US 20250267449A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2025/0267449 A1**

Narendra et al. (43) **Pub. Date: Aug. 21, 2025**

(54) **WEARABLE IDENTITY DEVICE FOR FINGERPRINT BOUND ACCESS TO A CLOUD SERVICE**

(71) Applicant: **SideAssure, Inc.**, Camas, WA (US)

(72) Inventors: **Siva G. Narendra**, Portland, OR (US); **Prabhakar Tadepalli**, Bangalore (IN); **Saurav Chakraborty**, West Bengal (IN); **Donald Allen Bloodworth**, Camas, WA (US)

(73) Assignee: **SideAssure, Inc.**, Camas, WA (US)

(21) Appl. No.: **19/204,300**

(22) Filed: **May 9, 2025**

Related U.S. Application Data

(63) Continuation of application No. 18/517,059, filed on Nov. 22, 2023, now Pat. No. 12,302,089, which is a continuation of application No. 18/056,250, filed on Nov. 16, 2022, now Pat. No. 11,832,095, which is a continuation of application No. 17/315,148, filed on May 7, 2021, now Pat. No. 11,523,273, which is a continuation of application No. 16/932,088, filed on Jul. 17, 2020, now Pat. No. 11,006,271, which is a continuation of application No. 16/675,670, filed on Nov. 6, 2019, now Pat. No. 10,721,071, which is a continuation of application No. 16/257,956, filed on Jan. 25, 2019, now Pat. No. 10,476,675, which is a continuation of application No. 15/903,935, filed on Feb. 23, 2018, now Pat. No. 10,211,988, which is a continuation of application No. 15/069,548, filed on Mar. 14, 2016, now Pat. No. 9,906,365, which is a continuation of application No. 13/843,402, filed on Mar. 15, 2013, now Pat. No. 9,319,881.

Publication Classification

(51) **Int. Cl.**

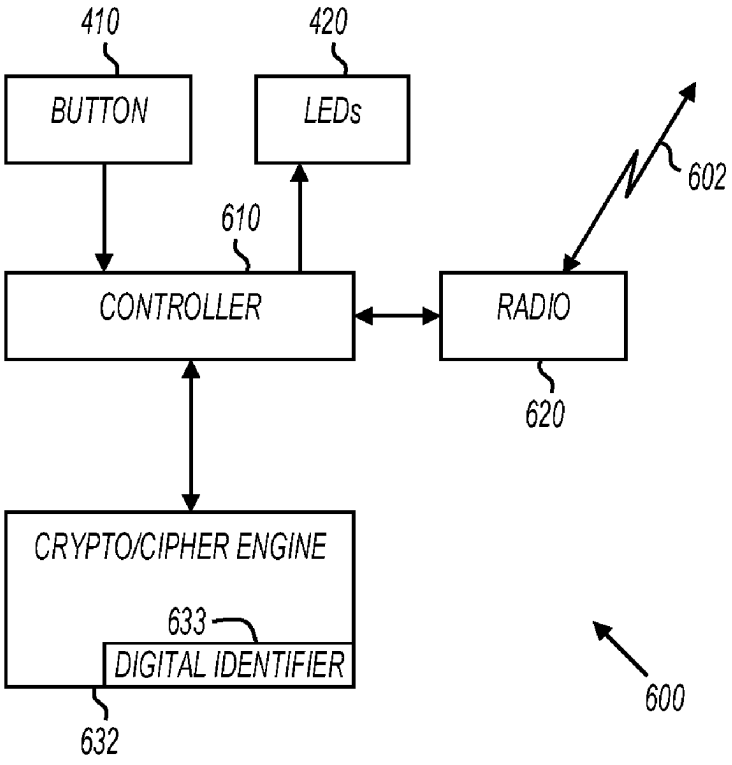
H04W 12/00	(2021.01)
H04B 5/00	(2024.01)
H04L 9/32	(2006.01)
H04L 9/40	(2022.01)
H04W 4/02	(2018.01)
H04W 4/80	(2018.01)
H04W 12/02	(2009.01)
H04W 12/06	(2021.01)
H04W 12/08	(2021.01)

(52) **U.S. Cl.**

CPC ***H04W 12/009*** (2019.01); ***H04B 5/00*** (2013.01); ***H04L 9/3231*** (2013.01); ***H04L 9/3271*** (2013.01); ***H04W 12/06*** (2013.01); ***H04W 12/068*** (2021.01); ***H04W 12/08*** (2013.01); *H04L 63/0853* (2013.01); *H04L 63/0861* (2013.01); *H04L 2209/24* (2013.01); *H04W 4/027* (2013.01); *H04W 4/80* (2018.02); *H04W 12/02* (2013.01)

(57) **ABSTRACT**

A personal digital ID device provides a digital identifier to a service for a predetermined duration in response to user interaction. The user interaction may include a button press. The personal digital ID device may be in the form of a bracelet, a key fob, or other form factor. The service may be provided by a mobile device, in the cloud, or elsewhere.



