



US 20140289116A1

(19) **United States**(12) **Patent Application Publication**
Polivanyi(10) **Pub. No.: US 2014/0289116 A1**(43) **Pub. Date: Sep. 25, 2014**(54) **SYSTEM AND METHOD FOR PERFORMING
AUTHENTICATION FOR A LOCAL
TRANSACTION**(52) **U.S. Cl.**CPC **G06Q 20/40145** (2013.01)USPC **705/44**(71) Applicant: **Igor Polivanyi**, Palo Alto, CA (US)(72) Inventor: **Igor Polivanyi**, Palo Alto, CA (US)(21) Appl. No.: **14/218,611**(22) Filed: **Mar. 18, 2014****Related U.S. Application Data**

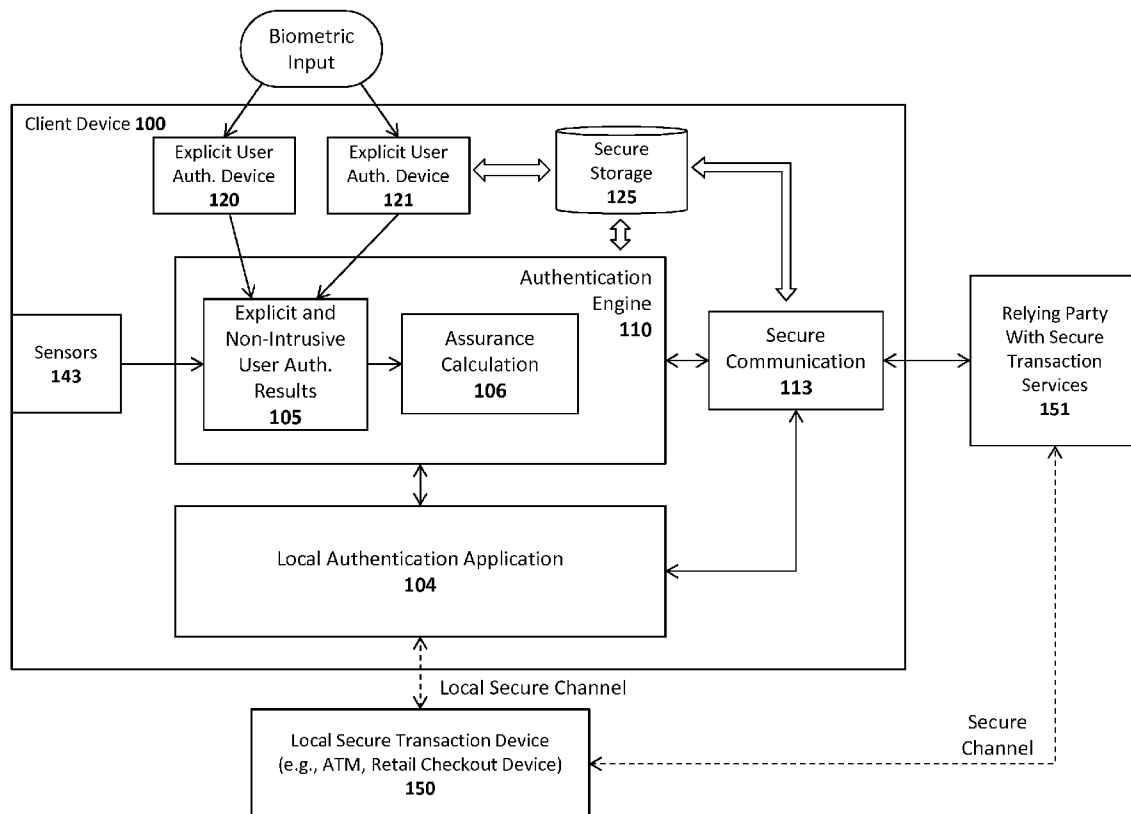
(60) Provisional application No. 61/804,568, filed on Mar. 22, 2013.

Publication Classification(51) **Int. Cl.**
G06Q 20/40

(2006.01)

(57) **ABSTRACT**

A system, apparatus, method, and machine readable medium are described for strong authentication for a local transaction. For example, one embodiment of a system comprises: a local transaction device; a client device performing one or more authentication transactions including receiving biometric input from the user to generate an authentication result; a secure transaction service communicatively coupled to the local transaction device over a network, the secure transaction service receiving the authentication result from the client device; and the remote secure transaction service transmitting a signal to the local transaction device to perform one or more operations if the authentication result is sufficient to complete a transaction.



