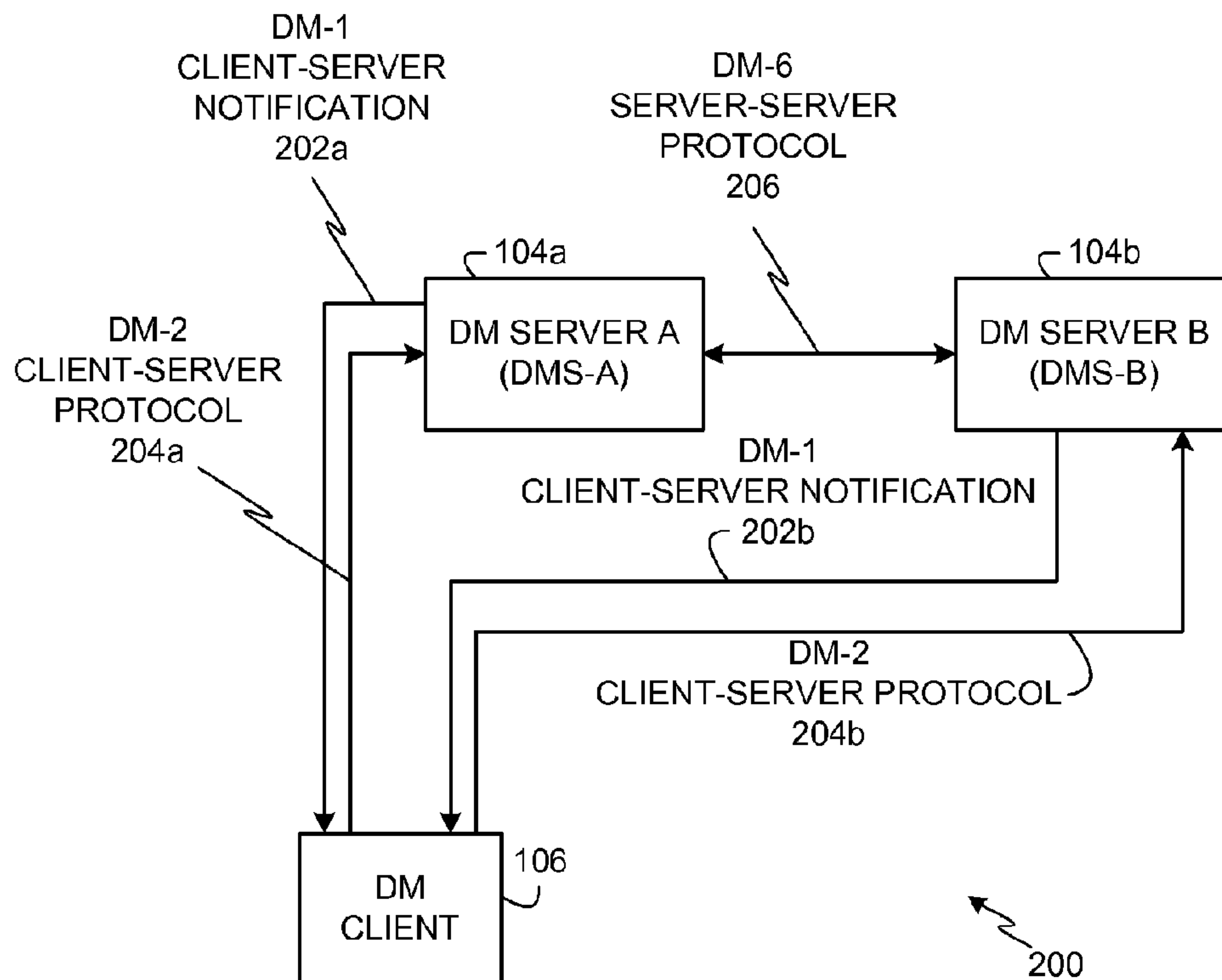




(86) Date de dépôt PCT/PCT Filing Date: 2011/03/24
 (87) Date publication PCT/PCT Publication Date: 2011/10/06
 (45) Date de délivrance/Issue Date: 2016/05/17
 (85) Entrée phase nationale/National Entry: 2012/09/27
 (86) N° demande PCT/PCT Application No.: US 2011/029822
 (87) N° publication PCT/PCT Publication No.: 2011/123329
 (30) Priorité/Priority: 2010/04/01 (US61/320,125)

(51) Cl.Int./Int.Cl. *H04L 12/24* (2006.01),
G06F 9/445 (2006.01), *H04L 29/08* (2006.01),
H04W 8/24 (2009.01), *H04W 12/06* (2009.01),
H04L 29/06 (2006.01), *H04W 12/08* (2009.01)
 (72) Inventeurs/Inventors:
 FERRAZZINI, AXEL, BE;
 CARTER, JASON LEE, US;
 GISBY, DOUGLAS MICHAEL, US;
 HOLMES, JOHN FRANCIS, US;
 LOPEZ, RICHARD ENRIQUE, US;
 PARRY, THOMAS OWEN, CA;
 ALFANO, NICHOLAS PATRICK, GB
 (73) Propriétaire/Owner:

(54) Titre : PROCÉDES ET APPAREIL PERMETTANT DE TRANSFERER LE CONTROLE DE GESTION D'UN CLIENT ENTRE DES SERVEURS
 (54) Title: METHODS AND APPARATUS TO TRANSFER MANAGEMENT CONTROL OF A CLIENT BETWEEN SERVERS



(57) **Abrégé/Abstract:**

An example method to be performed by an Open Mobile Alliance (OMA) Device Management (DM) server (104a) involves participating in mutual authentication (406) with a second OMA DM server (104b) and sending (408) a notification to the second OMA DM server (104b) for notifying the second OMA DM server (104b) to proceed with a delegation process. In addition, information (424) is sent to a DM client (106) for modifying an access control list (ACL).

(73) Propriétaires(suite)/Owners(continued):BLACKBERRY LIMITED, CA

(74) Agent: RIDOUT & MAYBEE LLP

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

(19) World Intellectual Property Organization
International Bureau(43) International Publication Date
6 October 2011 (06.10.2011)(10) International Publication Number
WO 2011/123329 A1

(51) International Patent Classification:

H04L 12/24 (2006.01) *H04L 29/06* (2006.01)
G06F 9/445 (2006.01) *H04W 12/08* (2009.01)
H04L 29/08 (2006.01) *H04W 12/06* (2009.01)
H04W 8/24 (2009.01)

(21) International Application Number:

PCT/US2011/029822

(22) International Filing Date:

24 March 2011 (24.03.2011)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

61/320,125 1 April 2010 (01.04.2010) US

(71) Applicant (for all designated States except US): **RESEARCH IN MOTION LIMITED** [CA/CA]; 295 Phillip Street, Waterloo, Ontario N2L 3W8 (CA).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **FERRAZZINI, Axel** [FR/BE]; 47 Rue Forestiere, B-1050 Brussels (BE). **CARTER, Jason, Lee** [US/US]; 68122-1200 Sawgrass

Corporate Parkway, Sunrise, FL 33323 (US). **GISBY, Douglas, Michael** [GB/US]; 66126-2550 West Golf Road, Rolling Meadows, IL 60008 (US). **HOLMES, John, Francis** [US/US]; 68124-1200 Sawgrass Corporate Parkway, Sunrise, FL 33323 (US). **LOPEZ, Ricard, Enrique** [US/US]; 68121-1200 Sawgrass Corporate Parkway, Sunrise, FL 33323 (US). **PARRY, Thomas, Owen** [CA/CA]; 72813-295 Phillip Street, Waterloo, Ontario, N2L 3W8 (CA). **ALFANO, Nicholas, P.** [CA/GB]; 44 Shelley Road, Stratford-Upon-Avon, WA CV37 7JS (GB).

(74) Agent: **HERNANDEZ, Felipe**; Hanley, Flight & Zimmerman, LLC, 150 S. Wacker Drive, Suite 2100, Chicago, IL 60606 (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, 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, KM, 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, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD,

[Continued on next page]

