



- (51) **International Patent Classification:**
H04W 68/00 (2009.01) *H04W 48/02* (2009.01)
- (21) **International Application Number:**
PCT/US2014/031737
- (22) **International Filing Date:**
25 March 2014 (25.03.2014)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
61/805,410 26 March 2013 (26.03.2013) US
- (71) **Applicant:** JVL VENTURES, LLC [US/US]; 230 Park Avenue, Suite 2829, New York, NY 10169-0005 (US).
- (72) **Inventors:** POON, Tommy; C/o Jvl Ventures, Llc, 230 Park Avenue, Suite 2829, New York, NY 10169-0005 (US). SUNG, Danny; C/o Jvl Ventures, LLC, 230 Park Avenue, Suite 2829, New York, NY 10169-0005 (US).
- (74) **Agents:** BERSCHADSKY, Jonathan et al.; Fitzpatrick, Cella, Harper & Scinto, 1290 Avenue Of The Americas, New York, NY 10104-3800 (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, LT, 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, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, 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))

(54) **Title:** SYSTEMS, METHODS, AND COMPUTER PROGRAM PRODUCTS FOR MANAGING ACCESS CONTROL

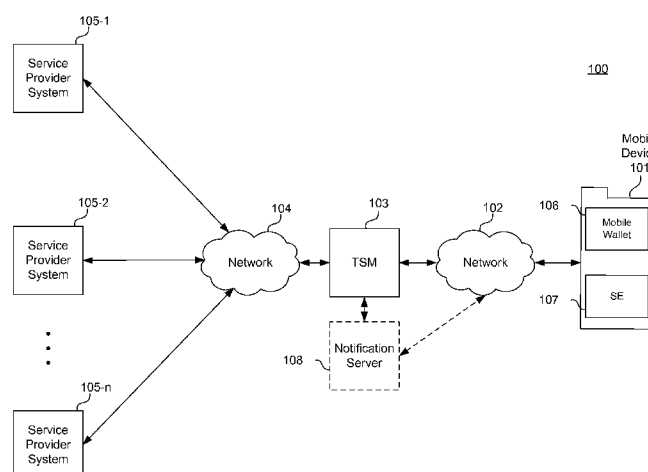


FIG. 1

(57) **Abstract:** Systems, methods, and computer program products are provided for managing access control. A first set of access control rules is stored in a memory of mobile communication device. The mobile communication device receives from a trusted server over a communication network a notification message indicating that an access control rule has been updated in a secure element. In response to receiving the notification message, the mobile communication device retrieves from the secure element a second set of access control rules including at least the access control rule that has been updated. The first set of access control rules is updated based on the second set of access control rules retrieved from the secure element. An applet stored on the secure element is accessed via an application running on the mobile communication device, in accordance with the updated first set of access control rules.



- 1 -

TITLE

**SYSTEMS, METHODS, AND COMPUTER PROGRAM PRODUCTS FOR
MANAGING ACCESS CONTROL**

BACKGROUND

Field

[0001] Example aspects described herein relate generally to mobile wallets in mobile communication devices for use in mobile commerce, and more particularly to systems, methods, and computer program products for managing access control for mobile communication devices that utilize secure elements.

Related Art

[0002] Mobile communication devices (also referred to herein as mobile devices) are becoming more and more versatile, and are being used in an increasing number of ways to make various everyday tasks simpler and/or more efficient. One area in

- 2 -

which mobile devices are being used is mobile commerce. For example, mobile devices are being made to include mobile wallets, which may be used to conduct financial transactions (*e.g.*, payments) and/or non-financial transactions (*e.g.*, venue admissions), without the need for physical cash, checks, credit cards, tickets, and/or the like. In order to safeguard sensitive information (*e.g.*, payment account information) that mobile wallets utilize in conducting such transactions, some mobile devices are made to include, and/or are communicatively coupled to, a secure element that stores such sensitive information.

[0003] Controlling access to the secure element is necessary for both security and business reasons. To this end, conventional access control specifications (*e.g.*, Global Platform Access Control (GPAC), for example as described in Global Platform Device Technology – Secure Element Access Control, Version 1.0, Document Reference GPE_SPE_013, May 2012, 86 pages); Gemalto Access Control (GAC); and Public-Key Cryptography Standard No. 15 (PKCS15), each of which is hereby incorporated by reference herein in its entirety, typically require access control rules (also referred to herein as simply “access rules”) to be stored on the secure element.

[0004] In general, each access rule in a set of access rules stored on the secure element indicates whether a particular application stored on the mobile device is permitted to access a particular applet stored on the secure element. Any given one of the access rules may correspond to one or more of the applications stored on the mobile device and one or more of the applets stored on the secure element.

[0005] Some access control specifications permit the access rules stored in the secure element to be updated (*e.g.*, added, modified, or deleted), for example, by way of a wireless communication protocol, such as an over-the-air (OTA) communication protocol. The secure element also stores a refresh tag (*e.g.*, a flag, a date, a time, and/or another type of temporal indicator) that includes a value that indicates when any of the access rules stored on the secure element was most recently updated. Each time any of the access rules stored on the secure element is updated in the secure element, the value of the refresh tag in the secure element is updated as well.

- 3 -

[0006] In some cases, an enforcer module (also referred to herein as “enforcer”) residing on the mobile device retrieves from the secure element, and stores, the set of access rules. According to some access control specifications, the enforcer is required to periodically poll the refresh tag to determine whether any of the access rules stored in the secure element has been updated since the last time the enforcer retrieved the access rules from the secure element. In addition to periodic polling, the enforcer polls the refresh tag of the secure element each time access control is to be enforced (*e.g.*, upon receiving a request for access to information and/or performance of an action that is protected by the rules, such as a request to open a secure communication channel using an application or applet stored on the secure element). If, upon polling the refresh tag, the enforcer determines that one or more pertinent access control rules has been updated since the most recent polling, then the enforcer retrieves from the secure element an updated set of access rules (or a subset of the updated set of access rules), and updates a local set of rules stored on the mobile communication device so as to be consistent with the rules stored in the secure element. One example of such a polling scheme may be found in GlobalPlatform Device Technology – Secure Element Access Control, Version 1.0, Document Reference GPE_SPE_013, Section 5 - Remote Interface Based on RAM, May 2012, 86 pages), the entire contents of which are hereby incorporated by reference herein.

[0007] In one example, in order to enable the enforcer to determine whether any of the access rules stored in the secure element has been updated since the last time the enforcer retrieved the access rules from the secure element, each time the enforcer retrieves from the secure element, and stores, the access rules, the enforcer also retrieves from the secure element, and stores, the refresh tag that includes a value that indicates when the set of access rules stored on the secure element was most recently updated. In this way, the enforcer may determine whether any of the access rules stored in the secure element has been updated since the last time the enforcer retrieved the access rules from the secure element, by comparing the value of the refresh tag stored in the secure element to the value of the refresh tag stored by the enforcer.

- 4 -

[0008] If the value of the refresh tag stored in the secure element matches the value of the refresh tag stored by the enforcer, then that would indicate that the access rules stored by the enforcer are up-to-date; that is, that none of the access rules stored in the secure element has been updated since the last time the enforcer retrieved the access rules from the secure element. If, on the other hand, the value of the refresh tag stored in the secure element does not match the value of the refresh tag stored by the enforcer, then that would indicate that the access rules stored by the enforcer are not up-to-date; that is, that one or more of the access rules stored in the secure element has been updated since the last time the enforcer retrieved the access rules from the secure element. In this case, the enforcer would retrieve from the secure element, and store, the updated set of access rules and the updated value of the refresh tag.

[0009] One drawback, however, to polling schemes such as the scheme described above, is that they can result in an inefficient utilization of computing resources, such as the utilization of processor power, processor time, memory, communication channels, and the like. For instance, when no updates have been made to the access rules, polling the refresh tag periodically would needlessly render a processor of the mobile communication device busy.

[0010] Likewise, when no updates have been made to the access rules, polling the refresh tag upon receiving a request for information and/or an action protected by the rules would needlessly render the processor busy, and would also negatively impact the user's experience by delaying the granting of the request until after the polling has been completed.