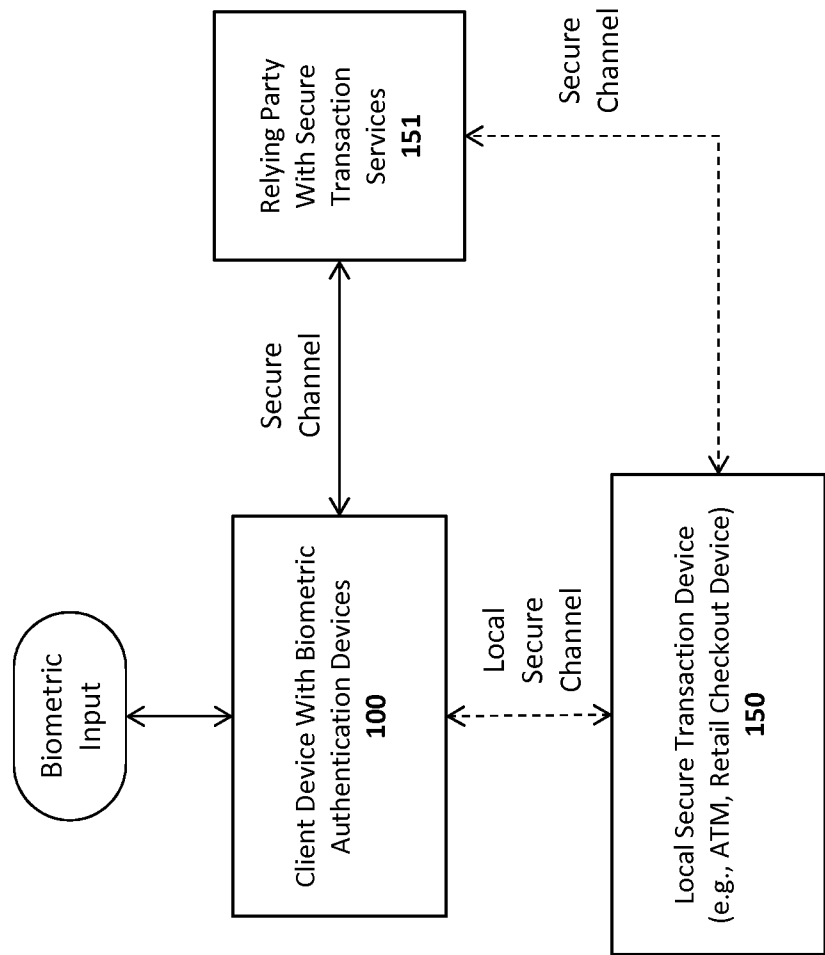


FIG. 1

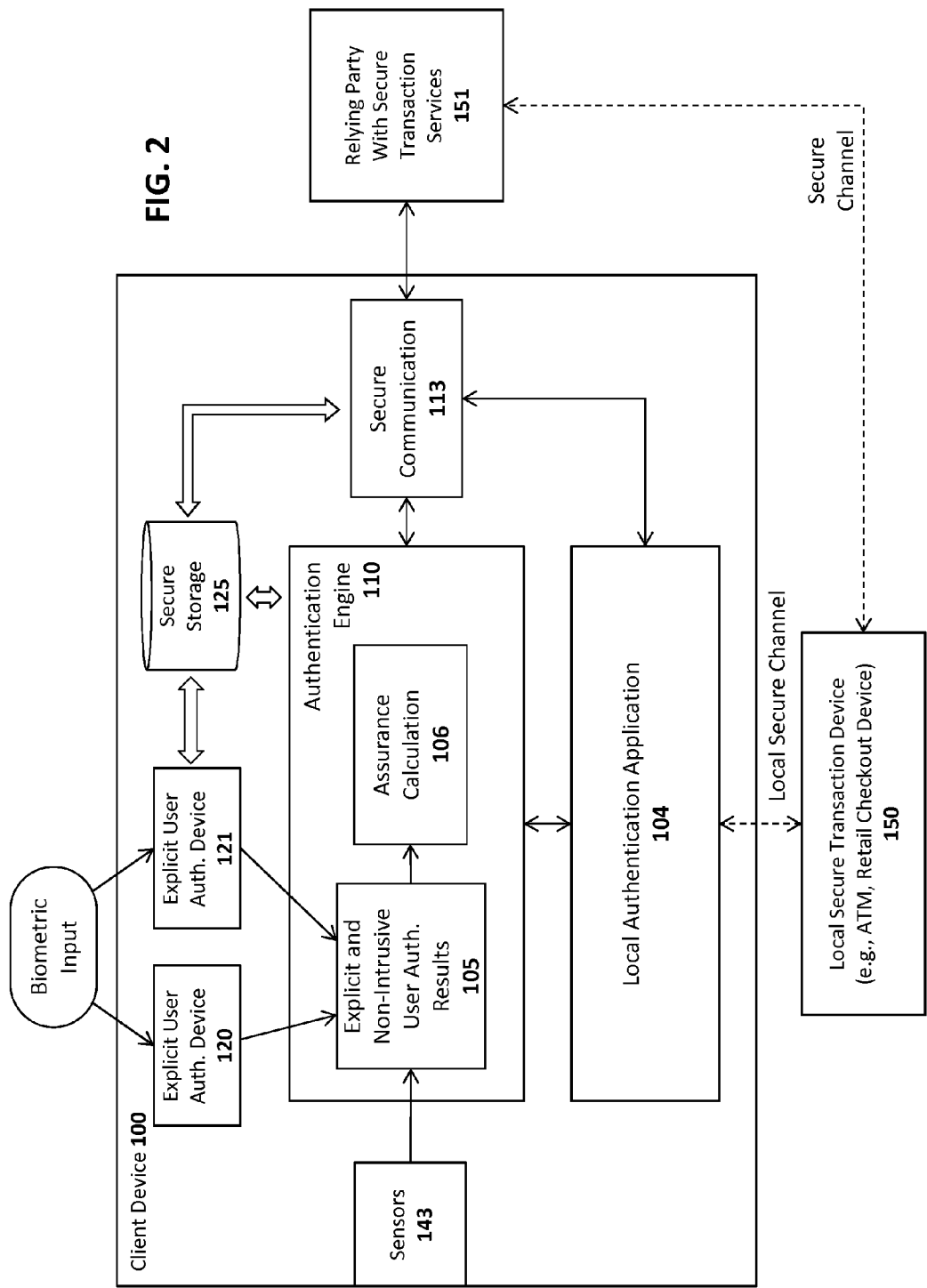
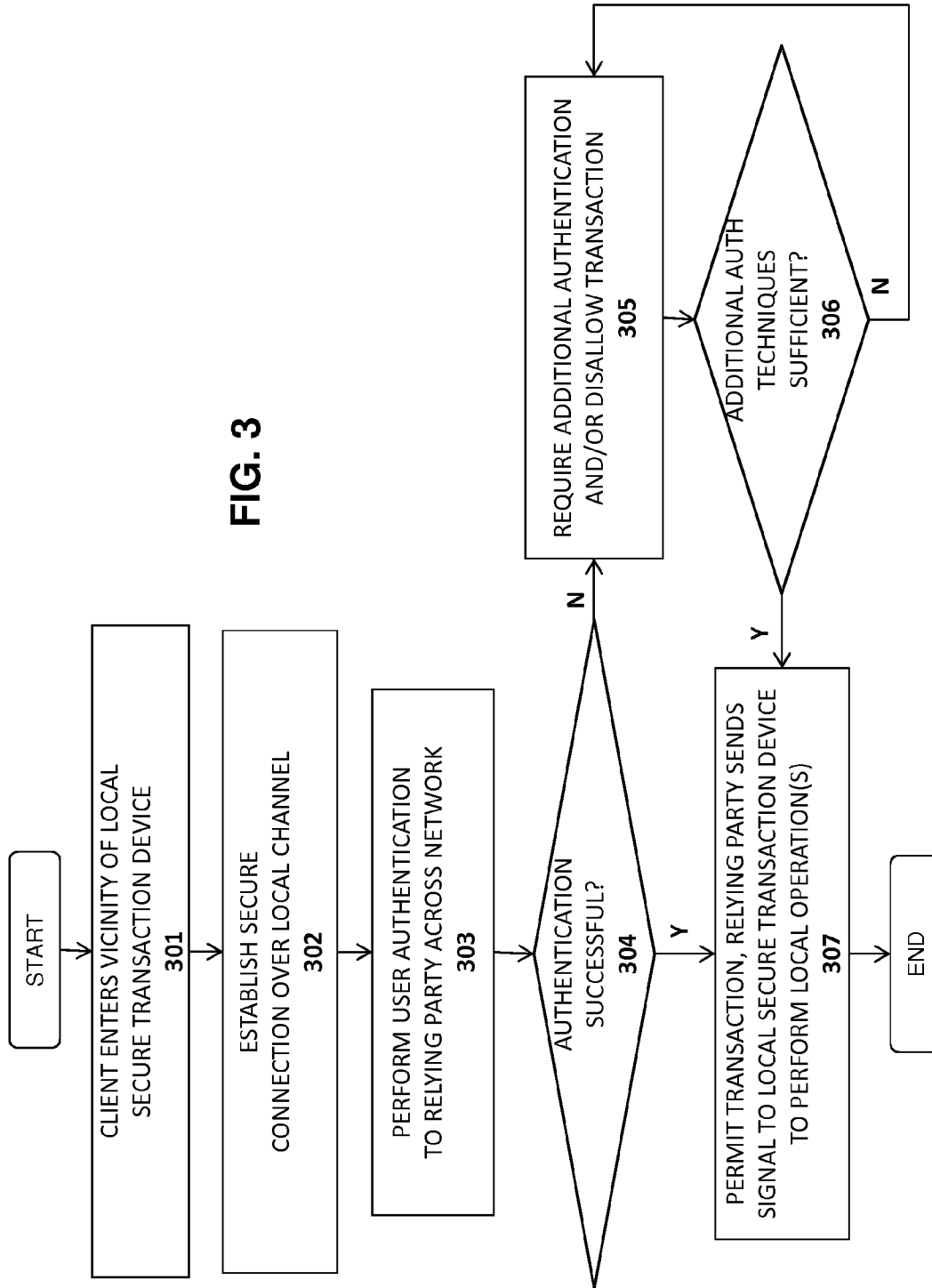


