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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 November 2014 (27.11.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/189748 Al

(51) International Patent Classification:
H04W 12/00 (2009.01) *H04W 88/18* (2009.01)

(21) International Application Number:
PCT/US20 14/038080

(22) International Filing Date:
15 May 2014 (15.05.2014)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/825,870 2 1 May 2013 (21.05.2013) US

(71) Applicant: **JVL VENTURES, LLC** [US/US]; 230 Park Avenue 27th Floor, New York, NY 10169-0005 (US).

(72) Inventors: **VINSON, Yale, P.;** 2709 Woodbury Drive, Flower Mound, TX 75028 (US). **MULLOY, Scott, T.;** 36 Stonewall Lane, Monroe, CT 06468 (US). **RANGANATHAN, Balamourougan;** 2095 Ravens Ridge Drive, Cumming, GA 30041 (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))*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

(54) Title: SYSTEMS, METHODS AND COMPUTER PROGRAM PRODUCTS FOR MANAGING DISABLING OF SERVICES

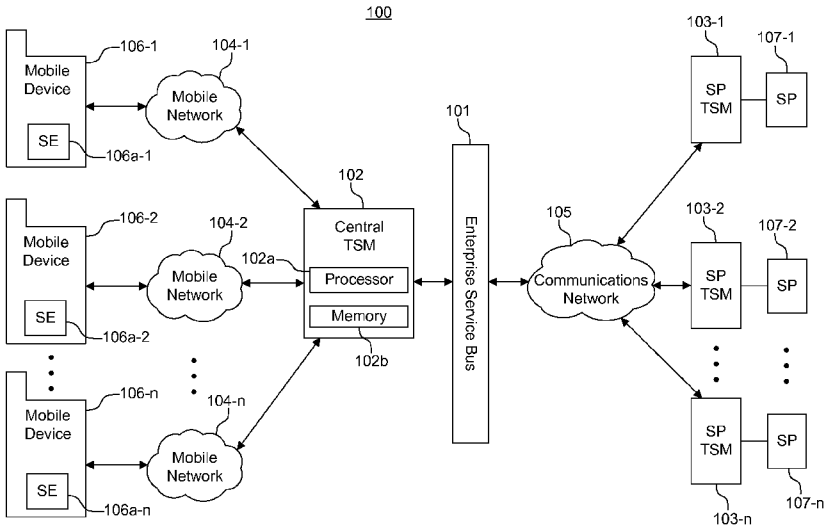

FIG. 1

(57) Abstract: A system, method, and computer readable storage medium for managing applications on a secure element. A request to modify the availability state of a version of a service, the availability state of the service being stored in a memory, is received. The availability state of the version of the service stored in the memory is modified in accordance with the request. More specifically, the availability state is modified to: (i) unavailable in a case where the request includes an instruction to disable the version of the service, and (ii) available in a case where the request includes an instruction to enable the version of the service. The service is associated with a secure element profile.

WO 2014/189748 A1

SYSTEMS, METHODS, AND COMPUTER PROGRAM PRODUCTS FOR MANAGING DISABLING OF SERVICES

BACKGROUND

Field

[0001] The present invention generally relates to managing applications on a secure element. More particularly, the present invention relates to systems, methods, and computer program products for managing the availability states of those applications.

Related Art

[0002] Mobile commerce is a rapidly growing industry in which users, through their mobile devices, purchase items in-store or online. To make these purchases, a mobile wallet is installed on a user's mobile device. The mobile wallet connects the user's bank account or credit cards to their mobile device. With the aid of a near-field communication chip (NFC), a user can use his/her mobile device to pay for goods and services from brick-and-mortar stores by contactlessly interacting with a NFC payment system. The mobile wallet itself is an application stored on the mobile device. Sensitive user information, in addition to one or more mobile commerce applications, may be stored on a secure element on the mobile device. The mobile commerce applications may originate from different sources, including service providers *(e.g.,* a merchant, a banking institution, or a credit card company) or an operator of a mobile network over which the mobile device communicates (also referred to as a mobile network operator (MNO)).

[0003] Mobile commerce applications are occasionally updated with newer versions, which are then delivered to the mobile devices. There is the potential, however, that an unforeseen issue may arise with an updated version of an application which may cause the user's mobile device to malfunction, or be rendered inactive altogether (commonly referred to as "bricking" a device). Considering that many mobile devices automatically update themselves, or are routinely updated by their users, a defective version may quickly propagate through a user community. Thus, with the release of each new version of an application, there is a potential for a cascading failure. To minimize this risk, new

versions of applications are tested extensively. Nevertheless, such testing cannot guarantee that an issue will not arise. Therefore, it would be advantageous to be able to stem the distribution of defective applications once a defect it discovered. Moreover, it would also be advantageous to quickly and efficiently stop the rollout of a defective application with minimal effort.

BRIEF DESCRIPTION

[0004] The present invention provides systems, methods, and computer program products for managing the availability states of applications on secure elements.

[0005] In one embodiment, a method of managing the availability of a service includes at least one receiving and modifying step. A request to modify an availability state of a version of the service is received. The availability state of the version of the service is stored in the memory and is modified in accordance with the request. The availability state is modified to: (i) unavailable in a case where the request includes an instruction to disable the version of the service, and (ii) available in a case where the request includes an instruction to enable the version of the service. The service is associated with a secure element profile.

[0006] In another embodiment, a data processing system for managing the availability of a service includes at least one memory that stores an availability state of a version of the service, a communication unit, and a processor. The communication unit is configured to receive a request to modify the availability state of the version of the service. The processor is coupled to the at least one memory and the communication unit, and is operable to: modify the availability state of the version of the service stored in the at least one memory in accordance

with the request, wherein the availability state is modified to: (i) unavailable in a case where the request includes an instruction to disable the version of the service, and (ii) available in a case where the request includes an instruction to enable the version of the service. The service is associated with a secure element profile.

[0007] In yet another embodiment, a method of managing the availability of a function comprising at least one receiving and modification step is described. A request to modify an availability state of a function is received. The availability state of the function is modified in accordance with the request. The availability state is modified to: (i) unavailable in a case where the request includes an instruction to disable the function, and (ii) available in a case where the request includes an instruction to enable the function. The function is associated with a secure element.

[0008] In still a further embodiment, a non-transitory computer readable storage medium having stored thereon instructions which, when executed by a system including at least one processor and at least one memory, cause the system to perform at least one receiving and modification step is described. A request to modify an availability state of a version of the service, the availability state of the service being stored in a memory, is received. The availability state of the version of the service stored in the memory is modified in accordance with the request. The availability state is modified to: (i) unavailable in a case where the request includes an instruction to disable the version of the service, and (ii) available in a case where the request includes an instruction to enable the version of the service. The service is associated with a secure element profile.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] The features and advantages of the present invention will become more apparent from the detailed description set forth below when taken in conjunction with the following drawings.

[0010] FIG. 1 is an overview of a mobile commerce system according to an example embodiment.

[0011] FIG. 2 is a sequence diagram of an installation operation according to an example embodiment.

[0012] FIG. 3 is a sequence diagram of an upgrade operation according to an example embodiment.

[0013] FIG. 4 is a flowchart illustrating the steps of modifying the availability state of a version of an application according to an example embodiment.

[0014] FIG. 5 is a flowchart illustrating the steps of modifying the availability state of a function according to an example embodiment.

[0015] FIG. 6 is a block diagram of a general or special purpose computer according to an example embodiment.

DETAILED DESCRIPTION

Mobile Commerce System

[0016] FIG. 1 is a diagram of an example mobile commerce system 100. The system allows service providers to efficiently communicate with mobile devices over a mobile network. As shown in FIG. 1, system 100 includes service provider trusted service managers ("SP TSM") 103-1, 103-2, …, 103-n (collectively "103").

Each of the SP TSMs 103 corresponds to a service provider 107-1, 107-2, …, 107-n (collectively "107"). A service provider 107 is an entity that provides one or more services to a user through one or more applications, applets, codes, or packages stored on the user's mobile device and/or secure element. Each SP TSM 103 serves as an intermediary between the service providers 107 and other entities including secure elements, MNOs, and another type of TSM (referred to herein as a "central TSM" 102), which may be managed, for example, by a mobile wallet provider.

[0017] Through a corresponding SP TSM 103, a service provider 107 can provide applications or instructions regarding those applications to the central TSM 102. As such, each of the SP TSMs 103 is communicatively coupled to the central TSM 102 via a communications network 105. Communications network 105 may be a virtual private network (VPN), a network using Transfer Control Protocol (TCP) / Internet Protocol (IP) standards *(e.g.,* Hypertext Transfer Protocol (HTTP) standards), or the like. Each of the SP TSMs 103 and the central TSM 102 may also secure these communications by using security protocols such as Secure Socket Layer (SSL), Transport Layer Security (TLS), or the like. Each of the SP TSMs 103 may also communicate with the central TSM 102 by using an application programming interface (API) such as a web service API.

[0018] In an exemplary embodiment, the central TSM 102 includes a processor 102a and a memory 102b. The central TSM 102 may be implemented via software stored on the memory 102b to serve as an intermediary between the SP TSMs 103 and the secure elements 106a-l, 106a-2, …, 106a-n (collectively "106a"). Secure elements 106a may be hardware and/or software implemented to store sensitive

information and/or code applets, applications and packages. Physically, the secure element may be implemented as a universal integrated circuit card, an embedded secure element, or a micro secure digital (micro SD) card. Alternatively, the secure element may be implemented as a secure storage communicatively connected to the mobile device. For example, such a secure element may be cloud-based, virtual or remote storage.

[0019] More specifically, the central TSM 102 provides each of the SP TSMs 103 with means to, for example, load, modify, install, or delete applications on the secure elements 106a. In addition, the SP TSMs 103, through the central TSM 102, can request pre-personalization of a secure element 106a or personalization of a payment service. That is, the central TSM 102 manages the communications between the SP TSMs 103 and the secure elements 106a.

