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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
11 June 2015 (11.06.2015)

WIPO | PCT

(10) International Publication Number
WO 2015/084816 A1

(51) International Patent Classification:
H04L 9/32 (2006.01)

(21) International Application Number:
PCT/US2014/068109

(22) International Filing Date:
2 December 2014 (02.12.2014)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
14/097,100 4 December 2013 (04.12.2013) US

(63) Related by continuation (CON) or continuation-in-part (CIP) to earlier application:
US 14/097,100 (CON)
Filed on 4 December 2013 (04.12.2013)

(71) Applicant: **EBAY INC.** [US/US]; 2145 Hamilton Avenue, San Jose, California 95125 (US).

(72) Inventor: **COCKCROFT, Oliver Nicholas**; 18010 Skyline Boulevard, Los Gatos, California 95033 (US).

(74) Agents: **SCHEER, Bradley, W.** et al.; P. O. Box 2938, Minneapolis, Minnesota 55402 (US).

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

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE,

[Continued on next page]

(54) Title: MULTI-FACTOR AUTHENTICATION SYSTEM AND METHOD

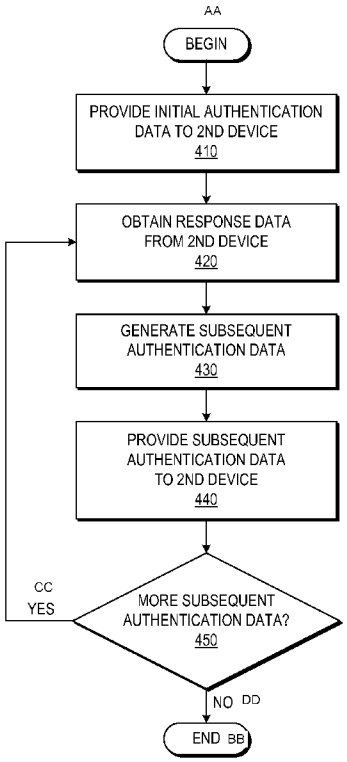

FIG. 4

(57) Abstract: A system and method of multi-factor authentication are described. In some embodiments, a first device provides an initial authentication data to a second device. The second device is different from the first device. The first device obtains a first response data from the second device. The first device generates a first subsequent authentication data using the first response data. The first subsequent authentication data is different from the initial authentication data. The first device provides the first subsequent authentication data to the second device. In some embodiments, obtaining the first response data comprises capturing the first response data from the second device using a camera on the mobile device, where the first response data is displayed on the second device.

WO 2015/084816 A1

DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

MULTI-FACTOR AUTHENTICATION SYSTEM AND METHOD

CLAIM OF PRIORITY

[0001] This PCT application claims the benefit of priority to US patent application serial number 14/097,100 filed December 4, 2013, the entire contents of which are hereby incorporated by reference herein in its entirety.

TECHNICAL FIELD

[0002] The present application relates generally to the technical field of data processing, and, in various embodiments, to systems and methods of multi-factor authentication.

BACKGROUND

[0003] Current techniques for authenticating users of devices are vulnerable to deception. As a result, the true owners of those devices and the accounts associated with them are susceptible to having transactions executed using their identity without their authorization.

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] Some embodiments of the present disclosure are illustrated by way of example and not limitation in the figures of the accompanying drawings, in which like reference numbers indicate similar elements, and in which:

[0005] FIGS. 1A-1C illustrate a multi-factor authentication system, in accordance with some embodiments;

[0006] FIGS. 2A-2C illustrate the exchange of data between a mobile device and an interface component of a point of sale (POS) terminal, in accordance with some embodiments;

[0007] FIGS. 3A-3B illustrate generation of subsequent authentication data in a multi-factor authentication system, in accordance with some embodiments;

[0008] FIG. 4 is a flowchart illustrating a method of multi-factor authentication, in accordance with some embodiments;

[0009] FIG. 5 is a flowchart illustrating a method of generating subsequent authentication data, in accordance with some embodiments;

[00010] FIG. 6 is a flowchart illustrating another method of generating subsequent authentication data, in accordance with some embodiments; and

[00011] FIG. 7 shows a diagrammatic representation of a machine in the example form of a computer system within which a set of instructions may be executed to cause the machine to perform any one or more of the methodologies discussed herein, in accordance with some embodiments.

DETAILED DESCRIPTION

[00012] The description that follows includes illustrative systems, methods, techniques, instruction sequences, and computing machine program products that embody illustrative embodiments. In the following description, for purposes of explanation, numerous specific details are set forth in order to provide an understanding of various embodiments of the inventive subject matter. It will be evident, however, to those skilled in the art that embodiments of the inventive subject matter may be practiced without these specific details. In general, well-known instruction instances, protocols, structures, and techniques have not been shown in detail.

[00013] The present disclosure describes systems and methods of multi-factor authentication. In some embodiments, the multi-factor authentication features disclosed herein are used in mobile payment processes to enable secure authenticated authorization of a payment for a transaction. During a mobile payment process, a mobile device can be used as a digital wallet. A mobile application on the mobile device can be used to employ the digital wallet functionality. The digital wallet can manage payment account information, including, but not limited to, credit card numbers, debit card numbers, other financial institution payment account information, expiration dates, security codes, shipping addresses, and billing addresses. When purchasing an item from a merchant, a user can use the digital wallet on his or her device to provide authentication data to a device of the merchant, such as an interface component of a POS terminal. This authentication data can then be used by the device of the merchant to initiate and verify payment using a secure payment server. Alternatively, the device of the merchant can provide the authentication data to the device of the user, which may then use the authentication data to initiate and verify payment using a secure payment server. It is contemplated that the

features of the present disclosure can be applied to other forms of mobile payment as well.

[00014] The features of the present disclosure add one or more subsequent layers of authentication to the mobile payment process by having a single device provide initial authentication data, and then subsequent authentication data different from the initial authentication data.

[00015] In some embodiments, a first device provides an initial authentication data to a second device. The second device is different from the first device. The first device obtains a first response data from the second device. The first device then generates a first subsequent authentication data using the first response data. The first subsequent authentication data is different from the initial authentication data. The first device provides the first subsequent authentication data to the second device.

[00016] In some embodiments, the first subsequent authentication data is provided during an authorization process for a transaction. In some embodiments, the first device is a mobile device. In some embodiments, obtaining the first response data comprises capturing the first response data from the second device using a camera on the mobile device, the first response data being displayed on the second device. In some embodiments, the second device is an interface component of a POS terminal.

[00017] In some embodiments, the first subsequent authentication data comprises image-based data. In some embodiments, the image-based data comprises a bar code. In some embodiments, the first subsequent authentication data comprises audio-based data.

[00018] In some embodiments, the first subsequent authentication data is generated using at least one of facial recognition data, fingerprint recognition data, and voice recognition data.

[00019] In some embodiments, the first device obtains a second response data from the second device, and generates a second subsequent authentication data using the second response data. The second subsequent authentication data is different from the initial authentication data and the first subsequent authentication data. The first device then provides the second subsequent authentication data to the second device.

[00020] In some embodiments, the first subsequent authentication data is

generated by the first device using an algorithm stored on the first device. In some embodiments, generating the first subsequent authentication data comprises transmitting an authentication data request to a third device, the third device being different from the first device and the second device, and then receiving the first subsequent authentication data from the third device.

[00021] The methods or embodiments disclosed herein may be implemented as a computer system having one or more modules (e.g., hardware modules or software modules). Such modules may be executed by one or more processors of the computer system. The methods or embodiments disclosed herein may be embodied as instructions stored on a machine-readable medium that, when executed by one or more processors, cause the one or more processors to perform the instructions.

[00022] FIGS. 1A-1C illustrate a multi-factor authentication system 100, in accordance with some embodiments. In some embodiments, multi-factor authentication system 100 comprises a first device 110. First device 110 is any computing device capable of receiving and providing data. First device 110 comprises a memory and at least one processor (not shown). In some embodiments, first device 110 comprises a mobile device. Examples of a mobile device include, but are not limited to, smartphones and tablet computers. Other types of mobile devices are also within the scope of the present disclosure.

