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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
31 July 2014 (31.07.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/116589 A1

(51) International Patent Classification:
G06F 9/44 (2006.01) *G06F 15/16* (2006.01)
G06F 21/00 (2013.01)

(21) International Application Number:
PCT/US2014/012339

(22) International Filing Date:
21 January 2014 (21.01.2014)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/756,853 25 January 2013 (25.01.2013) US
61/825,857 21 May 2013 (21.05.2013) US

(71) Applicant: **JVL VENTURES, LLC** [US/US]; 230 Park Avenue, Suite 2829, New York, NY 10169-0005 (US).

(72) Inventor: **GARGIULO, Michael, J.**; 3612 Leeds Court, Corinth, TX 76210 (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 DATA RE-INSTALLATION

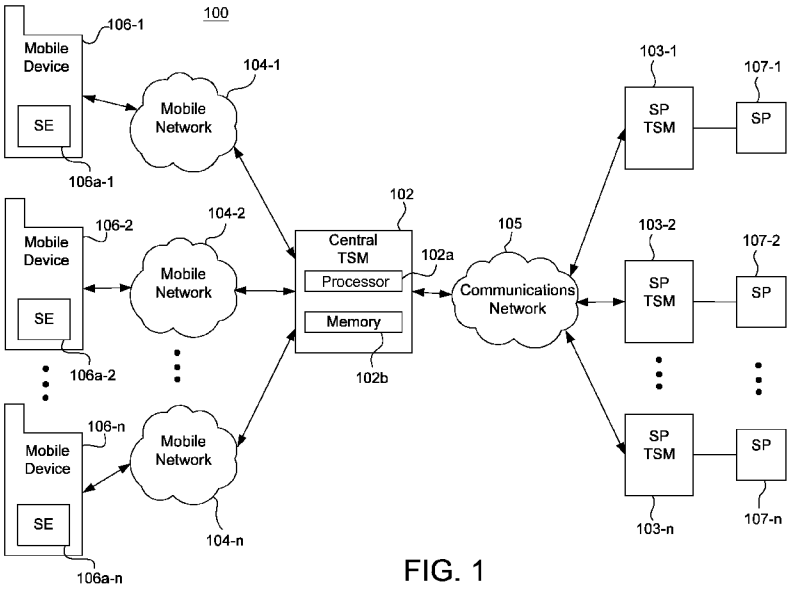


FIG. 1

(57) Abstract: Systems, methods, and computer program products are provided for managing data re-installation including service re-installation. A re-installation procedure re-installs and optionally activates data at least partially installed on a secure element without intervention middleware to repair a personalization procedure failure. Thus, personalization data on a secure element (SE) may be comprehensively managed by interfacing between one of a plurality of service provider (SP) trusted service managers (TSM) and a central trusted service manager (central TSM). The processing time required to manage the re¬ installation procedure is min - imized.

WO 2014/116589 A1

SYSTEMS, METHODS, AND COMPUTER PROGRAM PRODUCTS FOR MANAGING DATA RE-INSTALLATION

BACKGROUND

Field

[0001] The present invention relates to mobile networks, and more particularly to systems, methods, and computer program products for managing data re-installation including service re-installation.

Related Art

[0002] A service provider (SP) is a company, organization, entity, or the like, that provides services to customers or consumers. Examples of service providers include account-issuing entities such as merchants, card associations, banks, marketing companies, and transit authorities. A service may be an activity, capability, functionality, work, or use that is permitted or

provided by a service provider such as a payment service, a ticketing service, a gift, offer or loyalty service, a transit pass service, and the like. A service may include one or more applets as well as data (*e.g.*, credentials) associated with each of the applets.

[0003] In a mobile environment that involves contactless transactions between a mobile device and a service provider, information relating to the accounts and applets issued by the service providers is downloaded onto mobile devices in order to enable them to perform the contactless transactions.

[0004] A trusted service manager (TSM) is typically an independent entity serving mobile network operators (MNOs) and account-issuing service providers by provisioning applets, such as contactless applets associated with the service providers, to mobile devices. Typical TSMs can distribute and manage the contactless applets remotely because they have access to secure elements (SEs) in a near field communication (NFC) enabled mobile device.

[0005] Security-critical applets, such as those involving payment and account credentials, require secure hardware storage and a secure execution environment. On mobile devices, this is usually handled by the secure element.

[0006] The secure element is a platform onto which applets can be installed, personalized and managed. It consists of hardware, software, interfaces, and protocols that enable the secure storage of data such as credentials, and execution of applets for payment, authentication, and other services. An applet may correspond to a service (*e.g.*, payment, commerce, ticketing) offered by a service provider.

[0007] A secure element may be implemented in different form factors such as a Universal Integrated Circuit Card (UICC), an embedded secure element, or NFC enablers such as a separate chip or secure device, which can be inserted into a slot on the mobile device. Typically a UICC is in the form of a subscriber identity module (SIM), which is controlled by the MNOs. An embedded secure element gives service providers the option to embed the

secure element into the phone itself. One way in which secure element form factors are implemented is defined in, for example, GlobalPlatform Card Specification Versions 2.1.1, 2.2, and 2.2.1 (hereinafter "Global Platform").

[0008] A secure element may include one or more security domains (SDs), each of which includes a collection of data, such as packages, applets, and the like, that trust a common entity (*e.g.*, are authenticated or managed by using a common security key or token).

[0009] Security domains may be associated with service providers and may include service provider applets such as loyalty, couponing, and credit card, and transit applets.

[0010] A central TSM is a system for interfacing (*e.g.*, communicating, beginning a dialog) service providers and secure elements, for example for service providers to personalize services on a secure element, transmit scripts to be processed, and the like. An exemplary embodiment of a central TSM for managing communications between service providers and secure elements is described in more detail in U.S. Pat. Appln. No. 13/653,160 entitled "Systems, Methods, and Computer Program Products for Interfacing Multiple Service Provider Trusted Service Managers and Secure Elements," which is hereby incorporated by reference in its entirety.

[0011] Traditionally, when a SP attempts to personalize a service on a secure element, and during that personalization the procedure fails (*e.g.*, due to a communication error or a dropped connection), the SP would have to manage and execute multiple new individual processes outside of that initial personalization procedure to, for example, clean up (*e.g.*, delete) the partially personalized service and perform a recovery attempt to personalize the service. That is, traditionally the SP executes several steps that require intervention of the SP's middleware and the end-user or customer of the service to repair the personalization procedure failure. This is a time consuming and complex procedure, which requires extensive processing, coordinating, and use of resources.

[0012] One technical challenge involves centralizing a procedure within a TSM to re-install a partially personalized service without the intervention of the middleware of a SP.

[0013] Another technical challenge involves re-installing a service in accordance with requirements of the service (*e.g.*, a service having security-critical data).

BRIEF DESCRIPTION

[0014] The present invention provides systems, methods, and computer program products for managing data re-installation including service re-installation.

[0015] In one embodiment, a system for managing data re-installation includes a processor coupled to a memory. The processor (*e.g.*, included in a central trusted service manager, central TSM) receives, over a communications network (*e.g.*, from a service provider trusted service manager, SP TSM), a re-install request to re-install data at least partially installed on a secure element. The data is re-installed on the secure element and activated (*e.g.*, made usable or selectable).

[0016] In another embodiment, a method for managing data re-installation includes receiving, over a network, a re-install request to re-install data at least partially installed on a secure element, re-installing the data on the secure element, and activating the data re-installed on the secure element.

[0017] In another embodiment, a non-transitory computer-readable medium having stored thereon sequences of instructions, the sequences of instructions including instructions, which, when executed by a computer system cause the computer to: receive, over a network, a re-install request to re-install a data at least partially installed on a secure element; re-install the data on the secure element; and activate the data re-installed on the secure element.