[0020] To manage the communications between the SP TSMs 103 and the secure elements 106a, the central TSM 102 is constructed to communicate with a plurality of service providers 107 and SP TSMs 103, and with a plurality of secure elements 106a over a plurality of mobile networks 104-1, 104-2, …, 104-n (collectively "104"). In one embodiment, the central TSM 102 may include or be communicatively coupled to an enterprise service bus (ESB) 101. The ESB 101 is an architecture model for implementing the interactions and communications between entities *(e.g.,* secure elements 106a, SP TSMs 103, central TSM 102). In one example embodiment, the functions described herein that are performed by the central TSM 102 may be performed by an ESB *(e.g.,* ESB 101) or any system or device that is specifically programmed to perform such functions.

[0021] As noted above, the central TSM 102 is communicatively coupled to the secure elements 106a via corresponding mobile networks 104 used and/or managed by corresponding MNOs. Generally, the mobile networks 104 are used by MNOs to provide wireless communications services. The mobile networks 104 may be mobile phone cellular networks, radio networks, or the like. The central TSM 102 may communicate with the secure elements 106a, via the mobile networks 104, using security protocols such as Global Platform secure channel protocol, SSL, TLS, or the like.

[0022] The secure elements 106a are associated with corresponding mobile devices 106-1, 106-2, …, 106-n (collectively "106"), respectively. The secure elements 106a may be communicatively coupled to one or more processors and one or more memories, for example, of their respective mobile devices 106.

[0023] As discussed above, the secure elements 106a may include code, applets, applications, and packages. These items may be provided by service providers 107, mobile network operators, or a system administrator, and may be preloaded on the secure element 106a at the time of manufacture. Packages may include uninstantiated applets and/or applications, and may be loaded on the secure element 106a, for example, over-the-air (OTA). Applets and/or applications on the secure element 106a may also be in uninstantiated or instantiated form. Uninstantiated applets and/or applications may be loaded on the secure element 106a and later instantiated to create one or more instances of said applet and/or application. In addition, applets and/or applications may be loaded, for example, OTA after the secure element 106a has been manufactured *(e.g.,* after delivering the secure element 106a to a user).

[0024] Applets and applications may be generic or non-generic. Non-generic applets and applications correspond to a single service provider 107. For example, applets or applications corresponding to a single service provider's coupon or loyalty program are non-generic. Data used and/or associated with a non-generic applet or application *(e.g.,* offers, coupons) may be stored in the secure element 106a or in memory outside of the secure element 106a *(e.g.,* non-volatile memory of a mobile device 106).

[0025] Generic applets and applications can be used by multiple service providers 107. For example, a payment network application *(e.g.,* MasterCard®) may be instantiated for multiple service providers 107 by the central TSM 102, and therefore used by more than one service provider.

[0026] Exclusive ownership, control, and/or management of uninstantiated applets or applications allows a single entity to efficiently and cost effectively supervise the applets and/or applications. Further, exclusive ownership, control, and/or management increases security and minimizes the complexities caused by multiple service providers loading and controlling different applets and/or applications on a secure element 106a. For example, a service provider may utilize an instance of an uninstantiated applet and/or application instead of certifying and installing an independent applet or application on the secure element 106a.

[0027] An application, applet, package, or code, when executed by a processor causes the mobile device 106 to perform a corresponding service *(e.g.,* make a payment, receive a coupon, or receive an advertisement, etc.). An applet or application on a secure element 106a may function pursuant to requirements established by Global Platform, Europay, MasterCard®, Visa® (EMVCo.), MNOs,

and payment networks *(e.g.,* MasterCard®, Visa®, Discover®, American Express®). Applets or applications may be, for example, expresspay™, payWave™, PayPass™, Zip™, and the like.

Secure Element Profiles

[0028] Since mobile devices 106 operate on different mobile networks (104-1, 104-2, …, 104-n) and the secure elements 106a may have different hardware configurations, the central TSM 102 maintains a secure element profile that contains information regarding each of secure elements 106a. A secure element profile defines specific hardware and software features *(e.g.,* installed applets and applet versions) of a given secure element. One example of a secure element profile, including fields and descriptions of information of the secure element profile, is shown below. It should be understood that the following is simply an example, and that a secure element profile might contain more, fewer, or different fields.

FIELD	DESCRIPTION
SE Profile Name	Name of secure element profile *(e.g.,* UICC_01_P01001)
SE Profile Version	Version number of secure element profile
Applet A Version	Version of an applet named Applet A
Applet B Version	Version of another (different) Applet named Applet B
Applet C Version	Version of another (different) Applet named Applet C
Contactless Applet Version	Version of applet for contactless transactions *(e.g.,* contactless payment)
Payment Applet A Version	Version of applet for payment transactions
Payment Applet B Version	Version of another (different) applet for payment transactions named Payment

FIELD	DESCRIPTION
	Applet B
Payment Applet C Version	Version of another (different) applet for payment transactions named Payment Applet C
Secure Element Manufacturer	Identity of manufacturer of secure element
Secure Element Form Factor	*e.g.,* Universal Integrated Circuit Card, (UICC), embedded
Secure Element Pre-personalization	*e.g.,* an identity of a pre-set personalization of the secure element corresponding to the secure element manufacturer
Mobile Network Operator (MNO)	Carrier or mobile operator corresponding to a mobile device having a secure element
SE Part Number	Part number corresponding to the secure element *(e.g.,* the manufacturer's part number)
SE Manufacturer Version	Manufacturer version number corresponding to the secure element, *e.g.,* GP 2.2.1, UICC Configuration v1.0.1, Amendment A, Amendment B, and Amendment C (CGM not supported)
JavaCard version	Version number corresponding to the JavaCard, *e.g.,* JavaCard 2.2.2, parts of 3.0.1 for deselect, and Iso & Contactless interface management
Available volatile memory space limit	Total amount of volatile memory space available, *e.g.,* 13.5k/18k (total incl. OS 30k)
Available non-volatile memory space limit	Total amount of non-volatile memory space available, *e.g.,* 184k/256k
Volatile memory assigned at manufacture to trusted security domain	*e.g.,* volatile memory assigned at manufacturer to the trusted security domain for the system described herein
Non-volatile memory assigned at manufacture to trusted security domain	*e.g.,* non-volatile memory assigned at manufacturer to the trusted security domain for the system described herein
Platform Certificate Number (PCN)	e.g., PCN0012
PCN expiration date	*e.g.,* 14-Feb-2012

[0029] Other fields of the secure element profile may include, for example, OS version, GlobalPlatform version, extra capabilities of the secure element *(e.g.,* on-board key generation), loaded applications and their versions, etc.

[0030] A secure element profile may include or be associated with a secure element profile availability table, which details, among other things, the applets and/or applications (and their versions) that are compatible with each secure element 106a and/or secure element profile. As noted above, applications may be updated over time with newer versions. However, a newer version of an application may not be compatible with every type of secure element 106a, or even those secure elements 106a with which the previous version of the application was compatible. Such a change in compatibility may be caused by, for example, the newer version of the application requiring a different hardware configuration, and thus rendering it incompatible with older secure elements. Accordingly, the secure element profile availability table includes information on the compatible versions of each application for each secure element profile, as illustrated below in Table 1. It should be understood that a secure element table can be stored in and managed by a central TSM *(e.g.,* central TSM 102), ESB *(e.g.,* ESB 101) or the like.

Table 1

Secure Element Profile Name	**Appln. ID**	**Version(s)**			**Appln. ID**	**Version(s)**		
UICC_R1_MN01	101	1.0	1.1	-	102	1.0	1.1	1.2

UICC_R2_MN01	101	1.0	1.1	1.2	102	1.0	1.1	1.2
UICC_R1_MN02	101	1.0	1.1	-	102	1.0	1.1	1.2
UICC_R2_MN02	101	1.0	1.1	1.2	102	1.0	1.1	1.2
MSD_R1_MN01	101	1.0	1.1	-	102	1.0	1.1	1.2
MSD_R2_MN01	101	1.0	1.1	1.2	102	1.0	1.1	1.2
MSD_R1_MN02	101	1.0	1.1	-	102	1.0	1.1	1.2
MSD_R2_MN02	101	1.0	1.1	1.2	102	1.0	1.1	1.2

[0031] Table 1 is an exemplary secure element availability profile table, which includes fields for the secure element profile name, application ID corresponding to the application, and compatible version(s) of the application. In this example, each secure element profile name is based on the type of physical medium embodying the secure element 106a *(e.g.,* universal integrated circuit card (UICC), embedded secure element, or micro SD), the release version (Rl, R2), and the mobile network operator over which the mobile device 106 comprising the secure element 106a communicates (MNOl, MN02). The application ID field (Appln. ID) is a unique numerical value assigned to each application. The version field tracks all versions of the application corresponding to the application ID that are compatible with the secure element profile. For example, secure element profile "UICC_R1_MN01" is a profile of a first release secure element embodied in a universal integrated circuit card and to be used with mobile network operator 1. Version 1.0 and 1.1 of application 101 are compatible with UICC_RI_MNOI, but not version 1.2. In this example, version 1.2 is incompatible, for example, because

the first release (Rl) of the UICC lacks the necessary hardware. In contrast, UICC_R2_MN01, which is the second release (R2) of the UICC is compatible with version 1.2. For similar reasons, version 1.2 of application 101 is also incompatible with UCC_R1_MN02, MSD_R1_MN01 and MSD_R1_MN02. Of course, later versions of an application may be incompatible with a secure element profile for other reasons as well, such as the physical embodiment of the secure element 106a or the mobile network operator.

