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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 September 2006 (08.09.2006)

PCT

(10) International Publication Number
WO 2006/094048 A2

(51) International Patent Classification: Not classified

(21) International Application Number:
PCT/US2006/007246

(22) International Filing Date: 1 March 2006 (01.03.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/657,375	1 March 2005 (01.03.2005)	US
11/089,605	25 March 2005 (25.03.2005)	US
11/194,514	1 August 2005 (01.08.2005)	US
60/740,302	29 November 2005 (29.11.2005)	US

(71) Applicants *(for all designated States except US)*: **ID-CONFIRM, INC.** [US/US]; 1800 Boulder Street, Denver, Colorado 80211 (US). **BAIRD, Ronald N.** [US/US]; 2245 S. Pinewood Road, Sedalia, Colorado 80135 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **MORRISON, Robert A.** [US/US]; 2045 S. Pinewood Road, Sedalia, Colorado 80135 (US).

(74) Agent: **MARSH FISCHMANN & BREYFOGLE LLP**; FETTIG, Gregory T., 3151 S. Vaughn Way, Suite 411, Aurora, Colorado 80014 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

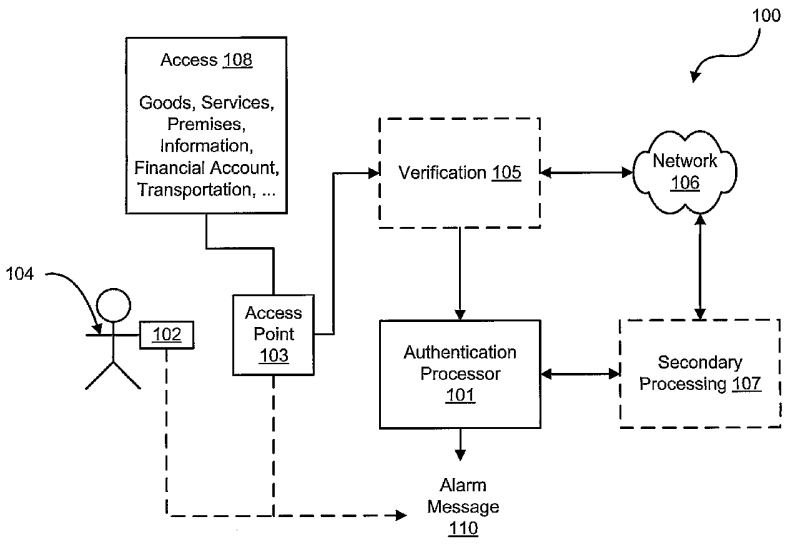
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

[Continued on next page]

(54) Title: SYSTEMS AND METHODS FOR BIOMETRIC AUTHENTICATION



(57) Abstract: Biometric authentication that allows a user to maintain control over his/her biometric information is presented herein. Generally, a biometric authentication system includes a sensor for sensing/scanning a biometric and for providing a first code in response to sensing the biometric. The system includes an authentication processor for evaluating the first code to authenticate the identity of a user of the sensor generally independent of the sensor. The authentication processor may generate a second code for evaluating the first code. For example, the authentication processor may include a comparator for comparing the first code and the second code to authenticate the user. In one embodiment, the sensor may include a code generator that is synchronizable with the code generator of the authentication processor. The system may also determine a situation of the user (e.g., authorized use of the biometric system) based on the sensed biometric.

WO 2006/094048 A2

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.

SYSTEMS AND METHODS FOR BIOMETRIC AUTHENTICATION

CROSS REFERENCE TO RELATED APPLICATIONS

This patent application, under 35 U.S.C. § 119, claims priority to U.S. Provisional Patent Application Nos. 60/657,375 (filed Mar. 1, 2005; hereinafter referred to as the '375 provisional) and 60/740,302 (filed Nov. 11, 2005; hereinafter referred to as the '302 provisional) and thus claims the benefit of their respective earlier filing dates. The entire contents of each of the '375 provisional and the '302 provisional are hereby incorporated within by reference. Additionally, this patent application is a continuation-in-part patent application of U.S. Patent Application Nos. 11/089,605 (filed Mar. 25, 2005; hereinafter referred to as the '605 application) and 11/194,514 (filed Aug. 1, 2005; hereinafter referred to as the '514 application) each of which also, under 35 U.S.C. § 119, claims priority to the '375 provisional. The entire contents of each of the '605 application and the '514 application are hereby incorporated within by reference.

TECHNOLOGICAL FIELD

The invention generally relates to biometric authentication. More specifically, the invention relates to authentication of a user's identity, wherein storage of the user's biometric information with a central processing system is generally not required.

BACKGROUND

Authentication of a person is often desirable and in many cases necessary. For example, to prevent unauthorized access, a central processing system controlling access (e.g., to a restricted area, a financial account, a medical account, etc.) may require authentication of a person attempting to gain such access. Once a person's identity has been authenticated, the central processing system may grant access to the information.

Various approaches to user authentication have included the storage of biometrics and the controlled access thereto by parties overseeing the control of access to, e.g., a given site for information. For example, a user may enter a particular biometric (e.g., retinal information, fingerprint information, ocular information, DNA, veinal information, arterial information, voice information, pulmonary information, etc.) into a biometric authentication system. The biometric authentication system commonly includes centralized processing that compares the user's entered biometric information to a user's stored biometric information with the centralized processing. The centralized processing may subsequently determine whether the person entering the biometric information is authorized, e.g., to access information and/or to enter a restricted area.

Growing concerns with privacy and unauthorized access to personal information, however, make such centralized storage of biometric information less than desirable. By way of example, third parties having access to a central processing system that stores biometric information may use another person's biometric information to gain access to information and/or entrance to restricted areas. Such use is commonly referred to as identity theft.

One example of identity theft commonly occurs with financial transactions. To illustrate, when a buyer attempts to make a credit card transaction without having the necessary credit card information (e.g., the credit card number), the buyer may be precluded from making a purchase. However, an unauthorized buyer may acquire the credit card information and perform a transaction because authentication also relies on the financial institution. Generally, the financial institution authenticates a buyer by authorizing a transaction as long as the card is deemed "active" (i.e., not canceled by the authorized buyer) thereby increasing the likelihood of identity theft when the card has been lost, stolen or when the card number has otherwise been undesirably exposed. In this regard, biometric authentication may also prove to be advantageous by decreasing the probability of identity theft in such financial transactions.

SUMMARY

Systems and methods presented herein provide for biometric authentication while allowing a user to maintain control over his or her biometric information. For example, biometric information of a user may be stored in a personal biometric device that is maintained by the user. In this regard, the biometric authentication system generally includes a sensor for sensing/scanning a biometric and for providing a first code in response to sensing the biometric. The system also includes an authentication processor for evaluating the first code to authenticate the identity of a user of the sensor generally independent of the sensor sensing the biometric.

Some non limiting examples of such biometrics may include retinal information, fingerprint information, ocular information, DNA, veinal information, arterial information, voice information, pulmonary information, or combinations thereof. The authentication processor may include a code generator to generate a second code for evaluating the first code. The authentication processor may also include a comparator for comparing the first code and the second code to authenticate the user. The sensor may include a code generator that is synchronizable with the code generator of the

authentication processor. For example, the code generator of the sensor and the code generator of the authentication processor may each generate codes according to a predetermined sequence. In one embodiment, this predetermined sequence may be implemented by seeding a particular mathematical function generator (e.g., a random number generator) with the same seed value such that codes may be synchronously produced.

The personal biometric device may be configured as a mobile biometric sensor. That is, the device may be carried with a user. In one embodiment, the personal biometric device is configured with a mobile handset (e.g., a cell phone). As such, components of the personal biometric device may be configured as embedded components with the handset. In addition to being mobile, the means for sensing may be configured to detect one or more of a variety of biometrics. In one embodiment, the personal biometric device senses one or more features of a user's biometric to assist in the authentication of the user. For example, a user may enter a biometric, such as a fingerprint, with the personal biometric device. The personal biometric device may detect one or more portions, or "sectors", of that fingerprint. Within each detected sector, the personal biometric devices may detect various ridges and valleys of the fingerprint. Biometrics other than fingerprints may be used as they may be equally suitable for such biometric sectorization. For example, sectors of a user's retinal scan may alternatively be used to generate a code.

In any case, the sectors may then be used to generate a code, which can be used by a system in a variety of ways (e.g., authentication, alarm generation, etc.). For example, detected features of a user biometric may be assigned values that are used in code generation (e.g., either by themselves or by seeding some code generation function, such as a random number generator). Additionally, selection of the sectors themselves may be a process which itself assists in code generation. For example, as each selected sector may have some value based on the sectorization, code values may be changed by varying the selection of the biometric sectors.

The system may also include means for determining a situation of the user based on the sensed biometric. For example, the personal biometric device may determine whether a person entering a biometric is authorized to use the personal biometric device. Alternatively, or in addition to, the biometric authentication system may determine a situation (e.g., a panic situation such as a force against his/her will) of an authorized user

based on a manner in which the authorized user enters a biometric. The system may also include means for generating an alarm message based on a determined situation of the user. For example, the system may include alarm generation features that assist the user in panic situations and/or prevent unauthorized use of the user's personal biometric device.

The means for determining a situation of the user may be incorporated into the personal biometric device or within a centralized processing system, such as an authentication processor as described hereinabove. When incorporated into the personal biometric device, the device may include a means for generating alarm message. For example, the personal biometric device may include an audible alarm and/or a data communication for conveying an alarm trigger. When using a data communication the personal biometric device may convey the alarm trigger to the authentication processor to alert the responsible authorities and/or deny access to an entrance. The alarm trigger may be incorporated into a code generated by the personal biometric device as described hereinbelow. In either case, the biometric information of the user is generally maintained with the personal biometric device.

The authentication processor may include a communication link (e.g., Internet, WLAN, LAN, etc.) configured for allowing a user to establish an account with the authentication system. The account is preferably devoid of a user's biometric. In one embodiment, the communication link may include an Internet server configured for maintaining software used to establish the account. In this regard, the communication link may be an Internet access link which may further include a database configured for storing a plurality of accounts. The authentication processor may also be independent of the sensor and may include an interface configured for receiving a generated code (e.g., the first code). In this regard, the authentication processor may include a comparator configured for receiving the generated code for comparison to one or more stored codes to determine a situation of the user. Additionally, the authentication processor may include the means for generating an alarm message based on a determined situation of the user.

Additionally, the system may include an input unit for receiving the first code and for granting access based on the first code. The input unit may be configured with the authentication processor. However, the input unit may be configured independent of the authentication processor. As such, the authentication may also include a communication

link between the authentication processor and the input unit for transferring an access indicator from the authentication processor to the input unit. The communication link may be configurable with one or more of a group consisting of a wide area network, a local area network, a wireless network, a public switching telephone network, and the Internet. The access may be to a financial account, a medical account, an entry, a computer, a means of transportation, or government information.

In another embodiment of the invention, a method of authentication includes using a biometric to generate a first code and authenticating a user based on the first code and independent of the step of using. The step of using a biometric may include a step of comparing the biometric with stored biometric information.

The method may also include a step of generating the first code with a device used to store the biometric information. The step of generating the first code may include a step of generating a random number based on a comparison of the biometric and the stored biometric information. Again, he stored biometric information may include retinal information, fingerprint information, ocular information, DNA, veinal information, arterial information, voice information, pulmonary information, or combinations thereof. The device may be a portable device.

The step of authenticating a user may include a step of generating a second code. The method may also include a step of granting a user access based on a comparison of the first code and the second code. Additionally, the method may include a step of entering the first code with an input device. The steps of entering the first code and generating a second code may be collocated steps.

The step of granting a user access may include a step of generating an access indicator for the input device. The step of granting a user access may further include a step of transferring the access indicator to an access point where the user is located. The step of transferring the access indicator may include a step of conveying the access indicator through a network, wherein the network is one or more of a group consisting of wide area network, a local area network, a wireless network, a public switching telephone network, and the Internet. The method may also include a step of transferring the first code from the input device to an authentication processor for comparison of the first code and the second code.

In yet another embodiment, a method of authenticating a user with a biometric includes sensing a user biometric and generating a code based on a sensed user biometric.

For example, when a user enters a biometric with a personal biometric device, the biometric device may generate a code for entrance into a biometric authentication system. Accordingly, the method may include transferring the code to an authentication processor for authentication, and processing the code to determine a situation of the user. For example, the authentication processor may compare the code to one or more stored codes to determine authorization and/or a panic situation of the user. In this regard, the method may further include comparing the user biometric to stored biometric information. As such, processing the code may include determining authorization for the user and/or a panic situation the user.

In response to determining when a user is unauthorized and/or in a panic situation, the method may include generating alarm message. The method may therefore further include transferring the alarm message to an access point, a responsible authority, or a combination thereof. In response to a favorable determination when processing the code, however, the method may include granting access to the user.

In another embodiment, a biometric authentication system includes a sensor that detects a biometric of a user to generate a code, and an authentication processor that processes the code to determine a situation of the user. For example, the authentication processor may process the code to determine a panic situation, an unauthorized use situation, or a combination thereof.

The biometric authentication system may further include an access point that receives the code from the sensor and transfers the code to the authentication processor. The access point may include a communication interface that receives the code via radio frequency, telephony, keypad input, infrared transmission, electronic data transmission, or a combination thereof. The access point may grant a user access to a financial account, an entry, a surety account, a medical account, a means of transportation, government information, a computer, or a combination thereof.

In another embodiment, systems and methods for performing a transaction using a mobile handset are provided. In this regard, a system that performs a transaction includes a mobile handset that has a biometric sensor. The biometric sensor detects a biometric from a user of the mobile handset. The mobile handset is associated with an account number. The system also includes an authentication processor configured to receive an authentication code from the mobile handset. The authentication processor uses the authentication code to authenticate the user and the user is granted access to an account

corresponding to the account number when the user is authenticated by the authentication processor.

The account number may be a phone number. For example, cell phones are typically associated with a unique phone number so that phone calls are correctly directed to intended users. Since these phone numbers are unique, a financial entity may be configured to associate an account number to a particular phone number of a mobile handset thereby allowing a mobile handset to access a user's account.

The mobile handset may include a radio frequency interface that transmits the authentication code to the authentication processor. For example, the mobile handset may be configured to communicate via the radio frequency interface using a signaling technique such as Global System for Mobile communications ("GSM"), Code Division Multiple Access ("CDMA"), Wideband Code Division Multiple Access ("WCDMA"), Time Division Multiple Access ("TDMA"), Global Positioning System ("GPS"), Frequency Division Multiple Access ("FDMA"), or a combination thereof.

The mobile handset may include a storage element that stores biometric information of the user for comparison to a detected biometric. The mobile handset may also include a comparator that compares stored biometric information to the detected biometric to generate an authentication indicator. Additionally, the mobile handset may include a code generator that generates the authentication code from the authentication indicator, the stored biometric information, the detected biometric, the account number, a phone number associated with the mobile handset, a serial number of the mobile handset, or a combination thereof.

The authentication processor may include an interface that receives the authentication code from the mobile handset. For example, the interface may be a telephony interface, an Internet connection, or a combination thereof. The authentication processor may further include a comparator that compares a received authentication code to a stored authentication code to authenticate the user. Additionally, the authentication processor may include an authenticator communicatively coupled to the comparator to generate an authentication indicator when the user is authenticated by the comparator.

The system may include a first processing entity communicatively coupled to the authentication processor to grant access to the account when the user is authenticated by the authentication processor. Additionally, the system may include a second processing entity communicatively coupled to the first processing entity, wherein the first processing

entity transfers money from the account to the second processing entity to perform the transaction for the user. The system may also include a transaction processor communicatively coupled to the mobile handset to transfer transaction information to the mobile handset. The transaction processor may be communicatively coupled to the second processing entity, wherein the second processing entity transfers a transaction indicator to the transaction processor to indicate transaction performance. Alternatively, the transaction processor may be communicatively coupled to the first processing entity, wherein the first processing entity transfers a transaction indicator to the transaction processor to indicate transaction performance. The transaction may be a financial transaction, a property transaction, or a combination thereof, as described hereinbelow.

In another embodiment, a method of performing a transaction includes registering a biometric with a mobile handset to generate a code, transferring the code from the mobile handset to an authentication processor to authenticate the biometric, and granting access to an account when the biometric is authenticated to perform a transaction. Registering a biometric may include detecting the biometric with a sensor configured with the mobile handset, comparing the biometric to stored biometric information, and generating the code when the biometric corresponds to the stored biometric information. Generating the code may include configuring the code from a phone number associated with the mobile handset, a serial number of the mobile handset, and detected biometric information, the stored biometric information, an account number, or a combination thereof.

Transferring the code may include configuring a radio frequency telephony signal with the code. The method may also include receiving the code with an interface of the authentication processor. Additionally, the method may include retrieving a stored authentication code for comparison to a received code. For example, the method may also include generating an authentication indicator based on the comparison of the stored authentication code to the received code and transferring the authentication indicator to a financial entity. Granting access to an account may thereby include granting access to the account based on the authentication indicator.

The biometric authentication system is a methods described hereinabove may find other advantageous uses. For example, in one embodiment, a system for performing a property transaction includes a mobile handset that includes a biometric sensor, wherein the biometric sensor compares a detected biometric to stored biometric information to

generate an authentication code and an authentication processor configured to receive the authentication code from the mobile handset and compare the authentication code to a stored authentication code to grant access to a processing entity and perform a property transaction. The authentication processor may include an interface configured to receive the authentication code from the mobile handset. As such, the mobile handset may include an interface that communicatively couples to the authentication processor to transfer the authentication code. The interface may be a cellular telephony interface.

The authentication processor may also include a comparator that compares the authentication code to the stored authentication code to determine authenticity of a user of the mobile handset. The authentication processor may further include an authenticator communicatively coupled to the comparator to generate an authentication indicator when the user of the mobile handset is authenticated by the comparator. The authentication indicator may include a phone number associated with the mobile handset.

In another embodiment, a mobile telephony handset includes a transceiver that communicatively links via a phone number, a sensor that receives first biometric information, and a processor that processes the first biometric information to perform a transaction using the phone number. The mobile telephony handset may also include a storage element that stores second biometric information.

The mobile telephony handset may further include a comparator that compares the first biometric information to the second biometric information to authenticate a user such that the user may perform the transaction using the phone number. Additionally, the mobile telephony handset may include a communication interface that communicatively couples the mobile telephony handset to a transaction processor, wherein the transaction processor determines authorization of the transaction based on the phone number. The communication interface provides for communications to the transaction processor via radio frequency, Internet, Ethernet, infrared, serial cable, parallel cable, or FireWire.

Another embodiment of the invention includes a communication device having a sensor that receives biometric information, a processor that processes received biometric information to generate authentication information for use in a transaction, and a transmitter that transfers the authentication information for external transaction authorization. The device may further include a comparator that compares stored biometric information to received biometric information. Accordingly, the device may include a storage element that stores stored biometric information. The device may also

include a communication interface coupled to the transmitter that communicatively couples the device to a transaction processor. The transaction processor may be associated with a financial institution or a seller.

The authentication information may include a code. That code may or may not include biometric information of the user, subject to design choice. In one instance, the biometric information is not transferred for external transaction authorization. For example, the authentication information may be devoid of the biometric information. The code may be synchronizeable based on a plurality of sensed biometric inputs, as described in the '375 provisional. Alternatively or additionally, the authentication information may include a phone number. As such, the communication device may be a mobile telephony handset. Such a mobile telephony handset may be a cellular telephone that uses GSM, CDMA, FDMA, TDMA, or combinations thereof.

In one embodiment, a method for performing a transaction includes steps of registering a biometric with a portable communication device to convert the biometric to electronic biometric information and, with the portable communication device, processing the electronic biometric information to authenticate a user generating authentication information for a transaction when the user is authenticated.

The step of registering a biometric may include a step of providing the biometric to an electronic sensor, wherein the biometric is selected from a group consisting of DNA, a follicle pattern, a veinal pattern, an arterial pattern, a cardio pattern, a fingerprint, a voice pattern, an aural pattern, a retinal pattern, a corneal pattern, a skin pattern, or any combination thereof. The method may further include a step of electronically sensing the biometric to convert the biometric to the electronic biometric information.

Processing the electronic biometric information may include a step of comparing the electronic biometric information to biometric information stored with the portable communication device to determine whether the electronic biometric information corresponds to the biometric information stored with the portable communication device. The step of processing the electronic biometric information may further include a step of generating a first indicator when the electronic biometric information corresponds to the biometric information stored with the portable communication device. For example, generating the authentication information may include a step of formatting a phone number within the authentication information based on the first indicator. The authentication information may be devoid of the electronic biometric information and the

biometric information stored with the portable communication device. Processing the electronic biometric information may further include a step of generating a second indicator when the electronic biometric information does not correspond to the biometric information stored with the portable communication device.

The method may further include a step of using the second indicator to deny the transaction. Additionally, the method may include a step of transferring the authentication information to a transaction processor for authorization of the transaction. For example, the step of transferring the authentication information to a transaction processor may include a step of communicatively coupling the portable communication device to the transaction processor via an interface that supports radio frequency communication, Internet communication, Ethernet communication, infrared communication, serial cable communication, parallel cable communication, or FireWire communication.

In yet another embodiment, a method of securing a transaction includes steps of authenticating a transaction party based on a biometric, generating transaction information based on an authentication of the transaction party, and transferring the transaction information to an external transaction processor. The method may further include a step of registering the biometric with a sensor that converts the biometric into electronic biometric information. For example, the step of authenticating a transaction party may include a step of comparing electronic biometric information to stored biometric information to authenticate the transaction party. Based on a comparison of the electronic biometric information to the stored biometric information, the method may include a step of generating authentication information for use in generating the transaction information. The authentication information may be devoid of biometric information.

Generating a transaction information may include a step of formatting the transaction information with a phone number for use by the external transaction processor in authorizing the transaction. Generating the transaction information may include a step of configuring the transaction information into a format transferable by radio frequency, Internet, Ethernet, infrared, serial cable, parallel cable, or FireWire.

In one embodiment, a method for performing a transaction includes entering a code to a mobile handset using a keypad configured with the handset, transferring the

code from the mobile handset to an authentication processor to authenticate the code, and granting access to an account when the code is authenticated to perform a transaction.

While various embodiments and features of the invention have been described hereinabove, those skilled in the art should readily recognize that the invention is not intended to be limited to a particular embodiment. Rather, various features of the above embodiments may be combined so as to provide a user with biometric authentication capabilities that are not specifically discussed hereinabove. For example, in one embodiment, a personal biometric device may be maintained by a user for gaining access to an entrance without necessarily requiring system level authentication as described hereinabove. In such an embodiment, the personal biometric device may authenticate a user by simply comparing an input biometric to biometric information stored with the device. In this regard, the personal biometric device may transmit a signal (e.g., comprising a personal identification number or other code) to an entrance access control device. The entrance access control device may thereby compare the signal to information stored therewith to verify if the user is to gain access to an entrance. If the comparison finds that the user is authorized access to the entrance, the entrance access control device may grant such.

In one embodiment, the personal biometric device transmits the signal via an radiofrequency interface. For example, the personal biometric device may be configured with a Bluetooth interface that allows the personal biometric device to communicate with the entrance access control device via Bluetooth communications. In this regard, the entrance access control device may transfer a Bluetooth identification (e.g., a Bluetooth personal identification number, or PIN) to the entrance access control device for verification of authorized access of the user.

Additionally, the personal biometric device may include features such as the sectorization described hereinabove. For example, the personal biometric device may scan various sectors of a fingerprint to generate a code. That code may then be transferred to the entrance access control device without disclosing the biometric information of the user either to the entrance access control device or any system in communication therewith.

In addition to the advantages of not disclosing a user's biometric, such a system may reduce processing by an entrance access control device. For example, biometric comparisons are often processor intensive. By offloading the biometric processing to the

personal biometric, the entrance access control device may be relegated to less processor intensive code comparisons. The savings in processing by the entrance access control device may thereby be dedicated to other useful applications.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a block diagram of a biometric authentication system, in one exemplary embodiment of the invention.

Figure 2 is an illustration of a biometric device for use with a biometric authentication system.

Figure 3 is a block diagram of an authentication processor operable with a biometric authentication system.

Figure 4 is a block diagram of an exemplary comparator that compares codes used in a biometric authentication system.

Figure 5 is a flowchart illustrating an exemplary process that is operable with a biometric authentication system.

Figure 6 is a flowchart illustrating an exemplary process element of the process of Figure 5.

Figure 7 is a flowchart illustrating another exemplary process element of the process of Figure 5.

Figure 8 is a flowchart illustrating an exemplary process of a biometric authentication system.

Figure 9 is a flowchart illustrating another exemplary process of a biometric authentication system.