[0011] Moreover, even when an update has been made to the access rules, polling the refresh tag upon receiving a request for information and/or an action protected by the rules would negatively impact the user's experience by delaying the granting of the request until after both the polling of the refresh tag and the updating of the local access rules have been completed.

- 5 -

[0012] Given the foregoing, it would be beneficial to enable access rules to be updated and enforced in an efficient manner that improves both the user's experience and the utilization of computing resources.

SUMMARY

[0013] The example embodiments herein provide systems, methods, and computer program products for managing access control.

[0014] In accordance with one example aspect herein, a first set of access control rules is stored in a memory of mobile communication device. The mobile communication device receives from a trusted server over a communication network a notification message indicating that an access control rule has been updated in a secure element. In response to receiving the notification message, the mobile communication device retrieves from the secure element a second set of access control rules including at least the access control rule that has been updated. The first set of access control rules is updated based on the second set of access control rules retrieved from the secure element. An applet stored on the secure element is accessed via an application running on the mobile communication device, in accordance with the updated first set of access control rules.

[0015] In another example embodiment, the notification message is pushed to the mobile communication device each time the trusted server transmits an update message to the secure element to cause at least one access control rule of the second set of access control rules to be updated.

[0016] In one example herein, the trusted server pushes the notification message to the mobile communication device by way of a notification server.

[0017] In accordance with some example aspects herein, a plurality of applets stored on the secure element are accessed, in succession, without performing a polling process of a refresh tag of the secure element in between each accessing.

[0018] In another example herein, the mobile communication device includes the secure element.

- 6 -

[0019] A request to access the applet is communicated, in one example, and the retrieving of the second set of access control rules from the secure element is performed before the communicating of the request to access the applet.

[0020] The access control rule that has been updated indicates whether the application has permission to access the applet stored on the secure element, in accordance with another example herein.

BRIEF DESCRIPTION OF THE DRAWINGS

[0021] The features and advantages of the example embodiments presented herein will become more apparent from the detailed description set forth below when taken in conjunction with the following drawings.

[0022] FIG. 1 is a diagram of an example system for managing access control, in accordance with various example embodiments herein.

[0023] FIG. 2 shows an example mobile communication device, in accordance with an example embodiment herein.

[0024] FIG. 3 shows an example procedure for managing access control, in accordance with an example embodiment herein.

[0025] FIG. 4 shows another example procedure for managing access control, in accordance with an example embodiment herein.

[0026] FIG. 5 is a block diagram of a general and/or special purpose computer that may be employed in accordance with various example embodiments herein.

DETAILED DESCRIPTION

I. Overview

[0027] The terms “payment product” and “card” may be used interchangeably herein to refer to a product, such as, for example, a credit card, a general purpose reloadable (GPR) card, and/or the like, that may be used to conduct financial transactions.

[0028] The term “service provider data” as used herein generally refers to data relating to one or more service providers, service provider systems, and/or services provided by one or more service providers. In some example embodiments herein,

- 7 -

service provider data refers to any data associated with a service provider that is stored in a wallet database and/or in a wallet client database.

The terms “access control rule” and “access rule” may be used interchangeably herein to refer to a rule that governs access to information stored on a secure element. For example, an access rule may indicate which applications installed on a mobile communication device are permitted to access which applications, applets, and/or other information stored on a secure element coupled to or installed in the mobile communication device. One example set of access rules that may be stored on a secure element and/or by an enforcer, and/or by another component of a mobile device is provided below in Table 1.

Table 1

Rule ID	Identifier (e.g., Hash Value) of Mobile Device Application	Application Identifier (AID) of Secure Element Applet	Permission for Mobile Device Application to Access Secure Element Applet
Rule 1	Hash value 1	AID A	Allow
Rule 2	Hash value 1	AID B	Disallow
Rule 3	Hash value 2	Any	Allow
Rule 4	Hash value 2	AID B	Disallow
Rule 5	Hash value 2	AID C	Disallow

[0029] Each of the example access rules shown in Table 1 indicate whether a particular mobile device application (e.g., as identified by a corresponding hash value) is allowed or disallowed to access a particular applet (e.g., as identified by an application identifier (AID)) stored on the secure element.

[0030] Another example set of access rules that may be stored on a secure element and/or by an enforcer, and/or by another component of a mobile device is provided below in Table 2.

Table 2

Rule ID	Application Identifier (AID) of Secure Element Applet	Rule Description
----------------	--	-------------------------

- 8 -

Rule 1	AID A	Allow mobile device applications signed with Certificate-A to access the secure element applet having AID A
Rule 2	AID B	Allow all mobile device applications to access the secure element applet having AID B
Rule 3	Any Applet	Allow mobile device applications signed with Certificate-B to access all secure element applets
Rule 4	AID C	Disallow mobile device applications signed with Certificate-C to access the secure element applet having AID C

[0031] The example access rules shown in Table 2 indicate conditions (*e.g.*, whether an application is signed with a particular certificate) based upon which access to one or more (or all) applets stored on the secure element is allowed or disallowed.

[0032] Presented herein are novel and inventive systems, methods, and computer program products for managing access control. In accordance with some aspects described herein, systems, methods, and computer program products are provided that enable access rules to be updated and enforced in an efficient manner that improves both the user's experience and the utilization of computing resources (*e.g.*, the utilization of processor power, processor time, memory, communication channels, and the like).

[0033] Unlike existing approaches to managing access control, which employ an inefficient polling scheme whereby, for example, a refresh tag associated with access rules is periodically polled, irrespective of whether any updates have been made to the access rules, in accordance with the example aspects described herein, a triggers scheme is provided such that updates to access rules need only be retrieved upon the access rules having been updated.

[0034] Also, the example aspects described herein, unlike existing approaches, avoid the need to poll the refresh tag upon receiving a request for information and/or an action protected by the access rules. The user's experience is thus improved since

- 9 -

the granting of the request need not be delayed until after both the polling of the refresh tag and the updating of the local access rules have been completed.

II. System

[0035] FIG. 1 is a diagram of an example system 100 for managing access control. The system 100 includes a mobile device 101, a network 102, a trusted service manager (TSM) 103, a network 104, and one or more service provider (SP) systems 105-1, 105-2, 105-n (collectively “105”).

[0036] The mobile device 101 may be a cellular phone, a tablet computer, or another type of electronic device with connectivity to one or more mobile networks. As will be described in further detail below in connection with FIG. 2, the mobile device 101 includes several components (such as, for example, a mobile wallet 106 and a secure element 107) which enable the mobile device to be used to conduct financial transactions (*e.g.*, payments) and/or non-financial transactions (*e.g.*, venue admissions), without the need for physical cash, checks, credit cards, tickets, and/or the like. Although the secure element 107 is shown in FIG. 1 as being included within the mobile device 101, this is for convenience only and should not be construed as limiting. In other example embodiments, the secure element 107 may be external to and/or removable from the mobile device 101.

[0037] The mobile device 101 is communicatively coupled to the TSM 103 by way of the network 102. The network 102 may be a mobile phone cellular network, a radio network, a WI-FI network, and/or another type of network. In some example embodiments, the network 102 is operated by a corresponding mobile network operator (MNO) (not shown in FIG. 1). The network 102 may be referred to as an “over-the-air” (OTA) network since it enables systems and/or devices to communicate using wireless standards.

[0038] The TSM 103 is a module, implemented in hardware and/or software, that functions as an intermediary between entities (*e.g.*, service provider systems 105, mobile wallets 106, secure elements 107, etc.) in a mobile commerce environment. In one example embodiment herein, the TSM 103 represents a central TSM managed by a mobile wallet provider (*e.g.*, a provider of the mobile wallet 106). The TSM

- 10 -

103, for example, manages communications between entities, such as the SP systems 105 and the mobile device 101 (*e.g.*, the mobile wallet 106, the secure element 107, and/or any other component of the mobile device 101), and also provides interfaces for communication with other computer systems. The TSM 103 communicates with the mobile device 101 via the network 102 using security protocols such as, for example, a GlobalPlatform secure channel protocol, secure sockets layer (SSL), transport layer security (TLS), and/or another security protocol.

[0039] The TSM 103 also provisions applets, such as contactless applets associated with the service provider systems 105, to the mobile device 101 for use by the mobile wallet 106, for example. The TSM 103 remotely distributes and remotely manages (*e.g.*, by updating access rules for the applets) the contactless applets by communicating with the secure element 107.