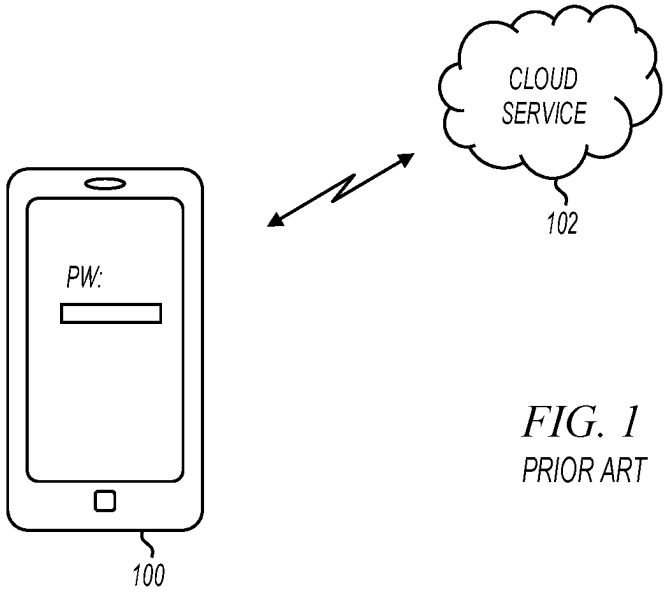


FIG. 1
PRIOR ART

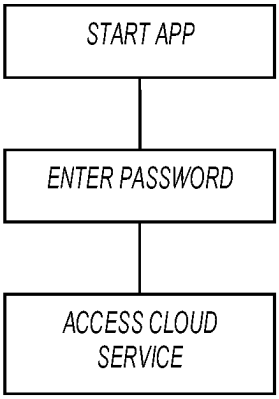


FIG. 2
PRIOR ART

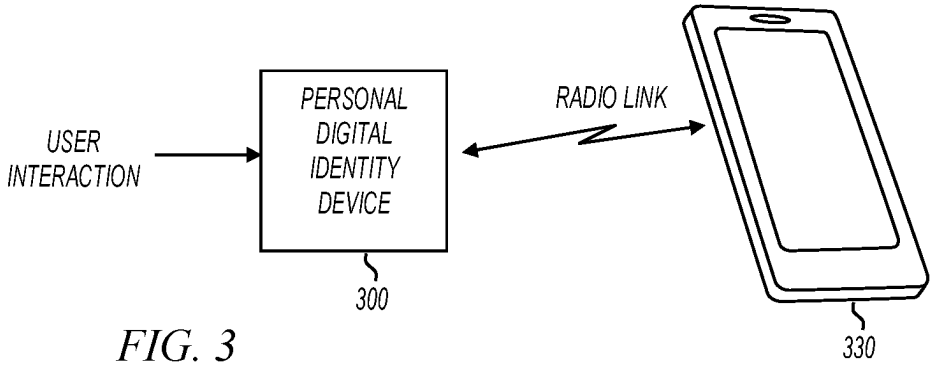


FIG. 3

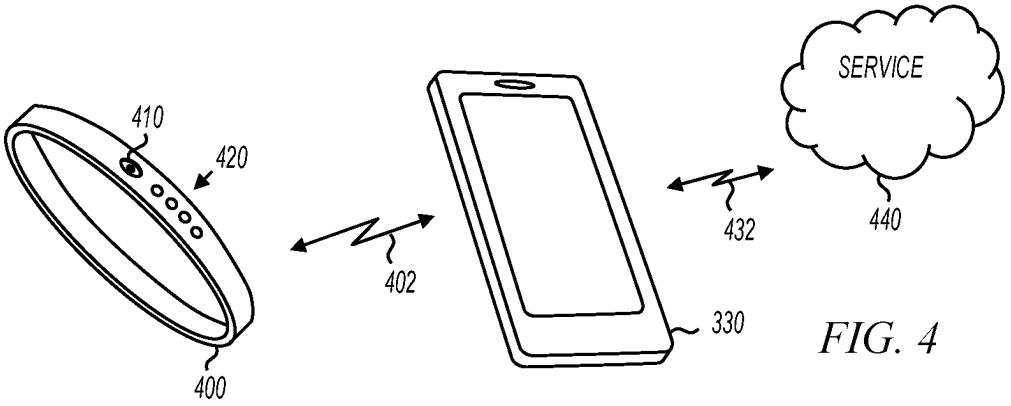


FIG. 4

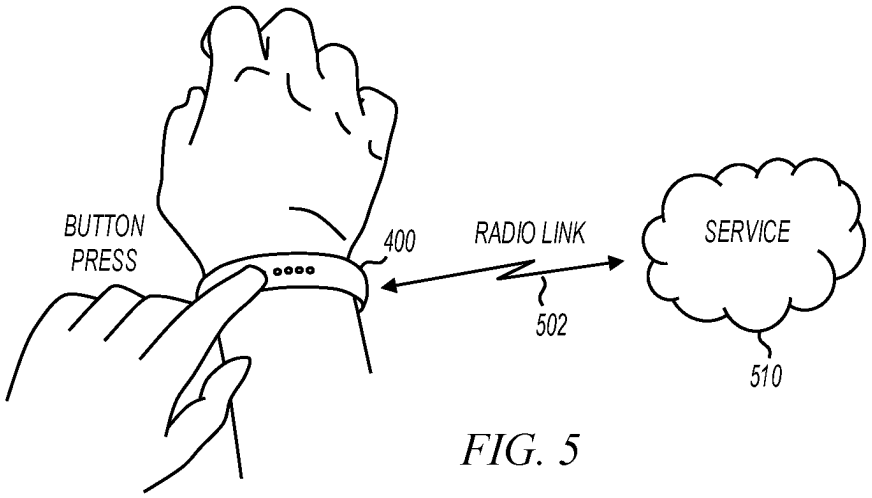


FIG. 5

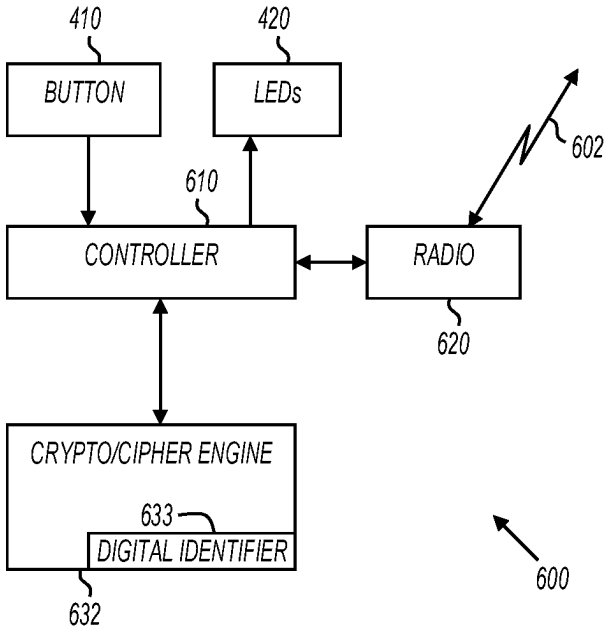

410
420
BUTTON
LEDs
602
610
CONTROLLER
RADIO
620
CRYPTO/CIPHER ENGINE
633
DIGITAL IDENTIFIER
632
600

FIG. 6

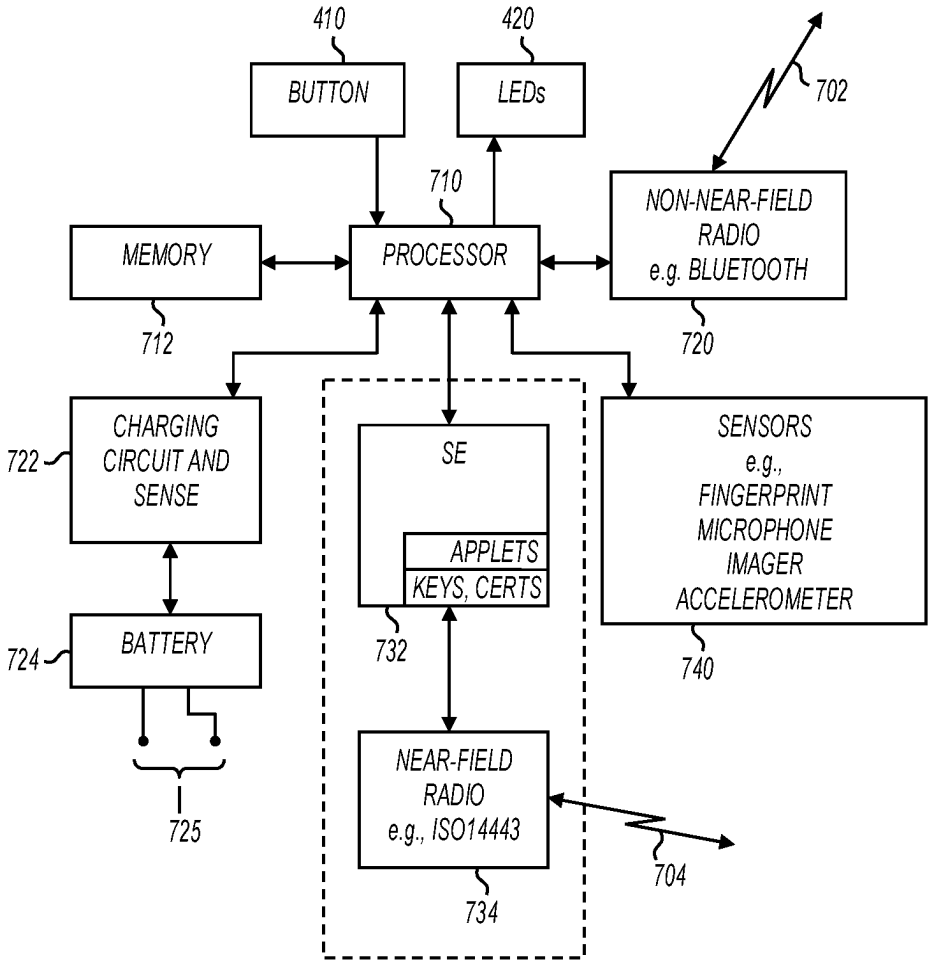

410
420
BUTTON
LEDs
702
710
NON-NEAR-FIELD
RADIO
e.g. BLUETOOTH
MEMORY
PROCESSOR
712
720
CHARGING
CIRCUIT AND
SENSE
722
SE
APPLETS
KEYS, CERTS
732
SENSORS
e.g.,
FINGERPRINT
MICROPHONE
IMAGER
ACCELEROMETER
740
BATTERY
724
725
NEAR-FIELD
RADIO
e.g., ISO14443
734
704

FIG. 7

700

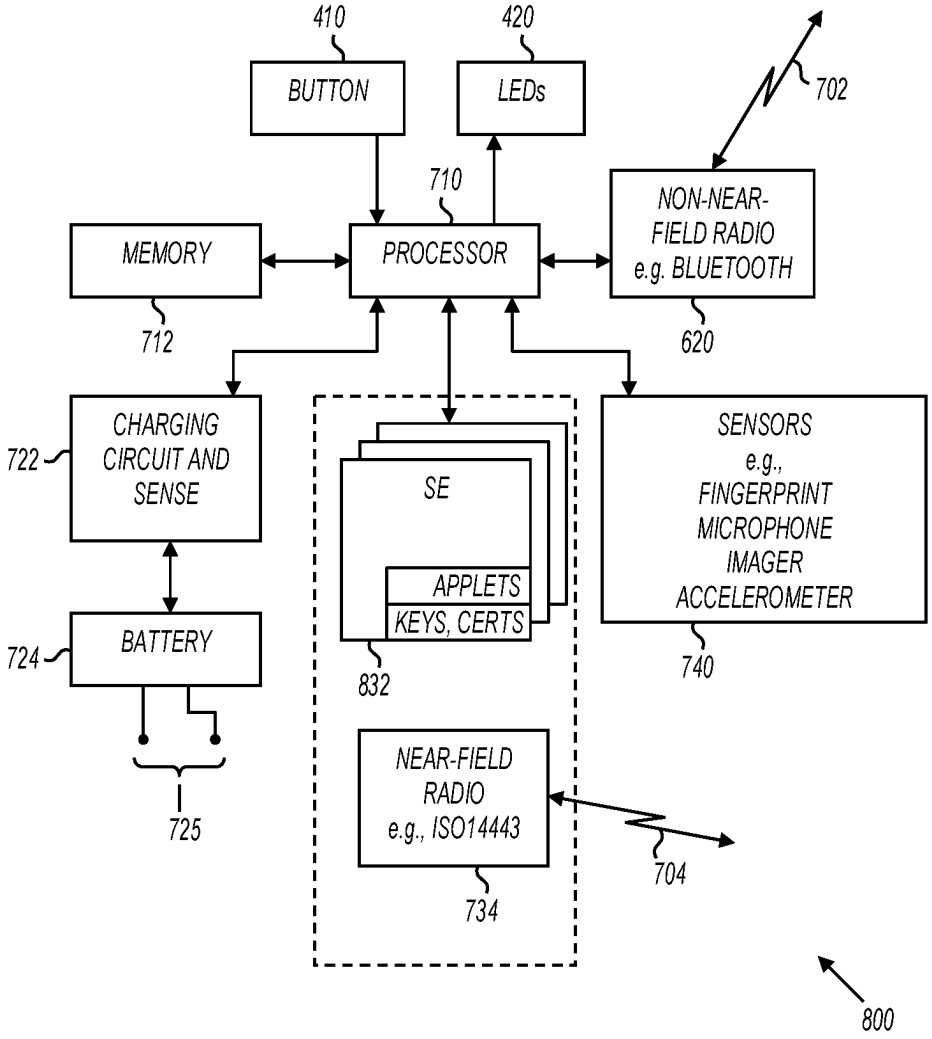

410
420
BUTTON
LEDs
702
710
NON-NEAR-FIELD RADIO e.g. BLUETOOTH
MEMORY
PROCESSOR
712
620
CHARGING CIRCUIT AND SENSE
722
SE
APPLETS
KEYS, CERTS
832
SENSORS e.g., FINGERPRINT MICROPHONE IMAGER ACCELEROMETER
740
BATTERY
724
725
NEAR-FIELD RADIO e.g., ISO14443
734
704
800