[00023] First device 110 is used by a user to interact with a second device 120 in order to complete a purchase of a product or a service. Second device 120 comprises a memory and at least one processor (not shown), and may be any computing device capable of receiving and providing data. In some embodiments, second device 120 comprises an interface component of a POS terminal. For example, the user may be attempting to purchase a cup of coffee at a POS terminal in a coffee shop. In order to complete the purchase of the cup of coffee, the first device 110 and the second device 120 exchange data to authenticate the transaction during an authorization process for the transaction.

[00024] In some embodiments, first device 110 comprises a multi-factor authentication module 115. In some embodiments, multi-factor authentication module 115 is part of a mobile application installed on the first device 110 and is executable by a processor. As seen in FIG. 1A, multi-factor authentication module 115 can be configured to provide an initial authentication data to second

device 120. Responsive or otherwise subsequent to obtaining the initial authentication data from first device 110, second device 120 provides response data to first device 110, as seen in FIG. 1B. Responsive or otherwise subsequent to obtaining the first response data from second device 120, multi-factor authentication module 115 generates a subsequent authentication data using the first response data, and then provide the subsequent authentication data to second device 120, as seen in FIG. 1C. The first subsequent authentication data is different from the initial authentication data.

[00025] The back and forth exchange of authentication data and response data between first device 110 and second device 120 can be repeated multiple times so that as many layers of authentication that are desired can be added. In this fashion, different subsequent authentication data can be generated and provided multiple times before the purchase is actually authorized and completed.

[00026] The initial authentication data, the response data, and the subsequent authentication data can be provided in a variety of different forms. In some embodiments, the initial authentication data, the response data, and the subsequent authentication data comprises image-based data. One example of image-based data that can be used is a barcode. For example, multi-factor authentication module 115 can be configured to generate and provide Quick Response (QR) codes as authentication data. It is contemplated that other types of image-based data are also within the scope of the present disclosure.

[00027] FIGS. 2A-2C illustrate the exchange of data between a mobile device 210 and an interface device 220 of a POS terminal, in accordance with some embodiments. In some embodiments, mobile device 210 can be first device 110 of FIG. 1 and comprise multi-factor authentication module 115, and interface device 220 can be second device 120 of FIG. 1. However, it is contemplated that other configurations are also within the scope of the present disclosure.

[00028] As seen in FIG. 2A, mobile device 210 can display image-based initial authentication data 214 on a display screen 212. As previously mentioned, image-based initial authentication data 214 can comprise a barcode. However, it is contemplated that other forms of image-based initial authentication data 214 are also within the scope of the present disclosure. In

some embodiments, interface device 220 can obtain image-based initial authentication data 214 by capturing it via a scanner (not shown).

[00029] As seen in FIG. 2B, in response or otherwise subsequent to interface device 220 obtaining image-based initial authentication data 214, interface device 220 can display image-based response data 224 on a display screen 222. As previously mentioned, image-based response data 224 can comprise a barcode. However, it is contemplated that other forms of image-based response data 224 are also within the scope of the present disclosure. In some embodiments, mobile device 210 can obtain image-based response data 224 by capturing it via a built-in camera component 230.

[00030] As seen in FIG. 2C, in response or otherwise subsequent to mobile device 210 obtaining image-based response data 224, mobile device 210 can display image-based subsequent authentication data 218 on display screen 212. As previously mentioned, image-based subsequent authentication data 218 can comprise a barcode. However, it is contemplated that other forms of image-based subsequent authentication data 218 are also within the scope of the present disclosure.

[00031] In addition or as an alternative to the image-based data discussed above, other forms of data can be used as well. In some embodiments, audio-based initial authentication data, audio-based response data, and audio-based subsequent authentication data can be used during the authentication process. For example, mobile device 210 can provide audio-based initial authentication data and audio-based subsequent authentication data via a built-in speaker 216, and interface device 220 can provide audio-based response data via a built-in speaker 226. This audio-based data can comprise a uniquely identifiable sound that can be used by an algorithm employed by the counterpart device to provide another uniquely identifiable sound or to authenticate the transaction at issue.

[00032] In some embodiments, initial authentication data, response data, and subsequent authentication data can be transmitted by one device to another device via wireless communication, such as near field communication. It is contemplated that other forms of data and transmitting data are also within the scope of the present disclosure.

[00033] Additionally, different forms or modes of data can be employed within the same authentication process. For example, in one embodiment,

mobile device 210 can provide the initial authentication data as a barcode displayed on display screen 212, interface device 220 can provide the response data in the form of uniquely identifiable audio via speaker 226, and then mobile device 210 can provide the subsequent authentication data as code via a near field communication transmission. Other configurations are also within the scope of the present disclosure.

[00034] In some embodiments, authentication data can be determined by an algorithm residing on the device directly involved in the transaction, such as first device 110 or second device 120 in FIG. 1 or mobile device 210 or interface device 220 in FIG. 2. However, in some embodiments, these devices can obtain the authentication data from an external independent device on which an algorithm that determines the authentication data resides, and then provide the authentication data to its counterpart device that is directly involved in the transaction. In some embodiments, the algorithm used to generate the authentication data can be unique and correspond to a key on the device (e.g., first device 110) that will be providing the authentication data to the other device (e.g., second device 120), or to a key registered or otherwise corresponding to an application on that device that will be providing the authentication data. In this respect, each device can have its own unique algorithm to generate and provide its own unique authentication data.

[00035] FIGS. 3A-3B illustrate the generation of subsequent authentication data in a multi-factor authentication system, in accordance with some embodiments. As seen in FIG. 3A, first device 110 can request authentication data from an external independent device, such as server 300. Server 300 may comprise an algorithm configured to generate the subsequent authentication data discussed above. In some embodiments, the request sent from first device 110 to server 300 comprises the response data provided by second device 120 to first device 110. Server 300 can then use the response data to generate the subsequent authentication data, which it can then provide to first device 110, as seen in FIG. 3B. First device 110 can then provide the subsequent authentication data to second device 120, as previously discussed. In some embodiments, first device 110 and server 300 communicate with each other via the Internet. However, other modes and channels of communication are also within the scope of the present disclosure.

[00036] FIG. 4 is a flowchart illustrating a method 400 of multi-factor authentication, in accordance with some embodiments. The operations of method 400 may be performed by a system or modules of a system (e.g., system 100, first device 110, or multi-factor authentication module 115).

[00037] At operation 410, first device 110 provides initial authentication data to second device 120. As previously discussed, the initial authentication data can be provided in a variety of forms, including, but not limited to, visual data, audio data, and near field communication data.

[00038] At operation 420, first device 110 obtains response data from second device 120. As previously discussed, the response data can be obtained in a variety of ways, including, but not limited to capturing the response data via a built-in camera on the first device 110.

[00039] At operation 430, first device 110 generates subsequent authentication data. As previously discussed, in some embodiments, first device uses the response data to generate subsequent authentication data that is different from the initial authentication data.

[00040] At operation 440, first device 110 provides the subsequent authentication data to second device 120. As previously discussed, the subsequent authentication data can be provided in a variety of forms, including, but not limited to, visual data, audio data, and near field communication data.

[00041] At operation 450, if additional layers of authentication are desired, then the method 400 can repeat at operation 420, where first device 100 can obtain response data again from second device 420, and then generate and provide subsequent authentication data at operations 430 and 440, respectively. For each layer and cycle of authentication, unique subsequent authentication data can be generated and provided. If additional layers of authentication are not desired at operation 450, then method 400 may come to an end.

[00042] It is contemplated that the operations of method 400 may incorporate any of the other features disclosed herein.