[0032] While multiple versions of an application may be compatible with a secure element 106a, not all versions of that application may necessarily be available at once. Rather, one or more of the compatible versions may be deemed to be available, while the other versions are unavailable. As such, the central TSM 102 is also constructed to store an availability state for each version of the application. Typically, the availability state of the latest version ***(e.g.,*** most recent or newer version) of an application is set to available. The availability state for each of the application versions shown in Table 1 is represented visually in Table 2 below.

Table 2

Secure Element Profile Name	**Appln. ID**	**Version(s)**			**Appln. ID**	**Version(s)**		
UICC_R1_MN01	101	1.0	***1.1***	-	102	1.0	1.1	***1.2***
UICC_R2_MN01	101	1.0	1.1	***1.2***	102	1.0	1.1	***1.2***
UICC_R1_MN02	101	1.0	***1.1***	-	102	1.0	1.1	***1.2***
UICC_R2_MN02	101	1.0	1.1	***1.2***	102	1.0	1.1	***1.2***
MSD_R1_MN01	101	1.0	***1.1***	-	102	1.0	1.1	***1.2***
MSD_R2_MN01	101	1.0	1.1	***1.2***	102	1.0	1.1	***1.2***

MSD_R1_MN02	101	1.0	***1.1***	-	102	1.0	1.1	***1.2***
MSD_R2_MN02	101	1.0	1.1	***1.2***	102	1.0	1.1	***1.2***

[0033] As shown in Table 2, versions of the application highlighted in bold and italics have availability states set to "available" while other versions of that application (which are not highlighted in bold) are set to unavailable.

[0034] Information on the availability states is especially useful when the secure element 106a is to be activated or personalized. The secure element 106a communicates with the central TSM 102 to determine whether the uninstantiated applications are the latest versions. This process is illustrated in FIG. 2.

[0035] As shown in FIG. 2, upon the central TSM 102 determining that installation of an application is to be performed, the central TSM 102 retrieves or identifies information regarding the version of the corresponding application loaded on the secure element 106a (S201). This may be done, for example, by analyzing the information in the secure element profile corresponding to the secure element 106a, which is maintained in and by the central TSM 102. The central TSM 102, in turn, compares the version information retrieved from the secure element profile corresponding to the secure element 106a with the information in the secure element profile availability table (S204). If the result of the comparison is that the latest compatible version of the application is loaded on the secure element 106a, the central TSM 102 sends an installation command to the secure element 106a to install the loaded version of the application. If, however, a newer version of the application is compatible and available, the newer version of the

application is sent to the secure element 106a via a corresponding mobile network 104 (S205). Upon receipt of either the installation command or the newer version of the application, the corresponding version of the application is installed on the secured element 106a (S206).

[0036] A similar process is performed when the central TSM 102 identifies or determines that a new version of an application is available for installation on secure elements, as illustrated in FIG. 3. First, the central TSM 102 updates the secure element profile availability table (Table 1) to show that a new compatible version of an application is available for one or more secure element profiles (S301). The availability state of the previous *(e.g.,* earlier) compatible version of the application is set to unavailable, and the availability state of the new version of the application is set to available. Next, an update query is received from the secure element 106a (via the mobile device 106) (S302). Typically, the mobile device 106 is configured to periodically check for updated applications. The update could be performed at a predetermined time or during a period where the mobile device 106 is not in use. Information about the versions of applications installed on the secure element 106a is stored and managed by the central TSM 102 (S302). The central TSM 102 then compares that version information to the available version for the corresponding secure element profile availability table (S303). Since the secure element profile availability table has been updated to reflect the availability of a new version of an application, particularly that the availability state of the new version of the application is set to available, the new version of the application is sent to the secure element 106a (S304) and installed (S305), in turn.

[0037] If the new version of the application is a critical update, then rather than waiting for the update query (S302) from the mobile device 106, the central TSM 102 can push the new application version to all the secure elements 106a corresponding to the secure element profile that includes the updated application.

Modifying the Availability State of a Version of an Application

[0038] As discussed above, with the release of a new version of an application, there is a risk that an unforeseen issue may arise that would impair the functionality of the application, or worse, cause the secure element 106a to become inoperative. As discussed below, however, by modifying the availability state of the malfunctioning version, the rollout of the malfunctioning version can be stopped quickly and efficiently.

[0039] FIG. 4 is a flowchart illustrating the steps of modifying the availability state of a version of an application. In step S401, the central TSM 102 receives a request to modify the availability state of a version of an application. The request includes a secure element profile name or identifier, application ID of an application, and a requested action *(e.g.,* whether the availability state is to be modified to available or unavailable). The request may also include the version ID *(e.g.,* version 1.0, 1.1, 1.2, etc.) of a specific version of the application whose availability state is to be modified. An exemplary request is illustrated below in Table 3.

Table 3

Secure Element Profile Name	Application ID	Version ID	Available/Unavailable

UICC_R2_MN01	101	1.2	Unavailable

[0040] The request may originate from a system administrator acting on the central TSM 102, for example, through a web portal, or may be received from a service provider 107 through one of the SP TSMs 103. Upon receipt of the request, the central TSM 102 determines whether or not the request includes the version ID of a specific version of the application whose availability state is to be modified. If the request does not identify a specific version of the application, then the availability state of the latest *(i.e.,* most recent) version of the application is modified in accordance with the request (S403). If the request does identify a specific version of the application, then the central TSM 102 determines whether or not an earlier version of the application is compatible with the secure element profile (S404). If no earlier version of the application is present, then the availability state of the identified version of the application is modified in accordance with the request (S405). If, however, it is determined that an earlier version of the application is compatible with the secure element profile in S404, and the request includes an instruction to modify the availability state of the identified version to unavailable, then such a modification is made (S407) and the availability state of the earlier version of the application is modified to available (S408).

[0041] In an alternative embodiment, even if the request does not include a version ID *(e.g.,* does not identify a specific version of the application), the central TSM 102 may refer to the secure element profile availability table to determine whether there is an earlier version of the application compatible with the secure

element profile. If so, the central TSM 102 may modify the availability state of that earlier version to available when the availability state of the latest version is modified to unavailable.

[0042] Assuming the secure element profile availability table shown in Table 2 is modified in accordance with the request shown in Table 3, the availability state of version 1.2 of the application corresponding to application ID 101 is set to unavailable for secure element profile UICC_R2_MNO 1. Moreover, because the request shown in Table 3 includes a version ID (version 1.2), the central TSM 102 determines that an earlier version of the application is compatible with the secure element profile (namely version 1.1), and will modify the availability state of the earlier compatible version to "available." After these operations are performed, the salient portion of the secure element profile availability tableshown in Table 3, will appear as shown in Table 4 below.

Table 4

Secure Element Profile Name	**Appln. ID**	**Version(s)**			**Appln. ID**	**Version(s)**		
UICC_R2_MNO1	101	1.0	**1.1**	1.2	102	1.0	1.1	**1.2**

[0043] In the case that the availability state of version 1.2 of the application corresponding to application ID 101 is set to unavailable, when the central TSM 102 compares information (in S204 and S303) from a secure element 106a regarding the version of the application corresponding to Appln. ID 101 to information in the secure element profile availability table, the central TSM 102 determines version 1.1 of the application to be the latest available version of the

application. By changing the availability state of version 1.2 to unavailable, the central TSM 102 may no longer provide or make availabile version 1.2 to the secure elements 106a, and the rollout of version 1.2 is stopped.

[0044] Through a similar process to the one described above, it also possible to make the latest version of an application, or a specific version of an application, available to the secure elements 106a. Such a process is useful when, for example, the error in the malfunctioning version of the application has been corrected.

[0045] Returning to FIG. 4, the central TSM 102 receives a request from a system administrator or from an SP TSM 103 to modify the availability state of a version of an application (S401). The central TSM 102 determines whether the request identifies a specific version of the application whose availability state is to be modified based on whether the request includes a version ID (S402). If the request does not include a version ID, then the availability state on the secure element profile availability table for the latest version of the application is modified in accordance with the request (S403). If the request includes a version ID and thus identifies a specific version of the application to modify, the central TSM 102 in turn determines whether there is an earlier compatible version (S404). If no earlier compatible version is identified, then the availability state of the identified version of the application is modified in accordance with the request (S405). If there is an earlier compatible version, but the request includes an instruction to modify the availability state of the identified version of the application to available *(i.e.,* NO in S409), the availability state of the identified version is modified to available (S410), and the availability state of the earlier version of the application is modified to unavailable (S41 1).

[0046] The central TSM 102 is also constructed to generate an error message that can be delivered to a system managed by a system administrator, for example, in the case where the availability state of the version to be modified is equal to unavailable and the request includes an instruction to disable the version of the service. Likewise, the central TSM 102 is constructed to generate an error message when the availability state of the version to be modified is equal to available and the request includes an instruction to enable the version of the service. That is, an error message can be sent by a central TSM 102, for example, when a request includes instructions to modify an availability state to a state in which an application is already in.

Managing the Availability of Functions

[0047] As described above, the central TSM 102 can modify the availability state of versions of applications stored on the secure element 106a. The central TSM 102, however, also is constructed to modify the availability state of a function. A function is a representation of executable code that when executed by the central TSM 102 causes one or more processes to be performed. Functions may be manifested as application program interfaces (APIs) that are exposed to some or all of the service providers 107, mobile network operators, and other systems managed by system administrators. Table 5 is an exemplary list of such functions and their description.