FIG. 8

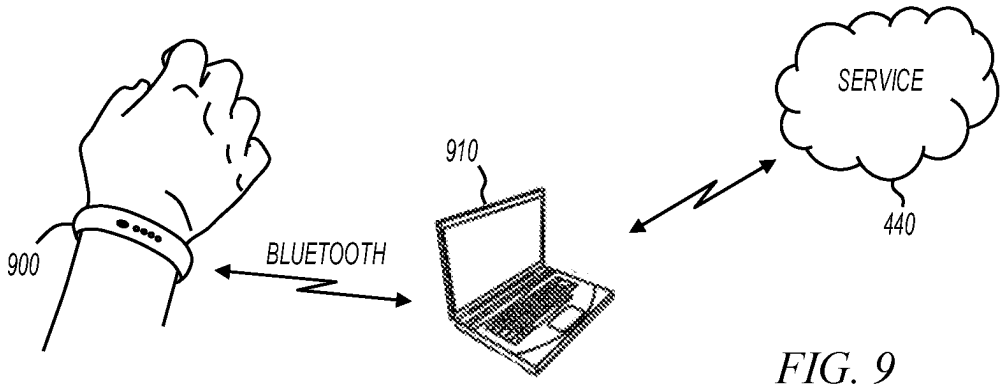


FIG. 9

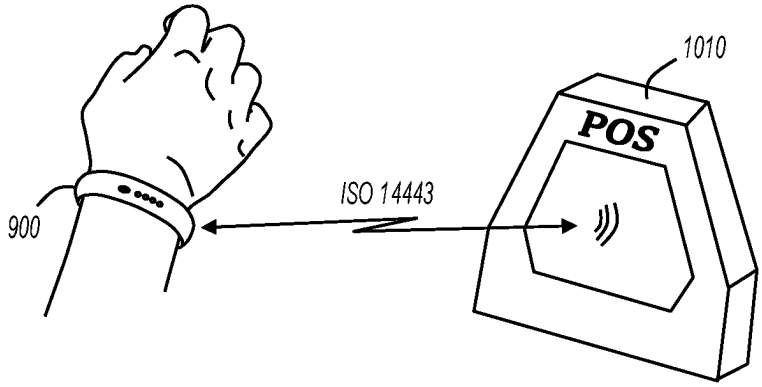


FIG. 10

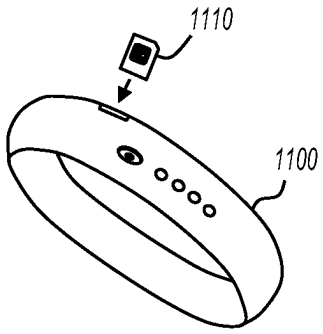


FIG. 11

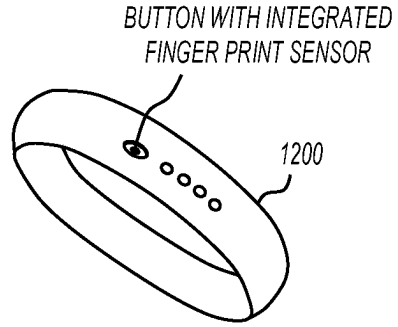

BUTTON WITH INTEGRATED
FINGER PRINT SENSOR
1200

FIG. 12

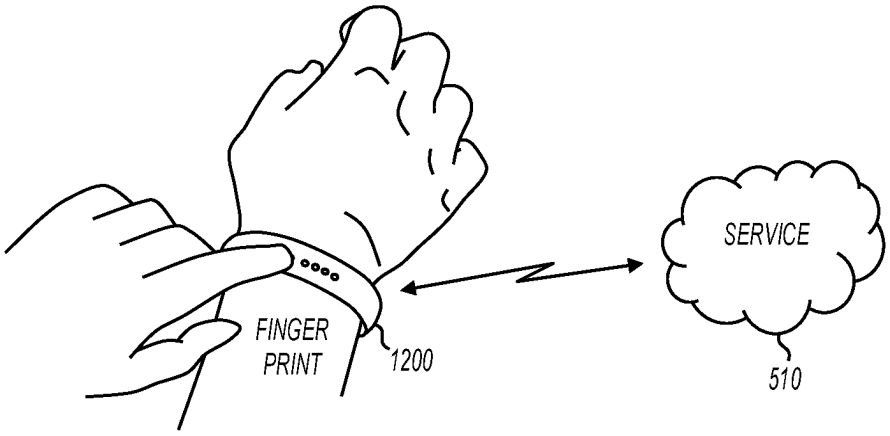

SERVICE
FINGER
PRINT
1200
510

FIG. 13

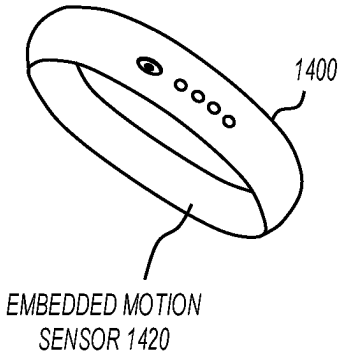


FIG. 14

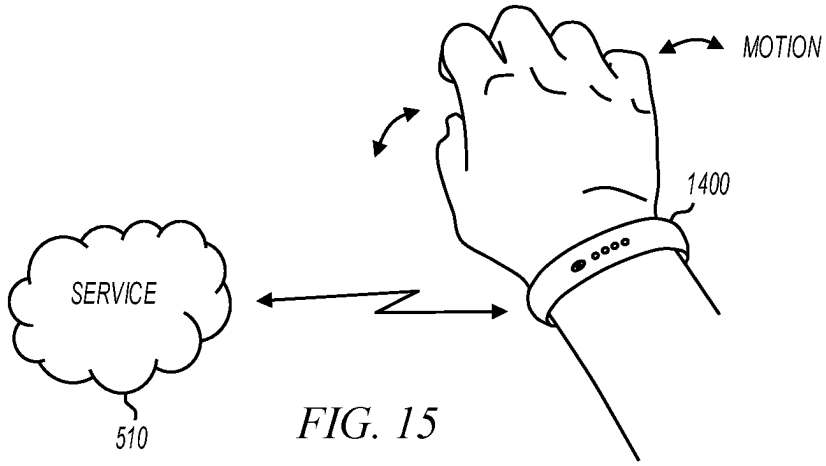


FIG. 15

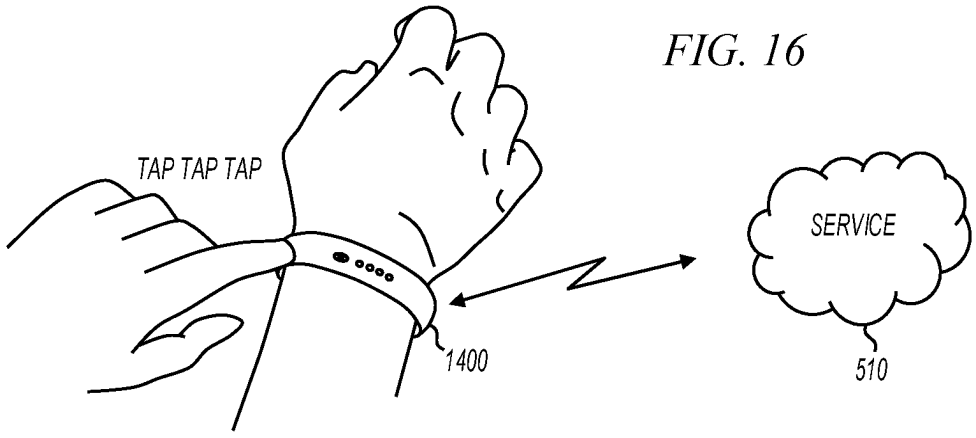


FIG. 16

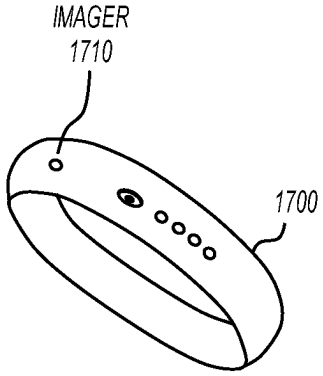

IMAGER
1710
1700

FIG. 17

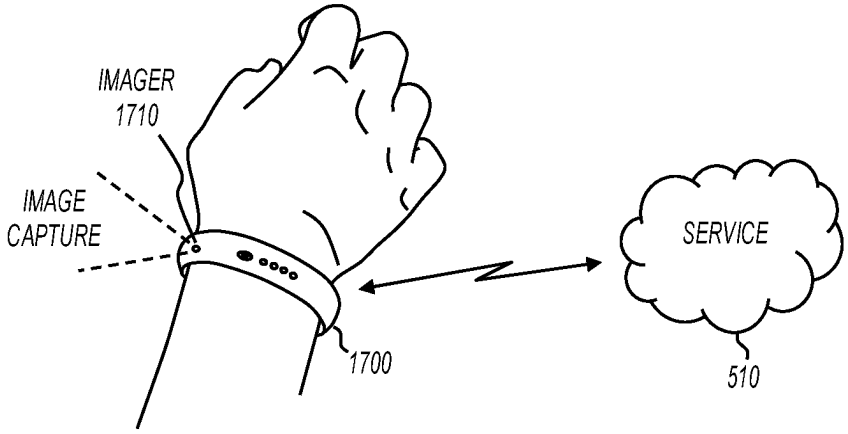

IMAGER
1710
IMAGE
CAPTURE
1700
SERVICE
510

FIG. 18

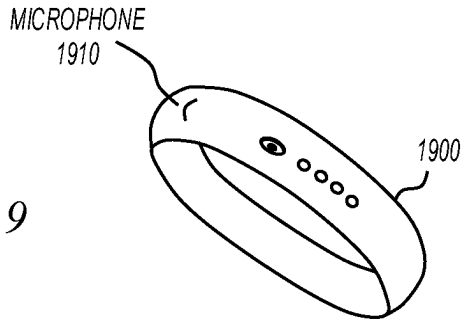

MICROPHONE
1910
1900

FIG. 19

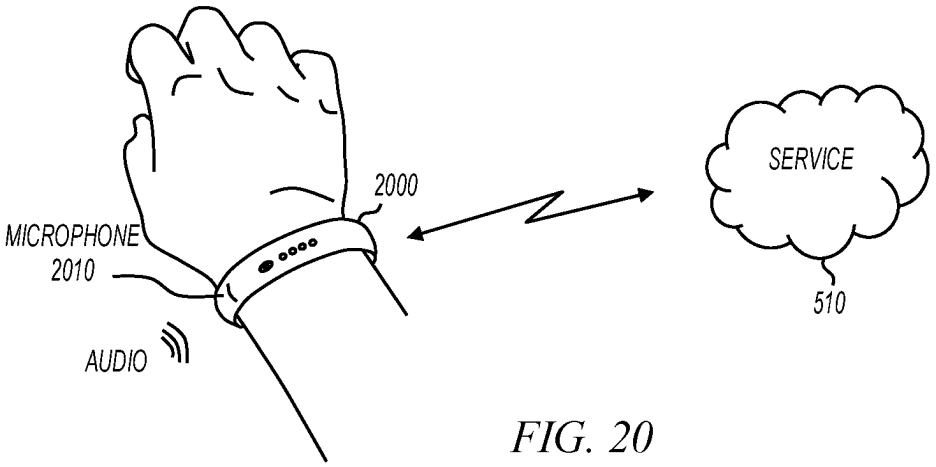

2000
MICROPHONE
2010
AUDIO
SERVICE
510

FIG. 20

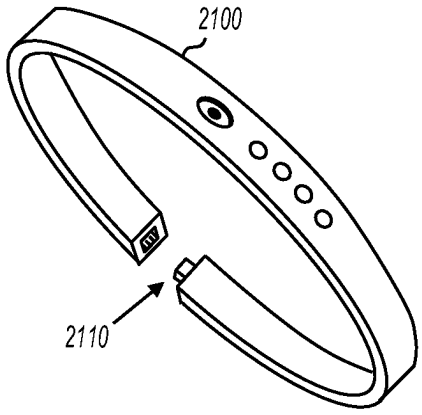


FIG. 21

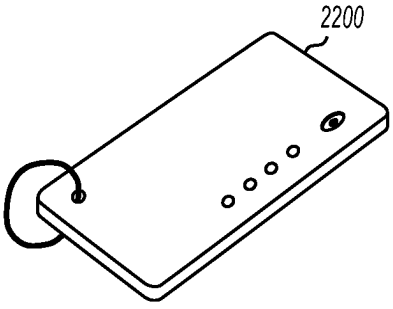


FIG. 22

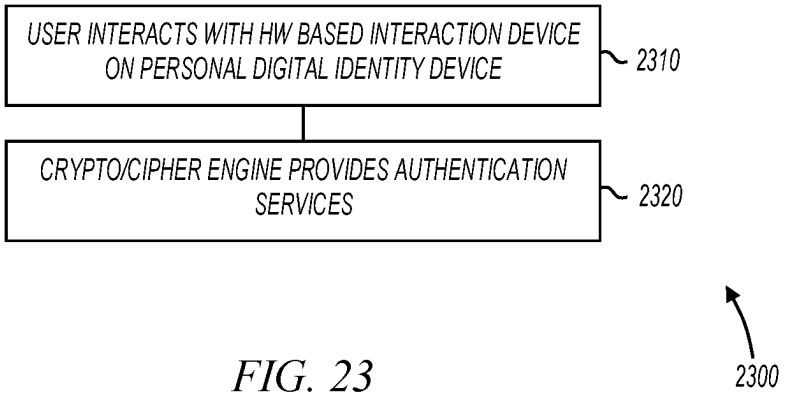

USER INTERACTS WITH HW BASED INTERACTION DEVICE ON PERSONAL DIGITAL IDENTITY DEVICE
2310
CRYPTO/CIPHER ENGINE PROVIDES AUTHENTICATION SERVICES
2320
2300

FIG. 23

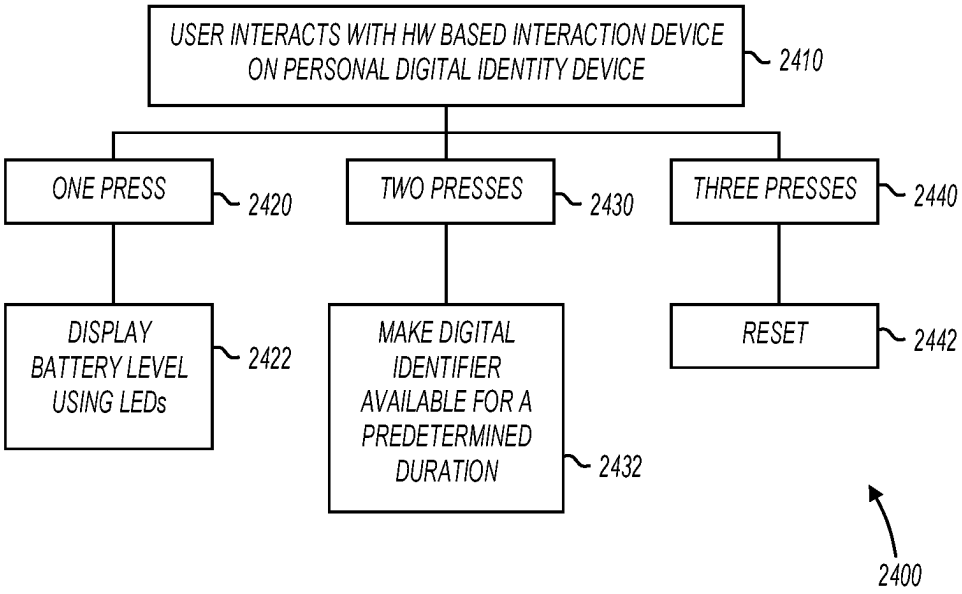

USER INTERACTS WITH HW BASED INTERACTION DEVICE ON PERSONAL DIGITAL IDENTITY DEVICE
2410
ONE PRESS
2420
TWO PRESSES
2430
THREE PRESSES
2440
DISPLAY BATTERY LEVEL USING LEDs
2422
MAKE DIGITAL IDENTIFIER AVAILABLE FOR A PREDETERMINED DURATION
2432
RESET
2442
2400

FIG. 24

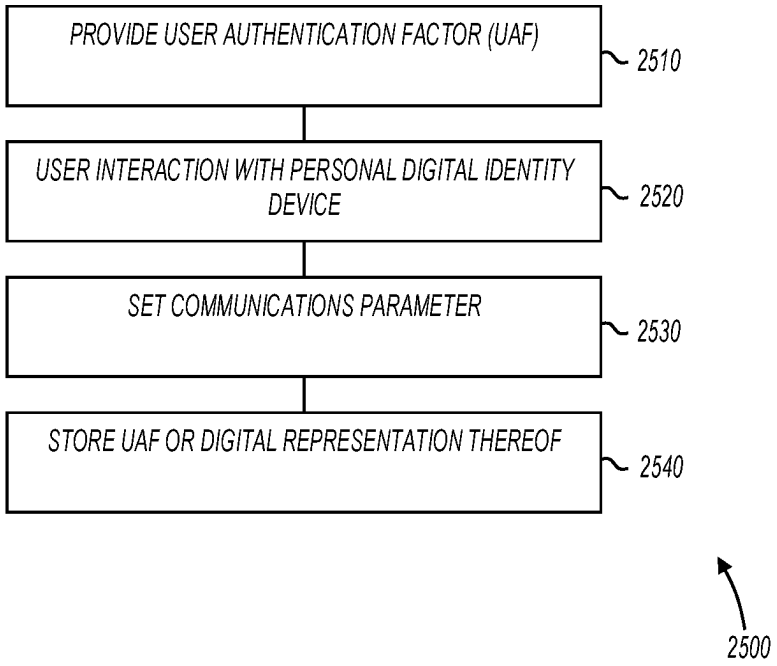

PROVIDE USER AUTHENTICATION FACTOR (UAF)
2510
USER INTERACTION WITH PERSONAL DIGITAL IDENTITY DEVICE
2520
SET COMMUNICATIONS PARAMETER
2530
STORE UAF OR DIGITAL REPRESENTATION THEREOF
2540
2500

FIG. 25

