US 20020174344A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2002/0174344 A1

Ting (43) Pub. Date: Nov. 21, 2002

(54) SYSTEM AND METHOD FOR AUTHENTICATION USING BIOMETRICS

(75) Inventor: **David M. T. Ting**, Sudbury, MA (US)

Correspondence Address:
TESTA, HURWITZ & THIBEAULT, LLP
HIGH STREET TOWER
125 HIGH STREET
BOSTON, MA 02110 (US)

(73) Assignee: **Imprivata, Inc.**, Lexington, MA (US)

(21) Appl. No.: **10/147,788**

(22) Filed: **May 17, 2002**

Related U.S. Application Data

(60) Provisional application No. 60/291,900, filed on May 18, 2001.

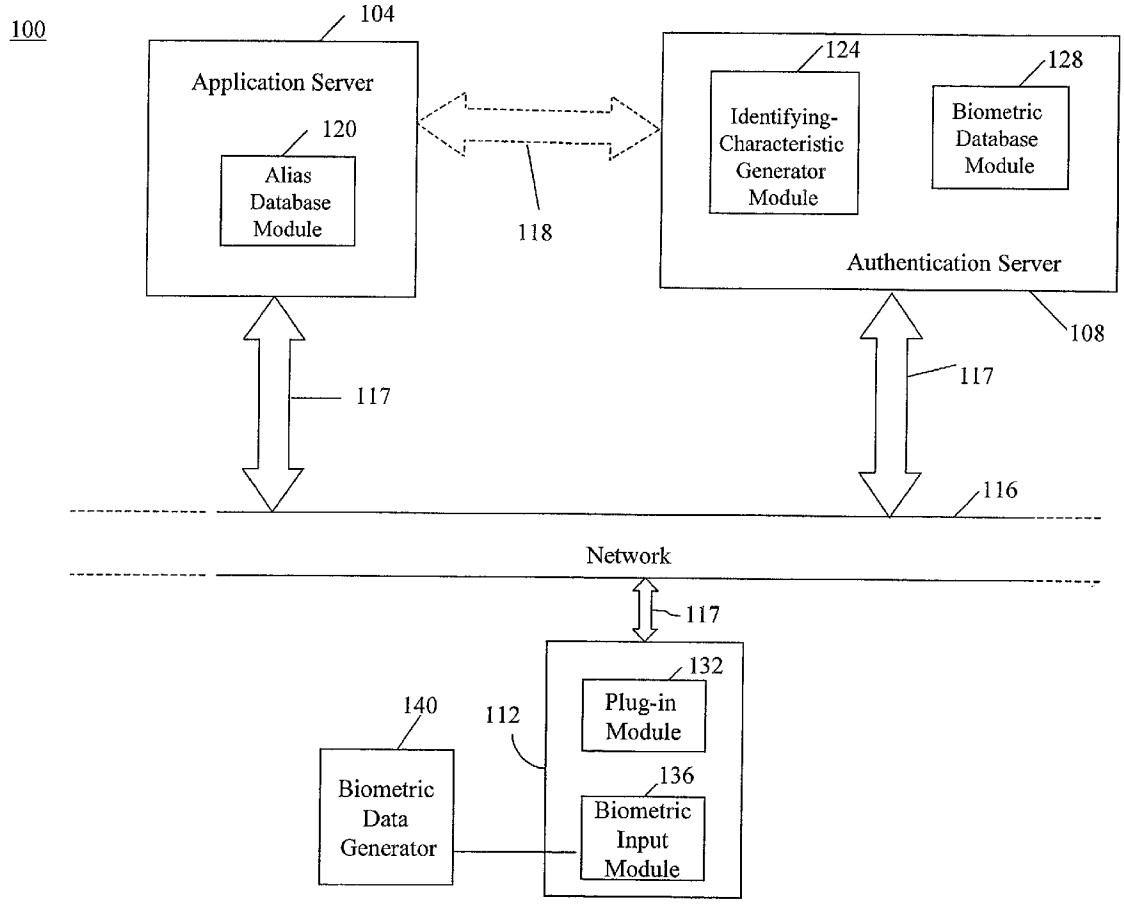
Publication Classification

(51) **Int. Cl.**[7] **H04K 1/00**

(52) **U.S. Cl.** **713/185**

(57) **ABSTRACT**

In one aspect the invention relates to authentication using biometrics. An alias for an individual is associated with a reference set of biometric data from the individual and, at a location separate from the reference set of biometric data, information associating the individual with the alias is stored. The invention may operate on an authentication request requesting authentication of a user identified by the alias, along with a candidate set of biometric data from the user and confirming authentication of the user as the registered individual; authentication is granted if the candidate set of biometric data sufficiently matches the reference set of biometric data.



