also be realized in various other industries. By way of example, and not limitation, the automobile and home security industries can benefit from being able to authenticate any keys used to engage ignitions, locks, and other security type systems.

According to the embodiment shown in Figure 6, a key 610 may include a hardware device of the invention. The key 610 may, for example, include a storage component 620 and a communication module 630 that are embedded within the key 610. The key 610 may also be configured with well-known electronic or magnetic means for communication (not shown) to communicate with a corresponding security system, such as lock 640. To ensure that the key 610 is authentic, the lock 640, ignition, or any such other type of security system accesses the hardware data and encrypted digest that are stored within the storage component 620 of the key 610 and, as generally described above, generate a decrypted digest and comparison digest to determine whether the key 610 is authentic. According to this embodiment of the invention, only an authentic key 610 can be used to successfully operate the security system 640.

To provide a remedy for situations in which the key 610 may become lost, damaged, or stolen, the manufacturer of the key 610 can maintain a database of the hardware data so that a replacement key can be made that contains the same hardware data so that it can be authenticated. Alternatively, if security concerns warrant the re-keying of the security system, the security system can be reprogrammed to authenticate a new key with a new digital certificate and to not authenticate the lost/stolen key, thereby effectively revoking the digital certificate of the lost/stolen key. It will be appreciated that in order to distinguish between the original key and the replacement key, at least some of the hardware data used to identify the corresponding keys be different, or alternatively, the digital certificates of the corresponding keys must be altered, such as, for example, by using different certification keys in the manufacture of the digital certificates.

Another industry that benefits from the present invention is the telecommunications industry. In particular, the present invention can be used to prevent the unauthorized use of wireless telephone source signals, in which, for example, a wireless telephone source signal is spoofed and used to make unauthorized telephone calls from an unauthentic or unauthorized device.

As shown in Figure 7, a wireless telephone 710 may include a hardware device that communicates with other communications devices through a communications tower 720. The communications tower 720 is configured as a hardware authenticating device, according to the invention, so that prior to enabling communications with another communications device, the telephone 710 must be authenticated as an authorized device. For example, telephone 710 is equipped with hardware data and an encrypted digest that, according to the invention, as generally described above, may be used to authenticate the telephone 710 as an authentic device. The tower 720, prior to enabling a desired communication with telephone 710, accesses the hardware data and encrypted digest that are stored in a storage component 730 of the telephone 710 and generates a comparison digest and decrypted digest to determine whether the telephone 710 is an authentic and authorized telephone device. Accordingly, the methods of the invention can generally be used to effectively prevent the use of an unauthorized telephone device or telephone source signal. Furthermore, if an authorized telephone device or telephone source signal is stolen, the digital certificate of the telephone device can be revoked and data can be supplied to the tower 720 that prevents the tower 720 from enabling communication from any telephone signal source incorporating the revoked certificate.

The present invention also has utility in preventing the use of unauthorized or illegally manufactured accessories to a base product. For example, according to the present embodiment, as shown in Figure 8, a computer circuit board 810 includes a base product that is capable of interoperating with various circuit board accessory components that may be replaced when damaged or whenever it is desired to upgrade or otherwise modify the circuit board 810. One such accessory component may include, for example, a memory chip 820.

To prevent unauthorized or illegal knockoff memory chips from being operably interchanged with the circuit board 810, according to the invention, chip 820 is configured with a storage component 830 that stores hardware data that identifies the chip 820 and an encrypted digest certifying the authenticity of the hardware data and corresponding chip 820.

According to this embodiment, the circuit board 810 operates as a hardware authenticating device and the chip operates as the hardware device to be authenticated. When the chip 820 is appropriately placed upon the circuit board 810, the circuit board 810 accesses the encrypted digest and hardware data from the storage component 830 of the chip 820. Then, before chip 820 can interoperate with the circuit board 810, the circuit board generates a decrypted digest and a comparison digest of the hardware data, as generally described above with reference to acts 260-266 of Figure 2. Finally, and only upon determining that the decrypted digest and the comparison digest are the same, the circuit board 810 enables the chip 820 to be utilized with the circuit board 810. If the decrypted digest and the comparison digest are not the same then the chip 820 includes an unauthorized knockoff and cannot be used with the circuit board 810.