WEARABLE IDENTITY DEVICE FOR FINGERPRINT BOUND ACCESS TO A CLOUD SERVICE

CLAIM FOR PRIORITY

[0001] This application is a Continuation of, and claims the benefit of priority to U.S. patent application Ser. No. 18/517,059, filed Nov. 22, 2023, which is a Continuation of, and claims the benefit of priority to U.S. patent application Ser. No. 18/056,250, filed Nov. 11, 2016, which is a Continuation of, and claims the benefit of priority to U.S. patent application Ser. No. 17/315,148, filed May 7, 2021, now issued as U.S. Pat. No. 11,523,273 on Dec. 6, 2022, which is a Continuation of, and claims the benefit of priority to U.S. patent application Ser. No. 16/932,088, filed Jul. 17, 2020, now issued as U.S. Pat. No. 11,006,271 on May 11, 2021, which is a Continuation of, and claims the benefit of priority to U.S. patent application Ser. No. 16/675,670, filed Nov. 6, 2019, now issued as U.S. Pat. No. 10,721,071 on Jul. 21, 2020, which is a Continuation of, and claims the benefit of priority to U.S. patent application Ser. No. 16/257,956, on Jan. 25, 2019, now issued as U.S. Pat. No. 10,476,675, on Nov. 12, 2019, which is a Continuation of, and claims the benefit of priority to U.S. patent application Ser. No. 15/903,935, on Feb. 23, 2018, now issued as U.S. Pat. No. 10,211,988 on Feb. 19, 2019, which is a Continuation of, and claims the benefit of priority to U.S. patent application Ser. No. 15/069,548, on Mar. 14, 2016, now issued as U.S. Pat. No. 9,906,365 on Feb. 27, 2018, which is a Continuation of, and claims the benefit of priority to U.S. patent application Ser. No. 13/843,402, on Mar. 15, 2013, now issued as U.S. Pat. No. 9,319,881 on Apr. 19, 2016, and which is incorporated by reference in entirety.