[00043] As previously discussed, although the authentication data discussed above can be generated by an algorithm residing on one of the devices (e.g., first device 110 or second device 120) directly involved in the transaction at issue, it is contemplated that, in some embodiments, another device that is external and independent of first device 110 and second device 120 can use an

algorithm to determine the subsequent authentication data and provide it to one of the devices directly involved in the transaction at issue.

[00044] FIG. 5 is a flowchart illustrating a method 500 of generating subsequent authentication data, in accordance with some embodiments. The operations of method 500 may be performed by a system or modules of a system (e.g., system 100, first device 110, or multi-factor authentication module 115). At operation 510, first device 110 can transmit a request for authentication data to a third device, such as server 300 in FIGS. 3A-3B. At operation 520, first device 110 can receive the subsequent authentication data generated the third device. It is contemplated that the operations of method 500 may incorporate any of the other features disclosed herein.

[00045] In some embodiments, the algorithm used to generate the subsequent authentication data can receive and use a variety of different data to generate the subsequent authentication data. FIG. 6 is a flowchart illustrating another method 600 of generating subsequent authentication data, in accordance with some embodiments. The operations of method 600 may be performed by a system or modules of a system (e.g., system 100, first device 110, or multi-factor authentication module 115). At operation 610, response data is received.

[00046] At operation 620, additional data other than the response data is received. In some embodiments, this additional data comprises recognition-based data. Examples of recognition-based data include, but are not limited to, facial recognition data, fingerprint recognition data, and voice recognition data. The recognition data can be obtained using data capturing devices, including, but not limited to, cameras, touchscreens, and microphones. In one example, a user attempting to purchase a product can apply his or her finger to the touchscreen of a smartphone, thereby enabling the smartphone to capture the user's fingerprint. In some embodiments, the additional data can include a key, token, or other identifier that is unique to and corresponds to the device (e.g., the user's smartphone) that is being used to pay for the product or service at issue.

[00047] At operation 630, the subsequent authentication data is generated and provided using the response data and the additional data. In some embodiments, the additional data is used by the algorithm that generates the subsequent authentication data in its generation of the subsequent authentication data. In some embodiments, the additional data is used to identify which

algorithm to use to generate the subsequent authentication data, such as by determining that the additional data corresponds to a particular user or device, and then determining the algorithm that corresponds to that particular user or device.

[00048] It is contemplated that the operations of method 600 may incorporate any of the other features disclosed herein.

[00049] As previously discussed, although examples disclosed herein show the multi-factor authentication module 115 and/or the algorithm used to generate the subsequent authentication data residing on first device 110, it is contemplated that the multi-factor authentication module 115 and/or the algorithm for generating the subsequent authentication data can reside on other devices as well, such as second device 120 and server 300.

MODULES, COMPONENTS AND LOGIC

[00050] Certain embodiments are described herein as including logic or a number of components, modules, or mechanisms. Modules may constitute either software modules (e.g., code embodied on a machine-readable medium or in a transmission signal) or hardware modules. A hardware module is a tangible unit capable of performing certain operations and may be configured or arranged in a certain manner. In example embodiments, one or more computer systems (e.g., a standalone, client, or server computer system) or one or more hardware modules of a computer system (e.g., a processor or a group of processors) may be configured by software (e.g., an application or application portion) as a hardware module that operates to perform certain operations as described herein.

[00051] In various embodiments, a hardware module may be implemented mechanically or electronically. For example, a hardware module may comprise dedicated circuitry or logic that is permanently configured (e.g., as a special-purpose processor, such as a field programmable gate array (FPGA) or an application-specific integrated circuit (ASIC)) to perform certain operations. A hardware module may also comprise programmable logic or circuitry (e.g., as encompassed within a general-purpose processor or other programmable processor) that is temporarily configured by software to perform certain operations. It will be appreciated that the decision to implement a hardware module mechanically, in dedicated and permanently configured circuitry, or in

temporarily configured circuitry (e.g., configured by software) may be driven by cost and time considerations.

[00052] Accordingly, the term "hardware module" should be understood to encompass a tangible entity, be that an entity that is physically constructed, permanently configured (e.g., hardwired) or temporarily configured (e.g., programmed) to operate in a certain manner and/or to perform certain operations described herein. Considering embodiments in which hardware modules are temporarily configured (e.g., programmed), each of the hardware modules need not be configured or instantiated at any one instance in time. For example, where the hardware modules comprise a general-purpose processor configured using software, the general-purpose processor may be configured as respective different hardware modules at different times. Software may accordingly configure a processor, for example, to constitute a particular hardware module at one instance of time and to constitute a different hardware module at a different instance of time.

[00053] Hardware modules can provide information to, and receive information from, other hardware modules. Accordingly, the described hardware modules may be regarded as being communicatively coupled. Where multiple of such hardware modules exist contemporaneously, communications may be achieved through signal transmission (e.g., over appropriate circuits and buses) that connect the hardware modules. In embodiments in which multiple hardware modules are configured or instantiated at different times, communications between such hardware modules may be achieved, for example, through the storage and retrieval of information in memory structures to which the multiple hardware modules have access. For example, one hardware module may perform an operation and store the output of that operation in a memory device to which it is communicatively coupled. A further hardware module may then, at a later time, access the memory device to retrieve and process the stored output. Hardware modules may also initiate communications with input or output devices and can operate on a resource (e.g., a collection of information).

[00054] The various operations of example methods described herein may be performed, at least partially, by one or more processors that are temporarily configured (e.g., by software) or permanently configured to perform the relevant operations. Whether temporarily or permanently configured, such processors

may constitute processor-implemented modules that operate to perform one or more operations or functions. The modules referred to herein may, in some example embodiments, comprise processor-implemented modules.

[00055] Similarly, the methods described herein may be at least partially processor-implemented. For example, at least some of the operations of a method may be performed by one or more processors or processor-implemented modules. The performance of certain of the operations may be distributed among the one or more processors, not only residing within a single machine, but deployed across a number of machines. In some example embodiments, the processor or processors may be located in a single location (e.g., within a home environment, an office environment or as a server farm), while in other embodiments the processors may be distributed across a number of locations.

[00056] The one or more processors may also operate to support performance of the relevant operations in a "cloud computing" environment or as a "software as a service" (SaaS). For example, at least some of the operations may be performed by a group of computers (as examples of machines including processors), these operations being accessible via a network (e.g., the network 104 of FIG. 1) and via one or more appropriate interfaces (e.g., APIs).

ELECTRONIC APPARATUS AND SYSTEM

[00057] Example embodiments may be implemented in digital electronic circuitry, or in computer hardware, firmware, software, or in combinations of them. Example embodiments may be implemented using a computer program product, e.g., a computer program tangibly embodied in an information carrier, e.g., in a machine-readable medium for execution by, or to control the operation of, data processing apparatus, e.g., a programmable processor, a computer, or multiple computers.

[00058] A computer program can be written in any form of programming language, including compiled or interpreted languages, and it can be deployed in any form, including as a stand-alone program or as a module, subroutine, or other unit suitable for use in a computing environment. A computer program can be deployed to be executed on one computer or on multiple computers at one site or distributed across multiple sites and interconnected by a communication network.

[00059] In example embodiments, operations may be performed by one or more programmable processors executing a computer program to perform functions by operating on input data and generating output. Method operations can also be performed by, and apparatus of example embodiments may be implemented as, special purpose logic circuitry (e.g., a FPGA or an ASIC).

[00060] A computing system can include clients and servers. A client and server are generally remote from each other and typically interact through a communication network. The relationship of client and server arises by virtue of computer programs running on the respective computers and having a client-server relationship to each other. In embodiments deploying a programmable computing system, it will be appreciated that both hardware and software architectures merit consideration. Specifically, it will be appreciated that the choice of whether to implement certain functionality in permanently configured hardware (e.g., an ASIC), in temporarily configured hardware (e.g., a combination of software and a programmable processor), or a combination of permanently and temporarily configured hardware may be a design choice. Below are set out hardware (e.g., machine) and software architectures that may be deployed, in various example embodiments.