Figure 10 illustrates an exemplary biometric sectorization.

Figure 11 illustrates an exemplary user registration and code generation using biometric sectorization.

Figure 12 is a block diagram illustrating an exemplary system for performing transactions with a mobile handset.

Figure 13 is a block diagram of an exemplary authentication processor used in the system of Figure 12.

Figure 14 illustrates an exemplary mobile handset.

Figure 15 is a block diagram of another exemplary system for performing transactions.

Figure 16 is a block diagram of yet another exemplary system for performing transactions.

Figure 17 is a flowchart illustrating an exemplary process for performing transactions.

Figure 18 is a flowchart illustrating another exemplary process for performing transactions.

Figure 19 is a flowchart illustrating yet another exemplary process for performing transactions.

Figure 20 illustrates an embodiment in which a user uses a personal biometric device to gain access to an entrance.

Figure 21 illustrates an exemplary block diagram of the personal biometric device used in Figure 20.

DETAILED DESCRIPTION OF THE DRAWINGS

While the invention is susceptible to various modifications and alternative forms, specific embodiments thereof have been shown by way of example in the drawings and are herein described in detail. It should be understood, however, that it is not intended to limit the invention to the particular form disclosed, but rather, the invention is to cover all modifications, equivalents, and alternatives falling within the scope and spirit of the invention as defined by the claims.

Figure 1 is a block diagram of exemplary biometric authentication system 100. In this embodiment, system 100 authenticates a user's biometric to grant user 104 access 108 to, for example, goods, services, premises information, a financial account, transportation, a computer, a network, a website, a database, a cell phone, etc. via access point 103. In addition to granting access to user 104, biometric authentication system 100 may be configured for generating alarm message 110 based on a particular situation for user 104. For example, if user 104 is in a panic situation (e.g., forced to operate against his or her will), user 104 may enter a biometric with personal biometric device 102 in a particular manner that triggers generation of alarm message 110. Alternatively, the generation of alarm message 110 may be triggered when user 104 is an unauthorized user entering the incorrect biometric.

Generally, biometric information of the user 104 is stored with a device 102 personal to the user. For example, personal biometric device 102 may have user 104's fingerprint information stored therewith. In this regard, user 104 may keep the fingerprint

information in his possession. User 104 may use personal biometric device 102 to scan user 104's fingerprint. Personal biometric device 102 may compare the inputted fingerprint information of user 104 to the stored fingerprint information and generate a code upon valid comparison of the inputted fingerprint information to the stored fingerprint information. User 104 may then use the generated code as an input at access point 103 for authentication processor 101 to authenticate. Although user 104's biometric information is stored with personal biometric device 102, system 100 does not require further storage of the biometric information. Additionally, system 100 may accomplish alarm message 110 generation without the need for storing biometric information of user 104 with centralized processing (e.g., authentication processor 101).

The code generated by personal biometric device 102 may be synchronized with codes of authentication processor 101. For example, authentication processor 101 may include a code generator, such as a random number generator, which generates codes associated with user 104's account. In one embodiment, the code is a random number that optionally includes at least part of an encoded version of the serial number of personal biometric device 102. Similarly, personal biometric device 102 may include a code generator that is algorithmically synchronized to the code generator of authentication processor 101. When user 104 inputs a generated code into access point 103, the access point may transfer that code to authentication processor 101 for comparison to a code generated by authentication processor 101. Upon a valid comparison of the two codes, authentication processor 101 may transfer an access indicator to access point 103 to grant access 108 to user 104. Examples of code generators are illustrated and described below in Figures 2 and 3.

Generation of alarm message 110 may also function in a similar manner. For example, personal biometric device 102 may be configured for receiving different biometrics, such as two different fingerprints. A first biometric may initiate code generation within personal biometric device 102 for authentication purposes. A second biometric may be used to covertly initiate generation of alarm message 110 when user 104 is in a panic situation. That is, the second biometric may cause personal biometric device 102 to generate a code that is designated for generating alarm message 110. The code may be entered with access point 103 and transferred to authentication processor 101 such that alarm message 110 may be generated and transferred to access point 103 (e.g., to deny access) and/or to a responsible authority (e.g., police, security, etc.).

Alternatively, personal biometric device 102 may be configured for receiving a particular biometric in a certain way that triggers generation of alarm message 110. For example, when user 104 scans a fingerprint with personal biometric device 102 in an incorrect manner (i.e., other than for authentication purposes), the personal biometric device may generate a code designated for generating alarm message 110. Again, the code may be entered with access point 103 and transferred to authentication processor 101 to generate alarm message 110.

Although described with respect to generating alarm message 110 with authentication processor 101, the invention is not intended to be limited to such alarm message generation. Rather, alarm message 110 may be generated at other points within system 100. For example, when user 104 scans a biometric for panic purposes, personal biometric device 102 may generate alarm message 110 to alert responsible authorities (e.g., either audibly or via data transmission such as through RF communications). Alternatively, personal biometric device 102 may generate a panic code that is instantly recognized when entered at access point 103. As such, access point 103 may generate alarm message 110 to alert the responsible authorities.

Regarding authentication, algorithmic synchronization of the two code generators (i.e., of personal biometric device 102 and authentication processor 101) as used herein implies that authentication processor 101 may not require continuous communication to personal biometric device 102. For example, authentication processor 101, as illustrated herein, has no access to biometric information stored with personal biometric device 102. Rather, personal biometric device 102 may be used for one-way communication (e.g., a simplex communication) to user 104 and/or to access point 103. Algorithmic synchronization, therefore, refers to the process in which codes are similarly generated between personal biometric device 102 and authentication processor 101.

In one embodiment, authentication processor 101 generates and stores a predetermined number of codes. When personal biometric device 102 becomes out of sync, or desynchronizes, with a "next in line" code of authentication processor 101, user 104 may be required to reenter a biometric (e.g., rescan user 104's fingerprint) and generate a new code for input to access point 103. For example, user 104 may use personal biometric device 102 to scan a fingerprint and generate a code. If user 104 does not use that freshly generated code, that code may expire and codes of authentication processor 101 may desynchronize with subsequent codes of personal biometric device

102. Once out of sync, user 104 may be required to rescan a fingerprint for a predetermined number of times to generate a corresponding sequence of codes. The sequenced input of these codes to access point 103 may correspond to a sequence of codes stored with authentication processor 101. Authentication processor 101 may, therefore, algorithmically search for the input sequence of codes from the stored sequence of codes and generate an access indicator based on the correctly input sequence. Authentication processor 101 may then transfer this access indicator to access point 103 to grant access 108 to user 104.

In one embodiment, system 100 includes one or more secondary processing elements 107 for processing portions of a code input by user 104 to access point 103. For example, the code processing of authentication processor 101 described hereinabove may be performed off authentication processor 101 by secondary processing element 107. In such an embodiment, a code input by user 104 to access point 103 may be compared entirely to a synchronized code of secondary processing element 107. However, security of such code processing may be enhanced via processing by a plurality of secondary processing elements 107 wherein each secondary processing element 107 processes a portion of a code entered by user 104. Such separable code processing by a plurality of secondary processing elements 107 may enhance security of system 100 because attempts to retrieve an entire code from system 100 (e.g., through "hacking" and/or other security attacks) are inhibited.

Additionally, system 100 may be configured with a verification element 105 which further enhances security. For example, verification element 105 may receive an access indicator from authentication processor 101 once the code has been successfully input to access point 103 by user 104. Verification element 105 may then require additional information from user 104, such as a password or account information (e.g., via the swiping of a magnetic strip on a credit card). The increased number of security features may lessen the probability of an unauthorized access by biometric authentication system 100.

In one embodiment, a Lock Administrator is responsible for distributing devices to users. The Lock Administrator, for example, might be an individual who is responsible for distributing a plurality of devices 102 to company employees. In this regard, the Lock Administrator would be able to delete a user and/or enroll a new user via authentication processor 101. The Lock Administrator, however, would not be able to delete himself

from biometric authentication system 100. To ensure integrity of biometric authentication system 100 in the event that Lock Administrator is removed from his position at the company, devices 102 may be disposed of or reconfigured for other users.

Biometric authentication system 100 may be configured in a variety of ways to implement the principles described herein. For example, authentication processor 101 may be a general-purpose computer or server hosting software configured to receive and process a code to grant access 108 to user 104. Secondary processing element 107 and verification element 105 may be similarly configured as general-purpose computers or servers to perform as described herein. Access point 103 may be any well-known device for authenticating a user that is configured for receiving an input code from the user. The manner in which access point 103 may be configured to receive such an input is typically a matter of design choice. For example, access point 103 may be configured with a key pad, a dataport (e.g., serial interface, ethernet interface, etc.), an infrared receiver, a Radio Frequency ("RF") receiver, etc. that receives a code from user 104 as appropriate. For at least these reasons, those skilled in the art should readily recognize that the invention should not be limited to any particular configuration used to implement the principles described herein.

Figure 2 is an illustration of exemplary personal biometric device 200 for use in a biometric authentication system, such as personal biometric device 102 used in biometric authentication system 100 of Figure 1. In this embodiment, personal biometric device 200 is configured for scanning a fingerprint 203 of a user (e.g., user 104 of Figure 1) and authenticating the scanned fingerprint. For example, biometric device may include a sensor 202 used to sense the user's fingerprint 203 being depressed against sensor 202 and/or "swiped" across sensor 202. Sensor 202 may subsequently convert the sensed fingerprint to electronic data representative of the sensed fingerprint and compare that electronic data to fingerprint information of the user stored with personal biometric device 200 to register the user. Personal biometric device 200 may then generate an authentication code via code generator 204 and display that code to the user via display unit 201. Generally, the authentication code is not continuously maintained with personal biometric device 200. For example, after a pre-determined period of time and/or a swipe of the fingerprint, the authentication code may be deleted from memory of personal biometric device 200. User registration and code generation are described in further detail in Figures 10 and 11.

Sensor 202 may be configured to scan fingerprint 203 in a manner that is subject to design choice. For example, sensor 202 may be configured to perform either optical scanning or capacitance scanning. In regard to optical scanning, sensor 202 may include a charge coupled device ("CCD"). A CCD is an array of light-sensitive diodes (a.k.a. photosites), which generates an electrical signal in response to photons. Each photosite records a pixel (i.e., a dot representing impinging light at a particular location). Collectively, light and dark pixels may be used to form an image of the scanned scene (e.g., a finger). An analog-to-digital converter is commonly used to process the analog electrical signal and generate a digital representation of this image. Sensor 202 may also include a light source (e.g., an array of light-emitting diodes) for illuminating the ridges of the finger. Using this illumination, the CCD may generate an inverted image of the finger, with darker areas representing more reflected light (e.g., the ridges of the finger) and lighter areas representing less reflected light (e.g., the valleys between the ridges). Those skilled in the art are familiar with CCDs and their applications for generating images.

In an alternative embodiment, sensor 202 may be configured to scan fingerprint 203 using capacitance. Like optical scanning, capacitive scanning may be used to generate an image of the ridges and valleys that make up a fingerprint. Instead of sensing the fingerprint using light, the capacitors use electrical current. In this regard, sensor 202 may be configured from one or more semiconductor chips containing an array of cells. Each cell may include two conductor plates covered with an insulating layer. The cells are generally smaller than the width of a ridge on a finger.

The two conductor plates form a basic capacitor. The surface of the finger acts as a third capacitor plate, separated by the insulating layers in the cell structure and, in the case of the fingerprint valleys, a pocket of air. Varying the distance between the capacitor plates (e.g., by moving the finger closer or farther away from the conducting plates) changes the total capacitance of the capacitor. That is, a cell capacitor proximate to a ridge has a greater capacitance than a cell capacitor proximate to a valley. Since the distance to the finger alters capacitance, a finger ridge will result in a different voltage output than a finger valley. These voltage differences may be processed to determine biometric features (e.g., ridges and/or valleys) and subsequently the used to generate an image of the fingerprint. Those skilled in the art are also familiar with capacitance scanning and its applications in generating images.

In accordance with the alarm message generation embodiments described hereinabove, personal biometric device 200 may be configured to sense a user's fingerprint 203 for panic situation determinations. For example, the user may swipe fingerprint 203 across sensor 202 with a finger designated for alarm generation and/or in a particular manner. Personal biometric sensor 200 may detect the alarm-causing fingerprint scan and generate a code that, when entered into an access point such as access point 103 of Figure 1, triggers generation of the alarm message. Alternatively, personal biometric device 200 may detect the alarm-causing fingerprint scan and generate an alarm message (e.g., audibly and/or via a data communication through communication port 205).

Although discussed in terms of fingerprint sensing and the electronic data conversion thereof, those skilled in the art should readily recognize that the invention is not intended to be limited to the illustrated embodiment. Implementations of such fingerprint sensing are often a matter of design choice. Additionally, those skilled in the art should readily recognize that personal biometric device 200 may be configured to sense other biometrics, such as retinal information, corneal information, pulse information, DNA, ocular information, etc. Accordingly, the invention should not be limited to the exemplary embodiment of fingerprint sensing described and illustrated herein.

Personal biometric device 200 may also be configured with an output communication port 205 for conveying a generated code to an authentication device, such as access point 103 of Figure 1. For example, output communication port 205 may be a serial port, an infrared port, an RF port, etc., each of which being configurable for conveying a code generated by personal biometric device 200 to access point 103. In such an embodiment, display unit 201 may be an alternative feature of personal biometric device 200 because the generated code information may no longer be useful to the user.

In one embodiment, a Lock Administrator may issue personal biometric device 200 to the user. When device 200 is issued to user 104, the user may be able to establish code synchronization without the assistance of a Lock Administrator. In such an embodiment, user 104 may, for example, initiate and/or resync personal biometric device 200 by pressing and holding a button and/or "swiping" a finger one or more times across sensor 202. However, user 104 may not delete himself after enrollment. Such disenrollment may be reserved for the Lock Administrator.

Once enrollment is successfully completed, the device may generate, for example, a 16 character alphanumeric registration code, which may be based on a random number, a serial number, and/or a sectorization of the user's fingerprint. This generated number may be stored in non-volatile memory (e.g., non-volatile random access memory; "NVRAM"). This code may be overwritten if the Lock Administrator disenrolls the user so that a new user may be enrolled. In this instance, a new registration code is created and stored on the device. The 16-character registration code may be displayed on display unit 201 immediately after a successful enrollment.

In one embodiment, display unit 201 is a liquid crystal display ("LCD") that displays 8 characters of the registration code. Accordingly, personal biometric device 200 via display unit 201 displays the first 8 characters and, e.g. after the push of a button, the next 8 characters. The button depression may be used to toggle between the first set of 8 characters and the second set of 8 characters. However, those skilled in the art should readily recognize that display unit 201 may be configured to display all 16 characters, for example, via two rows of 8 characters on the LCD. Additionally, the user may be able to retrieve this 16-character registration code at a later time following, for example, an authorized finger swipe and series of button pushes. In one embodiment, the registration code is communicated to the Lock Administrator who then enters it into a database of authentication processor 101 of Figure 1 to manage access privileges of biometric device users. Moreover, those skilled in the art should readily recognize that the invention is not intended to be limited to any particular length of registration code. For example, as encryption schemes become more complex and/or sophisticated, code may lengths may change.

Those skilled in the art are readily familiar with configuring a device, such as personal biometric device 200, with an LCD and buttons to control the LCD. For example, personal biometric device 200 may be configured as an embedded device controlled by a microprocessor and embedded software to control such features of the device. Moreover, personal biometric device 200 may be configured with a mobile handset (e.g., a cell phone) wherein features of the personal biometric device are included as embedded components of the mobile handset. Examples of such are shown and described in commonly owned and co-pending U.S. Patent Application No. 11/194,514 (filed Aug. 8, 2005). Those skilled in the art are readily familiar with embedded systems and software.

Figure 3 is a block diagram of exemplary authentication processor 101 of Figure 1 operable with access point 103. In this embodiment, authentication processor 101 is configured for receiving a code 301 from access point 103 as input by a user (e.g., user 104 of Figure 1). Authentication processor processes code 301 to generate an authentication indicator to grant access to the user via access point 103 (i.e., upon verification of a successful code entry). Alternatively, authentication processor may deny access to the user and generate alarm message 110 as described hereinabove in response to certain received codes.

To receive code 301, authentication processor 101 is communicatively coupled to access point 103 via communication link 312. Authentication processor 101 may include interface 302 for transferring information between access point 103 and authentication processor 101 via communication link 312. For example, authentication processor 101 may receive codes from access point 103 for processing. Authentication processor 101 may also transmit authentication indicators to access point 103. The communication link 312 between authentication processor 101 and access point 103 may be used to implement this communication. In this regard, communication link 312 may be configured in a variety of manners that are often a matter of design choice. For example, communication link 312 may be an Internet connection, a wireline connection (e.g., Universal Serial Bus, or "USB"; Institute for Electrical and Electronics Engineers standard 1394, or "FireWire"; American National Standards Institute twisted pair categories 1-6, or "ANSI Cat" 1-6; etc.), an infrared connection, and/or an RF connection. Those skilled in the art are readily familiar with establishing such communication links between devices.

Authentication processor 101 may include comparator 304 communicatively coupled to interface 302 for receiving code 301 from access point 103. Comparator 304 may be configured for comparing code 301 to codes 303 and/or 306 generated by authentication processor 101. For example, codes 306 may be used for authenticating a user to grant access as described hereinabove. Code 303 may, however, represent a panic code that comparator 304 compares to code 301 to determine a particular panic situation of the user (e.g., action against the user's will and/or unauthorized use).

Code 303 may be associated with a unique user account 308. For example, account number 308_1 may be associated with one user. When code 301 enters authentication processor 101 via access point 103, comparator 304 may correspond to

code with the user associated with account 308_1. Accordingly, comparator 304 may evaluate code 301 with respect to code 303 to determine a situation of the user. Once the situation of the user is determined, comparator 304 may generate alarm message 110 and transfer the alarm message to authenticator 305 for distribution. For example, authenticator 305 may transfer the alarm message to access point 103 to deny access (e.g., in the case of an unauthorized user) and/or alert responsible authorities (e.g., police, security, etc.). Although illustrated as one code (i.e., code 303), those skilled in the art should readily recognize that the invention is not intended to be limited to a single "panic code". For example, authentication processor 101 may use a plurality of codes to represent a corresponding plurality of user situations.

Regarding authentication, comparator 304 may compare code 301 to codes 306 upon determining whether a panic situation exists to determine whether access should be granted. For example, comparator 304 may indicate to authenticator 305 that a user be granted access upon a valid comparison of codes 301 and 306. Authenticator 305 may thereby generate an authentication indicator and transfer that authentication indicator to interface 302 for subsequent use by access point 103. Access point 103 may then use the authentication indicator to grant access to the user.

Codes 301 and 306 may be generated from synchronized code generators. For example, authentication processor 101 may include a code generator 307 configured for generating codes 306 for a particular user account 308. A biometric device, such as personal biometric device 200 of Figure 2, may include a code generator that generates code 301 upon verification of a biometric input with the biometric device. Code generator 307 may be configured in a manner similar to that of the biometric device wherein the two code generators are synchronized to each other when an authentication account is created for the user (discussed herein below). Once synchronized, the code generator 307 and the code generator of the biometric device may generate the same codes although the two code generators are independent of one another.

The code generator 307 and the code generator the biometric device may "desynchronize" over a period of time. For example, when a user scans a fingerprint across a sensor of the biometric device and the biometric device subsequently verifies the fingerprint, the biometric device generates a code 301. If that code is not used by the user (e.g., input to access point 103), the code generated by the biometric device may expire and the two code generators become unsynchronized.

To counter such desynchronization effects, code generator 307 may generate a plurality of codes 306. Since the code generator 307 and the code generator of the biometric device are similarly configured to generate the same code sequence, the two code generators may be resynchronized by having the user reenter a biometric to generate a new code for input to access point 103. Alternatively, authentication processor 101 may require the user to reenter a biometric, generate a new code and enter the new code into input device a predetermined number of times (e.g., input a sequence of codes with access point 103). Once a new code or a sequence of new codes has been correctly entered with access point 103 and authenticated by authentication processor 101, the code generator 307 resynchronizes with the code generator of the biometric device because code generator 307 will be aware of the next number generated by the biometric device. Accordingly, the codes generated by the biometric device and code generators 307 may be once again be synchronized for subsequent identity authentication. In one embodiment of the invention, the code generator 307 and the code generator of the biometric device are random number generators configured for generating random codes. Such codes may be alphanumeric in nature and contain various randomization techniques, such as those found in well-known 32-bit, 64-bit and 128 bit encryption techniques.

In one embodiment of the invention, authentication processor 101 has an account generator 311. The account generator 311 is communicatively coupled to interface 310 for establishing an account for a biometric user. For example, account generator 311 may generate an account 308 for a new biometric device user based on an organization's need for biometric authentication. The user may establish the account with account generator 311 by inputting certain information, such as name, birthday, address, phone number, social security number, etc., via interface 310. Interface 310 may be substantially any type of communication interface (e.g., a graphical user interface, or "GUI") that enables the user to communicate such information to account generator 311. Account generator 311 may then generate an account 308 for the user based on the user's entered information.

Once an account 308 is established, account generator may transfer a code synchronization "seed" to the user for entrance into the user's biometric device. For example, the code generator of the biometric device may generate random codes; however, randomization of the codes may begin from a certain predetermined number. Account generator 311 may generate that predetermined number as a seed from which the

code generator of the biometric device is to begin random code generation. To synchronize code generator 307 with the code generator of the biometric device, account generator 311 may similarly seed code generator 307.

Account generator 311 may be used to generate a plurality of accounts 308; for example, account generator 311 may generate one account for each registered biometric device. Code generator 307 may be used to generate a plurality of codes 306 (i.e., a code sequence) for each account 308. The accounts 308 and their associated authentication codes 306 may be stored in storage unit 309 of authentication processor 101. For example, authentication processor 101 may be a general-purpose computer or server having an account database configured within a hard disk drive thereof for storing and maintaining accounts 308.

Components of authentication processor 101 may be configured in a variety of ways that fall within the scope and spirit of the invention. For example, components (e.g., code generator 307, comparator 304, authenticator 305, account generator 311, interfaces 302 and 310 and storage unit 309) of authentication processor 101 may be configured from hardware, software, firmware or various combinations thereof and implemented as a sort of centralized processing. Those skilled in the art are readily familiar with hardware, software, firmware and their various combinations.

Figure 4 is a block diagram of exemplary comparator 304 that compares codes used in a biometric authentication system, such as biometric authentication system 100 of Figure 1. For example, comparator 304 may be configured with authentication processor, such as authentication processor 101 of Figure 3, to compare a code received from a personal biometric device (i.e., "Generated Code"), such as personal biometric device 200 of Figure 2, to one or more codes 303/306 that are associated with a user's account (i.e., "Access Code", "Panic Situation Code", and "Unauthorized User Code").

The comparison of the generated code to the codes associated with the user's account may be used to generate an authentication indicator and/or an alarm message. For example, comparator 304 may retrieve a code associated with the user's account to compare the Generated Code to the access code and thereby grant access to the user by generating an authentication indicator to an access point where the user is located. Comparator 304 may also retrieve a Panic Situation Code and an Unauthorized User Code associated with user's account for comparison to the Generated Code. When the Generated Code corresponds to the Panic Situation Code, comparator 304 may generate

an alarm message to alert the responsible authorities as described hereinabove. In one embodiment, comparator 304 may also generate an authorization indicator to grant access to the user while alerting the responsible authorities. For example, the biometric authentication system may be used to grant access to an unauthorized user to induce the unauthorized user into a position until the responsible authorities arrive. Similarly, when the Generated Code corresponds to an Unauthorized User Code, comparator 304 may generate an alarm message to alert the responsible authorities.

Although described with respect to being configured with an authentication processor, those skilled in the art should readily recognize that comparator 304 may be configured with other devices of the biometric authentication system. For example, comparator 304 may be configured with a personal biometric device or an access point, such as those described hereinabove, to achieve similar results. Accordingly, the invention is not intended to be limited to the exemplary embodiment described herein.

Additionally, the codes described herein (i.e., Generated Code, Panic Situation Code, Unauthorized User Code, and Access Code) illustrate separate and distinct codes. Those skilled in the art, however, should readily recognize that the codes may represent components of a synchronizable code as described hereinabove. For example, a personal biometric device and the authentication processor may be synchronized so as to grant access to a user even though that user has inadvertently generated a code by entering a biometric with the personal biometric device. The codes generated by the personal biometric device as well as the synchronized codes of the authentication processor may include code components which are used to indicate panic situation's and/or unauthorized use.

The system and associated components described hereinabove provide for general biometric authentication with optional features of alarm generation. Below, biometric methods are described in greater detail. Additionally, alarm generation methods, biometric sectorization and code generation, and transactional embodiments with biometric authentication are described below in greater detail.