It will be appreciated that although the foregoing example involves the authentication of an electronic computer chip, virtually any accessory, electrical, electro-mechanical, and mechanical, can be configured with a storage component and a communications module, according to the invention, to enable a corresponding base product to authenticate and interoperate with the accessory.

It will also be appreciated that if an accessory hardware device is originally authorized for use, but has subsequently been remanufactured or otherwise tampered with, the hardware device may still be rejected according to the invention. For example, the digital certificate can be stored in a storage device encapsulated within a tamperproof material that is damaged whenever the hardware device is remanufactured or otherwise tampered with, thereby rendering the storage device and the digital certificate inaccessible and unusable for authenticating the hardware device.

In summary, the present invention generally enables a hardware device incorporating a digital certificate, which generally includes a digest of hardware data that is encrypted with the private certification key of a trusted certificate authority, to be authenticated by another device with access to the corresponding public certification key. According to the invention, operation of the hardware device, the authenticating device, or any third party device or system can be made conditional on the authentication of the hardware device.

The present invention may be embodied in other specific forms without departing from its spirit or essential characteristics. The described embodiments are to be considered in all respects only as illustrative and not restrictive. The scope of the invention is, therefore, indicated by the appended claims rather than by the foregoing description. All changes which come within the meaning and range of equivalency of the claims are to be embraced within their scope.

What is claimed is:

1. A method for enabling a hardware device to be authenticated, the method comprising the acts of:

obtaining hardware data that is associated with the hardware device and that includes information identifying the hardware device;

creating a digital certificate that encrypts the hardware data and certifies the authenticity of the hardware data; and

providing the digital certificate to the hardware device such that the hardware device can make the digital certificate available to an authenticating device that can thereafter use the digital certificate to authenticate that hardware device.

2. A method as recited in claim 1, wherein the act of creating a digital certificate comprises the acts of:

using a hash algorithm to generate a digest of the hardware data; and

using a private certification key to encrypt the digest, wherein the private certification key and a corresponding public certification key comprise an asymmetric key pair associated with a trusted certification authority.

3. A method as recited in claim 1, wherein the hardware data comprises at least one of a name of the hardware device, a name of a manufacturer of the hardware device, a serial number of the hardware device, and a model number of the hardware device.

4. A method as recited in claim 1, wherein the hardware data further comprises a public hardware key, and wherein the public hardware key and a corresponding private hardware key comprise an asymmetric key pair assigned to the hardware data.

5. A method as recited in claim 1, wherein the hardware device is unable to perform a desired hardware function until the hardware device is authenticated by the authenticating component.

6. A method as recited in claim 5, wherein the hardware device comprises a wireless telephone and the desired hardware function comprises performing a telephonic communication.

7. A method as recited in claim 5, wherein the hardware device comprises a computer component and the desired hardware function comprises performing computer processing with the computer component.

8. A method as recited in claim 5, wherein the hardware device comprises an identification device, and wherein the desired hardware function comprises authenticating the identity of a user.

9. A method as recited in claim 8, wherein the identification device comprises a biometric device and the desired hardware function comprises verifying the identity of a user using the biometric device.

10. A method as recited in claim 5, wherein the hardware device comprises a key, and wherein the desired hardware function comprises opening a lock.

11. A method as recited in claim 5, wherein the desired hardware function further comprises enabling another device to perform a desired function.

12. A method as recited in claim 11, wherein said another device comprises a smart card storing a private hardware key, and wherein enabling the smart card to perform the desired function comprises enabling the smart card to digitally sign data with the private hardware key.