FIG. 3



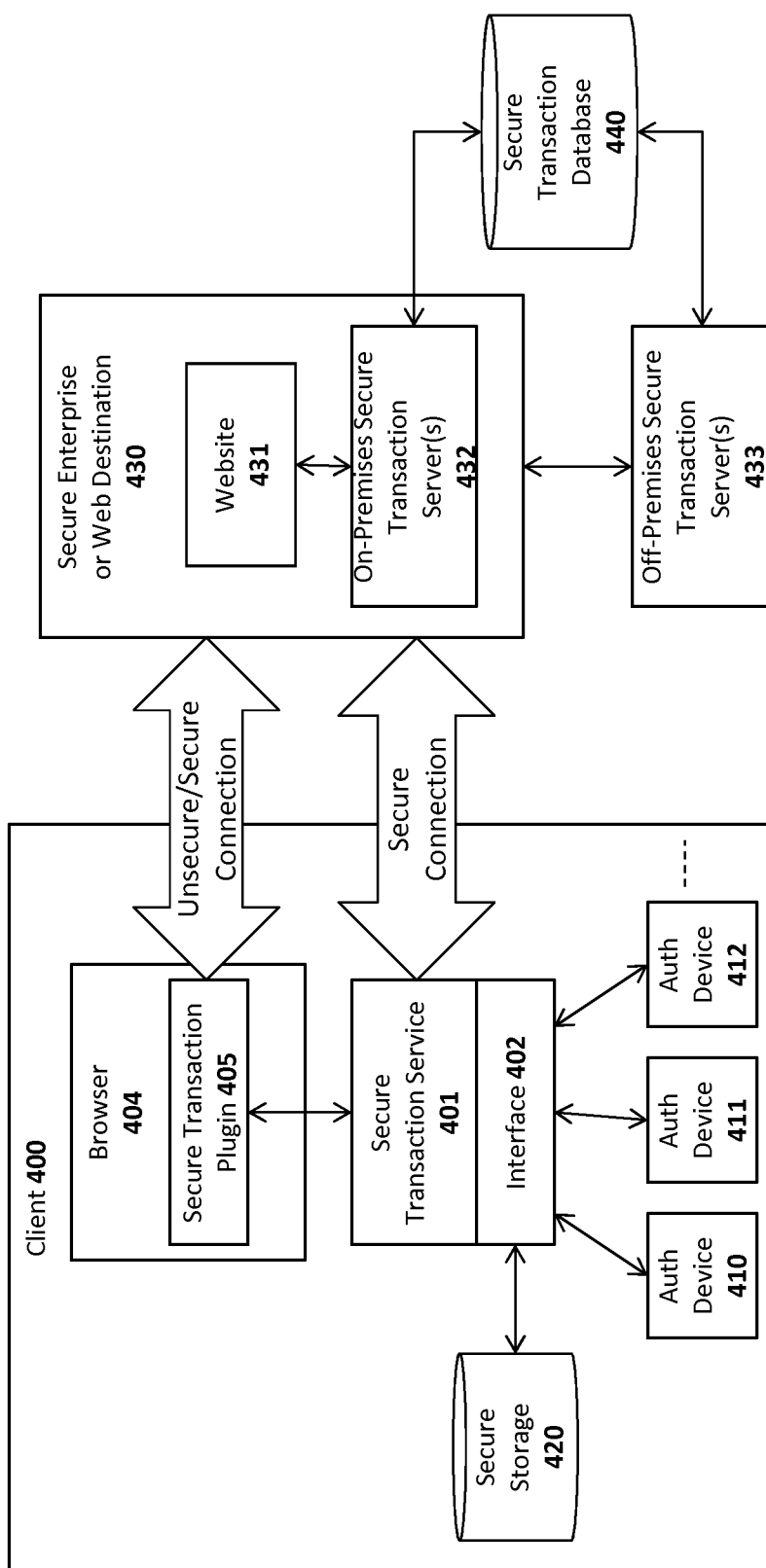


FIG. 4A

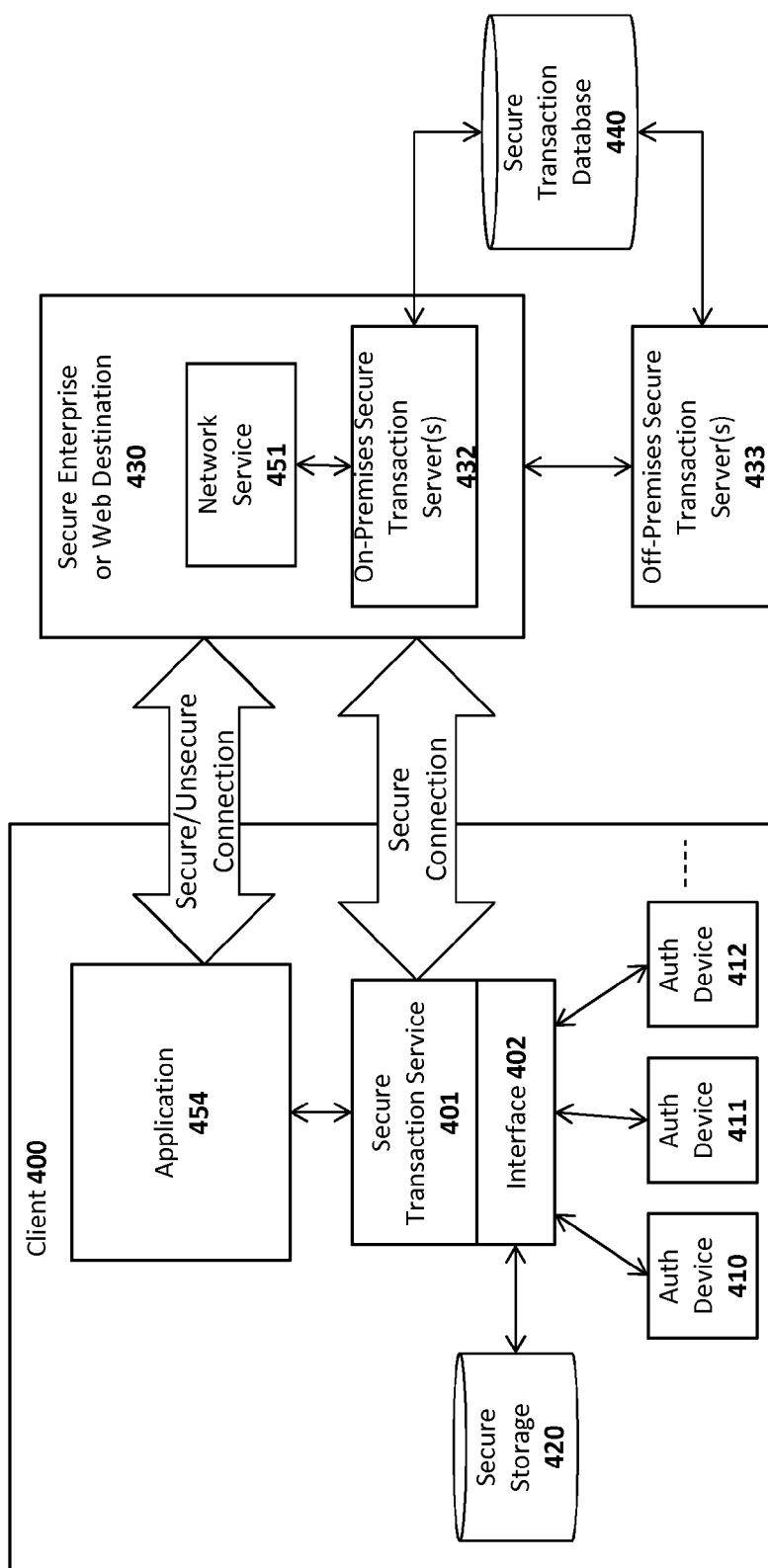


FIG. 4B

SYSTEM AND METHOD FOR PERFORMING AUTHENTICATION FOR A LOCAL TRANSACTION

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of and priority to co-pending U.S. Provisional Patent Application No. 61/804,568, filed, Mar. 22, 2013, entitled, “Advanced Methods of Authentication And Its Applications”.

BACKGROUND

[0002] 1. Field of the Invention

[0003] This invention relates generally to the field of data processing systems. More particularly, the invention relates to a system and method for performing authentication for a local transaction.

[0004] 2. Description of Related Art

[0005] Systems have been designed for providing secure user authentication over a network using biometric sensors. In such systems, the score generated by the application, and/or other authentication data, may be sent over a network to authenticate the user with a remote server. For example, Patent Application No. 2011/0082801 (“’801 Application”) describes a framework for user registration and authentication on a network which provides strong authentication (e.g., protection against identity theft and phishing), secure transactions (e.g., protection against “malware in the browser” and “man in the middle” attacks for transactions), and enrollment/management of client authentication tokens (e.g., fingerprint readers, facial recognition devices, smartcards, trusted platform modules, etc).

[0006] The assignee of the present application has developed a variety of improvements to the authentication framework described in the ’801 application. Some of these improvements are described in the following set of US Patent Applications (“Co-pending Applications”), all filed Dec. 29, 2012, which are assigned to the present assignee and incorporated herein by reference: Ser. No. 13/730,761, Query System and Method to Determine Authentication Capabilities; Ser. No. 13/730,776, System and Method for Efficiently Enrolling, Registering, and Authenticating With Multiple Authentication Devices; Ser. No. 13/730,780, System and Method for Processing Random Challenges Within an Authentication Framework; Ser. No. 13/730,791, System and Method for Implementing Privacy Classes Within an Authentication Framework; Ser. No. 13/730,795, System and Method for Implementing Transaction Signaling Within an Authentication Framework.

[0007] Briefly, the Co-Pending Applications describe authentication techniques in which a user enrolls with biometric devices of a client to generate biometric template data (e.g., by swiping a finger, snapping a picture, recording a voice, etc); registers the biometric devices with one or more servers over a network (e.g., Websites or other relying parties equipped with secure transaction services as described in the Co-Pending Applications); and subsequently authenticates with those servers using data exchanged during the registration process (e.g., encryption keys provisioned into the biometric devices). Once authenticated, the user is permitted to perform one or more online transactions with a Website or other relying party. In the framework described in the Co-Pending Applications, sensitive information such as finger-