General Biometric Authentication Methods

Figure 5 is a flowchart illustrating process 400 operable with a biometric authentication system, such as biometric authentication system 100 of Figure 1. In this embodiment, a user initiates biometric authentication by entering a biometric into a biometric device, such as biometric device 200 of Figure 2, in element 401. The

biometric device subsequently generates a first code which is optionally displayed with the biometric device, in element 402. For example, upon entering a valid biometric, the biometric device may generate a code for the user to input to an authentication device, such as access point 103 of Figure 1. The biometric device may display this code upon a display unit of the device such that the user may read the code and input the code to the authentication device. Alternatively, the biometric device may communicate the code directly to the authentication device (e.g., via infrared, RF, etc.). The code is thereby input to the authentication device, in element 403.

Once the code is input to the authentication device, the code is processed to verify that the code is valid. For example, a processor, such as authentication processor 101 of Figure 1, may generate a second code for comparison to the code generated by the biometric device (i.e., the first code), in element 404. Once the two codes are compared, processing is performed to determine whether the first and second codes match, in decision block 405. If the first and second codes match, then an authentication indicator is transferred to the authentication device where, for example, the user is located, in element 406. The authentication indicator is used to grant the user access to a secure site, in element 409. Examples of a secure site may include a secure entrance, financial account information, transportation, premises, goods, services, etc.

If the first and second codes do not match in decision block 405, a second decision may be made to determine whether the first code is unsynchronized with the second code, in element 407. For example, a user may enter a biometric into the user's personal biometric device to generate a code. If a code is not used, subsequent codes by the biometric device may be unsynchronized with respect to the second code. Decision block 407 may therefore determine if an entered code is within a certain sequence of codes maintained by the processor. If a determination is made that the first code and the second code are merely unsynchronized, processing of the method 400 may return to element 401 to have the user reenter a biometric into the user's personal biometric device. Method 400 may therefore continue processing as previously described. If, however, a determination is made in decision block 407 that the first and second codes are not unsynchronized, access is denied and the method terminates, in element 408.

Those skilled in the art should readily recognize that the features of method 400 are exemplary in nature and are not intended to limit the invention to a particular embodiment. Additionally, those skilled in the art should readily recognize that the

features of method 400 may be implemented in a variety of manners. Certain features of method 400 may be implemented in hardware, software, firmware or various combinations thereof to implement the concepts herein. For example, a biometric device may comprise a hardware sensor, a processor and firmware components to sense a user's biometric and generate the first code. Accordingly, those skilled in the art should readily recognize that the invention is not intended be limited to the exemplary embodiment described herein.

Figure 6 is a flowchart illustrating one exemplary process 401 of the methodical embodiment 400 of Figure 5. For example, entering a biometric into a biometric device may include sensing the biometric with a sensor, in element 421. Examples of such biometric sensing may include retinal scans, corneal scans, fingerprint scans, DNA sensing, ocular sensing, pulse sensing, etc. Once the biometric is sensed, the biometric may be converted to electronic information for comparison to stored biometric information within the device, in element 422. A decision is made in decision block 423 to determine whether the entered biometric matches the stored biometric information of the device. If the entered biometric does match the stored information of the biometric device, the process 401 may proceed to element 402 of method 400. If the entered biometric does not match the stored information of the biometric device, process 401 may be terminated, in element 424, as a security feature to prevent code generation for an unintended user.

Security may be enhanced in element 424 by configuring the determination process with certain optional features. For example, if the biometric device has an invalid biometric entered a certain number of times, element 424 may be configured to block out the biometric device from future biometric entries.

Figure 7 is a flowchart illustrating exemplary process 407 of the methodical embodiment 400 of Figure 5. For example, upon an indication that the first and second codes do not match in decision block 405, decision block 407 may determine if the first code is a "member code" of a sequence of codes generated by a processor, such as authentication processor 101 of Figure 1. The sequence of codes may be generated by a code generator of the processor that is synchronized to a code generator of a user's personal biometric device. The code generator of the processor may generate a sequence of codes in anticipation of codes generated by the biometric device. Accordingly, when a first code is generated by the biometric device that does not match, a determination may

be made in element 441 as to whether the first code is one of the sequence of codes generated by the processor.

If the first code is a member code, the processor may initiate synchronization of the two code generators, namely the code generator of the processor and the code generator of the biometric device, in element 442. This synchronization may be performed as described in Figure 5. For example, the decision block 407 may return to element 401 of Figure 5. If, however, the first code is not a member of the codes generated by the code generator of the processor, decision block 407 proceeds to terminate via element 408 of Figure 5.

Biometric Authentication and Alarm Generation Methods

Figure 8 is a flowchart illustrating exemplary process 400 operable with a biometric authentication system, such as biometric authentication system 100 of Figure 1. For example, flowchart 500 illustrates process elements of a biometric authentication system that grants access to a user and determines a situation of the user (e.g., unauthorized use and/or force against will). In this embodiment, a user initiates biometric authentication by entering a biometric into a personal biometric device, such as personal biometric device 200 of Figure 2, in process element 501. The personal biometric device compares the entered biometric with stored biometric information, in process elements 502. A personal biometric device then generates a code based on the comparison, in process element 503 that is used to grant access and/or determine the user's situation.

The generated code is transferred to an authentication processor, such as authentication processor 101 Figure 1, to process the code, in process element 504. For example, once the code is generated with the personal biometric device, the user may transfer the code to the authentication processor via an access point, such as access point 103 of Figure 1. The code may be transferred by entering the code through a key pad at the access point. Alternatively, the code may be transferred to the authentication processor by means of the data transmission, such as through RF communications or through wireline communications. Once received by the authentication processor, the code is processed to determine a situation of the user, in process element 505.

In processing the code, the authentication processor may compare the code (e.g., via a comparator such as comparator 304 of Figure 4) to a unique code associated with the user's account to determine a particular situation. For example, the authentication processor may compare the code to an unauthorized user code to determine whether the

code indicates that the user is authorized to use the personal biometric device, in process element 506. Such may occur when an unauthorized user uses the personal biometric device thereby generating an unauthorized user code. If the user is not authorized to use the personal biometric device, an alarm message may be generated, in process element 507. Once the alarm message is generated, the alarm message may be transferred to an access point for access denial and/or to a responsible authority, such as police and/or security, in process element 509. Alternatively, the alarm message may be transferred to the access point to grant access so as to induce an unauthorized user into a position until arrival of the responsible authority. If the code does not correspond to an unauthorized user code, process 500 continues to process element 508.

In process element 508, the authentication processor may determine whether the code indicates a panic situation for the user. For example, when a user is being forced against his will to use a personal biometric device to gain access to an account, the user may enter a biometric in a particular manner that triggers alarm message generation (e.g., by entering a biometric designated for panic situations). If the authentication processor determines from the code that the user is in a panic situation, the authentication processor may generate alarm message that alerts responsible authorities (e.g., in process element 509). If the authentication processor determines that the code does not indicate a panic situation for the user, process 500 continues to process element 510.

In process element 510, the authentication processor may process a code to grant access in accordance with that described hereinabove. For example, a personal biometric device may generate a code that is synchronized with code generation of the authentication processor. As such, the authentication processor may receive the code from the personal biometric device and determine whether the code corresponds to a synchronized code stored with the authentication processor. Once the authentication processor determines that the code corresponds to a synchronized code, the authentication processor may generate an authentication indicator to grant access to the user as described hereinabove.

Although one embodiment has been shown and described with respect to a particular process of a biometric authentication system, those skilled in the art should readily recognize that the invention is not intended to be limited to a particular embodiment. For example, certain process elements, such as process elements 506 and 508, within process 500 may be performed in other sequences. Nor is the invention

intended be limited to a particular type of code generation. For example, process 500 may be configured to process a code generated by a personal biometric device that includes code components indicative of unauthorized use, panic situations, and/or other situations relevant to a user. Process 500 is also described with respect to being primarily performed within an authentication processor; but, authentication and/or alarm generation may be similarly performed in other components. Process 600 in Figure 9 illustrates an exemplary alarm generation being performed primarily with a personal biometric device.

Figure 9 is a flowchart illustrating exemplary process 600 operable with a biometric authentication system. In this embodiment, alarm generation is performed primarily with a personal biometric device, such as personal biometric device 200 of Figure 2. A user may enter a biometric with a biometric sensor of the personal biometric device, in process element 601. The personal biometric device may then compare the entered biometric with biometric information stored therewith, in process element 602. Based on the entered biometric or the manner in which a biometric was entered, the personal biometric device may determine a situation of the user, in process element 603. For example, when a user enters an incorrect biometric (e.g., the wrong fingerprint) or when an unauthorized user enters a biometric, the personal biometric device may compare the incorrect biometric to the stored biometric information and determine whether the biometric indicates an unauthorized user, in process element 604. Another example of the incorrect biometric being entered includes swiping a finger print at a particular rate or speed that triggers alarm generation. Other examples include use of a dead or cut off finger (e.g., electrochemical properties may change detection properties) and the number of times that a biometric is entered (e.g., swiping a fingerprint two times as opposed to one time). Although described primarily with respect to fingerprints, those skilled in the art should readily recognize that the incorrect biometric may include other forms of biometric inputs such as those described herein.

If a determination is made that the user is not authorized use of the personal biometric device, process 600 continues to process element 605 to generate alarm message. The generated alarm message may be transferred to an access point and/or a responsible authority, in process element 608, as described hereinabove. If, however, a determination is made that the user is authorized use of the personal biometric device, a determination is made regarding the situation of the user, in process element 606. For example, if a user is forced to enter a correct biometric with a personal biometric device,

the user may enter a biometric in a manner that triggers alarm message generation. The personal biometric device may, therefore, determine whether the entered biometric indicates a panic situation for the user based on the manner in which the biometric was entered into the device. If the entered biometric indicates that the user is in a panic situation, process 600 continues to process element 605 to generate an alarm message.

If the entered biometric does not indicate a panic situation for the user, the personal biometric device may generate an authentication code to grant access, in process element 607. For example, the personal biometric device may generate an authentication code as described hereinabove so that the user may enter the authentication code with an access point for subsequent authentication by the authentication processor. Accordingly, the authentication code may be transferred to an authentication processor, in process element 609.

Again, while process 600 illustrates and describes one manner in which alarm generation may be performed within a biometric authentication system, those skilled in art should readily recognize that the invention is not intended to be limited to a particular embodiment. For example, process elements, such as process elements 604 and 606, may be performed in other manners while attaining essentially the same alarm message generation. Additionally, those skilled in the art should readily recognize that certain features of process 600, and for that matter process 500, may be implemented in hardware, software, firmware or various combinations thereof to implement the concepts herein. For example, a personal biometric device may comprise a hardware sensor, a processor and firmware components to sense a user's biometric and generate the first code.

Biometric Sectorization and Code Generation

Figure 10 illustrates biometric sectorization. In this embodiment, a sensor, such as sensor 200 of Figure 2, may be used to scan thumb print 700 in one or more sectors (e.g., sectors 701 - 710) to register a user. The sensor may generate a code therefrom for use in a biometric authentication system, such as biometric authentication system 100 in Figure 1. For example, each sector of thumb print 700 includes a plurality of biometric features 711 (e.g., ridges and valleys). The sensor may detect one or more of these biometric features within thumb print 700 (e.g., via optical scanning or capacitance scanning). The detected biometric features may be assigned values that are compared to biometric information of the sensor's user (e.g., possessor) to verify the authenticity of

the user. The values may also be used by a code generator, such as code generator 202 of Figure 2, to generate the code.

Regarding the assignment of values for detected biometric features, the sensor may assign vectors (e.g., vectors 712 through 718) that represent corresponding detected ridges. The assigned vectors may include values, which may be processed by comparing the values to biometric information stored with the sensor to determine a sensor user's authenticity. That is, the sensor may compare assigned vector values to stored biometric values of a sensor's user (e.g., possessor) to determine whether a person entering a biometric with the sensor is authorized to use the sensor. Upon authentication of the sensor's user, the sensor may use the assigned vector values to generate a code for use with a biometric authentication system.

As an exemplary illustration of user registration and code generation, the sensor may detect ridges and/or valleys on a particular scan of thumb print 700 and assign vectors thereto. Certain vectors, such as vectors 720 and 721, may be used as a reference frame that allows for the comparison of other vectors, such as vectors 712 through 718, to stored biometric values. For example, vectors 720 and 721 may be used to align sector grid lines 730 that form sectors 701 through 710 of biometric information stored with the sensor.

Assuming that a scanned biometric has features that correspond to vectors 720 and 721 and thereby align sector grid lines 730, the sensor may select one or more sectors (e.g., sectors 701 through 710) for comparison of detected biometric features to vectors within the selected sectors. For example, the sensor may select sector 705 for comparison of detected biometric features to vectors 715 and 716. If the detected biometric features correspond to vectors 715 and 716, the sensor may authenticate the user thereof and generate an authentication code for use with the biometric authentication system.

If, however, the grid alignment vectors 720 and 721 do not align, a biometric feature comparison may not occur and determine that the user is not authorized to use the sensor. As such, the comparison of detected biometric features to vectors 715 and 716 may serve as a backup to user registration. For example, if a detected biometric has features that correspond to grid alignment vectors 720 and 721 and thereby align grid lines 730 for sectorization, the sensor may still require vectors 715 and 716 to correspond to detected biometric features before the user may be registered.

Turning now to Figure 11, sector 705 is shown in a grid (i.e., grid lines 730 of Figure 7) bound by x-axis 801 and y-axis 802 to illustrate how code generation may proceed. In this embodiment, vectors, such as vectors 715 and 716, are selected for code generation and then assigned a code by assigning binary values to the grid. For example, the majority of vector 715 lies within the grid value of 010 on y-axis 802 and grid value 011 on x-axis 801. The two grid values of vector 715 may be combined as a six bit code component and, therefore, be assigned a value of 010011. Similarly, the majority of vector 716 lies within the grid value of 100 of y-axis 802 and 011 of x-axis 801. As such, a code for vector 716 may be assigned a value of 100011.

The codes for vectors 715 and 716 may be combined or arranged to generate an overall code as a matter of design choice. For example, the values of vector 715 and 716 may be modulo 2 summed to provide a code of 110000 or the two codes may be place side-by-side to form a 12 bit code (e.g., 010011100011). Additionally, a generated code may be combined with other information, such as a serial number of a biometric device. For example, the codes for vectors 715 and 716 as exemplified herein may have decimal values of 19 and 35, respectively, and thus a summed value of 54. This summed value may be added to a serial number of a biometric device and used as a code for the biometric authentication system. For example, the summed value of 54 may be added to a number that that is unique to the device using decimal, binary, or hexadecimal addition techniques.

Code generation may also be performed when a user is not authorized use of the sensor. For example, the sensor may detect that the user is not authorized use of the sensor. The sensor may subsequently generate an alarm code unbeknownst to the person entering a biometric with the sensor. Upon using alarm code with a biometric authentication system, the biometric authentication system may alert responsible authorities for inquiry thereto.

Although not essential to such user registration and subsequent code generation, selection of the sectors and/or the biometric features may be random or performed according to a predetermined sequence as an additional security measure. For example, the sensor, upon aligning grid lines 730, may randomly select one or more sectors 701 through 710. The sensor may then compare one or more vectors thereof to detected biometric features for user registration. The sensor may also randomly select from those one or more vectors to generate the code. For example, the sensor may use values from

all or a portion of those vectors to generate the code. The invention, however, is not intended to be limited to a particular selection of vectors and/or sectors for code generation. For example, vectors used for user registration may differ from vectors used in code generation. Nor is the invention intended to be limited to a particular code length. For example, in one embodiment, the generated code may be 16 bits that comprises the vector information and/or the serial number information.

Transactional Embodiments Using Biometric Authentication

Turning now to the drawings, Figure 12 is a block diagram illustrating system 810 which is operable to perform transactions with mobile handset 811. In this embodiment, system 810 may operate to transact money and/or property with transaction processor 812 via mobile handset 811. For example, mobile handset 811 may be configured with an interface that communicatively couples to transaction processor 812 to receive a transaction description (e.g., price, goods, services, etc.). Processing of the transaction description initiates with the authentication of a user of the mobile handset. Once the user is authenticated, mobile handset 811 may transfer the transaction description to financial institution 816 so that the user may access account 819 (i.e., the user's account) to perform the transaction. In one embodiment, mobile handset 811 is a cell phone and the account number associated with account 819 is the phone number for the mobile handset.

Mobile handset 811 may use typical means of cellular telephony, such as GSM, CDMA, WCDMA, FTM, TDM, or combinations thereof. Other means of telephony may include RF communications, such as GPS. For example, mobile handset 811 may include a radiofrequency transceiver operable to employ such communication techniques to interface communications between authentication processor 814 and a mobile handset. Mobile handset 811 may, therefore, be operable to communicate to authentication processor 814 via antenna 834 and via communication link 813 as implemented by the cellular telephony described herein. In communicating with authentication processor 814, mobile handset 811 may transmit a code to authentication processor 814 to authenticate a user of the mobile handset so that access may be granted to account 819 maintained by financial institution 816.

Mobile handset 811 may configure the code for user authentication in a variety of manners. One exemplary manner includes using a biometric sensor that is configured with mobile handset 811 to detect the biometric of a user and compare the biometric to biometric information stored with mobile handset 811. If the detected biometric

corresponds to the stored biometric information, mobile handset 811 may generate a code for use by authentication processor 814 to either authenticate the user or grant immediate access to account 819. For example, once mobile handset 811 generates a code and transfers it to authentication processor 814, authentication processor 814 may receive the code and compare it to another code stored with the authentication processor. If the received code corresponds to the stored code, authentication processor 814 may generate an authentication indicator for financial institution 16 to grant access to account 819. Alternatively, based on a valid comparison of the received code to the stored code, authentication processor 814 may grant direct access to account 819. As such, authentication processor 814 and financial institution 816 may be located or at least communicatively linked as a single entity 815. In either case, mobile handset 811 may generate the code based on, for example, a serial number of the mobile handset, a phone number of the mobile handset, the stored biometric information, various encryption standards (e.g., the Advanced Encryption Standard, "AES") and/or using the techniques described hereinabove (e.g., as in Figures 10 and 11).

In an alternative embodiment, mobile handset 811 may include a biometric sensor that detects the biometric of the user and converts the detected biometric to digital biometric information which may be used by authentication processor 814 to authenticate the user. For example, authentication processor 814 may receive encoded biometric information from mobile handset 811 and decode the biometric information for comparison to biometric information stored with authentication processor 814. The digital biometric information may be configured with or encoded by information such as a serial number of the mobile handset, a phone number of the mobile handset and/or various encryption standards (e.g., AES).

In either of the above-mentioned embodiments, the sensor may be configured to detect a variety of user biometrics. For example, the sensor may be configured to detect retinal information, fingerprint information, ocular information, DNA, veinal information, arterial information, voice information, and/or pulmonary information.

In yet another embodiment, mobile handset 811 may be operable to generate a code based on a user's entry with a keypad configured with the mobile handset. For example, a user may enter a series of numbers using the keypad of mobile handset 811 when a transaction is desired. Mobile handset 811 may use the series of numbers to either generate a code for use by authentication processor 814 or transfer the series of

numbers directly to authentication processor 814 for authentication of the user. In such an embodiment, authentication processor 811 may compare a received code to a code stored with the authentication processor to authenticate the user. If the received code corresponds to the stored code, authentication processor 814 may either grant direct access to account 819 or indicate the authentication of the user to financial institution 816 (e.g., via an authentication indicator).

Once the user is authenticated and granted access to account 819, financial institution 816 may review the transaction description and verify that account 819 is capable of fulfilling the transaction description (e.g., verify that sufficient monetary funds exist). If account 819 is capable of fulfilling the transaction description, financial institution 816 may perform the transaction with a financial institution of transaction processor 812. For example, transaction processor 812 may be associated with account 820 of financial institution 818. If account 819 has sufficient monetary funds to fulfill the transaction description, financial institution 816 will withdraw the necessary monetary funds and transfer them to account 820 of financial institution 818. Those skilled in the art, however, should readily recognize that the invention is not intended to be limited to a financial transaction between two financial institutions. For example, transaction processor 812 may be associated with the same financial institution as the user of mobile handset 811 (i.e., financial institution 816). Accordingly, financial institution 816 may simply transfer funds from the mobile handset user's account (i.e., account 819) to the transaction processor's account (i.e., account 820).

Upon completion of the transaction (e.g., when monetary funds are transferred from account 819 to account 820), financial institution 818 may indicate to transaction processor 812 that the transaction is complete. Similarly, financial institution 816 may indicate to mobile handset 811 via authentication processor 814 that the transaction is complete. Mobile handset 811 may then process and retain information pertaining to the transaction so that the mobile handset user may have an accessible record of the transaction. For example, mobile handset 811 may maintain a sortable record of all transactions made by the user of mobile handset 811.

Figure 13 is a block diagram of authentication processor 814 used in system 810 of Figure 12. In this embodiment, authentication processor 814 may perform in a manner that is similar to authentication processor 101 of Figures 1 and 3. Authentication processor 814 includes interface 821 that is configured to receive an authentication code

(e.g., the codes and/or biometric information described above in Figure 12) such that the user of mobile handset 811 may be granted access to an account (e.g., account 819 of Figure 12) upon authentication of the user. Additionally, interface 821 may also receive the transaction description as provided by mobile handset 811. Authentication processor 814 may thereby transfer the transaction description to the financial institution upon authentication of the user of mobile handset 811.

In this embodiment, interface 821 is communicatively coupled to comparator 822 to convey a received authentication code to the comparator. Comparator 822 may compare the received authentication code to stored authentication codes $826_{1...N}$ (wherein N is an integer greater than one). If the received authentication code corresponds to (e.g., matches) a stored authentication code 826, comparator 822 may authenticate the user of mobile handset 811.

Authentication processor 814 may include storage 825 that stores a plurality of pre-generated authentication codes $826_{1...N}$. Comparator 822 may compare the received authentication code to one or more of the pre-generated authentication codes $826_{1...N}$ to verify that the received authentication code matches one of the pre-generated authentication codes within a predefined range. If the received authentication code matches the first compared pre-generated authentication code 826_1, comparator 822 simply authenticates the user of mobile handset 811 and conveys such to authenticator 823. If the received authentication code matches one of the other pre-generated authentication codes (e.g. codes $826_{2...N}$), comparator 822 may indicate to mobile handset 811 via interface 821 that a code generator of the mobile handset is not synchronous with the codes stored in storage 825. In such an embodiment, mobile handset 811 may then resynchronize its code generator to correspond with a code generator of authentication processor 814. Such synchronization is shown and described hereinabove.

Upon authentication by comparator 822, authenticator 823 generates an authentication indicator for transfer to a processing entity via interface 824 (e.g., financial institution 816 of Figure 12 or processing entity 841 described hereinbelow). For example, the authentication indicator may include a user's account number, phone number, or other information useful to a financial entity. A processing entity may use the authentication indicator to grant access to an account as described hereinabove since the user of mobile handset 811 has been authenticated. For example, the processing entity

may grant a user access to the user's account because the processing entity is reasonably assured of the user's identity.

Those skilled in the art should readily recognize that authentication processor 814 is not intended to be limited to the configuration shown and described herein. For example, authentication processor 814 may be configured in other ways as a matter of design choice to implement the various aspects and features described herein. Additionally, those skilled in the art should readily recognize that authentication processor 814 may be configured from a variety of components that may include software, firmware, hardware, or combinations thereof. For example, interface 821 may be a standard hardware telephony interface configured for communicatively coupling to a Plain Old Telephone Service ("POTS"). Alternatively, interface 811 may be an Internet connection. Other components of authentication processor 814, such as comparator 822 and authenticator 823, may be implemented with a general-purpose processor operable to carry out the various aspects and features described herein when directed by software instructions. For example, software instructions may be configured to direct authentication processor 814 to access storage 825 and compare authentication codes 826 to an authentication code receive via interface 821. Examples of storage 825 include computer readable media, such as random access memory ("RAM"), disk drives, magnetic tapes, etc.

Figure 14 illustrates an example of mobile handset 811. In this embodiment, mobile handset 811 is configured as a cell phone operable to convey data and/or voice via RF telephony techniques such as GSM, CDMA, WCDMA, FTM, TDM, or combinations thereof. For example, mobile handset 811 may communicate with authentication processor 814 via communication link 813. Communication link 813 may be representative of a telephony network that employs one or more of the above-mentioned RF telephony techniques.

