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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 January 2003 (23.01.2003)

PCT

(10) International Publication Number
WO 03/007125 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number: PCT/US02/22200

(22) International Filing Date: 12 July 2002 (12.07.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/305,120	12 July 2001 (12.07.2001)	US
10/099,554	13 March 2002 (13.03.2002)	US
10/099,558	13 March 2002 (13.03.2002)	US

(71) Applicant *(for all designated States except US)*: **ICONTROL TRANSACTIONS, INC.** [US/US]; 1999 South Bascom Avenue, Suite 700, Campell, CA 95008 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **RUSSO, Anthony, P.** [US/US]; 58 W 75th Street, #3A, New York, NY 10023 (US). **MCCOY, Peter, A.** [GB/US]; 1453 130th Avenue, Santa Cruz, CA 95062 (US). **RÖSKE, Thorsten** [DE/DE]; Schieggstr. 8a, 81479 Munich (DE).

(74) Agents: **ANANIAN, R., Michael** et al.; Dorsey & Whitney LLP, 4 Embarcadero Center, Suite 3400, San Francisco, CA 94111 (US).

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

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (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*

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.

WO 03/007125 A2

(54) Title: SECURE NETWORK AND NETWORKED DEVICES USING BIOMETRICS

(57) Abstract: A biometric data sample is taken and compared with stored biometric data. If the biometric data sample matches stored data, access to a secure data storage module is enabled. The secure data storage module contains data necessary for successful communication with a server, as detailed further below. Accordingly, a biometric data match enables sensitive data retrieval, and ultimately secure communication with another device. In a preferred embodiment, the Subscriber Identity Module (SIM) in a GSM phone provides stored biometric data and processing capabilities for the matching function within a cellular phone. By storing biometric data on the SIM (a type of smart card) and performing the biometric matching process on the SIM, the need to transmit or store biometric data in a way that leaves it available for retrieval or tampering is minimized.

SECURE NETWORK AND NETWORKED DEVICES USING BIOMETRICS

Related Applications

This application claims the benefit under 35 U.S.C. §119 and/or 35 U.S.C. §120 of the filing date of: U.S. Provisional Application Serial Number 60/305,120, filed July 12, 2001, which is hereby incorporated by reference. and entitled SYSTEM, METHOD, DEVICE AND COMPUTER PROGRAM FOR NON-REPUDIATED WIRELESS TRANSACTIONS; United States Patent Application Serial No. 10/099,554 filed 03/13/02 and entitled SYSTEM, METHOD, AND OPERATING MODEL FOR MOBILE WIRELESS NETWORK-BASED TRANSACTION AUTHENTICATION AND NON-REPUDIATION; and United States Patent Application Serial No. 10/099,558 filed 03/13/02 and entitled FINGERPRINT BIOMETRIC CAPTURE DEVICE AND METHOD WITH INTEGRATED ON-CHIP DATA BUFFERING; each of which applications are incorporated by reference herein.

This application further relates to the following co-pending applications:

U.S. Application Serial Number 10/___,___, filed _____, entitled "METHOD AND SYSTEM FOR DETERMINING CONFIDENCE IN A DIGITAL TRANSACTION" (Attorney Docket No. A-70779/RMA/JML);

U.S. Application Serial Number 10/___,___, filed _____, entitled "BIOMETRICALLY ENHANCED DIGITAL CERTIFICATES AND SYSTEM AND METHOD FOR MAKING AND USING" (Attorney Docket No. A-70596/RMA/JML); and

U.S. Application Serial Number 10/___,___, filed _____, entitled "METHOD AND SYSTEM FOR BIOMETRIC IMAGE ASSEMBLY FROM MULTIPLE PARTIAL BIOMETRIC FRAME SCANS" (Attorney Docket No. A-70591/RMA/JML); all of which are hereby incorporated by reference.

Field of the Invention

This invention pertains generally to device, user, and transaction verification and authentication devices, systems, and methods; and more particularly to devices employing device, user, and transaction verification, authentication, and non-repudiation systems and

methods for mobile wireless applications that capture and utilize biometric data for transaction verification and authentication.

Background of the Invention

The security and integrity of information systems depends in part on authentication of individual users, that is accurately and reliably determining the identity of a user attempting to use the system. Once a user is authenticated, a system is then able to authorize the user to retrieve certain information or perform certain actions appropriate to the system's understanding of the user's identity. Examples of such actions include downloading a document, completing a financial transaction, or digitally signing a purchase.

A number of methods have been developed for authenticating users. Generally, as will be understood by those skilled in the art, authentication methods are grouped into three categories, also called authentication factors: 1) something you know - a secret such as a password or a PIN or other information; 2) something you have - such as a smartcard, the key to a mechanical lock, an ID badge, or other physical object; and 3) something you are - a measure of a person such as a fingerprint or voiceprint. Each method has advantages and disadvantages including those relating to ways that a system may be fooled into accepting a normally unauthorized user in cases where, for example, a password has been guessed or a key has been stolen.

The third category above – referred to herein as 'something you are' authentication methods - are the subject of the biometrics field. Biometric identification is used to verify the identity of a person by measuring selected features of some physical characteristic and comparing those measurements with those filed for the person in a reference database or stored in a token (such as a smartcard) carried by the person. Physical characteristics that are used today include fingerprints, voiceprints, hand geometry, the pattern of blood vessels on the wrist or on the retina of the eye, the topography of the iris of the eye, facial patterns, and the dynamics of writing a signature or typing on a keyboard. Biometric identification methods are widely used today for securing physical access to buildings and securing data networks and personal computers.

Many present biometric systems store a user's biometric data in a file on a workstation or a server where they could be retrieved or tampered with by unauthorized parties - or transmit biometric data over a medium that could be eavesdropped. This could compromise the user's privacy or the security and integrity of the information systems dependent on biometric authentication.