print data and other data which can be used to uniquely identify the user, may be retained locally on the user’s client device (e.g., smartphone, notebook computer, etc) to protect a user’s privacy.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] A better understanding of the present invention can be obtained from the following detailed description in conjunction with the following drawings, in which:

[0009] FIG. 1 illustrates one embodiment of a client performing a secure transaction with a local device;

[0010] FIG. 2 illustrates one embodiment of a client architecture for performing a secure transaction with a local device;

[0011] FIG. 3 illustrates one embodiment of a method for performing a secure transaction with a local device; and

[0012] FIGS. 4A-B illustrate different exemplary architectural arrangements within which embodiments of the invention may be implemented.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

[0013] Described below are embodiments of an apparatus, method, and machine-readable medium for authenticating a user for a local transaction such as one involving an automatic teller machine (ATM), retail checkout device, or other device with which the user wishes to initiate a transaction. Throughout the description, for the purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the present invention. It will be apparent, however, to one skilled in the art that the present invention may be practiced without some of these specific details. In other instances, well-known structures and devices are not shown or are shown in a block diagram form to avoid obscuring the underlying principles of the present invention.

[0014] The embodiments of the invention discussed below involve client devices with authentication capabilities such as biometric devices or PIN entry. These devices are sometimes referred to herein as “tokens,” “authentication devices,” or “authenticators.” While certain embodiments focus on facial recognition hardware/software (e.g., a camera and associated software for recognizing a user’s face and tracking a user’s eye movement), some embodiments may utilize additional biometric devices including, for example, fingerprint sensors, voice recognition hardware/software (e.g., a microphone and associated software for recognizing a user’s voice), and optical recognition capabilities (e.g., an optical scanner and associated software for scanning the retina of a user). The authentication capabilities may also include non-biometric devices such as trusted platform modules (TPMs) and smartcards.