Table 5

Function Name	Function	Description	Availability

	ID		State
LOCK APPLICATION	0001	Prevents use of an application on a secure element	Available
UNLOCK APPLICATION	0002	Allows use of a locked application on a secure element	Available
INSTALL APPLICATION	0003	Installs an application on a secure element	Available
REMOVE APPLICATION	0004	Removes an installed application from a secure element	Available
RENEW APPLICATION	0005	Renews an expired application on a secure element	Available
CHECK ELIGIBILITY	0006	Checks whether a user is eligible to use an application to be installed on the secure element	Available
INSTALL MOBILE WALLET	0007	Installs the mobile wallet on the mobile device	Available
INSTALL WALLET WITH PERSONALIZATION	0008	Installs the mobile wallet and executes a personalization routine	Available
PERSONALIZE WALLET	0009	Personalizes the mobile wallet	Available
WALLET UPGRADE	0010	Upgrades the version of the mobile wallet on the mobile device	Available
UPGRADE WITH	001 1	Upgrades the version of	Available

WALLET PERSONALIZATION		the mobile wallet on the mobile device and executes a personalization routine.	
UPDATE WALLET PASSCODE	0012	Updates the passcode for accessing the mobile wallet	Available
UPDATE WALLET HANDSET ID	0013	Updates the handset identifier (ID) of the mobile device stored in the secure element.	Available
UPDATE WALLET WIDGET	0014	Updates the wallet widget stored in the secure element	Available
UPDATE WALLET ICC ID	0015	Updates the ICC ID stored in the secure element.	Available
ACTIVATE WALLET	0016	Activates the mobile wallet	Available
SEND SCRIPT	0017	Sends personalization data to the secure element	Available
REDO INSTALLATION	0018	Reinstalls an application in a case where personalization failed	Available
LOCK AFTER PERSONALIZATION	0019	Locks an application on the secure element after personalization	Available
SUSPEND WALLET	0020	Informs the central TSM that a user's mobile wallet has been suspended	Available
TERMINATE WALLET	0021	Informs the central TSM	Available

		that a user has terminated his/her mobile wallet	
REACTIVATE WALLET	0022	Informs the central TSM that a user has reactivated his/her mobile wallet	Available

[0048] A system may disable, for example, any of the above-referenced functions through or with the assistance of the central TSM 102. In some instances, some functions may not be disabled, such as suspend wallet, terminate wallet, and reactivate wallet functions. As shown in FIG. 5, when the central TSM 102 receives a request to modify the availability state of one or more functions (S501), the central TSM 102 first determines which function(s) is/are identified in the request (S502). Next, the central TSM 102 identifies the requested modification, *i.e.*, whether the availability state is to be modified to available or unavailable (S503). The central TSM 102 in turn confirms that the requested modification is permissible for the identified function (S504). If so, then the availability state of the identified function is modified in accordance with the request (S505). If not, an error message is returned (S506). Thus, for example, if the request sought to modify the availability of the suspend wallet, terminate wallet, or reactivate wallet functions to unavailable, an error message would be generated.

[0049] By disabling one or more functions, a system administrator can stop the rollout of a malfunctioning version of an application. For example, by disabling the INSTALL MOBILE WALLET, PERSONALIZE WALLET, INSTALL WALLET WITH PERSONALIZATION, WALLET UPGRADE, or UPGRADE WITH WALLET PERSONALIZATION functions, installation and upgrade functions are

disabled, thus preventing a newer version of any application from being disseminated to the mobile devices 106.

[0050] As discussed above, by modifying the availability states of versions of applications and functions, the distribution of one or more applications to the secure elements 106a can be quickly and efficiently stopped.

Example Computer-Readable Medium Implementation

[0051] FIG. 6 is a block diagram of a general and/or special purpose computer 600, which may be a general and/or special purpose computing device, in accordance with some of the example embodiments of the invention. The computer 600 may be, for example, a user device, a user computer, a client computer and/or a server computer, among other things.

[0052] The computer 600 may include without limitation a processor device 610, a main memory 625, and an interconnect bus 605. The processor device 610 may include without limitation a single microprocessor, or may include a plurality of microprocessors for configuring the computer 600 as a multi-processor system. The main memory 625 stores, among other things, instructions and/or data for execution by the processor device 610. The main memory 625 may include banks of dynamic random access memory (DRAM), as well as cache memory.

[0053] The computer 600 may further include a mass storage device 630, peripheral device(s) 640, portable non-transitory storage medium device(s) 650, input control device(s) 680, a graphics subsystem 660, and/or an output display interface 670. For explanatory purposes, all components in the computer 600 are shown in FIG. 6 as being coupled via the bus 605. However, the computer 600 is not so limited. Devices of the computer 600 may be coupled via one or more data

transport means. For example, the processor device 610 and/or the main memory 625 may be coupled via a local microprocessor bus. The mass storage device 630, peripheral device(s) 640, portable storage medium device(s) 650, and/or graphics subsystem 660 may be coupled via one or more input/output (I/O) buses. The mass storage device 630 may be a nonvolatile storage device for storing data and/or instructions for use by the processor device 610. The mass storage device 630 may be implemented, for example, with a magnetic disk drive or an optical disk drive. In a software embodiment, the mass storage device 630 is configured for loading contents of the mass storage device 630 into the main memory 625.

[0054] The portable storage medium device 650 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 600. In some embodiments, the software for storing information may be stored on a portable storage medium, and may be inputted into the computer 600 via the portable storage medium device 650. The peripheral device(s) 640 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 600. For example, the peripheral device(s) 640 may include a network interface card for interfacing the computer 600 with a network 620.

[0055] The input control device(s) 680 provide a portion of the user interface for a user of the computer 600. The input control device(s) 680 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 handheld controller or mouse, a trackball, a stylus,

and/or cursor direction keys. In order to display textual and graphical information, the computer 600 may include the graphics subsystem 660 and the output display 670. The output display 670 may include a cathode ray tube (CRT) display and/or a liquid crystal display (LCD). The graphics subsystem 660 receives textual and graphical information, and processes the information for output to the output display 670.

[0056] Each component of the computer 600 may represent a broad category of a computer component of a general and/or special purpose computer. Components of the computer 600 are not limited to the specific implementations provided here.

[0057] Software embodiments of the example embodiments presented herein may be provided as a computer program product, or software, that may include an article of manufacture on a machine accessible or machine readable medium having instructions. The instructions on the non-transitory machine accessible machine readable or computer-readable medium may be used to program a computer system or other electronic device. The machine or computer-readable medium may include, but is not limited to, floppy diskettes, optical disks, CD-ROMs, and magneto-optical disks or other type of media/machine-readable medium suitable for storing or transmitting electronic instructions. The techniques described herein are not limited to any particular software configuration. They may find applicability in any computing or processing environment. The terms "computer-readable", "machine accessible medium" or "machine readable medium" used herein shall include any medium that is capable of storing, encoding, or transmitting a sequence of instructions for execution by the machine and that cause the machine to perform any one of the methods described herein.

Furthermore, it is common in the art to speak of software, in one form or another *(e.g.,* program, procedure, process, application, module, unit, logic, and so on) as taking an action or causing a result. Such expressions are merely a shorthand way of stating that the execution of the software by a processing system causes the processor to perform an action to produce a result.

[0058] 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.

[0059] 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.

[0060] 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 or 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.

[0061] 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 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.

[0062] 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.

[0063] 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 disclosure 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.

[0064] 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.

[0065] 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.

WHAT IS CLAIMED IS:

1. A method of managing the availability of a service, comprising the steps of:

receiving a request to modify an availability state of a version of the service, the availability state of the service being stored in a memory; and

modifying the availability state of the version of the service stored in the memory in accordance with the request,

wherein the availability state is modified to: (i) unavailable in a case where the request includes an instruction to disable the version of the service, and (ii) available in a case where the request includes an instruction to enable the version of the service,

wherein the service is associated with a secure element profile.

2. The method according to claim 1, wherein if the request includes a version identifier identifying a version of the service, then an availability state of the version of the service stored in the memory is modified in accordance with the request.

3. The method according to claim 1, wherein if the request does not include a version identifier identifying a version of the service, then an availability state of a latest version of the service stored in the memory is modified in accordance with the request.

4. The method according to claim 2, further comprising:

determining whether an earlier version of the service is compatible with the secure element profile; and

modifying an availability state of the earlier version of the service to available, in a case where (i) the request includes the instruction to disable the version of the service and (ii) the earlier version of the service is compatible with the secure element profile.

5. The method according to claim 1, wherein the service is an application stored on a secure element.

6. The method according to claim 1, further comprising:

generating an error message in a case where a current availability state of the version of the service is: (i) equal to unavailable and the request includes the instruction to disable the version of the service, or (ii) equal to available and the request includes the instruction to enable the version of the service.

7. A data processing system for managing the availability of a service, comprising:

at least one memory that stores an availability state of a version of the service;

a communication unit configured to receive a request to modify the availability state of the version of the service stored in the at least one memory; and

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

modify the availability state of the version of the service stored in the at least one memory in accordance with the request,

wherein the availability state is modified to: (i) unavailable in a case where the request includes an instruction to disable the version of the service, and (ii) available in a case where the request includes an instruction to enable the version of the service,

wherein the service is associated with a secure element profile.

8. The system according to claim 7, wherein if the request includes a version identifier identifying a version of the service, then the processor is further operable to modify an availability state of the version of the service stored in the at least one memory.

9. The system according to claim 7, wherein if the request does not include a version identifier identifying a version of the service, then an availability state of a latest version of the service stored in the at least one memory is modified in accordance with the request.

10. The system according to claim 8, wherein the processor is further operable to determine whether an earlier version of the service is compatible with the secure element profile, and to modify an availability state of the earlier version of the service stored in the at least one memory to available, in a case where (i) the request includes the instruction to disable the version of the service and (ii) the earlier version of the service is determined to be compatible with the secure element profile.

11. The system according to claim 7, wherein the service is an application stored on a secure element.

12. The system according to claim 7, wherein the processor is operable to generate an error message in a case where a current availability state of the version of the service is: (i) equal to unavailable and the request includes the instruction to disable the version of the service, and (ii) equal to available and the request includes the instruction to enable the version of the service.

13. A method of managing the availability of a function, comprising the steps of:

receiving a request to modify an availability state of a function; and

modifying the availability state of the function in accordance with the request,

wherein the availability state is modified to: (i) unavailable in a case where the request includes an instruction to disable the function, and (ii) available in a case where the request includes an instruction to enable the function,

wherein the function is associated with a secure element.