13. A method for enabling a hardware device to be authenticated by an authenticating device, the method comprising the acts of:

by the hardware device, receiving a digital certificate from a certificate authority, the digital certificate including encrypted hardware data associated with the hardware device and certifying the authenticity of the hardware device, the hardware data including information identifying the hardware device;

in preparation for communicating with another device, transmitting the digital certificate to the authenticating device, whereupon the authenticating device uses the digital certificate to authenticate the hardware device.

14. A method as recited in claim 13, wherein the hardware data comprises at least one of a name of the hardware device, a name of a manufacturer of the hardware device, a serial number of the hardware device, and a model number of the hardware device.

15. A method as recited in claim 14, wherein the hardware data further comprises a public hardware key, and wherein the public hardware key and a corresponding private hardware key comprise an asymmetric key pair associated with the hardware device.

16. A method as recited in claim 13, wherein the act of receiving a digital certificate comprises the act of storing the digital certificate in a storage component that is sealed in a tamperproof packaging.

17. A method as recited in claim 13, wherein the hardware device is unable to perform a desired hardware function until the hardware device is authenticated by the authenticating device.

18. A method as recited in claim 17, wherein the hardware device comprises a wireless telephone and the desired hardware function comprises performing a telephonic communication.

19. A method as recited in claim 17, wherein the hardware device comprises a computer component and the desired hardware function comprises performing computer processing with the computer component.

20. A method as recited in claim 17, wherein the hardware device comprises an identification device, and wherein the desired hardware function comprises authenticating the identity of a user.

21. A method as recited in claim 17, wherein the hardware device comprises a key, and wherein the desired hardware function comprises at least one of accessing and operating a security system with the key.

22. A method as recited in claim 13, wherein upon transmitting the digital certificate to the authenticating device the authenticating device performs the acts of:

using a hash algorithm to generate a comparison digest of the hardware data;

using the public certification key to generate a decrypted digest, wherein the decrypted digest is generated by decrypting an encrypted digest of the hardware data, and wherein the encrypted digest is transmitted with the digital certificate to the authenticating device;

comparing the decrypted digest with the comparison digest; and authenticating the hardware device when the decrypted digest and the comparison digest are identical.