[0015] In a mobile biometric implementation, the biometric device may be remote from the relying party. As used herein, the term “remote” means that the biometric sensor is not part of the security boundary of the computer it is communicatively coupled to (e.g., it is not embedded into the same physical enclosure as the relying party computer). By way of example, the biometric device may be coupled to the relying party via a network (e.g., the Internet, a wireless network link, etc) or via a peripheral input such as a USB port. Under these conditions, there may be no way for the relying party to know if the device is one which is authorized by the relying party (e.g., one which provides an acceptable level of authentication and integrity protection) and/or whether a

hacker has compromised the biometric device. Confidence in the biometric device depends on the particular implementation of the device.

[0016] The term “local” is used herein to refer to the fact that the user is completing a transaction in person, at a particular location such as at an automatic teller machine (ATM) or a retail checkout location. However, as discussed below, the authentication techniques employed to authenticate the user may involve non-location components such as communication over a network with remote servers and/or other data processing devices. Moreover, while specific embodiments are described herein (such as an ATM and retail location) it should be noted that the underlying principles of the invention may be implemented within the context of any system in which a transaction is initiated locally by an end user.

[0017] The term “relying party” is sometimes used herein to refer, not merely to the entity with which a user transaction is attempted (e.g., a Website or online service performing user transactions), but also to the secure transaction servers implemented on behalf of that entity which may performed the underlying authentication techniques described herein. The secure transaction servers may be owned and/or under the control of the relying party or may be under the control of a third party offering secure transaction services to the relying party as part of a business arrangement.

[0018] The term “server” is used herein to refer to software executed on a hardware platform (or across multiple hardware platforms) that receives requests over a network from a client, responsively performs one or more operations, and transmits a response to the client, typically including the results of the operations. The server responds to client requests to provide, or help to provide, a network “service” to the clients. Significantly, a server is not limited to a single computer (e.g., a single hardware device for executing the server software) and may, in fact, be spread across multiple hardware platforms, potentially at multiple geographical locations.

[0019] Embodiments for Authenticating the user for a Local Transaction

[0020] The embodiments of the invention described herein include techniques for authenticating a user for a local transaction initiated through a local secure transaction device. By way of example, the local transaction may be a withdrawal, transfer, or other user-initiated operation and the secure transaction device may be an ATM or other local device capable of executing financial transactions. Similarly, the local transaction may involve completing a payment to purchase goods or services at a retail store or other retail location equipped with a local secure transaction device.

[0021] As illustrated in FIG. 1, in one embodiment, a client device **100** with biometric authentication devices and associated software authenticates over a network to a relying party with secure transaction services **151** to perform a transaction on a local secure transaction device **150**. In particular, when the user of client device **100** wishes to perform a transaction locally with secure transaction device **150**, it initiates a series of authentication transactions with the relying party **151** (examples of which are described below). For example, the user may be required to swipe a finger on a fingerprint reader on the client device **100** and/or enter a PIN or other secret code via a client keypad. The results of the authentication may then be transmitted from the client device **100** to the relying party

151 without transmitting the user’s private data (e.g., the fingerprint data, PIN, or any other private user data), thereby protecting the user’s privacy.

[0022] In response to a successful authentication, the relying party **151** may transmit a signal to the local secure transaction device **150** to perform an operation. For example, if the local secure transaction device is an ATM, the signal may instruct the ATM to dispense a specified amount of cash. If the local secure transaction device **150** is a retail checkout device then an indication of successful payment may be transmitted and the user’s account may be debited.

[0023] In addition, as shown in FIG. 1, a local secure communication channel may be established between the client device **100** and the local secure transaction device **150** to supplement the user authentication process. The local secure channel may be established using wireless communication interfaces on the client device **100** and local secure transaction device **150** utilizing various wireless communication technologies such as near field communication (NFC), Bluetooth, or WiFi (e.g., an 802.11x channel), to name a few. For example, when in the vicinity of the location secure transaction device **150**, the client device **100** may perform a near-field communication (NFC) handshake via its wireless interface with the wireless interface of the local secure transaction device **150** and establish the local secure channel to exchange data during authentication.

[0024] The mere existence of the local secure channel comprises authentication data because it establishes the current location of the client device **100**. Consequently, this information may be used by the relying party **151** as proof of the current location of the client device **100** during the authentication process. In one embodiment, the relying party **151** may compare the location provided by the local secure transaction device **150** with the current GPS location reported by the client device **100** to confirm that the two location values match.

[0025] In addition, the relying party **151** may transmit a secret code or other authentication data to the client device **100**, which the client device **100** may then relay to the local secure transaction device **150** over the local secure channel to authenticate the client device. For example, in one embodiment, the relying party **151** transmits a barcode to the client device **100** and a corresponding code to the local secure transaction device. The local secure transaction device **150** may then read the barcode (e.g., from the display of the client device **100**) using a barcode scanner or camera to perform authentication (i.e., comparing the code received from the relying party with the code read from the barcode). Alternatively, the local secure transaction device **150** may transmit the code read from the barcode to the relying party, which will then confirm that the codes match. Conversely, the relying party **151** may transmit a secret code or other authentication data to the local secure transaction device **150** which will then relay the data to the client device **100** for authentication. Thus the local secure channel may be used to exchange data for a variety of authentication techniques.

[0026] As mentioned, in one particular embodiment, the local secure transaction device **150** is an ATM device. ATM machines are vulnerable devices, because their input/output controls (e.g., card-readers, keyboards, screens, cameras, etc) are exposed for the “outside world” and they are readily available for tampering. For example, debit card records and pins can be easily stolen with low-tech devices, such as hidden magnetic stripe readers, mirrors, and video cameras. In

one embodiment, remote authentication techniques involving communication between the client **100** and relying party **151** are used to provide significantly improved authentication for ATM machines. When integrated with this remote authentication, an ATM itself doesn't need to have legacy input/output controls, such as card-reader, touchscreen or keyboard. All it requires is a network connection and a slot to dispense cash. The authentication per se can be performed on the customer's client device **100** equipped with the biometric authentication devices.

[0027] In one embodiment, for a cash withdrawal, the user would enter the vicinity of the ATM machine and initiate the remote authentication application to authenticate to the relying party **151**. The user would then enter the amount for withdrawal and swipe her finger using the fingerprint sensor on the mobile device (or user any other type of authentication as discussed below). When the user's presence and authenticity are confirmed with the relying party **151**, a specified amount of money is dispensed from the ATM's slot.

