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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 March 2014 (27.03.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/047494 A1

(51) International Patent Classification:
H04W 12/06 (2009.01) *H04W 88/02* (2009.01)

(21) International Application Number:
PCT/US2013/061011

(22) International Filing Date:
20 September 2013 (20.09.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/704,405 21 September 2012 (21.09.2012) US

(71) Applicant: **APPLE INC.** [US/US]; 1 Infinite Loop, Cupertino, California 95014 (US).

(72) Inventor: **HAUCK, Jerrold von**; 1 Infinte Loop, Cupertino, California 95014 (US).

(74) Agents: **FERRAZANO, Michael J.** et al.; Womble Carlyle Sandridge & Rice LLP, 10050 North Wolfe Road, Suite 260, Cupertino, California 95014 (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, 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).

[Continued on next page]

(54) Title: APPARATUS AND METHODS FOR CONTROLLED SWITCHING OF ELECTRONIC ACCESS CLIENTS WITHOUT REQUIRING NETWORK ACCESS

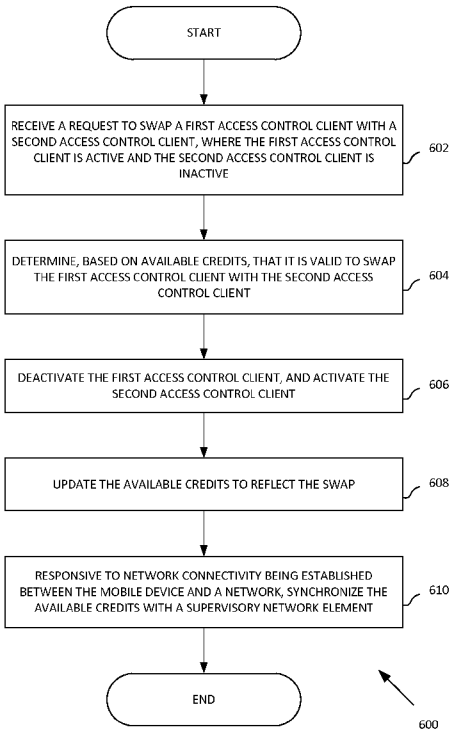


FIG. 6

(57) Abstract: Methods and apparatus for providing controlled switching of electronic access control clients without requiring network access are set forth herein. In one embodiment, a method for swapping of subscriptions and/or profiles for electronic Subscriber Identity Modules (eSIMs) without network supervision that prevents possibly malicious high frequency switching is disclosed. The disclosed embodiments offer reasonable management capabilities for network operators, without compromising the flexibility of eSIM operation.

WO 2014/047494 A1

Published:

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

APPARATUS AND METHODS FOR CONTROLLED SWITCHING OF ELECTRONIC ACCESS CLIENTS WITHOUT REQUIRING NETWORK ACCESS

BACKGROUND

Technical Field

[0001] The present disclosure relates generally to the field of communications systems, and more particularly in one exemplary embodiment to switching between access control clients in a controlled manner.

Description of Related Technology

[0002] Access control is required for secure communication in most prior art wireless radio communication systems. As an example, one simple access control scheme might include: (i) verifying the identity of a communicating party, and (ii) granting a level of access commensurate with the verified identity. Within the context of an exemplary cellular system (e.g., Universal Mobile Telecommunications System (UMTS)), access control is governed by an access control client, referred to as a Universal Subscriber Identity Module (USIM) executing on a physical Universal Integrated Circuit Card (UICC). The USIM access control client authenticates the subscriber to the UMTS cellular network. After successful authentication, the subscriber is allowed access to the cellular network. As used hereinafter, the term "access control client" refers generally to a logical entity, either embodied within hardware or software, suited for controlling access of a first device to a network. Common examples of access control clients include the aforementioned USIM, CDMA Subscriber Identification Modules (CSIM), Internet Protocol (IP) Multimedia Services Identity Module (ISIM), Subscriber Identity Modules (SIMs), Removable User Identity Modules (RUIM), etc.

[0003] Incipient research is directed to virtualization of access control clients. For example, an electronic Subscriber Identity Module (eSIM) is a virtualized access control client that is executed from a secure element within the client device. Virtualized access control clients can provide significant benefits for users and network operators. For example, a user can transfer an eSIM freely between devices; moreover, eSIMs can be flexibly stored, backed up, etc. Network operators can distribute and/or patch eSIMs via software distribution networks. However, due to the sensitive nature of the data used for network access (e.g., cryptographic information)

and user information (e.g., account information), the secure element and eSIM must be tightly controlled to prevent e.g., theft, misuse, malicious behavior, etc.

[0004] Unfortunately, for reasons described in greater detail herein, network operators have been reluctant to adopt eSIMs due to various perceived security concerns. For example, network operators have expressed some degree of apprehension that unsupervised switching of eSIMs could be misused. To these ends, network operators have required that eSIMs can only be transacted with network supervision. While supervised solutions may alleviate security concerns, such tight control effectively negates many of the advantages offered by eSIM technologies.

[0005] Accordingly, improved methods and apparatus for eSIM switching are needed. More generally, such solutions should ideally offer reasonable management capabilities for network operators, without compromising the flexibility of virtualized access control clients.

SUMMARY

[0006] The present disclosure addresses the foregoing needs by providing, inter alia, apparatus and methods for controlled switching of electronic access control clients without requiring network access.

[0007] A method for providing controlled switching of electronic access control clients without network access is disclosed. In one embodiment, the method includes: determining if an active access control client can be swapped with an inactive access control client based on one or more credits; when a swap can be performed: deactivating the active access control client; and activating the inactive access control client; and responsive to network connectivity being restored, synchronizing one or more log information with a supervisory network entity.

[0008] A wireless handset device configured to switch electronic access control clients without network access, is also disclosed.

[0009] Non-transitory computer-readable medium with at least one computer program stored thereon, the at least one computer program configured to, when executed on the processor, cause the processor to switch electronic access control clients without network access is further disclosed.

[0010] A supervisory network entity is additionally disclosed.

[0011] Further features of the various principles described herein, their nature and various advantages will be more apparent from the accompanying drawings and the following detailed description.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] FIG. 1 is a logical flow diagram of one embodiment of a method for controlled switching of electronic access control clients without requiring network access.

[0013] FIG. 2 is a logical flow diagram of one exemplary embodiment of a credit based system for controlling eSIM switching without requiring network access.

[0014] FIG. 3 is a logical flow diagram of one exemplary embodiment of a rate limited system for controlling eSIM switching without requiring network access.

[0015] FIG. 4A is a logical flow diagram of one exemplary embodiment of a human interaction system for controlling eSIM switching without requiring network access, where the mobile device is not trusted.

[0016] FIG. 4B is a logical flow diagram of one exemplary embodiment of a human interaction system for controlling eSIM switching without requiring network access, where at least portions of the mobile device are trusted.

[0017] FIG. 5 is logical block diagram of an exemplary embodiment of a mobile device configured in accordance with various ones of the principles described herein.

[0018] FIG. 6 is a logical flow diagram of one exemplary embodiment of a method for a credit based system for controlling eSIM switching and synchronizing with a network.

DETAILED DESCRIPTION

Detailed Description of Exemplary Embodiments

[0019] Exemplary embodiments are now described in detail. While these embodiments are primarily discussed in the context of electronic Subscriber Identity Modules (eSIMs) of a GSM, GPRS/EDGE, UMTS, or Long Term Evolution (LTE) cellular network, it will be recognized by those of ordinary skill that the present disclosure is not so limited. In fact, the various principles discussed herein are useful in any network (whether wireless cellular or otherwise) that can benefit from controlled switching of electronic access control clients without requiring network access.

[0020] It will also be recognized that while the term "subscriber identity module" is used herein (e.g., eSIM), this term in no way necessarily connotes or requires either (i) use by a subscriber *per se* (i.e., the disclosed embodiments may be practiced by a subscriber or non-subscriber); (ii) identity of a single individual (i.e., the disclosed embodiments may be practiced on behalf of a group of individuals such as a family,

or intangible or fictitious entity such as an enterprise); or (iii) any tangible "module" equipment or hardware.

Subscriber Identity Module (SIM) Operation

[0021] Within the context of the exemplary prior art UMTS cellular network, user equipment (UE) includes a mobile device and a Universal Subscriber Identity Module (USIM). The USIM is a logical software entity that is stored and executed from a physical Universal Integrated Circuit Card (UICC). A variety of information is stored in the USIM such as subscriber information, as well as the keys and algorithms used for authentication with the network operator in order to obtain wireless network services. In one embodiment, USIM software is based on the Java Card™ programming language. Java Card is a subset of the Java™ programming language that has been modified for embedded "card" type devices (such as the aforementioned UICC). Other implementations may include so-called "native" software implementations, and/or implementations that are proprietary, etc.