1 / 5

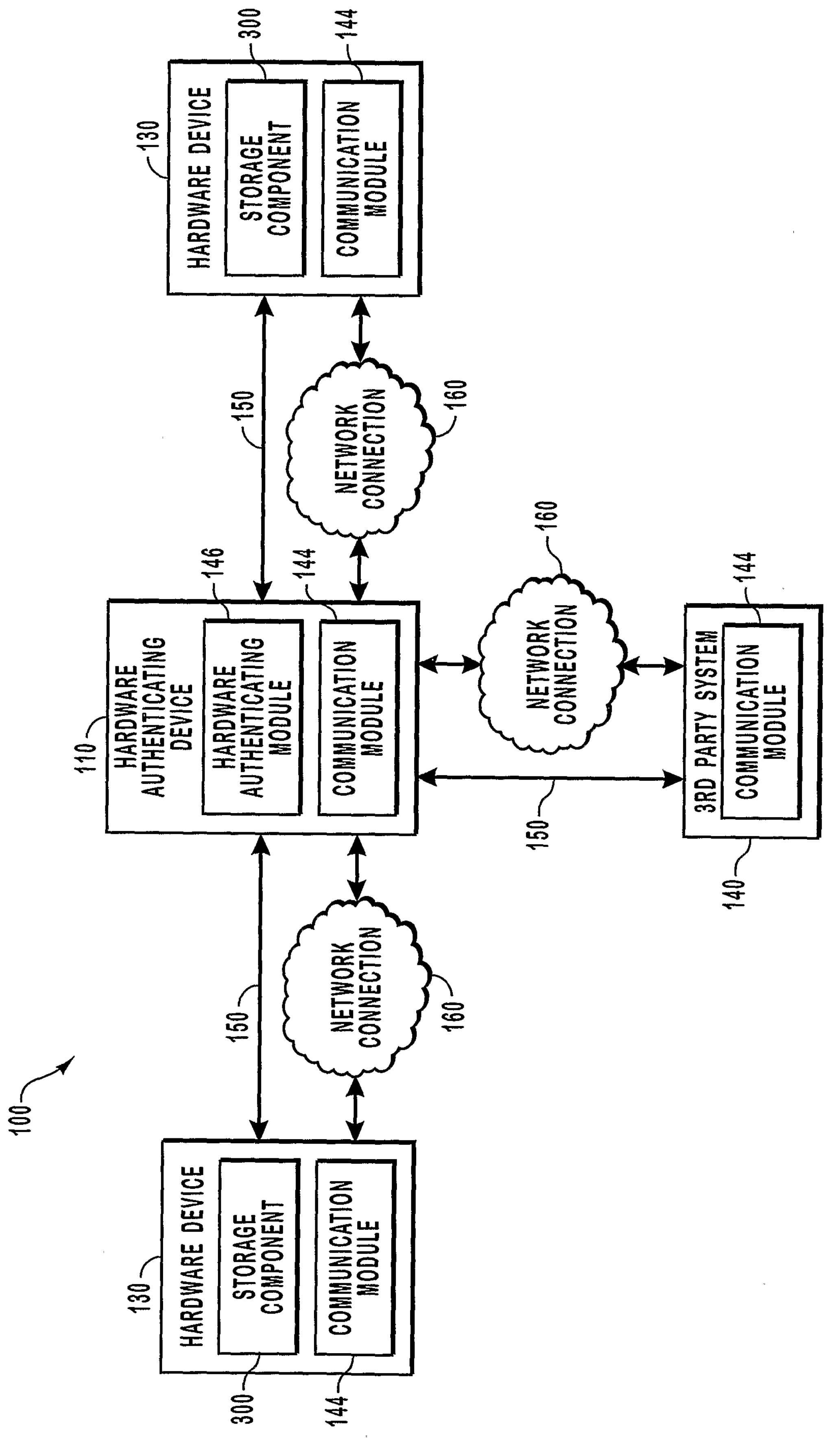

100
HARDWARE DEVICE
130
STORAGE COMPONENT
300
COMMUNICATION MODULE
144
150
NETWORK CONNECTION
160
HARDWARE AUTHENTICATING DEVICE
110
HARDWARE AUTHENTICATING MODULE
146
COMMUNICATION MODULE
144
150
NETWORK CONNECTION
160
HARDWARE DEVICE
130
STORAGE COMPONENT
300
COMMUNICATION MODULE
144
NETWORK CONNECTION
160
150
3RD PARTY SYSTEM
140
COMMUNICATION MODULE
144