Mobile handset 811 may include interface 834 to communicatively couple to transaction processor 812. For example, mobile handset 811 may receive a transaction description from transaction processor 812 via interface 834. Some examples that may be used to implement interface 834 include a serial interface, a parallel interface, a FireWire interface, an Ethernet interface, an infrared interface, an RF interface, or an optical interface. The invention, however, is not intended to be limited any of the exemplary interfaces described herein.

In one embodiment, mobile handset 811 includes biometric sensor 835 to detect a mobile handset user's biometric and authenticate the user. For example, biometric sensor 835 may detect a user's biometric for comparison to biometric information stored with mobile handset 11 as described hereinabove. Accordingly, mobile handset 811 may include storage element 836 that stores biometric information of the user. An example of storage element 836 may include nonvolatile RAM, or "NVRAM", that is only accessed by comparator 831 such that the user's biometric information is not compromised.

Comparator 831 is operable to access storage element 836 to retrieve stored biometric information for comparison to the user's biometric as detected by biometric sensor 835. In one embodiment, comparator 831 generates an authentication indicator when the user's detected biometric corresponds to the stored biometric information within storage element 836. Comparator 831 may then transfer the authentication indicator to code generator 832 so that an authentication code may be generated. For example, code generator 832 may generate the code in accordance with the code generation described hereinabove (e.g., using a serial number of mobile handset 811, a phone number of mobile handset 811, the user's biometric information, encryption techniques, or various combinations thereof) in response to receiving an authentication indicator from comparator 831.

Alternatively, comparator 831 may compare the detected user biometric to the stored biometric information and transfer an authentication indicator directly to authentication processor 814 and/or financial institution 816. For example, the authentication indicator as generated by comparator 831 may be sufficient to authenticate the user of mobile handset 811. As such, the authentication indicator may be transferred to financial institution 816 to grant access to account 819. Alternatively, the authentication indicator may include the user's biometric information which may be transferred to authentication processor 814 for additional authentication.

In one embodiment, mobile handset 811 may be configured to directly generate an authentication code. For example, a user may enter an authentication code using the keypad 837 of mobile handset 811. Mobile handset 811 may thereby transfer the entered authentication code to authentication processor 814 for authentication of the user of mobile handset 811, as described hereinabove. Alternatively, the user may enter an authentication code from which code generator 32 encodes prior to transfer to authentication processor 814.

To assist in performing various transactions, mobile handset 811 may be configured with menu 833. Menu 833 may be displayed with display unit 832 of mobile handset 811. For example, mobile handset 811 may be configured with software components which the mobile handset processes to display menu 833 with display unit 832. Menu 833 may include information such as a transaction identification number, the user's financial institution(s), the user's credit account(s), chronological listing of past transactions, balance information within an account, etc. This information may be only available to a user of mobile handset 811 upon the user's authentication. For example, once authentication processor 814 authenticates the user and indicates such to financial institution 816, the financial institution may transfer account information to mobile handset 811 for selectable display with display unit 832.

Figure 15 is a block diagram of system 840 operable to perform transactions. In this embodiment, mobile handset 811 is configured for communicatively coupling to transaction processor 812 to receive a transaction description from transaction processor 812. The transaction description may indicate an exchange of property and/or services between the user of mobile handset 811 and transaction processor 812. For example, transaction processor 812 may be communicatively coupled to processing entity 841 to direct processing entity 841 to release property to the user of mobile handset 811 upon authentication of the user. In such an embodiment, processing entity 841 may operate as an escrow entity that holds property for another. Alternatively, processing entity 841 may operate as a personnel processor. For example, processing entity 841 may be a jail or some other form of detention center that necessitates authentication of an escort before personnel can be handed over to the escort.

Mobile handset 811 may communicate to authentication processor 814 via RF telephony techniques such as those described hereinabove to communicate through a telephony network. Mobile handset 811 may transfer or various authentication information as described hereinabove to authentication processor 814 for authentication of the user of mobile handset 811. Once authentication processor 814 authenticates the user, the authentication processor may indicate such to processing entity 841 for processing a transaction between the user of mobile handset 811 and transaction processor 812. Processing entity 841 may receive an authentication indicator as well as the transaction description from authentication processor 814 and process the transaction of the transaction description based on the authentication indicator.

Figure 16 is a block diagram of system 850 operable to perform transactions. In this embodiment, a transaction is performed between two mobile handsets (i.e., mobile handset 811 and mobile handset 851). For example, mobile handset 851 may convey a transaction description to mobile handset 811. Such conveyance may be performed in a variety of manners subject to design choice that include for example wireline couplings (e.g., serial cable, FireWire, etc.), infrared communications, optical communications, or RF communications. Mobile handset 811 initiates authentication of a user of the mobile handset such that the transaction of the transaction description may be performed.

Authentication of the user may be performed using mobile handset 811 and/or authentication processor 814 as described hereinabove. Once the user is authenticated, mobile handset 811 may transfer the transaction description to processing entity 841 (i.e., via telephony network 842 and authentication processor 814) to perform the transaction. For example, processing entity 841 may be configured to receive transaction information from mobile handset 811 and process the transaction information to perform a transaction between the users of mobile handset 811 and mobile handset 851.

Similar to the authentication of mobile handset 811, mobile handset 851 may also communicate to an authentication processor to authenticate the user of mobile handset 851. For example, mobile handset 851 may operate in a manner similar to that of mobile handset 811 as described in Figure 14. In doing so, mobile handset 851 may communicate to authentication processor 854 via telephony network 852 by, for example, transferring an authentication code to authentication processor 854. Authentication processor 854 may then compare the authentication code to one or more authentication codes stored therewith. Once the user of mobile handset 851 is authenticated by authentication processor 854, the authentication processor may transfer an authentication indicator to processing entity 841 to enable processing of the transaction between mobile handset 811 and mobile handset 851.

Although mobile handset 851 is described with respect to generating a code, those skilled in the art should readily recognize that system 850 may be implemented with any of the embodiments described hereinabove or their combinations. For example, mobile handset 811 may be configured to sense a user's biometric and generate a code to authenticate the user via authentication processor 814 while mobile handset 851 is configured to allow a user to enter an authentication code via a keypad of mobile handset 851 for authentication of its user via authentication processor 854. Additionally, the

transaction information may be transferred from mobile handset 811 to mobile handset 851. Accordingly, system 850 is not intended to be limited to any one particular embodiment described herein.

Additionally, processing entity 841 may be configured from a general-purpose computer that connects to authentication processors 814 and 854 using standard communication techniques, such as the Internet. Accordingly, processing entity 841 may process software instructions operable to perform transactions between mobile handset 811 and mobile handset 851, regardless of the manner in which authentication of their respective users is achieved. For example, regardless of the manner in which authentication processor 814 and authentication processor 854 authenticates their respective users, each authentication processor may transfer and authentication indicator to processing entity 841. Processing entity 841 may compare the authentication indicators to one another, or to other authentication indicators, to validate a transaction between the users of the two mobile handsets.

Figure 17 is a flowchart illustrating process 870 for performing transactions. In this embodiment, process 870 initiates once a user registers a biometric with a mobile handset to generate an authentication code, in process element 871. For example, a user of mobile handset 811 may scan a biometric (e.g., a fingerprint) across a sensor (e.g., sensor 835 of Figure 14) configured with the mobile handset, in process element 872. The sensor may detect the user's biometric for comparison to biometric information stored with the mobile handset, in process element 873. A determination may then be made as to whether the biometric corresponds to the stored biometric information, in process element 874. If the biometric does correspond to the stored biometric information, the mobile handset may generate an authentication code, in process element 876. If, however, the biometric does not correspond to the stored biometric information, process 870 may end in process element 875, potentially requiring a user of the mobile handset to reenter the biometric.

If mobile handset 811 generates an authentication code in process element 876, mobile handset 811 may transfer the authentication code to an authentication processor, such as authentication processor 814 described hereinabove. Mobile handset 811 may transfer the authentication code to the authentication processor via RF telephony, in process element 878. Once the authentication processor receives the authentication code,

the authentication processor may retrieve one or more authentication codes from storage for comparison to the received authentication code, in process element 879.

Process 870 may generate an authentication indicator based on a comparison of the stored authentication code to the received authentication code, in process element 880. For example, the authentication processor may include a comparator that is used to compare one or more authentication codes stored within the storage element of the authentication processor. A comparator may compare these one or more authentication codes to the received authentication code to determine if the received authentication code corresponds to one of the stored authentication codes. A plurality of the authentication codes may be used for synchronization purposes, as described hereinabove. If the received authentication code matches one of the stored authentication codes, the authentication processor may generate an authentication indicator.

Authentication indicator may be used to indicate the authenticity of a user of the mobile handset. For example, a financial entity may use the authentication indicator to verify that the user of a mobile handset has been authenticated. A financial entity may therefore grant access to the user's account such that the user may perform a transaction. As such, the authentication processor may transfer the authentication indicator to a financial entity, such as financial institution 816 of Figure 12, in process element 881. Additionally, a financial entity may grant access to the user's account when the biometric is authenticated, in process element 882.

Although described with respect to registering a biometric with the mobile handset and having the mobile handset generate a code used for authentication of the user by an authentication processor, those skilled in the art should readily recognize that the invention is not intended to be limited to such an exemplary embodiment. For example, other embodiments, such as those described below in Figures 15 and 16, may implement authentication in other manners that are typically subject to design choice. To illustrate, code generation as described in process element 876 may be obviated should design specifications require authentication only through the detection of the user's biometric and subsequent comparison to biometric information stored within the mobile handset. In such an embodiment, a simple authentication indicator may be generated and transferred from the mobile handset directly to the financial entity to grant access to the user's account. Accordingly, such embodiments may also fall within the scope and spirit of the invention.

Figure 18 is a flowchart illustrating process 890 for performing transactions. In this embodiment, a user of a mobile handset (e.g., mobile handset 811) may register a biometric with the mobile handset to generate a code, in process element 891. For example, a user of mobile handset 811 may scan a biometric (e.g., a fingerprint) across a sensor (e.g., sensor 835 of Figure 14) configured with the mobile handset. The sensor may detect the user's biometric in process element 891 and generate a code therefrom in process element 893.

The generated code may be transferred from the mobile handset via RF telephony to an authentication processor to authenticate the biometric of the user, in process element 894. The code that is generated may be configured in a variety of manners that include a phone number associated with a mobile handset, a serial number of the mobile handset, digital biometric information of the user, and/or various encryption techniques, such as the AES. The authentication processor may retrieve one or more stored authentication codes, in process element 895, for comparison to the received code as generated by the mobile handset. For example, the authentication processor may compare the received code to one or more stored authentication codes to determine whether the two codes correspond to one another, in process element 896. If the codes do not correspond, the user is not authenticated and process 890 ends in process element 897. If, however, the two codes do correspond, the authentication processor may generate an authentication indicator based on the comparison of the two codes, in process element 898.

Once the authentication indicator is generated, the authentication processor may transfer the authentication indicator to a financial entity or other processing entity, in process element 899. The financial entity may grant access to a user's account when the biometric is authenticated to perform the transaction, in process element 900. For example, the financial entity may process the authentication indicator to determine that the user's biometric has been authenticated. As such, the financial entity may determine that the user may be granted access to the user's account to perform a transaction between the mobile handset and, e.g., a transaction processor such as transaction processor 812 of Figure 15.

Figure 19 is a flowchart illustrating process 910 for performing transactions. In this embodiment, a user of a mobile handset may enter a code with the mobile handset using a keypad configured therewith, in process element 911. For example, the user may enter a series of numbers using the keypad of the mobile handset. The mobile handset

may transfer the entered series of numbers to an authentication processor, such as authentication processor 814 described hereinabove, in process element 912.

The authentication processor may retrieve one or more stored authentication codes for comparison to the received code, in process element 913. The authentication processor may then compare the received code to the one or more stored authentication codes to determine whether the received code corresponds to one of the stored authentication codes, in process element 914. If the received code does not correspond to one of the stored authentication codes, process 910 ends in process element 915. If, however, the received code does correspond to one of the authentication codes, the authentication processor may generate an authentication indicator, in process element 916.

The authentication processor may transfer the authentication indicator to a financial entity, such as financial institution 816 of Figure 12, or some other processing entity, such as processing entity 841 of Figure 15, in process element 917. Based on that authentication indicator, the financial entity may grant access to a user's account because the user's identity has been authenticated, in process element 918. As such, the user may perform the transaction.

Although discussed with respect to entering a code with the keypad of a mobile handset and transferring that code to an authentication processor, the invention is not intended to be limited to such an embodiment. For example, a user may enter a first code into the mobile handset for the mobile handset to authenticate a user. The mobile handset may subsequently generate a second code for transfer to the authentication processor. Generating a second code may include encrypting the first code or even generating a completely unique second code in response to the authenticated first code. Such generation of a second code may prove advantageous because, among other reasons, the first code may be more securely transferred to the authentication processor or even the processing entity, thereby minimizing the exposure of the first code to unintended viewers. Accordingly, the invention is not intended to be limited to the exemplary embodiment shown and described herein.

Figure 20 illustrates an embodiment in which user 1001 uses a personal biometric device 1002 to gain access to an entrance 1003. In this embodiment, personal biometric device 1002 is configured with Bluetooth communications that enable the personal biometric device to communicate with a Bluetooth enabled entrance access control 1005

and subsequently gain access to entrance 1003. For example, user 1001 may swipe a finger with a sensor configured with personal biometric device 1002. Personal biometric device 1002 may detect a fingerprint of user 1001 and determine whether the user is authorized use of the personal biometric device.

Upon authentication of user 1001, personal biometric device 1002 may transfer the Personal Identification Number (PIN) of the personal biometric device to entrance access control 1005. In this regard, personal biometric device 1002 may communicate the PIN to Bluetooth receiver 1006 of entrance access control 1005 via Bluetooth communications link 1004 (i.e., via radio frequency transmission, or RF). Entrance access control 1005 may subsequently grant access to user 1001 to entrance 1003 upon Bluetooth linkage between personal biometric device 1002 and the entrance access control.

Generally, the Bluetooth RF physical layer operates in the unlicensed ISM band at 2.4GHz. It employs a frequency hop transceiver to combat interference and fading, and provides many FHSS carriers. RF operation uses a shaped, binary frequency modulation to minimize transceiver complexity. The symbol rate is 1 Megasymbol per second (Msps) supporting the bit rate of 1 Megabit per second (Mbps) or, with Enhanced Data Rate, a gross air bit rate of 2 or 3Mbps.

During typical operation, a physical radio channel is shared by personal biometric device 1002 and entrance access control 1005. Personal biometric device 1002 and entrance access control 1005 then become synchronized to a common clock and frequency hopping pattern. One entrance access control 1005 provides a synchronization reference, it is known as the master device. Personal biometric device 1002 thereby becomes a slave device and the master and slave devices together form a piconet via the fundamental form of communication for Bluetooth wireless technology.

Devices in a piconet use a specific frequency hopping pattern which is algorithmically determined by certain fields in the Bluetooth specification address and clock of the master. The basic hopping pattern is a pseudo-random ordering of the 79 frequencies in the ISM band. The hopping pattern may be adapted to exclude a portion of the frequencies that are used by interfering devices. The adaptive hopping technique improves Bluetooth technology co-existence with static (non-hopping) ISM systems when these are co-located.

The physical channel is sub-divided into time units known as slots. Data is transmitted between Bluetooth enabled devices in packets that are positioned in these slots. When circumstances permit, a number of consecutive slots may be allocated to a single packet. Frequency hopping takes place between the transmission or reception of packets. Bluetooth technology provides the effect of full duplex transmission through the use of a Time-Division Duplex (TDD) scheme.

A layering of links and channels and associated control protocols resides above the physical channel. The hierarchy of channels and links from the physical channel upwards includes a physical channel, a physical link, a logical transport, a logical link and an L2CAP channel. Within the physical channel, the physical link is formed between any two devices that transmit packets in either direction between them. In a piconet physical channel, there are restrictions on which devices may form a physical link. There is a physical link between each slave device and the master device. Physical links are generally not formed directly between slave devices in a piconet.

The physical link is used as a transport for one or more logical links that support unicast synchronous, asynchronous and isochronous traffic, and broadcast traffic. Traffic on logical links is multiplexed onto the physical link by occupying slots assigned by a scheduling function in the resource manager.

A control protocol for the baseband and physical layers is carried over logical links in addition to user data. This is the Link Manager Protocol (LMP) and devices that are active in a piconet have a default asynchronous connection-oriented logical transport that is used to transport the LMP protocol signaling. For historical reasons this is known as the ACL logical transport. The default ACL logical transport is created whenever a device joins a piconet. Additional logical transports may be created to transport synchronous data streams when required.

The link manager function uses LMP to control the operation of devices in the piconet and provide services to manage the lower architectural layers (radio frequency layer and baseband layer). The LMP protocol is carried on the default ACL logical transport and the default broadcast logical transport.

Above the baseband layer, the L2CAP layer provides a channel-based abstraction to applications and services. It carries out segmentation and reassembly of application data and multiplexing and de-multiplexing of multiple channels over a shared logical link. L2CAP has a protocol control channel that is carried over the default ACL logical

transport. Application data submitted to the L2CAP protocol may be carried on any logical link that supports the L2CAP protocol.

The Bluetooth PIN of personal biometric device 1002 is generally registered with entrance access control 1005 prior to linkage between the personal biometric device and the entrance access control. For example, entrance access control 1005 may include a list of Bluetooth PINs of all users that are authorized access to entrance 1003. Accordingly, once personal biometric device 1002 links with entrance access control 1005, entrance access control 1005 may simply compare the Bluetooth PIN of the personal biometric device to a list of Bluetooth pins stored with the entrance access control to verify if the PIN is authorized access.

In one embodiment, personal biometric device 1002 scans user 1001's fingerprint in sectors as described above in Figures 10 and 11. Accordingly, personal biometric device 1002 may be configured to generate multiple Bluetooth pins that may be used for other purposes, such as alarm generation. For example, when an unauthorized person uses personal biometric device 1002, the personal biometric device 1002 may generate a Bluetooth PIN that is registered with entrance access control 1005 as a type of alarm PIN. As such, entrance access control 1005 may generate an alarm and/or entice the unauthorized user into a situation that allows for securing the individual. Examples of such code generation are shown and described below in Figure 21.

In addition to the advantages of a user maintaining his or her personal biometric information as described hereinabove, entrance access control 1005 may advantageously offload processing onto personal biometric device 1002. For example, biometric processing can be processor intensive, particularly when that processing includes comparing a biometric to other biometrics (e.g., as with entrance access controls configured with biometric sensors). In some instances, the number of biometrics that may be compared are in the thousands. By enabling personal biometric sensor 1002 to perform such individualized biometric comparisons, entrance access control 1005's processing may be relegated to simply processing less intensive authentication codes.

In one embodiment, entrance access control 1005 is a touchStar access control, device model number 1800, produced by touchStar Inc. Those skilled in the art, however, should readily recognize that the invention is not intended to be limited to a particular type of access control device. Rather, personal biometric device 1002 may communicate with other Bluetooth enabled devices that require such user authentication.

Figure 21 illustrates an exemplary block diagram of personal biometric device 1002 as used in Figure 20. Personal biometric device 1002 is configured with sensor 1010 to read a user's biometric (e.g., any of those biometrics described hereinabove). The input biometric may be compared to stored biometric information 1012 by way of comparator 1011. If comparator 1011 determines that the input biometric of sensor 1010 corresponds to the stored biometric information 1012, comparator 1011 may trigger code generator 1013 to generate a code for summation with Bluetooth PIN 1014. For example, code generator 1013 may generate a code of all zeros that modulo 2 sums with Bluetooth PIN 1014 via summation module 1017. As such, Bluetooth PIN 1014 may be transferred to Bluetooth RF interface 1015 for communication to a Bluetooth enabled device, such as entrance access control 1005 of Figure 20.

If comparator 1011 determines that the input biometric of sensor 1010 does not correspond to the stored biometric information 1012, code generator 1013 may generate a code that, when summed with Bluetooth PIN 1014 via summation module 1017, registers as an alarm generation code. For example, if Bluetooth PIN 1014 is a four digit PIN of 1234, that PIN may be represented as a binary string of 0001001000110010. An alarm generation code of entrance access control 1005 may be preconfigured, e.g., as 1111000011110000. If the input biometric does not correspond to the stored biometric information 1012, code generator 1013 may generate code of 11100010111000100 that modulo 2 sums with the Bluetooth PIN of 0001001000110010 to generate the alarm code. Accordingly, when the alarm generation code registers with entrance access control 1005, the entrance access control may deny access and/or alert the responsible authorities.

While one embodiment has been shown and described herein, those skilled in the art should readily recognize that the invention is not intended to be limited to the illustrated embodiment. For example, personal biometric device 1002 may be configured to simply grant or deny access with entrance access control 1005. That is, if an input biometric does not correspond to stored biometric information, personal biometric device 1002 may not transfer the Bluetooth PIN 1014. Alternatively, personal biometric device may simply prevent Bluetooth linkage with entrance access control 1005. If, however, the input biometric does correspond with the stored biometric information 1014, personal biometric device may link with entrance access control 1005 and transfer Bluetooth PIN 1014. Additionally, those skilled in the art should readily recognize that the invention is

not intended to be limited to the code generation described herein. Rather, other types of code generation may be implemented as a matter of design choice.

While the invention has been illustrated and described in detail in the drawings and foregoing description, such illustration and description is to be considered as exemplary and not restrictive in character. Accordingly, it should be understood that only the preferred embodiment and minor variants thereof have been shown and described and that all changes and modifications that come within the spirit of the invention are desired to be protected.

CLAIMS

What is claimed is:

Basic Biometric System Authentication Claims

1. An authentication system, including:

a sensor for sensing a biometric and for providing a first code in response to sensing the biometric; and

a processor for evaluating the first code to authenticate a user of the sensor independent of said sensor sensing the biometric.

2. The authentication system of claim 1, wherein the biometric is one or more of a group consisting of: retinal information; fingerprint information; ocular information; DNA; veinal information; arterial information; voice information; and pulmonary information.

3. The authentication system of claim 1, wherein the processor includes a code generator to generate a second code for evaluating the first code.

4. The authentication system of claim 3, wherein the processor further includes a comparator for comparing the first code and the second code to authenticate the user.

5. The authentication system of claim 3, wherein the sensor includes a code generator synchronizable with the code generator of the processor.

6. The authentication system of claim 3, wherein the code generator of the processor is a random number generator.

7. The authentication system of claim 1, wherein the processor includes an Internet access link configured for allowing a user to establish an account with the authentication system.

8. The authentication system of claim 6, wherein the account is devoid of a user's biometric.

9. The authentication system of claim 6, wherein the Internet access link includes an Internet server configured for maintaining software used to establish the account.

10. The authentication system of claim 9, wherein the Internet access link further includes a database configured for storing a plurality of accounts.

11. The authentication system of claim 1, further including an input unit for receiving the first code and for granting access based on the first code.

12. The authentication system of claim 11, wherein the input unit is configured with the processor.

13. The authentication system of claim 11, wherein the input unit is configured independent of the processor.

14. The authentication system of claim 13, further including a communication link between the processor and the input unit for transferring an access indicator from the processor to the input unit.

15. The authentication system of claim 14, wherein the communication link is configurable with one or more of a group consisting of: a wide area network; a local area network; a wireless network; a public switching telephone network; and the Internet.

16. The authentication system of claim 11, wherein the access is to a financial account, a medical account, an entry, a computer, a means of transportation, or government information.

17. A method of authentication, including steps of:
using a biometric to generate a first code; and
authenticating a user based on the first code and independent of said step of using.

18. The method of claim 17, wherein the step of using a biometric includes a step of comparing the biometric with stored biometric information.

19. The method of claim 18, further including a step of generating the first code with a device used to store the biometric information.

20. The method of claim 19, wherein the step of generating the first code includes a step of generating a random number based on a comparison of the biometric and the stored biometric information.

21. The method of claim 18, wherein the stored biometric information is one or more of a group consisting of: retinal information; fingerprint information; ocular information; DNA; veinal information; arterial information; voice information; and pulmonary information.

22. The method of claim 18, wherein the device is a portable device.

23. The method of claim 17, wherein said step of authenticating a user includes a step of generating a second code.

24. The method of claim 23, further including a step of granting a user access based on a comparison of the first code and the second code.

25. The method of claim 23, further including a step of entering the first code with an input device.

26. The method of claim 24, wherein the steps of entering the first code and generating a second code are collocated steps.

27. The method of claim 24, wherein the step of granting a user access includes a step of generating an access indicator for the input device.

28. The method of claim 28, wherein the step of granting a user access further includes a step of transferring the access indicator to an access point where the user is located.

29. The method of claim 27, wherein the step of transferring the access indicator includes a step of conveying the access indicator through a network, wherein the network is one or more of a group consisting of: wide area network; a local area network; a wireless network; a public switching telephone network; and the Internet.