EXAMPLE MACHINE ARCHITECTURE AND MACHINE-READABLE MEDIUM

[00061] FIG. 7 is a block diagram of a machine in the example form of a computer system 700 within which instructions for causing the machine to perform any one or more of the methodologies discussed herein may be executed. In alternative embodiments, the machine operates as a standalone device or may be connected (e.g., networked) to other machines. In a networked deployment, the machine may operate in the capacity of a server or a client machine in a server-client network environment, or as a peer machine in a peer-to-peer (or distributed) network environment. The machine may be a personal computer (PC), a tablet PC, a set-top box (STB), a Personal Digital Assistant (PDA), a cellular telephone, a web appliance, a network router, switch or bridge, or any machine capable of executing instructions (sequential or otherwise) that specify actions to be taken by that machine. Further, while only a single machine is illustrated, the term "machine" shall also be taken to include any

collection of machines that individually or jointly execute a set (or multiple sets) of instructions to perform any one or more of the methodologies discussed herein.

[00062] The example computer system 700 includes a processor 702 (e.g., a central processing unit (CPU), a graphics processing unit (GPU) or both), a main memory 704 and a static memory 706, which communicate with each other via a bus 708. The computer system 700 may further include a video display unit 710 (e.g., a liquid crystal display (LCD) or a cathode ray tube (CRT)). The computer system 700 also includes an alphanumeric input device 712 (e.g., a keyboard), a user interface (UI) navigation (or cursor control) device 714 (e.g., a mouse), a disk drive unit 716, a signal generation device 718 (e.g., a speaker), and a network interface device 720.

MACHINE-READABLE MEDIUM

[00063] The disk drive unit 716 includes a machine-readable medium 722 on which is stored one or more sets of data structures and instructions 724 (e.g., software) embodying or utilized by any one or more of the methodologies or functions described herein. The instructions 724 may also reside, completely or at least partially, within the main memory 704 and/or within the processor 702 during execution thereof by the computer system 700, the main memory 704 and the processor 702 also constituting machine-readable media. The instructions 724 may also reside, completely or at least partially, within the static memory 706.

[00064] While the machine-readable medium 722 is shown in an example embodiment to be a single medium, the term "machine-readable medium" may include a single medium or multiple media (e.g., a centralized or distributed database, and/or associated caches and servers) that store the one or more instructions 724 or data structures. The term "machine-readable medium" shall also be taken to include any tangible medium that is capable of storing, encoding or carrying instructions for execution by the machine and that cause the machine to perform any one or more of the methodologies of the present embodiments, or that is capable of storing, encoding or carrying data structures utilized by or associated with such instructions. The term "machine-readable medium" shall accordingly be taken to include, but not be limited to, solid-state memories, and

optical and magnetic media. Specific examples of machine-readable media include non-volatile memory, including by way of example semiconductor memory devices (e.g., Erasable Programmable Read-Only Memory (EPROM), Electrically Erasable Programmable Read-Only Memory (EEPROM), and flash memory devices); magnetic disks such as internal hard disks and removable disks; magneto-optical disks; and compact disc-read-only memory (CD-ROM) and digital versatile disc (or digital video disc) read-only memory (DVD-ROM) disks.

TRANSMISSION MEDIUM

[00065] The instructions 724 may further be transmitted or received over a communications network 726 using a transmission medium. The instructions 724 may be transmitted using the network interface device 720 and any one of a number of well-known transfer protocols (e.g., HTTP). Examples of communication networks include a LAN, a WAN, the Internet, mobile telephone networks, POTS networks, and wireless data networks (e.g., WiFi and WiMax networks). The term "transmission medium" shall be taken to include any intangible medium capable of storing, encoding, or carrying instructions for execution by the machine, and includes digital or analog communications signals or other intangible media to facilitate communication of such software.

[00066] Although an embodiment has been described with reference to specific example embodiments, it will be evident that various modifications and changes may be made to these embodiments without departing from the broader scope of the present disclosure. Accordingly, the specification and drawings are to be regarded in an illustrative rather than a restrictive sense. The accompanying drawings that form a part hereof show, by way of illustration, and not of limitation, specific embodiments in which the subject matter may be practiced. The embodiments illustrated are described in sufficient detail to enable those skilled in the art to practice the teachings disclosed herein. Other embodiments may be utilized and derived therefrom, such that structural and logical substitutions and changes may be made without departing from the scope of this disclosure. This Detailed Description, therefore, is not to be taken in a limiting sense, and the scope of various embodiments is defined only by the

appended claims, along with the full range of equivalents to which such claims are entitled.

[00067] Such embodiments of the inventive subject matter may be referred to herein, individually and/or collectively, by the term "invention" merely for convenience and without intending to voluntarily limit the scope of this application to any single invention or inventive concept if more than one is in fact disclosed. Thus, although specific embodiments have been illustrated and described herein, it should be appreciated that any arrangement calculated to achieve the same purpose may be substituted for the specific embodiments shown. This disclosure is intended to cover any and all adaptations or variations of various embodiments. Combinations of the above embodiments, and other embodiments not specifically described herein, will be apparent to those of skill in the art upon reviewing the above description.

[00068] The Abstract of the Disclosure is provided to allow the reader to quickly ascertain the nature of the technical disclosure. It is submitted with the understanding that it will not be used to interpret or limit the scope or meaning of the claims. In addition, in the foregoing Detailed Description, it can be seen that various features are grouped together in a single embodiment for the purpose of streamlining the disclosure. This method of disclosure is not to be interpreted as reflecting an intention that the claimed embodiments require more features than are expressly recited in each claim. Rather, as the following claims reflect, inventive subject matter lies in less than all features of a single disclosed embodiment. Thus the following claims are hereby incorporated into the Detailed Description, with each claim standing on its own as a separate embodiment.

CLAIMS

1. A computer-implemented method comprising:

providing, by a first device having a memory and at least one processor, an initial authentication data to a second device, the second device being different from the first device, the first device comprising a mobile device;

obtaining, by the first device, a first response data from the second device, the obtaining of the first response data comprising capturing the first response data from the second device using a camera on the mobile device, the first response data being displayed on the second device;

generating, by the first device, a first subsequent authentication data using the first response data, the first subsequent authentication data being different from the initial authentication data; and

providing, by the first device, the first subsequent authentication data to the second device.

2. The method of claim 1, wherein the first subsequent authentication data is provided during an authorization process for a transaction.

3. The method of claim 1, wherein the second device is an interface component of a point of sale terminal.

4. The method of claim 1, wherein the first subsequent authentication data comprises image-based data.

5. The method of claim 4, wherein the image-based data comprises a bar code.

6. The method of claim 1, wherein the first subsequent authentication data comprises audio-based data.

7. The method of claim 1, wherein the first subsequent authentication data is generated using at least one of facial recognition data, fingerprint recognition data, and voice recognition data.

8. The method of claim 1, further comprising:

obtaining, by the first device, a second response data from the second device;

generating, by the first device, a second subsequent authentication data using the second response data, the second subsequent authentication data being different from the initial authentication data and the first subsequent authentication data; and

providing, by the first device, the second subsequent authentication data to the second device.

9. The method of claim 1, wherein the first subsequent authentication data is generated by the first device using an algorithm stored on the first device.

10. The method of claim 1, wherein generating the first subsequent authentication data comprises:

transmitting an authentication data request to a third device, the third device being different from the first device and the second device; and

receiving the first subsequent authentication data from the third device.

11. A system comprising:

a first machine having a memory and at least one processor, the first machine comprising a mobile device; and

a multi-factor authentication module, executable by the at least one processor, configured to:

provide an initial authentication data to a second machine, the second machine being different from the first machine;

obtain a first response data from the second machine by capturing the first response data from the second machine using a

camera on the mobile device, the first response data being displayed on the second machine;

generate a first subsequent authentication data using the first response data, the first subsequent authentication data being different from the initial authentication data; and

provide the first subsequent authentication data to the second machine.