[0022] Generally, UICCs are programmed with a USIM prior to subscriber distribution, where the pre-programming or "personalization" is specific to each network operator. For example, before deployment, the USIM is associated with an International Mobile Subscriber Identity (IMSI), a unique Integrated Circuit Card Identifier (ICC-ID) and a specific authentication key (K). The network operator stores the association in a registry contained within the network's Authentication Center (AuC). After personalization the UICC can be distributed to subscribers.

[0023] As a brief aside, during normal authentication procedures, the UE acquires the IMSI from the USIM. The UE passes the IMSI to the Serving Network (SN) of the network operator or the visited core network. The SN forwards the authentication request to the AuC of the Home Network (HN). The HN compares the received IMSI with the AuC's registry and obtains the appropriate key K. The HN generates a random number (RAND) and signs it with key K using an algorithm to create the expected response (XRES). The HN further generates a Cipher Key (CK) and an Integrity Key (IK) for use in cipher and integrity protection as well as an Authentication Token (AUTN) using various algorithms. The HN sends an authentication vector, consisting of the RAND, XRES, CK, and AUTN to the SN. The SN stores the authentication vector only for use in a one-time authentication process. The SN passes the RAND and AUTN to the UE.

[0024] Once the UE receives the RAND and AUTN, the USIM verifies if the received AUTN is valid. If so, the UE uses the received RAND to compute its own response (RES) using the stored key K and the same algorithm that generated the XRES. The UE passes the RES back to the SN. The SN compares the XRES to the received RES, and, if they match, the SN authorizes the UE to use the operator's wireless network services.

[0025] Typically, the Authentication and Key Agreement (AKA) procedure is performed by a secure processor that has been packaged within a SIM card. Prior art SIM cards have at least two (2) distinct and desirable properties: (i) SIM cards provide cryptographically secured storage for SIM data (e.g., account information, encryption keys, etc.), and (ii) SIM cards cannot be easily cloned.

[0026] A prior art SIM card includes a processor and a memory formed in a Universal Integrated Circuit Card (UICC). The SIM card may be filled with epoxy resin to prevent external probing of data signals on the UICC. Other tamper-proof structures may be included in the UICC if desired (e.g., shielding layers, masking layers, etc.). The SIM card has a secure interface to the processor, and the processor has an internal interface to the memory. The UICC receives power from the external device, which enables the processor to execute code stored in the memory. The memory itself is not directly accessible (i.e., internal filesystems are hidden from the user), and must be accessed via the processor.

[0027] During normal operation, the processor accepts a limited number of commands. Each of the commands is only conditionally accessible. Access conditions are constrained to the execution of commands to prevent unauthorized access. Access conditions may or may not be hierarchical, e.g., authorization for one level may not automatically grant authorization for another level. For example, one set of access conditions may include: (i) always accessible, (ii) never accessible, (iii) accessible to a first account, (iv) accessible to a second account, etc. Conditional access is granted only after successful completion of an appropriate security protocol. Common methods for verifying identity may include a password or Personal Identification Number (PIN), challenge of a shared secret, etc.

[0028] Conditional access, limited command set, and protected memory space ensure that the information stored within the SIM card is secure from external access. Cloning a SIM card would entail construction of a physical card as well as

construction of the internal filesystem and data. Thus, the combination of these features renders the physical SIM card impervious to practical forgery attempts.

Electronic Subscriber Identity Module (eSIM) Operation

[0029] While traditional SIM solutions are embodied within a removable Integrated Circuit Card (ICC) (also referred to as a "SIM card"), incipient research by the Assignee hereof is directed to virtualizing SIM operation within a software client executing within the mobile device. Virtualized SIM operation can reduce device size, increase device functionality, and provide greater flexibility.

[0030] Unfortunately, virtualized SIM operation also presents multiple new challenges for network operators and device manufacturers. For example, traditional SIM cards are manufactured and guaranteed by a trusted SIM vendor. These traditional SIM cards execute a single secure version of software that has been permanently "burned" to the SIM card. Once burned, the card cannot be tampered with (without also destroying the SIM card).

[0031] In contrast, mobile devices are manufactured by a wide range of device manufacturers, and may execute software provided by multiple or even unknown third party software vendors. Additionally, mobile devices are frequently "patched" with software, which can both fix existing bugs, and introduce new ones. Any software is susceptible to corruption, sabotage, and/or misuse. Moreover, while physical SIM cards are very difficult to replicate, software can be readily copied, multiplied, etc. Since each SIM represents a contracted amount of access to finite network resources, illicit use of a virtualized SIM can greatly impact network operation and user experience.

[0032] As a brief aside, the terms "conservation," "conserve," and "conserved," as used herein refer to an element (either physical or virtual) that cannot be trivially multiplied or diminished. For example, a conserved eSIM cannot be copied or replicated during normal operation.

[0033] Additionally, as used herein, the term "uniqueness" as applied to an element (either physical or virtual), refers to the property whereby the element is the one and only element having a particular property and/or characteristic. For instance, a unique eSIM cannot have a duplicate eSIM.

[0034] As used herein, the term "security" generally refers to protection of the data and/or software. For example, access control data security ensures that the data and/or software associated with an access control client is protected from theft,

misuse, corruption, publication and/or tampering, by unauthorized activities, and/or malicious third parties.

[0035] Moreover, as used herein, the term "user authorization" generally refers to specifying a user's access to resources. As a brief aside, with prior art physical SIM cards, user authorization is enforced with physical SIM card possession, where the physical card represents the user's authorization to access network resources. For example, when a physical SIM card is moved from a first phone to a second phone, it is assumed that the move was performed by the user (and implicitly authorized by the user). Within the context of eSIM operation, analogous capabilities are needed for user authorization of eSIM transfers. In particular, the "owner" of the eSIM (and also the network) needs assurances that the eSIM is only transferred to legitimate devices.

[0036] Generally, it is appreciated that software is more flexible than hardware; for example, software is easy to copy, modify, and distribute. Additionally, software can often be made cheaper, more power efficient, and physically smaller than hardware equivalents. Accordingly, while conventional SIM operation makes use of physical form factors such as cards (UICCs), current areas of research are focused toward virtualizing SIM operation within software. However, the sensitive nature of SIM data (e.g., subscriber specific information, etc.) requires special consideration. For example, various portions of SIM data are unique to subscribers, and should be carefully guarded from malicious third parties. Moreover, as previously stated, each SIM represents a contracted amount of access to finite network resources; thus, duplication, destruction, and/or reclamation of SIMs must be managed to prevent over and/or underutilization of network resources, as well as subrogation of service provider fees or revenue. Accordingly, virtualized SIMs should satisfy the following properties: (i) security, (ii) uniqueness, and (iii) conservation. Moreover, such properties should ideally be afforded at a cost that is commensurate with existing network infrastructure costs.

Method

[0037] Various embodiments of methods for controlled switching of electronic access control clients without requiring network access are described in greater detail herein. Specifically, the various exemplary methods detailed in greater detail herein allow swapping of subscriptions and/or profiles for access control clients without network supervision, while preventing high frequency switching. High frequency

switching of access control clients may possibly be used in e.g., denial of service type attacks and/or general disruption of device/network operation.

[0038] Referring now to FIG. 1, one embodiment of a method for controlled switching of electronic access control clients without requiring network access is presented. Consider a device that includes at least a secure element configured to select, activate, and execute at least one access control client, where the secure element is further configured to swap between a plurality of inactive access control clients. For example, a mobile device may have multiple electronic Subscriber Identity Modules (eSIMs) that are stored within an electronic Universal Integrated Circuit Card (eUICC).

[0039] At step 102, an inactive access control client and an active access control client are selected for a switching operation. For clarity, as used herein, the terms "active" and "inactive" refer to the execution status of the access control client, not the current connection status (i.e., an active access control client may or may not have a connection context to the network). It is appreciated by those of ordinary skill in the related arts that an access control client that is being executed by the secure element is "active," whereas an access control client that is not executed is "inactive."

[0040] In one embodiment, the selection is performed by a user. User selection may occur via a user interface. In other variants, user selection may occur via a physical operation, such as card insertion (e.g., where the physical card may include a SIM, or an eSIM on a SIM card form factor. In still other variants, user selection may occur based on a physical switch, etc.

[0041] In other embodiments, selection can be initiated by a software entity. Common examples of software entities include for example: the operating system (OS), the secure element OS, software applications, third party software applications, network applications, etc. In some embodiments, software embodiments may automatically implement swapping based on e.g., geographic location, time of day, usage, etc. For instance, the OS may automatically swap a first eSIM associated with a business account with a second eSIM associated with a personal account at designated times of the day. In other embodiments, the OS may automatically swap a first eSIM with a second eSIM to prevent and/or reduce roaming charges, etc.