30. The method of claim 25, further including a step of transferring the first code from the input device to a processor for comparison of the first code and the second code.

31. A system of authentication, including:

means for using a biometric to generate a first code; and

means for authenticating a user based on the first code and independent of said means for using.

32. The system of claim 31, wherein the means for using a biometric includes means for comparing the biometric with stored biometric information.

33. The system of claim 32, further including means for generating the first code with a device used to store the biometric information.

34. The system of claim 33, wherein the means for generating the first code includes means for generating a random number based on a comparison of the biometric and the stored biometric information.

35. The method of claim 32, wherein the stored biometric information is one or more of a group consisting of: retinal information; fingerprint information; ocular information; DNA; veinal information; arterial information; voice information; and pulmonary information.

36. The system of claim 32, wherein the device is a portable device.

37. The system of claim 31, wherein said means for authenticating a user includes means for generating a second code.

38. The system of claim 37, further including means for granting a user access based on a comparison of the first code and the second code.

39. The method of claim 37, further including means for entering the first code with an input device.

40. The system of claim 38, wherein the means for entering the first code and for generating a second code are collocated.

41. The system of claim 38, wherein the means for granting a user access includes means for generating an access indicator for the input device.

42. The system of claim 41, wherein the means for granting a user access further includes means for transferring the access indicator to an access point where the user is located.

43. The system of claim 42, wherein the means for transferring the access indicator includes means for conveying the access indicator through a network, wherein the network is one or more of a group consisting of: wide area network; a local area network; a wireless network; a public switching telephone network; and the Internet.

44. The system of claim 39, further including means for transferring the first code from the input device to a processor for comparison of the first code and the second code.

45. A biometric authentication system, including:
personal means for sensing a biometric of a user;
means for determining a situation of the user based on a sensed biometric; and
means for generating an alarm message based on a determined situation of the user.

46. The biometric authentication system of claim 45, wherein the personal means for sensing a biometric of a user include a mobile biometric sensor.

47. The biometric authentication system of claim 46, wherein the mobile biometric sensor is a mobile handset.

48. The biometric authentication system of claim 46, wherein the mobile biometric sensor incorporates said means for determining a situation of the user.

49. The biometric authentication system of claim 45, wherein the personal means for sensing a biometric of a user include means for generating a code based on a sensed biometric.

50. The biometric authentication system of claim 49, further including a processor independent of the personal means for sensing that includes an interface configured for receiving a generated code from said means for generating a code.

51. The biometric authentication system of claim 50, wherein the processor includes a comparator configured for receiving the generated code for comparison to one or more stored codes to determine a situation of the user.

52. The biometric authentication system of claim 51, wherein the processor includes the means for generating an alarm message based on a determined situation of the user.

53. The biometric authentication system of claim 52, wherein the determined situation includes a panic situation, an unauthorized use situation, or a combination thereof.

54. The biometric authentication system of claim 45, wherein the biometric is selected from a group consisting essentially of: retinal information; fingerprint information; ocular information; DNA; veinal information; arterial information; voice information; pulmonary information; and a combination thereof.

5

55. A method of authenticating a user with a biometric, including:
sensing a user biometric;
generating a code based on a sensed user biometric;
transferring the code to a processor for authentication; and
processing the code to determine a situation of the user.

56. The method of claim 55, further including comparing the user biometric to stored biometric information.

57. The method of claim 55, wherein processing the code includes determining authorization of the user.

58. The method of claim 57, further including generating alarm message upon determining when the user is unauthorized.

59. The method of claim 58, further including transferring the alarm message to an access point, a responsible authority, or a combination thereof.

60. The method of claim 55, wherein processing the code further includes determining a panic situation of the user.

61. The method of claim 60, further including generating alarm message upon determining when the user is in a panic situation.

62. The method of claim 61, further including transferring the alarm message to an access point, a responsible authority, or a combination thereof.

63. The method of claim 55, further including granting access to the user upon determination of a favorable situation of the user in response to processing the code.

64. A biometric authentication system, including:

a sensor that detects a biometric of a user to generate a code; and

an authentication processor that processes the code to determine a situation of the user.

65. The biometric authentication system of claim 64, wherein the situation includes a panic situation, an unauthorized use situation, or a combination thereof.

66. The biometric authentication system of claim 64, further including an access point that receives the code from the sensor and transfers the code to the authentication processor.

67. The biometric authentication system of claim 66, wherein the access point includes a communication interface that receives the code via radio frequency, telephony, keypad input, infrared transmission, electronic data transmission, or a combination thereof.

68. The biometric authentication system of claim 67, wherein the access point grants a user access to a financial account, an entry, a surety account, a medical account, a means of transportation, government information, a computer, or a combination thereof.

69. The biometric authentication system of claim 64, wherein the biometric is selected from a group consisting essentially of: retinal information; fingerprint information; ocular information; DNA; veinal information; arterial information; voice information; pulmonary information; and a combination thereof.

70. A system that performs a transaction, including:

a mobile handset that includes a biometric sensor, wherein the biometric sensor detects a biometric from a user of the mobile handset and wherein the mobile handset is associated with an account number; and

an authentication processor configured to receive an authentication code from the mobile handset, wherein the authentication processor uses the authentication code to authenticate the user and wherein the user is granted access to an account corresponding to the account number when the user is authenticated by the authentication processor.

71. The system of claim 70, wherein the account number is a phone number.

72. The system of claim 70, wherein the mobile handset includes a radio frequency interface that transmits the authentication code to the authentication processor.

73. The system of claim 72, wherein the mobile handset is configured to communicate via the radio frequency interface using a signaling technique selected from a group consisting essentially of: Global System for Mobile communications; Code Division Multiple Access; Wideband Code Division Multiple Access; Time Division Multiple Access; Global Positioning System; and Frequency Division Multiple Access.

74. The system of claim 72, wherein the authentication code includes biometric information of the user detected by the sensor.

75. The system of claim 70, wherein the mobile handset includes a storage element that stores biometric information of the user for comparison to a detected said biometric.

76. The system of claim 75, wherein the mobile handset further includes a comparator that compares stored said biometric information to the detected said biometric to generate an authentication indicator.

77. The system of claim 75, wherein the mobile handset further includes a code generator that generates the authentication code from the authentication indicator, the

stored said biometric information, the detected said biometric, the account number, a phone number associated with the mobile handset, a serial number of the mobile handset, or a combination thereof.

78. The system of claim 70, wherein the authentication processor includes an interface that receives the authentication code from the mobile handset.

79. The system of claim 78, wherein the interface is a telephony interface, an Internet connection, or a combination thereof.

80. The system of claim 70, wherein the authentication processor further includes a comparator that compares a received said authentication code to a stored authentication code to authenticate the user.

81. The system of claim 80, wherein the authentication processor further includes an authenticator communicatively coupled to the comparator to generate an authentication indicator when the user is authenticated by the comparator.

82. The system of claim 70, wherein the transaction is a financial transaction, a property transaction, a personnel transaction, or a combination thereof.

83. The system of claim 70, further including a first processing entity communicatively coupled to the authentication processor to grant access to the account when the user is authenticated by the authentication processor.

84. The system of claim 83, further including a second processing entity communicatively coupled to the first processing entity, wherein the first processing entity transfers money from the account to the second processing entity to perform the transaction for the user.

85. The system of claim 84, further including a transaction processor communicatively coupled to the mobile handset to transfer transaction information to the mobile handset.

86. The system of claim 85, wherein the transaction processor is communicatively coupled to the second processing entity, wherein the second processing entity transfers a transaction indicator to the transaction processor to indicate transaction performance.

87. The system of claim 83, further including a transaction processor communicatively coupled to the mobile handset to transfer transaction information to the mobile handset.

88. The system of claim 83, wherein the transaction processor is communicatively coupled to the first processing entity, wherein the first processing entity transfers a transaction indicator to the transaction processor to indicate transaction performance.

89. A method of performing a transaction, including:

registering a biometric with a mobile handset to generate a code;

transferring the code from the mobile handset to an authentication processor to authenticate the biometric; and

granting access to an account when the biometric is authenticated to perform a transaction.

90. The method of claim 70, wherein registering a biometric includes:

detecting the biometric with a sensor configured with the mobile handset.

91. The method of claim 71, wherein registering a biometric further includes:

comparing the biometric to stored biometric information; and

generating the code when the biometric corresponds to the stored biometric information.

92. The method of claim 71, wherein generating the code includes:

configuring the code from a phone number associated with the mobile handset, a serial number of the mobile handset, and detected biometric information, the stored biometric information, an account number, or a combination thereof.

93. The method of claim 70, wherein transferring the code includes:
configuring a radio frequency telephony signal with the code.

94. The method of claim 70, further including:
receiving the code with an interface of the authentication processor.

95. The method of claim 75, further including:
retrieving a stored authentication code for comparison to a received said code.

96. The method of claim 76, further including:
generating an authentication indicator based on the comparison of the stored authentication code to the received said code; and
transferring the authentication indicator to a financial entity.

97. The method of claim 77, wherein granting access to an account includes:
granting said access to said account based on the authentication indicator.

98. A system for performing a property transaction, including:
a mobile handset that includes a biometric sensor, wherein the biometric sensor compares a detected biometric to stored biometric information to generate an authentication code; and
an authentication processor configured to receive the authentication code from the mobile handset and compare the authentication code to a stored authentication code to grant access to a processing entity and perform a property transaction.

99. The system of claim 90, wherein the authentication processor includes an interface configured to receive the authentication code from the mobile handset.

100. The system of claim 71, wherein the mobile handset includes an interface that communicatively couples to the authentication processor to transfer the authentication code.

101. The system of claim 72, wherein the interface is a cellular telephony interface.

102. The system of claim 70, wherein the authentication processor includes a comparator that compares the authentication code to the stored authentication code to determine authenticity of a user of the mobile handset.

103. The system of claim 74, wherein the authentication processor further includes an authenticator communicatively coupled to the comparator to generate an authentication indicator when the user of the mobile handset is authenticated by the comparator.

104. The system of claim 75, wherein the authentication indicator includes a phone number associated with the mobile handset.

105. A mobile telephony handset, including:

a transceiver that communicatively links via a phone number;

a sensor that receives first biometric information; and

a processor that processes the first biometric information to perform a transaction using the phone number.

106. The mobile telephony handset of claim 70, further including a storage element that stores second biometric information.

107. The mobile telephony handset of claim 71, further including a comparator that compares said first biometric information to said second biometric information to authenticate a user such that the user may perform the transaction using the phone number.

108. The mobile telephony handset of claim 70, further including a communication interface that communicatively couples the mobile telephony handset to a transaction processor, wherein the transaction processor determines authorization of the transaction based on the phone number.

109. The mobile telephony handset of claim 73, wherein the communication interface provides for communications to the transaction processor via radio frequency, Internet, Ethernet, infrared, serial cable, parallel cable, or FireWire.

110. The mobile telephony handset of claim 70, wherein the transaction is a monetary transaction, a property transaction, a personnel transaction, or a combination thereof.

111. A communication device, including:

a sensor that receives biometric information;

a processor that processes received said biometric information to generate authentication information for use in a transaction; and

a transmitter that transfers the authentication information for external transaction authorization.

112. The device of claim 70, further including a comparator that compares stored biometric information to received said biometric information.

113. The device of claim 71, further including a storage element that stores said stored biometric information.

114. The device of claim 70, further including a communication interface coupled to the transmitter that communicatively couples the device to a transaction processor.

115. The device of claim 73, wherein the transaction processor is associated with a financial institution or a seller.

116. The device of claim 70, wherein the received said biometric information is not transferred for external transaction authorization.

117. The device of claim 70, wherein the authentication information includes a code.

118. The device of claim 76, wherein the code is synchronizeable based on a plurality of sensed biometric inputs.

119. The device of claim 76, wherein the authentication information is devoid of the biometric information.

120. The device of claim 76, wherein the authentication information includes a phone number and wherein the communication device is a mobile telephony handset.

121. The device of claim 79, wherein the mobile telephony handset is a cellular telephone that uses Global System for Mobile Communication, Code Division Multiple Access, Frequency Division Multiple Access, Time Division Multiple Access, or combinations thereof.

122. A method of performing a transaction, including steps of:

registering a biometric with a portable communication device to convert the biometric to electronic biometric information; and

with the portable communication device,

processing the electronic biometric information to authenticate a user, and

generating authentication information for a transaction when the user is authenticated.

123. The method of claim 70, wherein the step of registering a biometric includes a step of:

providing the biometric to an electronic sensor, wherein the biometric is selected from a group consisting of DNA, a follicle pattern, an veinal pattern, an arterial pattern, a cardio pattern, a fingerprint, a voice pattern, an aural pattern, a retinal pattern, a corneal pattern, and a skin pattern.

124. The method of claim 71, further including a step of:

electronically sensing the biometric to convert the biometric to the electronic biometric information.

125. The method of claim 70, wherein processing the electronic biometric information includes a step of:

comparing the electronic biometric information to biometric information stored with the portable communication device to determine whether the electronic biometric information corresponds to the biometric information stored with the portable communication device.

126. The method of claim 73, wherein processing the electronic biometric information further includes a step of:

generating a first indicator when the electronic biometric information corresponds to the biometric information stored with the portable communication device.

127. The method of claim 74, wherein the step of generating authentication information includes a step of:

formatting a phone number within the authentication information based on the first indicator.

128. The method of claim 75, wherein the authentication information is devoid of the electronic biometric information and the biometric information stored with the portable communication device.

129. The method of claim 75, wherein processing the electronic biometric information further includes a step of:

generating a second indicator when the electronic biometric information does not correspond to the biometric information stored with the portable communication device.

130. The method of claim 77, further including a step of:

using the second indicator to deny the transaction.

131. The method of claim 70, further including a step of:

transferring the authentication information to a transaction processor for authorization of the transaction.

132. The method of claim 79, wherein transferring the authentication information includes a step of:

communicatively coupling the portable communication device to the transaction processor via an interface that supports radio frequency communication, Internet communication, Ethernet communication, infrared communication, serial cable communication, parallel cable communication, or FireWire communication.

133. The method of claim 70, wherein the transaction is a financial transaction, a property transaction, a personnel transaction, or a combination thereof.

134. The method of claim 70, wherein the portable communication device is a cellular telephone.

135. A method of securing a transaction, including steps of:

authenticating a transaction party based on a biometric;

generating transaction information based on an authentication of the transaction party; and

transferring the transaction information to an external transaction processor.

136. The method of claim 70, further including a step of:

registering the biometric with a sensor that converts the biometric into electronic biometric information.

137. The method of claim 71, wherein the step of authenticating a transaction party includes a step of:

comparing electronic biometric information to stored biometric information to authenticate the transaction party.

138. The method of claim 72, further including a step of:

based on a comparison of the electronic biometric information to the stored biometric information, generating authentication information for use in generating the transaction information.

139. The method of claim 73, wherein the authentication information is devoid of biometric information.

140. The method of claim 70, wherein generating the transaction information includes a step of:

formatting the transaction information with a phone number for use by the external transaction processor in authorizing the transaction.

141. The method of claim 75, wherein generating the transaction information further includes a step of:

configuring the transaction information into a format transferable by radio frequency, Internet, Ethernet, infrared, serial cable, parallel cable, or FireWire.

142. The method of claim 70, wherein the external transaction processor is configured for performing a financial transaction, a property transaction, a personnel transaction, or a combination thereof.

143. A method of performing a transaction, including:

entering a code to a mobile handset using a keypad configured with the handset;

transferring the code from the mobile handset to an authentication processor to authenticate the code; and

granting access to an account when the code is authenticated to perform a transaction.

144. A system that authenticates a user, including:

a personal biometric device that reads a user's biometric to authenticate the user; and

an access control device that receives information pertaining to the user's authentication to grant the user access.

145. The system of claim 144, wherein the access includes entrance to a facility, entrance to a financial account, entrance to a computer, entrance to an area, entrance to a vehicle, entrance to a mobile device, or a combination thereof.

146. The system of claim 145, wherein the mobile device is a cell phone.

147. The system of claim 144, wherein the personal biometric device includes a sensor that detects the biometric of the user.

148. The system of claim 147, wherein the biometric is selected from a group consisting essentially of retinal information; fingerprint information; ocular information; DNA; veinal information; arterial information; voice information; pulmonary information; or a combination thereof

149. The system of claim 147, wherein the personal biometric device further includes a storage element that stores biometric information of the user

150. The system of claim 149, wherein the personal biometric device further includes a comparator that compares the detected biometric from the sensor to the stored biometric information.

151. The system of claim 149, wherein the stored biometric information includes sectorized biometric information.

152. The system of claim 149, wherein the personal biometric device further includes a processor that directs a comparison of one or more sectors of the stored biometric information.

153. The system of claim 152, wherein directing the comparison of the one or more sectors of the biometric information includes a random selection of the one or more sectors.

154. The system of claim 153, wherein directing the comparison of the one or more sectors of the biometric information includes a random selection of one or more features of the biometric information within at least one sector.

155. The system of claim 150, wherein the personal biometric device further includes a code generator that generates one or more codes based on comparison from the comparator.

156. The system of claim 155, wherein the one or more codes are selected from an alarm code, an authentication code, or a non authentication code.

157. The system of claim 144, wherein the personal biometric device includes a communication interface that communicates the information pertaining to the user's authentication to the access control device.

158. The system of claim 157, wherein the communication interface includes an RF interface.

159. The system of claim 158, wherein the RF interface is a Bluetooth interface.

160. The system of claim 155, wherein at least one of the one or more codes includes a Bluetooth personal identification number.

161. The system of claim 144, wherein the access control device includes a communication interface that receives the information pertaining to the user's authentication.

162. The system of claim 161, wherein the communication interface includes an RF interface.

163. The system of 162, wherein the RF interface is a Bluetooth interface.

164. The system of claim 144, wherein the access control device includes a processor that processes an authentication code from the personal biometric device to determine access for the user of the personal biometric device.

165. The system of claim 164, wherein the access control device includes a storage element that stores software instructions that direct the processor to compare the authentication code from the personal biometric device to a plurality of authentication codes maintained by the access control device to determine access for the user the personal biometric device.

166. The system of claim 144, further including an authentication processor communicatively coupled to the access control device to process a code transferred from the personal biometric device to the access control device and from the access control device to the authentication processor.

167. The system of claim 166, wherein the authentication processor includes a storage element that stores a plurality of codes associated with an account of the user of the biometric device.

168. The system of claim 167, wherein the authentication processor further includes a comparator that compares one or more of the plurality of codes associated with the account of the user to a code received from the access control device to authenticate the user of the personal biometric device.

169. The system of claim 168, wherein the personal biometric device includes a code generator that is synchronized to the one or more codes of the plurality of codes associated with the account of the user.

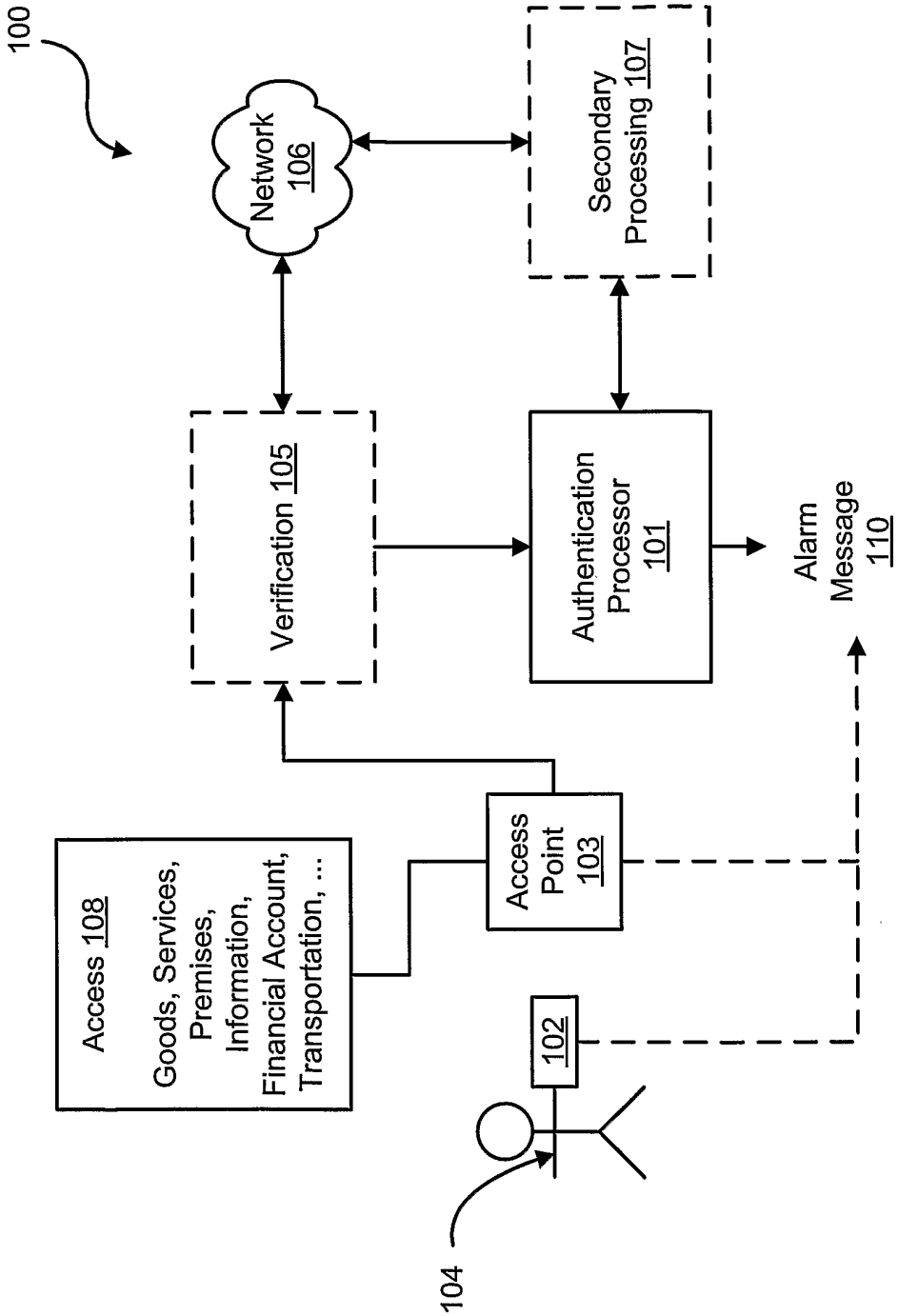

100
Network 106
Secondary Processing 107
Verification 105
Authentication Processor 101
Alarm Message 110
Access 108
Goods, Services, Premises, Information, Financial Account, Transportation, ...
Access Point 103
102
104