[0040] As will be described in further detail below in connection with FIG. 4, in one example embodiment, a notification service, running on the TSM 103 or on a separate notification server 108, is used to provide the mobile device 101 with notifications regarding updates to access rules. In this way, updates to access rules need only be retrieved from the secure element 107 upon the access rules having been updated. This enables access rules to be updated and enforced in an efficient manner that improves both the user's experience and the utilization of computing resources (*e.g.*, the utilization of processor power, processor time, memory, communication channels, and the like). Also, the example aspects described herein avoid the need to poll the refresh tag upon receiving a request for information and/or an action protected by the access rules. The user's experience thus may be improved since the granting of the request need not be delayed until after both the polling of the refresh tag and the updating of the local access rules have been completed.

[0041] The notification server 108 may be communicatively coupled to the mobile device 101 by way of the network 102, which, as described above, may be a mobile phone cellular network, a radio network, a WI-FI network, and/or another type of network. In some example embodiments, the notification server 108 is communicatively coupled to the mobile device 101 by way of an additional network

- 11 -

(*e.g.*, a mobile phone cellular network, a radio network, a WI-FI network, and/or another type of network; not shown in FIG. 1) that is distinct from the network 102. The notification server 108 may be communicatively coupled to the TSM 103 by way of a direct connection, a proprietary network, the network 102, and/or any other type of communication path.

[0042] In one example embodiment, the TSM 103 manages communications between the mobile wallet 106 and one of the SP systems 105 in order to request and obtain data for use in a mobile financial or non-financial transaction. For example, the TSM 103 provides access rules to the secure element 107 by way of the network 102, the access rules indicating which applications (*e.g.*, the mobile wallet 106) installed on the mobile device 101 have permission to access which information (*e.g.*, applets) stored on the secure element 107. The TSM 103 may provide the access rules upon an initial installation of a corresponding application on the mobile device 101, and/or may provide updates to the access rules after the corresponding application has been installed on the mobile device 101. The updates to the access rules may be initiated by the TSM 103, by the SP systems 105, by the mobile device 101, and/or by any other entity (*e.g.*, an entity not shown in FIG. 1).

[0043] The TSM 103 is communicatively coupled to the SP systems 105 by way of the network 104. The network 104 may be a virtual private network (VPN), a network using Hypertext Transfer Protocol (HTTP) standards, the Internet, and/or another type of network.

[0044] The SP systems 105, in some example embodiments, are systems owned, operated, maintained, and/or provided by service providers to enable customers or consumers to utilize one or more services of the service provider.

[0045] Having described the example system 100 for managing access control, reference will now be made to FIG. 2 to describe in further detail the example mobile device 101. As shown in FIG. 2, the mobile device 101 includes the mobile wallet 106 and the secure element 107, which are mentioned above in connection with FIG. 1. Although the secure element 107 is shown in FIG. 2 as being included within the mobile device 101, this is for convenience only and should not be

- 12 -

construed as limiting. In other example embodiments, the secure element 107 may be external to the mobile device 101.

[0046] The mobile device 101 also includes a processor 201, a memory 202, an enforcer 203, and locally stored (*e.g.*, stored locally in one or more memories of the mobile device 101) access rules 204. It should be understood that, although not shown in FIG. 2 for purposes of convenience, the mobile device 101 may include other components, such as a mobile operating system, other applications, a display (*e.g.*, a touchscreen display), a user interface, a keyboard, an antenna, and/or the like. Additionally, although not shown in FIG. 2 for purposes of convenience, the components of mobile device 101 may be interconnected via any number of paths, such as a communication bus, direct point-to-point links, and/or the like.

[0047] In general, the processor 201 executes instructions that may be stored in the memory 202, the mobile wallet 106, the enforcer 203, the secure element 107, and/or in any other component of the mobile device 101, to enable the mobile device 101 to perform certain functions. The memory 202 may also store data that is generated and/or used by the processor 201 in executing such instructions.

[0048] The mobile wallet 106 is an interactive application stored in a non-transitory memory of the mobile device 101. In one example embodiment, the mobile wallet 106 includes instructions that, when executed by the processor 201, enable the mobile communication device 101 to (1) access information or utilize one or more services provided by the service provider systems 105, (2) communicate with the service provider systems 105, and/or (3) interact with contactless services and/or control the operation of contactless hardware of the mobile device 101, for example, to conduct contactless transactions and/or process commerce information such as offer and/or loyalty information.

[0049] The mobile wallet 106 also includes instructions which, when executed by the processor 201, cause the mobile device 101 to act as an instrument for processing transactions such as financial transactions, in one example. The mobile wallet 106 provides an interface for receiving inputs and displaying outputs. The mobile wallet 106 communicates with the secure element 107 and applets 206 (described below)

- 13 -

stored on the secure element 107, using commands transmitted via application programming interfaces (APIs) (not shown in FIG. 2).

[0050] In one example, the mobile wallet 106 stores data (*e.g.*, an account number corresponding to an account provided by the service provider for use via the mobile wallet, and/or any other type of data associated with the mobile wallet and/or with a service provider) that the mobile wallet 106 utilizes to perform certain functions. For instance, the mobile wallet 106 may store applet data regarding one or more applet(s) (*e.g.*, the applets 206 described below) that the mobile wallet 106 uses to access and/or interact with the applets 206.

[0051] The secure element 107 is a platform onto which service account information and corresponding applications may be added, stored, personalized, and managed. The secure element 107 includes hardware and software, and implements interfaces and protocols that enable the secure storage of data, such as credentials, service account information, and applications (also referred to herein as “applets”) that may be used for conducting financial and/or non-financial transactions. In one example, the applets may correspond to a service (*e.g.*, payment, commerce, ticketing) offered by a service provider (*e.g.*, a service provider associated with one of the SP systems 105).

[0052] The secure element 107 may be implemented in different form factors, such as, for example, a Universal Integrated Circuit Card (UICC), an embedded secure element, and/or a separate chip or secure device (*e.g.*, a near-field communication (NFC) enabler) that can be inserted into a slot on the mobile device 101. In one example embodiment, the mobile wallet 106 communicates with the secure element 107 using ISO 7816 commands, in order to conduct contactless transactions. The secure element 107 also stores security-critical applets, such as those involving payment and account credentials, which require secure hardware storage and a secure execution environment.

[0053] The secure element 107 includes secure element access rules 205 and one or more applets 206-1, 206-2, 206-n (collectively “206”). In one example embodiment, the one or more applets 206-1, 206-2, 206-n are associated with respective ones of

- 14 -

the SP systems 105-1, 105-2...105-n described above in connection with FIG. 1. The applets may be, in one example, contactless applets associated with the service provider systems 105, which are provisioned by the TSM 103 on the mobile device 101 for use by the mobile wallet 106. The TSM 103 remotely distributes and remotely manages the contactless applets by accessing the secure element 107, for example, to provide updates to access rules associated with the applets.

[0054] The applets 206 may include instructions that, when executed by the processor 201, enable a user of the mobile device 101 to communicate with, and/or utilize one or more services provided by, the corresponding service provider. For example, an applet 206 provided by a payment product issuer, may enable the user to check a balance of the user's account, view transaction history and/or other notifications regarding the user's account, and/or the like.

[0055] The enforcer 203 is a module, implemented in hardware and/or software, that enforces access rules that govern which applications installed on the mobile device 101 are permitted to access which information (*e.g.*, applets 206) stored on the secure element 107. In some example embodiments herein, the enforcer 203 utilizes the memory 202 of the mobile device 101 and/or utilizes a separate memory included in the enforcer 203 (not shown in FIG. 2) to store data and/or instructions that the enforcer 203 uses to execute one or more functions (*e.g.*, to enforce access rules). As will be described in further detail below in connection with FIGS. 3 and 4, in accordance with one example embodiment, updates to the access rules 205 are provided to the secure element 107 by the TSM 103. The enforcer 203 also stores a local set of access rules 204 (*e.g.*, which may be stored on the memory 202 of the mobile device 101) that mirror the access rules 205 stored in the secure element 107. In this way, the mobile wallet 106 may access one or more of the applets 206 in the secure element 107 in accordance with the local access rules 204, without having to retrieve the access rules 205 in the secure element 107.