[0018] In another embodiment, a system for managing service re-installation includes a processor coupled to a memory. The processor (*e.g.*, included in a central TSM) receives, over a communications network (*e.g.*, from a SP

TSM), a re-installation request to re-install a service at least partially personalized on a secure element. The service is re-installed on the secure element and activated (*e.g.*, made usable or selectable).

[0019] In another embodiment, a method for managing service re-installation includes receiving, over a network, a re-installation request to re-install a service at least partially personalized on a secure element, re-install the service on the secure element, and activating the service re-installed on the secure element.

[0020] In another embodiment, a non-transitory computer-readable medium having stored thereon sequences of instructions, the sequences of instructions including instructions, which, when executed by a computer cause the computer to: receive, over a network, a re-installation request to re-install a service at least partially personalized on a secure element; re-install the service on the secure element; and activate the service re-installed on the secure element.

BRIEF DESCRIPTION OF THE DRAWINGS

[0021] 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.

[0022] Figure 1 is a diagram of a system for interfacing between service providers and mobile devices having secure elements according to an exemplary embodiment.

[0023] Figure 2 is a sequence diagram illustrating a sequence for managing a service re-installation request from a service provider trusted service manager to a central trusted service manager according to an exemplary embodiment.

[0024] Figure 3 is a flow chart illustrating a sequence of processing states of a service in the central TSM during re-installation of a service according to an exemplary embodiment.

[0025] Figure 4 is a flow chart illustrating a counter reset policy of the re-installation procedure according to an exemplary embodiment.

[0026] Figure 5 is a block diagram of an exemplary system useful for implementing the present invention.

DETAILED DESCRIPTION

Overview

[0027] The example embodiments of the invention presented herein describe systems, methods, and computer program products for managing re-installation of partially personalized services in secure elements in communication with a TSM. This is for convenience only, and is not intended to limit the application of the present invention. In fact, after reading the following description, it will be apparent to one skilled in the relevant art(s) how to implement the following invention in alternative embodiments, such as in other system components (*e.g.*, an enterprise service bus ("ESB")) capable of managing a re-installation request sent over a network to re-install a service having been partially personalized on a secure element or mobile device.

[0028] Generally, a service provider system (*e.g.*, service provider) communicates with a central TSM in order to install services (*e.g.*, one or more applets) on a secure element, install or personalize data on a secure element, re-install services at least partially personalized on the secure element, and/or activate data on the secure element.

[0029] It should be understood that "applets" as used herein refer to generic or instances of applets on a secure element.

[0030] The terms "applet," "application," and/or the plural form of these terms are used interchangeably herein to refer to an applet (functioning independently or in conjunction with other applets) or set or subset of instructions or code, which when executed by one or more processors (*e.g.*, in a mobile device, card reader, terminal, point of sale (POS) system, or server) causes the processor(s) to perform specific tasks.

[0031] In one exemplary embodiment, the service provider may transmit a request to the central TSM to install a service (*e.g.*, one or more applets) on a secure element. In response, the central TSM may install the service on the secure element, by generating at least one service provider security domain including corresponding temporary security keys, if required, and/or instantiating the service on the secure element.

[0032] Generally, service instantiation includes creating an instance of an uninstantiated applet on a secure element and extraditing that instance to a security domain on a secure element. Installing and/or instantiating a service on a secure element are described in more detail in U.S. Pat. Appln. No. 13/653,145 entitled "Systems, Methods, and Computer Program Products for Managing Secure Elements," which is hereby incorporated by reference in its entirety.

[0033] In another exemplary embodiment, the service provider may transmit a request to the central TSM to personalize a service (*e.g.*, an applet, multiple applets, or any other information to be associated with a service) on a secure element. In response, the central TSM may personalize the service by installing data (*e.g.*, credentials) into that service.

[0034] In addition, the service provider may transmit a re-installation request to a single source (*e.g.*, the central TSM) in the event that personalization of that service failed. The central TSM is able to manage the re-installation request to re-install a service on a secure element without the need to communicate with multiple intermediary sources (*e.g.*, service provider middleware, end-user or customer of the service).

[0035] That is, a SP TSM calls an application programming interface (API) such as a web service API that exists on a central TSM. Via the API, the central TSM internally processes removal of a corrupted instance of a service, creates and installs a new instance of the service on the SE, and notifies the SP TSM that the new (*e.g.*, clean) instance is available on the SE for a recovery attempt to personalize the service, without involving, for

example, service provider middleware or the end-user or customer of the service.

[0036] As a result, the processing time required to execute the re-installation request is minimized relative to, for example, a system requiring involvement of the middleware of the SP.

System

[0037] FIG. 1 is a diagram of an exemplary system 100 for interfacing between service providers and secure elements over mobile networks. As shown in FIG. 1, system 100 includes SP TSMs 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"). Each SP TSM 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").

[0038] Each of the SP TSMs 103 is communicatively coupled to central TSM 102 via a communications network 105. Communications network 105 may be a virtual private network (VPN), a network by using Hypertext Transfer Protocol (HTTP) standards, or the like.

[0039] 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 central TSM 102 by using an application programming interface (API) such as a web service API.

[0040] In an exemplary embodiment, the central TSM 102 is hardware and/or software that is implemented to serve as an intermediary between the SP TSMs 103 and secure elements 106a-1, 106a-2, ..., 106a-n (collectively "106a"). Specifically, the central TSM 102 allows each of the SP TSMs 103 to, for example, request installation of data (*e.g.*, a service) on a secure element (*e.g.*, secure elements 106a), re-install data (*e.g.*, re-install a service), generate and install new or temporary security domain keysets, and/or have data activated (*e.g.*, made usable or selectable). That is, the central TSM 102

manages the communications between the SP TSMs 103 and the secure elements 106a.

[0041] The central TSM 102, therefore, can 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").

[0042] In an example embodiment, the central TSM 102 includes a processor 102a and a memory 102b.

[0043] The central TSM 102 is communicatively coupled to the secure elements 106a via corresponding mobile networks 104 that are 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, by using security protocols such as Global Platform secure channel protocol, SSL, TLS, or the like.

[0044] As shown in FIG. 1, secure elements 106a are associated with corresponding mobile devices 106-1, 106-2, and 106-n (collectively "106"), respectively. The secure elements 106a may be communicatively coupled to one or more processors and one or more memories.

[0045] The secure elements 106a may include security domains, code, applets, and packages. The packages may include uninstantiated applets, and may be loaded on a secure element, for example, over-the-air (OTA). Applets on the secure element may be in uninstantiated or instantiated form, and uninstantiated applets may be preloaded on a secure element during manufacture of the secure element. Alternatively, applets may be loaded, for example, OTA after a secure element has been manufactured (*e.g.*, upon delivering the secure element to a user). Applets may be generic or non-generic. Non-generic applets may include couponing and loyalty applets, and/or any applet that is not generic to multiple service providers. That is, a non-generic applet may correspond to a single service provider. Data that

may be used and/or associated with a non-generic applet (*e.g.*, offers, coupons) may be stored in the secure element or in memory outside of the secure element (*e.g.*, non-volatile memory of a mobile device).

[0046] Generic applets may include applets that, when instantiated, can be used by multiple service providers. For example, a generic applet of a payment network (*e.g.*, MasterCard®) may be instantiated for multiple service providers by a central TSM, and therefore may be used by more than one service provider.

[0047] Additionally, uninstantiated applets may be instantiated, and each instance may then be extradited to a corresponding security domain. Instantiation may include personalizing applets by using data corresponding to the entity for which the instance is being generated or data corresponding to an end-user or customer of the service.

[0048] For example, multiple instances of an uninstantiated applet may be generated for different entities (*e.g.*, service providers) and each instance may be extradited to a different security domain for use by a different entity.

[0049] An applet on a secure element 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 may be, for example, expresspay™, payWave™, PayPass™, Zip™, and the like.