12. The system of claim 11, wherein the first subsequent authentication data comprises image-based data.

13. The system of claim 12, wherein the image-based data comprises a bar code.

14. The system of claim 11, wherein the first subsequent authentication data comprises audio-based data.

15. The system of claim 11, wherein the multi-factor authentication module is further configured to generate the first subsequent authentication using at least one of facial recognition data, fingerprint recognition data, and voice recognition data.

16. The system of claim 11, wherein the multi-factor authentication module is further configured to:

obtain a second response data from the second machine;

generate a second subsequent authentication data using the second response data, the second subsequent authentication data being different from the initial authentication data and the first subsequent authentication data; and

provide the second subsequent authentication data to the second machine.

17. A non-transitory machine-readable storage device storing a set of instructions that, when executed by at least one processor, causes the at least one processor to perform a set of operations comprising:

providing, by a first device having a memory and at least one processor, an initial authentication data to a second device, the second device being different from the first device, the first device comprising a mobile device;

obtaining, by the first device, a first response data from the second device, the obtaining of the first response data comprising capturing the first response data from the second device using a camera on the mobile device, the first response data being displayed on the second device;

generating, by the first device, a first subsequent authentication data using the first response data, the first subsequent authentication data being different from the initial authentication data; and

providing, by the first device, the first subsequent authentication data to the second device.

18. The storage device of claim 17, wherein the set of operations further comprises:

obtaining, by the first device, a second response data from the second device;

generating, by the first device, a second subsequent authentication data using the second response data, the second subsequent authentication data being different from the initial authentication data and the first subsequent authentication data; and

providing, by the first device, the second subsequent authentication data to the second device.

19. The storage device of claim 17, wherein generating the first subsequent authentication data comprises:

transmitting an authentication data request to a third device, the third device being different from the first device and the second device; and

receiving the first subsequent authentication data from the third device.

20. A machine-readable medium carrying a set of instructions that, when executed by at least one processor, causes the at least one processor to carry out the method of any one of claims 1 to 10.