14. The method according to claim 13, wherein the request includes a plurality of instructions respectively corresponding to a plurality of functions, and availability states of the plurality of functions are set in accordance with the plurality of instructions.

15. The method according to claim 13, wherein setting the availability state of the function in accordance with the request alters the availability of a version of a service installed on the secure element.

16. The method according to claim 14, wherein setting the availability states of the plurality of functions in accordance with the plurality of instructions included in the request, alters the availability of a version of a service installed on the secure element.

17. The method according to claim 13, further comprising:

generating an error message if the request includes an instruction to disable a suspend wallet function, a terminate wallet function, or a reactivate wallet function.

18. A non-transitory computer readable storage medium having stored thereon instructions which, when executed by a system including at least one processor and at least one memory, cause the system to perform the steps of:

receiving a request to modify an availability state of a version of the service, the availability state of the service being stored in a memory; and

modifying the availability state of the version of the service stored in the memory in accordance with the request,

wherein the availability state is modified to: (i) unavailable in a case where the request includes an instruction to disable the version of the service, and (ii) available in a case where the request includes an instruction to enable the version of the service,

wherein the service is associated with a secure element profile.

19. The computer readable medium according to claim 18, wherein if the request includes a version identifier identifying a version of the service, then an availability state of the version of the service stored in the memory is modified in accordance with the request.

20. The computer readable medium according to claim 18, wherein if the request does not include a version identifier identifying a version of the service, then an availability state of a latest version of the service stored in the memory is modified in accordance with the request.

21. The computer readable medium according to claim 19, wherein the instructions further cause the system to perform the steps of:

determining whether an earlier version of the service exists for the secure element profile; and

modifying an availability state of the earlier version of the service to available, in a case where (i) the request includes the instruction to disable the version of the service and (ii) the earlier version of the service is compatible with the secure element profile.

22. The computer readable medium according to claim 18, wherein the service is an application stored on a secure element.

23. The computer readable medium according to claim 18, wherein the instructions further cause the system to perform the step of:

generating an error message in a case where a current availability state of the version of the service is: (i) equal to unavailable and the request includes the instruction to disable the version of the service, or (ii) equal to available and the request includes the instruction to enable the version of the service.

24. The method according to claim 1, further comprising a step of transmitting an installation request to a secure element, wherein the installation request includes

at least instructions to install the version of the service having an availability state equal to available.

25. The system according to claim 7, wherein the processor is further operable to transmit an installation request to a secure element, wherein the installation request includes at least instructions to install the version of the service having an availability state equal to available.

26. The computer readable medium according to claim 18, wherein the instructions further cause the system to transmit an installation request to a secure element, wherein the installation request includes at least instructions to install the version of the service having an availability state equal to available.

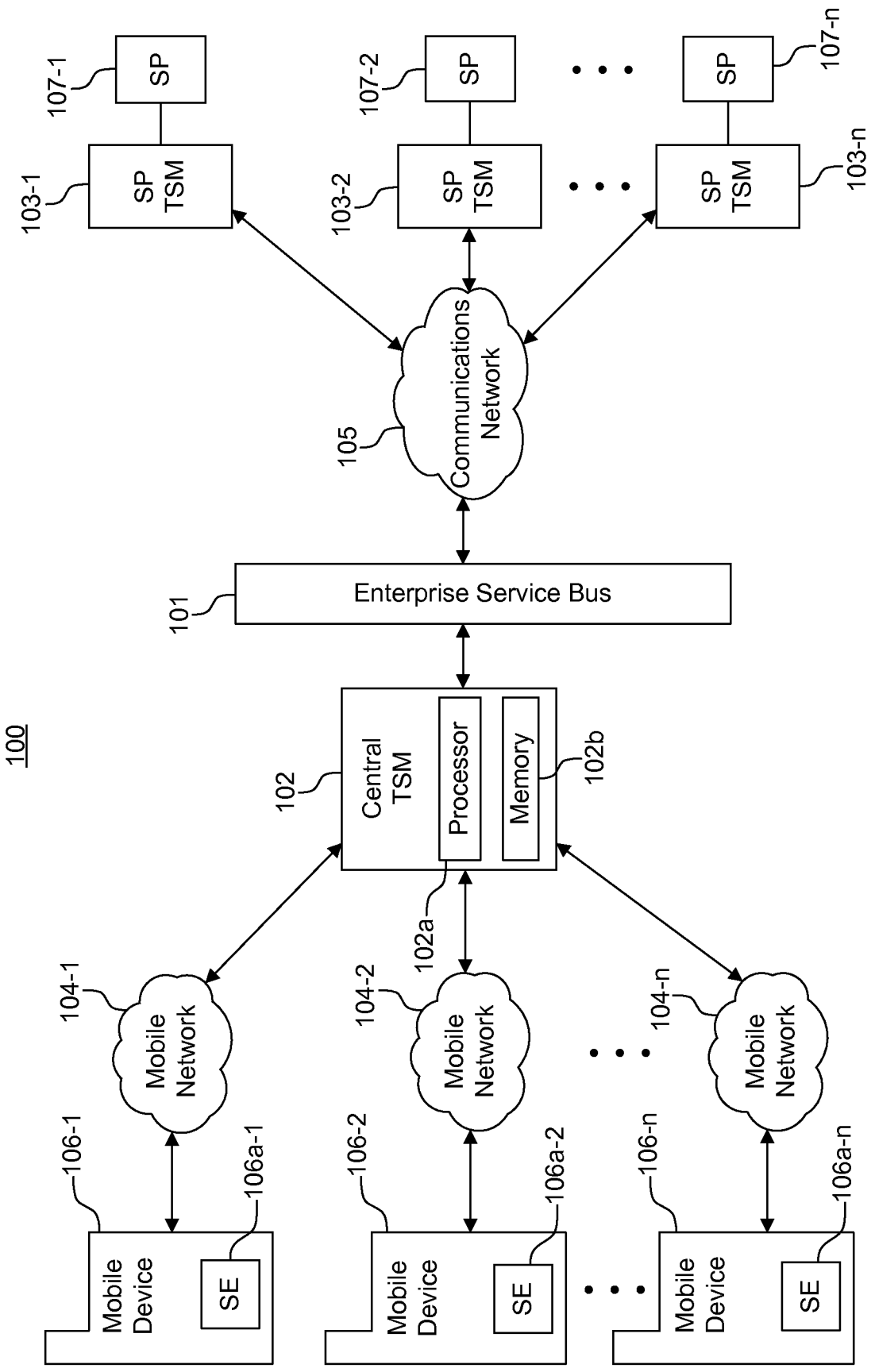
100
Mobile Device
SE
106-1
106a-1
Mobile Network
104-1
Mobile Device
SE
106-2
106a-2
Mobile Network
104-2
Mobile Device
SE
106-n
106a-n
Mobile Network
104-n
102a
Central TSM
Processor
Memory
102
102b
Enterprise Service Bus
101
Communications Network
105
SP TSM
103-1
SP
107-1
SP TSM
103-2
SP
107-2
SP TSM
103-n
SP
107-n

FIG. 1

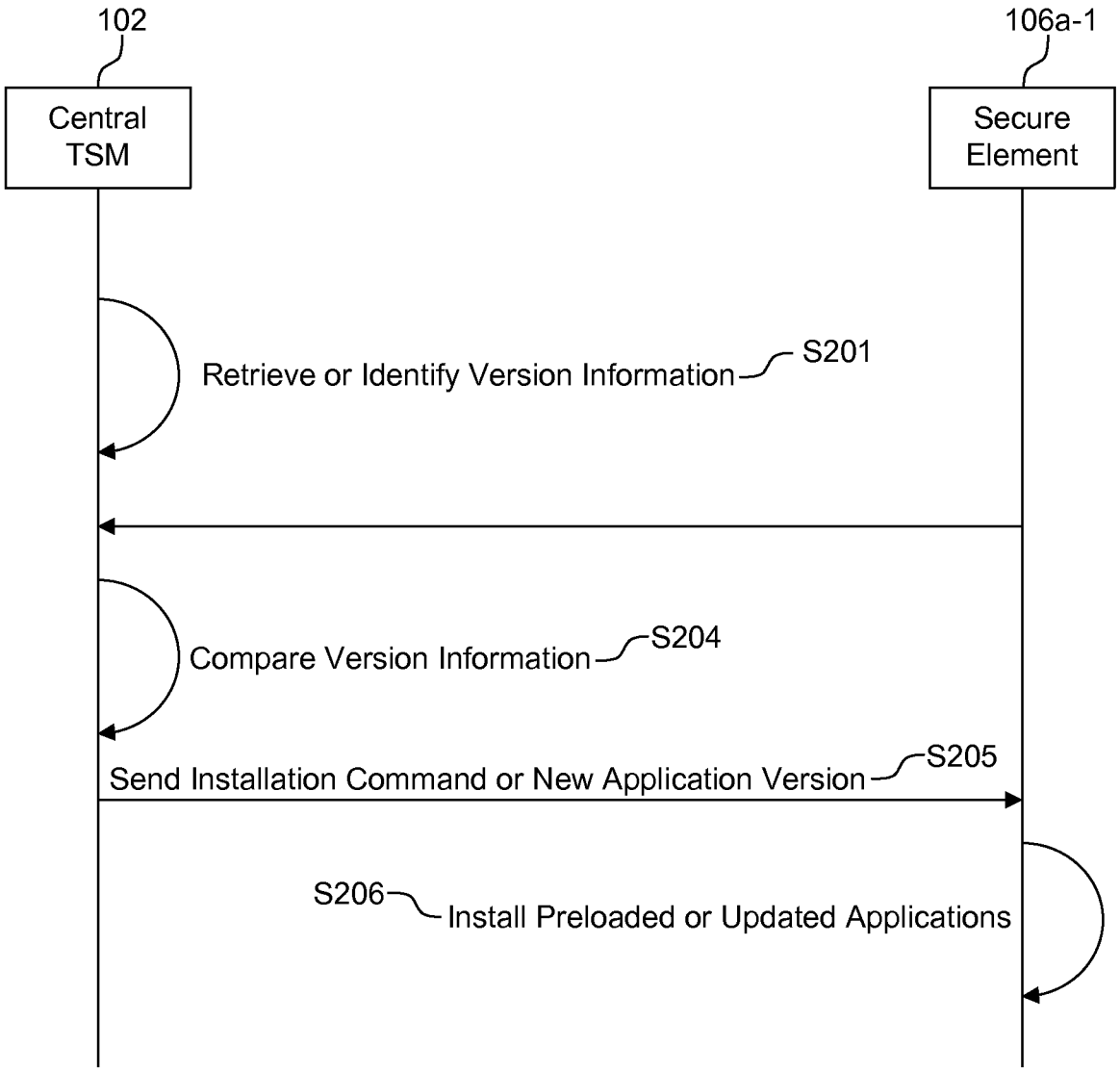
102
106a-1
Central TSM
Secure Element
Retrieve or Identify Version Information
S201
Compare Version Information
S204
Send Installation Command or New Application Version
S205
S206
Install Preloaded or Updated Applications