(54) Title: METHODS AND APPARATUS TO TRANSFER MANAGEMENT CONTROL OF A CLIENT BETWEEN SERVERS

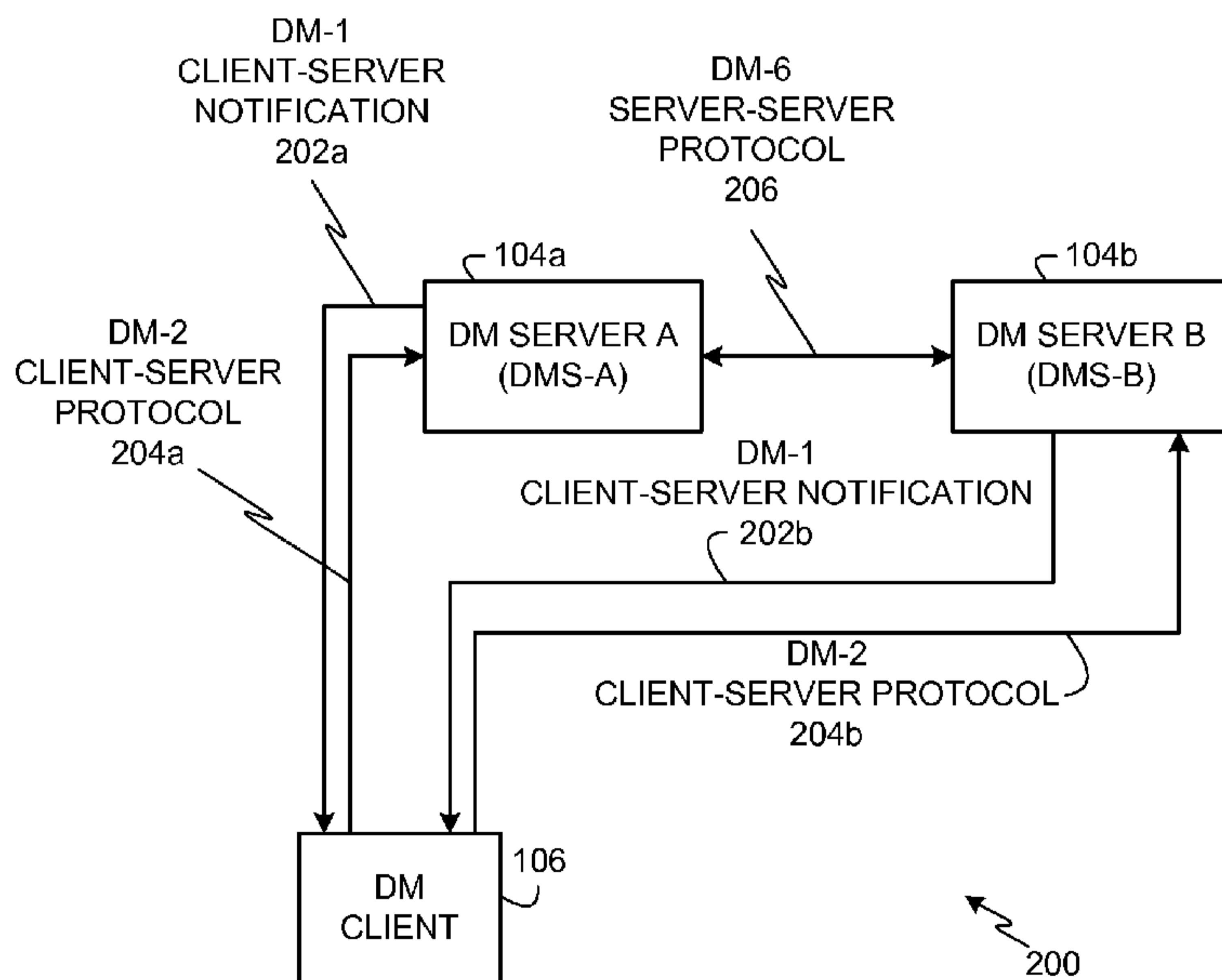


FIG. 2

(57) Abstract: An example method to be performed by an Open Mobile Alliance (OMA) Device Management (DM) server (104a) involves participating in mutual authentication (406) with a second OMA DM server (104b) and sending (408) a notification to the second OMA DM server (104b) for notifying the second OMA DM server (104b) to proceed with a delegation process. In addition, information (424) is sent to a DM client (106) for modifying an access control list (ACL).

WO 2011/123329 A1 

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, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, 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, ML, MR, NE, SN, TD, TG).

Published:

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

METHODS AND APPARATUS TO TRANSFER MANAGEMENT CONTROL
OF A CLIENT BETWEEN SERVERS

FIELD OF THE DISCLOSURE

[0002] The present disclosure relates generally to network communications and, more particularly, to methods and apparatus to transfer management control of a client between servers.

BACKGROUND

[0003] Mobile communications enable devices and/or users to communicate with one another through one or more wireless communication protocols using one or more services. In some mobile communication systems, mobile device services or operations are managed by service providers. For example, a service provider can provision client mobile devices for device management by one or more management servers of that service provider. The Open Mobile Alliance (OMA) group develops and defines guidelines or standards for implementing such server-client management relationships.

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] FIG. 1 depicts example mobile communication networks with device management servers that can implement device management control over a device management client in a mobile device.

[0005] FIG. 2 is an example communication architecture between two device management servers and a device management client showing different notification and protocol interfaces that can be used to implement the delegation processes of FIGS. 4, 5A, 5B, 6, and 7.

[0006] FIG. 3 is an example delegation type data structure that references several delegation types that can be used to specify the scope and type of device management control that can be delegated between device management servers.

[0007] FIG. 4 depicts example signaling exchanges between the device management servers and a device management client of FIGS. 1 and 2 to implement a delegation process to delegate control over the device management client from one device management server to another device management server.

[0008] FIGS. 5A and 5B depict a flow diagram representative of an example process that may be implemented using computer readable instructions to implement a delegation process to delegate management of a device management client between device management servers.

[0009] FIG. 6 depicts a flow diagram representative of an example process that may be implemented using computer readable instructions to process delegation setup information by a device management client.

[0010] FIG. 7 depicts a flow diagram representative of an example process that may be implemented using computer readable instructions to process a temporary delegation key in a DM client.

[0011] FIG. 8 depicts a block diagram of an example computing device that can be used to implement the example methods and apparatus described herein.

DETAILED DESCRIPTION

[0012] Although the present application discloses example methods and apparatus including, among other components, software executed on hardware, it should be noted that such methods and apparatus are merely illustrative and should not be considered as limiting. For example, any or all of these hardware and software components could be embodied exclusively in hardware, exclusively in software, exclusively in firmware, or in any combination of hardware, software, and/or firmware. Accordingly, while example methods and apparatus are described herein, persons having ordinary skill in the art will readily appreciate that the examples provided are not the only ways to implement such methods and apparatus.

[0013] The example methods and apparatus described herein can be used to transfer device management (DM) control (or management) of a DM client between DM servers. That is, according to the example methods and apparatus, a DM server is configured to delegate the management of a DM client to another DM server. The example methods and apparatus described herein can be used in connection with mobile communication devices, mobile computing devices, or any other device capable of accessing information over a mobile communications network. Such devices, also referred to as user equipment (UE), clients, or terminals, may include mobile smart phones (e.g., a BlackBerry® smart phone), personal digital assistants (PDA), laptop/notebook/netbook/tablet computers, desktop computers, etc.

[0014] The example methods and apparatus described herein can be implemented in connection with the Open Mobile Alliance (OMA) specifications related to device management

(DM) processes, which, among other things, specify protocols and mechanisms to manage mobile devices including specifying configurations to access services and management of software on mobile devices. The example methods and apparatus may additionally or alternatively be implemented in connection with other specifications, methods, or techniques to manage services and software on mobile devices.

[0015] The example methods and apparatus described herein enable a DM server to pass DM control (i.e., management) of a DM client (full or partial control, temporarily or permanently) to one or more other DM servers when two or more DM servers are available to manage a single DM client. Such transfer of DM control is implemented using a delegation process described herein to pass or transfer full or partial control (which may be permanent or temporary) over a DM client from one DM server to one or more other DM servers. In this manner, management of a DM client can be delegated between DM servers when, for example, the DM client is geographically moved between areas covered or managed by different DM servers. For example, a mobile device (e.g., having a DM client) homed in Europe can be registered for management by a European DM server of a mobile communications service provider. When the mobile device is moved to another country (e.g., Canada), management of the mobile device can be delegated by the European DM server to a Canadian (or North American) DM server so that access to services and software associated with that mobile device can be managed by the Canadian (or North American) DM server while the mobile device is in Canada.

[0016] Such delegation of control can be used to significantly reduce the communications overhead required between a home DM server (e.g., the European DM server in the above example) and a roaming DM server (e.g., the Canadian DM server in the above example) when, for example, a mobile device (having a DM client) is moved to areas managed by other DM

servers. That is, in traditional device management systems, a roaming DM server communicates with a home DM server to ensure that management of a roaming mobile device is in accordance with policies enforced by the home DM server. In addition, the example methods and apparatus described herein can be used when a mobile device is permanently moved to a different area managed by a respective DM server so that a previous controlling DM server can permanently release control over the mobile device to the DM server of the new location.

[0017] The techniques described herein for delegating DM control between different DM servers involve signaling information or notification exchanges between a DM server delegator, a DM server delegatee, and a DM client. In particular, a DM server delegator is the DM server that is implementing DM control over or currently managing a DM client prior to transferring or delegating that control to the DM server delegatee. In the example implementations described herein, such transfer or delegation of management of the DM client can be initiated by the DM server delegatee or by the DM server delegator. During the delegation process, access control information and device management account information associated with the subject DM client can be updated or created to establish permissions regarding how DM control over the DM client is to be implemented. In addition, the delegation process can be of a particular scope or type, such as, full or partial control, for a temporary or permanent duration. To ensure that the delegation is secure, a temporary delegation key can be generated and shared between the DM server delegator, the DM server delegatee, and the DM client. Such a security key can be used to prevent accidental or intentional hijacking of DM control over a DM client by, for example, a third party or any other entity.

[0018] Turning to FIG. 1, example mobile communication networks A 102a, B 102b, and C 102c (e.g., cellular or other wireless networks) include or are associated with respective DM

servers A 104a, B 104b, and C 104c that can implement DM control over (i.e., manage) a DM client 106 of a mobile device 108. In the illustrated example, the DM client 106 is a software component in the mobile device 108 (e.g., a managed device) that interprets commands, executes appropriate actions in the mobile device 108 and sends back relevant responses to an issuing management server (e.g., one of the DM servers 104a, 104b, and 104c). Also in the illustrated example, a DM server is a software component, which is configured to execute on a network device such as a server computer, that issues management commands to DM clients. In some example implementations, each of the DM servers 104a-c manages devices in a respective geographic area (e.g., in a respective country, territory, state, etc.) or for a respective network operator (e.g., entities that operate/manage or are otherwise associated with networks A, B, and C 102a-c). Additionally or alternatively, other partitioning or distribution of control responsibilities among the DM servers 104a-c can be used.

[0019] When the DM server A 104a is implementing DM control over the mobile device 108 to manage the device, and the mobile device 108 is moved to another geographic location managed by the DM server B 104b or the DM server C 104c, a delegation process is initiated in which the DM server A 104a operates as the DM server delegator and the DM server B 104b or the DM server C 104c operates as the DM server delegatee to receive management over the DM client 106. In some example implementations, a DM server delegator can transfer control over or management of a DM client to two or more DM server delegatees. For example, the DM server A 104a can delegate management of the DM client 106 to the DM server B 104b and the DM server C 104c, such that the DM servers 104b-c can share control over the DM client 106. In such an example, each of the DM servers 104b-c can receive partial control capabilities delegated by the DM server A 104a such that the combination of the DM servers 104b-c form

full control over the DM client 106. Example signaling exchanges between DM servers and a DM client are depicted in FIG. 4. In addition, FIGS. 5A, 5B, 6, and 7 depict example processes that can be used to exchange and process the information depicted in FIG. 4 to transfer management between DM servers.