At present, systems requiring user authentication from mobile devices – such as PDAs or mobile phones – usually use passwords or PIN codes, i.e., "something you know" authentication. However, mobile devices typically have small keypads, few buttons or rely on

handwriting recognition for user input. These limited user-input options make entering long passwords difficult, although longer alphanumeric passwords are generally known to be "stronger" (less likely to be guessed and compromised) than, for example a 4 digit numeric PIN – allowing only ten thousand combinations.

Some mobile devices provide facilities for the secure, tamper resistant processing and storage of data separate from the main processing and storage facility of the device. Mobile phones adhering to the Global System for Mobile Communications (GSM) body of standards use a Subscriber Identity Module, or SIM, which is a "smart card" that provides secure storage and processing facilities for the phone. SIMs are generally known in the art, see for example, "Digital cellular telecommunications system (Phase 2); Specification of the Subscriber Identity Module – Mobile Equipment (SIM – ME) interface (GSM 11.11 version 4.21.1) published by European Telecommunications Standards Institute (ETSI) of Valbonne, France, document ETS 300 608, ninth edition, Dec 1999, hereby incorporated by reference. The SIM contains and protects sensitive information that the phone uses to identify itself on and participate in a GSM network.

Accordingly, there is a need for a biometric authentication system that provides accurate, reliable identification of a user or transaction where the biometric data is stored and transmitted securely – that is, where the privacy of users as well as integrity of transactions is maintained.

Therefore, it is an object of the present invention to provide a secure biometric authentication system that leverages the strengths of 'what you have' authentication systems as well as biometric – 'what you are' authentication systems. It is a further object of the present invention to provide a mobile device capable of using a secure biometric authentication system.

Summary

In a first embodiment, the present invention provides a method for secure communication with a server, wherein said secure communication requires encryption information, said method comprising obtaining a biometric data sample, comparing said biometric data sample to stored biometric data, enabling access to said sensitive data if said biometric data sample matches said stored biometric data, and communicating with said server using said sensitive data.

In some embodiments of the method, secure communication comprises communicating message information, said communicating further comprises encrypting the message information using said sensitive data.

In some embodiments, obtaining a biometric data sample comprises processing a fingerprint scan. In other embodiments, obtaining a biometric data sample comprises processing an image, which may be, for example, a facial image. In still other embodiments, obtaining a biometric data sample comprises processing a speech sample.

In some embodiments, the sensitive data includes a private encryption key.

Some embodiments of a method according to the present invention further comprise processing said biometric data sample.

Other embodiments of the present invention provide methods for secure communication between a server and mobile device comprising obtaining a biometric data sample, comparing said biometric data sample to stored biometric data, and transmitting acceptance result to said server if said biometric data sample matches said stored biometric data.

Still other embodiments of the present invention provide devices for securely communicating with a server, said device comprising a biometric sensor, a secure data storage module containing stored biometric data and sensitive data required for communication with said server, in electronic communication with said biometric sensor, matching logic in electronic communication with said sensor and said biometric data memory, and a verification processor in electronic communication with said matching logic and said secure data storage module.

In some embodiments, the matching logic is provided on a smart card. In some preferred embodiments, the matching logic is provided on a SIM card.

In some embodiments, the verification processor is provided within a cellular phone. The biometric sensor may be on a front surface, on a rear surface, below a keypad on a surface, on a side surface, or embedded in a key, such as an ON key, of said cellular phone.

In some embodiments, the device further comprises an input device associated with said verification processor and the biometric sensor is located on said input device. In other embodiments, the device further comprises a display device associated with said verification processor and said biometric sensor is located on said display device.

In still other embodiments, the verification processor is provided within a personal digital assistant.

In another aspect of the present invention, a computer program product comprising a computer-readable memory is provided, where the computer-readable memory is encoded with an instruction set that, when executed, processes a biometric data sample, compares said biometric data sample with stored biometric data, enables access to sensitive data if said biometric data sample matches said stored biometric data, and transmits an acceptance result.

Brief Description of the Drawings

The present invention may be better understood, and its features and advantages made apparent to those skilled in the art by referencing the accompanying drawings.

FIG. 1 is a diagrammatic illustration of a secure networked device using biometrics according to an embodiment of the present invention.

FIG. 2 is a diagram of the initiation of an authentication process.

FIG. 3 is a diagram of the authentication process after a matching procedure has been performed.

FIG. 4 is a diagram of the matching procedure.

FIG. 5 is a schematic diagrams showing one exemplary biometric sensor placement location on a mobile phone.

FIG. 6 is a schematic diagram showing a second exemplary biometric sensor placement location on a mobile phone.

FIG. 7 is a schematic diagram showing a third exemplary biometric sensor placement location on a mobile phone.

FIG. 8 is a schematic diagram showing a fourth exemplary biometric sensor placement location on a mobile phone.

FIG. 9 is a schematic diagram showing a fifth exemplary biometric sensor placement location on a mobile phone.

FIG. 10 is a schematic diagram showing a sixth exemplary biometric sensor placement location on a mobile phone.

FIG. 11 is a schematic diagram showing a seventh exemplary biometric sensor placement location on a mobile phone.

Detailed Description of the Embodiments

The invention generally provides improved privacy and security in biometric systems. Briefly, private and secure communication between a user device and a server (or another user or administrator or service provider device) proceeds as follows. A biometric data sample is taken and compared with stored biometric data. If the biometric data sample matches stored data, access to a secure data storage module is enabled. The secure data storage module contains data necessary for successful communication with a server, as detailed further below. Accordingly, a biometric data match enables sensitive data retrieval, and ultimately secure communication with another device.

In preferred embodiments of the present invention, the stored biometric data and advantageously, but optionally, the matching procedure is performed within a smart card or other smart "what you have" token. In a preferred embodiment, the Subscriber Identity Module (SIM) in a GSM phone provides stored biometric data and processing capabilities for the matching function within the phone. By storing biometric data on the SIM (a type of smart card) and performing the biometric matching process on the SIM, the need to transmit or store biometric data in a way that leaves it available for retrieval or tampering is minimized.