Figure 1

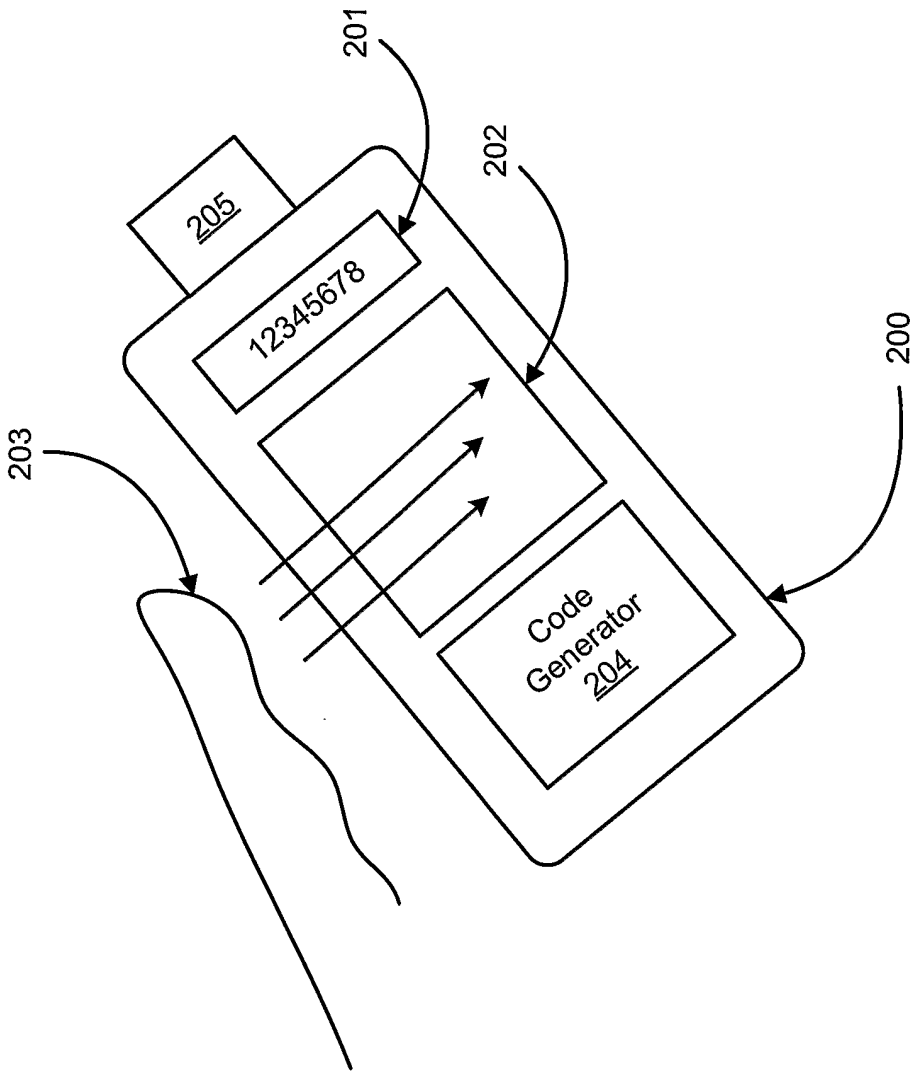


Figure 2

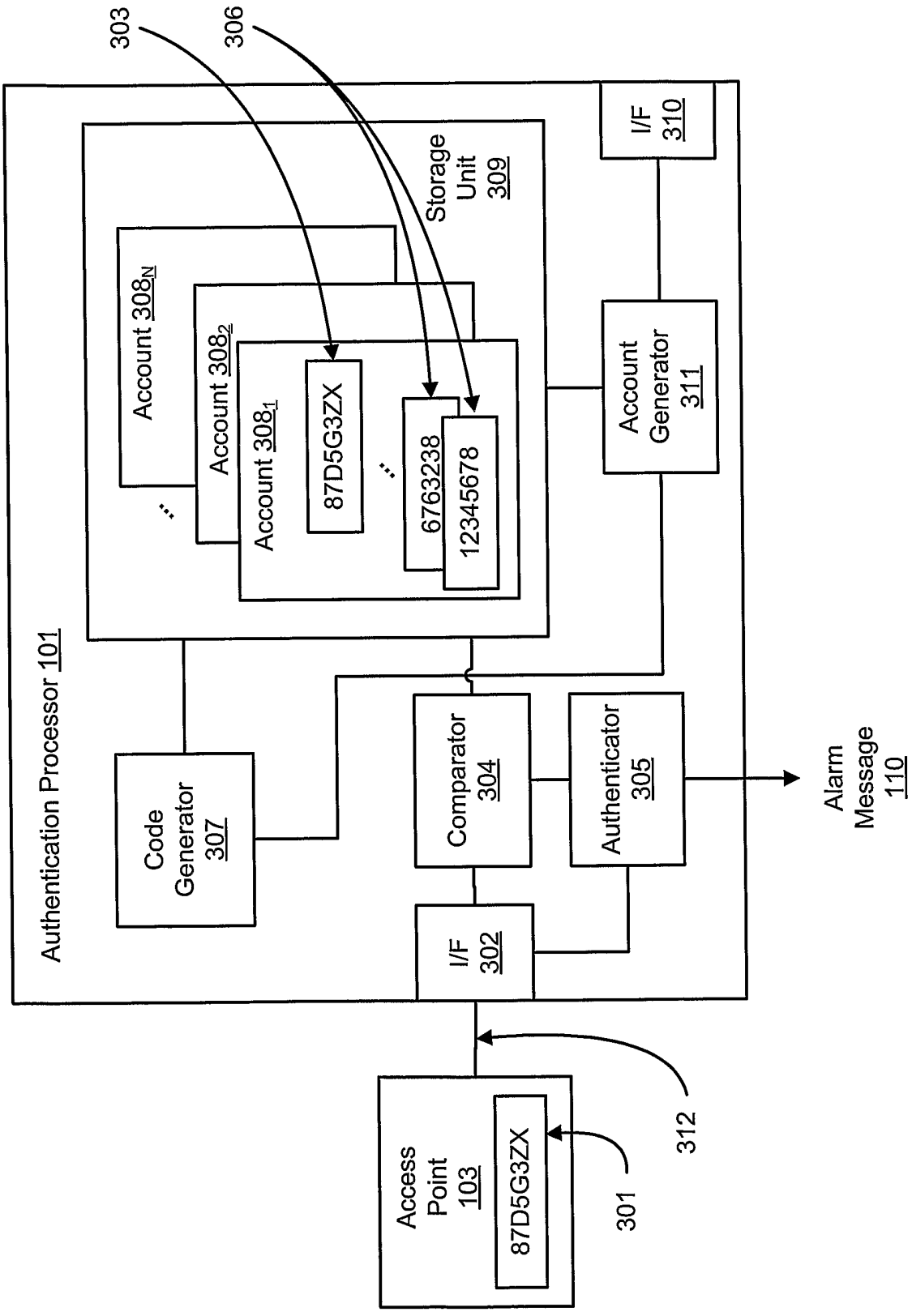

303
306
Authentication Processor 101
Storage Unit 309
Account 308N
Account 3082
Account 3081
87D5G3ZX
6763238
12345678
I/F 310
Account Generator 311
Code Generator 307
Comparator 304
Authenticator 305
Alarm Message 110
I/F 302
Access Point 103
87D5G3ZX
301
312

Figure 3

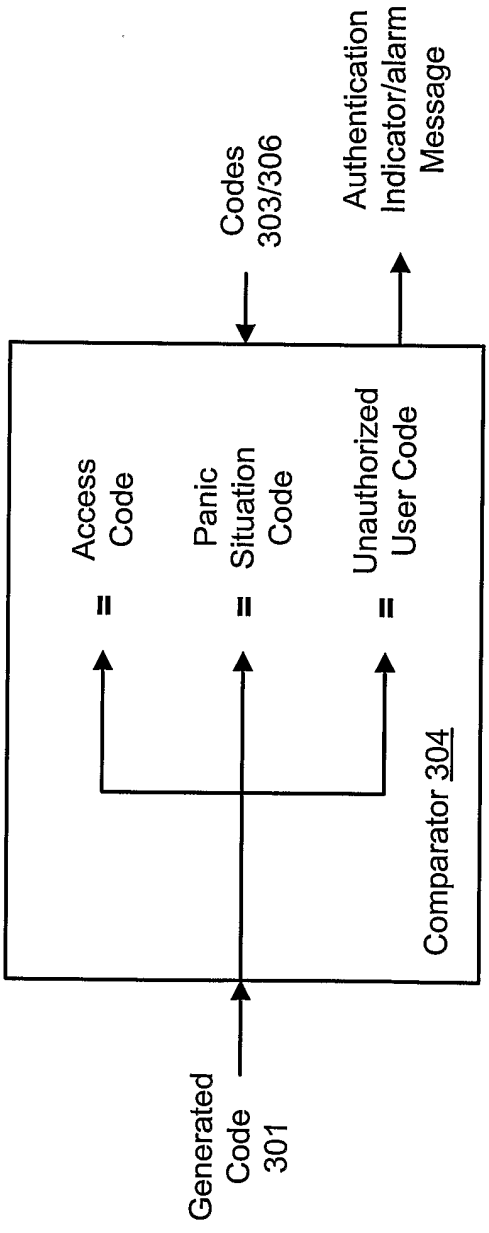

Codes
303/306
Authentication
Indicator/alarm
Message
Access
Code
=
Panic
Situation
Code
=
Unauthorized
User Code
=
Comparator 304
Generated
Code
301

Figure 4

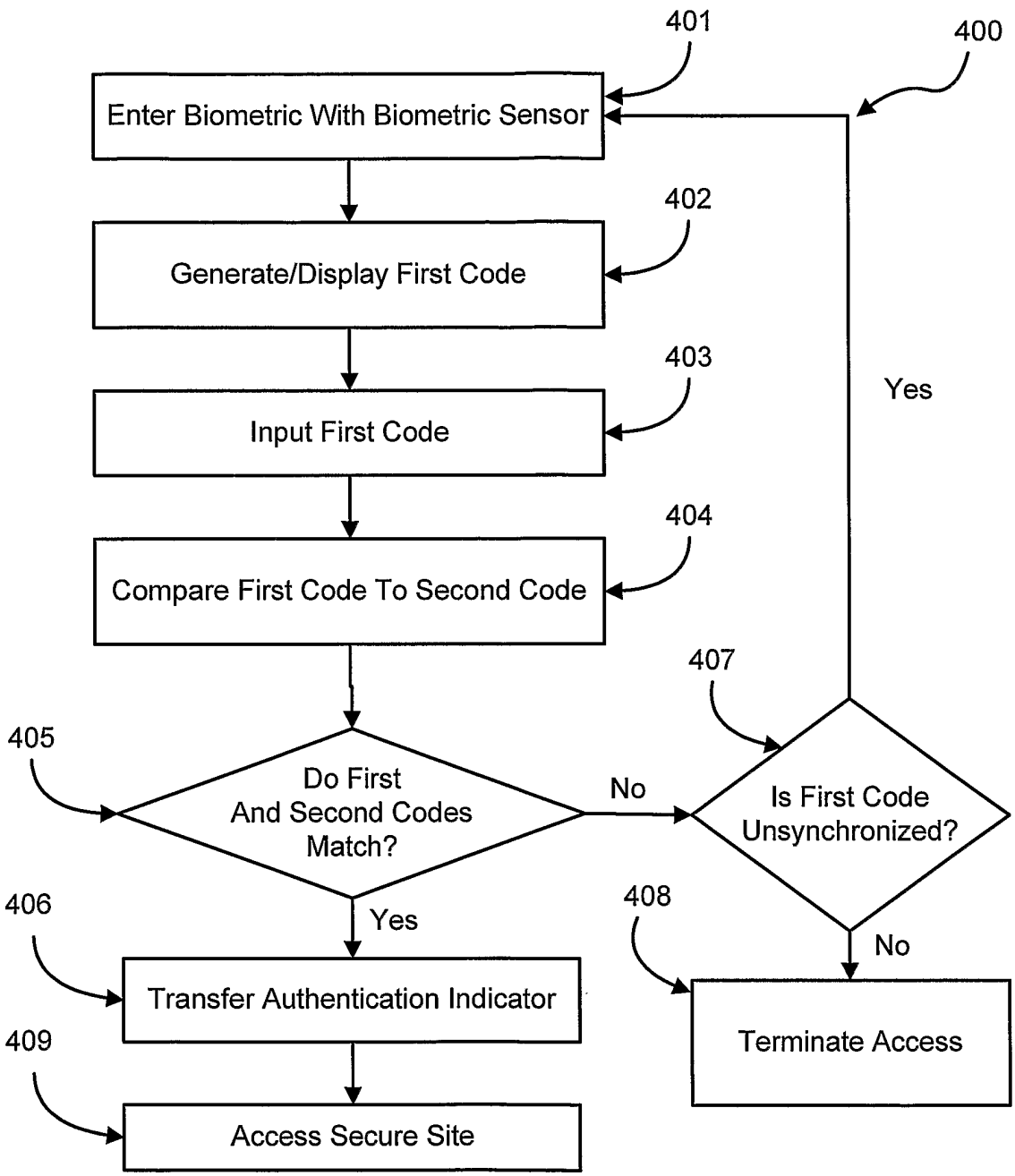

401
400
Enter Biometric With Biometric Sensor
402
Generate/Display First Code
403
Input First Code
404
Compare First Code To Second Code
407
405
Do First And Second Codes Match?
No
Is First Code Unsynchronized?
Yes
406
Yes
408
No
Transfer Authentication Indicator
409
Terminate Access
Access Secure Site

Figure 5

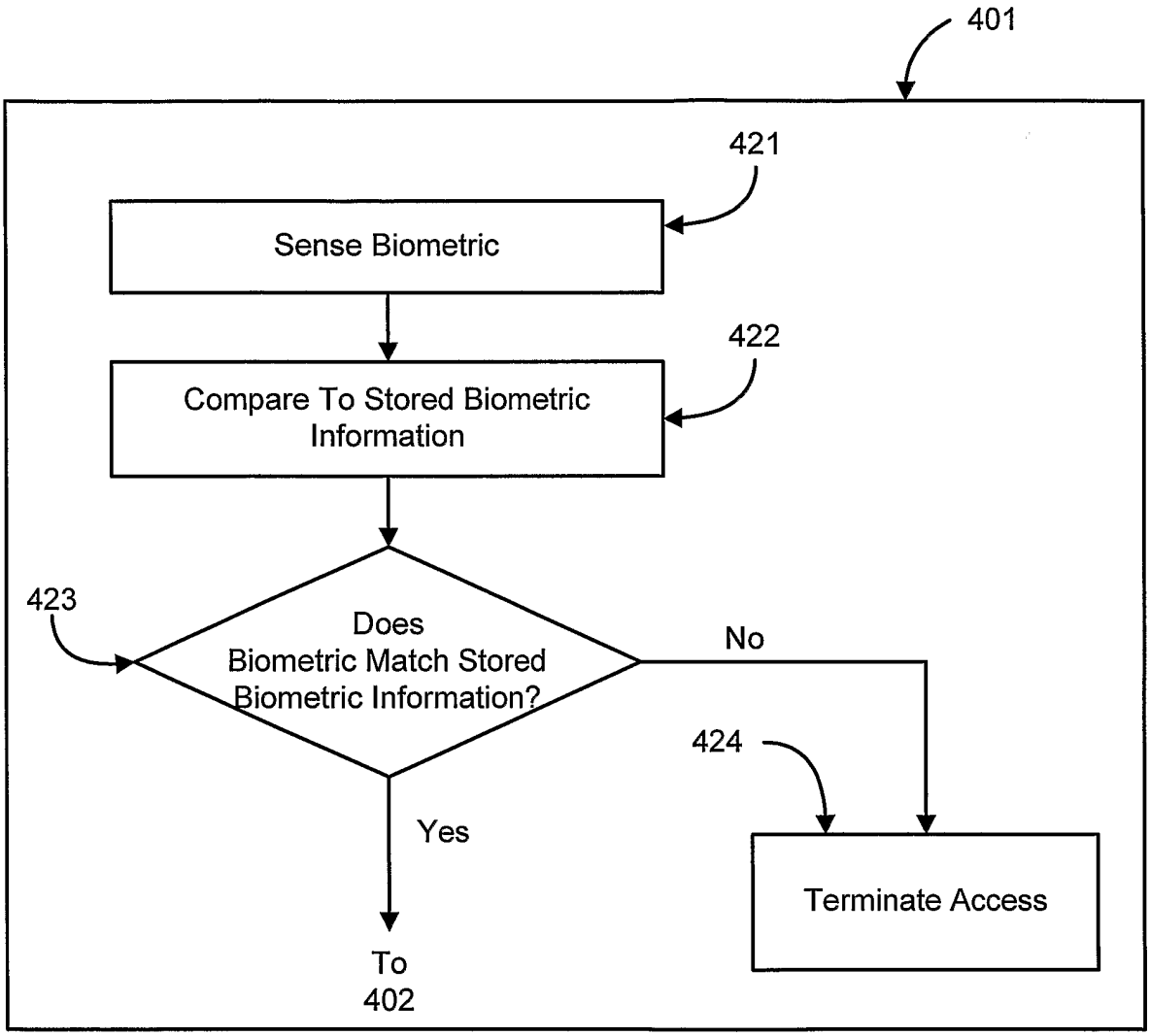

401
421
Sense Biometric
422
Compare To Stored Biometric Information
423
Does Biometric Match Stored Biometric Information?
No
424
Terminate Access
Yes
To 402

Figure 6

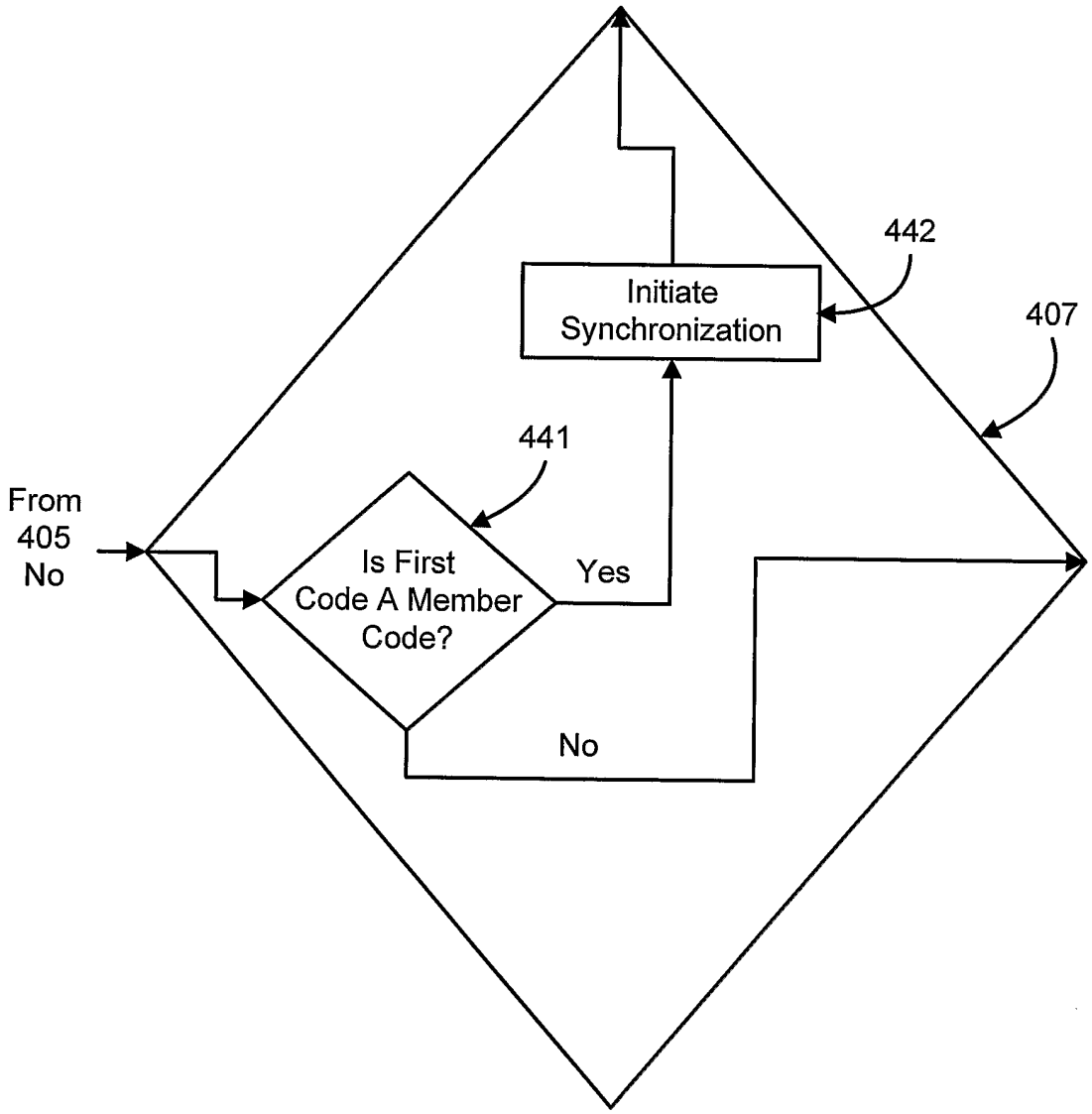

From
405
No
Is First
Code A Member
Code?
441
Yes
No
Initiate
Synchronization
442
407

Figure 7

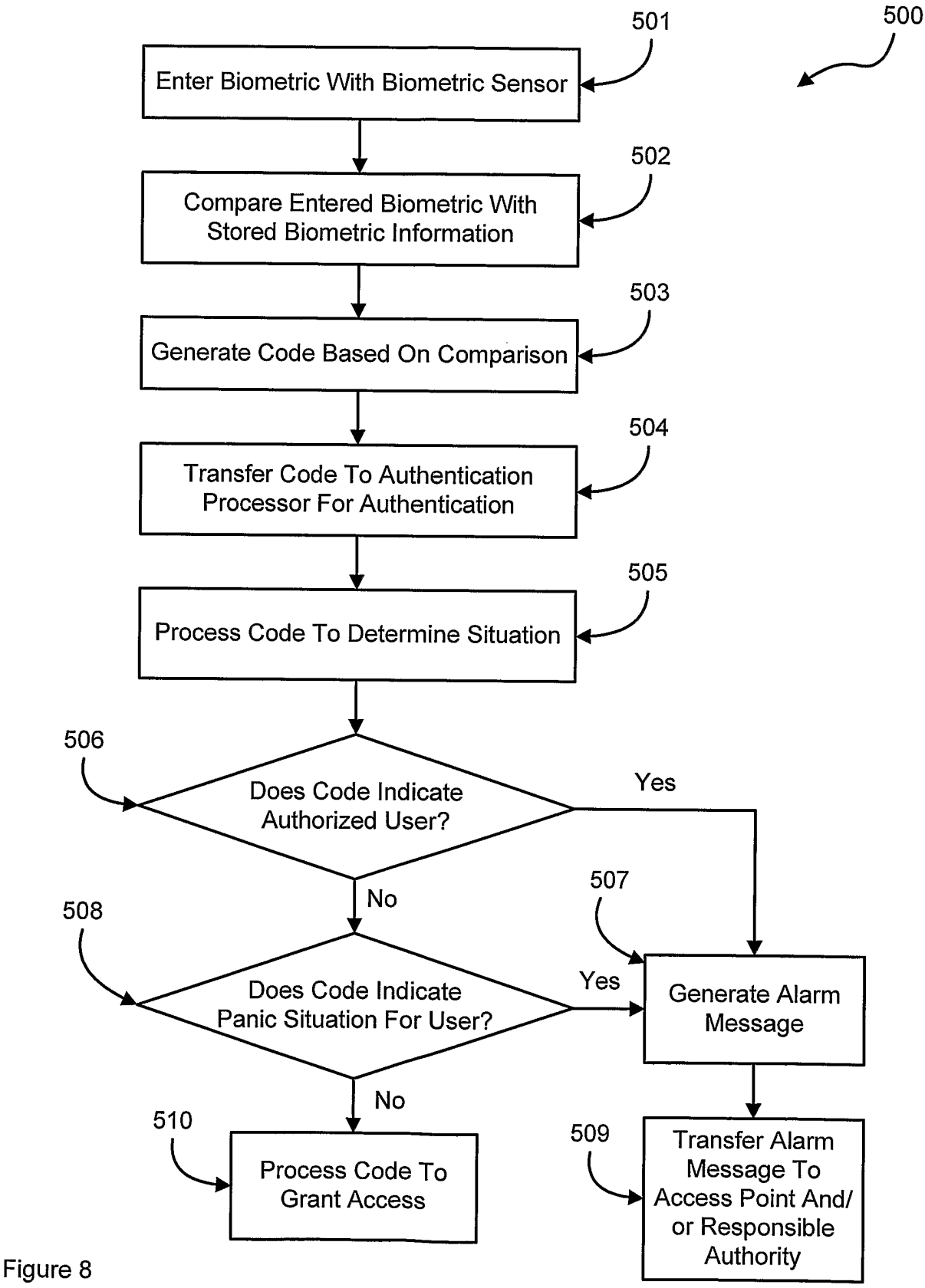

500
501
Enter Biometric With Biometric Sensor
502
Compare Entered Biometric With Stored Biometric Information
503
Generate Code Based On Comparison
504
Transfer Code To Authentication Processor For Authentication
505
Process Code To Determine Situation
506
Does Code Indicate Authorized User?
Yes
No
507
508
Does Code Indicate Panic Situation For User?
Yes
Generate Alarm Message
No
510
Process Code To Grant Access
509
Transfer Alarm Message To Access Point And/ or Responsible Authority