[0050] For example, the SP TSM 103-1 sends a request to the central TSM 102 via the communications network 105, and the central TSM 102 sends a response back to the SP TSM 103-1 via the communications network 105. The SP TSM 103-1 sends a request, intended for the secure element 106a-1, to the central TSM 102 via the communications network 105. In turn, the central TSM 102 sends that request to the secure element 106a-1 via the respective mobile network 104-1.

[0051] In an alternative embodiment, a plurality of service providers share one of the SP TSMs 103.

[0052] In an additional alternative embodiment, the memory 102b may be a database.

[0053] In another alternative embodiment, a plurality of mobile networks communicate with a plurality of SP TSMs.

[0054] In the exemplary embodiments described herein, the central TSM 102 functions as a pass-through mechanism for installation and personalization data and manages the re-installation and personalization of a partially personalized service on a secure element.

Process

A. Re-Installing a Service Having Security-Critical Data on a Secure Element

[0055] FIG. 2 is a sequence diagram illustrating a sequence for managing a service re-installation request from a SP TSM 203 (*e.g.*, FIG. 1, SP TSM 103-1) to a central TSM 202 (*e.g.*, FIG. 1, central TSM 102), according to an exemplary embodiment. In this example, the service to be re-installed has been partially personalized with security-critical data such as payment and account credentials of a service.

[0056] As shown in FIG. 2, at step 252, SP TSM 203 transmits a request to central TSM 202 to personalize a service on SE 201 (*e.g.*, FIG. 1, SE 106a-1). SE 201 includes one or more services installed prior to the personalization request transmitted at step 252. Each service includes at least one applet associated with a corresponding service provider.

[0057] The personalization request at step 252 may include one or more of the following attributes: a secure element identifier, a service identifier, and a service qualifier. In addition, the personalization request includes security-critical data such as a credit card account number, an expiration date, and a customer name. A sensitive key used to generate a dynamic cryptogram is also passed at this time.

[0058] The secure element identifier is a unique number or set of characters that is written to a secure element and is used (*e.g.*, by central TSM 202) to

identify the target secure element. For example, the secure element identifier may be a Card Image Number (CIN), which is written to the secure element during manufacture of the secure element.

[0059] The service identifier may include a service identifier number and version of the service, which are used (*e.g.*, by central TSM 202) to identify a target generic service on SE 201.

[0060] The service qualifier includes a service provider name and payment account reference number (PRN), and is used (*e.g.*, by central TSM 202) to identify the particular instance of the target service (*e.g.*, the service corresponding to the service identifier) that is to be acted on (*e.g.*, installed, deleted) by using requests, including commands.

[0061] At step 254, central TSM 202 identifies the target service and the target secure element using the information in the personalization request received at step 252. In turn, central TSM 202 begins to personalize that service on SE 201 by transmitting one or more commands to SE 201 to deliver the security-critical data received in the personalization request. If the personalization procedure is successfully completed, SE 201 transmits, at step 256, a personalization result to central TSM 202. The personalization result may be in the form of an identifier, referred to as a "status word," that corresponds to a predetermined list of potential results. Status words are described in more detail below in connection with Table 2. For example, as shown in Table 2, if the personalization request was successfully processed and the personalization of the service was successfully completed, central TSM 202 receives a status word from the SE 201 (*e.g.*, status words '90' '00') indicating that success. The central TSM 202 may, in turn, transmit the personalization result to the SP TSM 203, at step 258.

[0062] Alternatively, during the personalization of the service on the SE 201 an error may occur (*e.g.*, due to a communication error or a dropped connection) that causes the personalization process of step 254 to fail. As a result, the service is left partially personalized on SE 201, meaning that all of the personalization data was not fully and successfully installed on the

service during the personalization process. The personalization procedure failure may be detected by central TSM 202 or by SE 201.

[0063] If a personalization error or failure is identified by the central TSM 202, the failure or error is reported to SP TSM 203 by the central TSM 202, at step 258. In particular, central TSM 202 transmits an error notification including a subject code and or reason code indicating that the personalization process of the service was not successful. Examples of errors identified by the central TSM 202 include: a null pointer exception due to an internal error at central TSM 202 or a dropped communication in which a database (*e.g.*, in SP TSM 203) went offline and the central TSM 202 could not communicate with the database. Examples of errors identified by central TSM 202, including subject codes and reason codes are described in more detail below in Table 1. Typically, a description and instruction correspond to a subject code and reason code of an error. The description is an explanation of why the error occurred during the personalization process, and the instruction is a suggested step or steps to take with regard to the installation of the service being personalized.

Table 1

Subject Code	Reason Code	Description	Instruction
1.2	5	OTA transport error	Re-installation of service should not be initiated
2.6	5	Failure in sending scripts	Re-installation of service should be initiated ***Note:*** • Take into consideration SCP02 counter may increment

[0064] If a personalization error or failure is identified by the SE 201, the failure or error is reported to the central TSM 202 at step 256, which in turn transmits the failure or error to the SP TSM 203 at step 258. In particular, SE 201 transmits an error notification including a status word or status code indicating that the personalization process of the service was not successful at step 256. Examples of errors identified by the SE 201 include: incorrect

data sent to the SE, SE out of memory, or an internal error occurred on the SE. Examples of errors identified by SE 201, including status words (SWs) are described in more detail below in Table 2. Typically, a status word of an error includes a description of the error and a corresponding instruction as to what step should or should not be initiated. The description is an explanation of why the error occurred during the personalization process, and the instruction is a suggested step or steps to take with regard to the installation of the service being personalized.

Table 2

SW1	SW2	Description	Instruction
'65'	'81'	Memory failure	Re-installation of service should not be initiated
'6A'	'80'	Incorrect parameters in data field	Re-installation of service should be initiated ***Note***: • Parameter(s) in data fields (*i.e.*, data in the personalization request) shall be properly rebuilt before new personalization script is sent • Take into consideration SCP02 counter may increment
'6A'	'84'	Not enough memory space	Re-installation of service should not be initiated
'6A'	'88'	Referenced data not found	Re-installation of service should be initiated ***Note***: • Referenced data (*i.e.*, data in the personalization request) shall be properly set before new personalization script is sent • Take into consideration SCP02 counter may increment

'6A'	'80'	Incorrect values in command data	Re-installation of service should be initiated ***Note***: • Command data (*i.e.*, data in the personalization request) shall be properly set before new personalization script is sent • Take into consideration SCP02 counter may increment
'64'	'00'	No specific diagnoses	Re-installation of service should be initiated
'67'	'00'	Wrong length in Lc	Re-installation of service should be initiated ***Note***: • Lc value and data length must correspond to each other before new personalization script is sent • Take into consideration SCP02 counter may increment
'69'	'85'	Condition of use not satisfied	Re-installation of service should be initiated ***Note***: • Take into consideration SCP02 counter may increment
'6A'	'86'	Incorrect P1 P2	Re-installation of service should be initiated ***Note***: • P1 P2 shall be properly set before new personalization script is sent • Take into consideration SCP02 counter may increment
'90'	'00'	A successful execution of the APDU (application protocol data unit)	Re-installation of service should be initiated when the number of the response APDUs are not equal to the number of the command APDUs ***Note:*** • Take into consideration SCP02 counter may increment

[0065] At step 260, using the personalization result information transmitted to it by central TSM 202, SP TSM 203 determines that the personalization requested at step 252 has failed. SP TSM 203 can then take any action it

deems necessary including, for example, requesting the re-installation of the service which was partially personalized.

[0066] Due to the nature of security-critical data, once personalization has begun, the personalization is to be completed in sequence and without a connection drop in order to assure the same security context according to the design requirements of certain security-critical applets (*e.g.*, payment applets). For example, in order to prevent fraud (*e.g.*, if authentication keys are breached), sensitive payment or account credentials of a service that are already on the secure element may not be overwritten or appended without requiring steps 264-270 of FIG. 2 to be performed. Indeed, most payment applets do not allow an audit to identify what data may have been written to the secure element during a personalization attempt. Therefore, the partially personalized service is re-installed and then personalized, rather than having the previously installed service re-personalized.