Accordingly, devices suitable for use with the present invention include substantially any device suited for electronic communication with a network server (or any other device). Generally, any device for which user authentication is desired may utilize the systems and methods of the present invention, with mobile devices being particularly preferred. Fig. 1 schematically illustrates device 101 according to an embodiment of the present invention. In a preferred embodiment, device 101 comprises a mobile phone. Mobile phones utilizing the global system for mobile communications (GSM) protocol are particularly preferred, such as the Handspring™ Treo™ 270 (Handspring, Inc.; Mountain View, CA). In other embodiments, other protocols may be used, including code division multiple access (CDMA), time division multiple access (TDMA) protocol, and PCS protocols. Other devices suitable for use with the present invention include personal digital assistants (PDA), laptop computers, personal computers, televisions, telephones, and other terminals such as payment stations, point-of-sale stations, cash registers, Automated Teller Machines (ATMs), and related devices.

Generally, device 101 interacts with network server 102. The network server, as used herein, may generally be any device with which device 101 carries out a communication. In a preferred embodiment, network server 102 is an Internet web server with which the device communicates for the manipulation and display of private information as in the case of stock purchases or banking. Any number of transactions, including transfer and analysis of medical data, any other purchases, insurance information, data transfer, or the like. Network server 102 may alternatively represent a cellular base station, another user device (such as another cellular phone, laptop, PDA, etc), or a server machine. Suitable web servers are known in the art and include Apache and Jakarta Tomcat from the Apache Software Foundation (The Apache Software Foundation; Forest Hill, MD), Websphere® from IBM (IBM Corporation; White Plains, NY), Sun™ ONE from Sun Microsystems (Sun Microsystems, Inc; Santa Clara, CA), and Internet Information Server from Microsoft™ (Microsoft Corporation; Redmond, WA).

In a preferred embodiment, a plurality of devices, including device 101, communicate with network server 102. Generally, anywhere from one to millions of devices may advantageously communicate with server 102. The number of devices in communication with server 102 at any time will vary according to user traffic and server capacity.

Networking capability component 103 is integral to device 101 and provides device 101 with its means of connecting to a network, which may be wired or wireless. Component 103 may be, for example, an antenna and associated transmitter and receiver in a cellular phone, or an Ethernet connection for a personal computer. In a preferred embodiment, component 103 represents the antenna, transmitter and receiver of a GSM mobile phone, which allows the phone to communicate with server 102.

Device 101 contains verification processor 104, which is in electronic communication with networking capability component 103, and integral to device 101. Verification processor 104 here generally comprises a CPU and RAM component and provides the device with a general purpose computing capability adequate for the execution of necessary software to support functions described herein, including network communications and the local processing of biometric data. In some embodiments, processor 104 also performs the processing necessary for the transmission of data. In one embodiment, a 33MHz Motorola Dragonball CPU with 16MB RAM in a Handspring Treo 270 GSM cellular phone is sufficient to perform functions described herein, although the particular processor and RAM utilized will vary according to the device and server used, the desired functionality, and the efficiency of the software.

Secure storage module 105 provides device 101 with secure non-volatile data storage. Secure storage module 105 is at least in electronic communication with verification processor 104. In some embodiments, secure storage module 105 is integral to device 101. In other embodiments, secure storage module 105 is integral to smart card or SIM 106, described further below, and brought into electronic communication with verification processor 104 during operation. In still other embodiments, another form a secure storage, such as a separate memory card, may be used.

Data for which protection and security is desired – 'sensitive data', 'sensitive information', or 'secure data' as used herein - is stored in secure storage module 105. Further as used herein, for secure communication between device 101 and network server 102, secure storage module 105 is encoded with data required for communication with network server 102 – such as a private key, in one embodiment. Sensitive information in storage module 105 may only be accessed when unlocked after a biometric data match. That is, secure storage module 105 is in electronic communication with verification processor 104, but verification processor 104 may only access sensitive data within module 105 when the secure data module receives an unlocking signal from an object owned by the authentic user – 'what you have' authentication, as used herein. In a preferred embodiment, that unlocking object is smart card or SIM 106.

In some embodiments, verification processor 104 cannot read or write data to or from secure storage module 105 unless the storage module is unlocked. In other embodiments,

verification processor 104 can write data to storage module 105, but cannot read data from storage module 105 without it being unlocked. In still other embodiments, verification processor 104 can read data from storage module 105, but cannot write data to storage module 105 without it being unlocked.

Sensitive information, that is data stored by module 105 generally may include two types of data – (1) data required for communication with network server 102 including encryption keys (for example, private keys used in asymmetric ciphers, other passwords, codes, and the like; and (2) stored biometric data – that is, reference biometric data which will be compared to a biometric data sample. In another embodiment, data required for communication, such as encryption keys are stored by module 105 while reference biometric data is stored in a separate stored biometric data module. Stored, or 'reference' biometric data may include one or more of the following - biometric templates or other stored biometric data including fingerprint data, voice information, facial feature data, retinal scan information, and the like.

In other embodiments of the invention, secure storage module may contain other personal information including, but not limited to, biographical data including, for example, name, address, age, business data including credit card numbers, credit ratings, insurance policy numbers, medical data – including, for example, genetic data, medical history, blood type, prescription information, etc., bank account numbers and balances, purchasing history, financial portfolio information, stock information, and the like.