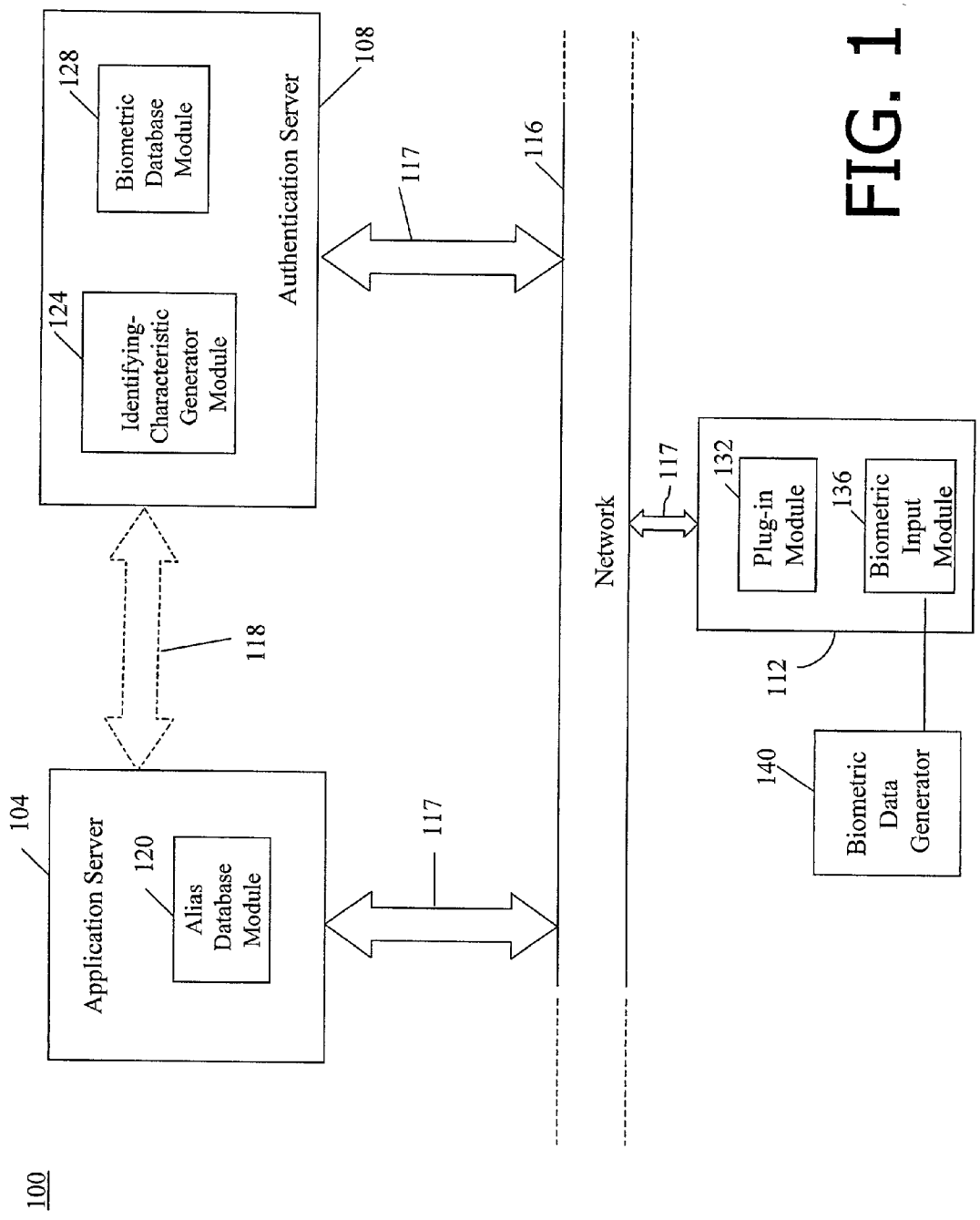

100
104
Application Server
120
Alias Database Module
118
108
Authentication Server
128
Biometric Database Module
124
Identifying-Characteristic Generator Module
117
116
Network
117
112
132
Plug-in Module
136
Biometric Input Module
140
Biometric Data Generator

FIG. 1

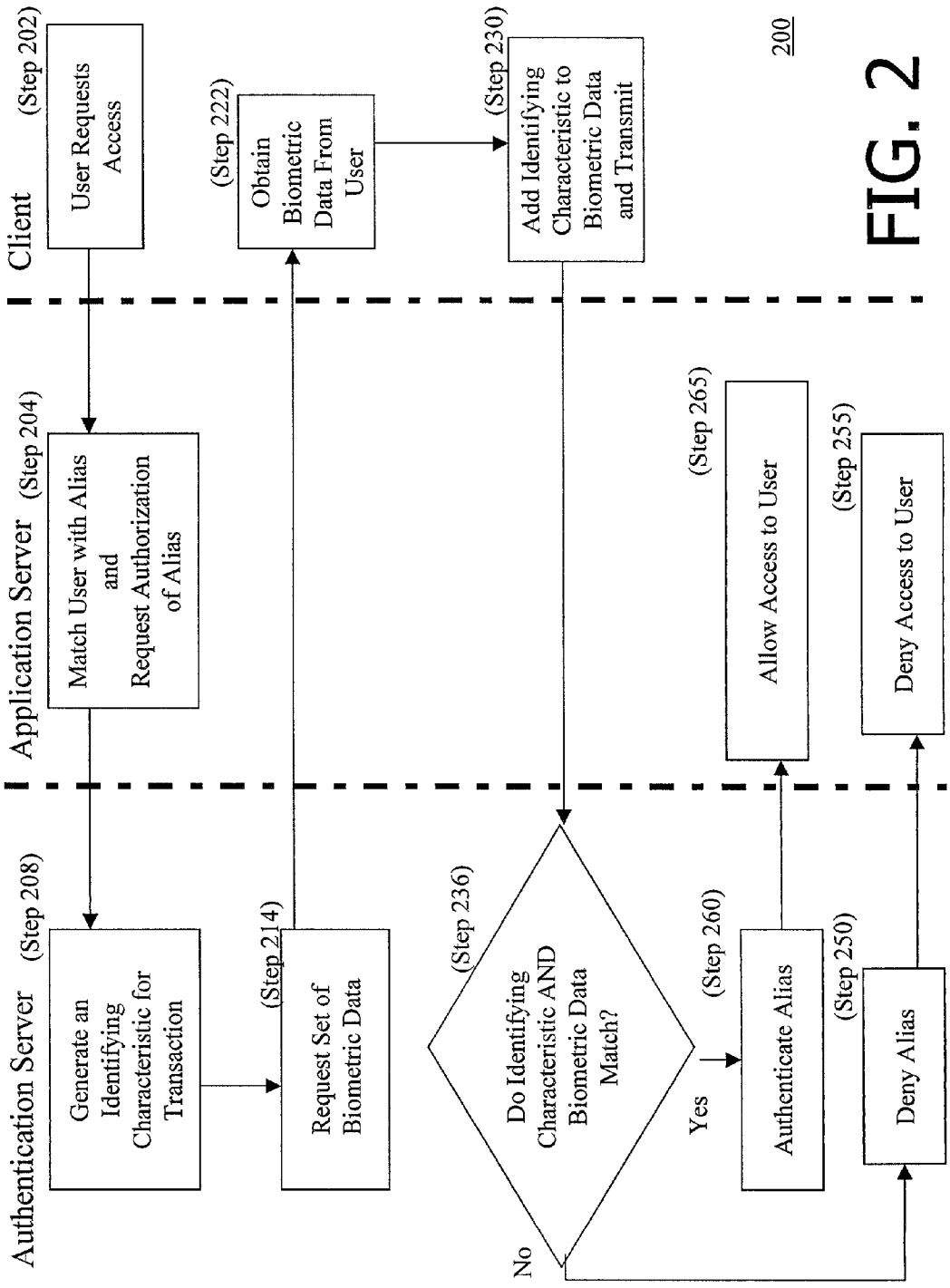

Client
Application Server
Authentication Server
User Requests Access
(Step 202)
Match User with Alias and Request Authorization of Alias
(Step 204)
Generate an Identifying Characteristic for Transaction
(Step 208)
Request Set of Biometric Data
(Step 214)
Obtain Biometric Data From User
(Step 222)
Add Identifying Characteristic to Biometric Data and Transmit
(Step 230)
Do Identifying Characteristic AND Biometric Data Match?
(Step 236)
Yes
No
Authenticate Alias
(Step 260)
Allow Access to User
(Step 265)
Deny Alias
(Step 250)
Deny Access to User
(Step 255)
200