[0067] At step 262, in order to re-install the service, SP TSM 203 transmits, over the network, a re-installation request to central TSM 202 to re-install the service that was partially personalized. The re-installation request may include one or more of the following attributes that identifies the service to be re-installed: a secure element identifier, service identifier, and service qualifier.

[0068] In one example embodiment, if a personalization process of a service has failed, the service is deleted prior to being re-installed.

[0069] At step 264, the central TSM 202 (*e.g.*, via an API) manages the deletion of the partially personalized service on the SE 201 by transmitting one or more commands to the SE 201. In other example embodiments, the service does not have to be deleted prior to being re-installed on the SE 201. Instead, the service may be overwritten by the re-installation of the service.

[0070] At step 266, central TSM 202 (*e.g.*, via the API) manages re-installation of the service (*e.g.*, instantiates a new instance of the service on SE 201 and notifies SP TSM 203 that the new instance is available for a recovery attempt to re-install the service) and activation of the service (*e.g.*,

made usable or selectable). Activating a service includes activating the service of a service provider and making the applets associated with that service selectable on a particular secure element. As described above, the service identifier and service qualifier are used to identify the general and particular instance of the service to be activated on the secure element.

[0071] At step 268, central TSM 202 (*e.g.*, via the API) manages service instance extradition (*e.g.*, extradites the instantiated instance of the service) into a corresponding security domain on SE 201.

[0072] Service deletion, activation, and extradition are described in U.S. Pat. Appln. No. 13/653,145 entitled "Systems, Methods, and Computer Program Products for Managing Secure Elements," which is hereby incorporated by reference in its entirety. In particular, service deletion, activation and extradition are performed by the central TSM transmitting commands (*e.g.*, APDU commands) to a target secure element on a mobile device.

[0073] When the re-installation has been completed (*e.g.*, service deleted, re-installed, instantiated, activated and extradited) the central TSM 202, at step 270, transmits a response, over the network, to the SP TSM 203, including information indicating the result (*e.g.*, success, failure) of the re-installation requested by the SP TSM 203 at step 262.

[0074] At step 272, the SP TSM 203 transmits a request to the central TSM 202 to personalize the service re-installed on the SE 201. The request may include one or more of a secure element identifier, service identifier, and service qualifier, as well as security-critical data. In turn, at step 274, the central TSM 202 personalizes the SE 201. Service personalization, described above, is performed by the central TSM 202 transmitting one or more commands to the SE 201 to add and/or install data including security-critical data.

[0075] In an alternative embodiment, service re-installation may also include performing a technical eligibility check (*e.g.,* TSM eligibility check) or a business eligibility check (*e.g.,*, MNO eligibility check). Exemplary technical eligibility checks and business eligibility checks are described in

more detail in U.S. Pat. Appln. No. 13/848,962 entitled "Systems, Methods, and Computer Program Products for Provisioning Payment Accounts into Mobile Wallets and Managing Events," which is hereby incorporated by reference in its entirety. For example, a technical eligibility check may be used to determine whether SE 201 has sufficient memory space to have data installed on it and a business eligibility check may include validating a mobile directory number associated with a secure element identified in an service installation request.

B. Re-Installing a Service Having Non-Security-Critical Data on a Secure Element

[0076] In another exemplary embodiment, a service to be re-installed does not include security-critical data. Such services may include, for example, a transit pass service or a ticketing service. In such an exemplary embodiment, if data (*e.g.*, transit passes, movie tickets) is partially personalized or installed on a service in a SE due to a failure or error as described above, that data may be re-personalized or re-installed starting from the point at which the failure or error occurred. That is, to complete a personalization process, the service need not be deleted. Instead, the data to be re-personalized or re-installed is the data that was not successfully personalized or installed. In addition, a clean-up (*e.g.*, deletion and re-instantiation of the service) is not required.

[0077] In FIG. 2, if personalization fails (*e.g.*, due to a communication error or a dropped connection) for a service having non-security-critical data, SP TSM 203 can retry and send the same data again at step 262. Personalization data that is already on the service on SE 201 can be overwritten or appended without requiring steps 264-270 of FIG. 2 to be performed.

C. Re-Installing Data on a Secure Element

[0078] In another exemplary embodiment, the request at step 262 of FIG. 2 may include a re-installation request for data other than services. That is, if personalization or installation of data on a secure element is not successfully

performed, the SP TSM can transmit a re-installation request to the central TSM. In turn, the central TSM can attempt to re-install the unsuccessfully installed data on the secure element.

D. Processing States of the Service in the Central TSM During Re-Installation

[0079] FIG. 3 is a flow chart illustrating a sequence of processing states of a service in a central TSM during service re-installation according to an exemplary embodiment. Exemplary states of the service include: "PERSONALIZING," "REMOVING," "REMOVED," "INSTALLING," and "INSTALLED."

[0080] Referring to both FIGs. 2 and 3, the states are managed and monitored by central TSM 202 during the re-installation process. In particular, management of a state includes central TSM 202 storing in its memory a state corresponding to a service being re-installed on the SE 201 by the central TSM 202.

[0081] At block 358, a service provider communicates with a central TSM 202 to request re-installation of a service on SE 201. Upon receiving the request, at block 360, the central TSM 202 determines the state of the service to be re-installed. The central TSM 202 performs re-installation of a service when the state of the service in the central TSM 202 is "PERSONALIZING."

[0082] A service is in "PERSONALIZING" state when the personalization process of the service fails. That is, the "PERSONALIZING" state indicates that personalization has been initiated but has not been completed (*e.g.*, communication dropped or an error occurred).

[0083] If central TSM 202 determines at block 362 that the state of the service is "PERSONALIZING," the central TSM 202 updates the state of the service to "REMOVING," at block 364, during the service deletion step 262 and updates the state of the service to "REMOVED," at block 366, when the deletion step is completed.

[0084] If central TSM 202 determines that the service state is "PERSONALIZING," at block 362, the central TSM 202 implements the re-installation request, at step 262, and updates the state of the service to "INSTALLING," at block 368, to indicate that the service is being re-installed.

[0085] If central TSM 202 determines that the service state is other than "PERSONALIZING," at block 362, an error message (*e.g.*, "Operation Not Allowed") is returned by central TSM 202 to SP TSM 203, at block 372.

[0086] Upon completion of service re-installation and activation, the state of the service is updated to "INSTALLED," at block 370, to indicate that the re-installation procedure is complete.

[0087] Central TSM 202 transmits a response, over the network, to SP TSM 203, at block 374, including a result of processing the re-installation request (*e.g.,* re-installation success or failure).

E. Counter Reset Policy

[0088] FIG. 4 is a flow chart illustrating a counter reset policy of the re-installation procedure according to an exemplary embodiment.

[0089] As shown in FIG. 4, a counter (*e.g.*, Global Platform Secure Channel Protocol '02' (SCP02) counter) counts a number of re-installation requests from the network. The counter is included in central TSM 202 of FIG. 2. Referring to both FIGs. 2 and 4, when central TSM 202 receives a re-installation request, at step 262 of FIG. 2 or block 458 of FIG. 4, to re-install a service at least partially personalized on a secure element, the counter is incremented, at block 460.

[0090] To avoid infinite loops, central TSM 202 implements a counter reset policy, at block 462, such that the number of re-installation requests is limited to a predetermined number (*e.g.*, three) of re-installation attempts. That predetermined number is shown as variable "X" in block 462.

[0091] Subsequent attempts (*e.g.*, re-installation requests) received by central TSM 202 from SP TSM 203 to re-install a service are allowed up

until the maximum number of re-installation requests has been reached, at block 464.