Figure 8

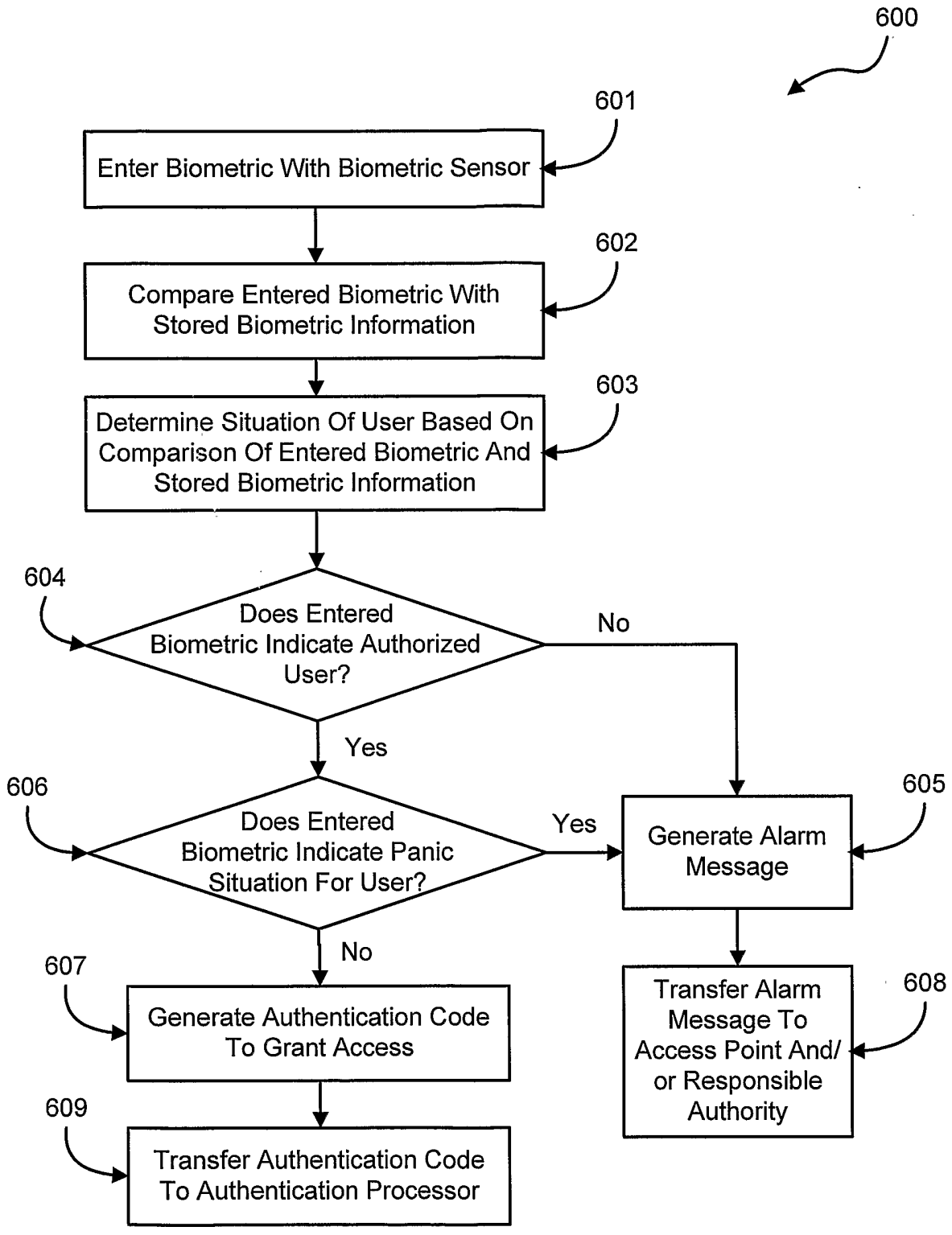

600
601
Enter Biometric With Biometric Sensor
602
Compare Entered Biometric With Stored Biometric Information
603
Determine Situation Of User Based On Comparison Of Entered Biometric And Stored Biometric Information
604
Does Entered Biometric Indicate Authorized User?
No
Yes
606
Does Entered Biometric Indicate Panic Situation For User?
Yes
605
Generate Alarm Message
No
607
Generate Authentication Code To Grant Access
608
Transfer Alarm Message To Access Point And/ or Responsible Authority
609
Transfer Authentication Code To Authentication Processor

Figure 9

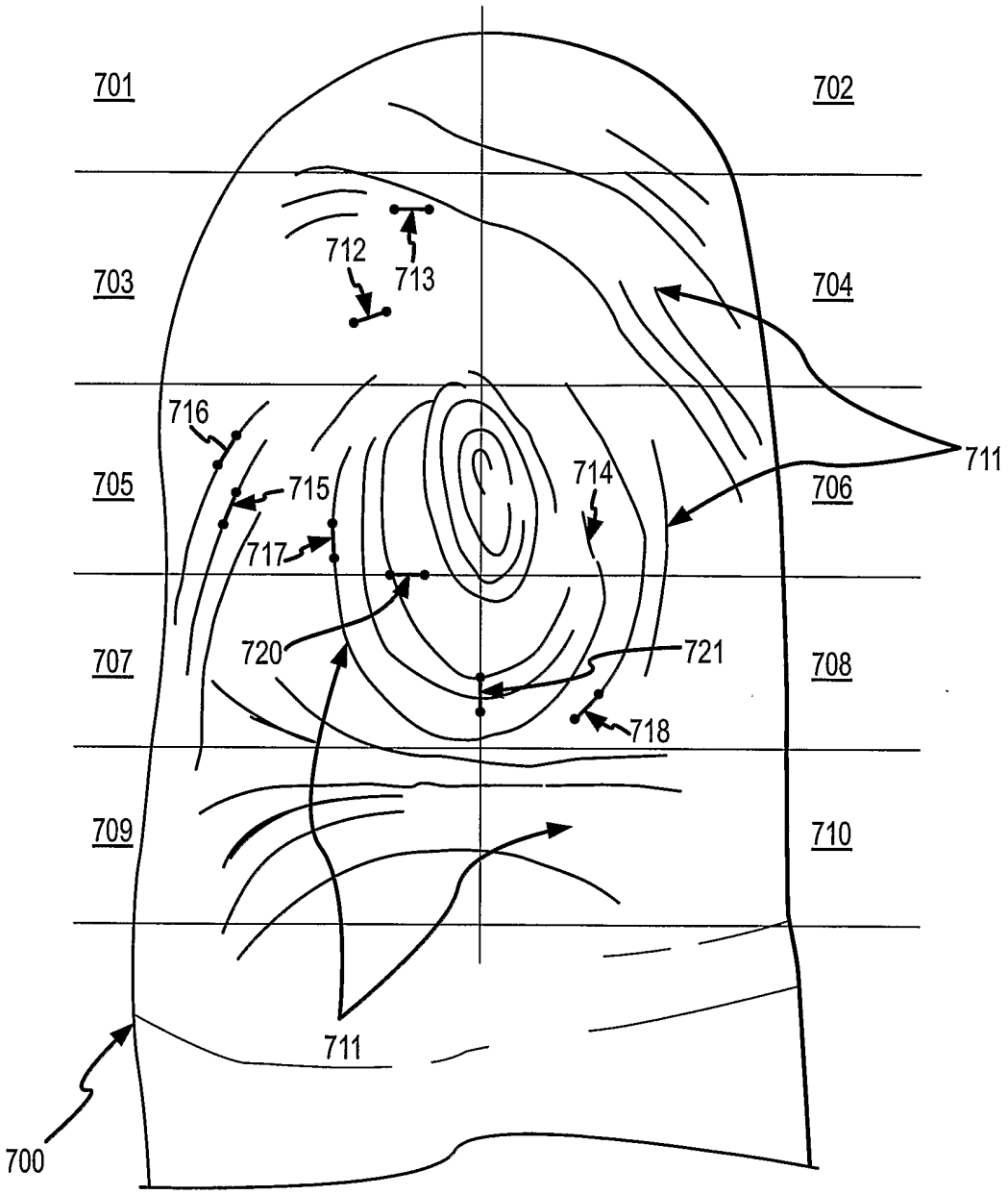

701
702
703
704
705
706
707
708
709
710
712
713
716
715
714
711
717
720
721
718
711
700

FIG.10

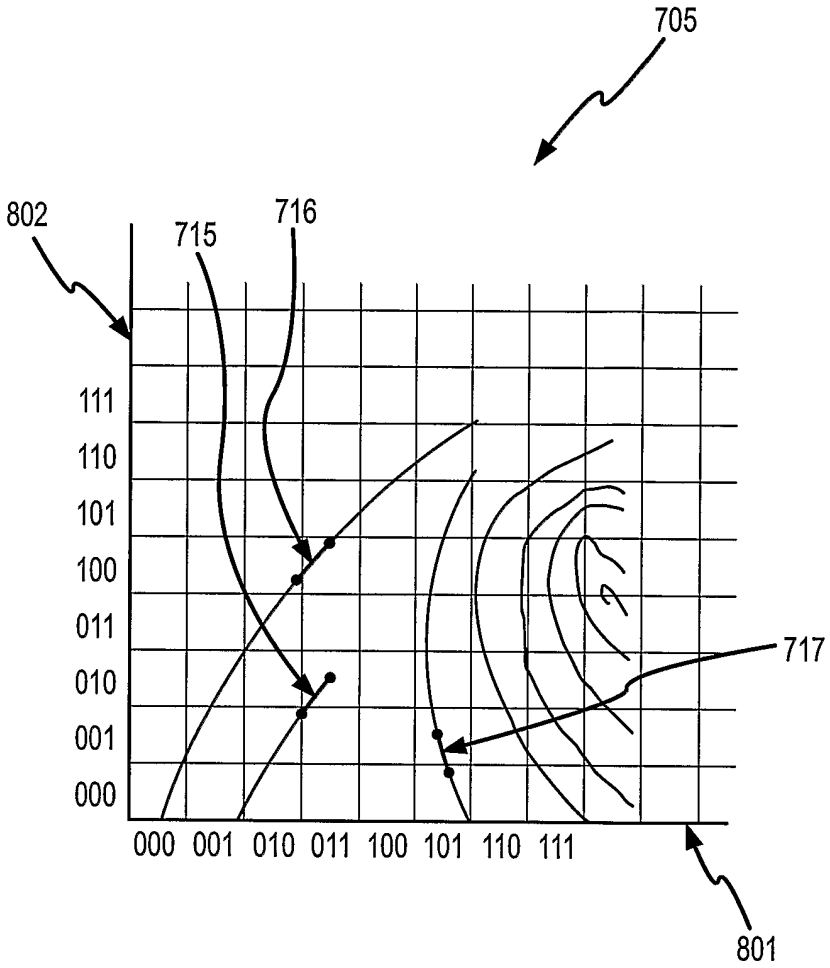

705
802
715
716
717
111
110
101
100
011
010
001
000
000 001 010 011 100 101 110 111
801

FIG.11

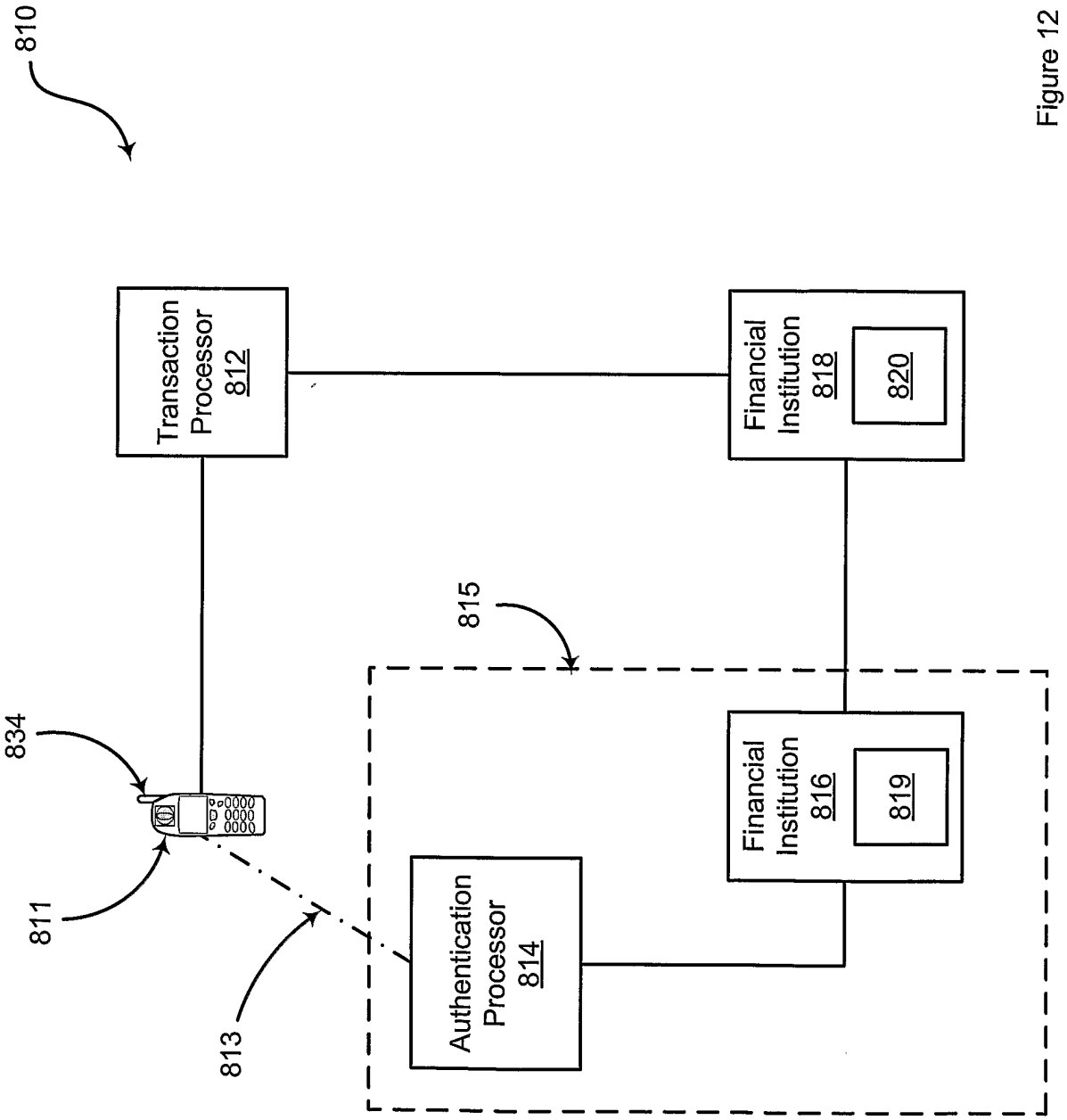

810
Transaction Processor 812
Financial Institution 818
820
815
834
811
813
Authentication Processor 814
Financial Institution 816
819

Figure 12

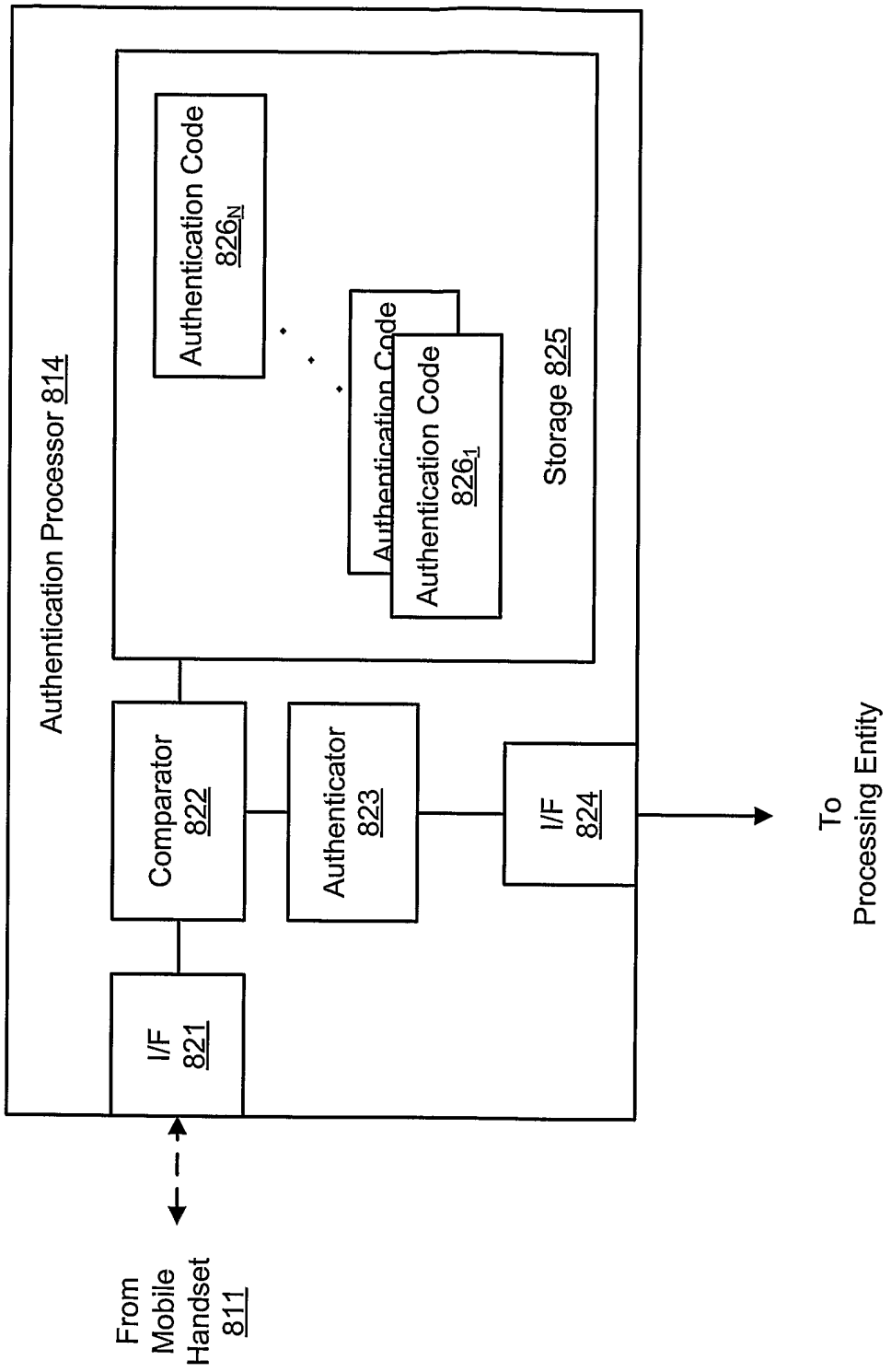

Authentication Processor 814
Storage 825
Authentication Code 826N
Authentication Code 8261
Comparator 822
Authenticator 823
I/F 824
I/F 821
To Processing Entity
From Mobile Handset 811

Figure 13

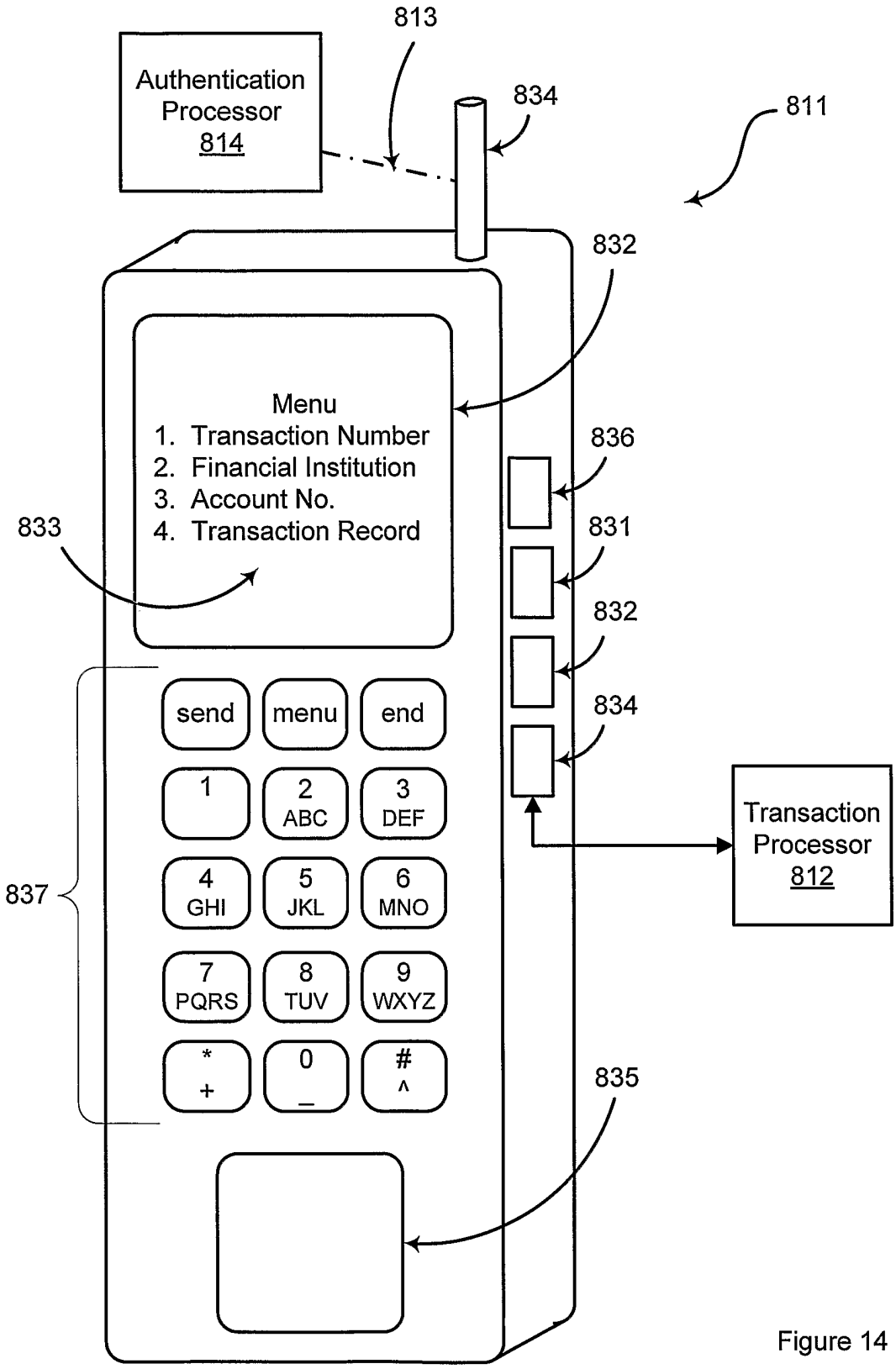

Authentication Processor 814
813
834
811
832
Menu
1. Transaction Number
2. Financial Institution
3. Account No.
4. Transaction Record
836
833
831
832
834
send
menu
end
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
*
+
0
_
#
^
837
Transaction Processor 812
835