Smart Card or SIM 106 provides the device with a "smart card" computing facility such as that of a SIM card used in GSM phones. In one embodiment, smart card 106 contains matching logic 110, capable of performing biometric matching of fingerprint, voice, facial features, and/or other biometric authentication methods. In another embodiment, matching logic 110 is integral to device 101, and secure data storage module 105 resides on smart card 106. Smart card 106 is in electronic communication with, or capable of being brought into electronic communication with, verification processor 104. Further, smart card 106 is capable of being brought into electronic communication with matching logic 110 in embodiments where logic 110 is not resident within smart card 106.

Biometric sensor component 107 provides the device with a means of collecting biometric information from the user of the device 101, such as a fingerprint sensor for fingerprint matching, microphone for voiceprint matching, or camera for facial geometry, retina, or iris matching. A wide variety of sensors are known in the art, such as the Veridicom FPS 200 (Veridicom, Inc.; Sunnyvale, CA) or Atmel Fingerchip™ fingerprint sensors (Atmel Corporation; San Jose, CA), and substantially any sensor capable of recording information about an individual may be employed – those that record blood type, genetic information, and the like. In a preferred embodiment, the biometric sensor is a fingerprint sensor. In a

preferred embodiment, biometric sensor 107 is integrated with or adhered to a surface of device 101. In other embodiments, biometric sensor 107 is electronically coupled to device 101. In some embodiments, a plurality of biometric sensors are provided.

The present invention further provides methods for accessing sensitive information and securely authenticating a user. FIG. 2 illustrates the initiation of a method according to a preferred embodiment of securely authenticating a device's user. Those skilled in the art will readily appreciate that the method can generally be extending to providing secure communications between devices and providing secured access to sensitive data. The authentication procedure generally begins when access to sensitive information is requested, or when secure communication with another device is initiated. A biometric data sample is obtained in step 203 – which may also represent the step of prompting a user to initiate a biometric data sampling activity. Generally, the biometric data sample will be obtained through use of a biometric sensor, described above – including, for example a fingerprint sensor.

For example, a user may be prompted to place or swipe his/her finger over a fingerprint sensor, speak a passphrase into a microphone for voice recognition systems, look into a camera for face recognition, or perform some other data-generating action, thereby generating a raw biometric data sample. A variety of biometrics are known in the art – see for example "A Practical Guide to Biometric Security Technology", Simon Liu and Mark Silverman, IEEE Computer Society, IT Pro - Security, Jan-Feb, 2001, hereby incorporated by reference. In some embodiments, only one such action is required. In other embodiments, two or more such biometric data samples are required – either multiple instances of the same action (two or more fingerprint scans, for example), or a combination of actions (a fingerprint scan and speaking a passphrase, for example).

The device then processes the raw biometric data sample (or samples), such as fingerprint images or audio waveforms, in step 204, to put the samples in a form suitable for submission to match logic 110 for matching. In some embodiments, match logic 110 performs a searching function, where a stored collection of biometric data is searched for a match to the biometric data sample. Processing 204 may include the reduction of the raw biometric data to a biometric template as is well known for various biometric methods. See, for example, A.K. Jain, L. Hong, S. Pankanti and R. Bolle; "An Identity Authentication System Using Fingerprints", *Proc. IEEE Vol. 85, No. 9, pp. 1365-1388, 1997*; D. Maio, D. Maltoni: "Direct Gray-scale Minutiae Detection in Fingerprints", *IEEE Trans. On Pattern Analysis and Machine Intelligence, Vol. 19, No. 1, pp. 27-40, 1997;*and W.M. Campbell and C.C. Broun, *Text-Prompted Speaker Recognition with Polynomial Classifiers*, Motorola Human Interface Laboratory, 2001, all of which are hereby incorporated by reference. Device 101 submits the

biometric data for secure biometric match (or search) by match logic 110 in step 205. Procedures performed by match logic 110 are described further below.

In Fig. 3, match logic 110 returns a match result in step 208 indicating acceptance or rejection of the sampled biometric data against the stored biometric reference template (or set of templates). General methods to establish an acceptable match are well known in the art and include, for example, statistical methods, piecewise linear classifiers, and rule-based methods. See for example, R.O. Duda, P.E. Hart and D. G. Stork, Pattern Classification (2nd Edition), Wiley-Interscience, 2000, incorporated herein by reference. See also A.K. Jain, A. Ross and S. Prabhakar, "Fingerprint Matching Using Minutiae and Texture Features", *Proc. ICIP, Thessaloniki, pp. 282-285, Oct.* 2001, for an example of a fingerprint match algorithm. If the match is accepted, then verification processor 104 requests and retrieves sensitive data from storage module 105 in step 209. In a preferred embodiment, the user's private encryption key and/or other secure local data necessary to complete, sign, and submit information to server 102 is retrieved. The acceptance result is signed, (or a message is signed) using the retrieved sensitive information, and is sent to network server 102 in step 210 notifying the server that the match was accepted. If the match is rejected, then verification processor 104 submits a notification to network server 102 that the match was rejected in step 211. The network server can then use the acceptance or rejection notification to provide or restrict the user's access to information stored on the server, or allow or reject communication with the user as appropriate.

In embodiments where a plurality of biometric data samples are taken, a predetermined number of samples must receive a match before secure data may be accessed.

FIG. 4 is a schematic outline of a biometric matching process according to an embodiment of the present invention – this process will generally be performed by matching logic 110. In a preferred embodiment, the process outlined in Fig. 3 is performed within smart card 106. In other embodiments, the process activity is shared between smart card 106 and components integral to device 101. A biometric data sample (either raw or a processed template) is submitted in step 301. Matching logic 110 then matches, step 302, the submitted data to a reference template stored in secure data storage component 105 – or elsewhere within device 101 or smart card 106. As discussed above, matching procedures are well known for various biometric methods and generally involve determining if the template data of the previously enrolled biometric matches the template data of the recently scanned biometric to within a predetermined tolerance level. If the match is accepted, step 303. then matching logic 110 unlocks secure data storage component 105 in step 304 by issuing an unlocking command, enabling verification processor 104 (or another module of device 101) temporary access to contents of storage component 105 and returns, step 305, an accept result to

verification processor 104. Suitable interfaces for communicating with, and unlocking, secure data storage component 105 will vary according to the embodiment of the component and associated processors and are known in the art, for example, JavaCard™ API (Sun Microsystems, Inc; Santa Clara, CA). If the match is rejected, step 303, then matching logic 110 does not unlock the secure data storage component 105, but rather returns, step 306, a reject result to verification processor 104.