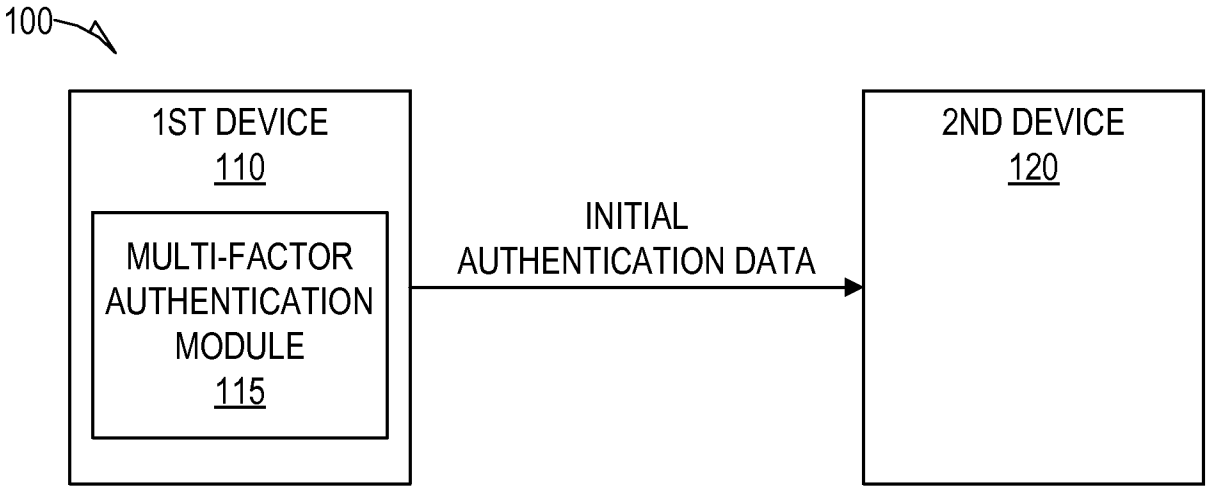

FIG. 1A

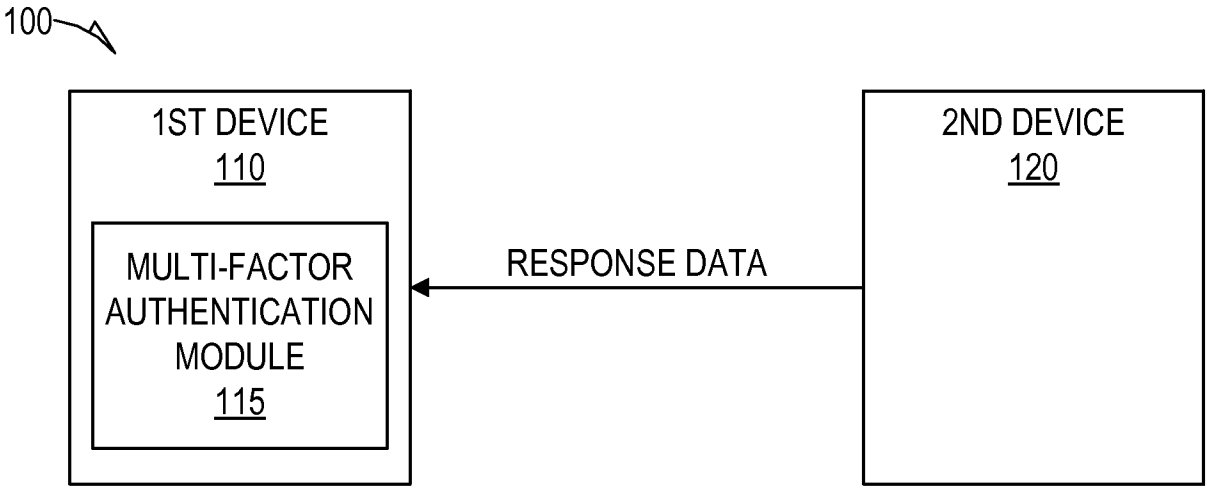

FIG. 1B

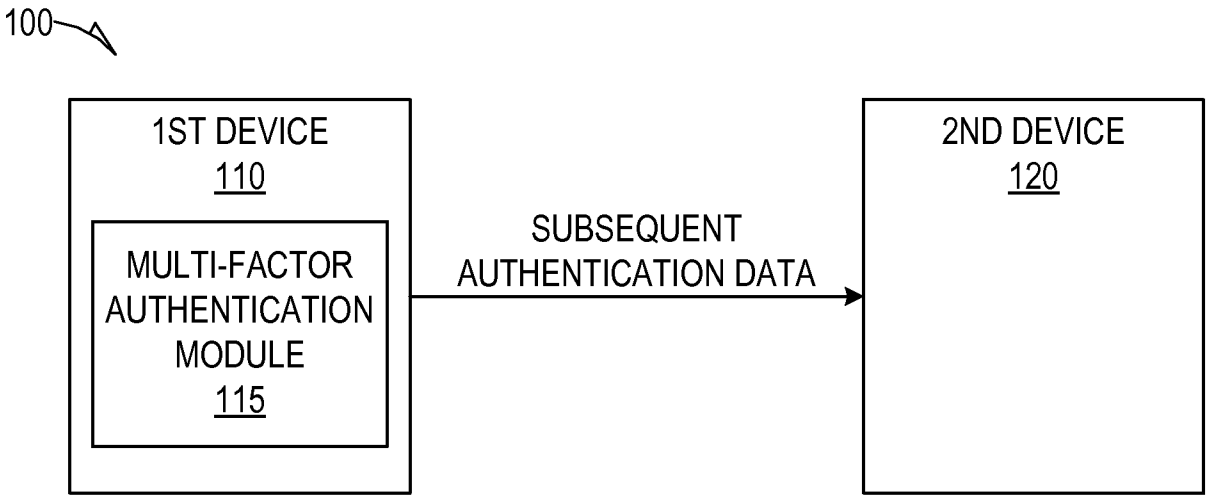

FIG. 1C

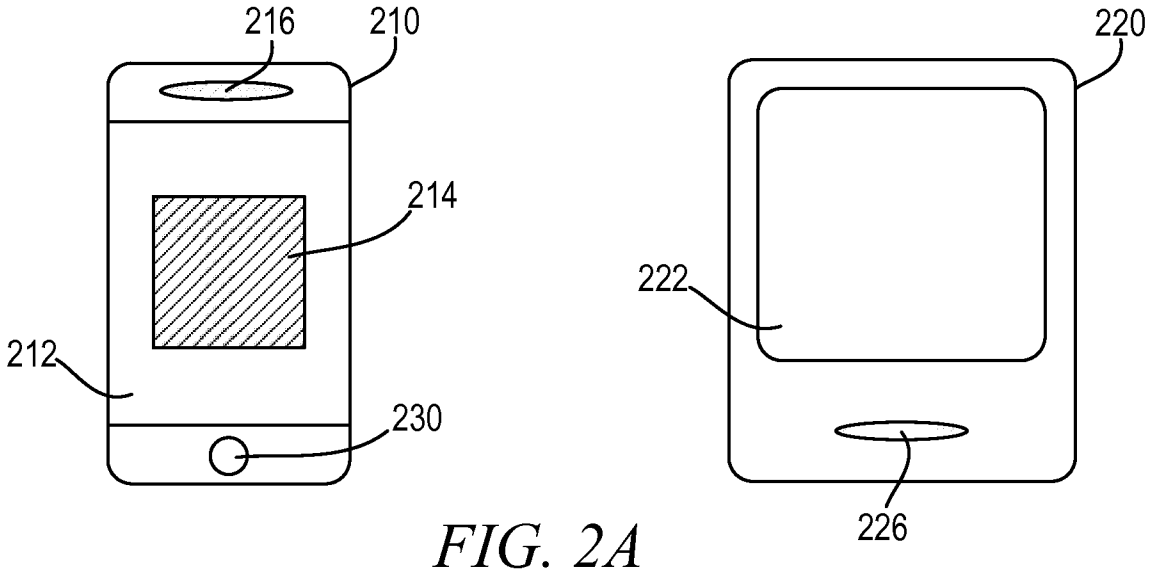

FIG. 2A

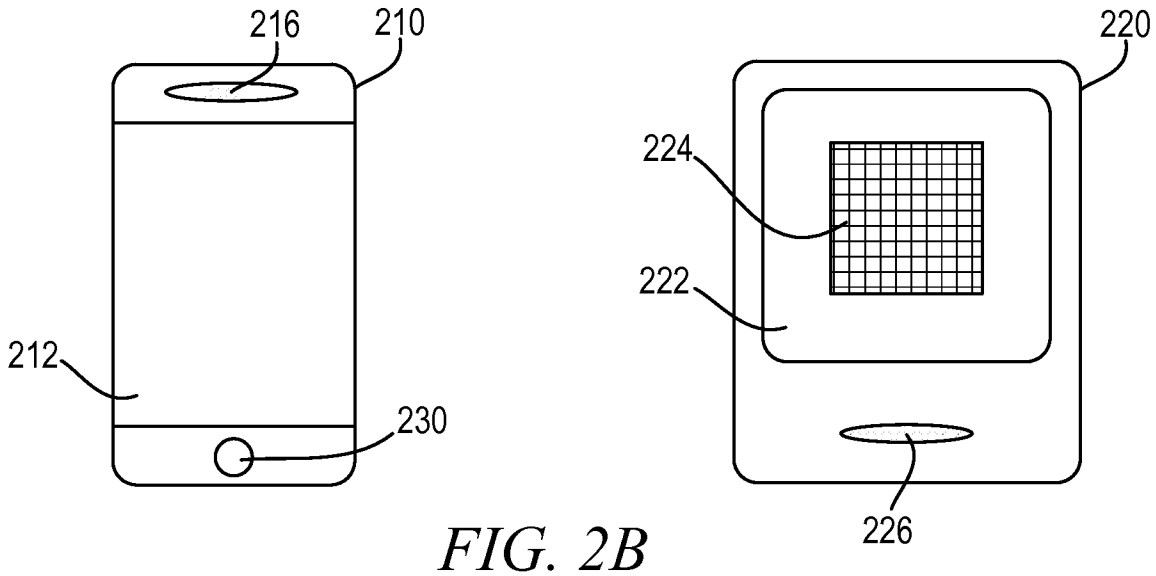

FIG. 2B

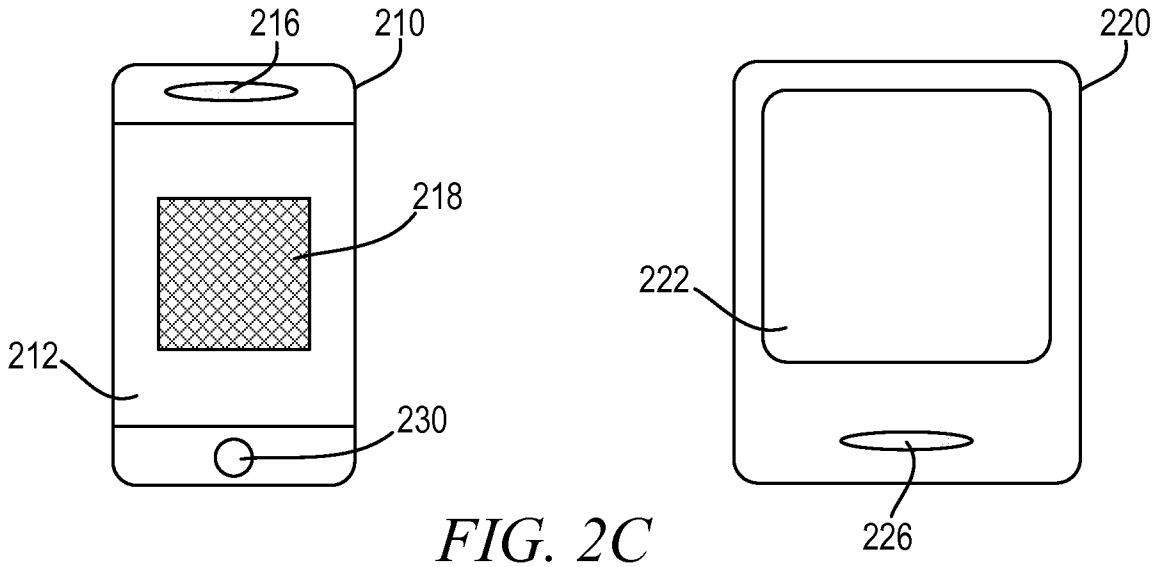

FIG. 2C

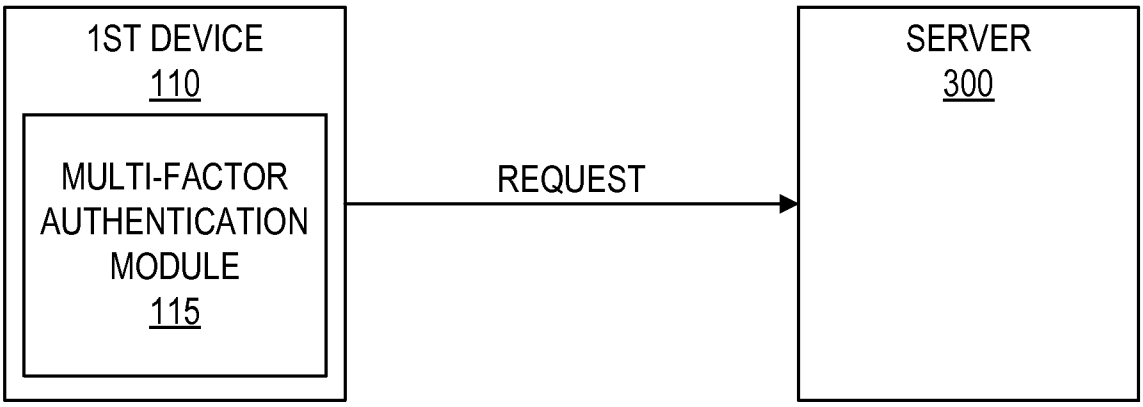
1ST DEVICE
110
MULTI-FACTOR AUTHENTICATION MODULE
115
REQUEST
SERVER
300

FIG. 3A


1ST DEVICE
110
MULTI-FACTOR AUTHENTICATION MODULE
115
SUBSEQUENT AUTHENTICATION DATA