FIG. 2

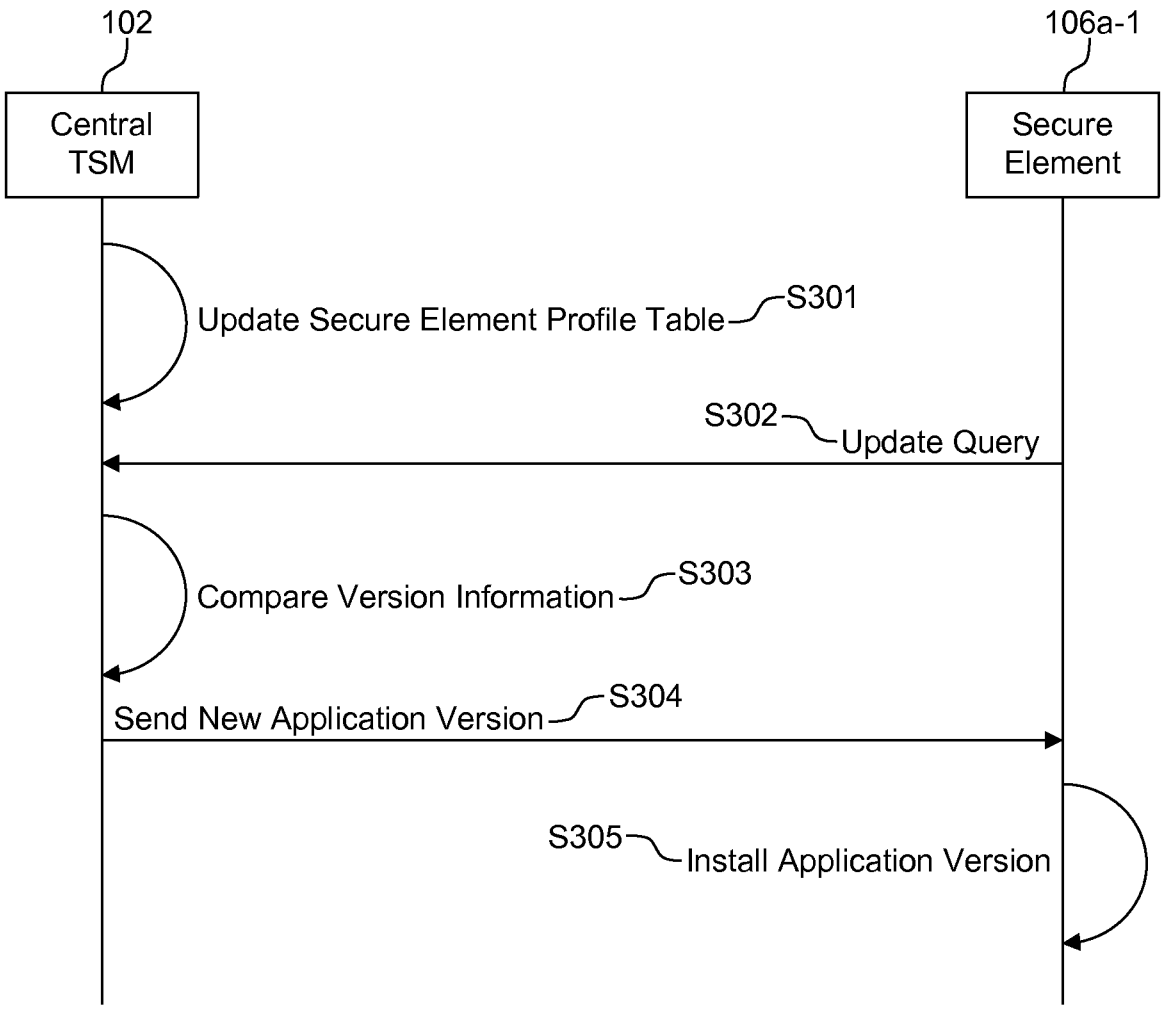
102
106a-1
Central TSM
Secure Element
Update Secure Element Profile Table
S301
S302
Update Query
Compare Version Information
S303
Send New Application Version
S304
S305
Install Application Version

FIG. 3

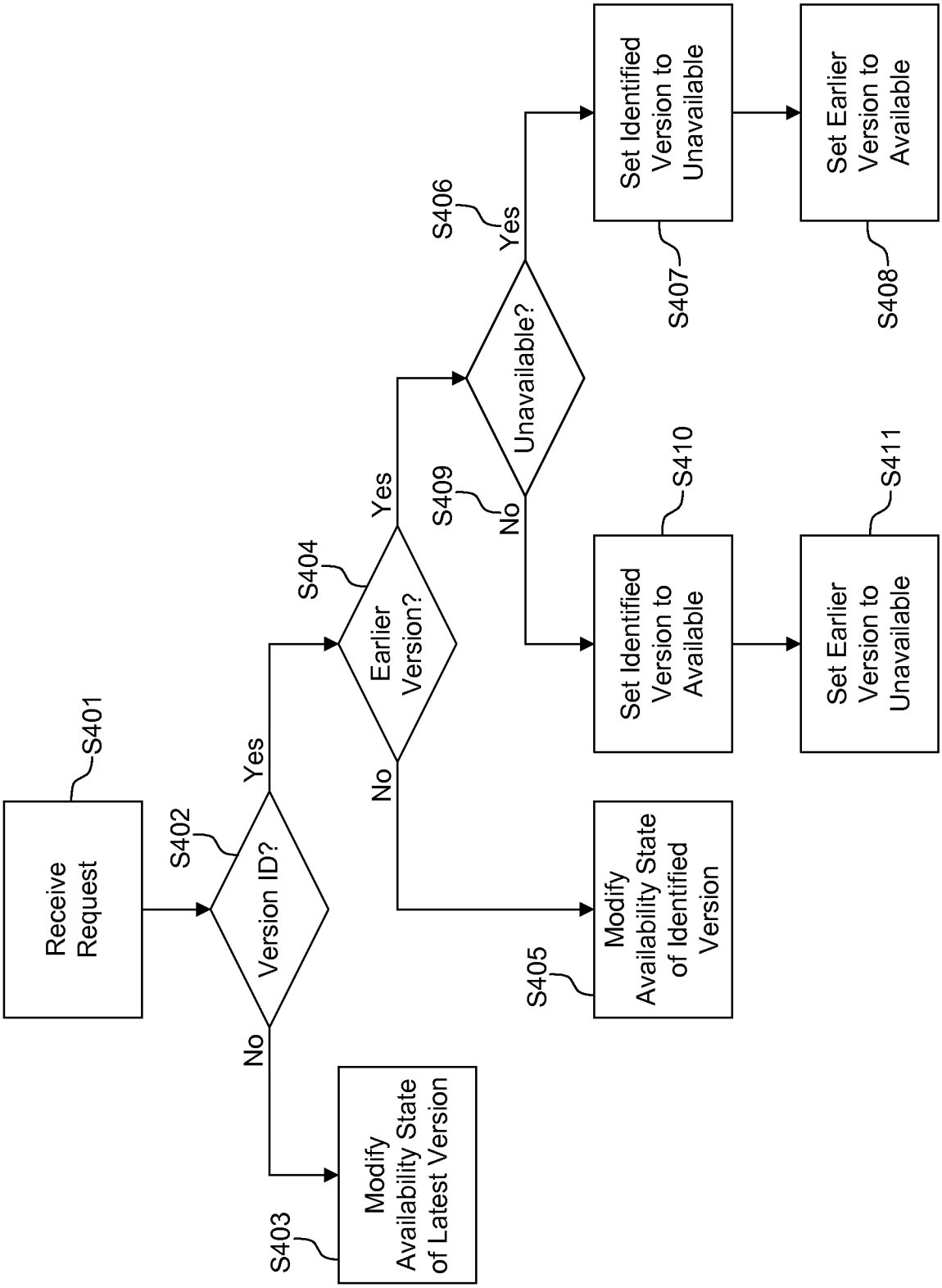
Receive Request
S401
Version ID?
S402
Yes
No
Modify Availability State of Latest Version
S403
Earlier Version?
S404
Yes
No
Modify Availability State of Identified Version
S405
Unavailable?
S406
Yes
No
Set Identified Version to Unavailable
S407
Set Earlier Version to Available
S408
S409
Set Identified Version to Available
S410
Set Earlier Version to Unavailable
S411