[0042] Moreover, those of ordinary skill in the related arts will recognize that the following examples are purely illustrative. For example, in other schemes, the swapping may be performed with a different number of access control clients. In one

such scheme the secure element may attempt to swap two (2) eSIMs into operation in place of one (1) previously active eSIM; i.e., the number of eSIMs being "swapped" does not need to be a one-for-one relationship.

[0043] Furthermore, while the following examples are presented in the context that no network access is available, the various principles of the present disclosure are equally applicable to scenarios where the switch can be executed without using existing network access. For example, in some circumstances, network connectivity may be undesirable based on e.g., power consumption, network congestion, etc. Moreover, the switch may be executed at the behest of a network entity or process.

[0044] Still further it is appreciated that in various disclosed embodiments, the selection of either the active or inactive access control client may be implicit. For example, in some implementations, a user may deactivate an active access control client, which results in the active access control client being replaced with a previously inactive default access control client. In a similar example, where a user has selected to activate one access control client that overlaps the capabilities of a currently active access control client, the currently active access control client may be replaced (rather than keeping both access control clients active).

[0045] At step 104 of the method 100, the secure element determines if a swap can be executed. Specifically, the secure element evaluates and prevents excessive and/or high frequency switching.

[0046] In one exemplary embodiment, the secure element applies one or more criteria to make the aforementioned determination; e.g., the secure element limits the total number of transactions that can be performed without supervision. In this manner, regardless of how fast the switching occurs, the secure element cannot perform too many swapping operations. For example, in one variant, the secure element and network operate on a "credit" system, where the secure element can perform functions without network supervision for a credited number of transactions. At a later point, the secure element can connect to the network and synchronize its transactions with the network (and receive new credits). In this manner, the user can be granted a reasonable amount of autonomy, while limiting the degree to which such flexibility can be exploited.

[0047] In some variants, the credit system may be limited to a subset of operations. For example, a user may be allowed to freely deselect an operational

profile or eSIM, but have only a limited number of credits for selecting operational profiles.

[0048] In some embodiments, the credit system may be further monitored by a supervisory network element. According to one embodiment, the supervisory network element represents any hardware device (e.g., a server device) or a service (e.g., a software component) that is configured to monitor transactions that take place within the credit system. For example, where a secure element appears to be requesting top-off credits too frequently (indicating an unusually high amount of swapping behavior), the network entity may flag the secure element/mobile device as possibly malicious or compromised. In other examples, the network entity may throttle (increase or reduce) the refreshing of credits to control the amount of swapping behavior (e.g., increasing credits may reduce network overhead for swapping operations, reducing credits increases the networks supervisory responsibilities).

[0049] In other embodiments, the secure element either directly or indirectly limits the rate of swapping. For example, the secure element may be able to determine, e.g., based on an internal time base and log information, the amount of time that has elapsed since the last swap. A swap request that occurs too soon after a prior swap may be rejected. In a similar embodiment, the secure element may require that an access control client is active for at least a minimum time interval before swapping. Various other schemes for time based rate limiting will be recognized by those of ordinary skill in the related arts, given the contents of the present disclosure.

[0050] In another example, the rate limiting may be indirectly enforced. For example, in one variant, the secure element may require human interaction to execute the swap. Human interaction elements may include e.g., PINs, so-called Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) type challenge-response tests (e.g., a distorted image that can be easily solved by a human, but are difficult for computers to process), physical switches and/or button presses, etc. Those of ordinary skill in the related arts will recognize that human interactions are significantly slower (several seconds) than software (several milliseconds), and thus have a reasonably low frequency, thereby effecting the desired rate limitations.

[0051] Moreover, it is further appreciated that human interaction elements can also serve to verify that the user of the mobile device is initiating the transfer (and not malicious software). In some embodiments, the mobile device can be manufactured with a physical presence pin (PPP) that is characterized in that it cannot be accessed

or otherwise spoofed within software. Such a PPP can be connected to an external button (or switch, dial, etc.) that must be manipulated by a human during the swap (such as to initiate or confirm the swap) in order to complete the procedure.

[0052] Furthermore, those of ordinary skill in the related arts will readily recognize that certain ones of the aforementioned schemes may provide an additional benefit of verifying the legitimacy of the request. For example, a PIN code will verify that the requestor is a legitimate user. Similarly, biometric data (e.g., retinal scan image, fingerprint, voiceprint, facial recognition software image, etc.) may be used to verify the identity of the user. In some variants, the swap may be further limited based on information specific to one of the access control clients. For example, the user may be required to enter the PIN code of the active access control client (or alternately, the inactive access control client that is being swapped to replace the active access control client).

[0053] It is additionally recognized that for software initiated swaps, the requesting application may be required to provide some proof of legitimacy. Common examples include digital certificates, cryptographic challenges, etc.

[0054] While the foregoing schemes have been presented, those of ordinary skill in the related arts will readily recognize, given the contents of the present disclosure, that a wide multitude of rate limiting and/or verification schemes are possible in conjunction with the methods disclosed herein.

[0055] Referring now back to FIG. 1, when the determination of step 104 indicates that a swap can be performed, the secure element deactivates its currently active access control client (step 106); when a swap cannot be performed, the secure element ignores the request (step 108). At step 110, the secure element activates the previously inactive access control client.

[0056] Generally, the secure element deactivates/activates the access control clients via existing protocols and sequences. In some embodiments, these may be proprietary protocols specific to the access control client. In other embodiments, the protocols may be standardized for a wide array of different access control clients. Common examples of such a standardized protocol include the ISO/IEC 7816-4, which specifies, e.g., access protocols, and security mechanisms for messaging for smart card communications.

[0057] In one embodiment, the secure element decrements one or more credits from the total number of available credits. In some embodiments, the number of

credits decremented may be adjusted based on various network preferences. For example, the network operator may be concerned with a type of swapping behavior, or a type of access control client. By increasing the number of credits decremented during these swaps, the mobile device will not be able to perform as many swaps before requiring a refresh.

[0058] In one embodiment, the secure element logs the transaction within an internal logging database. The database may track information including, without limitation: time of transaction, elapsed usage, access control client, number of attempts (e.g., for failed attempts), etc. In one embodiment, the internal logging database is stored within the secure element. In other embodiments, the logging database may be stored in the mobile device. In some variants, the logging database may be further secured via, e.g., encryption.

[0059] At step 112, the secure element synchronizes its transactions with a supervisory network entity (also referred to herein as the "network entity," "network security entity," "network server entity," and "supervisory network element") after network connectivity has been restored. In some embodiments, the synchronization is triggered during reconnection. In other embodiments, synchronization may be based on the amount of credits left. For example, where the secure element has an ample supply of credits, it may postpone synchronization. In still other embodiments, synchronization may be initiated on an as-needed basis, or alternately when directed by the user or an application.

[0060] During synchronization, the secure element transfers the logged transaction history to the network. The network can use the logged transaction history to, e.g., detect malicious activity, determine access control client usage, adjust billing, etc. In some embodiments, the secure element can replenish its balance of credits upon successfully completing synchronization. In other embodiments, the network determines the amount of credits the secure element should replenish. For example, where the network has identified malicious high frequency swapping, the network may not allow the secure element to replenish any credits.

Example Operation

[0061] Various exemplary implementations of the embodiment of the method presented in FIG. 1 are now discussed.

[0062] First, consider a cellular user equipment (UE) device that includes a secure electronic Universal Integrated Circuit Card (eUICC) having multiple electronic

Subscriber Identity Modules (eSIMs). The eSIMs may be associated with one or more cellular networks having an associated cellular network technology. For example, in one exemplary scenario, the UE has eSIMs for: Carrier A operating a UMTS network (voice and data), Carrier B operating a Code Division Multiple Access (CDMA) 2000 (voice and data), and Carrier C operating an LTE network (data only).

Credit System

[0063] FIG. 2 illustrates one exemplary credit based system 200 for controlling eSIM switching without requiring network access.

[0064] Within the system of FIG. 2, the eUICC allows a preset maximum number of unauthorized (local) swap commands in 'offline' mode, where the eUICC has a number of credits equal to the preset maximum number.

[0065] At step 202, the mobile device enters an 'offline' mode during which the mobile device does not have network connectivity. In one exemplary scenario, the mobile device moves into an area with no network connectivity (e.g., an airplane). In other scenarios, the mobile device may disable operation, e.g., to reduce power consumption.

[0066] At step 204, an offline swap is requested. For example, a user may intentionally select a new eSIM while on an airplane, based on the flight destination.

[0067] At step 206, if credits are available, then a credit is decremented and the swap is performed. However, if there are no credits available (or insufficient credits), further offline swap requests are rejected.

[0068] Once the mobile device returns to online operation (i.e., where the mobile device has resumed network connectivity), the credit balance is increased or reset via an authorized command from an authorizing network server entity (step 208). The network server entity can monitor the requests to identify possibly suspicious behavior.