FIELD

[0002] The present invention relates generally to mobile devices, and more specifically to identity representation in mobile devices.

BACKGROUND

[0003] Mobile devices typically authenticate to cloud services using passwords. For example, as shown in FIG. **1**, mobile device **100** may prompt a user for a password in order access cloud service **102**. This operation is also shown in FIG. **2**, where an application is started on the mobile device, and then a user enters a password to access the cloud service.

[0004] As an example, a user may open a web browser on a smartphone (or any other app on the mobile device) and then navigate to a merchant's website (cloud service). The merchant website then prompts for the user's password prior to allowing the user access to the user's account at the merchant. The user's account at the merchant may store sensitive information such as credit card numbers, addresses, phone numbers, and the like.

[0005] Password-based cloud service authentication is vulnerable to hacking. If a hacker gains access to a password file (storing hashed passwords) from the merchant, then the universe of hashed password values can be compared to entries in the password file to gain access to individual user accounts. Sensitive user information may be compromised as a result.

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] FIGS. **1** and **2** show a mobile device authenticating to a cloud service in accordance with the prior art;

[0007] FIG. **3** shows a block diagram of a personal digital identity device interacting with a user and a mobile device in accordance with various embodiments of the present invention;

[0008] FIG. **4** shows a personal digital identity device interacting with a mobile device and cloud service in accordance with various embodiments of the present invention;

[0009] FIG. **5** shows a user interacting with the personal digital identity device of FIG. **4**;

[0010] FIGS. **6**, **7**, and **8** show block diagrams of personal digital identity devices in accordance with various embodiments of the present invention;

[0011] FIG. **9** shows a personal digital identity device interacting with a laptop computer and cloud service in accordance with various embodiments of the present invention;

[0012] FIG. **10** shows a personal digital identity device interacting with a point of sale terminal in accordance with various embodiments of the present invention;

[0013] FIG. **11** shows a personal digital identity device with a removable crypto/cipher engine in accordance with various embodiments of the present invention;

[0014] FIG. **12** shows a personal digital identity device with a fingerprint sensor in accordance with various embodiments of the present invention;

[0015] FIG. **13** shows a user interacting with the personal digital identity device of FIG. **12**;

[0016] FIG. **14** shows a personal digital identity device with a motion sensor in accordance with various embodiments of the present invention;

[0017] FIGS. **15** and **16** show users interacting with the personal digital identity device of FIG. **14**;

[0018] FIG. **17** shows a personal digital identity device with an imager in accordance with various embodiments of the present invention;

[0019] FIG. **18** shows a user interacting with the personal digital identity device of FIG. **17**;

[0020] FIG. **19** shows a personal digital identity device with a microphone in accordance with various embodiments of the present invention;

[0021] FIG. **20** shows a user interacting with the personal digital identity device of FIG. **19**;

[0022] FIG. **21** shows a personal digital identity device with a connector;

[0023] FIG. **22** shows an alternate form factor personal digital identity device in accordance with various embodiments of the present invention; and

[0024] FIGS. **23-25** show flowcharts of methods in accordance with various embodiments of the present invention.

DESCRIPTION OF EMBODIMENTS

[0025] In the following detailed description, reference is made to the accompanying drawings that show, by way of illustration, various embodiments of an invention. These embodiments are described in sufficient detail to enable those skilled in the art to practice the invention. It is to be understood that the various embodiments of the invention, although different, are not necessarily mutually exclusive. For example, a particular feature, structure, or characteristic described in connection with one embodiment may be

implemented within other embodiments without departing from the scope of the invention. In addition, it is to be understood that the location or arrangement of individual elements within each disclosed embodiment may be modified without departing from the scope of the invention. The following detailed description is, therefore, not to be taken in a limiting sense, and the scope of the present invention is defined only by the appended claims, appropriately interpreted, along with the full range of equivalents to which the claims are entitled. In the drawings, like numerals refer to the same or similar functionality throughout the several views.

[0026] FIG. **3** shows a block diagram of a personal digital identity device interacting with a user and a mobile device in accordance with various embodiments of the present invention. Personal digital identity (ID) device **300** is shown communicating with mobile device **330** over a radio link. In some embodiments, personal digital ID device **300** stores a digital identifier that is provided to mobile device **330** only after a user interacts with device **300**. For example, the radio link may be available only after user interaction with personal digital ID device **300**. Mobile device **330** may be any electronic device such as a smartphone, a table, a personal computer, a laptop, a phablet, a mobile phone, a set top box, a kiosk, a point-of-sale terminal, or the like.

[0027] The digital identifier provided by personal digital ID device **300** may be used for authentication. For example, the user in possession of personal digital ID device **300** may interact with the device for the purpose of authenticating to mobile device **330** or authenticating to a service in communication with mobile device **300**. Personal digital ID device **300** may take any form. For example, personal digital ID device **300** may be a bracelet, a card, a key fob, or the like.

[0028] FIG. **4** shows a personal digital identity device interacting with a mobile device and cloud service in accordance with various embodiments of the present invention. Personal digital ID device **400** communicates with mobile device **330** over radio link **402**, and mobile device **330** communicates with a cloud service **440** over radio link **432**. The combination of elements shown in FIG. **4** may be advantageously used to increase security when accessing cloud services using a mobile device.

[0029] In some embodiments, radio link **402** is a near-field radio link and in other embodiments, radio link **402** is a non-near-field radio link. For example, radio link **402** may be a BLUETOOTH™ radio link (non-near-field), or may be a near-field communications (NFC) radio link (near-field) such as an ISO 14443 compatible radio link, an ISO 18092 compatible radio link, or an IEEE 802.15.4 compatible radio link.

[0030] As used herein, the term "near-field" refers to communication protocols and compatible radios in which the maximum intended communication distance is less than the wavelength of the radio wave used for that communication. ISO 14443 (NFC) is an example of near-field because the wavelength is on the order of 870 inches and the intended communication distance is only a few inches. All communications protocols and compatible radios that are not near-field are referred to herein as "non-near-field." An example of a non-near-field protocol is BLUETOOTH™ because the wavelength is on the order of 4.5 inches and the intended communication distance is typically much greater than 4.5 inches. The use of the term "non-near-field radio" is not meant to imply that the distance of communication cannot be less than the wavelength for the non-near-field radio.

[0031] Communication link **432** between mobile device **330** and cloud service **440** may be any type of link that is possible between a mobile device and cloud service. For example, communication link **432** may be a radio link such as a cell phone signal or a WiFi signal, or may be a wired link such as a universal serial bus (USB) or Ethernet link.

[0032] Personal digital ID device **400** includes button **410** and light emitting diodes (LEDs) **420**. In some embodiments, personal digital ID device **400** includes a housing in the shape of a personal accessory. For example, personal digital ID device **400** is shown as a bracelet in FIG. **4**. In some embodiments the housing is flexible, such that the personal digital ID device may be stretched. In other embodiments, the housing is rigid. One skilled in the art will understand that personal digital ID device **400** may be constructed from various different materials to achieve a desired level of pliability, and constructed in various different shapes and sizes.

[0033] In operation, a user may start an application on mobile device **330** with the intention of accessing cloud services **440**. The application then prompts the user to press button **410** on personal digital ID device **400**. Personal digital ID device **400** then communicates with mobile device **330** over radio link **402**. In some embodiments, personal digital ID device **400** includes security hardware that provides a secure level of authentication only after button **410** is pressed. In these embodiments, user interaction (button press) with personal digital ID device **400** is required before authentication can take place.

[0034] In some embodiments, secure authentication may take place between personal digital ID device **400** and mobile device **330**. For example, a button press may make security hardware within personal digital ID device **400** available for authentication purposes for a predetermined period of time. Mobile device **330** may then communicate with security hardware within personal digital ID device **400** to authenticate the user to the mobile device.

[0035] In other embodiments, secure authentication may take place between personal digital ID device **400** and cloud service **440**. For example, a button press may make security hardware within personal digital ID device **400** available for authentication purposes for a predetermined period of time. Cloud service **440** may then communicate with the security hardware within personal digital ID device **400** to authenticate the user to the cloud service. Because personal digital ID device **400** uses radio link **402** to reach mobile device **330** which in turn uses communication link **432** to reach service **440**, one can say that in some embodiments, personal digital ID device **400** is able to communicate with service **440** with the mobile device **330** as an intermediary. In these embodiments, both mobile device **330** and personal digital ID device **400** are used for successful access to service **440**.

[0036] Because personal digital ID device **400** requires user interaction before making the security hardware available, a user must be in possession of personal digital ID device **400** in order to be authenticated. This is significantly more robust than a password-only authentication method. Hackers are unable to hack into a user's account using software techniques alone.

[0037] Button **410** is an example of a hardware-based interaction device. Authentication is only possible after the

user interacts with the hardware-based interaction device. The various embodiments of the present invention are not limited to a button. For example, any type of hardware interaction may be employed without departing from the scope of the present invention. Additional examples of hardware-based interactions devices are described below.