FIG. 4

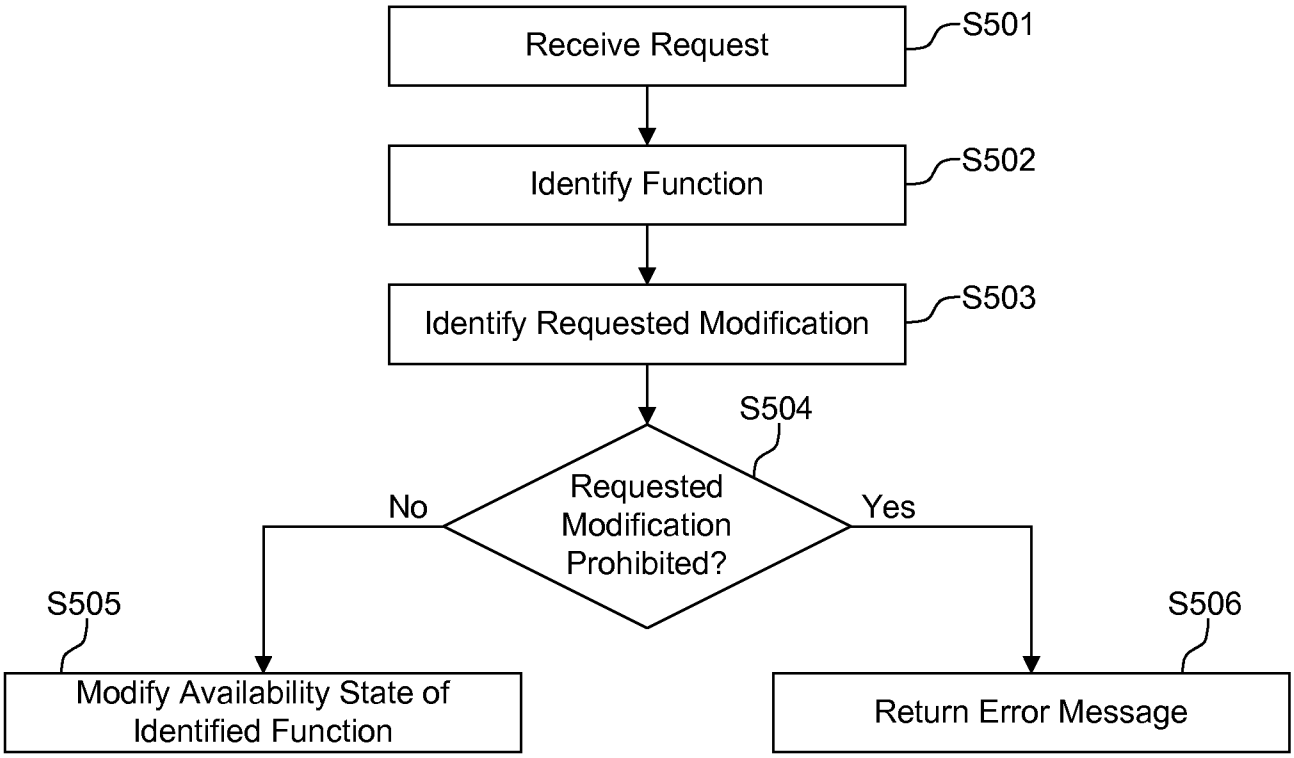
Receive Request
S501
Identify Function
S502
Identify Requested Modification
S503
S504
Requested Modification Prohibited?
No
Yes
S505
Modify Availability State of Identified Function
S506
Return Error Message

FIG. 5

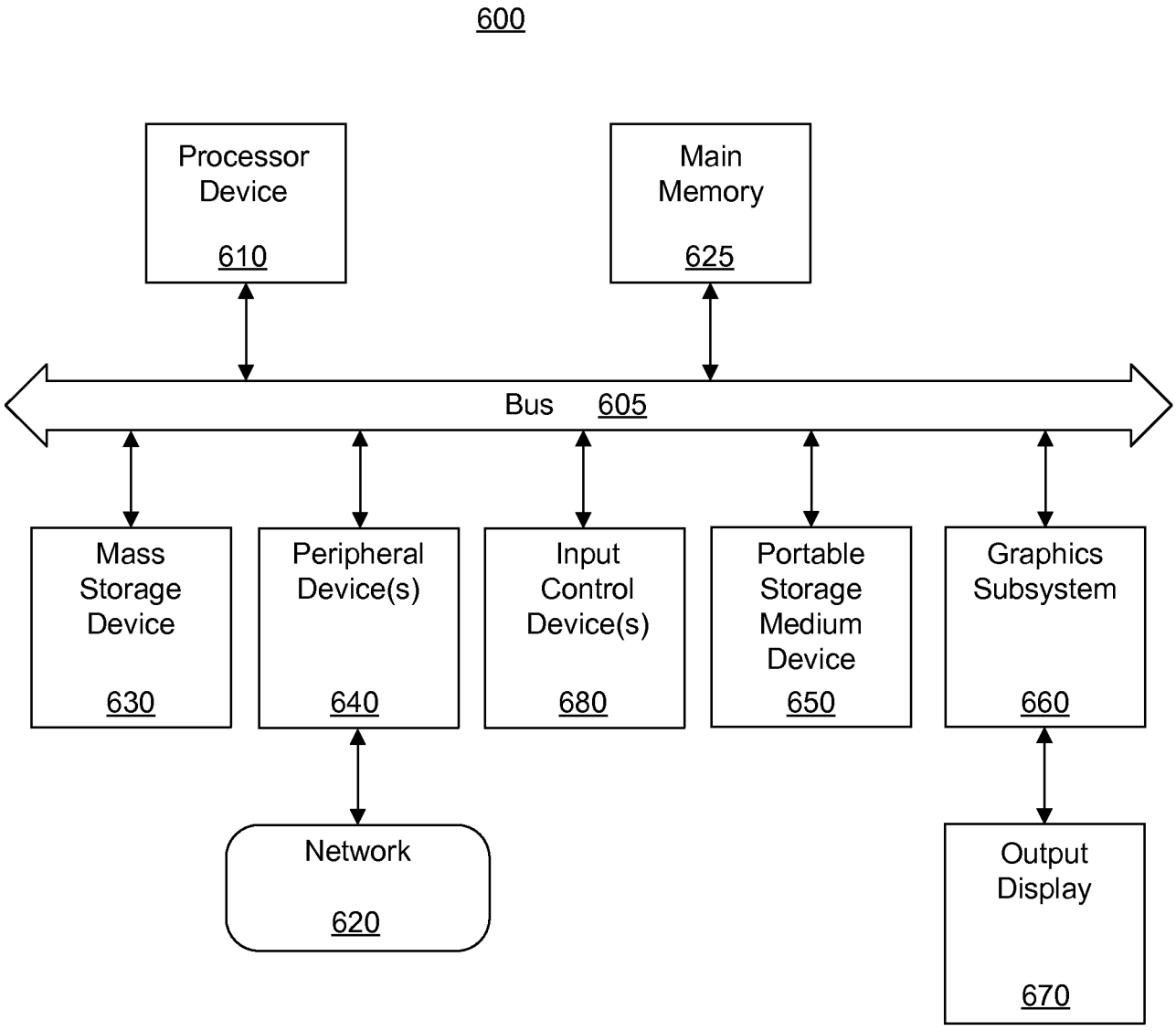
600
Processor Device 610
Main Memory 625
Bus 605
Mass Storage Device 630
Peripheral Device(s) 640
Input Control Device(s) 680
Portable Storage Medium Device 650
Graphics Subsystem 660
Network 620
Output Display 670

FIG. 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2014/038080

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/00(2009.01)i, H04W 88/18(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 12/00; G06F 15/16; G06F 15/173; H04M 3/42; H04L 12/28; G06F 3/12; H04W 88/18

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: version, service, state, manag*

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2010-0198939 Al (GREGORY G.RALEIGH) 05 August 2010 See abstract, figures 3-5 and claims 1-32.	1-26
A	US 2006-0119884 Al (YOUNG-WOO CHOI) 08 June 2006 See abstract, figures 2,4 and claims 1-37.	1-26
A	US 2010-0246597 Al (XIAO JUN MA et al.) 30 September 2010 See abstract, figure 5 and claims 1-8.	1-26
A	US 2004-0203684 Al (JUKKA JOKINEN et al.) 14 October 2004 See abstract, figures 2,5 and claims 1-22.	1-26

☐ 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	Date of mailing of the international search report
24 September 2014 (24.09.2014)	**24 September 2014 (24.09.2014)**

Name and mailing address of the ISA/KR
International Application Division
Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701, Republic of Korea
Facsimile No. +82-42-472-7140

Authorized officer
YOO, Sun Jung
Telephone No. +82-42-481-5775

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2014/038080

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2010-0198939 Al	05/08/2010	AU 2010-208183 Al	05/08/2010
		AU 2010-208294 Al	05/08/2010
		AU 2010-208296 Al	05/08/2010
		AU 2010-208297 Al	05/08/2010
		AU 2010-208314 Al	05/08/2010
		AU 2010-208316 Al	05/08/2010
		AU 2010-208317 Al	05/08/2010
		AU 2010-208483 Al	05/08/2010
		AU 2010-208484 Al	05/08/2010
		AU 2010-208485 Al	05/08/2010
		AU 2010-208486 Al	05/08/2010
		AU 2010-208488 Al	05/08/2010
		AU 2010-208489 Al	05/08/2010
		AU 2010-208543 Al	05/08/2010
		AU 2010-208544 Al	05/08/2010
		AU 2010-208545 Al	05/08/2010
		AU 2010-208546 Al	05/08/2010
		AU 2010-208547 Al	05/08/2010
		AU 2010-208551 Al	05/08/2010
		AU 2010-208552 Al	05/08/2010
		AU 2010-208553 Al	05/08/2010
		AU 2010-208554 Al	05/08/2010
		AU 2010-208556 Al	05/08/2010
		AU 2010-208557 Al	05/08/2010
		AU 2010-208558 Al	05/08/2010
		AU 2010-208565 Al	05/08/2010
		CA 2764888 Al	29/12/2010
		CA 2786746 Al	05/08/2010
		CA 2786749 Al	05/08/2010
		CA 2786752 Al	05/08/2010
		CA 2786815 Al	05/08/2010
		CA 2786825 Al	05/08/2010
		CA 2786828 Al	05/08/2010
		CA 2786830 Al	05/08/2010
		CA 2786832 Al	05/08/2010
		CA 2786864 Al	05/08/2010
		CA 2786865 Al	05/08/2010
		CA 2786868 Al	05/08/2010
		CA 2786870 Al	05/08/2010
		CA 2786873 Al	05/08/2010
		CA 2786875 Al	05/08/2010
		CA 2786876 Al	05/08/2010
		CA 2786878 Al	05/08/2010
		CA 2786881 Al	05/08/2010
		CA 2786884 Al	05/08/2010
		CA 2786886 Al	05/08/2010
		CA 2786887 Al	05/08/2010
		CA 2786892 Al	05/08/2010
		CA 2786893 Al	05/08/2010