SERVER
300

FIG. 3B

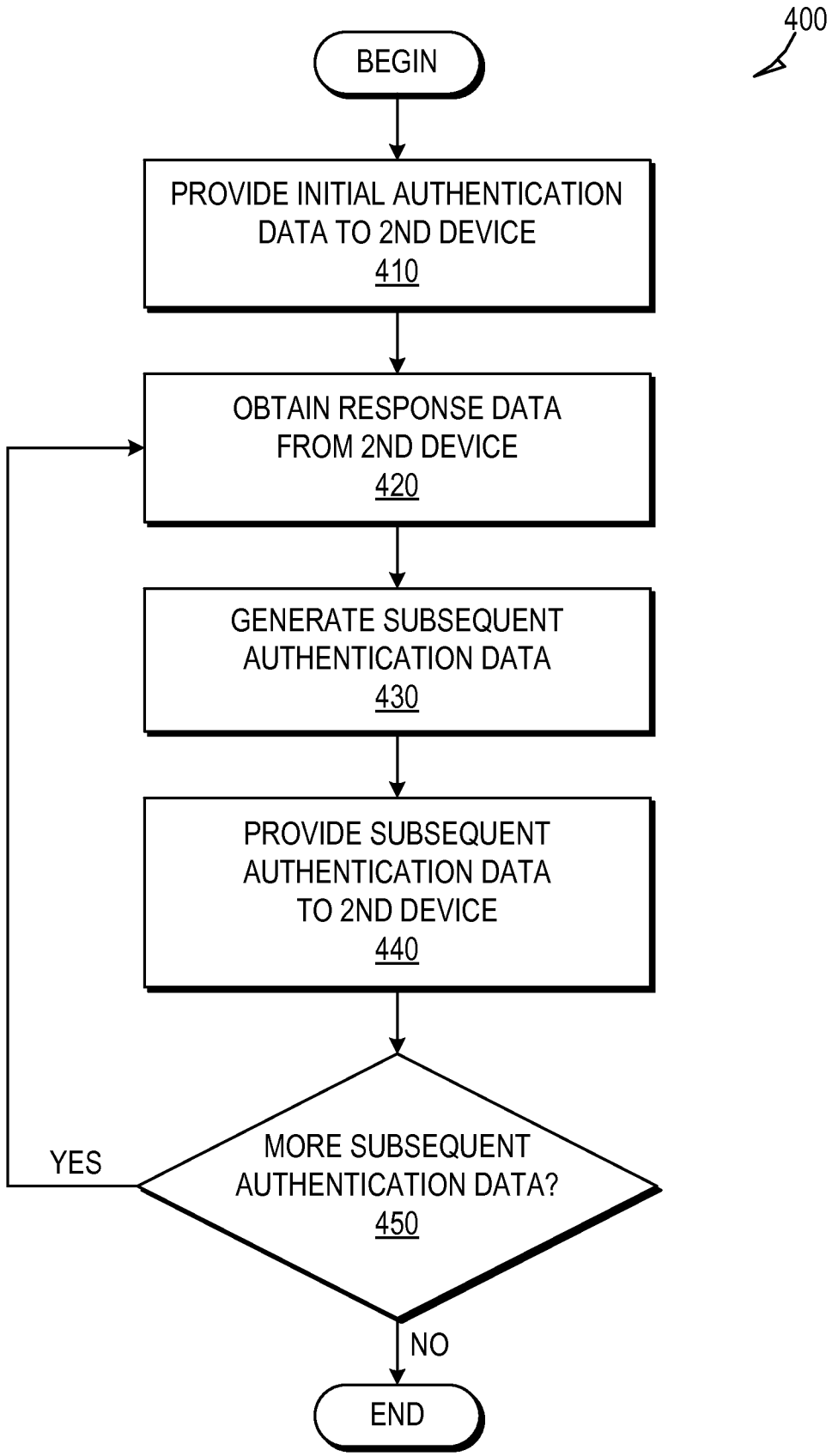
400
BEGIN
PROVIDE INITIAL AUTHENTICATION DATA TO 2ND DEVICE
410
OBTAIN RESPONSE DATA FROM 2ND DEVICE
420
GENERATE SUBSEQUENT AUTHENTICATION DATA
430
PROVIDE SUBSEQUENT AUTHENTICATION DATA TO 2ND DEVICE
440
MORE SUBSEQUENT AUTHENTICATION DATA?
450
YES
NO
END

FIG. 4

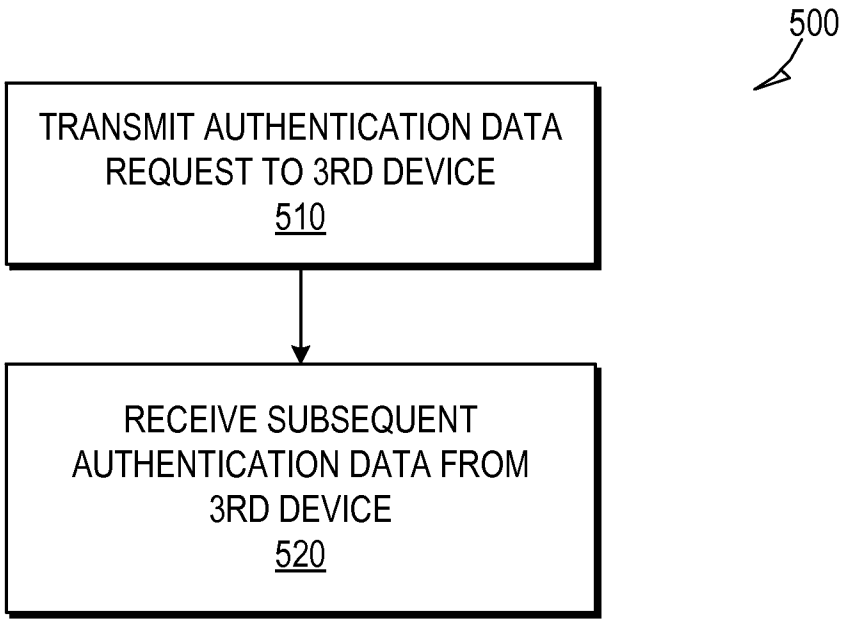
500
TRANSMIT AUTHENTICATION DATA REQUEST TO 3RD DEVICE
510
RECEIVE SUBSEQUENT AUTHENTICATION DATA FROM 3RD DEVICE
520