[0020] Turning to FIG. 2, an example communication architecture 200 between the DM server A 104a, the DM server B 104b, and the DM client 106 is shown in connection with different notification and protocol interfaces that can be used to implement the delegation processes of FIGS. 4, 5A, 5B, 6, and 7. In the illustrative example of FIG. 2, the DM server A 104a is the delegator or delegating server and the DM server B 104b is the delegatee server. As shown, the DM servers A 104a and B 104b communicate with the DM client 106 using DM-1 client-server notification interfaces 202a-b, and the DM client 106 communicates with the DM server A 104a and the DM server B 104b using DM-2 client-server protocol interfaces 204a-b.

[0021] In the illustrated example of FIG. 2, the DM-1 client-server notification interfaces 202a-b are bearer neutral and can operate over different protocols such as wireless application protocol (WAP) push, short message service (SMS), HTTP, and session initiation protocol (SIP) push. The DM servers 104a-b can use the DM-1 client-server notification interfaces 202a-b to send device management notifications to DM clients.

[0022] In the illustrated example of FIG. 2, the DM-2 client-server protocol interfaces 204a-b can be used by the DM servers 104a-b to send device management commands to the DM client 106 and can be used by the DM client 106 to return status and alerts to the DM servers 104a-b. The DM-2 client-server protocol interfaces 204a-b are bearer neutral and provide standardized bindings including hypertext transfer protocol (HTTP) and secure HTTP (HTTPS). The DM-2 client-server protocol interfaces 204a-b may be exposed over an airlink-based data bearer

protocol (e.g., general packet radio service (GPRS)) to provide over-the-air device management capability.

[0023] Example requirements and capabilities of the DM-1 client-server notification interfaces 202a-b and the DM-2 client-server protocol interfaces 204a-b can be found in the OMA specifications related to device management processes. However, changes in the information exchanged via the DM-1 client-server notification interfaces 202a-b and the DM-2 client-server protocol interfaces 204a-b, as discussed below in connection with FIG. 4, enable implementing delegation processes to transfer or delegate management between different DM servers using the example methods and apparatus described herein.

[0024] Also shown in FIG. 2 is a DM-6 server-server protocol interface 206 used to exchange management commands and responses between the DM server A 104a and the DM server B 104b to, for example delegate or transfer DM control. The DM-6 server-server protocol interface 206 is bearer neutral and provides standardized bindings including HTTP and HTTPS. Preferably, but not necessarily, HTTPS can be used for security reasons. Signaling and information exchanged between the DM servers 104a-b via the DM-6 server-server protocol 206 are described below in connection with FIGS. 4, 5A, 5B, 6, and 7.

[0025] Turning briefly to FIG. 3, an example delegation type data structure 300 references several delegation types that can be used to specify the scope and type of DM control that is delegated between DM servers (e.g., the DM servers 104a-c of FIG. 1). In the illustrated example, each of the delegation types is an enumerated type. Although only unrestricted (e.g., full control), restricted (e.g., partial control), permanent, and temporary delegation types are shown, the delegation types can be extended and further enumerated to specify additional delegation types. One or more of the delegation types may be used to delegate a type of

management to another DM server. For example, the DM server A 104a may delegate an unrestricted and permanent type of management for a mobile device (e.g., the mobile device 108) that is permanently being relocated to another geographic location. In some example implementations, the delegation types shown in the delegation type data structure 300 can be stored in DM account management objects (DMAcc MOs) and/or associated access control lists (ACLs) (described below) based on the types of management responsibilities being delegated.

[0026] FIG. 4 depicts example signaling exchanges between the DM server A 104a, the DM server B 104b, and the DM client 106 of FIGS. 1 and 2 to implement a process to delegate management of the DM client 106 from the DM server A 104a to the DM server B 104b. In the illustrative example of FIG. 4, the DM server A 104a operates as the DM server delegator and the DM server B 104b operates as the DM server delegatee to receive management responsibility from the DM server A 104a to manage the DM client 106. The DM servers 104a-b use the DM client 106, a DM management tree object, a DM account management object (DMAcc MO), and associated access control lists (ACLs) to transfer control over the DM client 106 from the DM server A 104a to the DM server B 104b.

[0027] The structures and syntaxes of DM management tree objects, DMAcc MOs, and ACLs are specified in the OMA specifications related to device management processes. In example implementations associated with OMA DM, each device (e.g., the mobile device 108 of FIG. 1) that supports OMA DM contains or stores a management tree for a DM client of the device. The management tree organizes the available management objects (MOs) in the device as nodes in a hierarchical tree structure where each of the nodes can be uniquely addressed with a universal resource identifier (URI). Each node can be manipulated (or nodes can be added or removed) by a DM server (e.g., one of the DM servers 104a-c of FIG. 1) using management

actions carried over an OMA DM protocol (e.g., the DM-1 client-server protocol interface 202a-b of FIG. 2). During runtime, a DM server can explore a management tree of a DM client using a GET command and extend or otherwise modify the management tree using ADD or REPLACE commands. In addition, a DM client can extend its management tree based on user input or in response to attachment of an accessory (e.g., a removable memory, an I/O add-on, etc.) to the device.

[0028] Devices compliant with OMA DM (e.g., the mobile device 108 of FIG. 1) support DMAcc MOs to store settings for communications via a DM protocol (e.g., the DM-2 client-server protocol interfaces 204a-b of FIG. 2) with or by the DM client (e.g., the DM client 106). Such settings include login credentials that the DM client uses to authorize access by DM servers. In the illustrated examples described herein, when a DM server delegator (e.g., the DM server A 104a) transfers or delegates management of a DM client (e.g., the DM client 106) to one or more DM server delegatees (e.g., the DM server B 104b), the DM server delegator creates a new DMAcc in the DM client to allow the DM server delegatee(s) to establish a DM control session with the DM client.

[0029] Devices compliant with OMA DM (e.g., the mobile device 108 of FIG. 1) also support ACLs. An ACL is a node property of a DM management tree object and is used to grant access rights to server identifiers of DM servers (e.g., the DM servers 104a-c of FIG. 1) to access a DM client (e.g., the DM client 106 of FIG. 1) or a specific node or nodes of the DM tree associated with a DM client. An ACL can grant access permissions to DM servers on a per-command basis. For example, to allow a particular command (e.g., open a DM control session) to be issued by the DM server B 104b to the DM client 106, an ACL of the DM client 106 associates the server identifier of the DM server B 104b to the particular command. Without the

server identifier of the DM server B 104b being associated or assigned to the command, the DM server B 104b is not authorized to issue the command to the DM client 106. During the delegation process of FIG. 4, the DM server A 104a can transfer or delegate management of the DM client 106 by modifying the ACL of the DM client 106. In this manner, the DM server B 104b is allowed to establish a DM control session with the DM client 106 to complete the transfer of DM control to the DM server B 104b.

[0030] For example implementations in which DM control over a DM client is transferred to multiple DM servers, the ACLs of the DM client can be updated to indicate a hierarchical control structure for the multiple DM servers to indicate the ordering of control priority (e.g., primary priority, secondary priority, tertiary priority, etc.) allocated to each of the DM servers. In addition, the ACLs of the DM client may be updated to indicate a default DM server. The priority and default information can be used by the DM client to communicate information to a DM server when it has multiple DM servers to choose from. In this manner, the DM client need not communicate the same information to more than one DM server to ensure that all of the DM servers are synchronized. Instead, the information communicated by the DM client to one of the DM servers can be synchronized to the other DM servers without involvement by the DM client for such synchronization.

[0031] In the illustrated example of FIG. 4, the depicted messages or signaling exchanges are communicated between the DM server A 104a, the DM server B104b, and/or the DM client 106 via respective ones of the DM-1 client-server notification interfaces 202a-b, the DM-2 client-server protocol interfaces 204a-b, and the DM-6 server-server protocol interface 206 of FIG. 2. In particular, the DM servers 104a-b use the DM-6 server-server protocol interface 206 (FIG. 2) to communicate between each other initialize delegation process signalings

[INIT_DELEGATION_PROC] 402 and 404, a mutual authentication exchange
[MUTUAL_AUTHENTICATION] 406, a start delegation process notification
[START_DELEGATION_PROC_NOTIFICATION] 408, a delegation success/fail notification
[DELEGATION_SUCCESS/FAIL_NOTIFICATION] 414, and a delegation success notification
[DELEGATION_SUCCESS_NOTIFICATION] 420.

[0032] The DM server A 104a communicates delegation setup information [DELEGATION_SETUP_INFO] 410 to the DM client 106 via the DM-1 client-server notification interface 202a (FIG. 2), and the DM client 106 communicates a delegation acknowledgement [DELEGATION_ACK] 412 to the DM server A 104a via the DM-2 client-server protocol interface 204a (FIG. 2). The DM server B 104a communicates an initialize DM session signaling [INIT_DM_SESSION] 416 to the DM client 106 via the DM-1 client-server notification interface 204b (FIG. 2), and the DM client 106 communicates a delegation success acknowledgement [DELEGATION_SUCCESS_ACK] 418 to the DM server B 104b via the DM-2 client-server protocol interface 204b (FIG. 2). As known in the art, one or both of signaling messages 416 and 418 relate to an operation referred to in OMA DM as “bootstrapping” the DM client 106.

[0033] The use of the messages or signaling exchanges depicted in the delegation process of FIG. 4 are described in more detail below in connection with the description of the example process of FIG. 5. In brief, the DM servers 104a-b connect and exchange information indicating that the DM server A 104a intends to transfer DM management control over the DM client 106 to the DM server B 104b. The delegation process can be initiated by the DM server delegator (e.g., the DM server A 104a in the illustrated example) as shown by the initialize delegation process (INIT_DELEGATION_PROC) signaling 402 communicated by the DM server A 104a

to the DM server B 104b, or the delegation process can be initiated by the DM server delegatee (e.g., the DM server B 104b in the illustrated example) as shown by the initialize delegation process (INIT_DELEGATION_PROC) signaling 404 communicated by the DM server B 104b to the DM server A 104a. In either case, the sending of the initialize delegation process signaling 402 or 404 can be triggered upon detection that the DM client 106 has registered or is attempting to register with the DM server B 104b. For example, the DM client 106 may be associated with a mobile subscriber plan having a roaming feature (e.g., international roaming, national roaming, or any other regional roaming feature) such that the DM client 106 is allowed to register with and operate while in communication with DM servers outside of its home area.