[0028] This embodiment not only provides stronger authentication, but it also converts complex and expensive ATMs into simple and reliable money dispensers that are significantly cheaper to build and maintain. These new ATM's may be used for a long time. They will not require frequent updates, because all updates to the biometrics-related authentication features are introduced directly on the client devices **100** and/or the relying party's secure transaction servers **151**.

[0029] Additional architectural details of one embodiment of the invention are illustrated in FIG. 2. As illustrated, the client device **100** of this embodiment includes a local authentication application **104** which communicates with both the local secure transaction device **150** and relying party **151** to coordinate the various local authentication techniques described herein. In one embodiment, the local authentication application **104** establishes the local secure channel with the local secure transaction device **150** and an authentication engine **110** performs remote authentication with the relying party to verify that the legitimate user is in possession of the client device **100**.

[0030] In one embodiment, the authentication engine **110** performs authentication by entering into a series of transactions with the secure transaction servers of the relying party as described in the co-pending patent applications mentioned above. For example, these transactions may include an enrollment process in which a user enrolls with biometric devices of a client to generate biometric template data (e.g., by swiping a finger, snapping a picture, recording a voice, etc). Enrollment may be under the direction of the secure transaction servers of the relying party or may be done autonomously by the user. The user may then register the biometric devices with the secure transaction servers over the network and subsequently authenticate with those servers using data exchanged during the registration process (e.g., encryption keys provisioned into the biometric devices).

[0031] In one embodiment, the authentication engine **110** includes an assurance level calculation module **106** for calculating an assurance level corresponding to a likelihood that the legitimate user is in possession of the client device **100**. It may then use this assurance level to determine whether the relying party **151** should authorize a local transaction at the local secure transaction device **150** (e.g., such as a financial transaction, a retail purchase, an access to confidential information in the user's account, etc). In one embodiment, the

relying party **151** may specify the level of assurance required for a given transaction. For example, for a financial transaction involving the transfer of a significant amount of money, the relying party **151** may require a relatively higher assurance level than, for example, a transaction involving access to a user's account.

[0032] In one embodiment, the assurance level calculation module **106** transmits the assurance level (e.g., specified as a value, percentage, code, etc) to the relying party **151**, without disclosing any confidential user information, thereby protecting the user's privacy. In another embodiment, the assurance level calculation module **106** knows the assurance level required for the current transaction, determines whether the assurance level is sufficiently high, and transmits an indication of whether the transaction is permitted or denied to the relying party **151**, once again, without disclosing the user's private information to the relying party **151**.

[0033] In one embodiment, the communication between the client device **100** and relying party **151** is secured via a secure communication module **113**, which may encrypt outgoing communication using a first key and decrypt incoming communication using a second key. In a symmetric key encryption scheme the first and second keys are the same. In an asymmetric key encryption scheme, the keys are different. However, the underlying principles of the invention are not limited to any particular type of encryption.

[0034] In one embodiment, the assurance level calculation module **106** determines the assurance level based, at least in part, on current user authentication results **105** which may include the results of a current or recent explicit user authentication via one or more explicit user authentication devices **120-121**. This may include, for example, fingerprint authentication via a fingerprint device, facial recognition authentication via a camera and facial recognition hardware/software, voice recognition via a microphone and voice recognition hardware/software, retinal scanning using a camera and associated hardware/software, a password/PIN entry by the end user via a keypad, and/or various other types of explicit user authentication devices and/or techniques.

[0035] In one embodiment, a secure storage **125** cryptographically protects the biometric reference data records for each user authentication device **120-121** (e.g., wrapping the data using a symmetric key to make the storage **125** secure). While the secure storage **125** is illustrated outside of the secure perimeter of the authentication device(s) **120-121**, in one embodiment, each authentication device **120-121** may have its own integrated secure storage to cryptographically protect the biometric reference data records.

[0036] In addition to explicit user authentication, one embodiment of the authentication engine **110** collects data from sensors **143** to be used by the assurance calculation module **106** to generate the assurance level. By way of example, the sensors **143** may include location sensors such as GPS sensors to indicate a current location of the user. If the client device **100** is in an expected location such as the known vicinity of the local secure transaction device **150**, then this increases the likelihood that the user is the legitimate user. By contrast, if the GPS reading indicates that the user is not in the vicinity of the local secure transaction device **150**, then this indicates that the user initiating the transaction is not the legitimate user. Thus, in one embodiment, the assurance calculation module **106** will tend to increase the assurance level if the user is in an expected location and decrease the assurance level if the user is in an unexpected location.

[0037] Various additional sensors **143** such as temperature sensors, humidity sensors and accelerometers may be used to collect data relevant to user authentication. For example, the temperature/humidity sensors may provide a current temperature/humidity which may be compared against the known temperature/humidity for the location specified by the location sensor. If the values are significantly different, then this may indicate that the client device **100** is being spoofed. The comparison of the asserted location and the temperature/humidity may be done at a remote server such as the secure transaction server(s) used by the relying party **151**. In another embodiment, accelerometers on the device may be used to measure the gait of the user and compare these measurements against the known gait of the user. If the gaits match (within a specified threshold), then this increases the likelihood that the legitimate user is in possession of the client device **100**.

[0038] The local authentication application **104** may be implemented in a variety of ways while still complying with the underlying principles of the invention. For example, in one embodiment, the local authentication application **104** is designed specifically for the relying party **151**. For example, if the relying party is a banking institution (e.g., Wells Fargo®), then the local authentication application **104** may be an application specifically designed by/for that bank. In another embodiment, the same local authentication application **104** may be shared among a variety of relying parties, for example, as a universal local authentication application. Moreover, while illustrated in FIG. 2 as separate logical components, the authentication engine **110** shown in FIG. 2 may be integrated within the local authentication application **104**. In another embodiment, the local authentication application **104** may be a Web browser or an application executed within the Web browser context (e.g., when the user enters the vicinity of the local secure transaction device **150** or connects to the relying party web page to initiate the transaction).

[0039] The local authentication application **104** may perform a variety of local functions depending on the implementation required by the relying party. For example, in one embodiment, the local authentication application **104** receives the secret code (or other authentication data) provided by the relying party **151** and securely transmits the secret code to the local secure transaction device **150** for authentication (e.g., via a barcode or using other communication techniques as discussed above). Alternatively, in one embodiment, the user may manually enter the secret code in the local secure transaction device **150**. Similarly, authentication data such as a secret code received by the local secure transaction device **150** may be relayed to the local authentication application **104** which then relays the authentication data to the authentication engine **110** and/or relying party **151** (e.g., as proof of the location of the client device **100**).

[0040] One embodiment of a method for performing authentication of a client device is illustrated in FIG. 3. The method may be implemented on the architecture shown in FIGS. 1-2 but is not limited to any particular system architecture.