III. Procedure

[0056] Having described an example system 100 for managing access control, reference will now be made to FIG. 3 to describe an example procedure 300 for

- 15 -

managing access control, in accordance with an example embodiment herein. In the following description of the procedure 300, reference will also be made to certain elements of FIG. 1 (*e.g.*, one or more of elements 101 through 108) and/or of FIG. 2 (*e.g.*, one or more of elements 201 through 206), which are described in further detail above.

[0057] At step 301, the enforcer 203 locally (*e.g.*, in a memory local to the mobile device 101) stores an initial version of the access rules 204, which, in one example, are received (not shown in FIG. 3) from the TSM 103 upon an initial provisioning of the applets 206 on the secure element 107. The initial version of the access rules 204 may include a plurality of access rules corresponding to the plurality of applets 206-1, 206-2...206-n, respectively. Additionally, although not shown in FIG. 3 for purposes of convenience, in one example, a copy/duplicate of the initial version of the access rules 204 is also stored on the secure element 107 in the form of the access rules 205, upon the initial provisioning of the applets 206 on the secure element 107.

[0058] At step 302, the TSM 103 communicates an update to one or more access rules 205 stored on the secure element 107. The update may be triggered by a service provider system 105, the TSM 103 itself, by an administrator computer (not shown in the Figures) coupled to the TSM 103, and/or by another system. The update may include, for example, new credentials, a new payment account number, and/or the like to be used in connection with any of the applets 206.

[0059] Upon receiving the update from the TSM 103 at block 302, the updated access rules 205 are stored in the secure element 107.

[0060] Once the access rules are successfully updated, the TSM 103 communicates, at step 303, a notification message to the enforcer 203, indicating that at least one of the access rules has been updated.

[0061] In one example embodiment, the enforcer 203 is configured such that the receipt of the notification message communicated at step 303 triggers the enforcer 203 to retrieve, at step 304, the updated access rules 205 from the secure element 107. By virtue of this trigger, the enforcer 203 may avoid the need to poll the refresh tag of the secure element 107 (whether periodically and/or upon receiving a request

- 16 -

to access information on the secure element 107) to determine whether the access rules are up-to-date. That is, in accordance with this example embodiment, no polling of the refresh tag is required unless and until a notification message is received by the enforcer 203 indicating that the access rules have been updated. In this way, processing resources may be more efficiently utilized and network traffic may be decreased, since unnecessary polling messages may be discontinued.

[0062] At step 305, the enforcer 203 updates the locally stored access rules 204 based on the updated access rules 205 retrieved from the secure element 107 at step 304.

[0063] At step 306, the enforcer 203 receives a request for access to an applet 206 stored on the secure element 107. The request for access to the applet 206 may, in one example, be triggered by a request from a user to access a payment product associated with the applet 206 (*e.g.*, an applet 206 associated with one of the SP systems 105) and provided via the mobile wallet 106.

[0064] At step 307, the enforcer 203 retrieves, from the locally stored access rules 204, one or more access rules that are associated with the applet 206 to which access was requested at step 306.

[0065] At step 308, the enforcer 203 grants or denies access to the applet 206 (stored in the secure element 107) that was requested at step 306, in accordance with the one or more corresponding access rules retrieved at step 307 from the locally stored access rules 204. Since no polling of the refresh tag is required upon receiving at step 306 the request for access, the user experience may be improved, since the granting of the request need not be delayed until after both the polling of the refresh tag and the updating of the local access rules have been completed.

[0066] At step 309, the enforcer 203 receives a subsequent request for access to an applet 206 stored on the secure element 107. The applet 206 to which access is requested at step 309 may be the same as or different from the applet 206 to which access was requested at step 306.

- 17 -

[0067] At step 310, the enforcer 203 retrieves, from the locally stored access rules 204, one or more access rules that are associated with the applet 206 to which access was requested at step 309.

[0068] At step 311, the enforcer 203 grants or denies access to the applet 206 (stored in the secure element 107) that was requested at step 309, in accordance with the one or more corresponding access rules retrieved at step 308 from the locally stored access rules. Again, since no polling of the refresh tag is required upon receiving at step 309 the request for access, the user experience may be improved, since the granting of the request need not be delayed until after both the polling of the refresh tag and the updating of the local access rules have been completed. Additionally, since no polling of the refresh tag need be performed in between successively received requests for access to applets, processing resources may be more efficiently utilized.

[0069] Having described a first example procedure 300 for managing access control, reference will now be made to FIG. 4 to describe another example procedure 400 for managing access control, in accordance with an example embodiment herein.

[0070] As will be apparent from the description below, one difference between the example procedure 300 described above and the example procedure 400 described below is that the procedure 400 employs an optional notification server 108. In one example embodiment, the notification server 108 provides the TSM 103 with communication protocol flexibility. For instance, the TSM 103 may push notifications to the mobile device 101 by using WI-FI, 3G, 4G LTE, the Short Message Service (SMS) protocol, or any other suitable communication protocol. In one example, the TSM 103 may utilize the notification server 108 to push notifications to the mobile device 101 by using a communication protocol that is different from the communication protocol(s) available by way of the network 102.

[0071] At step 401, the enforcer 203 locally stores an initial version of the access rules 204, which, in one example, are received (not shown in FIG. 4) from the TSM 103 upon an initial provisioning of the applets 206 on the secure element 107. The initial version of the access rules 204 may include a plurality of access rules

- 18 -

corresponding to the plurality of applets 206-1, 206-2...206-n, respectively. Additionally, although not shown in FIG. 4 for purposes of convenience, in one example, a copy/duplicate of the initial version of the access rules 204 is also stored on the secure element 107 in the form of the access rules 205, upon the initial provisioning of the applets 206 on the secure element 107.

[0072] At step 402, the TSM 103 communicates an update to one or more access rules 205 stored on the secure element 107. The update may be triggered by a service provider system 105, the TSM 103 itself, by an administrator computer (not shown in the Figures) coupled to the TSM 103, and/or by another system. The update may include, for example, new credentials, a new payment account number, and/or the like to be used in connection with any of the applets 206.

[0073] Upon receiving the update from the TSM 103 at block 402, the updated access rules 205 are stored in the secure element 107.

[0074] At step 403, upon successfully updating the access rules 205 stored in the secure element 107, the TSM 103 communicates to the notification server 108 a request that the notification server 108 push a notification message to the enforcer 203 to indicate that the access rules 205 have been successfully updated.

[0075] Upon receiving at step 403 the request from the TSM 103, the notification server 108 communicates, at step 404, a notification message to the enforcer 203, indicating that at least one of the access rules has been updated.

[0076] In one example embodiment, the enforcer 203 is configured such that the receipt of the notification message communicated at step 404 triggers the enforcer 203 to retrieve, at step 405, the updated access rules 205 from the secure element 107. By virtue of this trigger, the enforcer 203 may avoid the need to poll the refresh tag of the secure element 107 (whether periodically and/or upon receiving a request to access information on the secure element 107) to determine whether the access rules are up-to-date. That is, in accordance with this example embodiment, no polling of the refresh tag is required unless and until a notification message is received by the enforcer 203 indicating that the access rules have been updated. In

- 19 -

this way, processing resources may be more efficiently utilized and network traffic may be decreased, since unnecessary polling messages may be discontinued.

[0077] At step 406, the enforcer 203 updates the locally stored access rules 204 based on the updated access rules 205 retrieved from the secure element 107 at step 304.

[0078] At step 407, the enforcer 203 receives a request for access to an applet 206 stored on the secure element 107. The request for access to the applet 206 may, in one example, be triggered by a request from a user to access a payment product associated with the applet 206 (*e.g.*, an applet 206 associated with one of the SP systems 105) and provided via the mobile wallet 106.

[0079] At step 408, the enforcer 203 retrieves, from the locally stored access rules 204, one or more access rules that are associated with the applet 206 to which access was requested at step 407.

[0080] At step 409, the enforcer 203 grants or denies access to the applet 206 (stored in the secure element 107) that was requested at step 407, in accordance with the one or more corresponding access rules retrieved at step 408 from the locally stored access rules 204. Since no polling of the refresh tag is required upon receiving at step 407 the request for access, the user experience may be improved, since the granting of the request need not be delayed until after both the polling of the refresh tag and the updating of the local access rules have been completed.