[0069] In one embodiment, the eUICC always attempts to 'top off' its credits whenever it resumes network connectivity. In this manner, the network server entity will be notified almost immediately of suspicious swapping behavior. If the network server entity detects any suspicious/fraudulent activity, the network server entity can, e.g., limit the number of credits issued, not issue credits, or in some cases flag the device for possible corrective actions.

[0070] In some variants, the eUICC further splits the swap into 'deselect' and 'select' operations. Specifically, the eUICC may freely allow offline deselect

commands without authorization but require 'select' commands to be based on credits. In one such variant, there may be a default selectable profile that is useful for provisioning and or limited contact with the network server entity, but not e.g., user data access, voice calls, etc. During operation the default provisioning profile enables operation of the mobile device to load in other functional eSIMs, receive updates pushed from the network, etc.

Rate Limited System

[0071] FIG. 3 illustrates one exemplary rate limited system 300 for controlling eSIM switching without requiring network access.

[0072] In one exemplary embodiment, the eUICC has access to a time base that can be measured. While existing eUICCs do not have an internal clock (crystal oscillator, etc.), the secure element does receive a clock signal from the mobile device. This clock signal is not necessarily accurate (it can be intermittent), but it does provide sufficient timing to support an incrementing count that can be used to ensure that swap commands are not issued too frequently.

[0073] At step 302, the mobile device enters an 'offline' mode during which the mobile device does not have network connectivity, and, at step 304, an offline swap is requested.

[0074] At step 306, the eUICC estimates an amount of time that has elapsed since the last swap. In one embodiment, the eUICC maintains an incrementing count of clock ticks since the last swap event. When the clock ticks exceed a minimum threshold, the eUICC can perform a swap. Otherwise, the swap is ignored or alternately postponed (step 308).

[0075] Once the mobile device returns to online operation, the eUICC may provide its log information to the network server entity (optional step 310).

Human Interaction System

[0076] In other embodiments, the eUICC attempts to verify that the offline swap was requested by a human (presumably the user of the mobile device). FIG. 4A illustrates one exemplary human interaction system 400 for controlling eSIM switching without requiring network access, where the mobile device is not trusted (i.e., where the only known secure element is the eUICC itself).

[0077] At step 402, the mobile device enters an 'offline' mode during which the mobile device does not have network connectivity, and, at step 404, an offline swap is requested.

[0078] At step 406, the eUICC verifies the presence of a human by, e.g., requesting a password or personal identification number (PIN) code that is uniquely associated with the eSIM that is being swapped. In some cases, the PIN code may be acquired by the user via an out-of-band mechanism (e.g., calling customer service); the additional security and time of PIN code entry ensures that the process is both rate limited and verifiable.

[0079] If the PIN code entry is correct, then the swap can proceed, otherwise the attempt is ignored (step 408).

[0080] In alternate implementations, the eUICC could produce a puzzle challenge easily solved by humans but not by computers such as a CAPTCHA. A correct answer to the puzzle within a time limit authorizes the command.

[0081] Referring now to FIG. 4B one exemplary human interaction system 450 for controlling eSIM switching without requiring network access, where the mobile device is trusted is illustrated. In this embodiment, human interaction can be constructed with the aid of other components in a mobile device that are external to the eUICC. In such cases, the mobile device may be additionally configured in a manner that provides a physical presence pin (PPP) that cannot be manipulated by untrusted software.

[0082] At step 452, the mobile device enters an 'offline' mode during which the mobile device does not have network connectivity, and, at step 454, an offline swap is requested.

[0083] At step 456, the eUICC waits for the PPP to be asserted. In one such example, the PPP is exclusively routed between a hardware 'eject' switch on the mobile device and the eUICC.

[0084] In other embodiments, the PPP may be routed to another trusted/certified co-processor in the mobile device. During the verification process, the trusted processor may additionally implement secure input/output (I/O), biometric sensor data, or a CAPTCHA like mechanism to prove the human interaction, and then provide the appropriate signaling on the PPP.

Apparatus

[0085] Various apparatus useful in conjunction with the above described methods are now described in greater detail.

[0086] Referring now to FIG. 5, an exemplary mobile device 500 (e.g., a user equipment (UE)) in accordance with various principles described herein is illustrated.

[0087] The exemplary UE apparatus of FIG. 5 is a wireless device with a processor subsystem 502 such as a digital signal processor, microprocessor, field-programmable gate array, or plurality of processing components mounted on one or more substrates. The processing subsystem may also include an internal cache memory. The processing subsystem is in communication with a memory subsystem 504 including memory that may, for example, include SRAM, flash, and/or Synchronous Dynamic Random Access Memory (SDRAM) components. The memory subsystem may implement one or a more of Direct Memory Access (DMA) type hardware, so as to facilitate data accesses as is well known in the art. The memory subsystem contains computer-executable instructions that are executable by the processor subsystem.

[0088] In one exemplary embodiment, the device can include of one or more wireless interfaces 506 adapted to connect to one or more wireless networks. The multiple wireless interfaces may support different radio technologies such as GSM, CDMA, UMTS, LTE/LTE-A, WiMAX, WLAN, Bluetooth, etc. by implementing the appropriate antenna and modem subsystems.

[0089] The user interface subsystem 508 includes any number of well-known I/O including, without limitation: a keypad, touch screen (e.g., multi-touch interface), a Liquid Crystal Display (LCD), backlight, speaker, and/or microphone. However, it is recognized that in certain applications, one or more of these components may be obviated. For example, PCMCIA card-type client embodiments may lack a user interface (as they could piggyback onto the user interface of the host device to which they are physically and/or electrically coupled).

[0090] In the illustrated embodiment, the device includes a secure element 510 that contains and operates the eUICC application. The eUICC is capable of storing and accessing a plurality of access control clients to be used for authentication with a network operator. The secure element includes in this embodiment a secure processor executing software stored in a secure media. The secure media is inaccessible to all other components (other than the secure processor). Moreover, the secure element may be further hardened to prevent tampering (e.g., encased in resin) as previously described.

[0091] The secure element 510 is capable of receiving and storing one or more access control clients. In one embodiment, the secure element stores an array or plurality of eSIMs associated with a user (e.g., one for work, one for personal, several

for roaming access, etc.), and/or according to another logical scheme or relationship (e.g., one for each of multiple members of a family or business entity, one for each of personal and work use for the members of the family, and so forth). Each eSIM includes a small file system including computer readable instructions (the eSIM program), and associated data (e.g., cipher keys, integrity keys, etc.)

[0092] The secure element is further adapted to enable switching of eSIMs within the mobile device. Specifically, the secure element can be switch one or more eSIMs into "active" or "inactive" states.

[0093] In one exemplary embodiment, the secure element further includes an internal database configured to store an access control client transaction history. In one variant, the internal database tracks one or more of: time of transaction, elapsed usage, access control client, number of attempts (e.g., for failed attempts), etc.

[0094] In other embodiments, the secure element further includes access to a physical presence pin (PPP), where the PPP cannot be manipulated by untrusted software (i.e., requires physical manipulation, or is otherwise connected to a trusted software entity).

[0095] Furthermore, various realizations of the exemplary embodiment include instructions that, when executed, launch a challenge/response security protocol. The challenge response security protocol is configured to verify requests made by an unknown third party, based on appropriate generation of challenges and/or responses. Alternately, in one exemplary embodiment, the secure element can verify a digital certificate signed by a trusted authority.

[0096] In addition, FIG. 6 is a logical flow diagram of one exemplary embodiment of a method 600 for a credit based system for controlling eSIM switching and synchronizing with a network. As shown in FIG. 6, the method 600 begins at step 602, where a mobile device receives a request to swap a first access control client with a second access control client, where the first access control client is active and the second access control client is inactive. At step 604, the mobile device determines, based on available credits, that it is valid to swap the first access control client with the second access control client. At step 606, the mobile device deactivates the first access control client, and activates the second access control client. At step 608, the mobile device updates the available credits to reflect the swap. Finally, at step 610, the mobile device, responsive to network connectivity

being established between the mobile device and a network, synchronizes the available credits with a supervisory network element.

[0097] It will be recognized that while certain features are described in terms of a specific sequence of steps of a method, these descriptions are only illustrative of the broader methods disclosed herein, and may be modified as required by the particular application. Certain steps may be rendered unnecessary or optional under certain circumstances. Additionally, certain steps or functionality may be added to the disclosed embodiments, or the order of performance of two or more steps permuted. All such variations are considered to be encompassed within the disclosure and claimed herein.

[0098] While the above detailed description has shown, described, and pointed out novel features as applied to various embodiments, it will be understood that various omissions, substitutions, and changes in the form and details of the device or process illustrated may be made by those skilled in the art. The foregoing description is of the best mode presently contemplated. This description is in no way meant to be limiting, but rather should be taken as illustrative of the general principles described herein.