FIG. 2

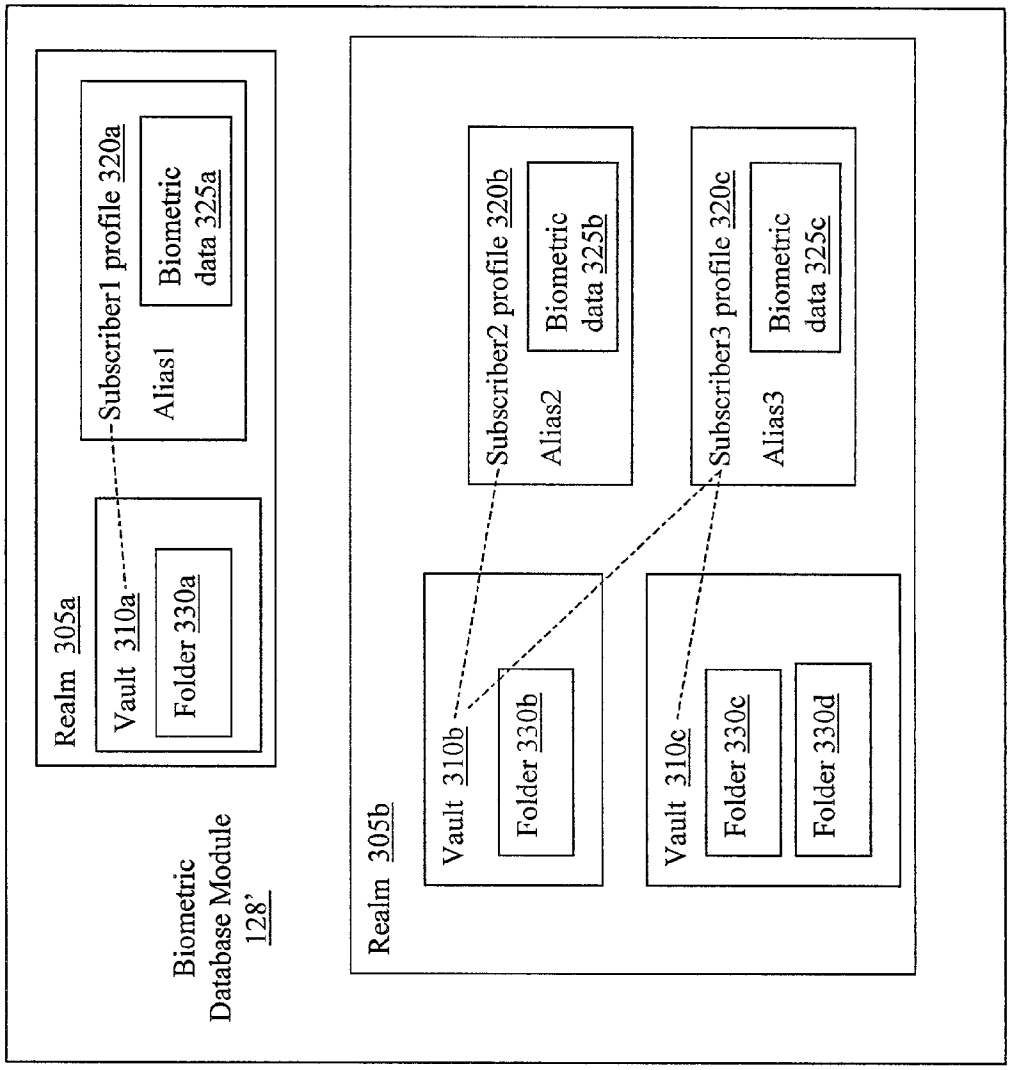

Realm 305a
Vault 310a
Folder 330a
Subscriber1 profile 320a
Alias1
Biometric data 325a
Biometric Database Module 128'
Realm 305b
Vault 310b
Folder 330b
Subscriber2 profile 320b
Alias2
Biometric data 325b
Vault 310c
Folder 330c
Folder 330d
Subscriber3 profile 320c
Alias3
Biometric data 325c
Alias Database Module 120'
300

FIG. 3

SYSTEM AND METHOD FOR AUTHENTICATION USING BIOMETRICS

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of and priority to the co-pending U.S. Provisional Application, Serial No. 60/291,900, filed May 18, 2001, entitled "Network-Based Biometric Authentication," the entirety of which is incorporated herein by reference.

FIELD OF INVENTION

[0002] The invention relates generally to biometrics. More specifically, in one embodiment, the invention relates to systems and methods for using biometric authentication over a network.

BACKGROUND

[0003] The Internet accords a global community of computer users access to applications and information that traditionally were highly restricted. For example, users can now undertake a wide variety of financial transactions online, or obtain access to financial and other sensitive records online. The increased accessibility of such information, while enormously convenient, jeopardizes privacy and invites tampering and electronic theft. In some known prior art systems, sensitive information that was once physically guarded can now be obtained on the Internet by anyone who can generate the correct server URL, logon and password.

[0004] Indeed, the mere need for Internet users to keep track of multiple URLs, logon names, passwords and PINs in order to access different information further increases the chances of unauthorized use and loss of private information. Users may resort to using the same logon name and password combinations for all accounts, rendering them equally vulnerable if unauthorized access to a single account is obtained. On the other hand, security-conscious users who maintain different logon names and passwords for individual accounts may, to avoid confusion, write them down where they may be found or store them on easily stolen devices such as personal digital assistants—thereby undermining their own efforts. It can be argued that those who routinely change their passwords but record them on paper or in a computer file are at greater risk of being compromised than those who use a single but difficult-to-crack password. At the very least, such security-conscious individuals risk forgetting their access information, necessitating time-consuming calls to customer-support lines.

[0005] From the perspective of authentication, passwords and PINs cannot guarantee identity; the identification is no more reliable than the security of the password. In some known prior art systems with password authentication, the server carrying out a transaction can only prove that the correct password was entered—not that it was entered by an authorized person. A password can originate from password-cracking software just as easily as from the real user. Digital certificates improve security by authenticating an end point (i.e., that a message originated with a particular client terminal), but cannot create a non-repudiated link to support the claim that a particular user really did engage in a transaction.

SUMMARY OF THE INVENTION

[0006] The present invention utilizes biometric indicia to offer highly reliable authentication that creates links that cannot be repudiated for transactions initiated within the context of an authenticated session. Unlike passwords, which are no more than secrets vulnerable to theft, biometrics validation matches physical characteristics of the user against stored characteristics to identify the user. Once a user is positively identified, in one embodiment, the server unlocks and validates the user's credentials for presentation to other servers that request such authentication. A user's credentials may, for example, represent an account login/password combination or X.509 certificate. This biometric approach offers substantial flexibility in terms of accessibility (from computers, mobile devices, etc.) and relieves the user from responsibility for managing the integrity of such credentials. Biometric scanners are inexpensive and small, and may, for example, be easily incorporated into keyboards and mobile client devices.

[0007] In one aspect the invention relates to a method for authentication using biometrics. The method comprises associating an alias for an individual with a reference set of biometric data from the individual and storing, at a location separate from the reference set of biometric data, information associating the individual with the alias. The method also comprises receiving an authentication request requesting authentication of a user identified by the alias, receiving a candidate set of biometric data from the user and confirming authentication of the user as the registered individual, if the candidate set of biometric data sufficiently matches the reference set of biometric data. In one embodiment, the method further comprises transmitting to the user a data request for the candidate set of biometric data, the data request including an identifying characteristic, wherein the confirming step comprises, confirming to the application server authentication of the user as the registered individual, if the candidate set of biometric data includes the identifying characteristic and sufficiently matches the reference set of biometric data.