In some embodiments, a user is given another opportunity to provide a biometric sample – such as to take another image of facial features, speak the passphrase again, or take another fingerprint scan if a first match is rejected. In other embodiments, the secure data storage component remains locked for a predetermined period or permanently after a rejected scan, or after a predetermined number of rejected scans.

FIGS. 5-11 depict a variety of physical locations at which a biometric sensor, such as fingerprint sensor 500, may be placed on a mobile phone. These exemplary locations are identified respective of a mobile phone but it will be appreciated that the biometric sensor may be placed on a great variety of physical locations on any device with which the biometric sensor will be used. Fig. 5 displays sensor 500 on front surface 510 of phone 520 along top surface 525. Fig. 6 displays sensor 500 on front surface 510 below keypad 505. Figs. 7 and 8 depict sensor 500 on the right side 403 and left side 406 of phone 520. Figs. 9 and 10 depict two locations of sensor 500 on back surface 550 of mobile phone 520. Sensor 500 may also be located on a battery pack. In some embodiments, as shown in Fig. 11, fingerprint sensor 500 may be embedded within one or more keys – including the ON key or power key - on the keypad 505 itself. Embedding it in the on key may provide for optional and user friendly identity verification at the time of device power-up or wake from a sleep mode. Biometric sensors may generally be placed on or embedded in any input device including mice, pens and wands, for example a Touchpad™ mouse (Synaptics, Inc.; San Jose, CA). Further, a biometric sensor may be placed on or embedded in part of an integrated display or an associated display device. Optionally providing an automatic turn off or deactivation of the biometric sample after some predetermined time may add additional security. In another embodiment, a biometric sensor is embedded in a display screen of a device. In other embodiments, a biometric sensor is not permanently attached to the device, but rather is capable of being brought into electronic communication with the device. That is, an external sensor, such as a camera or other sensor, could plug into the device or communicate with the device through a wireless interface. For example, an add-on keyboard comprising a biometric sensor may plug into the device, in one embodiment. In another embodiment, a network card or memory card for use in the device comprises a biometric sensor. In another embodiment, a biometric sensor is in wireless communication with the device through known protocols such as, for example, BlueTooth.

The invention may advantageously implement the methods and procedures described herein on a general purpose or special purpose computing device, such as a device having a processor for executing computer program code instructions and a memory coupled to the processor for storing data and/or commands. It will be appreciated that the computing device may be a single computer or a plurality of networked computers and that the several procedures associated with implementing the methods and procedures described herein may be implemented on one or a plurality of computing devices. In some embodiments the inventive procedures and methods are implemented on standard server-client network infrastructures with the inventive features added on top of such infrastructure or compatible therewith.

Those skilled in the art will readily appreciate that the inventive concepts described herein are readily applicable and operable in a variety of communications devices to secure transactions and sensitive data. The examples provided above are intended to be instructive and illustrative and are not intended to limit the invention to a specific embodiment, device, or data type described. Further, a variety of implementations are possible placing certain functions or groups of functions on the 'what you have' authentication object – such as a smart card. Generally, the methods and devices described herein require some function or data to be performed within or stored on a 'what you have' authentication object. Examples of those functions and data are given, but are not intended to be limiting.

We claim:

1. A method for secure communication with a server, wherein said secure communication requires encryption information, said method comprising:

obtaining a biometric data sample;

comparing said biometric data sample to stored biometric data;

enabling access to said sensitive data if said biometric data sample matches said stored biometric data; and

communicating with said server using said sensitive data.

2. A method according to claim 1, wherein said secure communication comprises communicating message information, said communicating step further comprising encrypting said message information using said sensitive data.

3. A method according to claim 1, wherein said obtaining comprises processing a fingerprint scan.

4. A method according to claim 1, wherein said obtaining comprises processing an image.

5. A method according to claim 4, wherein said image is a facial image.

6. A method according to claim 1, wherein said obtaining comprises processing a speech sample.

7. A method according to claim 1, wherein said sensitive data includes a private encryption key.

8. A method according to claim 1, further comprising processing said biometric data sample.

9. A method for secure communication between a server and mobile device comprising:

obtaining a biometric data sample;

comparing said biometric data sample to stored biometric data;

transmitting acceptance result to said server if said biometric data sample matches said stored biometric data.

10. A device for securely communicating with a server, said device comprising:

a biometric sensor;

a secure data storage module containing stored biometric data and sensitive data required for communication with said server, in electronic communication with said biometric sensor;

matching logic in electronic communication with said sensor and said biometric data memory; and

a verification processor in electronic communication with said matching logic and said secure data storage module.

11. The device of claim 10, wherein said matching logic is provided on a SIM card.

12. The device of claim 10, wherein said matching logic is provided on a smart card.

13. The device of claim 10, wherein said verification processor is provided within a cellular phone.

14. The device of claim 13, wherein said biometric sensor is on a front surface of said cellular phone.

15. The device of claim 13, wherein said biometric sensor is on a rear surface of said cellular phone.

16. The device of claim 13, wherein said biometric sensor is below a keypad on a surface of said cellular phone.

17. The device of claim 13, wherein said biometric sensor is on a side surface of said cellular phone.

18. The device of claim 13, wherein said biometric sensor is embedded in a key on said cellular phone.

19. The device of claim 18, wherein said key is an ON key.

20. A device according to claim 10, further comprising an input device associated with said verification processor and wherein said biometric sensor is located on said input device.