[0092] After a last allowed unsuccessful re-installation attempt, further attempts are prohibited by the central TSM 202. The incident (*e.g.*, that the service was unsuccessfully attempted to be re-installed the maximum number of times) may be logged into a database in central TSM 202 and an investigation is initiated, at block 466. A message may be communicated to a mobile device containing the SE 201, which in turn is displayed or otherwise communicated through the mobile device and ultimately to a user of the mobile device through a user interface such as a display or audio system. The mobile device can then be used to route the user to a customer care center associated with the central TSM 202 at block 468, where a customer representative may assist in troubleshooting the error.

F. Computer Readable Medium Implementation

[0093] The present invention (*e.g.*, system 100, sequence 200, flowcharts 300 and 400, or any part(s) or function(s) thereof) can be implemented by using hardware, software, or a combination thereof, and can be implemented in one or more mobile device or other processing systems. To the extent that manipulations performed by the present invention were referred to in terms of human operation, no such capability of a human operator is necessary, or desirable in most cases, in any of the operations described herein which form part of the present invention. Rather, the operations described herein are machine operations. Useful machines for performing the operations of the present invention include mobile phones, smartphones, personal digital assistants (PDAs) or similar devices.

[0094] In one embodiment, the invention is directed toward one or more systems capable of carrying out the functionality described herein. An example of a system 500 is shown in FIG. 5.

[0095] The system 500 includes one or more processors, such as processor 501. The processor 500 is coupled to a communication infrastructure 502 (e.g., communication bus, network). Various embodiments are described in

terms of this exemplary system. After reading this description, it will become more apparent to a person skilled in the relevant art(s) how to implement the invention by using other systems and/or architectures.

[0096] The system 500 also includes a main memory 503, which may be a database, or the like.

[0097] The system 500 also includes a receiving module 504 for receiving data, such as requests (*e.g.*, to install and re-install data), from other entities over a network. Receiving data, such as requests, is described in further detail above with reference to FIGS. 2-4.

[0098] The system 500 also includes a transmission module 505 for transmitting data, such as requests and responses, to other entities over a network. Transmitting data, such as requests and responses, is described in further detail above with reference to FIGS. 2-4.

[0099] Each of modules 504 and 505 may be implemented by using hardware, software or a combination of the two.

[0100] The example embodiments described above such as, for example, the systems and procedures depicted in or described in connection with FIGS. 1 to 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.

[0101] 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.

[0102] 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.

[0103] Some embodiments include a computer program product. The computer program product may be a non-transitory 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.

[0104] Stored on any one of the non-transitory 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 applets. Ultimately, such computer readable media further includes software for performing example aspects of the invention, as described above.

[0105] 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.

[0106] 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.

[0107] 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.

[0108] 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 system for managing data re-installation, the system comprising:
a processor coupled to a memory, the processor being operable to:
receive, over a network, a re-install request to re-install data at least partially installed on a secure element;
re-install the data on the secure element; and
activate the data re-installed on the secure element.

2. The system of Claim 1, wherein the data is a service.

3. The system of Claim 2, the processor being further operable to extradite the service re-installed on the secure element into a security domain on the secure element.

4. The system of Claim 1, the processor being further operable to delete the data at least partially installed on the secure element.

5. The system of Claim 4, the processor being further operable to delete the data at least partially installed on the secure element prior to performing the re-installation.

6. The system of Claim 1, wherein the re-install request includes a secure element identifier, a service identifier, and service qualifier.

7. The system of Claim 1, the processor being further operable to transmit a response over the network including a result of processing the re-install request.

8. The system of Claim 1,
the memory being operable to store a state of the data, and
the processor being further operable to:

determine, upon receiving the re-install request, the state of the data;

update the state of the data to indicate the data is being installed on the secure element if it is determined that the state of the data is personalizing; and

return an error message over the network if it is determined that state of the data is other than personalizing.

9. The system of Claim 8, the processor being further operable to update the state of the data to indicate that the data is being deleted from the secure element if it is determined that the state of the data is personalizing.

10. The system of Claim 1, the processor being further operable to perform a technical eligibility check and a business eligibility check.

11. The system of Claim 1, the processor being further operable to count a number of re-install requests from the network, wherein the number of re-install requests is limited to a predetermined number.

12. A method for managing data re-installation, the method comprising:

receiving, over a network, a re-install request to re-install data at least partially installed on a secure element;

re-installing the data on the secure element; and

activating the data re-installed on the secure element.

13. The method of Claim 12, wherein the data is a service.

14. The method of Claim 13, further comprising a step of extraditing the service re-installed on the secure element into a security domain on the secure element.

15. The method of Claim 12, further comprising a step of deleting the data at least partially installed on the secure element.

16. The method of Claim 15, wherein the deleting step occurs prior to the re-installing step.

17. The method of Claim 12, wherein the re-install request includes a secure element identifier, a service identifier, and service qualifier.

18. The method of Claim 12, further comprising a step of transmitting a response over the network including a result of processing the re-install request.

19. The method of Claim 12, further comprising steps of:

determining, upon receiving the re-install request, the state of the data;

updating the state of the data to indicate the data is being installed on the secure element if it is determined that the state of the data is personalizing; and

returning an error message over the network if it is determined that state of the data is other than personalizing.

20. The method of Claim 19, further comprising a step of updating the state of the data to indicate that the data is being deleted from the secure element if it is determined that the state of the data is personalizing.

21. The method of Claim 12, further comprising a step of performing a technical eligibility check and a business eligibility check.

22. The method of Claim 12, further comprising a step of counting a number of re-install requests from the network, wherein the number of re-install requests is limited to a predetermined number.

23. A non-transitory computer-readable medium having stored thereon sequences of instructions, the sequences of instructions including instructions, which, when executed by a computer, cause the computer to:

receive, over a network, a re-install request to re-install a data at least partially installed on a secure element;

re-install the data on the secure element; and

activate the data re-installed on the secure element.

24. The computer-readable medium of Claim 23, wherein the data is a service.

25. The computer-readable medium of Claim 24, the sequence of instructions further includes instructions which, when executed by the computer, cause the computer to extradite the service re-installed on the secure element into a security domain on the secure element.

26. The computer-readable medium of Claim 23, the sequence of instructions further includes instructions which, when executed by the computer, cause the computer to delete the data at least partially installed on the secure element.

27. The computer-readable medium of Claim 26, the sequence of instructions further includes instructions which, when executed by the computer, cause the computer to delete the data at least partially installed on the secure element prior to performing the re-installation.

28. The computer-readable medium of Claim 23, wherein the re-install request includes a secure element identifier, a service identifier, and service qualifier.

29. The computer-readable medium of Claim 23, the sequence of instructions further includes instructions which, when executed by the

computer, cause the computer to transmit a response over the network including a result of processing the re-install request.

30. The computer-readable medium of Claim 23, the sequence of instructions further includes instructions which, when executed by the computer, cause the computer to:

determine, upon receiving the re-install request, the state of the data;

update the state of the data to indicate the data is being installed on the secure element if it is determined that the state of the data is personalizing; and

return an error message over the network if it is determined that state of the data is other than personalizing.

31. The computer-readable medium of Claim 30, the sequence of instructions further includes instructions which, when executed by the computer, cause the computer to update the state of the data to indicate that the data is being deleted from the secure element if it is determined that the state of the data is personalizing.

32. The computer-readable medium of Claim 23, the sequence of instructions further includes instructions which, when executed by the computer, cause the computer to perform a technical eligibility check and a business eligibility check.

33. The computer-readable medium of Claim 23, the sequence of instructions further includes instructions which, when executed by the computer, cause the computer to count a number of re-install requests from the network, wherein the number of re-install requests is limited to a predetermined number.