[0008] In another embodiment, the method further comprises generating the identifying characteristic including a public key, generating a private key corresponding to the public key and encrypting the data request using the private key. In another embodiment, the method further comprises generating the identifying characteristic having a limited validity lifetime. In another embodiment, the method further comprises generating the identifying characteristic including a random identifier. In another embodiment, the method further comprises generating the identifying characteristic including a time identifier. In another embodiment, the method further comprises destroying the identifying characteristic after completion of the confirming step.

[0009] In another embodiment, the method further comprises updating the reference set of biometric data using the candidate set of biometric data, if authentication of the user is confirmed. In another embodiment, the method further comprises transmitting, by a first server, the authentication request to a second server, wherein the second server performs the confirming step. In another embodiment, the method further comprises encrypting the reference set of biometric data using a predetermined function based at least in part on the alias. In another embodiment, the method

further comprises morphing the reference set of biometric data using a predetermined function based at least in part on the alias. In another embodiment, the method further comprises encrypting the reference set of biometric data using a second function based at least in part on the alias, if security is compromised. In another embodiment, the method further comprises morphing the reference set of biometric data using a second function based at least in part on the alias, if security is compromised.

[0010] In another embodiment, the invention relates to a system for authentication using biometrics. The system includes an application server and an authentication server. The application server includes an alias database module configured to store information associating an individual with an alias. The authentication server includes a biometric database, a transceiver module and a comparison module. The biometric database module associates the alias for the individual with a reference set of biometric data from the individual. The transceiver module is configured to i) receive an authentication request requesting authentication of a user identified by the alias and ii) to receive a candidate set of biometric data from the user. The comparison module is configured to determine if the candidate set of biometric data sufficiently matches the reference set of biometric data and, if so, to generate a confirmation of authentication of the user as the registered individual.

[0011] In one embodiment, the application server further comprises a transceiver module configured to transmit an authentication request requesting authentication of a user identified by the alias, where the application server is in communication with the authentication server over a network. In another embodiment, the authentication server further comprises an identifying characteristic generator module configured to generate an identifying characteristic to be transmitted with a user data request for the candidate set of biometric data, wherein the comparison module is further configured to determine if the candidate set of biometric data includes the identifying characteristic. In another embodiment, the identifying characteristic generator module is further configured to generate the identifying characteristic including a public key, to generating a private key corresponding to the public key, and to encrypt the user data request using the private key.

[0012] In another embodiment, the identifying characteristic generator module is further configured to generate the identifying characteristic having a limited validity lifetime. In another embodiment, the identifying characteristic generator module is further configured to generate the identifying characteristic including a random identifier. In another embodiment, the identifying characteristic generator module is further configured to generate the identifying characteristic including a time identifier. In another embodiment, the identifying characteristic generator module is further configured to destroy the identifying characteristic after completion of the confirming step.

[0013] In another embodiment, the biometric database module is further configured to update, if authentication of the user is confirmed, the reference set of biometric data using the candidate set of biometric data. In another embodiment, the biometric database module is further configured to encrypt the reference set of biometric data using a predetermined function based at least in part on the alias. In another embodiment, the biometric database module is further configured to morph the reference set of biometric data using a predetermined function based at least in part on the alias. In another embodiment, the biometric database module is further configured to encrypt, if security is compromised, the reference set of biometric data using a second function based at least in part on the alias. In another embodiment, the biometric database module is further configured to morph, if security is compromised, the reference set of biometric data using a second function based at least in part on the alias. In another embodiment, the system further comprises a client. The client includes a plug-in configured to receive a request for the candidate set of biometric data, to obtain the candidate set of biometric data for the user of the client and to transmit the candidate set of biometric data in response to the request.

[0014] In another aspect, the invention relates to a method of organizing authentication information within a storage space. The method comprises partitioning the storage space into a plurality of realms, each realm containing a set of subscriber profiles, each subscriber profile comprising an alias associated with a respective subscriber and a reference set of biometric data from that respective subscriber and storing, at a location separate from the storage space, information associating the identity of the alias with the respective subscriber. The method also includes partitioning each realm into a plurality of vaults and associating each subscriber with at least one vault. The method also includes partitioning each vault into at least one folder, each folder containing protected data and being accessible only to one or more subscribers associated with the vault and according access to the vault and the folders therein only upon presentation of i) the alias of a subscriber associated with the vault and ii) a candidate set of biometric data sufficiently matching the reference set of the biometric data corresponding to the alias. In one embodiment, the method further comprises transmitting a data request for the candidate set of biometric data, the data request including an identifying characteristic, wherein the according access step comprises according access to the vault and the folders therein only upon presentation of i) the alias of a subscriber associated with the vault, ii) the identifying characteristic and iii) a candidate set of biometric data sufficiently matching the reference set of the biometric data corresponding to the alias.

[0015] In another aspect, the invention relates to an article of manufacture having computer-readable program portions embodied therein for authentication using biometrics. The article comprises computer-readable program portions for performing the method steps as described above.

BRIEF DESCRIPTION OF THE DRAWINGS

[0016] The above and further advantages of the invention may be better understood by referring to the following description taken in conjunction with the accompanying drawing, in which:

[0017] **FIG. 1** is a block diagram of an illustrative embodiment of a system to authenticate a user using biometrics in accordance with the invention;

[0018] **FIG. 2** is a flow diagram of an illustrative embodiment of a process to authenticate a user using biometrics in accordance with the invention; and

[0019] **FIG. 3** is a block diagram of a data structure used to authenticate a user using biometrics in accordance with the invention.

DETAILED DESCRIPTION

[0020] In broad overview, **FIG. 1** illustrates an embodiment of a system **100** to authenticate a user using biometrics in accordance with the invention. The system **100** includes a first computing system ("a first server node") **104**, a second computing system ("a second server node") **108** and a third computing system ("a client node") **112**, all in communication with a network **116**. The first server node **104**, the second server node **108** and the client node **112** are in communication with the network using communication channels **117**. Also shown is an optional communication channel **118** over which the first server node **104** and the second server node **108** can communicate with each other, instead of or in addition to communicating via the network **116**.

[0021] For example, the network **116** and the communication channels **117** and **118** can be part of a local-area network (LAN), such as a company Intranet, a wide area network (WAN) such as the Internet or the World Wide Web or the like. The nodes **104**, **108** and **112** communicate with the network **116** through the communication channels **117** and **118** using any of a variety of connections including, for example, standard telephone lines, LAN or WAN links (e.g., T1, T3, 56 kb, X.25), broadband connections (ISDN, Frame Relay, ATM), wireless connections and the like. The connections can be established using a variety of communication protocols (e.g., HTTP(S), TCP/IP, SSL, IPX, SPX, NetBIOS, Ethernet, RS232, direct asynchronous connections, a proprietary protocol and the like). In one embodiment, the servers **104** and **108** and the client **112** encrypt all communication when communicating with each other.