21. A device according to claim 10, further comprising a display device associated with said verification processor and wherein said biometric sensor is located on said display device.

22. A device according to claim 10, wherein said verification processor is provided within a personal digital assistant.

23. A computer program product comprising a computer-readable memory encoded with an instruction set that when executed:

processes a biometric data sample;

compares said biometric data sample with stored biometric data;

enables access to sensitive data if said biometric data sample matches said stored biometric data; and

transmits an acceptance result.

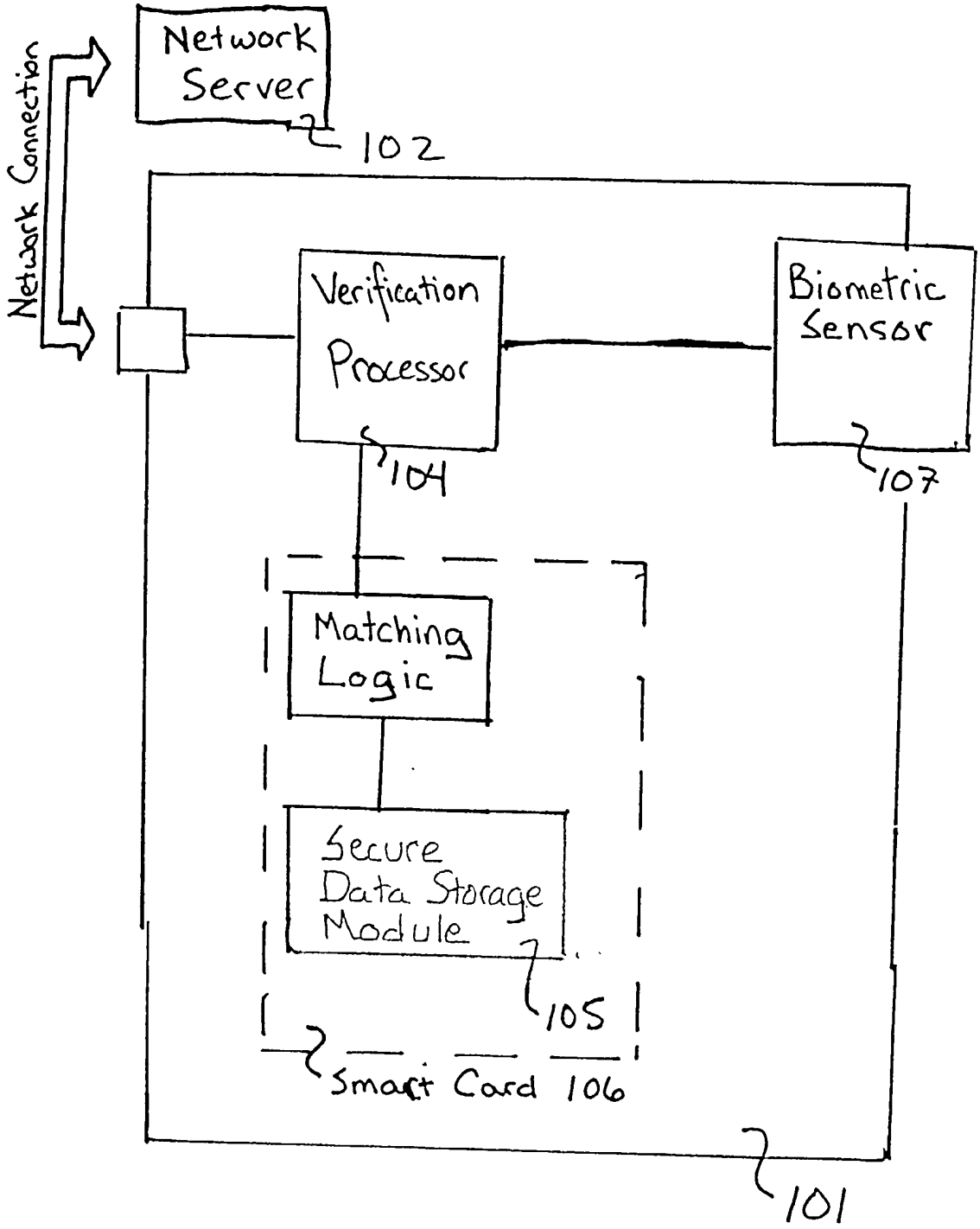
Network Server
102
Network Connection
Verification Processor
104
Biometric Sensor
107
Matching Logic
Secure Data Storage Module
105
Smart Card 106
101

FIG. 1

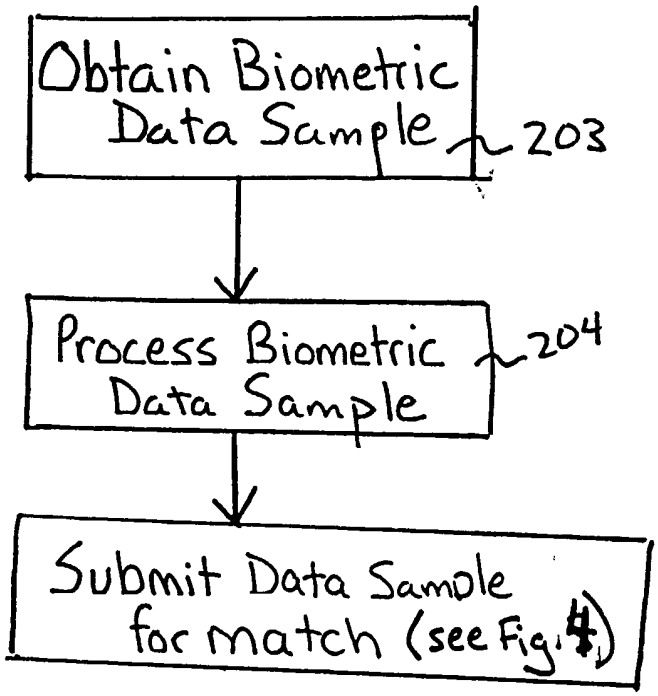
Obtain Biometric Data Sample
203
Process Biometric Data Sample
204
Submit Data Samole for match (see Fig. 4)