[0081] At step 410, the enforcer 203 receives a subsequent request for access to an applet 206 stored on the secure element 107. The applet 206 to which access is requested at step 410 may be the same as or different from the applet 206 to which access was requested at step 407.

[0082] At step 411, the enforcer 203 retrieves, from the locally stored access rules 204, one or more access rules that are associated with the applet 206 to which access was requested at step 410.

[0083] At step 412, the enforcer 203 grants or denies access to the applet 206 (stored in the secure element 107) that was requested at step 410, in accordance with the one or more corresponding access rules retrieved at step 411 from the locally stored

- 20 -

access rules. Again, since no polling of the refresh tag is required upon receiving at step 410 the request for access, the user experience may be improved, since the granting of the request need not be delayed until after both the polling of the refresh tag and the updating of the local access rules have been completed. Additionally, since no polling of the refresh tag need be performed in between successively received requests for access to applets, processing resources may be more efficiently utilized.

IV. Example Computer-readable Medium Implementations

[0084] The example embodiments described above, such as, for example, the systems and procedures depicted in or discussed in connection with FIGs. 1 through 4 or any part or function thereof, may be implemented by using hardware, software or a combination of the two. The implementation may be in one or more computers or other processing systems. While manipulations performed by these example embodiments may have been referred to in terms commonly associated with mental operations performed by a human operator, no human operator is needed to perform any of the operations described herein. In other words, the operations may be completely implemented with machine operations. Useful machines for performing the operation of the example embodiments presented herein include general-purpose digital computers or similar devices.

[0085] FIG. 5 is a block diagram of a general and/or special purpose computer 500 that may be employed in accordance with various example embodiments herein. The computer 500 may be, for example, a user device, a user computer, a client computer, and/or a server computer, among other things.

[0086] The computer 500 may include without limitation a processor device 510, a main memory 525, and an interconnect bus 505. The processor device 510 may include without limitation a single microprocessor, or may include a plurality of microprocessors for configuring the computer 500 as a multi-processor system. The main memory 525 stores, among other things, instructions and/or data for execution by the processor device 510. The main memory 525 may include banks of dynamic random access memory (DRAM), as well as cache memory.

- 21 -

[0087] The computer 500 may further include a mass storage device 530, peripheral device(s) 540, portable storage medium device(s) 550, input control device(s) 580, a graphics subsystem 560, and/or an output display 570. For explanatory purposes, all components in the computer 500 are shown in FIG. 5 as being coupled via the bus 505. However, the computer 500 is not so limited. Devices of the computer 500 may be coupled via one or more data transport means. For example, the processor device 510 and/or the main memory 525 may be coupled via a local microprocessor bus. The mass storage device 530, peripheral device(s) 540, portable storage medium device(s) 550, and/or graphics subsystem 560 may be coupled via one or more input/output (I/O) buses. The mass storage device 530 may be a nonvolatile storage device for storing data and/or instructions for use by the processor device 510. The mass storage device 530 may be implemented, for example, with a magnetic disk drive or an optical disk drive. In a software embodiment, the mass storage device 530 is configured for loading contents of the mass storage device 530 into the main memory 525.

[0088] The portable storage medium device 550 operates in conjunction with a nonvolatile portable storage medium, such as, for example, a compact disc read only memory (CD-ROM), to input and output data and code to and from the computer 500. In some embodiments, the software for storing an internal identifier in metadata may be stored on a portable storage medium, and may be inputted into the computer 500 via the portable storage medium device 550. The peripheral device(s) 540 may include any type of computer support device, such as, for example, an input/output (I/O) interface configured to add additional functionality to the computer 500. For example, the peripheral device(s) 540 may include a network interface card for interfacing the computer 500 with a network 520.

[0089] The input control device(s) 580 provide a portion of the user interface for a user of the computer 500. The input control device(s) 580 may include a keypad and/or a cursor control device. The keypad may be configured for inputting alphanumeric characters and/or other key information. The cursor control device may include, for example, a mouse, a trackball, a stylus, and/or cursor direction keys.

- 22 -

In order to display textual and graphical information, the computer 500 may include the graphics subsystem 560 and the output display 570. The output display 570 may include a cathode ray tube (CRT) display and/or a liquid crystal display (LCD). The graphics subsystem 560 receives textual and graphical information, and processes the information for output to the output display 570.

[0090] Each component of the computer 500 may represent a broad category of a computer component of a general and/or special purpose computer. Components of the computer 500 are not limited to the specific implementations provided here.

[0091] Portions of the example embodiments of the invention may be conveniently implemented by using a conventional general-purpose computer, a specialized digital computer and/or a microprocessor programmed according to the teachings of the present disclosure, as is apparent to those skilled in the computer art. Appropriate software coding may readily be prepared by skilled programmers based on the teachings of the present disclosure.

[0092] Some embodiments may also be implemented by the preparation of application-specific integrated circuits, field programmable gate arrays, or by interconnecting an appropriate network of conventional component circuits.

[0093] Some embodiments include a computer program product. The computer program product may be a storage medium or media having instructions stored thereon or therein which can be used to control, or cause, a computer to perform any of the procedures of the example embodiments of the invention. The storage medium may include without limitation a floppy disk, a mini disk, an optical disc, a Blu-Ray Disc, a DVD, a CD-ROM, a micro-drive, a magneto-optical disk, a ROM, a RAM, an EPROM, an EEPROM, a DRAM, a VRAM, a flash memory, a flash card, a magnetic card, an optical card, nanosystems, a molecular memory integrated circuit, a RAID, remote data storage/archive/warehousing, and/or any other type of device suitable for storing instructions and/or data.

[0094] Stored on any one of the computer readable medium or media, some implementations include software for controlling both the hardware of the general and/or special computer or microprocessor, and for enabling the computer or

- 23 -

microprocessor to interact with a human user or other mechanism utilizing the results of the example embodiments of the invention. Such software may include without limitation device drivers, operating systems, and user applications. Ultimately, such computer readable media further includes software for performing example aspects of the invention, as described above.

[0095] Included in the programming and/or software of the general and/or special purpose computer or microprocessor are software modules for implementing the procedures described above.

[0096] As can be appreciated in view of the foregoing description, the example aspects herein provide a system, method, and computer-readable medium for managing access control that enable access rules to be updated and enforced in an efficient manner that improves both the user's experience and the utilization of computing resources (*e.g.*, the utilization of processor power, processor time, memory, communication channels, and the like).

[0097] Unlike existing approaches to managing access control, which employ an inefficient polling scheme whereby, for example, a refresh tag associated with access rules is periodically polled, irrespective of whether any updates have been made to the access rules, in accordance with the example aspects described herein, updates to access rules are retrieved only upon the rules having been updated.

[0098] Also, the example aspects described herein, unlike existing approaches, avoid the need to poll the refresh tag upon receiving a request for information and/or an action protected by the access rules. The user's experience is thus improved since the granting of the request need not be delayed until after both the polling of the refresh tag and the updating of the local access rules have been completed.

[0099] While various example embodiments of the invention have been described above, it should be understood that they have been presented by way of example, and not limitation. It is apparent to persons skilled in the relevant art(s) that various changes in form and detail can be made therein. Thus, the invention should not be limited by any of the above described example embodiments, but should be defined only in accordance with the following claims and their equivalents.

- 24 -

[00100] In addition, it should be understood that the figures are presented for example purposes only. The architecture of the example embodiments presented herein is sufficiently flexible and configurable, such that it may be utilized and navigated in ways other than that shown in the accompanying figures.

[00101] Further, the purpose of the Abstract is to enable the U.S. Patent and Trademark Office and the public generally, and especially the scientists, engineers and practitioners in the art who are not familiar with patent or legal terms or phraseology, to determine quickly from a cursory inspection the nature and essence of the technical disclosure of the application. The Abstract is not intended to be limiting as to the scope of the example embodiments presented herein in any way. It is also to be understood that the procedures recited in the claims need not be performed in the order presented.