FIG. 1

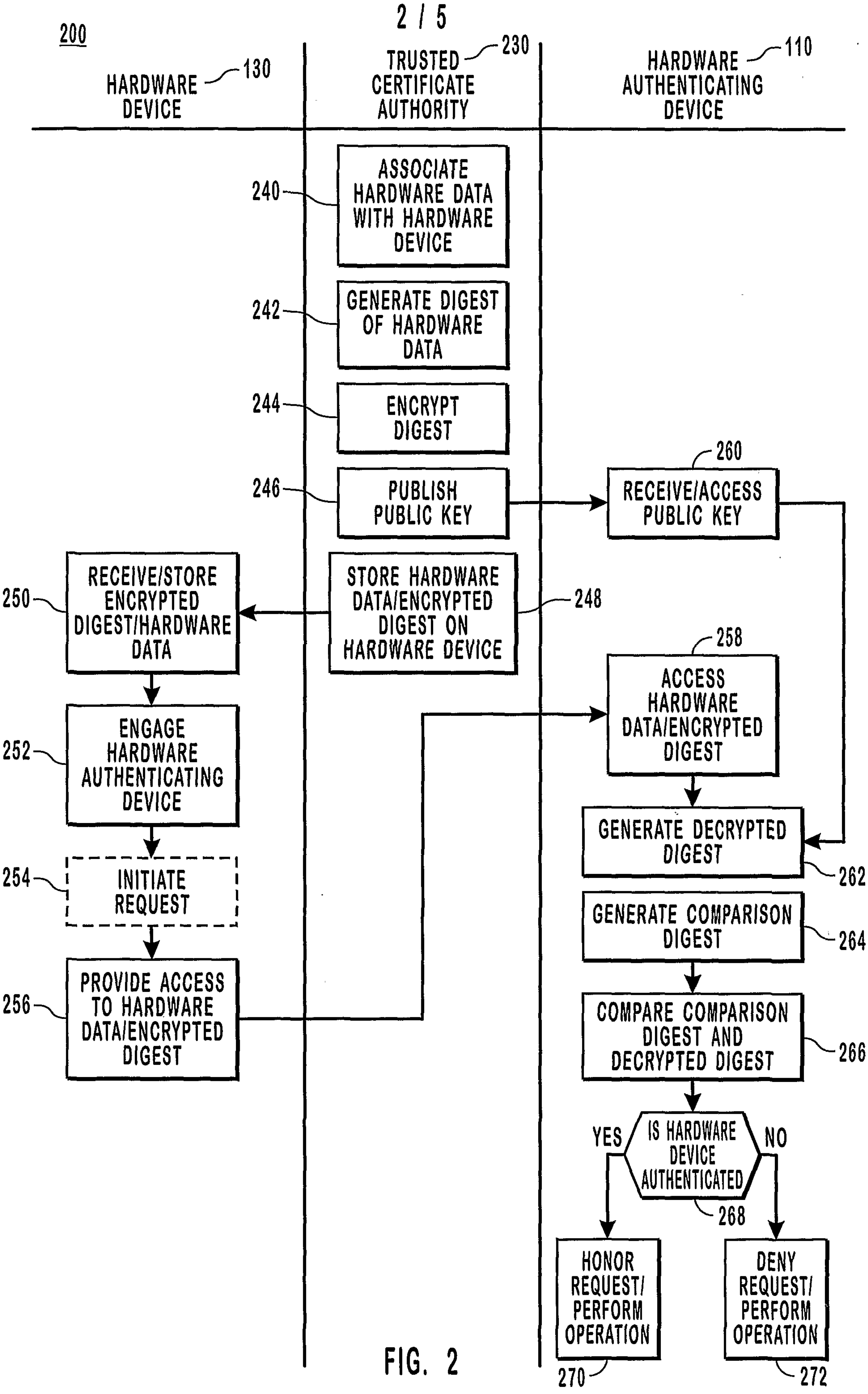

200
HARDWARE DEVICE
130
TRUSTED CERTIFICATE AUTHORITY
230
HARDWARE AUTHENTICATING DEVICE
110
240
ASSOCIATE HARDWARE DATA WITH HARDWARE DEVICE
242
GENERATE DIGEST OF HARDWARE DATA
244
ENCRYPT DIGEST
246
PUBLISH PUBLIC KEY
260
RECEIVE/ACCESS PUBLIC KEY
250
RECEIVE/STORE ENCRYPTED DIGEST/HARDWARE DATA
STORE HARDWARE DATA/ENCRYPTED DIGEST ON HARDWARE DEVICE
248
258
ACCESS HARDWARE DATA/ENCRYPTED DIGEST
252
ENGAGE HARDWARE AUTHENTICATING DEVICE
GENERATE DECRYPTED DIGEST
262
254
INITIATE REQUEST
GENERATE COMPARISON DIGEST
264
256
PROVIDE ACCESS TO HARDWARE DATA/ENCRYPTED DIGEST
COMPARE COMPARISON DIGEST AND DECRYPTED DIGEST
266
YES
IS HARDWARE DEVICE AUTHENTICATED
NO
268
HONOR REQUEST/ PERFORM OPERATION
DENY REQUEST/ PERFORM OPERATION
270
272