[0034] The DM server A 104a communicates message 410 to the DM client 106 and uses a DMAcc mod field 422 to create a new DM account management object (DMAcc MO) in the DM client 106 for the DM server B 104b if one does not exist. In the illustrated example, the DM server A 104a uses the DMAcc mod field 422 to populate the DMAcc MO with credentials that allow the DM server B 104b to establish a DM control session with the DM client 106. In addition, the DM server A 104a may use an ACL mod field 424 to add the server identifier of the DM server B 104b to ACLs of the DM client 106 for which the DM server A 104a would like to transfer management control to the DM server B 104b. The DM server A 104a also sends one or more delegation type identifiers (e.g., one or more of the delegation type identifiers of the delegation type data structure 300 of FIG. 3) via a delegation type field 426 to the DM client 106 to inform the DM client 106 of the scope and type of management that is being delegated to the DM server B 104b.

[0035] To ensure a secure transfer of control to the DM server B 104b, the DM server A 104a generates and sends a temporary delegation key (TEMP_DELEGATION_KEY) in a

TEMP_DELEGATION_KEY field 428 to the DM client 106 along with an expiration value in an expiration field 430. The temporary delegation key is a unique key known only to the DM server A 104a, the DM server B 104b, and the DM client 106. The temporary delegation key may be time limited using the expiration value of the expiration field 430 to add further security and authentication to the delegation process. The expiration value may be a time-date stamp or any other value (e.g., a counter value, a timer value, etc.) indicative of when the temporary delegation key is no longer valid for use by the DM server B 104b for connecting to the DM client 106.

[0036] In some example implementations, to enable the DM client 106 to connect with the DM server B 104b, the DM server A 104a may also communicate network information or parameters to the DM client 106 for use by the DM client 106 for connecting with the DM server B 104b. Such network information can be communicated in the DMAcc mod field 422 or a separate field (e.g., a network field) (not shown) of the delegation setup information message [DELEGATION_SETUP_INFO] 410 and can include, for example, an access point name (APN) and/or other type of network information to enable the DM client 106 to connect to the DM server B 104b. The network information may be stored in a 'ToConRef' branch and/or a 'PreConRef' node of a DMAcc MO.

[0037] The DM server A 104a notifies the DM server B 104b that it has made the DM client 106 ready so that the DM server B 104b may connect to it and establish partial or full control over the DM client 106. In the illustrated example, the DM server A 104a sends the DM server B 104b ACL information in an ACL field 434 indicative of the access control permissions assigned to the DM server B 104b in the DM client 106. The DM server A 104a also sends the DM server B 104b the one or more delegation type identifiers in a delegation type field 436 that

were also sent to the DM client 106 in the delegation type field 410. The DM server A 104a also sends the DM server B 104b the temporary delegation key shared with the DM client 106 and the expiration value for the key in a TEMP_DELEGATION_KEY field 438 and an expiration field 440.

[0038] In response, the DM server B 104b connects to the DM client 106 forwarding the temporary delegation key in a TEMP_DELEGATION_KEY field 444, verifies it has control over some or all of the DM client 106, and begins management of the DM client 106. The DM server B 104b may communicate to the DM server A 104a that it has successfully completed the control allocation mechanism to establish management over the DM client 106.

[0039] FIGS. 5A, 5B, 6, and 7 depict example flow diagrams representative of processes that may be implemented using, for example, computer readable instructions that may be used to transfer or delegate management of a DM client from one DM server to one or more other DM servers. The example processes of FIGS. 5A, 5B, 6, and 7 may be performed using a processor, a controller and/or any other suitable processing device. For example, the example processes of FIGS. 5A, 5B, 6, and 7 may be implemented using coded instructions (e.g., computer readable instructions) stored on a tangible computer readable medium known in the art such as optical or magnetic media, a flash memory, a read-only memory (ROM), and/or a random-access memory (RAM) or any other storage media (e.g., optical, magnetic, solid state, etc.) in which information is stored for any duration (e.g., for extended time periods, permanently, brief instances, for temporarily buffering, and/or for caching of the information). As used herein, the term tangible computer readable medium is expressly defined to include any type of computer readable storage medium and to exclude propagating signals.

[0040] Additionally or alternatively, the example processes of FIGS. 5A, 5B, 6, and 7 may be implemented using coded instructions (e.g., computer readable instructions) stored on a non-transitory computer readable medium such as a flash memory, a read-only memory (ROM), a random-access memory (RAM), a cache, or any other storage media in which information is stored for any duration (e.g., for extended time periods, permanently, brief instances, for temporarily buffering, and/or for caching of the information). As used herein, the term non-transitory computer readable medium is expressly defined to include any type of computer readable medium and to exclude propagating signals.

[0041] Alternatively, some or all of the example processes of FIGS. 5A, 5B, 6, and 7 may be implemented using any combination(s) of application specific integrated circuit(s) (ASIC(s)), programmable logic device(s) (PLD(s)), field programmable logic device(s) (FPLD(s)), discrete logic, hardware, firmware, etc. Also, some or all of the example processes of FIGS. 5A, 5B, 6, and 7 may be implemented manually or as any combination(s) of any of the foregoing techniques, for example, any combination of firmware, software, discrete logic and/or hardware. Further, although the example processes of FIGS. 5A, 5B, 6, and 7 are described with reference to the flow diagrams of FIGS. 5A, 5B, 6, and 7, other methods of implementing the processes of FIGS. 5A, 5B, 6, and 7 may be employed. For example, the order of execution of the blocks may be changed, and/or some of the blocks described may be changed, eliminated, sub-divided, or combined. Additionally, any or all of the example processes of FIGS. 5A, 5B, 6, and 7 may be performed sequentially and/or in parallel by, for example, separate processing threads, processors, devices, discrete logic, circuits, etc.

[0042] Turning in detail to FIGS. 5A and 5B, the example flow diagram depicts an example delegation process that can be used to delegate management of the DM client 106 from the DM

server A 104a to the DM server 104b as shown in FIG. 4. Initially, a DM server initiates a delegation process (block 502) (FIG. 5A). For example, as shown in FIG. 4, the delegation process can be initiated by the DM server A 104a (e.g., a DM server delegator) by sending the initialize delegation process (INIT_DELEGATION_PROC) signaling 402 to the DM server B 104b (e.g., a DM server delegatee). Alternatively, the delegation process can be initiated by the DM server B 104b (e.g., a DM server delegatee) by sending the initialize delegation process (INIT_DELEGATION_PROC) signaling 404 to the DM server A 104a (e.g., a DM server delegator). The INIT_DELEGATION_PROC signaling 402 or 404 includes a request, by the initiating server, for delegation information (e.g., delegation type, temporary delegation key, ACL permissions, etc.).

[0043] The DM servers 104a-b participate in a mutual authentication process (block 504) using, for example, the mutual authentication exchange [MUTUAL_AUTHENTICATION] 406 of FIG. 4. The mutual authentication process can be implemented using an agreed upon authentication method to confirm the identities of the DM servers 104a-b before proceeding with the delegation process. The DM server A 104a notifies the DM server B 104b of the start of the delegation process (block 506) using, for example, the start delegation process notification [START_DELEGATION_PROCESS_NOTIFICATION] 408 of FIG. 4.

[0044] The DM server A 104a sends the delegation setup information 410 (FIG. 4) to the DM client 106 (block 508). As shown in FIG. 4, the delegation setup information [DELEGATION_SETUP_INFO] 410 includes information in the DMAcc mod field 422, the ACL mod field 424, the delegation type field 426, the temporary delegation key field 428, and the expiration field 430 discussed above in connection with FIG. 4. As shown in FIG. 5, the DM

client 106 processes the delegation setup information 410 (block 510). An example process that may be used to implement block 510 is discussed below in connection with FIG. 6.

[0045] After processing the delegation setup information 410 at block 510, the DM client 106 acknowledges the delegation (block 512) by, for example, communicating the delegation acknowledgement [DELEGATION_ACK] 412 of FIG. 4 to the DM server A 104a. In the illustrated example, the delegation acknowledgement 412 can be a success acknowledgment or a failure acknowledgment to notify the DM server A 104a whether the DM client 106 has successfully implemented the changes instructed by the DM server A 104a via the delegation setup information [DELEGATION_SETUP_INFO] 410 of block 508 in preparation for transferring management of the DM client 106 to the DM server B 104b.

[0046] The DM server A 104a then notifies the DM server B 104b of the success or failure of the delegation process (block 514) (FIG. 5B) using, for example, the delegation success/fail notification [DELEGATION_SUCCESS/FAIL_NOTIFICATION] 414 of FIG. 4. If the delegation success/fail notification 414 is indicative of a success (block 516), the DM server A 104a also sends the delegation information discussed above in connection with FIG. 4 in the ACL field 434, the delegation type field 436, the TEMP_DELEGATION_KEY field 438, and the expiration field 440 to the DM server B 104b (block 518).

[0047] The DM server B 104b initiates a DM session with the DM client 106 using the delegation information (block 520) by, for example, communicating the initialize DM session signaling [INIT_DM_SESSION] 416 of FIG. 4 to the DM client 106. In particular, the DM server B 104b uses the ACL information to identify permissions in the new DMAcc MO of the DM client 106 allotted to the DM server B 104b. In addition, the DM server B 104b forwards

the temporary delegation key in the TEMP_DELEGATION_KEY field 444 of FIG. 4 of the initialize DM session signaling [INIT_DM_SESSION] 416.