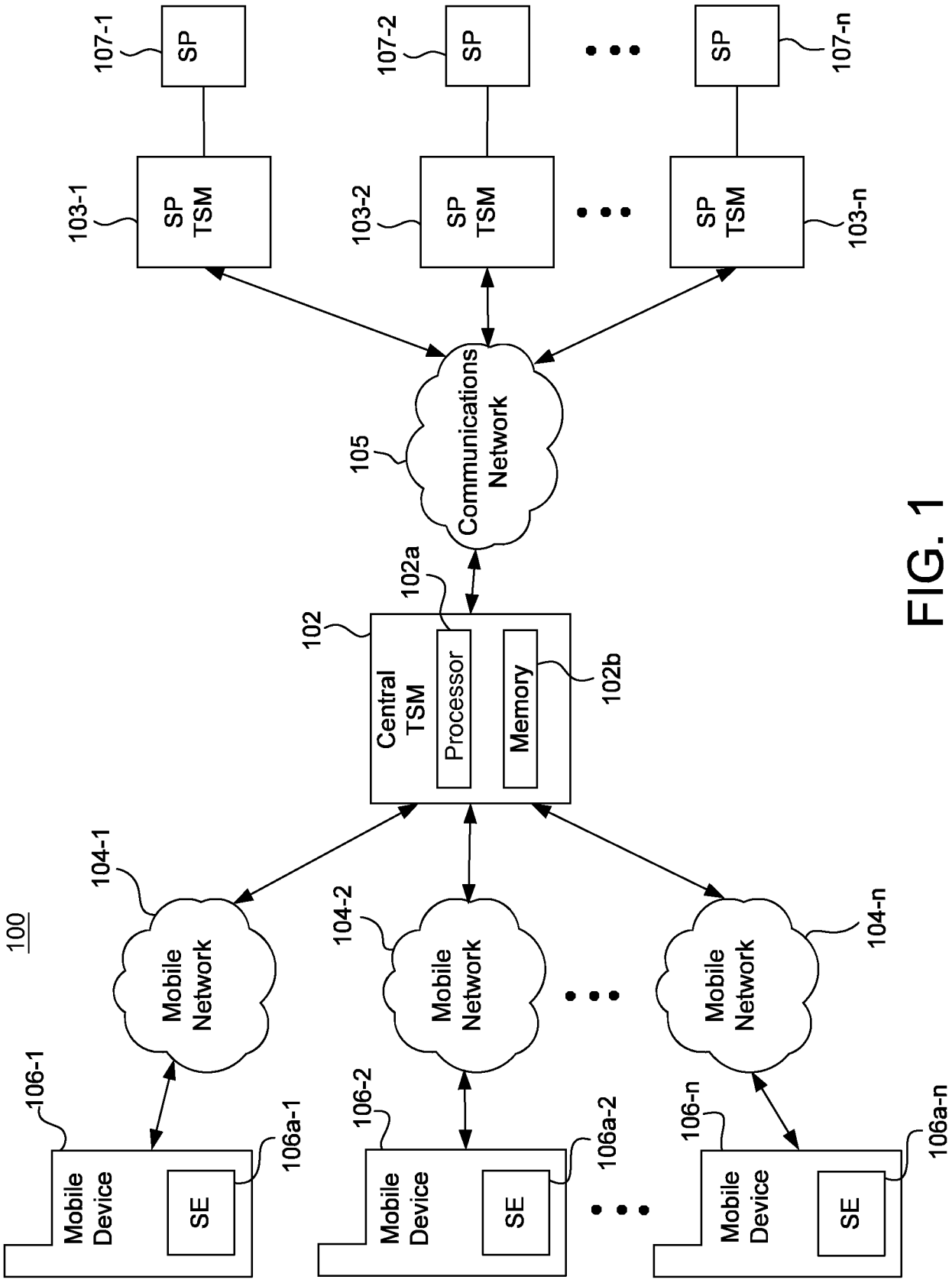

100
Mobile Device
SE
106-1
106a-1
106-2
106a-2
106-n
106a-n
Mobile Network
104-1
104-2
104-n
Central TSM
Processor
Memory
102
102a
102b
Communications Network
105
SP TSM
103-1
103-2
103-n
SP
107-1
107-2
107-n

FIG. 1

FIG. 2

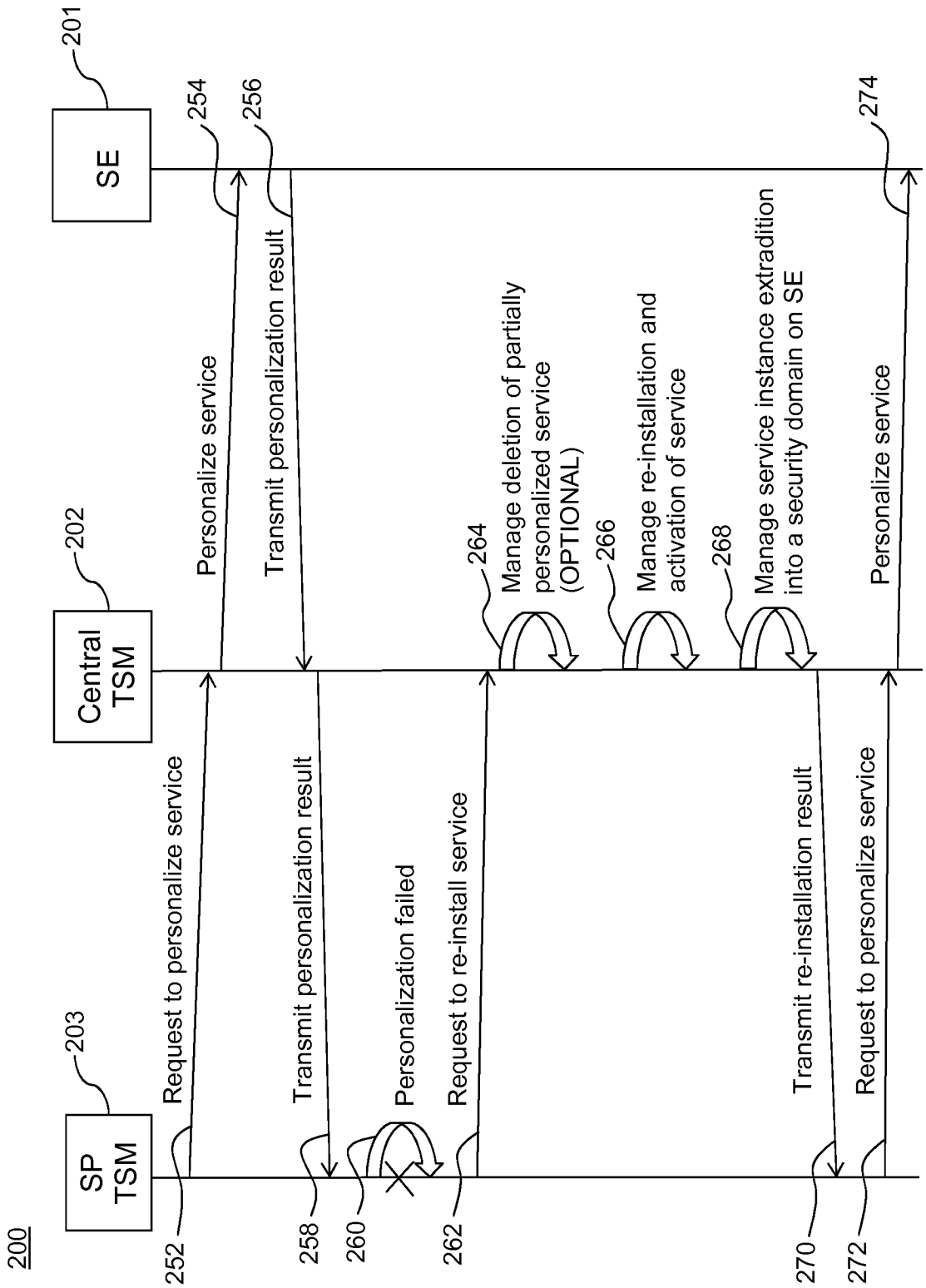

200
SP TSM
203
Central TSM
202
SE
201
Request to personalize service
252
Transmit personalization result
258
Personalization failed
260
Request to re-install service
262
Personalize service
254
Transmit personalization result
256
Manage deletion of partially personalized service (OPTIONAL)
264
Manage re-installation and activation of service
266
Manage service instance extradition into a security domain on SE
268
Transmit re-installation result
270
Request to personalize service
272
Personalize service
274