[0038] Light emitting diodes **420** may be used for any purpose. For example, in some embodiments, LEDs **420** are used to provide the user with state information such as battery level or connection state. In some embodiments, LEDs **420** include at least one red LED and at least one non-red LED. Battery charge information may be provided by illuminating a number of non-red LEDs corresponding to the charge remaining. When a low battery level exists, one or more red LEDs may be illuminated. As shown in FIG. **4**, LEDs **420** may be located in a line on personal digital ID device **400**, but this is not a limitation of the present invention.

[0039] An example authentication sequence between personal digital ID device **400** and cloud service **440** is now described. This example uses an online bookseller as the cloud service, a smartphone as the mobile device, and a bracelet shaped personal digital ID device with a button. The online bookseller stores credit card information in a user's account and requires users to authenticate to the cloud service before allowing access to the user's account.

[0040] A user in possession of both personal digital ID device **400** and mobile device **330** wishes to purchase an item from the bookseller's online store. The user opens an application on mobile device **330**. This application may be a web browser or any other application that provides access to the bookseller's online store. The mobile device then prompts the user to press the button on the personal digital ID device in order to authenticate. The user presses the button and is authenticated to the online bookseller. In some embodiments, this is the extent of user involvement in the authentication process. That is to say, after one button press, the user is authenticated. In other embodiments, the authentication sequence may require more interaction from the user. For example, the user may also be required to enter a password or answer a security question using mobile device **330**, or the like.

[0041] The user authenticated by pressing the button once in previous example. In some embodiments, the user authenticates by pressing the button twice or more times. In still further embodiments, the user is authenticated only after pressing the button for longer than a predetermined duration of time (e.g., longer than a threshold).

[0042] After the user interacted with the button, one more action took place without the user's involvement. For example, in response to the button press, personal digital ID device **400** made a security mechanism available or communication over radio link **402**. In some embodiments, personal digital ID device **400** makes the security device available by powering up a radio for a predetermined amount of time.

[0043] FIG. **5** shows a user interacting with the personal digital identity device of FIG. **4**. In the example of FIG. **5**, a user is wearing personal digital ID device **400** on a wrist. The button is pressed to authenticate to service **510** over radio link **502**. Note that radio link **502** is not necessarily the same as radio link **402** (FIG. **4**). In some embodiments, radio link **402** may be a non-near-field radio link, and radio link **502** may a near-field radio link. In other embodiments, radio link **402** may be a near-field radio link, and radio link **502** may a non-near-field radio link. In still further embodiments, both radio links **402** and **502** are near-field radio links or non-near-field radio links.

[0044] Service **510** may be a service accessible on a mobile device such as mobile device **330** (FIG. **3**), or may be a service accessible through a mobile device, such as service **440** (FIG. **4**). Service **510** may also be a service unrelated to a mobile device. For example, service **510** may be a building access control device. In these embodiments, a button press may provide a user access to a building. Also, for example, service **510** may be a point of sale (POS) device, a set top box, a kiosk, or the like. In these embodiments, a button press may effect a mobile payment resulting in the purchase of digital or physical goods.

[0045] Service **510** may be thick or thin application on a smartphone, or a website running on a tablet or any combination. Service **510** may also be in the cloud, in which case, personal digital ID device **400** communicates with a mobile device (e.g., smartphone), which then communicates with the service in the cloud.

[0046] Service **510** may also be an application running on another device, such as a phone, a device in the cloud, or a device on the other end of a near-field link, such as a POS or a kiosk.

[0047] FIG. **6** shows a block diagram of a personal digital identity device in accordance with various embodiments of the present invention. Personal digital ID device **600** shows an example architecture for personal digital ID device **300** (FIG. **3**) or personal digital ID device **400** (FIG. **4**), or any of the other personal digital ID devices described herein.

[0048] Personal digital ID device **600** includes controller **610**, radio **620**, button **410**, LEDs **420**, and crypto/cipher engine **632** with digital identifier **633**. Button **410** is an example of a hardware-based interaction device as described above. LEDs **420** are also described above. Radio **620** may be any type of radio, including a near-field radio or a non-near-field radio.

[0049] Controller **610** is coupled to button **410**, LEDs **420**, radio **620**, and crypto/cipher engine **632**. Controller **610** is any type of controller capable of making digital identifier **633** available over radio link **602** in response to user interaction with button **410**. For example, in some embodiments, controller **610** may be a dedicated state machine that is not programmable beyond its initial design, although this is not a limitation of the present invention. In these embodiments, controller **610** may not be modified by a user with ill intent without modifying hardware. This is a difficult task and adds to security. In other embodiments, controller **610** is a microcontroller with a dedicated, hard coded, program store. In these embodiments, controller **610** performs actions in response to stored instructions; however, modifying instructions still requires a change in hardware. In still further embodiments, controller **610** is a processor such as a microprocessor or a digital signal processor. In these embodiments, controller **610** performs actions in response to executing stored instructions. An example personal digital ID device with a processor is described below with reference to FIG. **7**.

[0050] Crypto/cipher engine **632** is any device that can provide a secure data store and/or encryption capabilities in the service of personal digital ID device **600**. For example, in some embodiments, crypto/cipher engine **632** may be a dedicated secure storage and computation area within con-

troller **610** that stores and processes digital identifier **633**, either as encrypted data or as clear data or in any combination of encrypted and clear data. In other embodiments, controller **610** is part of the crypto/cipher engine **632** and crypto/cipher engine **632** is a smartcard secure element. In other embodiments, crypto/cipher engine **632** is separate from controller **610**, such as a smartcard secure element. Various embodiments having smartcard secure elements are described in more detail below.

[0051] In operation, personal digital ID device **600** provides identity and/or authentication services to a user in response to user interaction with the device. For example, in some embodiments, controller **610** turns on radio **620** for a predetermined period of time (e.g., a few seconds to a few minutes) in response to user interaction with button **410**. Also for example, in some embodiments, controller **610** makes services provided by crypto/cipher engine **632** (including, but not limited to, digital identifier **633**) available over radio link **620** for a predetermined period of time in response to user interaction with button **410**. The ID and/or authentication services may be used to authenticate a user to a mobile device or to a cloud service, or to any other service. The predetermined period of a few seconds to a few minutes is provided as an example, and the various embodiments of the invention are not so limited.

[0052] Digital identifier **633** may take on any form. For example, in some embodiments, digital identifier **633** may represent an actual identity such as a credit card number or a more complex combination of various data and a program executing on the data to uniquely identify the personal digital ID device. An example of a program executing could be a security applet such as PKCS #**15** or payment applet such as a Visa VSDC applet running on a java card operating system of a smartcard device. Here the smartcard device is the crypto/cipher engine. An example of various data could be an X.509 Certificate or Visa Card Personalization Data. In some embodiments, digital identifier **633** may be a fixed value, and in other embodiments, digital identifier **633** may be a variable value. For example, in some embodiments, digital identifier **633** may include random information that pads the actual useful data for obfuscation purposes.

[0053] In some embodiments, digital identifier **633** may be a password, a fingerprint, or other user authentication factor (UAF), encrypted or in the clear; digital certificates, keys, keys for symmetric or asymmetric cryptography functions, unique digital identifiers, or the like. The UAF can come to the personal digital ID device via any of the radio links, or from the personal digital ID device itself, or any combination thereof.

[0054] In some embodiments, digital identifier **633** includes two shared secret keys K**1** and K**2** that are shared with a cloud service. Once personal digital ID device **600** is made available to a cloud service, the digital ID device could generate a random number R**1**, encrypt it with the shared secret key K**1**, and send it to the cloud service. The cloud service will then decrypt R**1** with key K**1**, then encrypt with key K**2** both R**1** and another random value R**2** and send the result back to personal digital ID device **600**. Personal digital ID device **600** will then decrypt this payload with K**2**. If it successfully recovers R**1**, then it knows that it is communicating with an authenticated cloud service that it trusts. Personal digital ID device **600** then encrypts R**2** back with K**1** and sends it to the cloud service which will in turn decrypt it with K**1** and if it successfully recovers R**2**, then it knows that it is communicating with an authenticated personal digital ID device it trusts. The use of K**1**, K**2**, R**1**, and R**2** are mere examples. The authentication sequence of events is also provided as an example. Other embodiments use different authentication sequences. The authentication sequence mentioned above could involve more complex steps such as the use of public key infrastructure standards such as PKCS or involve methods for challenge-response. The connection made available could not only be used for authentication or mutual authentication but also for establishment of a secure channel between the personal digital ID device and the cloud service where additional unique data stored in the personal digital ID device such as payment information could then be communicated securely by encrypting with a session specific key such as R**2** to enact transactions in the cloud service.

[0055] Again, the use of R**2** for secure communication post secure mutual authentication is only to be considered an example. The entire set of processes defined above is to illustrate what it means to make the personal digital ID device available to a service in response to user interaction. Many such processes are possible and known to those skilled in the art of security engineering, cyber security, secure identity, identity management, trusted service management, or smartcard protocols. Such processes could also help the intermediate device send secure information to a cloud service or receive secure information from the cloud service. Such secure information could be but not limited to transactions and outcomes, additional personal information, files, emails, voice connections, and messages.

[0056] FIG. **7** shows a block diagram of a personal digital identity device in accordance with various embodiments of the present invention. Personal digital ID device **700** shows an example architecture for personal digital ID device **300** (FIG. **3**) or personal digital ID device **400** (FIG. **4**), or any of the other personal digital ID devices described herein.

[0057] Personal digital ID device **700** includes processor **710**, non-near-field radio **720**, button **410**, LEDs **420**, memory **712**, charging circuits **722**, battery **724**, sensors **740**, secure element (SE) **732**, and near-field radio **734**. Button **410** is an example of a hardware-based interaction device as described above. LEDs **420** are also described above. Although FIG. **7** shows a non-near-field radio communicating over link **702**, this is not a limitation of the present invention. For example, in some embodiments, radio **720** is a near-field radio.