[0048] The DM client 106 processes the temporary delegation key (block 522) to confirm that the DM server B 104b is authorized to establish DM control over the DM client 106. An example process that can be used to implement block 522 is discussed below in connection with FIG. 7. When the DM client 106 successfully confirms that the DM server B 104b is authorized to assume management of the DM client 106 (block 524), the DM client 106 acknowledges a success of the delegation (block 526) by, for example, sending the delegation success acknowledgement [DELEGATION_SUCCESS_ACK] 418 of FIG. 4 to the DM server B 104b. The DM server B 104b then notifies the DM server A 104a of the success of the delegation (block 528) by, for example, sending the delegation success notification [DELEGATION_SUCCESS_NOTIFICATION] 420 to the DM server A 104a. In some example implementations, if the delegation of management to the DM server B 104b is a permanent and full control delegation (block 530), the DM server B 104b can remove the DM server A 104a from the ACLs of the DM client 106 (block 532) and remove the DMAcc MO corresponding to the DM server A 104a from the DM client 106 (block 534). In this manner, only the DM server B 104b would have complete management of the DM client 106.

[0049] After the DM server B 104b removes the DMAcc MO corresponding to the DM server A 104a from the DM client 106 (block 534) or if the transferred DM control is not permanent and full control (block 530) or if the verification of the temporary delegation key was not successful (block 524) or if the delegation success/fail notification 414 from the DM server A 104a to the DM server B 104b is not indicative of a success (block 516), the example process of FIGS. 5A and 5B ends.

[0050] FIG. 6 depicts a flow diagram representative of an example process that may be used to process delegation setup information by the DM client 106 of FIGS. 1, 2, and 4. The example process of FIG. 6 may be used to implement block 510 of FIG. 5A to process delegation setup information (e.g., the delegation setup information [DELEGATION_SETUP_INFO] 410 of FIG. 4) at the DM client 106.

[0051] Initially, the DM client 106 parses the delegation setup information 410 (block 602) by, for example, identifying the respective information in the DMAcc mod field 422, the ACL mod field 424, the delegation type field 426, the temporary delegation key field 428, and the expiration field 430 shown in FIG. 4. The DM client 106 stores a DMAcc MO from the DMAcc mod field 422 (block 604) to enable the DM server B 104b to establish a DM control session with the DM client 106. In addition, the DM client 106 stores the ACLs associated with the DM server B 104b from the ACL mod field 424 of FIG. 4 (block 606) to attribute permissions for respective commands to the DM server B 104b.

[0052] The DM client 106 stores the delegation type information (block 608) from the delegation type field 426 of FIG. 4. In addition, the DM client 106 stores the temporary delegation key and the expiration value (block 610) from the TEMP_DELEGATION_KEY field 428 and the expiration field 430 of FIG. 4. In this manner, the DM client 106 can verify whether a DM server (e.g., the DM server B 104b) is authorized to establish a DM control session with it based on the temporary delegation key. If the operations of FIG. 6 were successfully completed (e.g., if the DM client 106 confirmed that the DM server A 104a had access permissions to instruct the DM client 106 in this fashion) (block 612), the DM client 106 indicates a successful completion of the operations of FIG. 6 (block 614) in preparation for the DM server A 104a to delegate management of the DM client 106 to the DM sever B 104b. Otherwise, the example

process of FIG. 6 ends without indicating a successful completion (e.g., indicating a failure) of the operations of FIG. 6. In either case, the example process of FIG. 6 ends and control returns to a calling process or function such as the example process of FIG. 5.

[0053] FIG. 7 depicts a flow diagram representative of an example process that may be used to process a temporary delegation key in the DM client 106. The example process of FIG. 7 can be used to implement block 522 of FIG. 5B to confirm that the temporary delegation key communicated by the DM server B 104b in the TEMP_DELEGATION_KEY field 444 of the initialize DM session signaling [INIT_DM_SESSION] 416 is valid and correct to allow the DM server B 104b to establish a DM control session with the DM client 106.

[0054] Initially, the DM client 106 receives the temporary delegation key (block 702) from, for example, the TEMP_DELEGATION_KEY field 444 of the initialize DM session signaling [INIT_DM_SESSION] 416. The DM client 106 determines whether the temporary delegation key is expired (block 704). For example, the DM client 106 can refer to the expiration value stored therein at block 610 of FIG. 6 to determine whether the valid duration of the temporary delegation key has not expired. In some example implementations, the DM client 106 can compare the expiration value to a time value of a real-time clock (e.g., the real-time clock 822 of FIG. 8). When the DM client 106 confirms that the temporary delegation key is not expired (block 706), the DM client 106 determines whether the received temporary delegation key matches its stored temporary delegation key (e.g., the temporary delegation key stored at block 610 of FIG. 6) (block 708). When the DM client 106 confirms a match between the received temporary delegation key and the stored temporary delegation key (block 710), the DM client 106 allows establishing a DM control session with the DM server B 104b (block 712). However, if the temporary delegation key is expired (block 706) or the received temporary delegation key

and the stored temporary delegation key do not match (block 710), the example process of FIG. 7 ends without allowing a DM control session to be established with the DM server B 104b. In any case, the example process of FIG. 7 ends and control returns to a calling function or process such as the example process of FIG. 5.

[0055] FIG. 8 depicts an example computing device 800. In some instances, the computing device 800 may be adapted and configured as a server device which implements a DM server (e.g., the DM servers 104a-c). In other instances, the computing device 800 of FIG. 8 may be configured as the mobile device 108 of FIG. 1 which implements a DM client (e.g., the DM client 106). In the illustrated example, the mobile device 800 includes a processor 802 that may be used to control the overall operation of the device 800. The processor 802 may be implemented using a controller, a general purpose processor, a digital signal processor, dedicated hardware, or any combination thereof.

[0056] The device 800 is provided with a FLASH memory 804, a random access memory (RAM) 806, and an expandable memory interface 808 communicatively coupled to the processor 802. The FLASH memory 804 can be used to, for example, store computer readable instructions and/or data. In some example implementations, the FLASH memory 804 can be used to store the delegation type data structure 300 of FIG. 3 and computer readable instructions to implement the DM client 106 or a DM server 104a-c of FIGS. 1, 2, and 4. The RAM 806 can also be used to, for example, store data and/or instructions. The device 800 is also provided with an external data I/O interface 810. The external data I/O interface 810 may be used by a user to transfer information to and from the device 800 through a wired medium.

[0057] The device 800 is provided with a communication subsystem 812 to enable communications with networks such as the mobile communication networks 102a-c of FIG. 1.

In the illustrated examples described herein, the communication subsystem 812 can be configured in accordance with a cellular communication standard. In other example implementations, the communication subsystem 812 can be implemented using an IEEE® 802.11 standard, a BLUETOOTH® radio, a ZIGBEE® device, a wireless USB device, or an ultra-wideband (UWB) radio (e.g., WiMax). However, the communication subsystem 812 may also facilitate wired communications between the device 800 and a local area network (LAN) and the like.

[0058] To enable a user to use and interact with or via the device 800 when it is configured as the mobile device 108, the device 800 is provided with a speaker 814, a microphone 816, a display 818, and a user input interface 820. The display 830 can be an LCD display, an e-paper display, etc. The user input interface 820 could be an alphanumeric keyboard and/or telephone-type keypad, a multi-direction actuator or roller wheel with dynamic button pressing capability, a touch panel, etc. As discussed above, the example methods and apparatus described herein can also be advantageously used in connection with wireless terminals that do not have user interfaces and, thus, the speaker 814, the microphone 816, the display 818, the user input interface 820, and/or any combination thereof may be optionally omitted.

[0059] The device 800 is also provided with a real-time clock (RTC) 822 to track dates and a current time of day and/or to implement time-based and/or date-based operations (e.g., identifying the expiration of temporary delegation key). In the illustrated example, the device 800 is a battery-powered device and is, thus, provided with a battery 824 and a battery interface 826. However, the device 800 may receive voltage and current via another source such as direct current or alternating current power outlets and the like.

[0060] Although certain methods, apparatus, and articles of manufacture have been described herein, the scope of coverage of this disclosure is not limited thereto. To the contrary, this disclosure covers all methods, apparatus, and articles of manufacture fairly falling within the scope of the claims either literally or under the doctrine of equivalents.

What is Claimed is:

1. A method performed by an Open Mobile Alliance, OMA, Device Management, DM, server, the method comprising:

 sending a first message to a second OMA DM server, wherein the first message initiates delegation with respect to a client;

 creating or modifying an OMA Device Management Account, DMAcc, and/or a DM management tree Access Control List, ACL, in the client to set a node property with an identifier of the second server; and

 receiving a second message from the second server, wherein the second message indicates success of the delegation.

2. The method of claim 1, wherein the first message initiates the delegation with the second OMA DM server.

3. The method of claim 1, wherein the server uses an interface to send communications directly to the second server, the communications referring to delegation setup information.

4. The method of any one of claims 1 to 3 wherein the delegation is specified by a delegation type, and optionally sending the delegation type to the second OMA DM server, and further optionally wherein the delegation type is one of full delegation or partial delegation, and one of temporary delegation or permanent delegation.

5. A computer-readable storage medium storing instructions which, when executed by a processor of a device, cause the device to perform the operations of any one of claims 1 to 4.

6. A network device comprising a processor configured to execute an Open Mobile Alliance, OMA, Device Management, DM, server that performs the operations of any one of claims 1 to 4.