FIG. 2

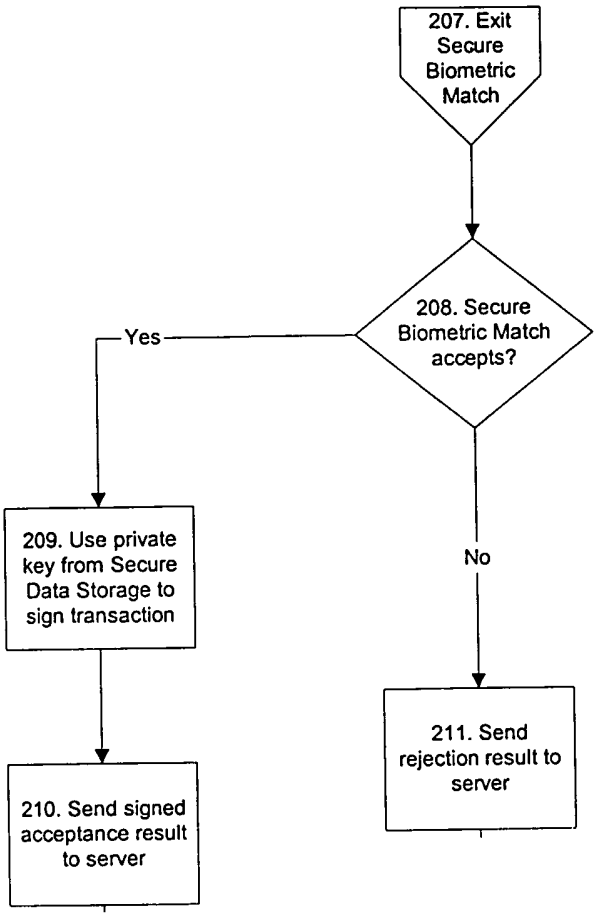
207. Exit Secure Biometric Match
208. Secure Biometric Match accepts?
Yes
No
209. Use private key from Secure Data Storage to sign transaction
210. Send signed acceptance result to server
211. Send rejection result to server

FIG. 3

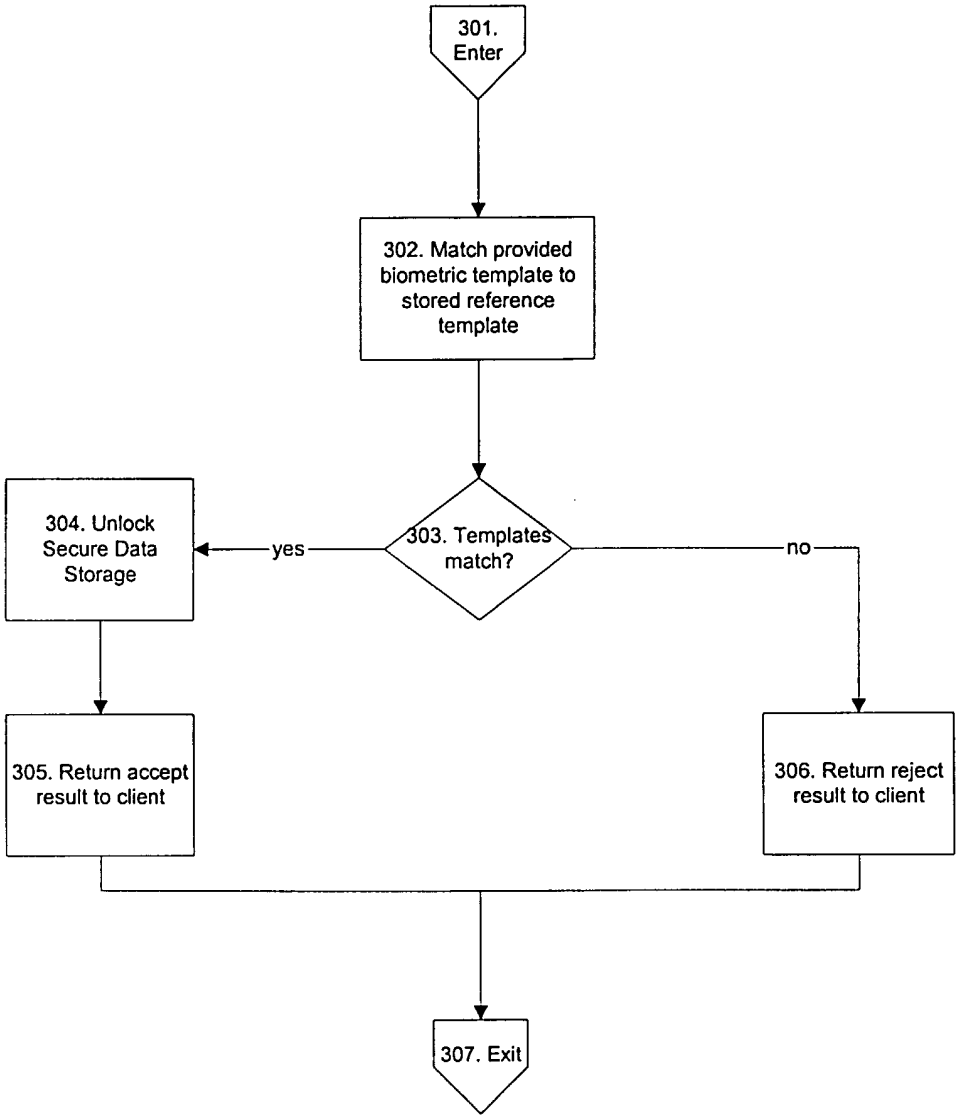
301. Enter
302. Match provided biometric template to stored reference template
303. Templates match?
yes
no
304. Unlock Secure Data Storage
305. Return accept result to client
306. Return reject result to client
307. Exit