[0041] At **301**, the client enters the vicinity of the local secure transaction device (e.g., an ATM) and, at **302**, a secure connection is established with the local secure transaction device over a local channel. As mentioned, the local channel may be implemented using near field communication, Bluetooth, Wifi, or any other type of protocol supported by both the client device and the local secure transaction device. Operation **302** may not be required in some embodiments.

For example, when the client device is capable of authenticating with the relying party with a high level of assurance that the legitimate user is in possession of the client device and if the client device is capable of verifying its current location to the relying party, then the local channel may not be necessary.

[0042] At **303**, the client device authenticates with the relying party over the network. Any available techniques for generating an assurance level that the legitimate user is in possession of the device may be used for this operation. For example, the user may perform explicit authentication by swiping a finger on a biometric fingerprint device, capturing a facial image for facial recognition, and/or entering a secret code. Alternatively, non-intrusive authentication techniques may be performed such as determining whether the user has explicitly authenticated with the client device recently (e.g., within a specified time period) and/or using sensor data such as location data, temperature/pressure data, and/or accelerometer data.

[0043] Regardless of how the assurance level is generated, the results of the authentication may be provided to the relying party over the network in a manner which protects the user's privacy (e.g., without providing data that specifically identifies the client device). For example, as previously mentioned, the assurance level itself and/or an indication of the success or failure of authentication may be provided to the relying party, without disclosing any confidential user information.

[0044] If authentication is successful, determined at **304**, then at **307** the local transaction is permitted. In one embodiment, this involves the relying party transmitting a signal instructing the local secure transaction device to perform one or more operations. For example, if the local secure transaction device is an ATM, then the operations may include dispensing a user-specified amount of cash. If the local secure transaction device is a debit device (e.g., at a retail store or other location where the user is making a purchase), then the signal transmitted by the relying party may confirm payment for the transaction (and debit the user's account accordingly). It should be noted that these are merely illustrative examples. Various alternative applications may be employed while still complying with the underlying principles of the invention.

[0045] If the authentication at **304** is unsuccessful (e.g., because an acceptable assurance level was not reached), then at **305**, the transaction is denied and/or one or more additional authentication techniques may be required. For example, the user may be required to provide additional authentication using one or more additional techniques (e.g., entering a secret code if the initial authentication was a fingerprint, etc.). If the additional techniques are sufficient, determined at **306**, then the transaction is permitted at **307**. If not, then the transaction is again denied and/or additional authentication techniques are attempted.

Exemplary System Architectures

[0046] It should be noted that the term "relying party" is used herein to refer, not merely to the entity with which a user transaction is attempted (e.g., a Website or online service performing user transactions), but also to the secure transaction servers implemented on behalf of that entity which may performed the underlying authentication techniques described herein. The secure transaction servers may be owned and/or under the control of the relying party or may be under the control of a third party offering secure transaction

services to the relying party as part of a business arrangement. These distinctions are specified in FIGS. 4A-B discussed below which show that the “relying party” may include Websites **431** and other network services **451** as well as the secure transaction servers **432-433** for performing the authentication techniques on behalf of the websites and network services.

[0047] In particular, FIGS. 4A-B illustrate two embodiments of a system architecture comprising client-side and server-side components for authenticating a user. The embodiment shown in FIG. 4A uses a browser plugin-based architecture for communicating with a website while the embodiment shown in FIG. 4B does not require a browser. The various techniques described herein for performing strong authentication on local devices may be implemented on either of these system architectures. For example, the authentication engine **110** and local authentication application **104** shown in FIGS. 1-2 may be implemented as part of the secure transaction service **401** including interface **402**. It should be noted, however, that the embodiment illustrated in FIGS. 1-2 stands on its own and may be implemented using logical arrangements of hardware and software other than those shown in FIGS. 4A-B.

[0048] Turning to FIG. 4A, the illustrated embodiment includes a client **400** equipped with one or more authentication devices **410-412** for enrolling and authenticating an end user. As mentioned above, the authentication devices **410-412** may include biometric devices such as fingerprint sensors, voice recognition hardware/software (e.g., a microphone and associated software for recognizing a user’s voice), facial recognition hardware/software (e.g., a camera and associated software for recognizing a user’s face), and optical recognition capabilities (e.g., an optical scanner and associated software for scanning the retina of a user) and non-biometric devices such as a trusted platform modules (TPMs) and smartcards. A user may enroll the biometric devices by providing biometric data (e.g., swiping a finger on the fingerprint device) which the secure transaction service **401** may store as biometric template data in secure storage **420** (via interface **402**).

[0049] While the secure storage **420** is illustrated outside of the secure perimeter of the authentication device(s) **410-412**, in one embodiment, each authentication device **410-412** may have its own integrated secure storage. Additionally, each authentication device **410-412** may cryptographically protect the biometric reference data records (e.g., wrapping them using a symmetric key to make the storage **420** secure).

[0050] The authentication devices **410-412** are communicatively coupled to the client through an interface **402** (e.g., an application programming interface or API) exposed by a secure transaction service **401**. The secure transaction service **401** is a secure application for communicating with one or more secure transaction servers **432-433** over a network and for interfacing with a secure transaction plugin **405** executed within the context of a web browser **404**. As illustrated, the Interface **402** may also provide secure access to a secure storage device **420** on the client **400** which stores information related to each of the authentication devices **410-412** such as a device identification code, user identification code, user enrollment data (e.g., scanned fingerprint or other biometric data), and keys used to perform the secure authentication techniques described herein. For example, as discussed in detail below, a unique key may be stored into each of the authentication devices and used when communicating to servers **430** over a network such as the Internet.

[0051] In addition to enrollment of devices, the secure transaction service **401** may then register the biometric devices with the secure transaction servers **432-433** over the network and subsequently authenticate with those servers using data exchanged during the registration process (e.g., encryption keys provisioned into the biometric devices). The authentication process may include any of the authentication techniques described herein (e.g., generating an assurance level on the client **400** based on explicit or non-intrusive authentication techniques and transmitting the results to the secure transaction servers **432-433**).

[0052] As discussed below, certain types of network transactions are supported by the secure transaction plugin **405** such as HTTP or HTTPS transactions with websites **431** or other servers. In one embodiment, the secure transaction plugin is initiated in response to specific HTML tags inserted into the HTML code of a web page by the web server **431** within the secure enterprise or Web destination **430** (sometimes simply referred to below as “server **430**”). In response to detecting such a tag, the secure transaction plugin **405** may forward transactions to the secure transaction service **401** for processing. In addition, for certain types of transactions (e.g., such as secure key exchange) the secure transaction service **401** may open a direct communication channel with the on-premises transaction server **432** (i.e., co-located with the website) or with an off-premises transaction server **433**.