[0022] Each of the server nodes **104** and **108** can be any computing device capable of providing the services requested by the other server or by the client node **112**. Particularly, this includes authenticating a user at the client node **112** using biometric data, as described in more detail below. The first server node **104**, also referred to as an application server **104**, includes an alias database module **120**. The second server node **108**, also referred to as an authentication server **108**, includes an identifying-characteristic generator module **124** and a biometric database module **128**. The modules throughout the specification are implemented as a software program and/or a hardware device (e.g., ASIC, FPGA, processor, memory, storage and the like).

[0023] For clarity, **FIG. 1** depicts server node **104** as an entity separate and distinct from server node **108** and each node is in communication with the network **116**, representing that the two nodes **104** and **108** are logically independent. It is to be understood, however, that the server nodes **104** and **108** can also be implemented, for example, on a single server (e.g., as logically distinct modules), distributed on portions of several (i.e., more than two) servers, and/or as part of a single server node or server farm in communication with the network **116** through, for example, a single Web server (not shown). It should be understood that even if two logical servers are running in the same physical machine, they may be secured logically if any of the following conditions is met: (1) the servers run in different process spaces (so there is no possibility for one process to access the memory of another process); (2) the servers access different logical databases (which may be further partitioned) with different credential or entry requirements; (3) sensitive data in the server node **104** and the server node **108** are encrypted using separate encryption keys; or (4) the server applications are launched (e.g., in a Unix environment) under two different logon accounts. For heightened security, it is possible to encrypt all the data used by the server node **108** using a key maintained by the server node **104** or an external key server; this approach enhances security in that a breach of the of the sever node **108** and its database would yield only encrypted data.

[0024] The client node **112** can be any computing device (e.g., a personal computer, set top box, wireless mobile phone, handheld device, personal digital assistant, kiosk, etc) used to provide a user interface to access the application server **104**. The client node **112** includes a plug-in module **132** and a biometric input module **136**.

[0025] To use the system **100**, a user, also referred to as a subscriber, registers that user's biometric data with the system **100**. The biometric data can include, for example, data associated with the individual's fingerprint(s), facial characteristics, voice and the like. The system **100** stores data identifying the user to the system (e.g., username, logon ID, employee ID and the like) in the alias database module **120**. The alias database **120** associates an alias with that stored data. For example, employee #2054 may be associated with the alias 25xHy63. The alias database **120** transmits this associated alias to the plug-in module **126** in the client node **112**.

[0026] In the illustrated embodiment, the plug-in **132** communicates with the biometric input module **136** to obtain biometric data from a biometric device **140**, for example, a fingerprint reader associated with the client **112**. The plug-in **132** transmits the stored alias (previously received from the application server **104**) and the corresponding biometric data to the authentication server **108**, which stores the alias and reference set of biometric data in the biometric database module **128**. There are security measures that the system **100** can use to ensure that a listening device does not capture this reference biometric data, or if the data is captured, that it is not usable by itself. For example, the client **112** can belong to an administrator, with a direct, secure communication channel to the biometric database **128**; the plug-in **132** can encrypt the alias and the biometric data independently; the plug-in **132** and the biometric database **128** can communicate with each other using SSL and/or public and private keys; and the plug-in **132** can transmit the alias and the biometric data independently to the biometric database **128**.

[0027] The registration process can be initiated in several different ways. The administrator may initiate the registration. The administrator can have the user come to the administrator's client **112** or a secure client **112** used only for registration when the employee starts work, when a customer purchases services accessible via the application server **104**, and the like. The application server **104** can initiate the registration when the user first requests a service from the application server **104** requiring authentication of the user. The client **112** can display a graphical user interface

("GUI") leading the user through the registration process. The level of authentication of the user at registration is based on the administrators of the system **100** and can range, for example, from a user presenting the correct password to the application server **104** to a user being present in person in front of an administrator who can check the identification of the user.

[**0028**] Once the system **100** registers an individual, the system **100** creates an association between the data identifying the user to the system and the user's alias in the alias database **120**, and an association between the user's alias and the user's biometric data in the biometric database **128**. Storing the two associations at locations separate from each other requires a breach in security of both the alias database **120** and the biometric database **128** to put biometric data together with some identifying data. Further, if the identifying data is just another unique identifier that does not reveal identity by itself, for example an employee number, then the security of a third database containing the association between the employee number and the identity (e.g., name and address of the employee) would have to be breached to match the identity of the user with that individual's biometric data.

[**0029**] With an individual registered (i.e., with user-identifying information, an alias, and biometric information obtained and stored), a process **200** as shown in **FIG. 2** may be used to authenticate a user using biometric data and a system as depicted, for example, in **FIG. 1**. The user of the client **112** requests (step **202**) access to a service (e.g., execution of an application program, access to a financial or medical database, access to an electronic vault with which the user is associated, download of data and/or application program and the like) provided by the application server **104**. The application server **104** uses data identifying the user to the system (e.g., username, logon ID, employee ID and the like) and queries the alias database module **120** for a match. Upon matching (step **204**) the data, the application server **104** retrieves the associated alias and transmits (step **204**) a request for authentication to the authentication server **108**, including the alias with the request. The application server **104** can transmit this request via the network **116** or via the backend connection **118**. The authentication server **108** receives the request for authentication for the retrieved alias.

[**0030**] In response to the request for authentication, the identifying-characteristic generator module **124** ("ID generator") generates (step **208**) an identifying characteristic, also referred to as a session code, to identify this particular transaction/session (e.g., response to the authentication request). In addition to identifying a particular session, the identifying characteristic also prevents someone who captures the biometric data from using the captured data in a subsequent transaction. By combining the identifying characteristic with the biometric data, as described below, any captured data is rendered unusable in subsequent transactions because the ID generator **124** generates a new identifying characteristic for each transaction.

[**0031**] Generating an identifying characteristic can be accomplished in various ways to identify a particular transaction/session. For example, the identifying-characteristic generator **124** can generate a random and/or unique identifier, for example a random alphanumeric ID that is temporarily associated with the transaction; or the ID generator **124** can generate a time identifier, for example a date/time stamp; or it can generate a time limit ID, after which the ID is destroyed and deemed void. Either the time limit ID or the time identifier allows the identifying characteristic to have a limited lifetime during which the identifying characteristic is valid. Regardless of the type of identifying characteristic used, it is generally destroyed after the transaction is complete (e.g., after the authentication server **108** responds to the application server **104** with a decision regarding authentication).

[**0032**] In one embodiment, the ID generator **124** generates a private/public key pair for use with a particular transaction. The authentication server **108** will use this single-use private/public key pair to encrypt a request for a candidate set of biometric data, as described below. First, however, the authentication server **108** generates the request, which includes any parameters needed by the plug-in module **132** to fulfill the request. For example, if the authentication server **108** only has fingerprint data for a single digit for the particular alias, the authentication request includes a request for that particular digit, so that the proper digit is read at the client **112**.