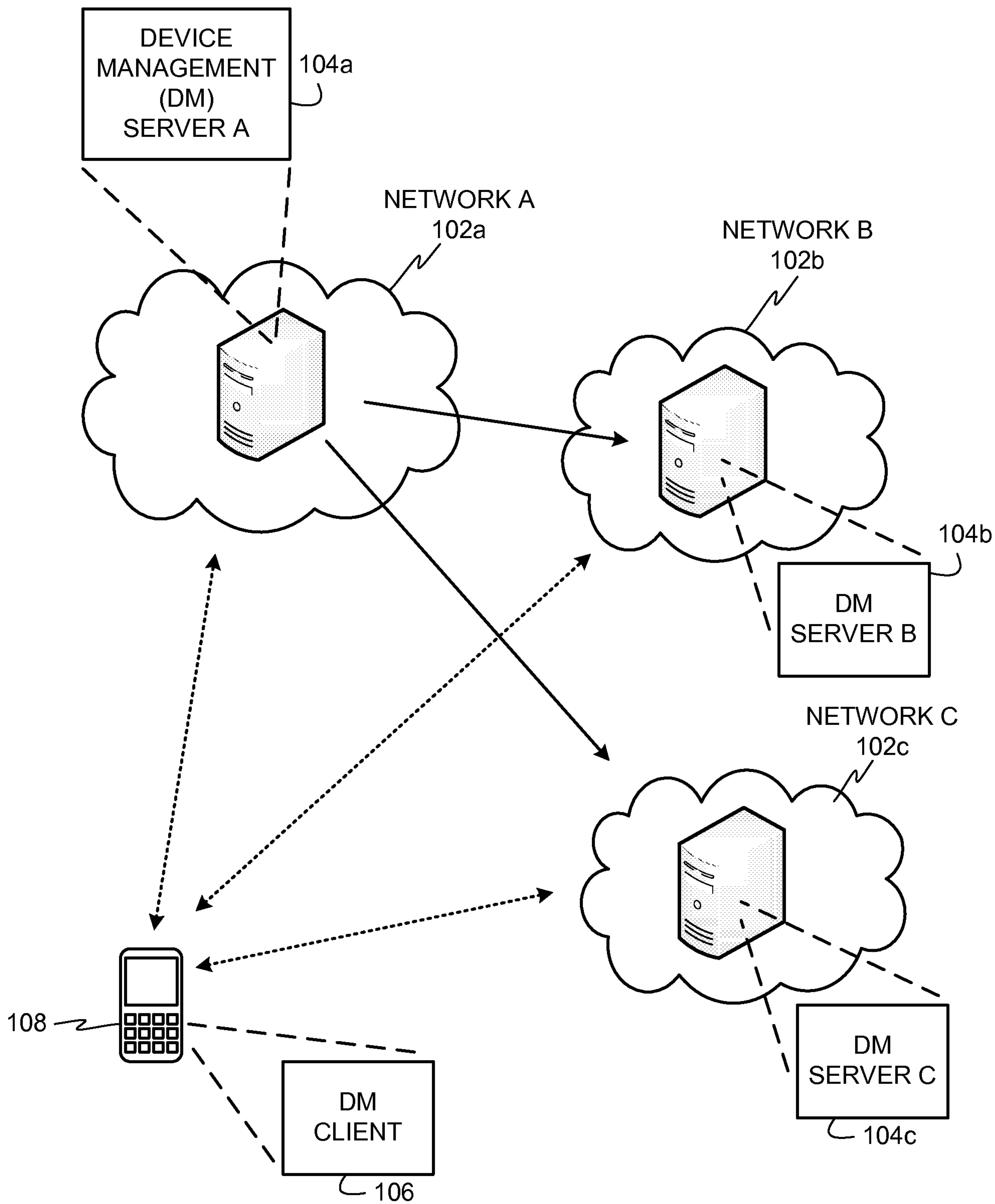


FIG. 1

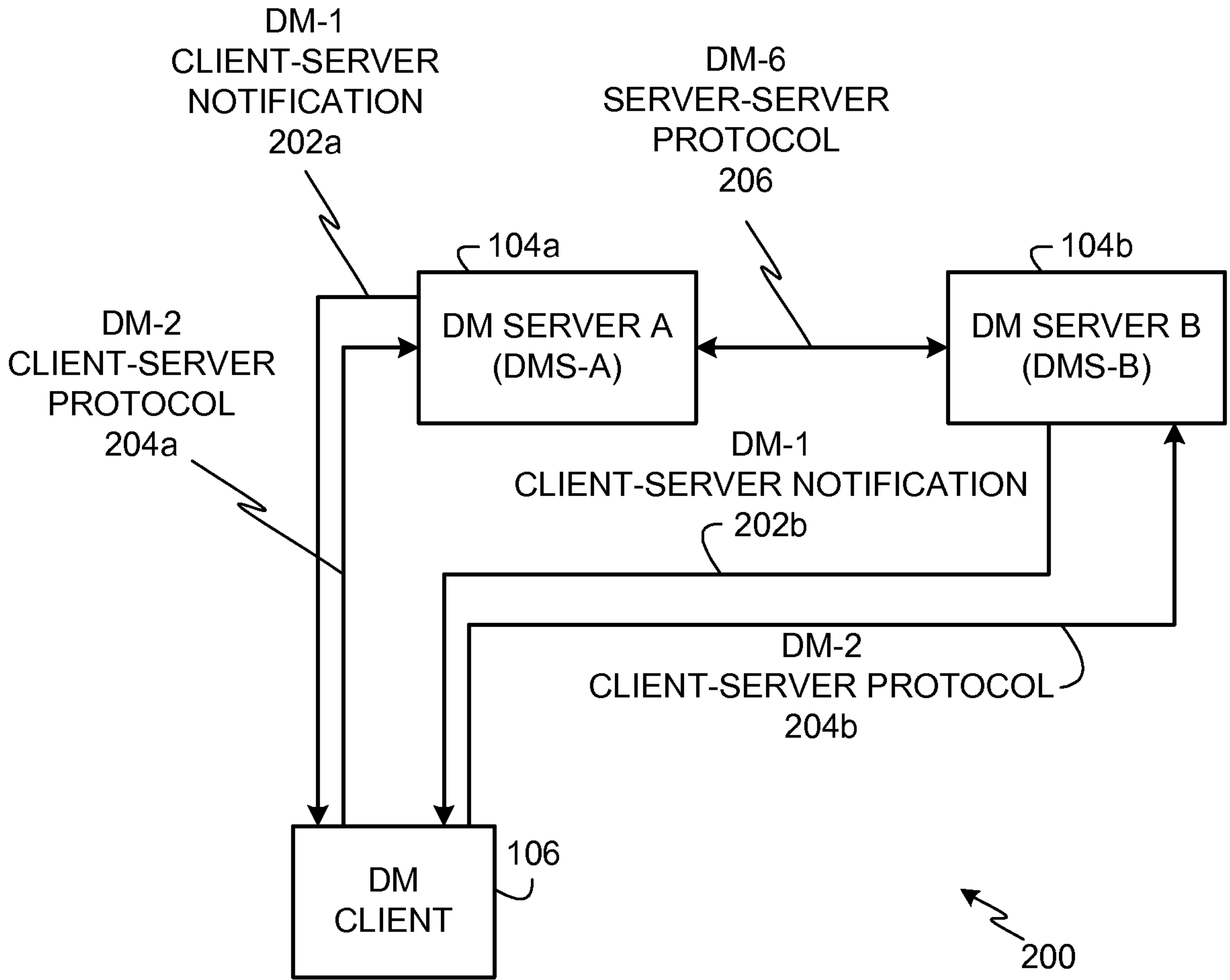


FIG. 2

ENUM ID	DELEGATION TYPE
01	UNRESTRICTED
02	RESTRICTED
03	PERMANENT
04	TEMPORARY