CLAIMS

What is claims is:

1. A method for providing controlled switching of access control clients within a mobile device without requiring access to a network, comprising:

receiving a request to swap a first access control client with a second access control client, wherein the first access control client is active and the second access control client is inactive;

determining, based on available credits, that it is valid to swap the first access control client with the second access control client, wherein swapping includes:

deactivating the first access control client, and

activating the second access control client;

updating the available credits to reflect the swap; and

responsive to network connectivity being established between the mobile device and the network, synchronizing the available credits with a supervisory network element.

2. The method of claim 1, wherein the request is generated by a user operating the mobile device.

3. The method of claim 1, wherein the request is generated when a smart card is inserted into a bay included in the mobile device.

4. The method of claim 1, wherein the request is generated when a physical switch included on the mobile device is operated by a user.

5. The method of claim 1, wherein the request is generated based on one or more of: a geographic location of the mobile device, a usage level of the mobile device, and a time-based component.

6. The method of claim 1, further comprising:

receiving, from the supervisory network element, an authorization to replenish the available credits; and

replenishing the available credits based on the received authorization.

7. The method of claim 1, wherein the available credits comprise:

deactivation credits associated with deactivating access client controls; and

activation credits associated with activating access client controls.

8. The method of claim 1, wherein determining that it is valid to swap the first access control client with the second access control client is further based on a correct response to a Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) challenge provided by a user of the mobile device.

9. The method of claim 1, wherein determining that it is valid to swap the first access control client with the second access control client is further based on a personal identification number (PIN) that is input by a user of the mobile device via a physical presence pin (PPP) component coupled to the mobile device.

10. The method of claim 1, further comprising:

subsequent to activating the second access control client, receiving an additional request to swap the second access control client with a third access control client, wherein the third access control client is inactive; and

when an activity time of the second access control client is below a threshold level of time, preventing the swap of the second access control client with the third access control client from being carried out.

11. The method of claim 1, wherein updating the available credits to reflect the swap is based on a type of the first access control client or a type of the second access control client.

12. A mobile device capable of switching between access control clients without requiring access to a network, comprising:

a processor;

a wireless interface configured to operate with the network;

a secure element storing at least a first access control client, a second access control client, and available credits; and

a memory storing instructions that, when executed by the processor, cause the processor to:

receive a request to swap the first access control client with the second access control client, wherein the first access control client is active and the second access control client is inactive;

determine, based on the available credits, that it is valid to swap the first access control client with the second access control client, wherein swapping includes:

deactivating the first access control client, and

activating the second access control client;

update the available credits to reflect the swap; and

responsive to network connectivity being established between the mobile device and the network via the wireless interface:

synchronize the available credits stored in the secure element with a supervisory network element.

13. The mobile device of claim 12, wherein the instructions, when executed by the processor, further cause the processor to:

receive, from the supervisory network element, an authorization to replenish the available credits; and

replenish the available credits based on the received authorization.

14. The mobile device of claim 12, wherein the available credits comprise:

deactivation credits associated with deactivating access client controls; and

activation credits associated with activating access client controls.

15. The mobile device of claim 12, wherein the instructions, when executed by the processor, further cause the processor to:

subsequent to activating the second access control client, receive a request to swap the second access control client with a third access control client also stored in the secure element, wherein the third access control client is inactive;

when an activity time of the second access control client is below a threshold level of time, prevent the swap of the second access control client with the third access control client from being carried out.

16. The mobile device of claim 12, wherein the processor determines that it is valid to swap the first access control client with the second access control client based on a correct response to a Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) challenge provided by a user of the mobile device.

17. The mobile device of claim 12, wherein the processor determines that it is valid to swap the first access control client with the second access control client based on a personal identification number (PIN) that is input by a user of the mobile device via a physical presence pin (PPP) component included on the mobile device.

18. A supervisory network element configured to manage a rate at which a mobile device swaps between access control clients stored on the mobile device, comprising:

a processor; and

a memory storing instructions that, when executed by the processor, cause the processor to:

receive, from the mobile device, a synchronization update that includes usage levels of credits stored on the mobile device, wherein the usage levels indicate a rate at which the mobile device has swapped between access control clients; and

issue to the mobile device an authorization that permits the mobile device to replenish the credits to a particular degree, wherein the authorization is based on the usage levels included in the received synchronization update.

19. The supervisory network element of claim 18, wherein the instructions, when executed, further cause the processor to:

receive, from the mobile device, a subsequent synchronization update that includes usage levels of the credits stored on the mobile device after the mobile device receives the synchronization update;

determine that the mobile device has exceeded a threshold usage level of the credits stored on the mobile device;

flag the mobile device as malicious; and

withhold issuing to the mobile device a subsequent authorization that permits the mobile device to replenish the credits in order to prevent the mobile device from carrying out any subsequent access control client swaps.

20. The supervisory network element of claim 19, wherein the credits include:

deactivation credits associated with deactivating access client controls; and

activation credits associated with activating access client controls.

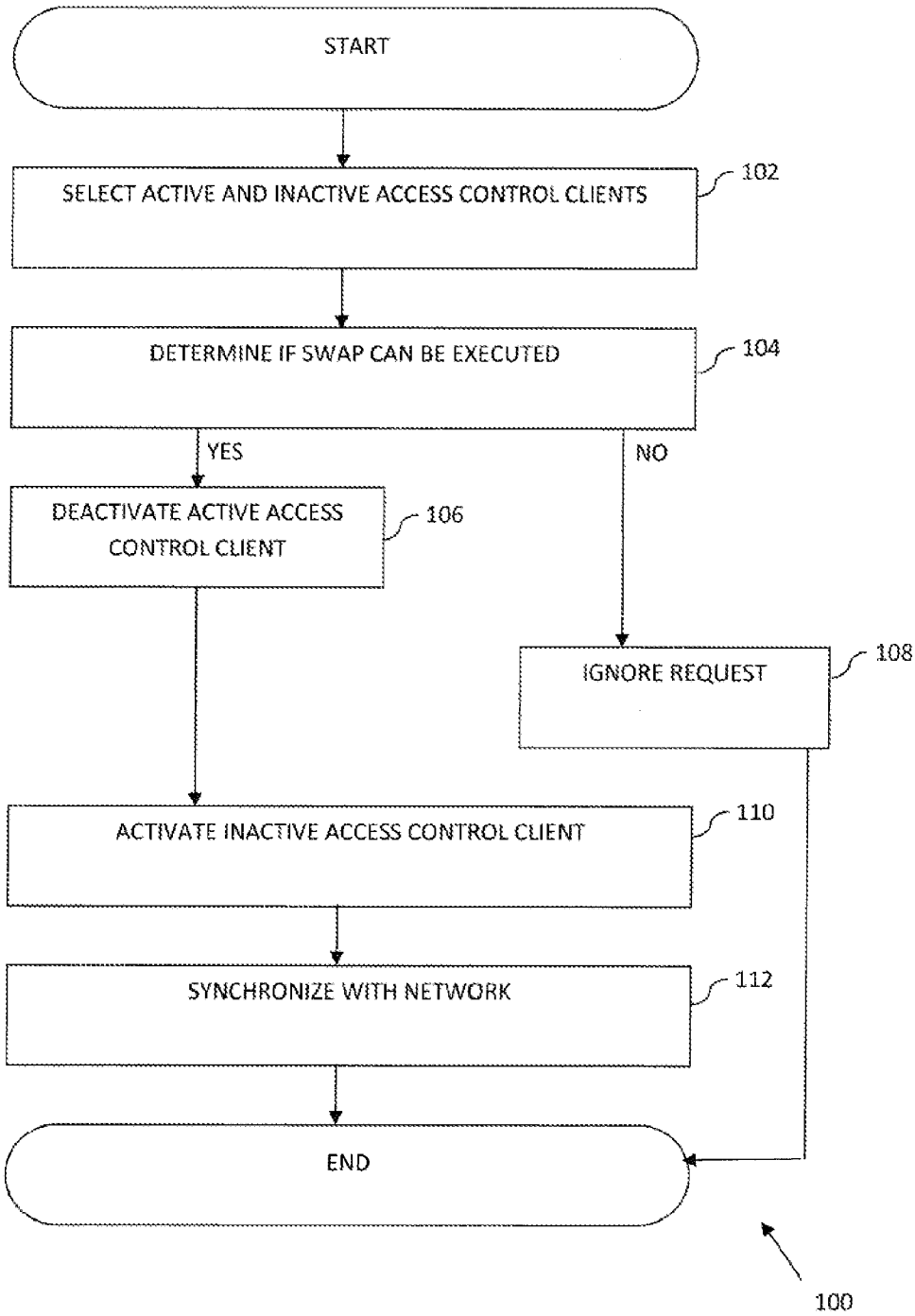

START
SELECT ACTIVE AND INACTIVE ACCESS CONTROL CLIENTS
102
DETERMINE IF SWAP CAN BE EXECUTED
104
YES
NO
DEACTIVATE ACTIVE ACCESS CONTROL CLIENT
106
IGNORE REQUEST
108
ACTIVATE INACTIVE ACCESS CONTROL CLIENT
110
SYNCHRONIZE WITH NETWORK
112
END
100