[**0033**] The authentication server **108** incorporates the identifying characteristic and any needed parameters into the request. The authentication server **108** encrypts the request using a symmetric secret key that is understood only by the client **112**, and signs the digest for the message with the private key of the single-use private/public key pair for the particular transaction. The authentication server **108** also includes with the request the public key of the single-use private/public key pair. With the request complete, the authentication server **108** transmits (step **214**) the request to the client **112**. The authentication server **108** can transmit the request directly to the client **112**. Alternatively, the authentication server **108** can transmit the request, for example, through the application server **104**, using the existing session created when the user requested (step **202**) a service from the application server **104**. This transmission can also include encrypting the request using a second public/private key pair established between application server **104** and the client **112**. With this further encryption, the client **112** ensures that the request has not been altered in transit and/or is from a trusted source.

[**0034**] The plug-in module **112** receives the request for a candidate set of biometric data. Using the public key received with the request, the plug-in **132** verifies that the signature of the request is authentic (i.e., that it was signed using the private key of the single-use private/public key pair generated by the ID generator **124**). The plug-in **132** decrypts the request using its own secret key to obtain any needed parameters included therewith. In one embodiment, a portion of the request including the identifying characteristic remains encrypted and undecipherable by the plug-in **132**. For example, in one embodiment if the session code is a random alphanumeric string and there is no reason for the client **112** to decipher this code because the client **112** does not use it, the client **112** simply has to retransmit the encrypted identifying characteristic back to the authentication server **108** with the candidate set of biometric data.

[**0035**] In response to the request, the plug-in **132** obtains (step **222**) the biometric data from the user using the

biometric data generator **140**, for example, a fingerprint scanner. In one embodiment, the plug-in **132** includes the drivers needed to directly interact with the biometric data generator **140**. The plug-in **132** adds (step **230**) the identifying characteristic, whether encrypted or not, to the biometric data and transmits (step **230**) this combination back to the authentication server **108**. In one embodiment, the plug-in **132** encrypts the combination using the received public key. For example, in one approach, the plug-in **132** generates a symmetric key to encrypt the message, encrypts the symmetric key with the public key, and sends the encrypted message to the application server **104**; upon receiving the message, the server **104** utilizes the corresponding private key to decrypt the symmetric key, which it then uses to decrypt the message. In another embodiment, the plug-in **132** transmits (step **230**) this combination back to the application server **104**, where the application server **104** manages all communication to and from the authentication server **108**.

[**0036**] The authentication server **108** receives the combination of the identifying characteristic and the candidate set of biometric data. The authentication server **108** decrypts the received combination and extracts the identifying characteristic. The authentication server **108** thereupon decrypts this portion further if needed. The authentication server **108** verifies (step **236**) that the received identifying characteristic matches the identifying characteristic previously generated by the ID generator **124**. If the identifying characteristic includes a limited lifetime validity, the authentication server **108** verifies (step **236**) that the lifetime has not expired. If the identifying characteristic does not match or the lifetime has expired, the authentication server **108** responds to the request (step **202**) from the application server **104** by denying (step **250**) authentication of the alias associated with that request. In response to the rejection (step **250**), the application server **104** denies (step **255**) access to the user associated with the alias for the requested (step **202**) service.

[**0037**] If the identifying characteristic matches and the lifetime has not expired, the authentication server **108** verifies (step **236**) that the candidate set of biometric data received from the client **117** sufficiently matches the reference set of biometric data stored in the biometric database **128** record associated with the alias. The authentication server **108** may determine the sufficiency of the match by statistically analyzing the two sets of biometric data and determining whether the probability that they come from the same individual is above a certain predetermined threshold. In one embodiment, an administrator of the system **100** sets the predetermined threshold. The predetermined threshold determines both the false acceptance rate (i.e., the probability that the authentication server **108** will incorrectly authenticate a user) and the false rejection rate (i.e., the probability that the authentication server **108** will incorrectly reject authentication of the user when that user is in fact the registered individual). The administrator sets the predetermined threshold such that the false acceptance rate and the false rejection rate are both acceptable to the users of the system **100**. The statistical analysis can be any of the well-known analysis techniques employed by those skilled in the art (e.g., statistical pattern matching or image-registration techniques, pattern-recognition techniques involving feature extraction and classification in either the spatial domain or the frequency domain, or heuristic methods involving, e.g., neural networks). For example, for fingerprint comparison, the number of landmarks (e.g., ridges) and their location (e.g., x, y coordinates) and the variance between the sets of data are statistically analyzed for to calculate a probability that the candidate set of biometric data matches the reference set of biometric data.

[**0038**] If the candidate set of biometric data does not sufficiently match the reference set of biometric data, the authentication server **108** responds to the request (step **202**) from the application server **104** by denying (step **250**) authentication of the alias associated with that request. In response to the rejection (step **250**), the application server **104** denies (step **255**) access to the user associated with the alias for the requested (step **202**) service. If the identifying characteristic matches and the candidate set of biometric data does sufficiently match the reference set of biometric data, the authentication server **108** responds to the request (step **202**) from the application server **104** by authenticating (step **260**) the alias associated with that request. In response to the acceptance (step **260**), the application server **104** allows (step **265**) access to the user associated with the alias for the requested (step **202**) service.

[**0039**] In other embodiments, another layer of protection is added by not storing and/or transmitting the biometric data in its native format, i.e., by not storing and/or transmitting the biometric data in the same way that it is transmitted from the biometric data generator **140** (for example, a fingerprint scanner). In one embodiment, the plug-in module **132** modifies the biometric data, both at registration of a reference set of biometric data and when fulfilling a request for a candidate set of biometric data. The algorithm used for the modification can use the alias as an input parameter or variable, so that the modification for each individual is different. The modification can include encrypting and/or morphing (e.g., using a transformation algorithm) the biometric data. Even if someone captures the modified biometric data, it is unusable unless that someone also had i) the associated alias, which in one embodiment, is never transmitted along with the biometric data, and ii) the modification algorithm. If security were to be compromised, the system **100** could re-store the reference biometric data using a different modification algorithm, making any acquired biometric data unusable.

[**0040**] For example, morphing the captured image uses a predefined mathematical algorithm to create a distorted image, and storing features from the distorted image rather than from the source biometric image. This facilitates creation of multiple alias biometric identities from an individual's unique biometric features. In use, an individual is assigned a morphing function and parameters relating thereto. These are used to predistort the image, thereby creating distorted landmarks. During testing, a candidate biometric image is subjected to the same function and parameters prior to comparison with the stored image.

[**0041**] This approach avoids storage of an individual's true biometric identity. Moreover, if an individual's biometric identity is compromised (e.g., stolen from the server), the user can simply enroll again with a different morphing function and/or parameters. Morphing can be performed either at the image level or after the features are computed through a transform that maps the (x,y) coordinates for each minutiae point to new coordinates (x',y') using a predefined f(x,t) and g(y,t) function for all x, y values and t.

[0042] In yet another embodiment, the authentication server **108** and/or the client **112** employs additional techniques to process the received candidate set of biometric data and to extract the unique features that distinguish one set of biometric data (e.g., fingerprint) from another. For example, the authentication server **108** and/or the client **112** may normalize the biometric data into a format used by the authentication server **108**. The normalization can include, for example, a translation algorithm, a transformation algorithm and the like. The normalization allows the biometrics data to be converted into a standard image suitable for subsequent processing and preferably includes geometric processing to adjust for size differences between sensors, orientation adjustments to invert or rotate images, density adjustments to correct for number of gray levels/dynamic range and sampling adjustments to account for different sensor resolutions. This allows the client **112** to interface with different types of biometric input devices **140** without the need to re-register the user or change the format of the biometric data in the biometric database module **128**.