DELEGATION TYPES

FIG. 3

300

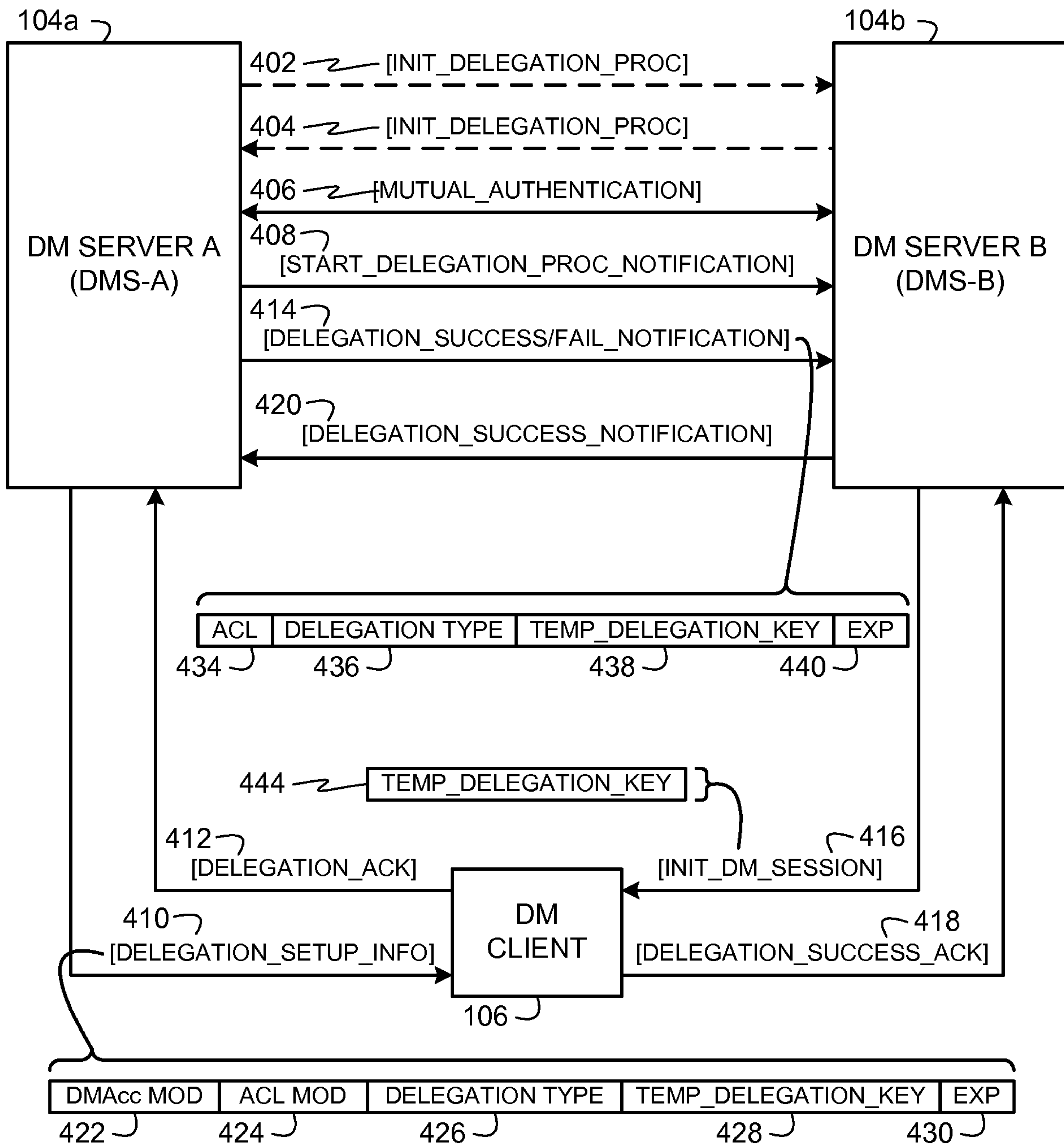


FIG. 4

4/8

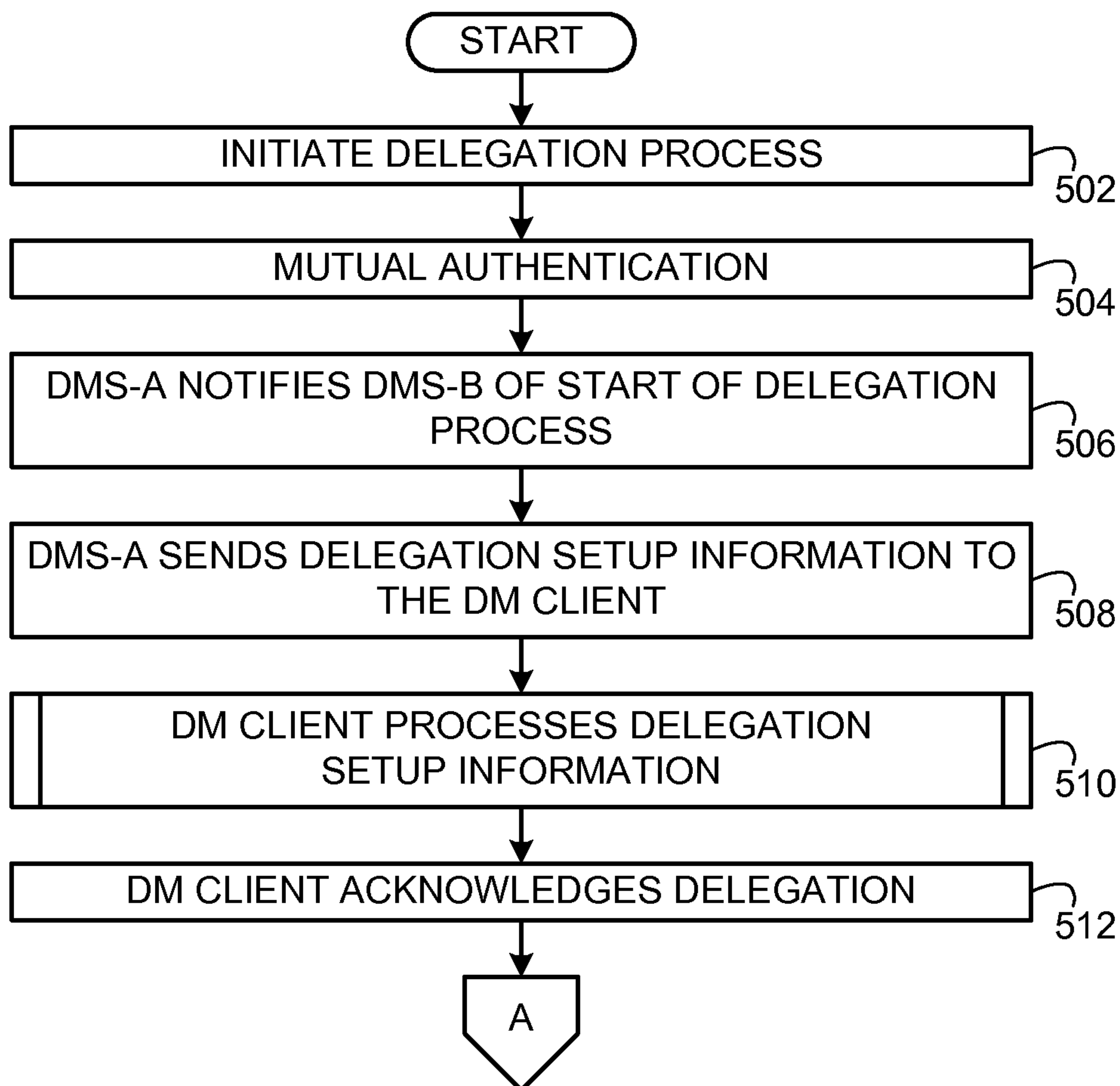


FIG. 5A

5/8

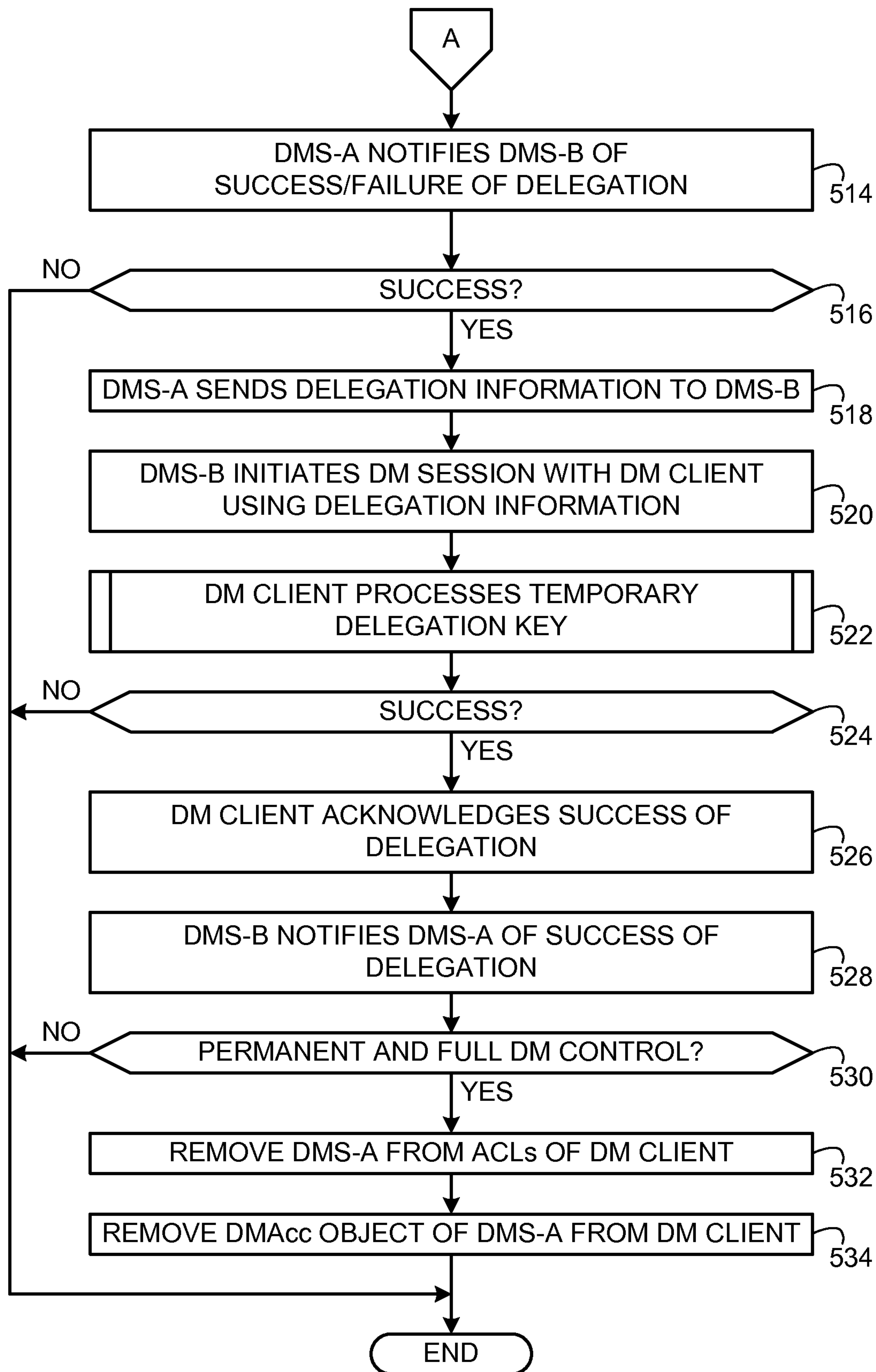