- 25 -

WHAT IS CLAIMED IS:

1. A method for managing access control, the method comprising steps of:
 - storing a first set of access control rules in a memory of mobile communication device;
 - receiving, by the mobile communication device from a trusted server over a communication network, a notification message indicating that an access control rule has been updated in a secure element;
 - retrieving, by the mobile communication device from the secure element, a second set of access control rules including at least the access control rule that has been updated,
 - wherein the retrieving of the second set of access control rules from the secure element is performed in response to the receiving of the notification message;
 - updating the first set of access control rules based on the second set of access control rules retrieved from the secure element; and
 - accessing an applet stored on the secure element via an application running on the mobile communication device, in accordance with the updated first set of access control rules.
2. The method of claim 1, wherein the notification message is pushed to the mobile communication device each time the trusted server transmits an update message to the secure element to cause at least one access control rule of the second set of access control rules to be updated.
3. The method of claim 2, wherein the trusted server pushes the notification message to the mobile communication device by way of a notification server.
4. The method of claim 1, further comprising a step of:

- 26 -

accessing, in succession, a plurality of applets stored on the secure element, without performing a polling process of a refresh tag of the secure element in between each accessing.

5. The method of claim 1, wherein the mobile communication device includes the secure element.

6. The method of claim 1, further comprising:

communicating a request to access the applet,

wherein the retrieving of the second set of access control rules from the secure element is performed before the communicating of the request to access the applet.

7. The method of claim 1, wherein the access control rule that has been updated indicates whether the application has permission to access the applet stored on the secure element.

8. A system for managing access control, the system comprising:

at least one memory operable to store a first set of access control rules; and

a processor coupled to the at least one memory, the processor being operable to:

receive, from a trusted server over a communication network, a notification message indicating that an access control rule has been updated in a secure element;

retrieve from the secure element a second set of access control rules including at least the access control rule that has been updated,

wherein the retrieval of the second set of access control rules from the secure element is performed in response to the receipt of the notification message;

update the first set of access control rules based on the second set of access control rules retrieved from the secure element; and access an applet stored on

- 27 -

the secure element via an application running on the system in accordance with the updated first set of access control rules.

9. The system of claim 8,

wherein the trusted server is communicatively coupled to the system via the communication network, and

wherein the notification message is pushed to the processor each time the trusted server transmits an update message to the secure element to cause at least one access control rule of the second set of access control rules to be updated.

10. The system of claim 9, wherein the trusted server pushes the notification message to the processor by way of a notification server.

11. The system of claim 8, the processor being further operable to:

access, in succession, a plurality of applets stored on the secure element without performing a polling process of a refresh tag of the secure element in between each accessing.

12. The system of claim 8, further comprising the secure element.

13. The system of claim 8, wherein the processor is further operable to:

communicate a request to access the applet,

wherein the retrieval of the second set of access control rules from the secure element is performed before the communication of the request to access the applet.

14. The system of claim 8, wherein the access control rule that has been updated indicates whether the application has permission to access the applet stored on the secure element.

- 28 -

15. A non-transitory computer-readable medium having stored thereon sequences of instructions that, when executed by a computer processor, cause the computer processor to:

- store a first set of access control rules in a memory of a mobile communication device;

- receive, by the mobile communication device from a trusted server over a communication network, a notification message indicating that an access control rule has been updated in a secure element;

- retrieve, by the mobile communication device from the secure element, a second set of access control rules including at least the access control rule that has been updated,

- wherein the retrieval of the second set of access control rules from the secure element is performed in response to the receipt of the notification message;

- update the first set of access control rules based on the second set of access control rules retrieved from the secure element; and

- access an applet stored on the secure element via an application running on the mobile communication device, in accordance with the updated first set of access control rules.

16. The non-transitory computer-readable medium of claim 15, wherein the notification message is pushed to the mobile communication device each time the trusted server transmits an update message to the secure element to cause at least one access control rule of the second set of access control rules to be updated.

17. The non-transitory computer-readable medium of claim 16, wherein the trusted server pushes the notification message to the mobile communication device by way of a notification server.

- 29 -

18. The non-transitory computer-readable medium of claim 15, wherein the sequences of instructions, when executed by the computer processor, further cause the computer processor to:

access, in succession, a plurality of applets stored on the secure element, without performing a polling process of a refresh tag of the secure element in between each accessing.

19. The non-transitory computer-readable medium of claim 15, wherein the sequences of instructions, when executed by the computer processor, further cause the computer processor to:

communicate a request to access the applet,

wherein the retrieval of the second set of access control rules from the secure element is performed before the communication of the request to access the applet.

20. The non-transitory computer-readable medium of claim 15, wherein the access control rule that has been updated indicates whether the application has permission to access the applet stored on the secure element.