FIG. 1

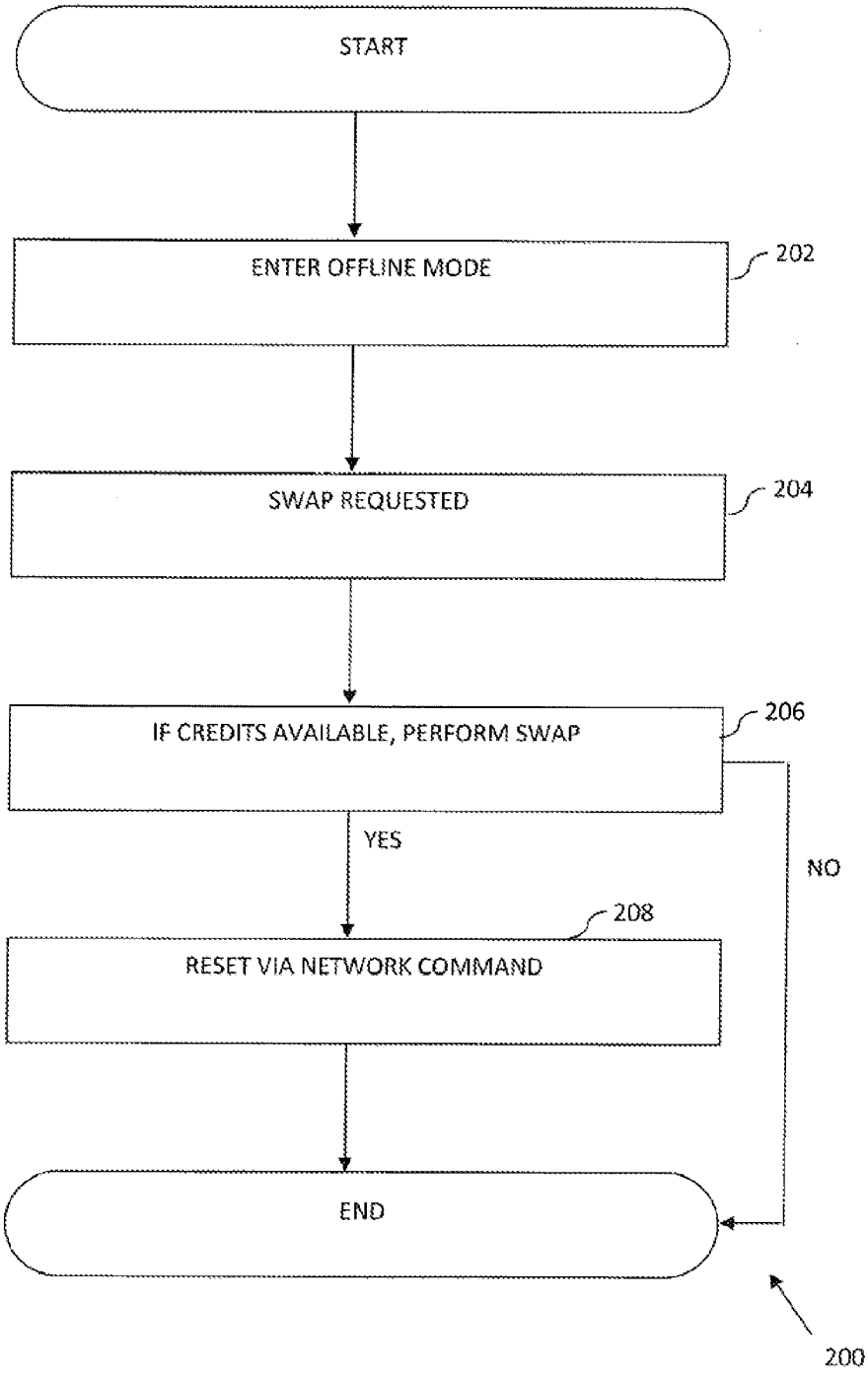

START
ENTER OFFLINE MODE
202
SWAP REQUESTED
204
IF CREDITS AVAILABLE, PERFORM SWAP
206
YES
NO
208
RESET VIA NETWORK COMMAND
END
200

FIG. 2

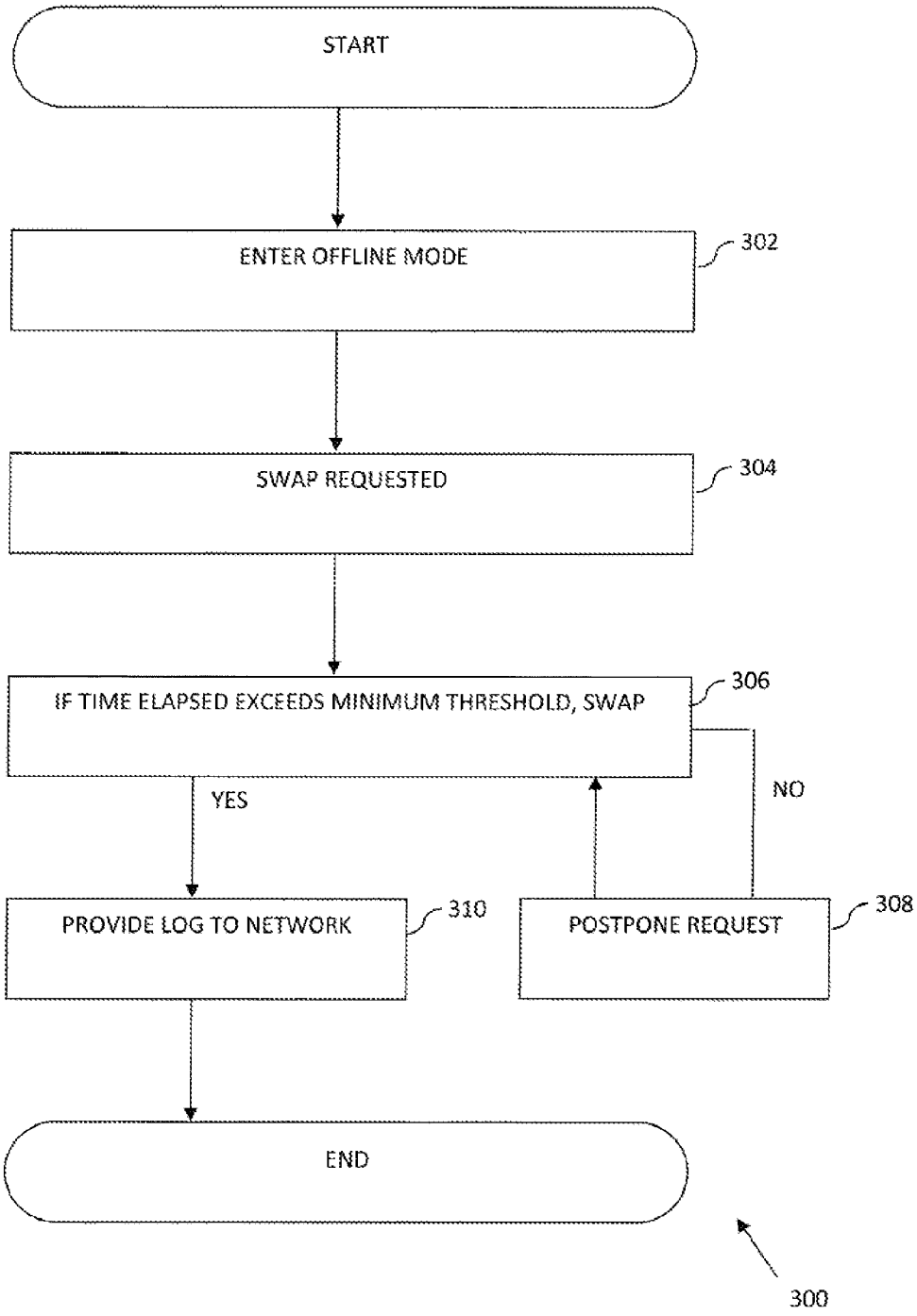

START
ENTER OFFLINE MODE
302
SWAP REQUESTED
304
IF TIME ELAPSED EXCEEDS MINIMUM THRESHOLD, SWAP
306
YES
NO
PROVIDE LOG TO NETWORK
310
POSTPONE REQUEST
308
END
300