Figure 14

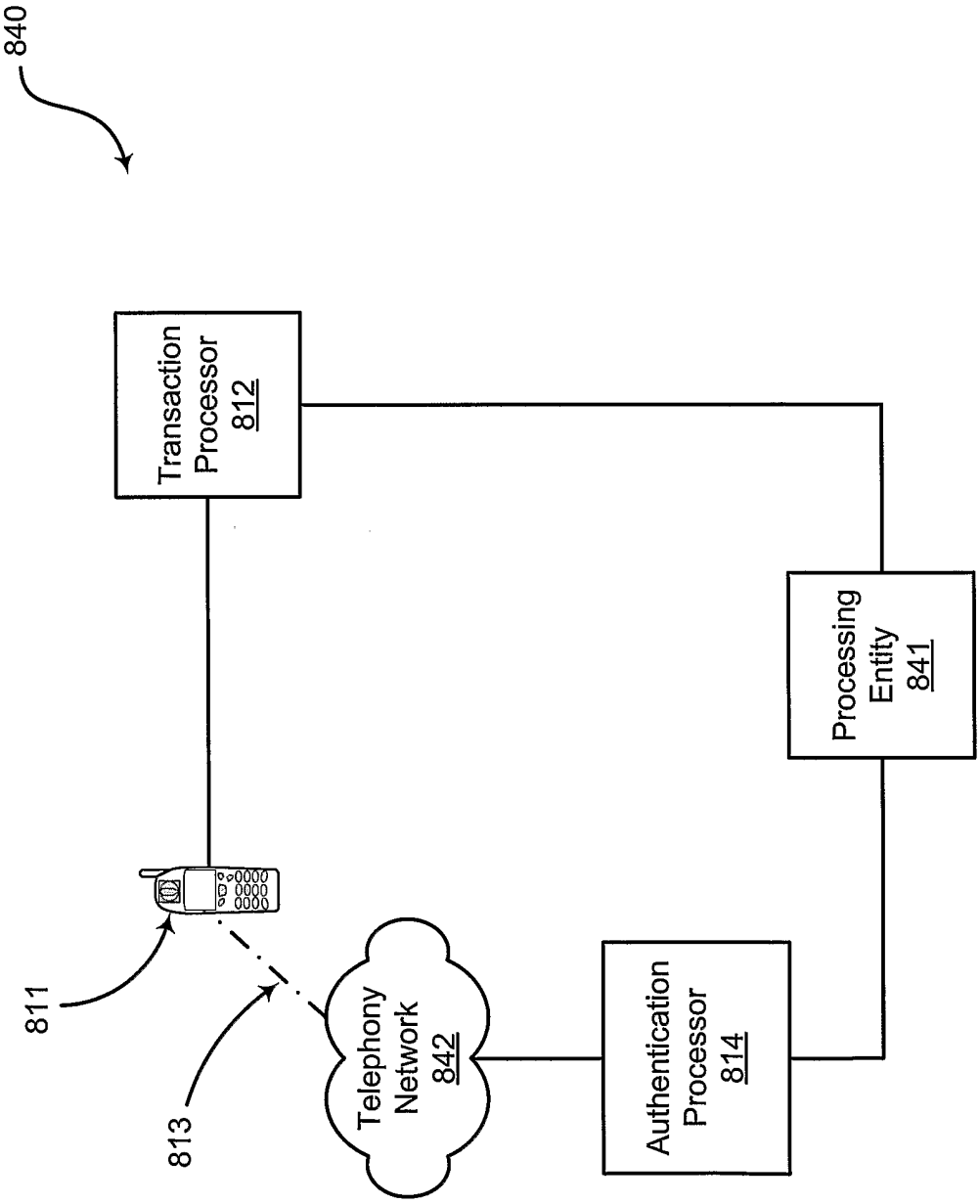

840
Transaction Processor 812
Processing Entity 841
811
813
Telephony Network 842
Authentication Processor 814

Figure 15

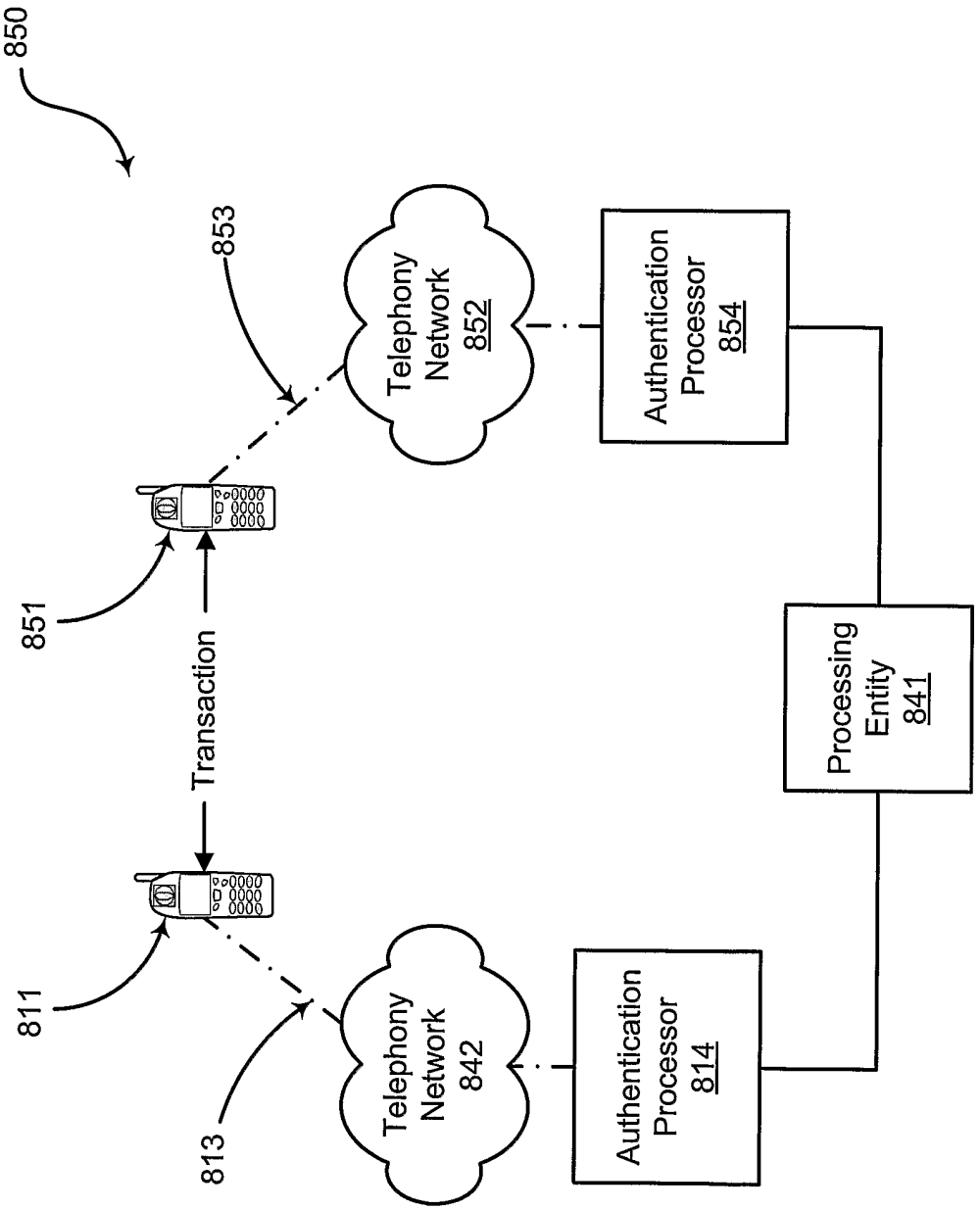

850
853
Telephony Network 852
Authentication Processor 854
851
Transaction
Processing Entity 841
811
813
Telephony Network 842
Authentication Processor 814

Figure 16

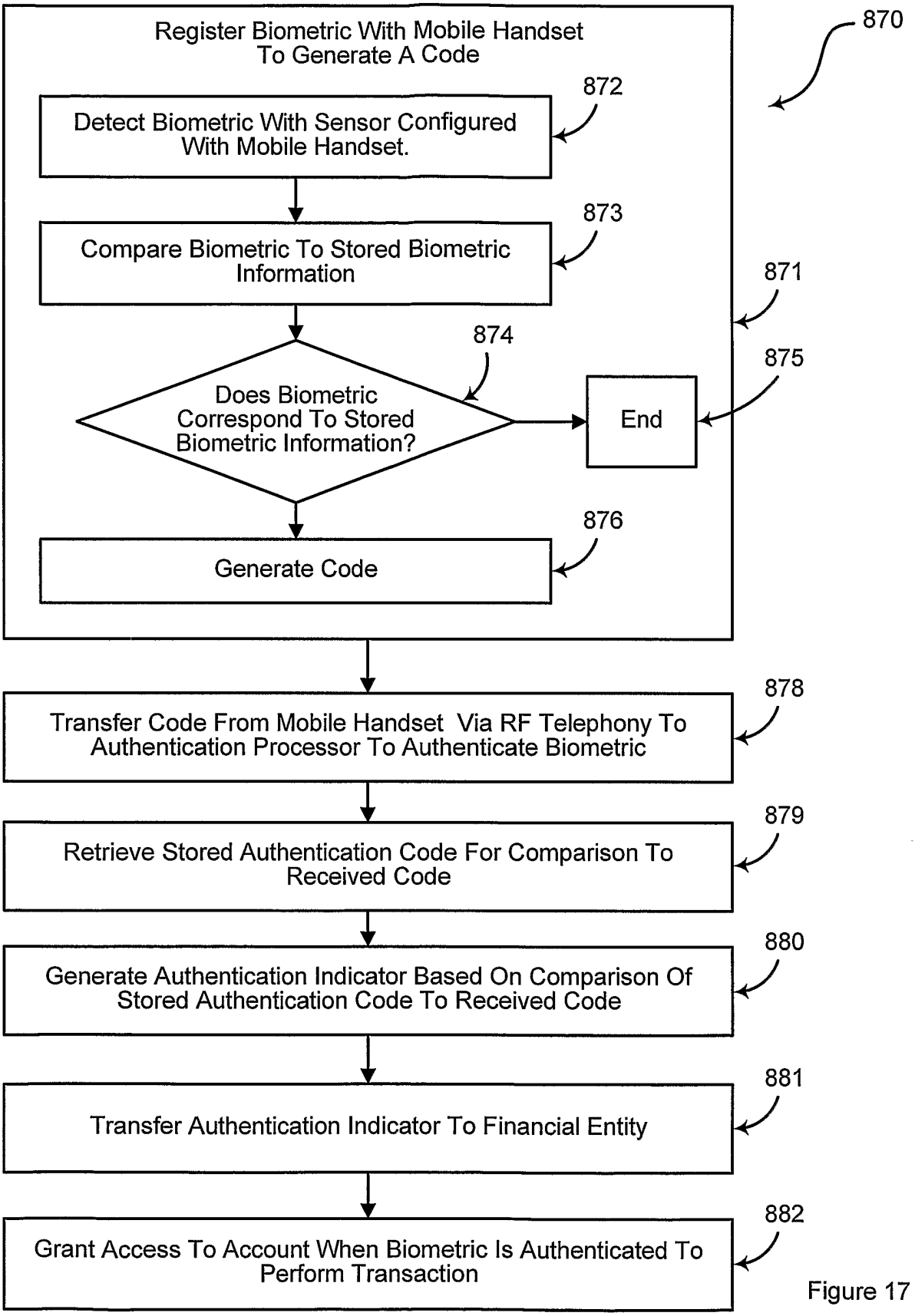

Register Biometric With Mobile Handset To Generate A Code
870
872
Detect Biometric With Sensor Configured With Mobile Handset.
873
Compare Biometric To Stored Biometric Information
871
874
Does Biometric Correspond To Stored Biometric Information?
875
End
876
Generate Code
878
Transfer Code From Mobile Handset Via RF Telephony To Authentication Processor To Authenticate Biometric
879
Retrieve Stored Authentication Code For Comparison To Received Code
880
Generate Authentication Indicator Based On Comparison Of Stored Authentication Code To Received Code
881
Transfer Authentication Indicator To Financial Entity
882
Grant Access To Account When Biometric Is Authenticated To Perform Transaction

Figure 17

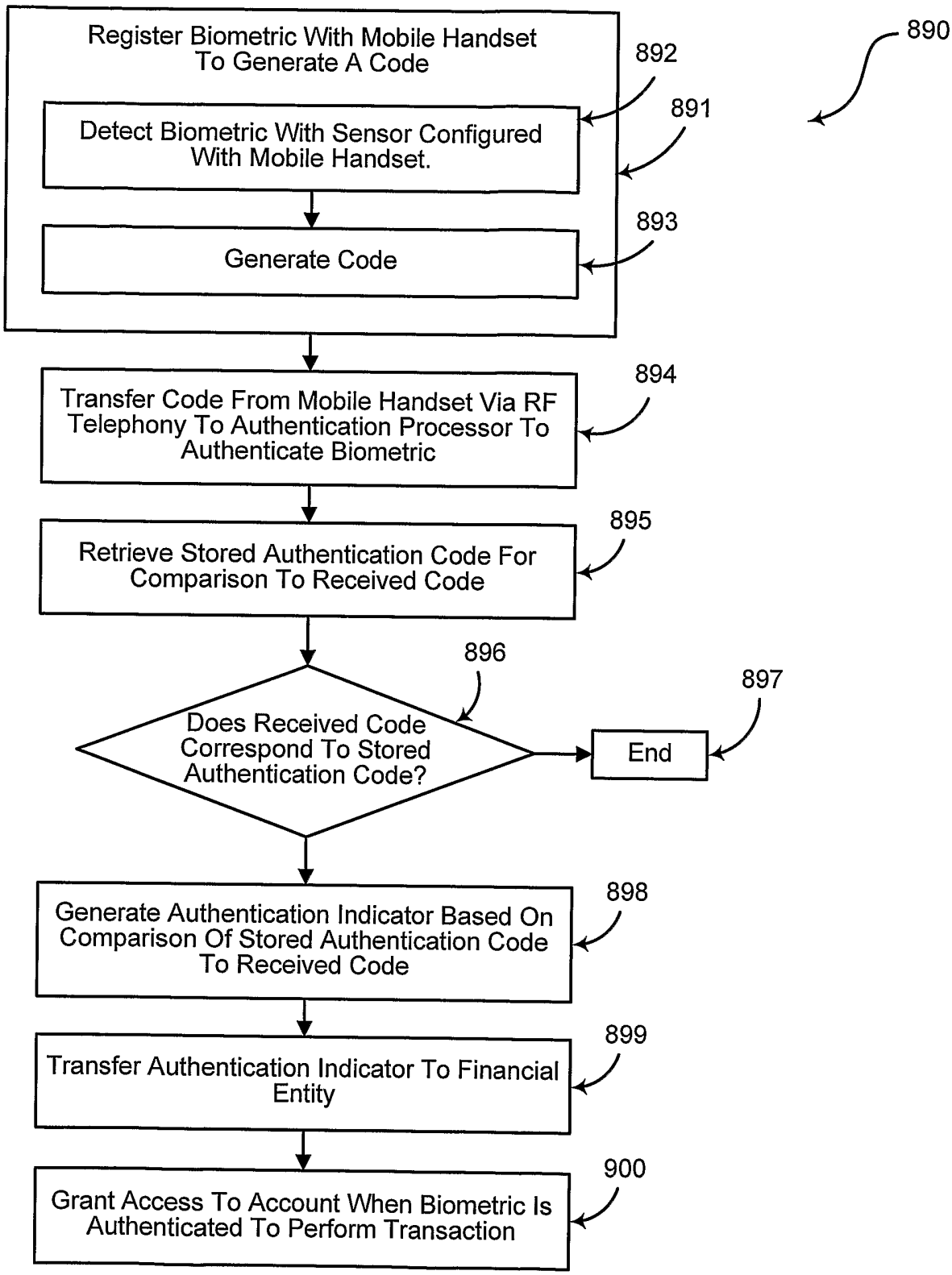

Register Biometric With Mobile Handset To Generate A Code
890
892
891
Detect Biometric With Sensor Configured With Mobile Handset.
893
Generate Code
894
Transfer Code From Mobile Handset Via RF Telephony To Authentication Processor To Authenticate Biometric
895
Retrieve Stored Authentication Code For Comparison To Received Code
896
897
Does Received Code Correspond To Stored Authentication Code?
End
898
Generate Authentication Indicator Based On Comparison Of Stored Authentication Code To Received Code
899
Transfer Authentication Indicator To Financial Entity
900
Grant Access To Account When Biometric Is Authenticated To Perform Transaction

Figure 18

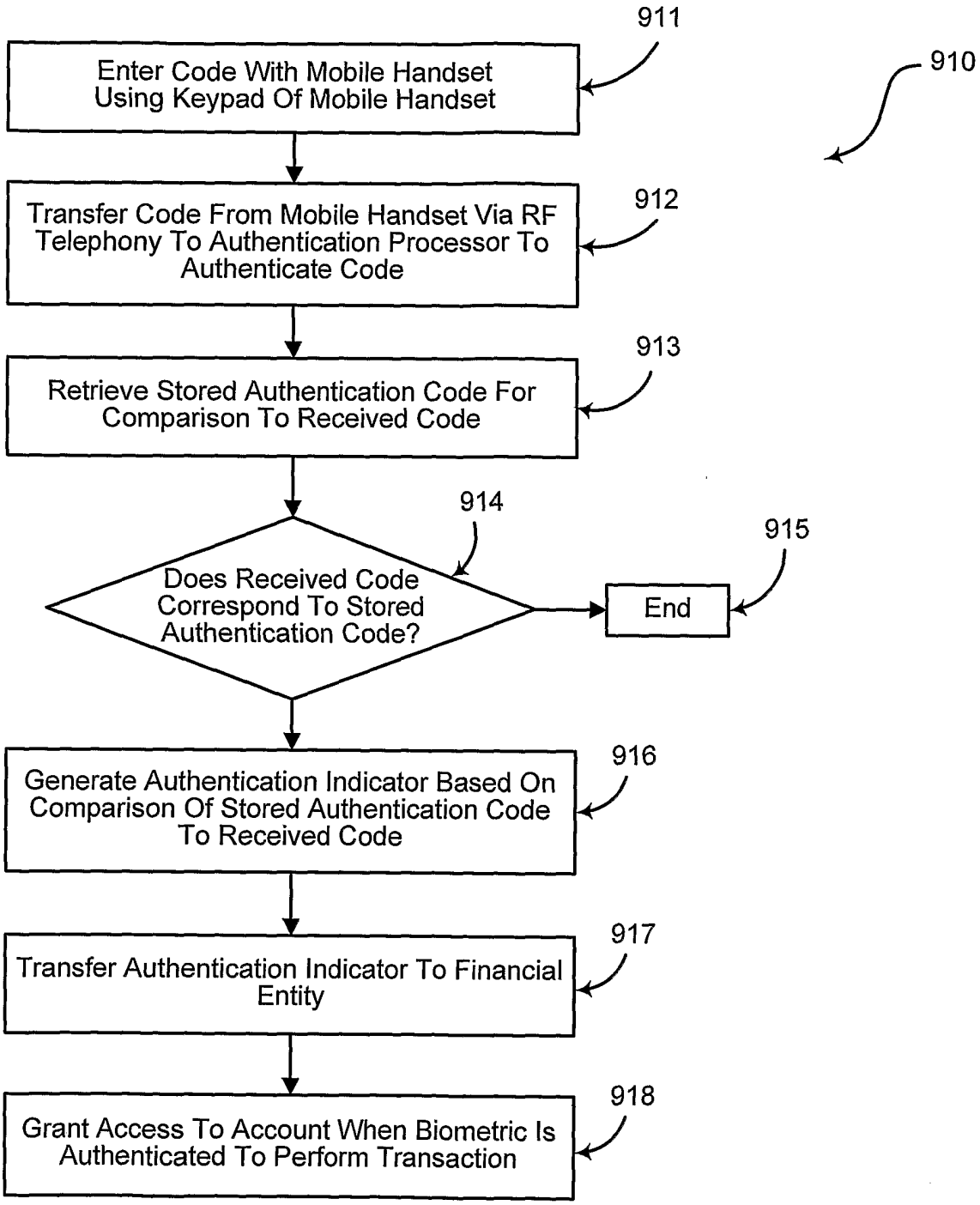

911
910
Enter Code With Mobile Handset Using Keypad Of Mobile Handset
912
Transfer Code From Mobile Handset Via RF Telephony To Authentication Processor To Authenticate Code
913
Retrieve Stored Authentication Code For Comparison To Received Code
914
915
Does Received Code Correspond To Stored Authentication Code?
End
916
Generate Authentication Indicator Based On Comparison Of Stored Authentication Code To Received Code
917
Transfer Authentication Indicator To Financial Entity
918
Grant Access To Account When Biometric Is Authenticated To Perform Transaction

Figure 19

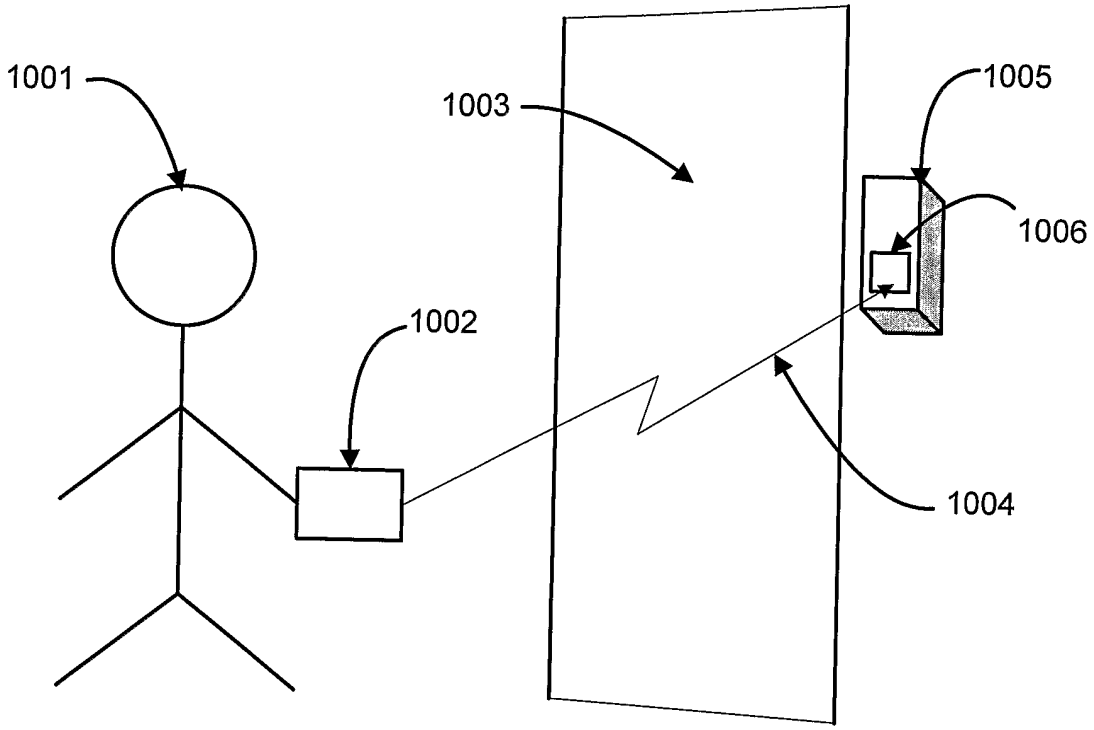


Figure 20

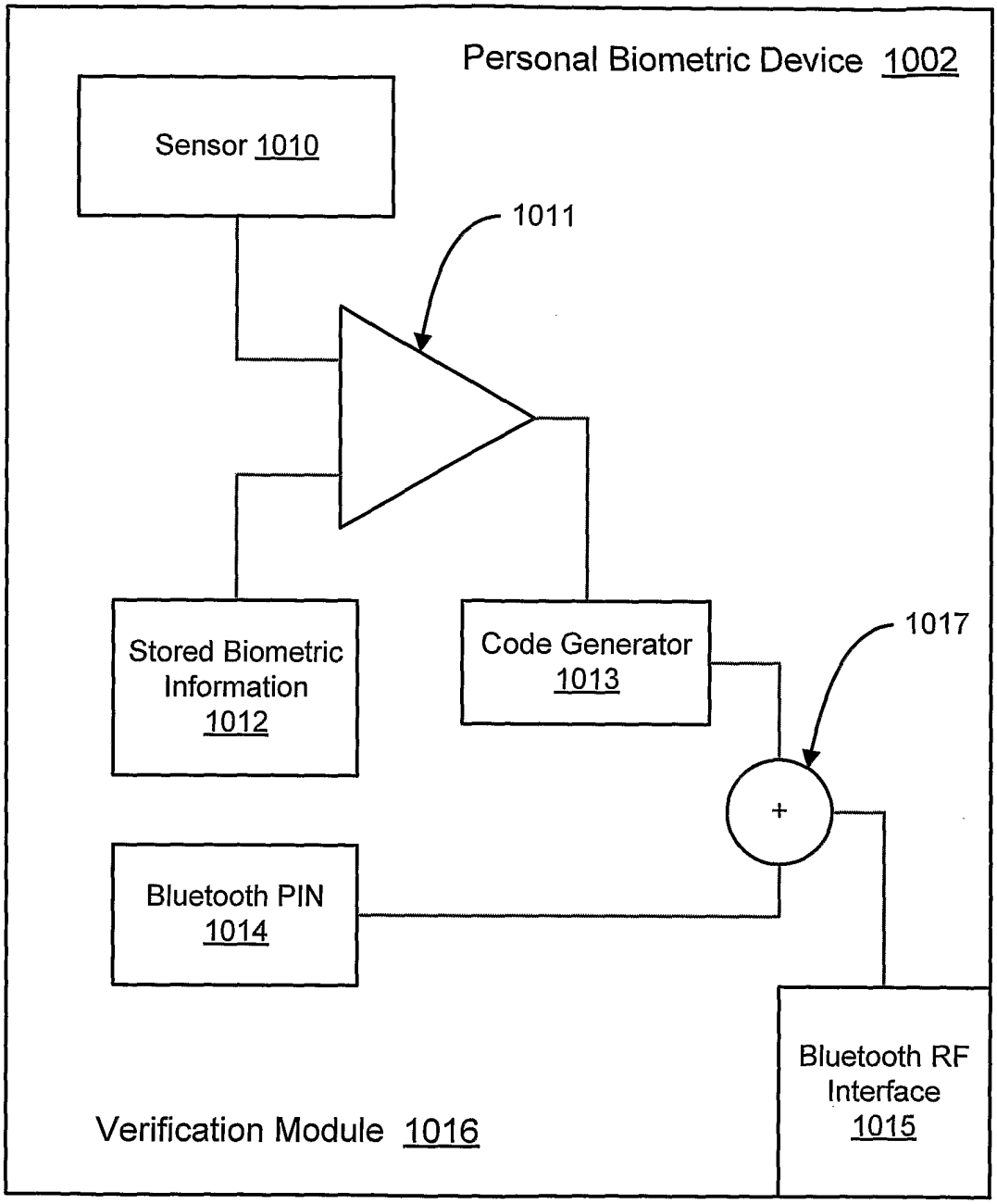

Personal Biometric Device 1002
Sensor 1010
1011
Stored Biometric Information 1012
Code Generator 1013
1017
+
Bluetooth PIN 1014
Bluetooth RF Interface 1015
Verification Module 1016

Figure 21