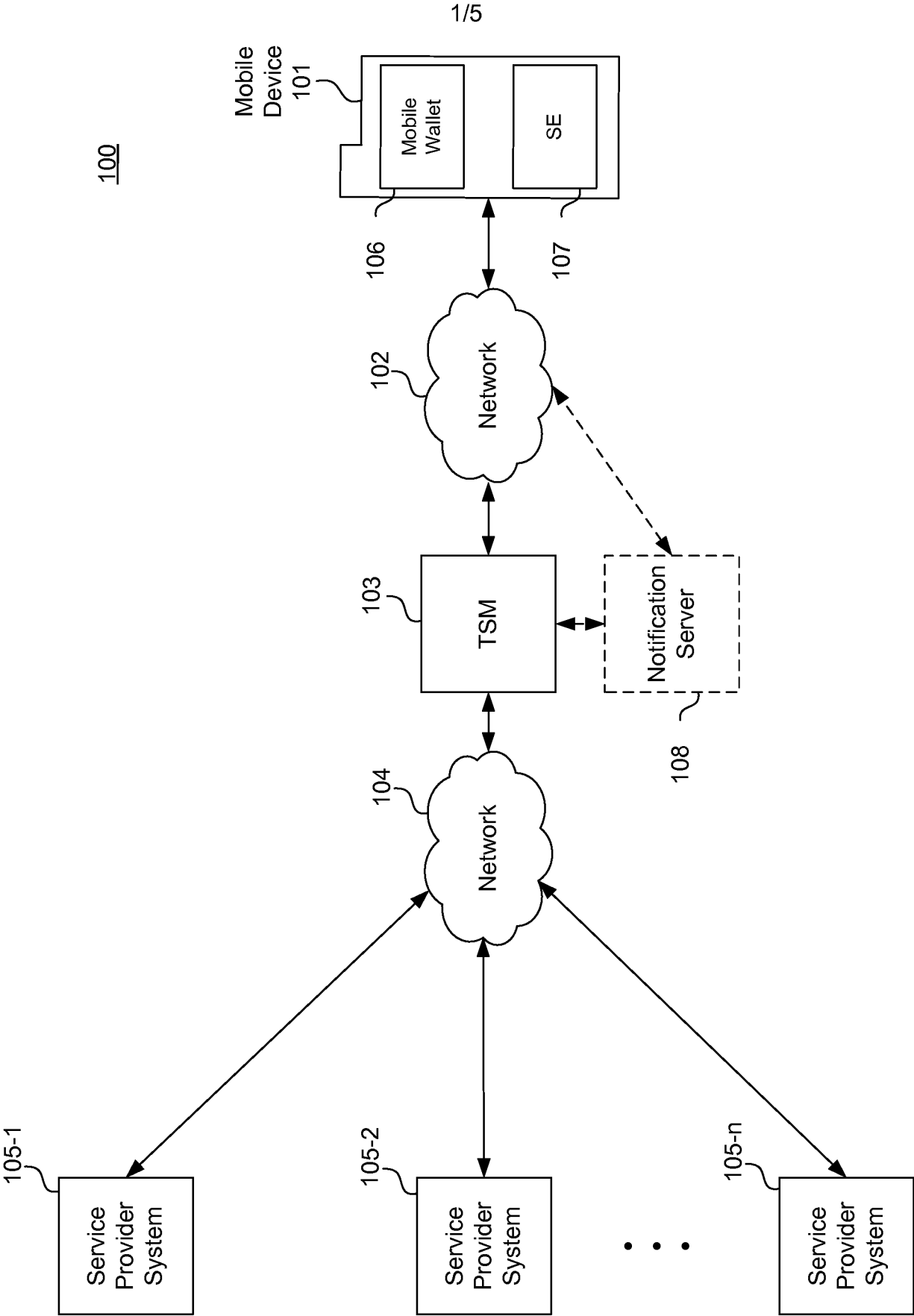


FIG. 1

2/5

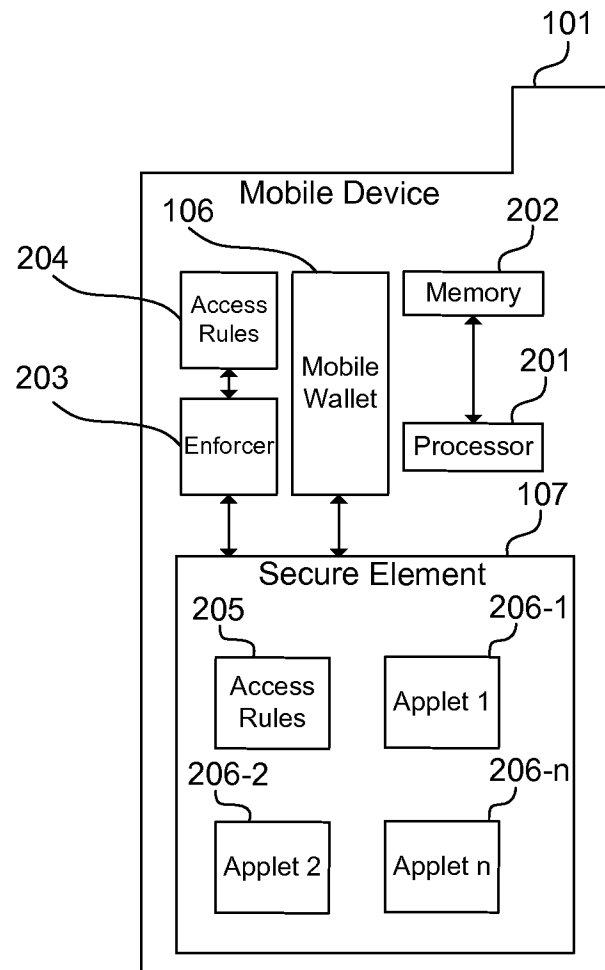


FIG. 2

3/5

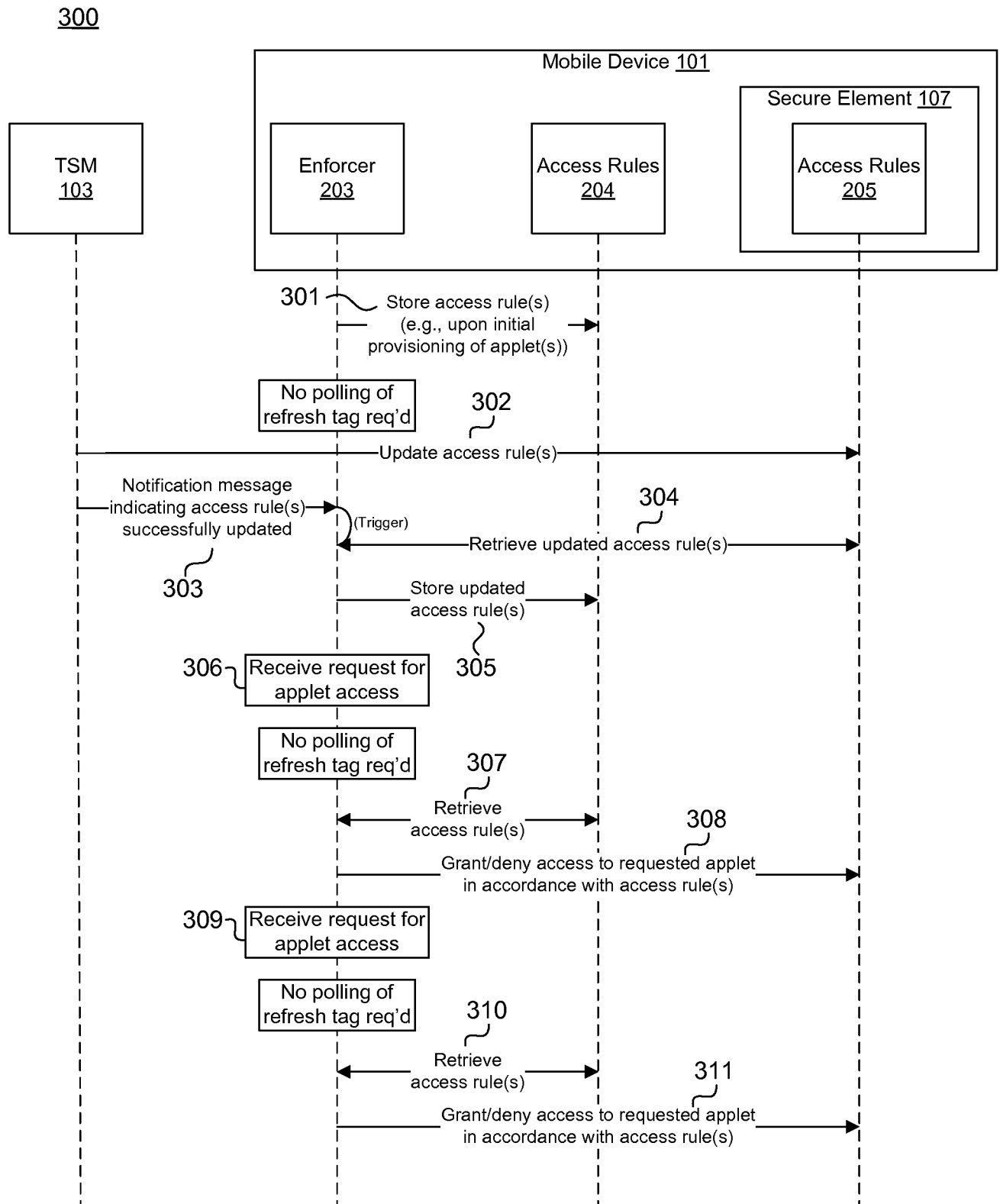


FIG. 3

4/5

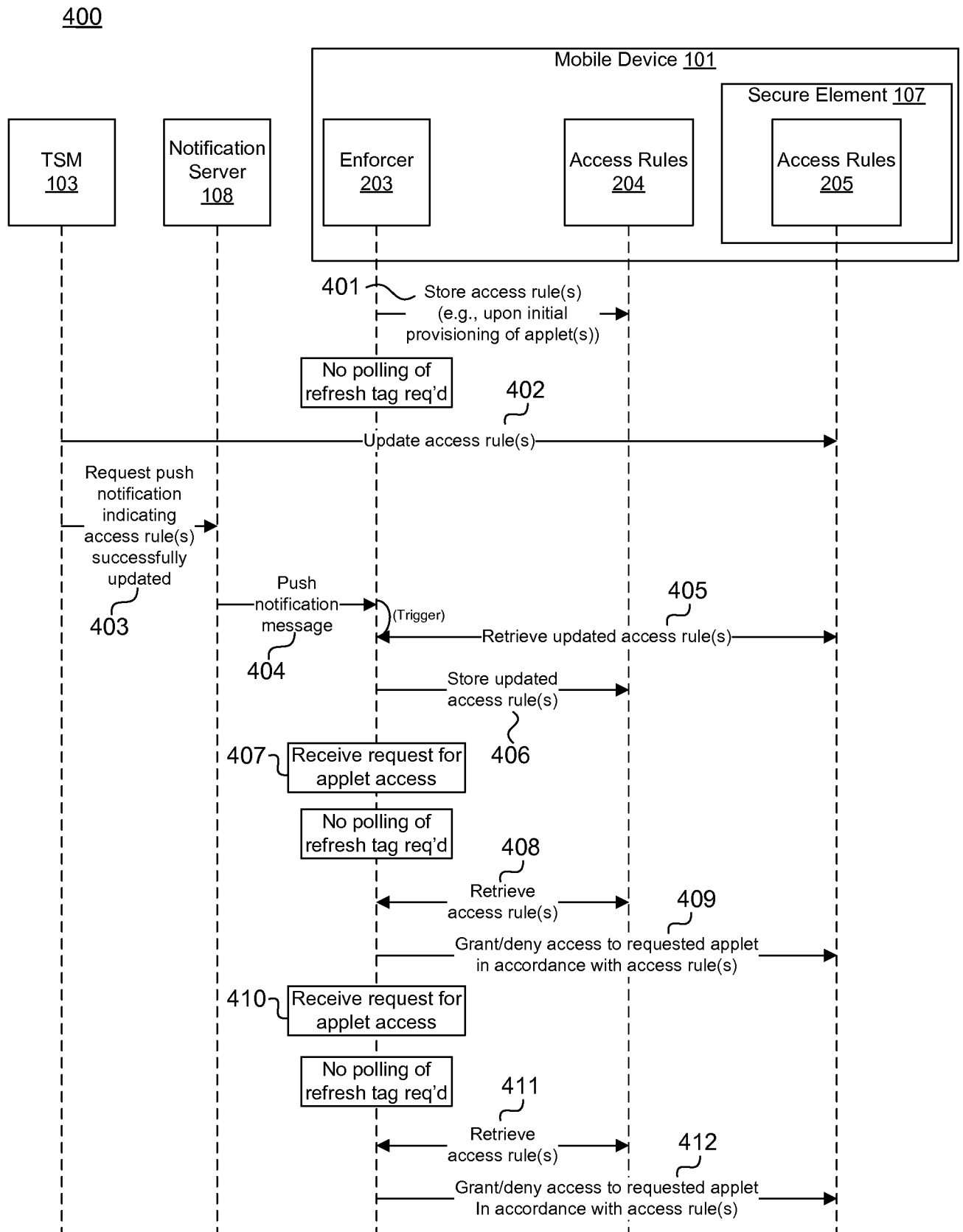
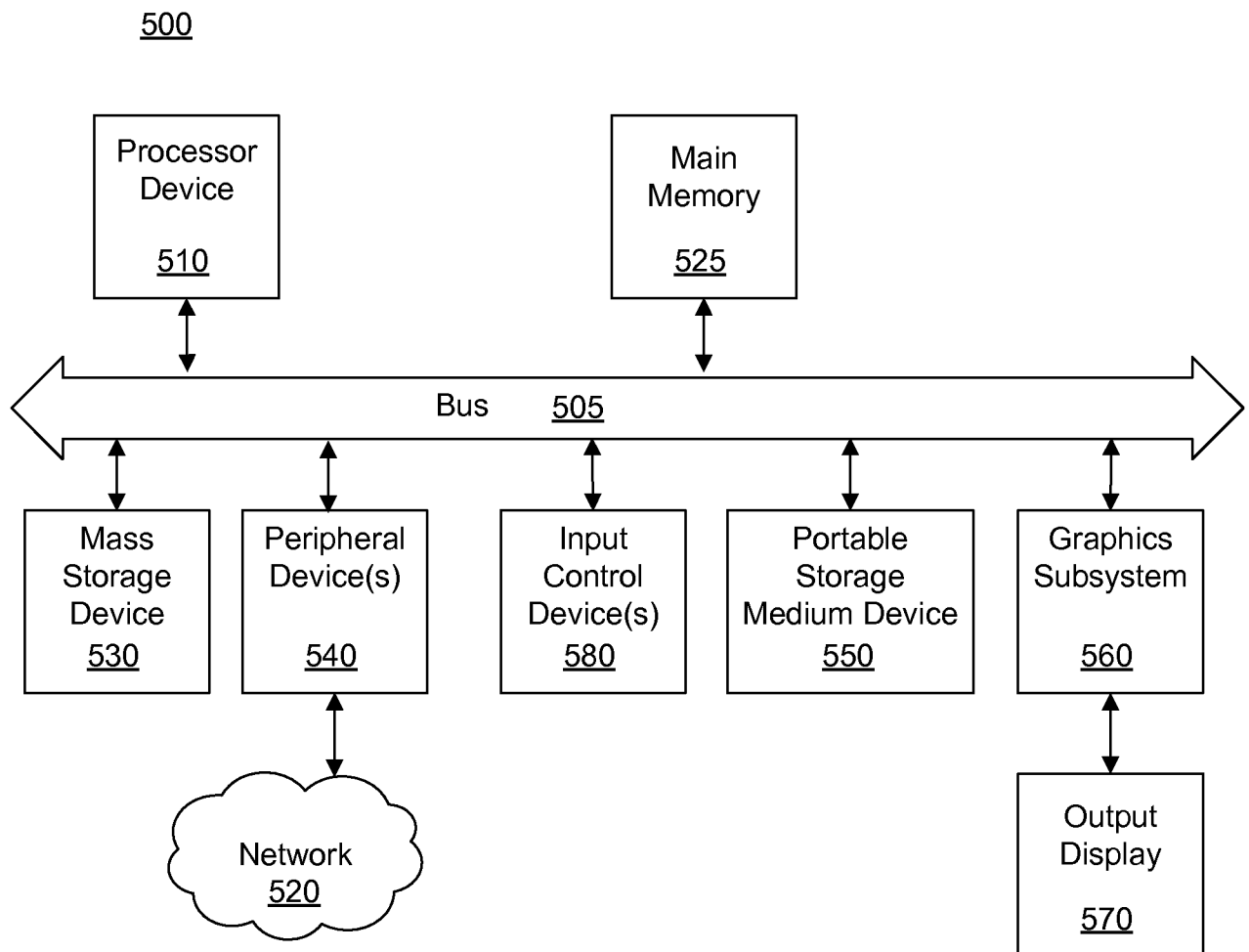


FIG. 4

5/5

**FIG. 5**

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2014/031737**A. CLASSIFICATION OF SUBJECT MATTER****H04W 68/00(2009.01)i, H04W 48/02(2009.01)i**

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)

H04W 68/00; G06F 21/12; G06F 15/173; G06F 17/30; H04M 1/66; H04W 48/02

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean utility models and applications for utility models

Japanese utility models and applications for utility models

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

eKOMPASS(KIPO internal) & Keywords: mobile, secure element, access rule, update, local and simliar terms.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2007-0207777 A1 (RUSSELL OWEN et al.) 06 September 2007 See paragraphs [0028]-[0054]; figure 2; and claim 1.	1-20
A	US 2012-0246119 A1 (CHRIS A. HAUDENSCHILD et al.) 27 September 2012 See paragraphs [0050]-[0058]; and figure 1.	1-20
A	US 2011-0302310 A1 (JOHN DIACHINA et al.) 08 December 2011 See paragraphs [0048]-[0049]; and figure 4.	1-20
A	US 2009-0221266 A1 (KEN OHTA et al.) 03 September 2009 See paragraphs [0053]-[0068]; and figures 1-6.	1-20