FIG. 3

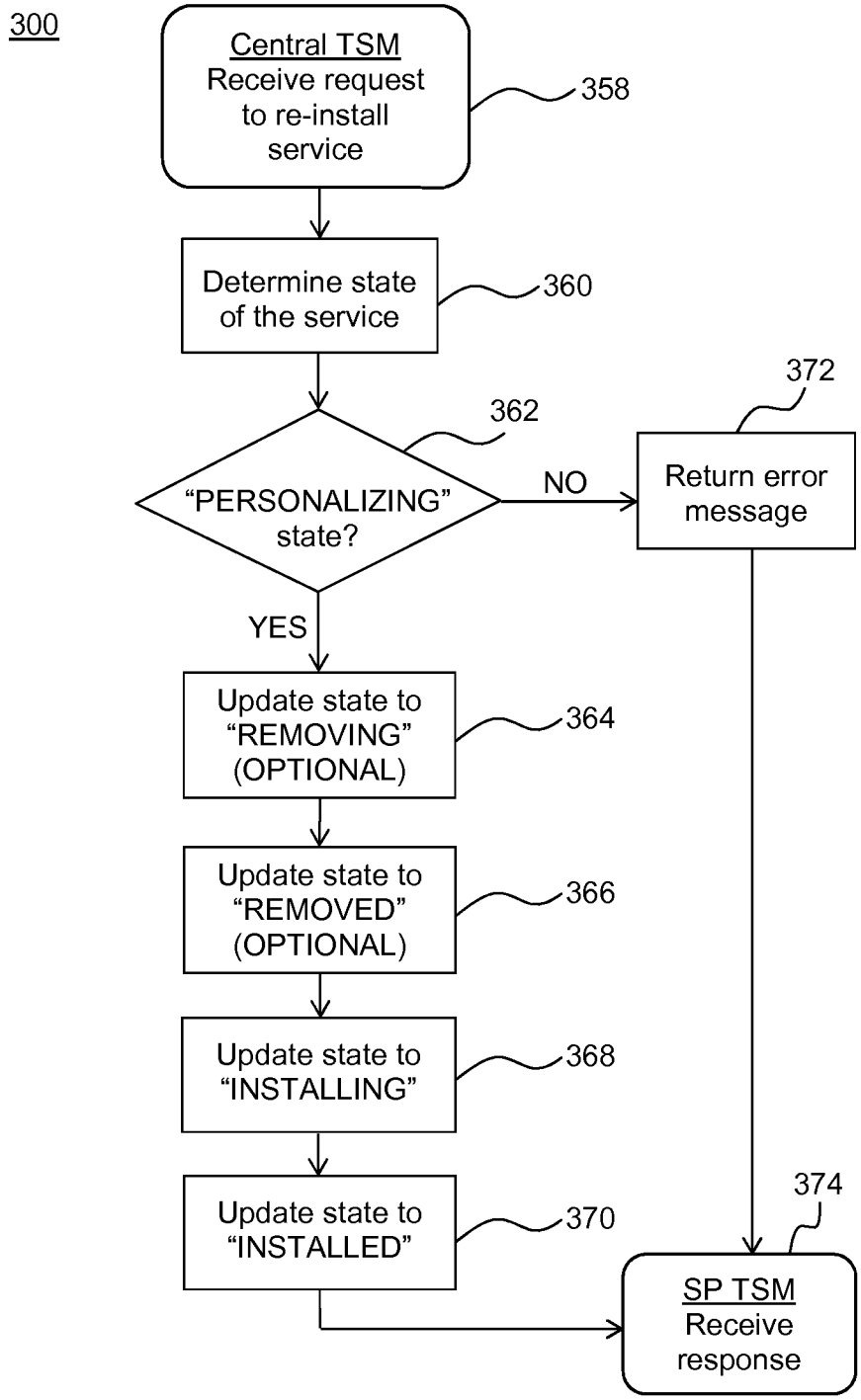

300
Central TSM
Receive request to re-install service
358
Determine state of the service
360
362
"PERSONALIZING" state?
NO
372
Return error message
YES
Update state to "REMOVING" (OPTIONAL)
364
Update state to "REMOVED" (OPTIONAL)
366
Update state to "INSTALLING"
368
Update state to "INSTALLED"
370
374
SP TSM
Receive response

FIG. 4

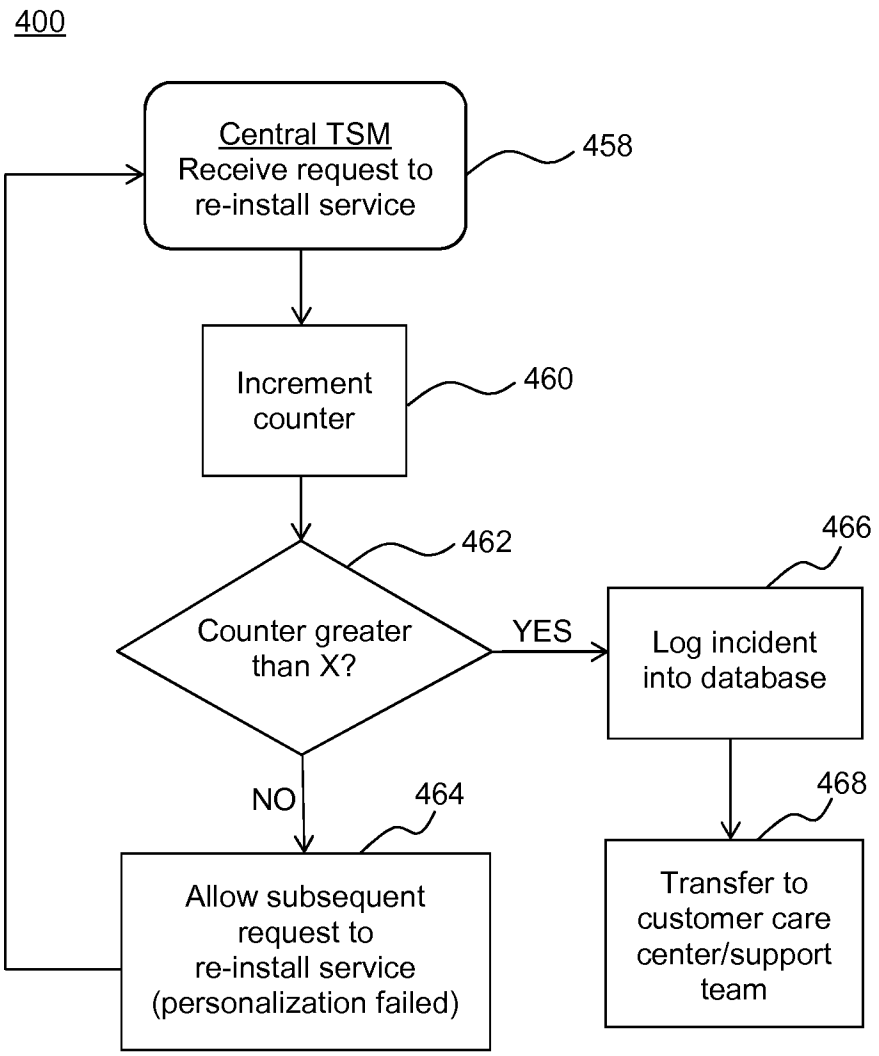
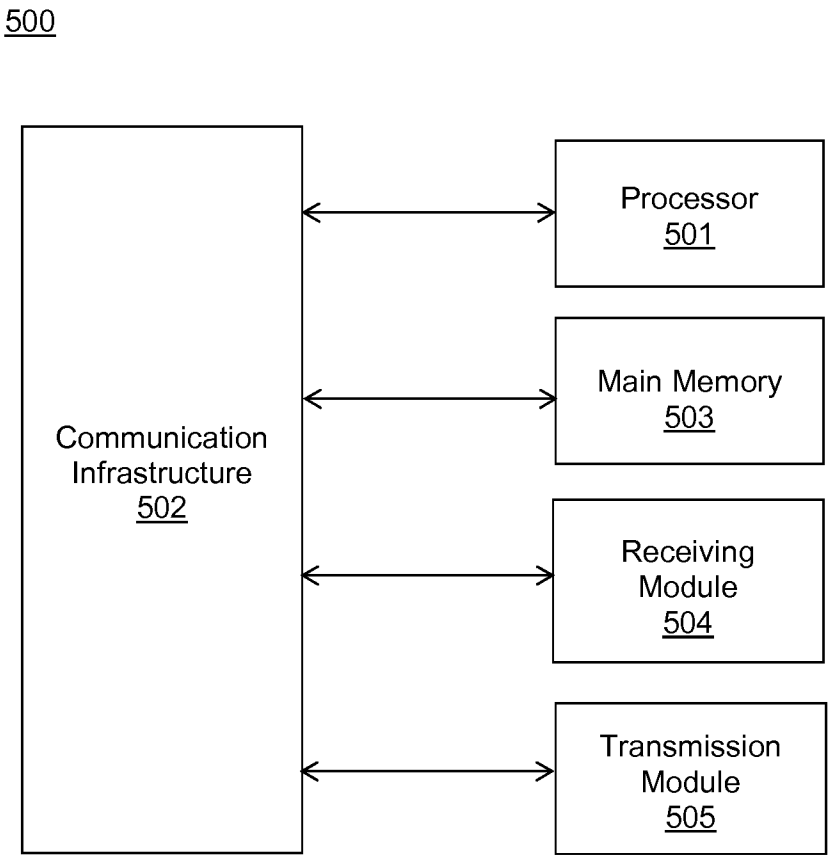