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2014/038080

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
		CA 2786894 A1	05/08/2010
		CA 2786899 A1	05/08/2010
		CA 2787061 A1	05/08/2010
		CA 2787066 A1	05/08/2010
		CA 2810066 A1	15/03/2012
		CA 2811230 A1	29/03/2012
		CA 2811577 A1	29/03/2012
		CA 2813026 A1	19/04/2012
		CA 2813071 A1	12/04/2012
		CA 2813073 A1	12/04/2012
		CA 2813321 A1	12/04/2012
		CA 2819634 A1	07/06/2012
		CA 2819643 A1	07/06/2012
		CA 2825441 A1	02/08/2012
		CA 2832186 A1	11/10/2012
		CA 2832437 A1	11/10/2012
		CN 102342052 A	01/02/2012
		CN 102349065 A	08/02/2012
		CN 102356581 A	15/02/2012
		CN 102356596 A	15/02/2012
		CN 102362479 A	22/02/2012
		CN 102362539 A	22/02/2012
		CN 102365554 A	29/02/2012
		CN 102365620 A	29/02/2012
		CN 102365623 A	29/02/2012
		CN 102365623 B	20/03/2013
		CN 102365630 A	29/02/2012
		CN 102365631 A	29/02/2012
		CN 102365632 A	29/02/2012
		CN 102365633 A	29/02/2012
		CN 102365642 A	29/02/2012
		CN 102365643 A	29/02/2012
		CN 102365840 A	29/02/2012
		CN 102365842 A	29/02/2012
		CN 102365847 A	29/02/2012
		CN 102365853 A	29/02/2012
		CN 102365855 A	29/02/2012
		CN 102365858 A	29/02/2012
		CN 102365876 A	29/02/2012
		CN 102365877 A	29/02/2012
		CN 102365878 A	29/02/2012
		CN 102365890 A	29/02/2012
		CN 102365890 B	18/06/2014
		CN 102483730 A	30/05/2012
		CN 102802916 A	28/11/2012
		CN 103201730 A	10/07/2013
		CN 103202007 A	10/07/2013
		CN 103221941 A	24/07/2013
		CN 103221943 A	24/07/2013
		CN 103250401 A	14/08/2013

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2014/038080

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
		CN 103329119 A	25/09/2013
		EP 2391940 Al	07/12/2011
		EP 2391942 Al	07/12/2011
		EP 2391947 Al	07/12/2011
		EP 2391948 Al	07/12/2011
		EP 2391949 Al	07/12/2011
		EP 2391950 Al	07/12/2011
		EP 2391951 Al	07/12/2011
		EP 2391952 Al	07/12/2011
		EP 2391965 Al	07/12/2011
		EP 2391966 Al	07/12/2011
		EP 2391977 Al	07/12/2011
		EP 2392088 Al	07/12/2011
		EP 2392090 Al	07/12/2011
		EP 2392094 Al	07/12/2011
		EP 2392102 Al	07/12/2011
		EP 2392109 Al	07/12/2011
		EP 2392121 Al	07/12/2011
		EP 2392124 Al	07/12/2011
		EP 2392126 Al	07/12/2011
		EP 2392129 Al	07/12/2011
		EP 2392153 Al	07/12/2011
		EP 2392154 Al	07/12/2011
		EP 2392155 Al	07/12/2011
		EP 2392170 Al	07/12/2011
		EP 2392182 Al	07/12/2011
		EP 2394181 Al	14/12/2011
		EP 2445698 A2	02/05/2012
		EP 2445698 Bl	24/04/2013
		EP 2577332 Al	10/04/2013
		EP 2577333 Al	10/04/2013
		EP 2614446 Al	17/07/2013
		EP 2619684 Al	31/07/2013
		EP 2619970 Al	31/07/2013
		EP 2622503 Al	07/08/2013
		EP 2622506 Al	07/08/2013
		EP 2622835 Al	07/08/2013
		EP 2625626 A2	14/08/2013
		EP 2646903 Al	09/10/2013
		EP 2646930 Al	09/10/2013
		EP 2668584 A2	04/12/2013
		JP 2012-530625A	06/12/2012
		JP 2013-530640A	25/07/2013
		JP 2013-53408 1A	29/08/2013
		JP 2013-541278A	07/11/2013
		JP 2013-543676A	05/12/2013
		JP 2013-545323A	19/12/2013
		JP 2013-546212A	26/12/2013
		JP 2014-500989A	16/01/2014
		JP 2014-502066A	23/01/2014

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2014/038080

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
		JP 2014-502383A	30/01/2014
		KR 10-2011-0108416 A	05/10/2011
		KR 10-2011-0110360 A	06/10/2011
		KR 10-2011-0110829 A	07/10/2011
		KR 10-2011-0110830 A	07/10/2011
		KR 10-2011-0110831 A	07/10/2011
		KR 10-2011-0110832 A	07/10/2011
		KR 10-2011-0110833 A	07/10/2011
		KR 10-2011-0110834 A	07/10/2011
		KR 10-2011-0110835 A	07/10/2011
		KR 10-2011-0110836 A	07/10/2011
		KR 10-2011-0110837 A	07/10/2011
		KR 10-2011-0110838 A	07/10/2011
		KR 10-2011-0110839 A	07/10/2011
		KR 10-2011-0113192 A	14/10/2011
		KR 10-2011-0113640 A	17/10/2011
		KR 10-2011-0116189 A	25/10/2011
		KR 10-2011-0116190 A	25/10/2011
		KR 10-2011-0116191 A	25/10/2011
		KR 10-2011-0116192 A	25/10/2011
		KR 10-2011-0117200 A	26/10/2011
		KR 10-2011-0119763 A	02/11/2011
		KR 10-2011-0124258 A	16/11/2011
		KR 10-2011-0124259 A	16/11/2011
		KR 10-2011-0124260 A	16/11/2011
		KR 10-2011-0124261 A	16/11/2011
		KR 10-2011-0126638 A	23/11/2011
		KR 10-2012-0052197 A	23/05/2012
		KR 10-2013-0088041 A	07/08/2013
		KR 10-2013-0108328 A	02/10/2013
		KR 10-2013-0113344 A	15/10/2013
		KR 10-2013-0114663 A	18/10/2013
		KR 10-2013-0114664 A	17/10/2013
		KR 10-2013-0140678 A	24/12/2013
		KR 10-2013-0143693 A	31/12/2013
		KR 10-2014-0003409 A	09/01/2014
		KR 10-2014-0009171 A	22/01/2014
		US 2010-188975 Al	29/07/2010
		US 2010-188990 Al	29/07/2010
		US 2010-188991 Al	29/07/2010
		US 2010-188992 Al	29/07/2010
		US 2010-188993 Al	29/07/2010
		US 2010-188994 Al	29/07/2010
		US 2010-188995 Al	29/07/2010
		US 2010-190470 Al	29/07/2010
		US 2010-191575 Al	29/07/2010
		US 2010-191576 Al	29/07/2010
		US 2010-191604 Al	29/07/2010
		US 8023425 B2	20/09/2011
		US 8229812 B2	24/07/2012

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2014/038080

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
		US 8250207 B2	21/08/2012
		US 8270310 B2	18/09/2012
		US 8270952 B2	18/09/2012
		US 8275830 B2	25/09/2012
		US 8321526 B2	27/11/2012
		US 8326958 Bl	04/12/2012
		US 8331901 B2	11/12/2012
		US 8340634 B2	25/12/2012
		US 8346225 B2	01/01/2013
		US 8355337 B2	15/01/2013
		US 8391834 B2	05/03/2013
		US 8402111 B2	19/03/2013
		US 8406748 B2	26/03/2013
		US 8548428 B2	01/10/2013
		US 8583781 B2	12/11/2013
		US 8630192 B2	14/01/2014
		US 8634821 B2	21/01/2014
		US 8675507 B2	18/03/2014
US 2006-0119884 Al	08/06/2006	CN 1783008 A	07/06/2006
		CN 1783008 CO	27/02/2008
		EP 1667051 A2	07/06/2006
		KR 10-0793955 Bl	16/01/2008
		KR 10-2006-0062435A	12/06/2006
US 2010-0246597 Al	30/09/2010	BR PI1000905A2	17/01/2012
		CN 101951496 A	19/01/2011
		EP 2237517 Al	06/10/2010
		JP 2010-239617A	21/10/2010
		KR 10-2010-0109452 A	08/10/2010
US 2004-0203684 Al	14/10/2004	AU 2003-264930 Al	19/04/2004
		CN 100413356 CO	20/08/2008
		CN 1692664 A	02/11/2005
		EP 1547417 Al	29/06/2005
		EP 1547417 Bl	13/07/2011
		KR 10-2005-0051675 A	01/06/2005
		WO 2004-030389 Al	08/04/2004