A	KR 10-2011-0125698 A (SK PLANET CO. LTD.) 22 November 2011 See paragraphs [0074]-[0079]; figure 1; and claim 10.	1-20



Further documents are listed in the continuation of Box C.



See patent family annex.

* 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

10 July 2014 (10.07.2014)

Date of mailing of the international search report

10 July 2014 (10.07.2014)

Name and mailing address of the ISA/KR

International Application Division
Korean Intellectual Property Office
189 Cheongsu-ro, Seo-gu, Daejeon Metropolitan City, 302-701,
Republic of Korea

Facsimile No. +82-42-472-7140

Authorized officer

KO, Yeon Hwa

Telephone No. +82-42-481-8569



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2014/031737

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2007-0207777 A1	06/09/2007	US 2005-0191991 A1 US 2009-0253424 A1 US 7142848 B2 US 7532882 B2 US 7751809 B2	01/09/2005 08/10/2009 28/11/2006 12/05/2009 06/07/2010
US 2012-0246119 A1	27/09/2012	US 2012-179663 A1 US 8386442 B2 US 8688649 B2	12/07/2012 26/02/2013 01/04/2014
US 2011-0302310 A1	08/12/2011	CN 102907064 A EP 2577933 A1 WO 2011-151747 A1	30/01/2013 10/04/2013 08/12/2011
US 2009-0221266 A1	03/09/2009	CN 100583118 C CN 101288084 A EP 1950681 A1 EP 1950681 A4 JP 04778970 B2 US 8135385 B2 WO 2007-043659 A1	20/01/2010 15/10/2008 30/07/2008 04/04/2012 21/09/2011 13/03/2012 19/04/2007
KR 10-2011-0125698 A	22/11/2011	None	