400
Central TSM
Receive request to re-install service
458
Increment counter
460
462
Counter greater than X?
YES
466
Log incident into database
NO
464
468
Allow subsequent request to re-install service (personalization failed)
Transfer to customer care center/support team

FIG. 5


500
Communication Infrastructure 502
Processor 501
Main Memory 503
Receiving Module 504
Transmission Module 505

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2014/012339

A. CLASSIFICATION OF SUBJECT MATTER

G06F 9/44(2006.01)i, G06F 21/00(2006.01)i, G06F 15/16(2006.01)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)
G06F 9/44; H04W 12/06; H04W 4/00; G09G 5/00; G06F 11/00; G06F 21/00; G06F 15/16

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: reinstall, secure, element

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2002-0089543 A1 (CHRISTIAN OSTERGAARD et al.) 11 July 2002 See paragraphs [0023]-[0060]; claims 1,7; and figures 4-10.	1-33
A	US 2009-0125755 A1 (HERSCOVITZ ELI et al.) 14 May 2009 See paragraphs [0062]-[0136]; claims 7,8,21; and figures 1a-6.	1-33
A	US 2012-0264400 A1 (KHAN SHOAIB S. et al.) 18 October 2012 See paragraphs [0017],[0051]-[0071]; claims 1,3; and figure 1.	1-33
A	US 2012-0190354 A1 (MERRIEN LIONEL et al.) 26 July 2012 See paragraphs [0070]-[0095]; and figure 1.	1-33

☐ 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
29 May 2014 (29.05.2014)	**30 May 2014 (30.05.2014)**

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
CHOI, Jeong Kwon
Telephone No. +82-42-481-8507

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2014/012339

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2002-0089543 A1	11/07/2002	EP 1215580 A2	19/06/2002
		EP 1215580 A3	11/01/2006
		GB 0030692 D0	31/01/2001
		GB 2370192 A	19/06/2002
US 2009-0125755 A1	14/05/2009	WO 2007-007326 A2	18/01/2007
		WO 2007-007326 A3	22/05/2009
US 2012-0264400 A1	18/10/2012	CA 2769933 A1	01/09/2012
		US 8660533 B2	25/02/2014
US 2012-0190354 A1	26/07/2012	CA 2819396 A1	14/06/2012
		CA 2819764 A1	14/06/2012
		CA 2819766 A1	14/06/2012
		CA 2819781 A1	14/06/2012
		CA 2819782 A1	14/06/2012
		CA 2819949 A1	14/06/2012
		CN 103329501 A	25/09/2013
		CN 103329502 A	25/09/2013
		CN 103329578 A	25/09/2013
		CN 103329582 A	25/09/2013
		CN 103329584 A	25/09/2013
		CN 103329585 A	25/09/2013
		CN 103329586 A	25/09/2013
		CN 103339972 A	02/10/2013
		CN 103339975 A	02/10/2013
		CN 103503036 A	08/01/2014
		EP 2461613 A1	06/06/2012
		EP 2649594 A1	16/10/2013
		EP 2649822 A2	16/10/2013
		EP 2649823 A1	16/10/2013
		EP 2649824 A1	16/10/2013
		EP 2649825 A1	16/10/2013
		EP 2649826 A1	16/10/2013
		EP 2649827 A1	16/10/2013
		EP 2649828 A1	16/10/2013
		EP 2649829 A1	16/10/2013
		EP 2649830 A1	16/10/2013
		EP 2649831 A1	16/10/2013
		EP 2649832 A1	16/10/2013
		JP 2013-545418 A	19/12/2013
		JP 2013-545419 A	19/12/2013
		JP 2014-500555 A	09/01/2014
		JP 2014-500678 A	09/01/2014
		JP 2014-500679 A	09/01/2014
		JP 2014-500680 A	09/01/2014
		JP 2014-504080 A	13/02/2014
		JP 2014-505287 A	27/02/2014
		KR 10-2013-0093676 A	22/08/2013

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2014/012339

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
		KR 10-2013-0095828 A	28/08/2013
		KR 10-2013-0097798 A	03/09/2013
		KR 10-2013-0097799 A	03/09/2013
		KR 10-2013-0106866 A	30/09/2013
		KR 10-2013-0106867 A	30/09/2013
		KR 10-2013-0107339 A	01/10/2013
		KR 10-2013-0108637 A	04/10/2013
		KR 10-2013-0114191 A	16/10/2013
		KR 10-2013-0114192 A	16/10/2013
		MX 2013006273 A	12/12/2013
		MX 2013006274 A	06/12/2013
		MX 2013006275 A	06/12/2013
		MX 2013006276 A	12/12/2013
		MX 2013006316 A	01/10/2013
		MX 2013006317 A	01/10/2013
		US 2013-0318355 A1	28/11/2013
		US 2013-0324091 A1	05/12/2013
		US 2013-0329683 A1	12/12/2013
		US 2014-0019760 A1	16/01/2014
		US 2014-024343 A1	23/01/2014
		US 2014-031083 A1	30/01/2014
		US 2014-057680 A1	27/02/2014
		WO 2012-076419 A1	14/06/2012
		WO 2012-076421 A1	14/06/2012
		WO 2012-076424 A1	14/06/2012
		WO 2012-076425 A1	14/06/2012
		WO 2012-076437 A2	14/06/2012
		WO 2012-076437 A3	16/08/2012
		WO 2012-076440 A1	14/06/2012
		WO 2012-076461 A1	14/06/2012
		WO 2012-076464 A1	14/06/2012
		WO 2012-076480 A1	14/06/2012
		WO 2012-076482 A1	14/06/2012
		WO 2012-076485 A1	14/06/2012
		WO 2012-076525 A1	14/06/2012