FIG. 3

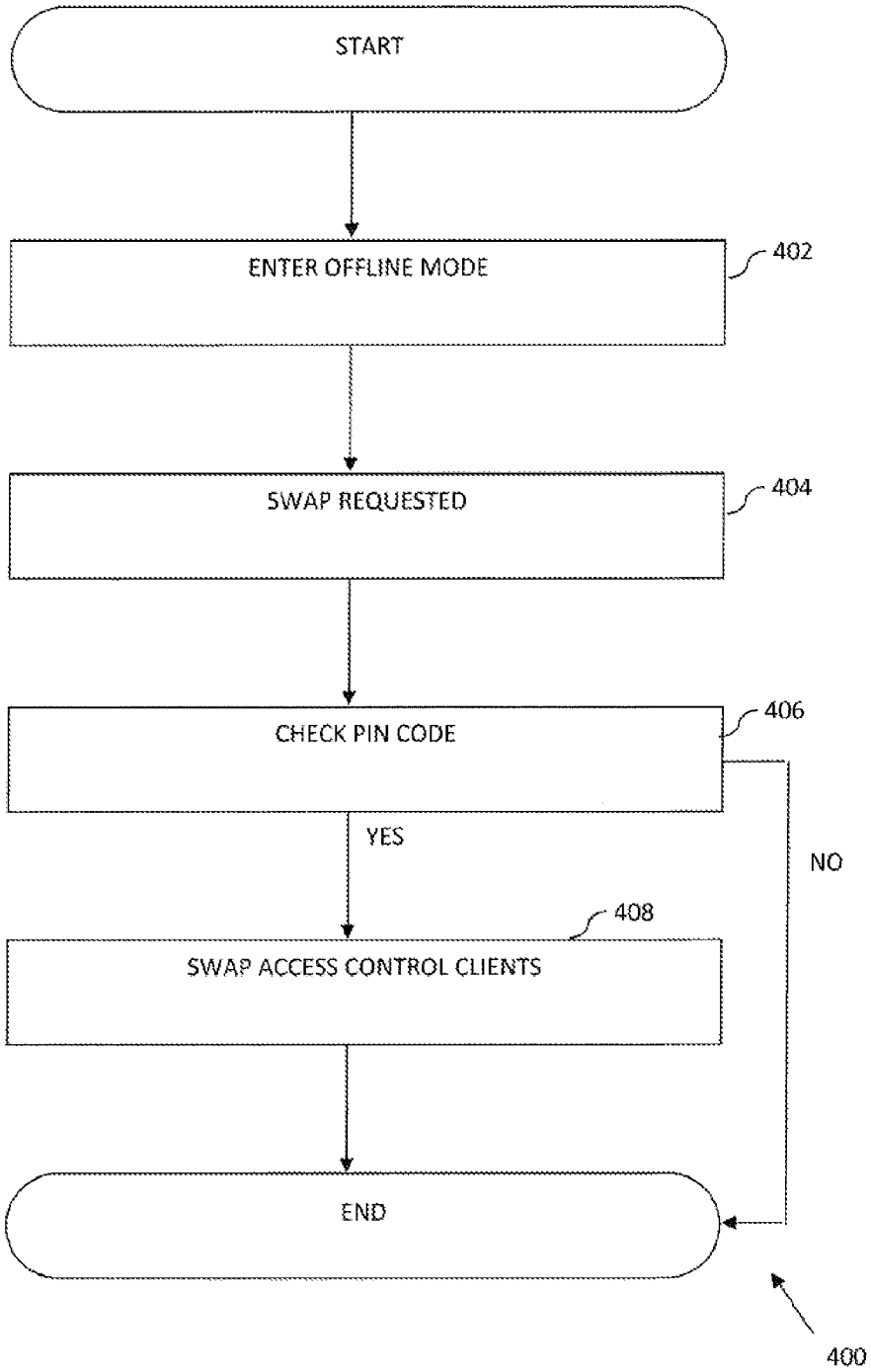

START
ENTER OFFLINE MODE
402
SWAP REQUESTED
404
CHECK PIN CODE
406
YES
NO
408
SWAP ACCESS CONTROL CLIENTS
END
400

FIG. 4A

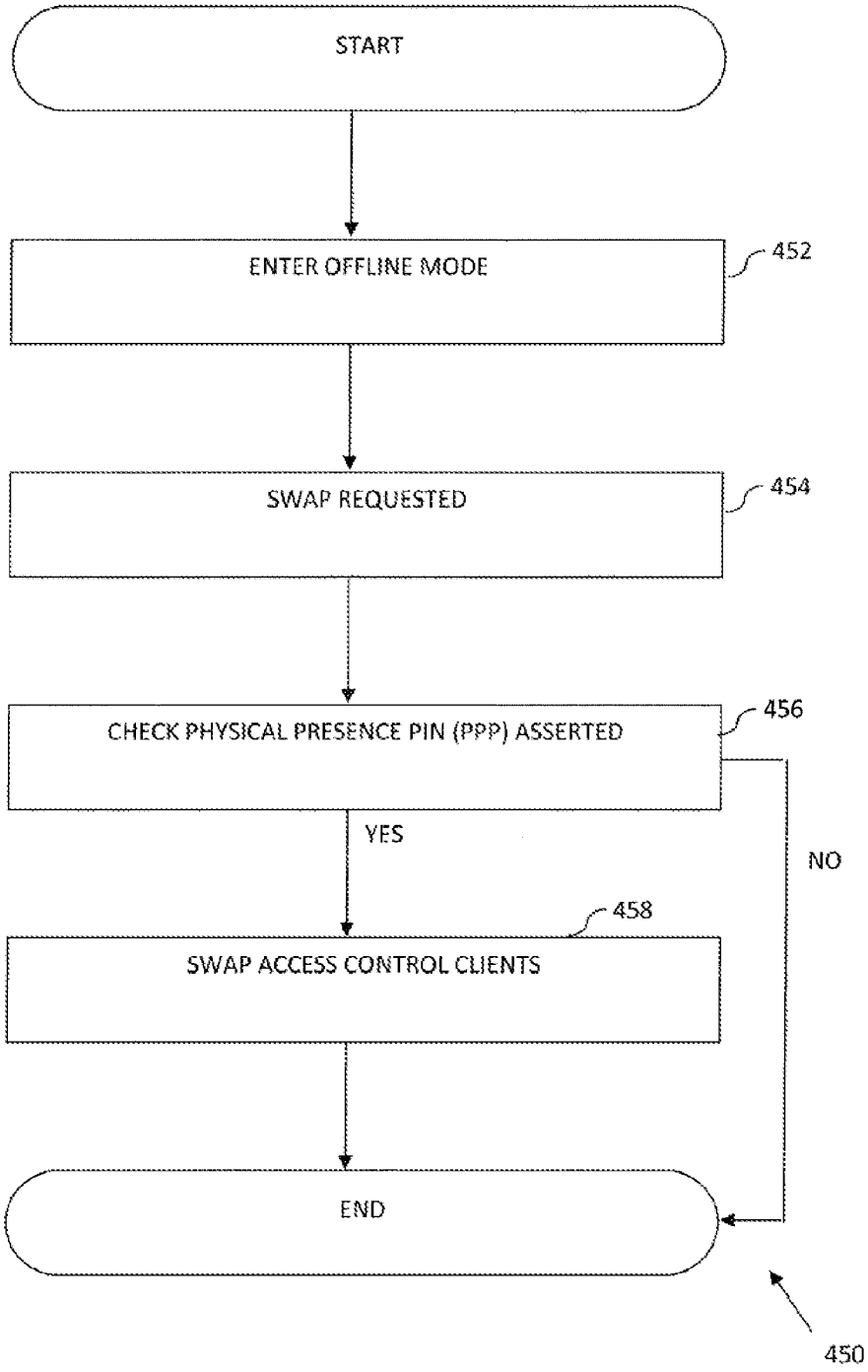

START
ENTER OFFLINE MODE
452
SWAP REQUESTED
454
CHECK PHYSICAL PRESENCE PIN (PPP) ASSERTED
456
YES
NO
458
SWAP ACCESS CONTROL CLIENTS
END
450