FIG. 5B

6/8

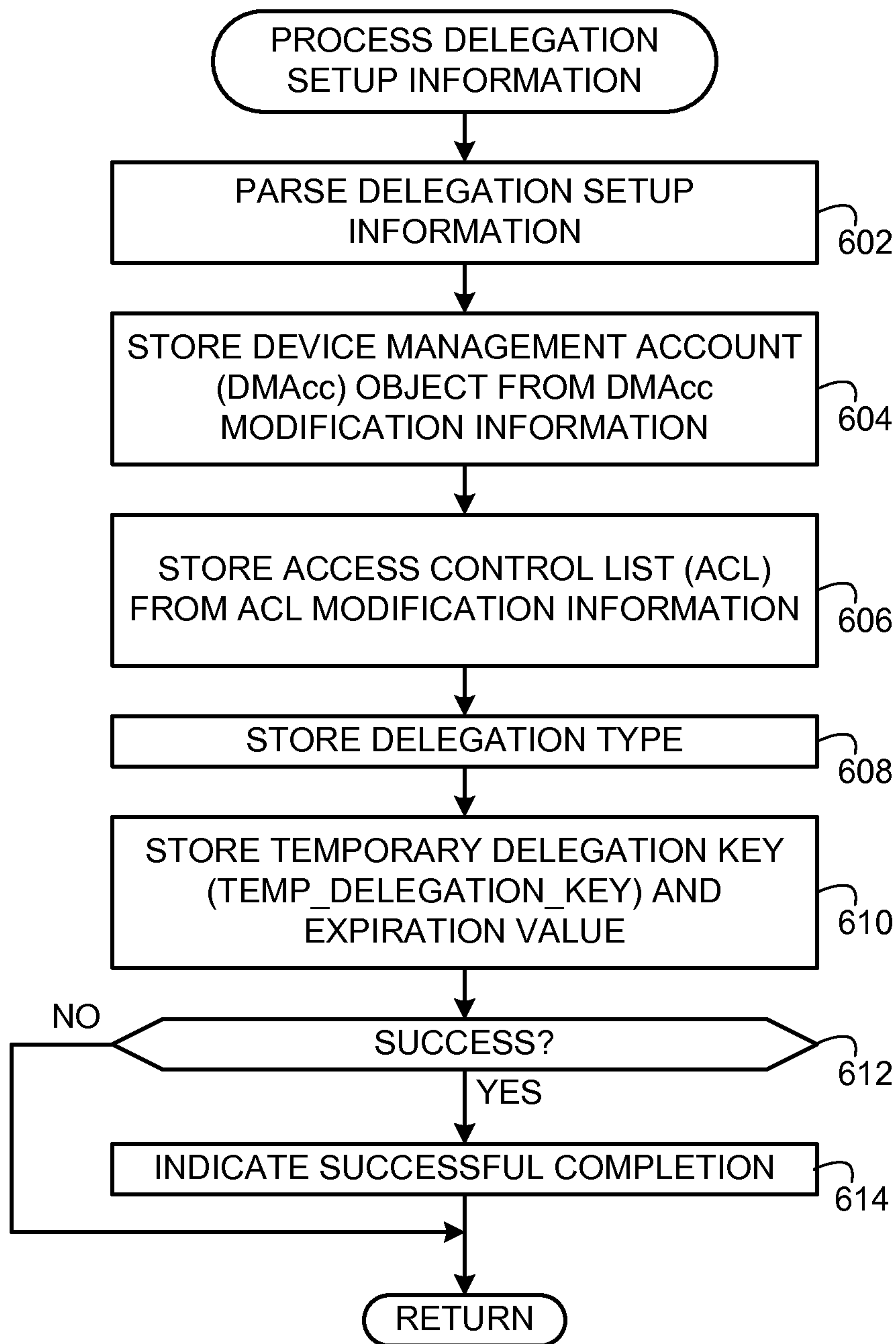


FIG. 6

7/8

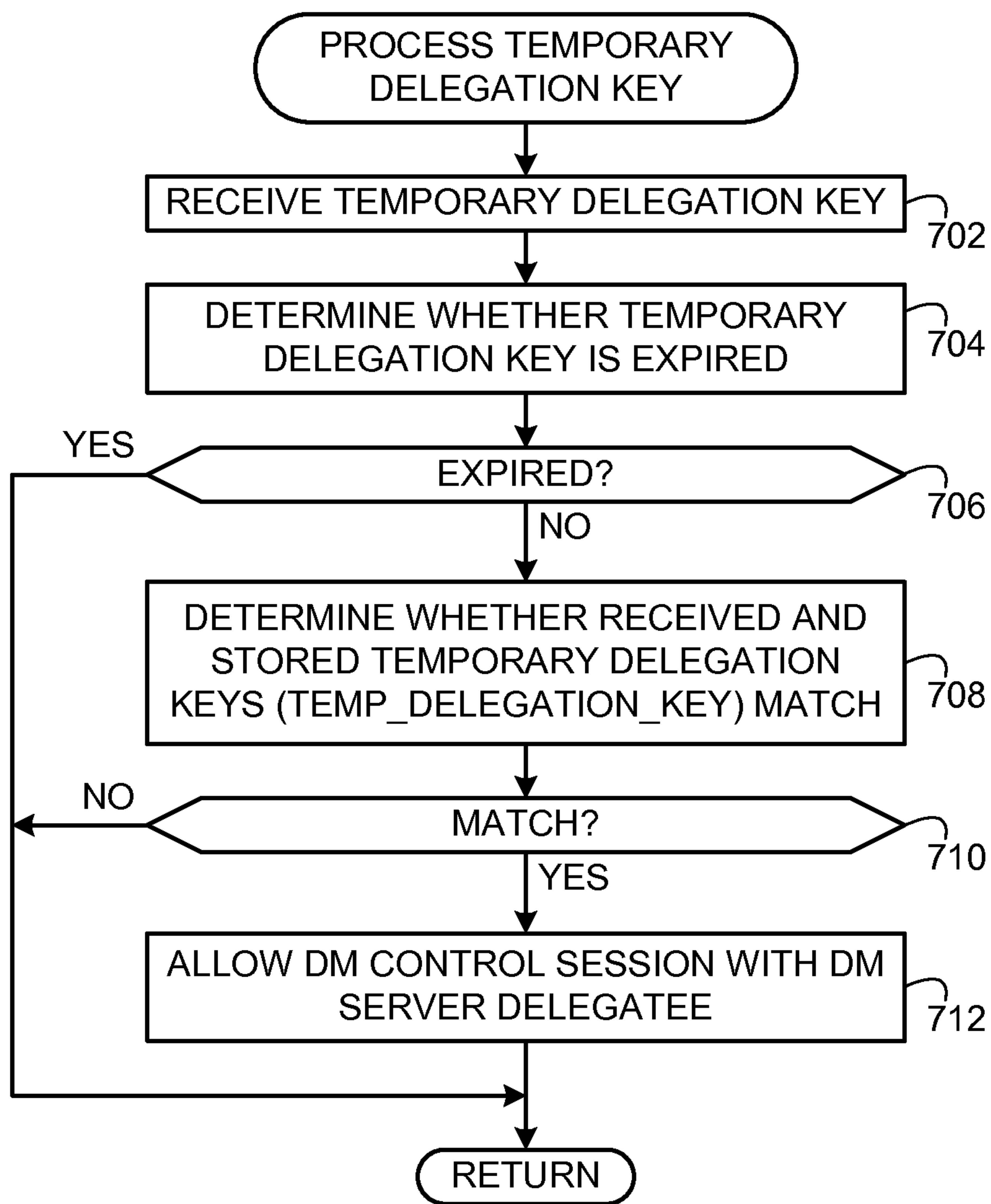


FIG. 7

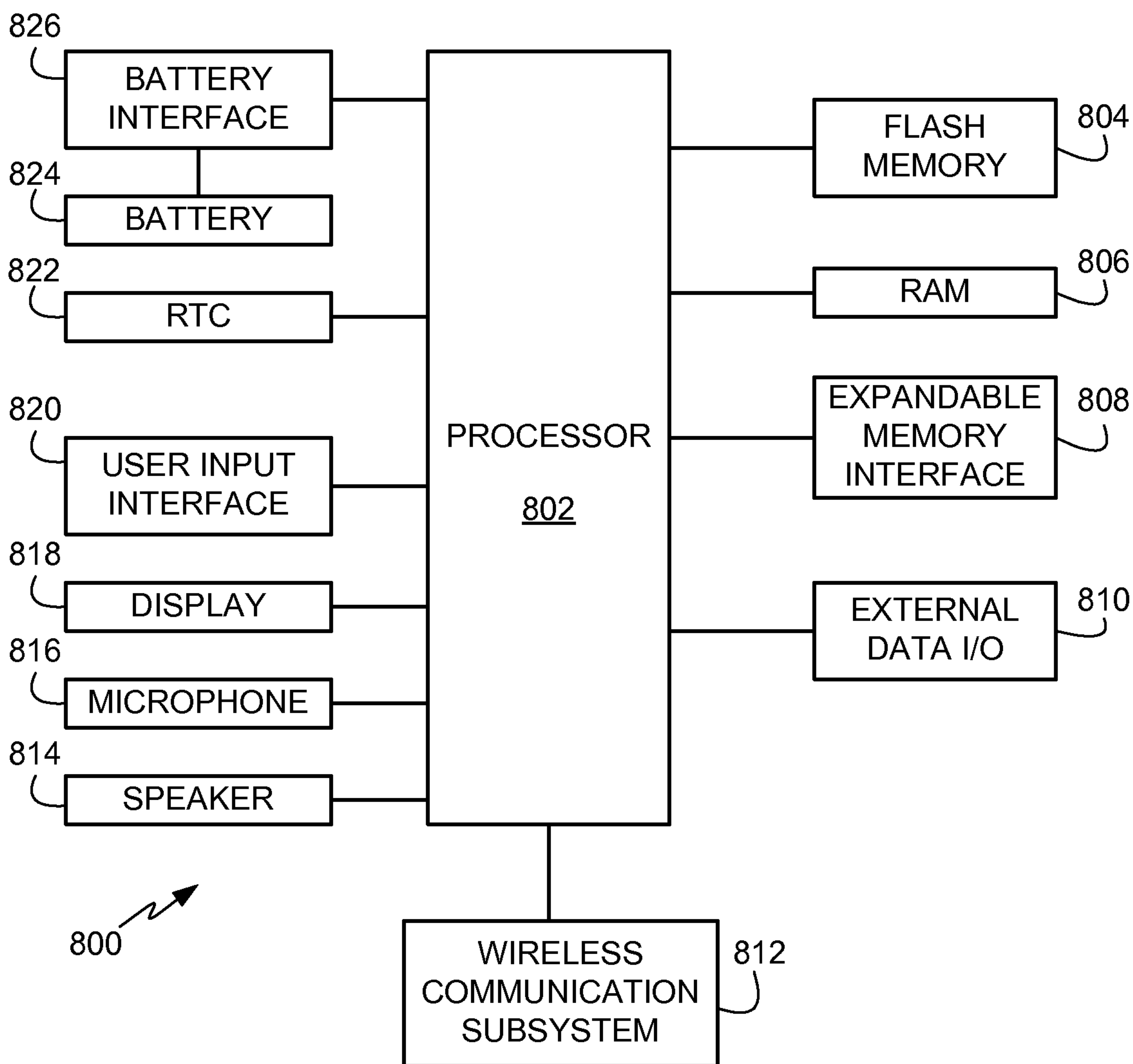


FIG. 8