[0058] Processor **710** may be any type of processor capable of executing instructions stored in memory **712** and capable of interfacing with the various components shown in FIG. **7**. For example, processor **710** may be a microprocessor, a digital signal processor, an application specific processor, or the like. In some embodiments, processor **710** is a component within a larger integrated circuit such as a system on chip (SOC) application specific integrated circuit (ASIC).

[0059] Memory **712** may include any type of memory device. For example, memory **712** may include volatile memory such as static random-access memory (SRAM), or nonvolatile memory such as FLASH memory. Memory **712** is encoded with (or has stored therein) one or more software modules (or sets of instructions), that when accessed by processor **710**, result in processor **710** performing various functions. In some embodiments, memory **710** includes a software application to turn on one or both of radios **720** and

734 in response to user interaction, and does not include an operating system (OS). The lack of an operating system increases the security of personal digital ID device **700** in part because it is more difficult for a hacker to run illicit software on the device. The lack of an operating system in personal digital ID device **700** is not a limitation of the present invention.

[0060] Memory **712** represents a computer-readable medium capable of storing instructions, that when accessed by processor **710**, result in the processor performing as described herein. For example, when processor **710** accesses instructions within memory **712**, processor **710** turns on one or both of radios **720** and **734** in response to user interaction.

[0061] Secure element **732** provides secure information storage. In some embodiments, secure element **732** is a smartcard compatible secure element commonly found in credit card applications and/or security applications. Near-field radio **734** provides near-field communications capability between mobile device personal digital ID device **700** and other devices nearby. In some embodiments, near-field radio **734** may be an ISO 14443 compatible radio operating at 13.56 megahertz, although this is not a limitation of the present invention.

[0062] In some embodiments, secure element **732** is combined with near-field radio **734** in a single integrated circuit such as a smartcard controller. In other embodiments, secure element **732**, or a combination of secure element **732** and near-field radio **734** are integrated into another semiconductor device such as processor **710**.

[0063] Examples of smart card controllers that combine secure element **732** with near-field radio **734** are the "SmartMX" controllers sold by NXP Semiconductors N.V. of Eindhoven, The Netherlands. In some embodiments, the secure element has an ISO/IEC 7816 compatible interface that communicates with other components within personal digital ID device **700** (e.g., processor **710**), although this is not a limitation of the present invention.

[0064] In some embodiments, secure element **732** includes applets, keys and digital certificates. Digital certificates are used to validate the identity of the certificate holder. Certificate authorities typically issue digital certificates. Digital certificates and their functionality are well known. Secure element applets and encryption keys are also well known. In some embodiments, personal digital ID device **700** makes available one or more of applets, keys, and/or digital certificates available to a service using either radio **720** or **734** in response to user interaction for a predetermined duration. Applets, keys, and certificates are examples of digital identifier **633** (FIG. **6**).

[0065] Sensors **740** include one or more devices that may provide for user interaction. For example, sensors **740** may include a fingerprint sensor, a microphone, an imager, a motion sensor (e.g., accelerometer), or the like. In some embodiments, processor **710** may make a digital identifier available to a service in response to user interaction with one or more of sensors **740**. Various embodiments of user interaction with sensors **740** are described more fully below.

[0066] Charging circuit **722** charges battery **724** and also senses the level of charge. For example, processor **710** may sense the battery charge level using charging circuit **722** and report the charge level using LEDs **420**.

[0067] Battery **724** may be any type of battery capable of powering the components shown in FIG. **7**. In some embodiments, battery **724** is removable, and in other embodiments, battery **724** is nonremovable.

[0068] Terminals **725** are used to provide power to the various components in personal digital ID device **700**. Individual connections are not shown. In some embodiments, terminals **725** are disconnected when a connector on personal digital ID device **700** is disconnected. See FIG. **21** below.

[0069] FIG. **8** shows a block diagram of a personal digital identity device in accordance with various embodiments of the present invention. Personal digital ID device **800** shows an example architecture for personal digital ID device **300** (FIG. **3**) or personal digital ID device **400** (FIG. **4**), or any of the other personal digital ID devices described herein.

[0070] Personal digital ID device **800** includes all the component of personal digital ID device **700** (FIG. **7**), and also includes multiple secure elements **832**. In some embodiments, the different secure elements are used for different purposes. For example, one secure element may be used for access control, while another secure element may be use for payments, and still another secure element may be used for authentication to a service.

[0071] FIG. **9** shows a personal digital identity device interacting with a laptop computer and cloud service in accordance with various embodiments of the present invention. As shown in FIG. **9**, a user is wearing personal digital ID device **900**, which is in the shape of a bracelet. Personal digital ID device **900** is shown communicating with mobile device **910** (e.g. laptop computer) using a non-near-field radio (e.g., BLUETOOTH™). The mobile device is in turn shown communicating with cloud service **440**.

[0072] Personal digital ID device **900** communicates with mobile device **900** after user interaction. Example user interactions include, but are not limited to, button presses, motions, fingerprints, images, audio communications, or the like or any combination thereof. Examples of these user interactions and others are described more fully below.

[0073] In some embodiments some or all of the user authentication factors (UAF) such as fingerprints, motions, images or even passwords or PIN, or the like, or any combination thereof or any representation of such, could come to the personal digital ID device including 900 via the a radio link such as the BLUETOOTH™ non-near-field radio from a mobile device such as the laptop computer. The type of radio link (e.g. BLUETOOTH™) and the type of mobile device (e.g. laptop computer) for the personal digital ID device to receive UAF are provided as examples and the various embodiments of the invention are not so limited.

[0074] FIG. **10** shows a personal digital identity device interacting with a point of sale terminal in accordance with various embodiments of the present invention. As shown in FIG. **10**, a user is wearing personal digital ID device **900**, which is in the shape of a bracelet. Personal digital ID device **900** is shown communicating with point of sale (POS) device **1010** using a near-field radio (e.g., ISO 14443).

[0075] Personal digital ID device **900** communicates with POS **1010** after user interaction. Example user interactions include, but are not limited to, button presses, motions, fingerprints, images, audio communications, or the like or any combination thereof. Examples of these user interactions and others are described more fully below.

[0076] FIG. **11** shows a personal digital identity device with a removable crypto/cipher engine in accordance with various embodiments of the present invention. Personal digital ID device **1100** is shown accepting a subscriber identity module (SIM) card **1110**, which includes a smartcard secure element, where the smartcard secure element is the crypto/cipher engine. In these embodiments, identities may be quickly changed. For example, a user may purchase personal digital ID device **1100** and then personalize it by inserting SIM card **1110** with the user's digital identifier installed. In some embodiments there may be more than one SIM card.

[0077] FIG. **12** shows a personal digital identity device with a fingerprint sensor in accordance with various embodiments of the present invention. Personal digital ID device **1200** includes a button with an integrated fingerprint sensor on the surface of the button. In operation, a user may press the button to interact with personal digital ID device **1200** as described above. In addition, personal digital ID device **1200** may take a fingerprint of the user.

[0078] In some embodiments, this corresponds to processor **710** (FIG. **7**) receiving a fingerprint when the user presses the button. The fingerprint (or data representing the fingerprint) may be passed to SE **732** for comparison with a stored fingerprint to validate the user. If there is a match, the user is validated, and then the personal digital ID device may allow communication with a service outside the device.

[0079] Fingerprints may also be collected or verified during setup or configuration of personal digital ID device **1200**. Setup and configuration are described more fully below.

[0080] FIG. **13** shows a user interacting with the personal digital identity device of FIG. **12**. As shown in FIG. **13**, the user wearing personal digital ID device **1200** is pressing the button and providing a fingerprint at the same time. In response to the user interaction, personal digital ID device **1200** communicates with service **510**.

[0081] In some embodiments the fingerprint user authentication factor comes to personal digital ID device **1200** via its radio link.

[0082] FIG. **14** shows a personal digital identity device with a motion sensor in accordance with various embodiments of the present invention. Personal digital ID device **1400** includes an embedded motion sensor **1420**. Embedded motion sensor **1420** may be any type of sensor capable of detecting motion. For example, motion sensor **1420** may be an accelerometer. In operation, a user may make motions to interact with personal digital ID device **1400** as described above.

[0083] In some embodiments, this corresponds to processor **710** (FIG. **7**) receiving data from motion sensor **1420** that describes motion of the device. The data representing the motion may be passed to SE **732** for comparison with a stored value to validate the user. If there is a match, the user is validated, and then the personal digital ID device may allow communication with a service outside the device.

[0084] Motion data may also be collected or verified during setup or configuration of personal digital ID device **1400**. Setup and configuration are described more fully below.

[0085] In some embodiments the motion data user authentication factor comes to the personal digital ID device **1400** via its radio link.

[0086] FIGS. **15** and **16** show users interacting with the personal digital identity device of FIG. **14**. In FIG. **15**, a user is shown interacting with personal digital ID device **1400** by making gross arm movements. In some embodiments, this may correspond to a gesture that is recognized by personal digital ID device **1400**. When the gesture is recognized, personal digital ID device **1400** may allow communication with a service outside the device.

[0087] In FIG. **16**, a user is shown interacting with personal digital ID device **1400** by making fine movements. In some embodiments, the fine movements are performed making a series of tapping motions with varying spacing and intensity. This may be viewed by a user as similar to typing a password, but instead of remembering and typing a character sequence, the user remembers and taps a rhythmic sequence.

[0088] FIG. **17** shows a personal digital identity device with an imager in accordance with various embodiments of the present invention. Personal digital ID device **1700** includes imager **1710**. Imager **1710** may be any type of image capture device. For example, imager **1710** may be a CMOS camera similar to those commonly found in smartphones. In operation, a user may capture an image to interact with personal digital ID device **1700** as described above.