FIG. 4B

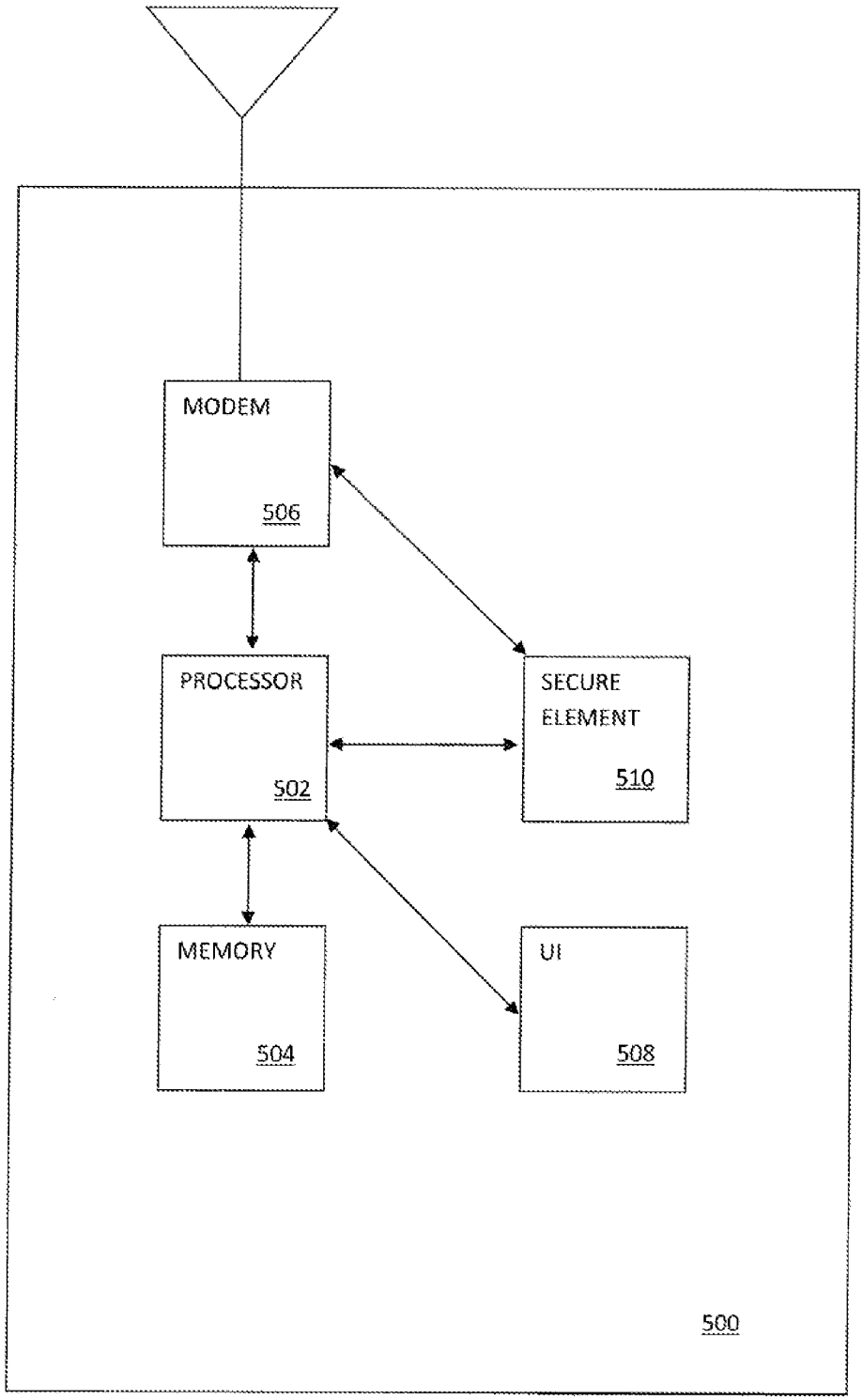

MODEM
506
PROCESSOR
502
SECURE
ELEMENT
510
MEMORY
504
UI
508
500

FIG. 5

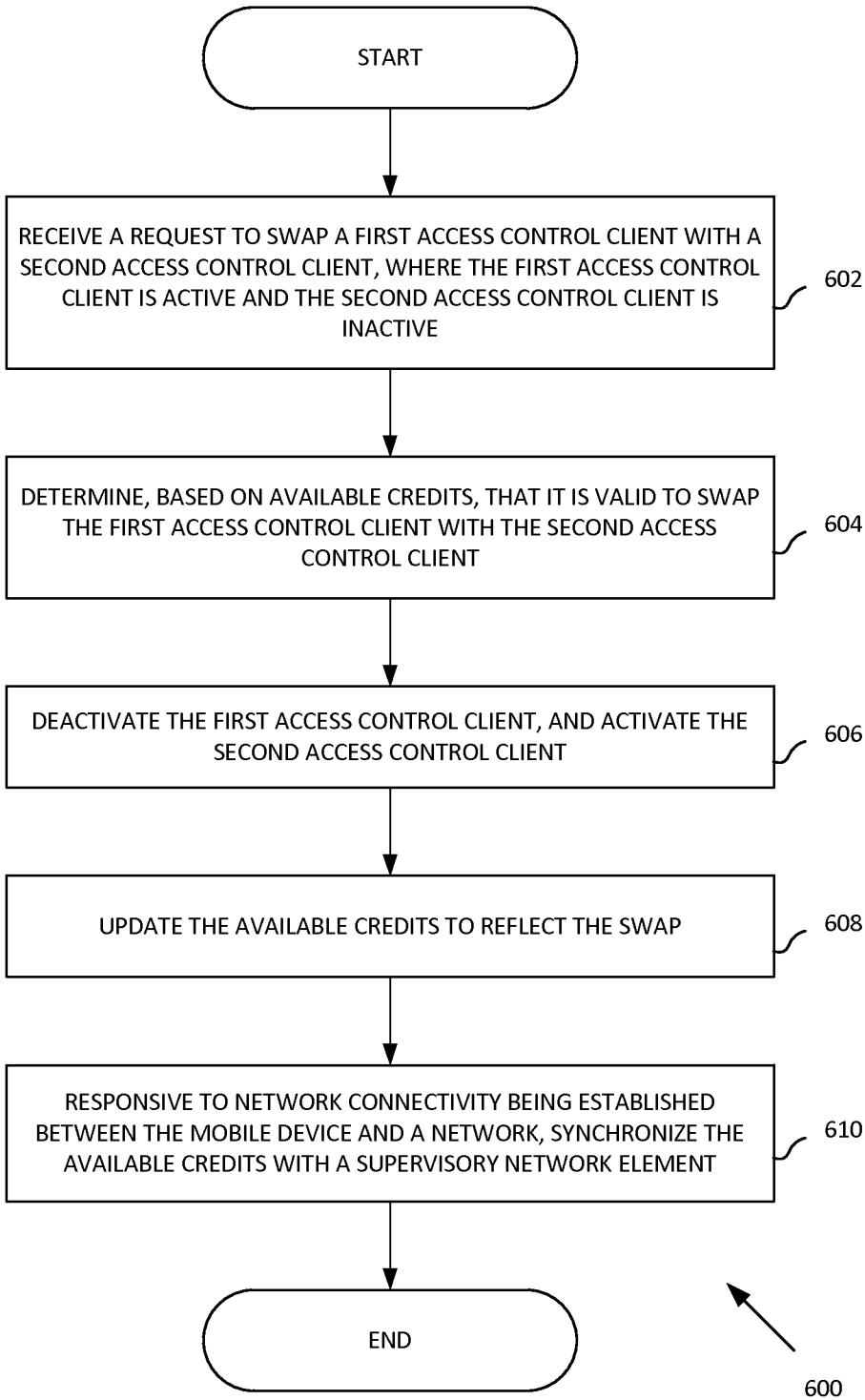

START
RECEIVE A REQUEST TO SWAP A FIRST ACCESS CONTROL CLIENT WITH A SECOND ACCESS CONTROL CLIENT, WHERE THE FIRST ACCESS CONTROL CLIENT IS ACTIVE AND THE SECOND ACCESS CONTROL CLIENT IS INACTIVE
602
DETERMINE, BASED ON AVAILABLE CREDITS, THAT IT IS VALID TO SWAP THE FIRST ACCESS CONTROL CLIENT WITH THE SECOND ACCESS CONTROL CLIENT
604
DEACTIVATE THE FIRST ACCESS CONTROL CLIENT, AND ACTIVATE THE SECOND ACCESS CONTROL CLIENT
606
UPDATE THE AVAILABLE CREDITS TO REFLECT THE SWAP
608
RESPONSIVE TO NETWORK CONNECTIVITY BEING ESTABLISHED BETWEEN THE MOBILE DEVICE AND A NETWORK, SYNCHRONIZE THE AVAILABLE CREDITS WITH A SUPERVISORY NETWORK ELEMENT
610
END
600

FIG. 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2013/061011

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/06(2009.01)i, H04W 88/02(2009.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04W 12/06; H04W 28/08; H04W 88/02

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & Keywords:active, inactive, credit, wireless networks

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2011-142786 A1 (SYMBOL TECHNOLOGIES, INC. et al.) 17 November 2011 See abstract; claims 1-5.	1-20
A	CARL EKLUND et al., "IEEE Standard 802.16: A Technical Overview of the WirelessMAN™ Air Interface for Broadband Wireless Access," IEEE Communications Magazine, June 2002 See abstract; page 98, right col., lines 7 - 28.	1-20

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

☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of 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
25 November 2013 (25.11.2013)	**09 December 2013 (09.12.2013)**
Name and mailing address of the ISA/KR 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 LEE, Seoung Young Telephone No. +82-42-481-8591

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2013/061011

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2011-142786 A1	17/11/2011	CN 102893653 A	23/01/2013
		EP 2569975 A1	20/03/2013
		US 2011-0280118 A1	17/11/2011