FIG. 5

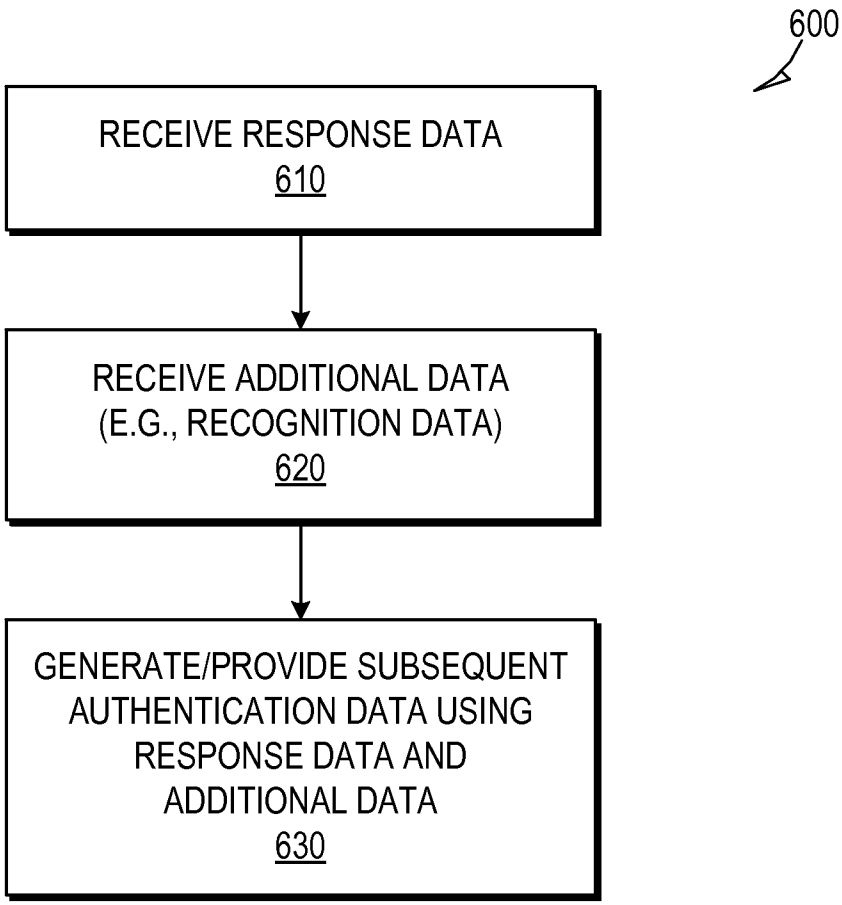
600
RECEIVE RESPONSE DATA
610
RECEIVE ADDITIONAL DATA (E.G., RECOGNITION DATA)
620
GENERATE/PROVIDE SUBSEQUENT AUTHENTICATION DATA USING RESPONSE DATA AND ADDITIONAL DATA
630

FIG. 6

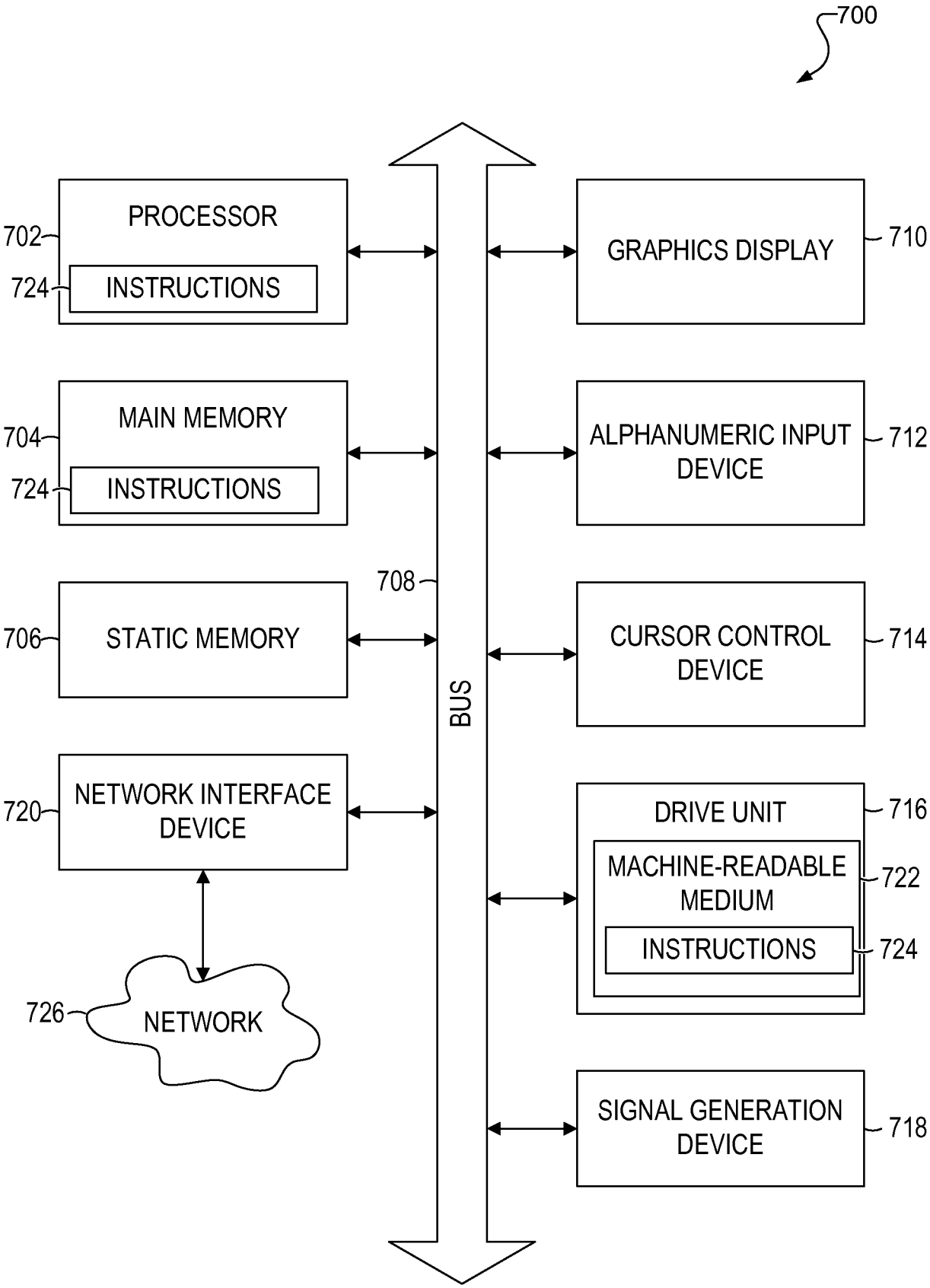
700
PROCESSOR
702
INSTRUCTIONS
724
MAIN MEMORY
704
INSTRUCTIONS
724
STATIC MEMORY
706
NETWORK INTERFACE DEVICE
720
NETWORK
726
708
BUS
GRAPHICS DISPLAY
710
ALPHANUMERIC INPUT DEVICE
712
CURSOR CONTROL DEVICE
714
DRIVE UNIT
716
MACHINE-READABLE MEDIUM
722
INSTRUCTIONS
724
SIGNAL GENERATION DEVICE
718

FIG. 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2014/068109

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - H04L 9/32 (2015.01)
CPC - H04W 12/06 (2014.12)
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC(8) - G06F 21/00, 21/32; G06K 9/00; H04L 9/32, 29/06; H04W 12/06 (2015.01)
USPC - 380/ 33; 382/ 115; 455/ 411; 705/ 45, 64, 67, 72, 76; 709/ 225; 713/ 155, 168, 182, 183, 186; 726/ 2, 3, 4, 5, 6, 7, 19;

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
CPC - G06F 21/32; G06Q 20/32, 20/204, 20/3224; H04L 63/08, 0861; H04W 12/06 (2014.12) (keyword delimited)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

PatBase, Orbit, Google Patents, Google Scholar, Google.
Search terms used:multi-factor authentication, MFA, biometrics, camera, mobile, phone

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2013/0282589 A1 (Shoup et al.) 24 October 2013 (24.10.2013) entire document	1-20
A	US 2012/0110341 A1 (Homayoon) 03 May 2013 (03.05.2012) entire document	1-20
A	US 8,578,454 B1 (Grim) 05 November 2013 (05.11.2013) entire document	1-20
A	US 2008/0307515 A1 (Drokov et al.) 11 December 2008 (11.12.2008) entire document	1-20

☐ Further documents are listed in the continuation of Box C. ☐

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
02 February 2015	16 MAR 2015
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774