[0089] In some embodiments, this corresponds to processor **710** (FIG. **7**) receiving an image from imager **1710**. The image may be of anything. For example, the image may be of a user's face, a user's personal possession, a landmark, or any other item. The data representing the image may be passed to SE **732** for comparison with a stored value to validate the user. If there is a match, then the personal digital ID device may allow communication with a service outside the device.

[0090] Image data may also be collected or verified during setup or configuration of personal digital ID device **1700**. Setup and configuration are described more fully below.

[0091] FIG. **18** shows a user interacting with the personal digital identity device of FIG. **17**. As shown in FIG. **18**, the user wearing personal digital ID device **1700** is capturing an image with imager **1710**. In response to the user interaction, the user is validated, and personal digital ID device **1700** communicates with service **510**.

[0092] In some embodiments the captured image user authentication factor comes to the personal digital ID device **1700** via its radio link.

[0093] FIG. **19** shows a personal digital identity device with a microphone in accordance with various embodiments of the present invention. Personal digital ID device **1900** includes microphone **1910**. Microphone **1910** may be visible on personal digital ID device **19**, or may not be visible. In operation, a user provides an audio signal to interact with personal digital ID device **1900** as described above.

[0094] In some embodiments, this corresponds to processor **710** (FIG. **7**) receiving audio data from microphone **1910**. The audio may represent anything. For example, a user may speak a phrase or provide another signature. The data representing the audio may be passed to SE **732** for comparison with a stored value to validate the user. If there is a match, the user is validated, and then the personal digital ID device may allow communication with a service outside the device. In some embodiments, this corresponds to performing a voiceprint analysis.

[0095] Audio data may also be collected or verified during setup or configuration of personal digital ID device **1900**. Setup and configuration are described more fully below.

[0096] FIG. **20** shows a user interacting with the personal digital identity device of FIG. **19**. As shown in FIG. **20**, the user wearing personal digital ID device **2000** is capturing audio information with microphone **2010**. In response to the user interaction, personal digital ID device **2000** communicates with service **510**.

[0097] In some embodiments the audio information user authentication factor comes to the personal digital ID device **2000** via its radio link.

[0098] FIG. **21** shows a personal digital identity device with a connector. Personal digital ID device **2100** includes connector **2110**. In some embodiments, connector **2110** is strictly a mechanical connector. For example, connector **2110** may be disconnected while all electrical functionality remains intact. In other embodiments, connector **2110** is a mechanical connector as well as an electrical connector. In these embodiments, the electrical connector may disconnect the battery when the connector is open. In operation, connector **2110** allows the bracelet shape of personal digital ID device **2100** to be open or closed.

[0099] FIG. **22** shows an alternate form factor personal digital identity device in accordance with various embodiments of the present invention. Personal digital ID device **2200** is shown as a key fob, but this is not a limitation of the present invention. For example, personal digital ID device **2200** may take any form, including for example, a credit card shape.

[0100] FIG. **23** shows a flowchart of methods in accordance with various embodiments of the present invention. In some embodiments, method **2300** may be performed by a personal digital ID device such as any of those shown in previous figures. Further, in some embodiments, method **2300** may be performed by a processor such as processor **710** (FIG. **7**). Method **2300** is not limited by the type of system or entity that performs the method. The various actions in method **2300** may be performed in the order presented, in a different order, or simultaneously. Further, in some embodiments, some actions listed in FIG. **23** are omitted from method **2300**.

[0101] Method **2300** begins at **2310** in which a user interacts with a hardware-based interaction device on a personal digital identity device. In some embodiments, this corresponds to a user pressing a button, or providing a fingerprint, motion, an image, or audio. At **2320**, a crypto/cipher engines provides authentication services.

[0102] In some embodiments, the actions of method **2300** are performed by a processor configured to perform the operations by virtue of stored software instructions. For example, processor **710** (FIG. **7**) may be configured to perform actions corresponding to receiving user interactions, and making a digital identifier available for a predetermined time in response thereto. The digital identifier may be made available by turning one or more radios, such as a near-field radio and/or a non-near-field radio.

[0103] FIG. **24** shows a flowchart of methods in accordance with various embodiments of the present invention. In some embodiments, method **2400** may be performed by a personal digital ID device such as any of those shown in previous figures. Further, in some embodiments, method **2400** may be performed by a processor such as processor **710** (FIG. **7**). Method **2400** is not limited by the type of system or entity that performs the method. The various actions in method **2400** may be performed in the order presented, in a different order, or simultaneously. Further, in some embodiments, some actions listed in FIG. **24** are omitted from method **2400**.

[0104] Method **2400** begins at **2410** in which a user interacts with a hardware-based interaction device on a personal digital identity device. In some embodiments, this corresponds to a user pressing a button, or providing a fingerprint, motion, an image, or audio. Different actions are taken depending on the number of button presses. If there has been one button press **2420**, then the personal digital ID device displays a battery level at **2422**. If there have been two button presses **2430**, then the personal digital ID device makes a digital identifier available for a predetermined duration at **2432**. If there have been three button presses **2440**, then the personal digital ID device performs a reset at **2442**.

[0105] In some embodiments, the actions of method **2400** are performed by a processor configured to perform the operations by virtue of stored software instructions. For example, processor **710** (FIG. **7**) may be configured to perform actions corresponding to receiving user interactions, and performing different actions based on the type of user interaction that occurred.

[0106] Method **2400** provides one set of possible actions that are performed in response to different user interactions. In some embodiments, different user interactions are received, and different actions are performed in response. For example, a user may press a button for a predetermined duration rather than just once, twice, etc. Any action may be taken in response to the long button press. Also for example, a user may provide a fingerprint, motion, imagery, or audio. In some embodiments, these may be provided in addition to a button press.

[0107] FIG. **25** shows a flowchart of methods in accordance with various embodiments of the present invention. In some embodiments, method **2500** may be performed by a personal digital ID device such as any of those shown in previous figures. Further, in some embodiments, method **2500** may be performed by a processor such as processor **710** (FIG. **7**). Method **2500** is not limited by the type of system or entity that performs the method. The various actions in method **2500** may be performed in the order presented, in a different order, or simultaneously. Further, in some embodiments, some actions listed in FIG. **25** are omitted from method **2500**. The actions of method **2500** provide for configuration or setup of a personal digital ID device.

[0108] Method **2500** begins at **2510** in which a user provides a user authentication factor (UAF). The user authentication factor may be any information provided by a user to authenticate. Examples include, but are not limited to voiceprint, motion, fingerprint, or imagery. At **2520**, the user interacts with the personal digital identity device. In some embodiments, this corresponds to pressing a button one or more times, or pressing a button for a predetermined duration. At **2530**, communications parameters are set. In some embodiments, this corresponds to a BLUETOOTH™ radio becoming discoverable or discovering other devices. At **2540**, the UAF (or a digital representation thereof) is stored. In some embodiments, LEDs, such as LEDs **420** (FIG. **4**) are used to report communication parameters.

[0109] Although the present invention has been described in conjunction with certain embodiments, it is to be understood that modifications and variations may be resorted to without departing from the spirit and scope of the invention as those skilled in the art readily understand. Such modifications and variations are considered to be within the scope of the invention and the appended claims.

We claim:

1. An apparatus comprising:

a processor circuitry coupled to a crypto/cipher engine, a surface, and a fingerprint sensor, wherein the processor circuitry is to validate a user through a fingerprint scan via the fingerprint sensor, wherein the processor circuitry is to make one or more keys for a challenge-response available to perform authentication with a cloud service through a device.

2. The apparatus of claim **1**, wherein the processor circuitry is to power for a predetermined duration based on an interaction of a validated user with the surface.

3. The apparatus of claim **1**, wherein the fingerprint sensor is positioned on the surface to allow for fingerprint scanning when the user interacts with the surface.

4. The apparatus of claim **1**, wherein the crypto/cipher engine includes at least one digital identifier including the one or more keys for the challenge-response.

5. The apparatus of claim **1**, wherein the crypto/cipher engine is user-removable from the device.

6. The apparatus of claim **4**, wherein the device is a wearable device.

7. The apparatus of claim **1**, wherein the crypto/cipher engine comprises a smartcard controller.

8. The apparatus of claim **1**, wherein the crypto/cipher engine resides on a subscriber identity module card.

9. The apparatus of claim **1**, wherein the one or more keys comprise a symmetric key.

10. The apparatus of claim **1**, wherein the one or more keys comprises an asymmetric key.

11. The apparatus of claim **1**, wherein the processor circuitry is to display a power level in response to an interaction with the fingerprint sensor.

12. The apparatus of claim **1** further comprises a radio coupled to the processor circuitry, wherein the radio comprises a near-field radio.

13. The apparatus of claim **12**, wherein the near-field radio comprises an ISO 18092 compatible radio or an ISO 14443 compatible radio.

14. The apparatus of claim **1** comprising a connector that when opened modifies electrical functionality of the apparatus.

15. The apparatus of claim **1** further comprising a housing formed to encircle a wrist of the user, the housing comprising a connector that when opened modifies electrical functionality of the device.

16. An apparatus comprising:

a scanner to scan a fingerprint when a user interacts with a surface;

a circuitry to make available one or more keys for a challenge-response to validate the user with a cloud service by powering a radio for a predetermined duration in response to the user interacting with the surface; and

a display configured to display a power level in response to a second interaction with the surface.

17. The apparatus of claim **16**, wherein the surface is part of a wearable personal digital device.

18. The apparatus of claim **17**, wherein the one or more keys are part of a digital identifier which is part of a crypto/cipher engine.

19. The apparatus of claim **18** wherein the crypto/cipher engine is user-removable from the wearable personal digital device.

20. The apparatus of claim **18**, wherein the crypto/cipher engine comprises a smartcard controller.

* * * * *