FIG. 2

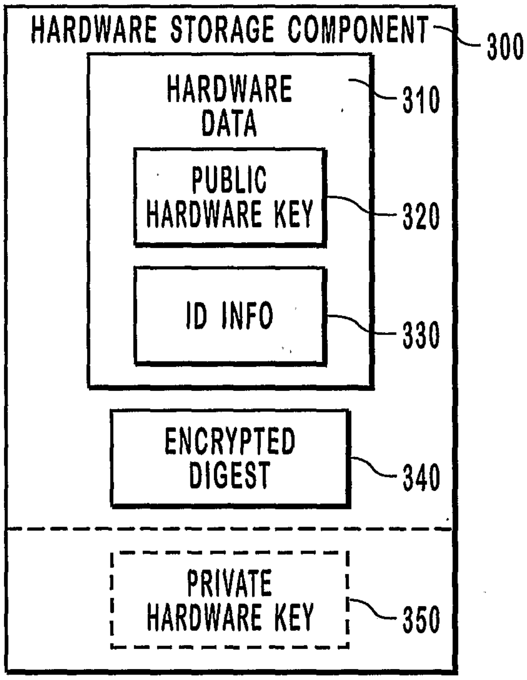


FIG. 3

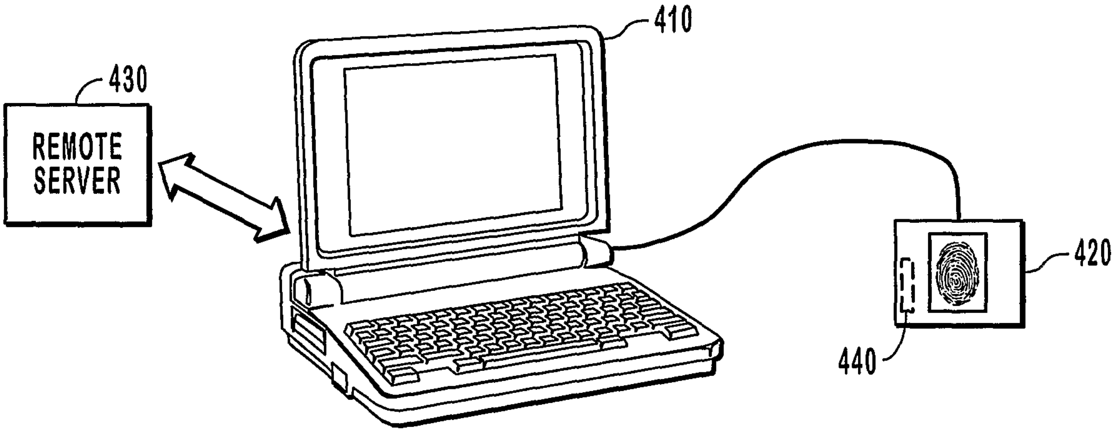


FIG. 4

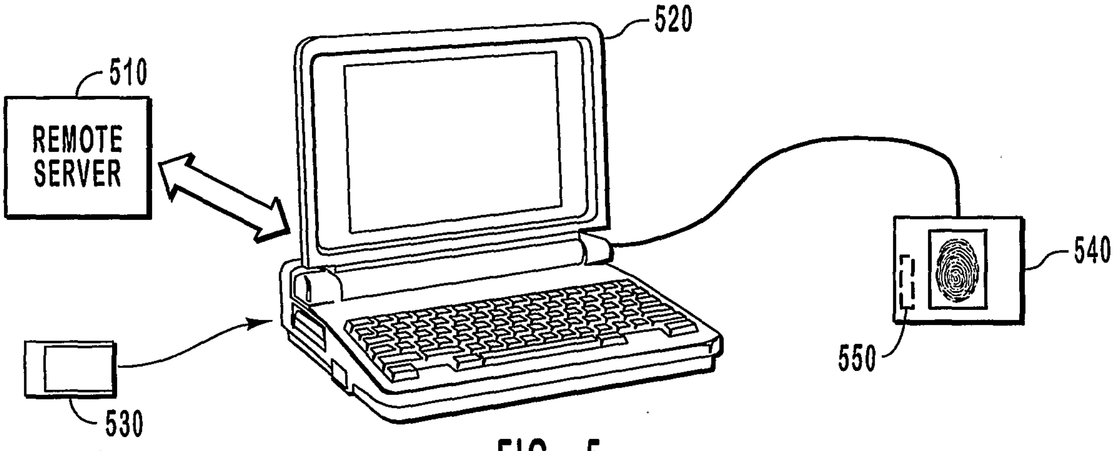


FIG. 5

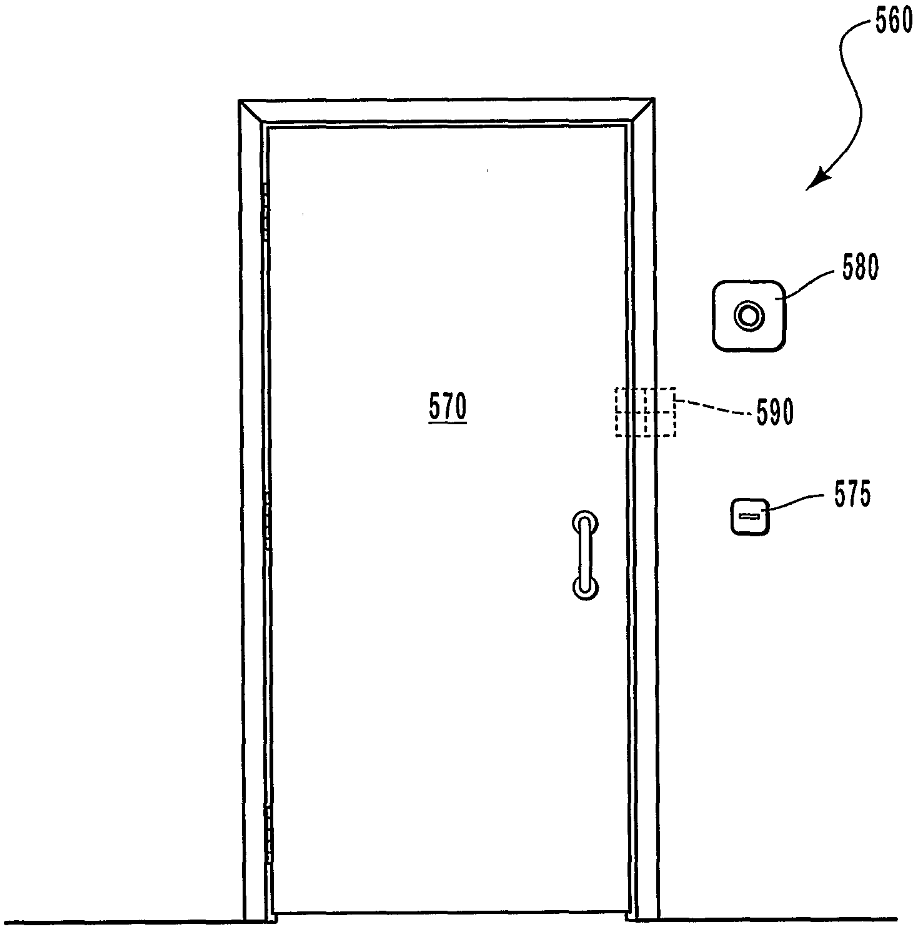


FIG. 5A

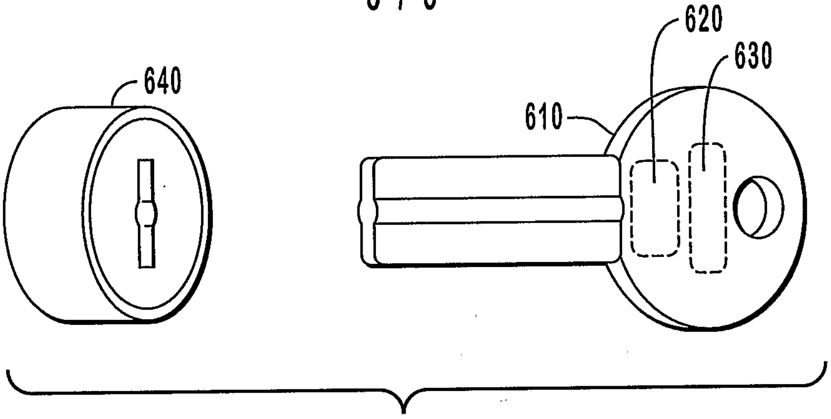


FIG. 6

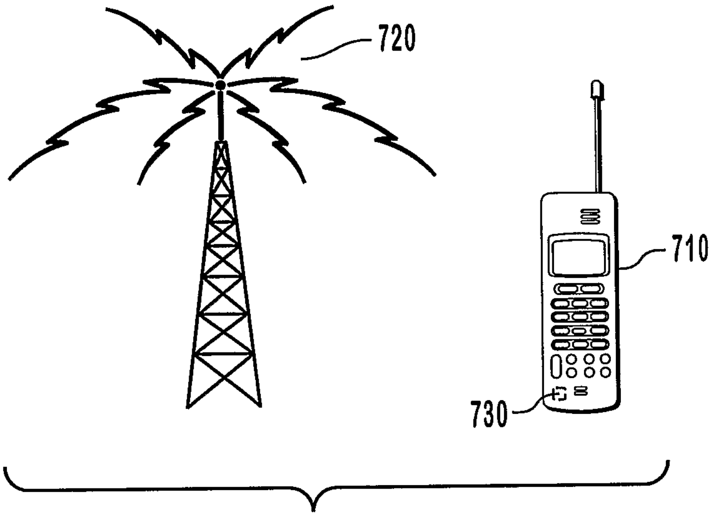


FIG. 7

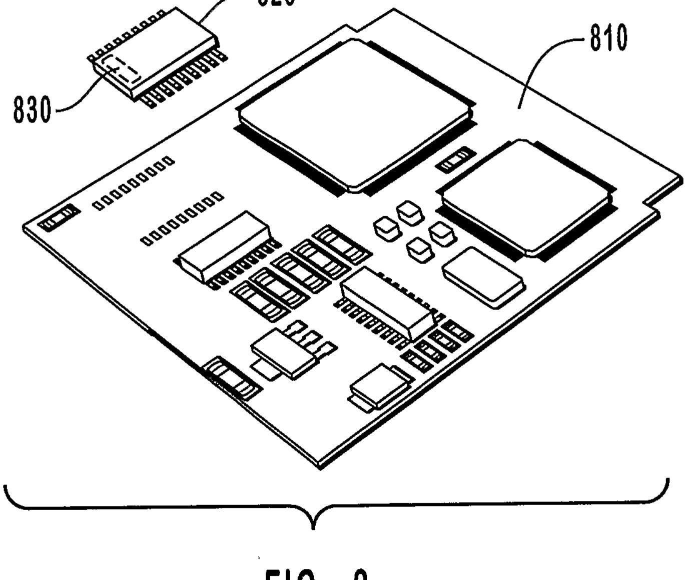


FIG. 8

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US03/04411

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : H04L 9/00; H04K 1/00
US CL : 713/155, 168, 189, 193, 194; 380/277, 282
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/155, 168, 189, 193, 194; 380/277, 282

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
USPTO, EPO ABSTRACTS, DERWENT - certificate, authentication, hardware device, public key

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,568,552 A (DAVIS) 22 October 1996 (22.10.1996), col. 2, line 61 to col. 3, line 18 and col. 7, line 11 to col. 9, line 17.	1-22
Y	US 6,233,685 B1 (SMITH et al) 15 May 2001 (15.05.2001), col. 2, line 45 to col. 4, line 21. and col. 6, line 13 to col. 11, line 45.	1-22

□ Further documents are listed in the continuation of Box C. □ See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search 24 April 2003 (24.04.2003)	Date of mailing of the international search report 13 MAY 2003
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703)305-3230	Authorized officer Matthew B Smithers Telephone No. (703) 305-3900