FIG. 4

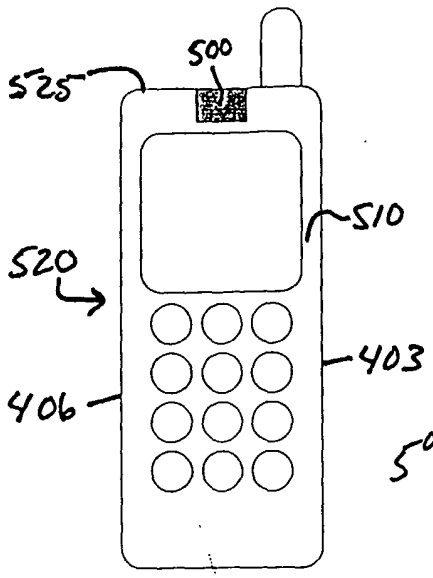

FIG. 5

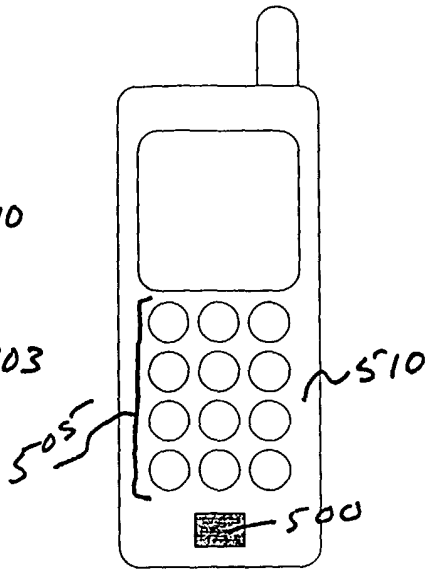

FIG. 6

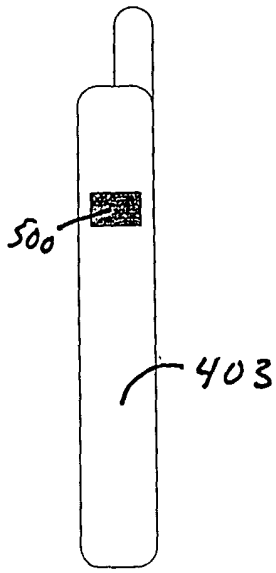

FIG. 7

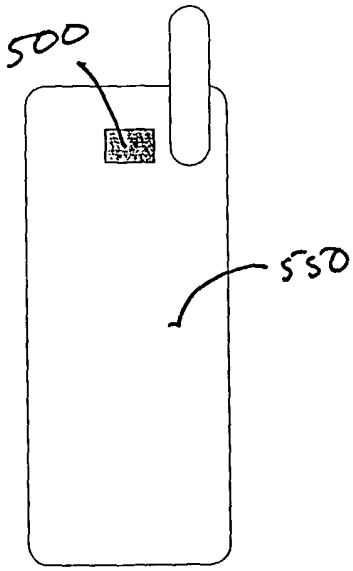

FIG. 10

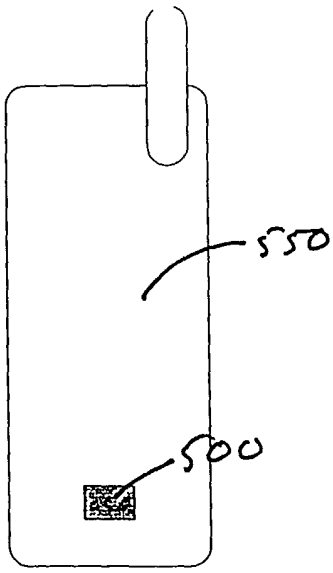

FIG. 9

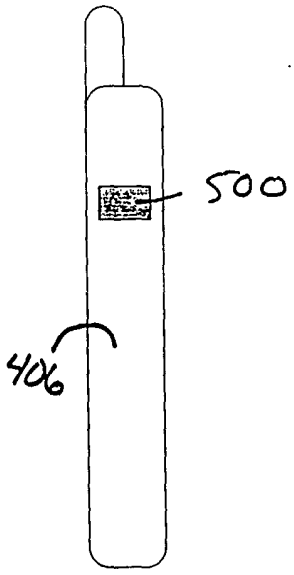

FIG. 8

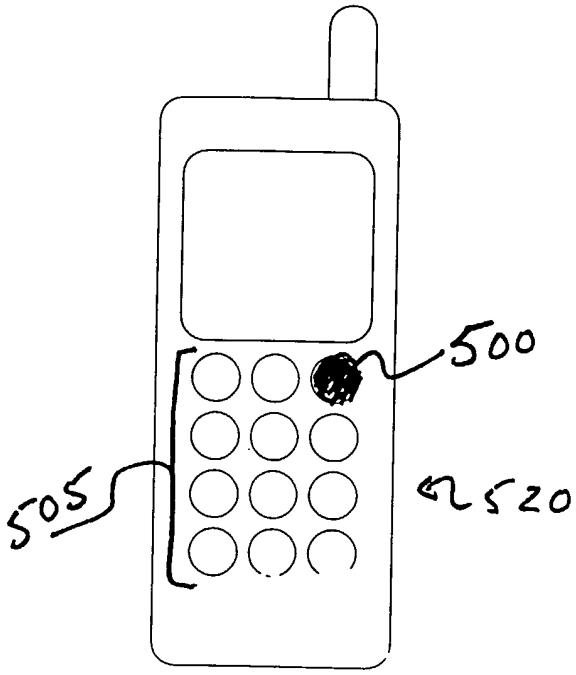

FIG. 11