[0043] The authentication server **108** and/or the client **112** may also filter the received candidate set of biometric data. The filtering can include filtering algorithms for correcting blurring of the image, for removing random noise in the image and the like. For example, all captured scans can be checked for partial or blurred prints that exhibit greater than expected amount of change between consecutive frames as well as contrast. Images that exhibit excessive blur can be rejected. Contrast issues can be resolved by asking the user to press down to make better contact with the sensor. Image processing software may be used to enhance the quality of the image and involve signal averaging, noise filtering, ridge/valley enhancement as well as gray scale equalization. The filtering can also include filtering algorithms dictated by the type of the biometric device **140** or the type of user features the biometric device **140** uses. The filtering can also include filtering algorithms based on the type of image (e.g., grainy, wet, fine grain and the like), the finger type and/or personal biometric characteristics (e.g., sex, age and the like). In an embodiment where the filter module **144** is implemented on the client **112**, the filter module **114** operates in conjunction with the biometric input device **116** to perform blur removal, finger detection and time based enhancements. For example, two or more scans may be taken to ensure the user **170** has placed a stable finger (not moving) on the sensor. A difference is then taken between subsequent scans to ensure consistency between the two scans. With noisy sensors, the filter module **144** may integrate consecutive images to reduce the noise level in the captured image.

[0044] The authentication server **108** and/or the client **112** may also extract the associated geometric data of features and/or minutiae from the candidate set of biometric data. In an embodiment where the extractor module **146** is implemented on the client **112**, the extractor module **146** transmits the results to the authentication module **128** using the network **116**. Biometric data, for example in the case of fingerprints, can be divided into global features that are spatial in nature and local features that represent details captured in specific locations. The geometric data can include, for example, the locations (e.g., x, y coordinates) of the features, the type of feature (e.g., ridge ending, bifurcation and the like), the angular data of the features, the slope of the ridge, the neighborhood ridge counts and/or the like. Once processed, the authentication server **108** can compare, for example, the minutiae data of the reference set of biometric data stored in the biometric database module **128** with the candidate set of biometric data to produce a goodness of fit or confidence of match by examining the local features on a minutiae by minutiae basis.

[0045] To calculate the goodness of fit, the authentication server **108** determines the best spatial alignment between the location of minutiae points within the reference set of biometric data and corresponding minutiae points within the candidate set of biometric data. Determining the best spatial alignment involves, for example, finding the rotation angle that produces the greatest number of matching points. This may be accomplished, for example, using a spatial correlation algorithm in which the features of the candidate set of biometric data are translated and rotated about a test alignment point and then compared against the features in the reference set. Different alignment points and rotation angles are tested to determine the lowest difference between the candidate and reference feature set. Matching can be a relative term, meaning the points are close to each other within some predefined distance. The determining process can accommodate both spatial and rotational displacement between the reference set of biometric data and the candidate set of biometric data. The authentication server **108** then sums the goodness of fit for local features at each of the matching minutiae points. The authentication server **108** determines the sufficiency of the match by statistically analyzing the goodness of fit for local features at each of the matching minutiae points and determining whether the probability that they come from the same individual is above a certain predetermined threshold, as described above.

[0046] **FIG. 3** illustrates a system **300** employing a data structure used to securely store user credentials. The data structure is hierarchically organized into realms, vaults, and folders, as further explained below, and is useful in connection with the system **100** as well as in other authentication systems.

[0047] The system **300** includes a biometric database module **128'** and an alias database module **120'** that is logically or physically separate from the biometric database module **128'**. The biometric database module **128'** includes a first realm **305***a* and a second realm **305***b*, generally referred to as **305**. In general, a realm **305** is a security partition, grouping subscribers according to a scheme relevant to an application server. For example, a financial-services company might group subscribers by state or by service tier. In one embodiment, each security realm **305** corresponds to a separate set of objects assigned its own symmetric encryption key to ensure that data from one realm (e.g., **305***a*) is not usable by another realm (e.g., **305***b*).

[0048] The first realm **305***a* includes a first vault **310***a* and a first subscriber profile **320***a*. The first subscriber profile **320***a* includes an alias associated with the subscriber and a reference set of biometric data **325***a* associated with the alias. The first vault **310***a* includes a first folder **330***a*. As illustrated, subscriber**1** is associated with the first vault **310***a*. In this context, the term "subscriber" refers to an individual identified by his/her alias, which is associated with biometric data **325**. The biometric data **325** represents a set of biometric characteristics that uniquely identifies the subscriber, including but not limited to finger templates,

facial templates, retinal templates, and/or voice prints. Each vault **310** contains one or more folders **330**, and is accessible to one or more subscribers, so that each subscriber owns one or more vaults **310** within a realm. The folders **330** within each vault **310**, in turn, contain assets and/or user credentials (e.g., login accounts, URL/password combinations, digital certificates and the like). A folder **330** can be modified only by the owner of the vault **310**, and is associated with a list of subscribers **320**, or "folder users," eligible for access.

[**0049**] The second realm **305***b* includes a second vault **310***b* and a third vault **310***c*, generally referred to as **310**. The second realm **305***b* also includes a second subscriber profile **320***b* and a third subscriber profile **320***c*, generally referred to as **320**. The second subscriber profile **320***b* includes an alias associated with subscriber**2** and a reference set of biometric data **325***b* associated with the alias. The third subscriber profile **320***c* includes an alias associated with subscriber**3** and a reference set of biometric data **325***c* associated with the alias. The second vault **310***b* includes a second folder **330***b*. The third vault **310***c* includes a third folder **330***c* and a fourth folder **330***d*, generally referred to as **330**. As illustrated, subscriber**2** is associated with the second vault **310***b*. Subscriber**3** is associated with the second vault **310***b* and the third vault **310***c*. Accordingly, there need not exist a one-to-one mapping between subscribers and vaults; more than one subscriber may have access to a single vault, for example, and a single subscriber may have access to multiple vaults within a realm.

[**0050**] In one embodiment, accessing a vault follows the same process as described in connection with **FIG. 2**. For example, the subscriber (e.g., subscriber**2**) requests access to the subscriber's associated folder (e.g., **330***b*), or an application server can request a specific set of subscriber's credentials to access a service the subscriber requests. The alias database module **120'** finds the associated alias (e.g., alias**2**) of the subscriber and passes a request for the credentials to the biometric database module **128'**. After receiving the candidate biometric data, the biometric database module **128'** verifies there is a sufficient match with the reference biometric data associated with the alias (e.g., **325***b*). With authentication, the subscriber is allowed access to the folder (e.g., **330***b*) or the requested credentials within the folder are transmitted to the application server.