[0053] The secure transaction servers **432-433** are coupled to a secure transaction database **440** for storing user data, authentication device data, keys and other secure information needed to support the secure authentication transactions described below. It should be noted, however, that the underlying principles of the invention do not require the separation of logical components within the secure enterprise or web destination **430** shown in FIG. 4A. For example, the website **431** and the secure transaction servers **432-433** may be implemented within a single physical server or separate physical servers. Moreover, the website **431** and transaction servers **432-433** may be implemented within an integrated software module executed on one or more servers for performing the functions described below.

[0054] As mentioned above, the underlying principles of the invention are not limited to a browser-based architecture shown in FIG. 4A. FIG. 4B illustrates an alternate implementation in which a stand-alone application **454** utilizes the functionality provided by the secure transaction service **401** to authenticate a user over a network. In one embodiment, the application **454** is designed to establish communication sessions with one or more network services **451** which rely on the secure transaction servers **432-433** for performing the user/client authentication techniques described in detail below.

[0055] In either of the embodiments shown in FIGS. 4A-B, the secure transaction servers **432-433** may generate the keys which are then securely transmitted to the secure transaction service **401** and stored into the authentication devices within the secure storage **420**. Additionally, the secure transaction servers **432-433** manage the secure transaction database **440** on the server side.

[0056] Embodiments of the invention may include various steps as set forth above. The steps may be embodied in machine-executable instructions which cause a general-purpose or special-purpose processor to perform certain steps. Alternatively, these steps may be performed by specific hardware components that contain hardwired logic for performing

the steps, or by any combination of programmed computer components and custom hardware components.

[0057] Elements of the present invention may also be provided as a machine-readable medium for storing the machine-executable program code. The machine-readable medium may include, but is not limited to, floppy diskettes, optical disks, CD-ROMs, and magneto-optical disks, ROMs, RAMs, EPROMs, EEPROMs, magnetic or optical cards, or other type of media/machine-readable medium suitable for storing electronic program code.

[0058] Throughout the foregoing description, for the purposes of explanation, numerous specific details were set forth in order to provide a thorough understanding of the invention. It will be apparent, however, to one skilled in the art that the invention may be practiced without some of these specific details. For example, it will be readily apparent to those of skill in the art that the functional modules and methods described herein may be implemented as software, hardware or any combination thereof. Moreover, although some embodiments of the invention are described herein within the context of a mobile computing environment, the underlying principles of the invention are not limited to a mobile computing implementation. Virtually any type of client or peer data processing devices may be used in some embodiments including, for example, desktop or workstation computers. Accordingly, the scope and spirit of the invention should be judged in terms of the claims which follow.

We claim:

1. A method comprising:
 - receiving a request from a client device to perform a transaction at a local transaction device; and
 - performing one or more authentication transactions including receiving biometric input from the user on the client device to generate an authentication result;
 - transmitting the authentication result to a remote secure transaction service; and
 - the remote secure transaction service transmitting a signal to the local transaction device to perform one or more operations if the authentication result is sufficient to complete the transaction.
2. The method as in claim 1 wherein performing one or more authentication transactions comprises determining an assurance level that a current user of the client is a legitimate user for the transaction.
3. The method as in claim 2 further comprising:
 - establishing a local communication channel between the client device and the local transaction device; and
 - utilizing the local communication channel for one of the one or more authentication transactions.
4. The method as in claim 3 wherein the local communication channel comprises a near field communication (NFC) channel, a Bluetooth communication channel and/or a Wifi communication channel.
5. The method as in claim 3 wherein the client device receives first authentication data from the remote secure transaction service and passes the authentication data to the local transaction device over the local communication channel.
6. The method as in claim 5 wherein the first authentication data comprises a code transmitted to the local transaction device over the local communication channel.
7. The method as in claim 1 wherein the local transaction device comprises a automatic teller machine (ATM) and

wherein the one or more operations includes dispensing a user-specified amount of cash.

8. The method as in claim 1 wherein the assurance level is determined based, at least in part, on one or more explicit user authentication operations in which the biometric data provided by the user is compared against biometric reference data.

9. The method as in claim 8 wherein the biometric data comprises fingerprint data, facial image data, and/or voice data.

10. The method as in claim 8 wherein the assurance level is determined based, at least in part, on results of one or more non-intrusive authentication techniques in which the user is not required to enter biometric or other user data.

11. The method as in claim 9 wherein the non-intrusive authentication techniques include determining a period of time since a last explicit user authentication.

12. The method as in claim 9 wherein the non-intrusive authentication techniques include collecting and analyzing sensor data from one or more sensors on the client device.

13. The method as in claim 12 wherein at least one of the sensors comprises a location sensor indicating a current location of the client device.

14. A system comprising:

a local transaction device;

a client device performing one or more authentication transactions including receiving biometric input from the user to generate an authentication result;

a secure transaction service communicatively coupled to the local transaction device over a network, the secure transaction service receiving the authentication result from the client device; and

the remote secure transaction service transmitting a signal to the local transaction device to perform one or more operations if the authentication result is sufficient to complete a transaction.

15. The system as in claim 14 wherein performing one or more authentication transactions comprises determining an assurance level that a current user of the client is a legitimate user for the transaction.

16. The system as in claim 15 further comprising:

a first communication interface on the local transaction device;

a second communication interface on the client device;

wherein the client device and the local transaction device establish a local communication channel through the network interfaces and utilize the local communication channel for one of the one or more authentication transactions.

17. The system as in claim 16 wherein the local communication channel comprises a near field communication (NFC) channel, a Bluetooth communication channel and/or a Wifi communication channel.

18. The system as in claim 16 wherein the client device receives first authentication data from the remote secure transaction service and passes the authentication data to the local transaction device over the local communication channel.

19. The system as in claim 18 wherein the first authentication data comprises a code transmitted to the local transaction device over the local communication channel.

20. The system as in claim 14 wherein the local transaction device comprises a automatic teller machine (ATM) and

wherein the one or more operations includes dispensing a user-specified amount of cash.

21. The system as in claim **14** wherein the assurance level is determined based, at least in part, on one or more explicit user authentication operations in which the biometric data provided by the user is compared against biometric reference data.

22. The system as in claim **21** wherein the biometric data comprises fingerprint data, facial image data, and/or voice data.

23. The system as in claim **21** wherein the assurance level is determined based, at least in part, on results of one or more non-intrusive authentication techniques in which the user is not required to enter biometric or other user data.

24. The system as in claim **22** wherein the non-intrusive authentication techniques include determining a period of time since a last explicit user authentication.

25. The system as in claim **22** further comprising one or more sensors on the client device, wherein the non-intrusive authentication techniques include collecting and analyzing sensor data collected from the one or more sensors.

26. The system as in claim **25** wherein at least one of the sensors comprises a location sensor indicating a current location of the client device.

* * * * *