[**0051**] Equivalents

[**0052**] The invention can be embodied in other specific forms without departing from the spirit or essential characteristics thereof. The foregoing embodiments are therefore to be considered in all respects illustrative rather than limiting on the invention described herein. Scope of the invention is thus indicated by the appended claims rather than by the foregoing description, and all changes which come within the meaning and range of equivalency of the claims are therefore intended to be embraced therein.

What is claimed is:

1. A method for authentication using biometrics, the method comprising:

associating an alias for an individual with a reference set of biometric data from the individual;

storing, at a location separate from the reference set of biometric data, information associating the individual with the alias;

receiving an authentication request requesting authentication of a user identified by the alias;

receiving a candidate set of biometric data from the user; and

if the candidate set of biometric data sufficiently matches the reference set of biometric data, confirming authentication of the user as the registered individual.

2. The method of claim 1 further comprising transmitting to the user a data request for the candidate set of biometric data, the data request including an identifying characteristic, wherein the confirming step comprises:

if the candidate set of biometric data includes the identifying characteristic and sufficiently matches the reference set of biometric data, confirming to the application server authentication of the user as the registered individual.

3. The method of claim 2 further comprising:

generating the identifying characteristic including a public key;

generating a private key corresponding to the public key; and

encrypting the data request using the private key.

4. The method of claim 2 further comprising generating the identifying characteristic having a limited validity lifetime.

5. The method of claim 2 further comprising generating the identifying characteristic including a random identifier.

6. The method of claim 2 further comprising generating the identifying characteristic including a time identifier.

7. The method of claim 2 further comprising destroying the identifying characteristic after completion of the confirming step.

8. The method of claim 1 further comprising, if authentication of the user is confirmed, updating the reference set of biometric data using the candidate set of biometric data.

9. The method of claim 1 further comprising transmitting, by a first server, the authentication request to a second server, wherein the second server performs the confirming step.

10. The method of claim 1 further comprising encrypting the reference set of biometric data using a predetermined function based at least in part on the alias.

11. The method of claim 9 wherein the encrypting step comprises morphing the reference set of biometric data using a predetermined function based at least in part on the alias.

12. The method of claim 1 further comprising, if security is compromised, encrypting the reference set of biometric data using a second function based at least in part on the alias.

13. The method of claim 11 wherein the encrypting step comprises, if security is compromised, morphing the reference set of biometric data using a second function based at least in part on the alias.

14. A system for authentication using biometrics, the system comprising:

an application server including:

an alias database module configured to store information associating an individual with an alias; and

an authentication server including:

a biometric database module associating the alias for the individual with a reference set of biometric data from the individual,

a transceiver module configured to i) receive an authentication request requesting authentication of a user identified by the alias and ii) to receive a candidate set of biometric data from the user, and

a comparison module configured to determine if the candidate set of biometric data sufficiently matches the reference set of biometric data and, if so, to generate a confirmation of authentication of the user as the registered individual.

15. The application server of claim 14 further comprising a transceiver module configured to transmit an authentication request requesting authentication of a user identified by the alias, the application server being in communication with the authentication server over a network.

16. The authentication server of claim 14 further comprising an identifying characteristic generator module configured to generate an identifying characteristic to be transmitted with a user data request for the candidate set of biometric data, wherein the comparison module is further configured to determine if the candidate set of biometric data includes the identifying characteristic.

17. The authentication server of claim 16 wherein the identifying characteristic generator module is further configured to generate the identifying characteristic including a public key, to generating a private key corresponding to the public key, and to encrypt the user data request using the private key.

18. The authentication server of claim 16 wherein the identifying characteristic generator module is further configured to generate the identifying characteristic having a limited validity lifetime.

19. The authentication server of claim 16 wherein the identifying characteristic generator module is further configured to generate the identifying characteristic including a random identifier.

20. The authentication server of claim 16 wherein the identifying characteristic generator module is further configured to generate the identifying characteristic including a time identifier.

21. The authentication server of claim 16 wherein the identifying characteristic generator module is further configured to destroy the identifying characteristic after completion of the confirming step.

22. The authentication server of claim 14 wherein the biometric database module is further configured to update, if authentication of the user is confirmed, the reference set of biometric data using the candidate set of biometric data.

23. The authentication server of claim 14 wherein the biometric database module is further configured to encrypt the reference set of biometric data using a predetermined function based at least in part on the alias.

24. The authentication server of claim 14 wherein the biometric database module is further configured to morph the reference set of biometric data using a predetermined function based at least in part on the alias.

25. The authentication server of claim 14 wherein the biometric database module is further configured to encrypt, if security is compromised, the reference set of biometric data using a second function based at least in part on the alias.

26. The authentication server of claim 14 wherein the biometric database module is further configured to morph, if security is compromised, the reference set of biometric data using a second function based at least in part on the alias.

27. The system of claim 14 further configured comprising:

a client including:

a plug-in configured to receive a request for the candidate set of biometric data, to obtain the candidate set of biometric data for the user of the client and to transmit the candidate set of biometric data in response to the request.

28. A method of organizing authentication information within a storage space, the method comprising the steps of:

partitioning the storage space into a plurality of realms, each realm containing a set of subscriber profiles, each subscriber profile comprising an alias associated with a respective subscriber and a reference set of biometric data from that respective subscriber;

storing, at a location separate from the storage space, information associating the identity of the alias with the respective subscriber;

partitioning each realm into a plurality of vaults;

associating each subscriber with at least one vault;

partitioning each vault into at least one folder, each folder containing protected data and being accessible only to one or more subscribers associated with the vault; and

according access to the vault and the folders therein only upon presentation of i) the alias of a subscriber associated with the vault and ii) a candidate set of biometric data sufficiently matching the reference set of the biometric data corresponding to the alias.

29. The method of claim 28 further comprising transmitting a data request for the candidate set of biometric data, the data request including an identifying characteristic, wherein the according access step comprises:

according access to the vault and the folders therein only upon presentation of i) the alias of a subscriber associated with the vault, ii) the identifying characteristic and iii) a candidate set of biometric data sufficiently matching the reference set of the biometric data corresponding to the alias.

30. An article of manufacture having computer-readable program portions embodied therein for authentication using biometrics, the article comprising:

a computer-readable program portion for associating an alias for an individual with a reference set of biometric data from the individual;

a computer-readable program portion for storing, at a location separate from the reference set of biometric data, information associating the individual with the alias;

a computer-readable program portion for receiving an authentication request requesting authentication of a user, the user identified by the alias;

a computer-readable program portion for receiving a candidate set of biometric data from the user; and

a computer-readable program portion for confirming authentication of the user as the registered individual if the candidate set of biometric data sufficiently matches the reference set of biometric data.

31. The article of claim **30** further comprising:

a computer-readable program portion for transmitting to the user a data request for the candidate set of biometric data, the data request including an identifying characteristic, and

wherein the computer-readable program portion for confirming authentication comprises:

a computer-readable program portion for confirming authentication of the user as the registered individual if the candidate set of biometric data includes the identifying characteristic and sufficiently matches the reference set of biometric data.

* * * * *