(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 3 657 729 B1**

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
06.10.2021 Bulletin 2021/40

(21) Application number: **17923031.3**

(22) Date of filing: **28.08.2017**

(51) Int Cl.:
H04W 4/12 *(2009.01)* ***H04W 12/126*** *(2021.01)*
H04W 12/30 *(2021.01)* ***H04W 4/24*** *(2018.01)*
H04L 9/32 *(2006.01)* ***H04W 4/50*** *(2018.01)*
H04W 8/18 *(2009.01)* ***H04W 12/04*** *(2021.01)*
H04W 12/06 *(2021.01)* ***H04W 12/10*** *(2021.01)*
H04M 15/00 *(2006.01)* ***H04W 8/20*** *(2009.01)*

(86) International application number:
PCT/CN2017/099267

(87) International publication number:
WO 2019/041086 (07.03.2019 Gazette 2019/10)

(54) **INFORMATION VERIFICATION METHOD AND RELATED EQUIPMENT**

VERFAHREN ZUR INFORMATIONSÜBERPRÜFUNG UND ENTSPRECHENDE AUSRÜSTUNG

PROCÉDÉ DE VÉRIFICATION D'INFORMATIONS ET ÉQUIPEMENT ASSOCIÉ

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

(43) Date of publication of application:
27.05.2020 Bulletin 2020/22

(60) Divisional application:
21191099.7

(73) Proprietor: **Huawei Technologies Co., Ltd.**
Longgang District
Shenzhen, Guangdong 518129 (CN)

(72) Inventors:
- **FAN, Shunan**
  Shenzhen
  Guangdong 518129 (CN)
- **LONG, Shuiping**
  Shenzhen
  Guangdong 518129 (CN)
- **GAO, Linyi**
  Shenzhen
  Guangdong 518129 (CN)

(74) Representative: **Grünecker Patent- und Rechtsanwälte**
PartG mbB
Leopoldstraße 4
80802 München (DE)

(56) References cited:
EP-A1- 3 073 770
EP-A2- 2 854 432
CN-A- 101 141 253
CN-A- 101 277 297
CN-A- 101 389 060
US-A1- 2010 228 973
US-A1- 2014 329 502

EP 3 657 729 B1

Description

TECHNICAL FIELD

[0001] This application relates to the field of wireless network technologies, and in particular, to an information verification method and a related device.

BACKGROUND

[0002] Currently, a user may purchase a subscriber identity module (Subscriber Identity Module, SIM) from a communications operator, to obtain a number resource of the operator, so as to be entitled to use a communications service provided by the operator. As technologies and requirements evolve, an embedded universal integrated circuit card (embedded Universal Integrated Circuit Card, eUICC), also referred to as an eSIM (embedded SIM), emerges. The eUICC is a newly defined secure element that is used by a plurality of communications operators to remotely manage a subscriber, and is placed into a terminal in a plug-in manner or a welding manner. A user may select an operator network for user equipment (User Equipment, UE) of the user, and download a profile (Profile) from the operator network. After the profile is downloaded to the eUICC, the user equipment may access the selected operator network by using data provided in the profile. In addition, the user may alternatively select another operator, and download a profile of the another operator to implement a scenario such as a handover between the operator networks. Because internet of things exists in different industries, it is relatively convenient to provide an eUICC for a device in the internet of things, so that the device accesses and uses the network. For example, it is more convenient for a device such as a smart meter or a smart in-vehicle system to use an eUICC to be connected to and authenticated by the network and to use the network. Many international and national standard organizations are formulating related standards for an eUICC, mainly including Global System for Mobile Communications Association (Global System for Mobile Communication Association, GSMA) and European Telecommunications Standards Institute (European Telecommunications Standards Institute, ETSI).

EP3073770A1 discloses a security control method for an eUICC, including: verifying, by an embedded integrated circuit card eUICC, whether a subscription manager-secure routing SM-SR entity is authorized to manage the eUICC; and if yes, establishing, by the eUICC, a secure transmission channel with the SM-SR entity, where the secure transmission channel is used for management interaction of the eUICC; and further discloses an eUICC; for which security of the eUICC can be ensured by the disclosed method.

[0003] In an existing eUICC architecture, the following function definitions are provided: An integrated circuit card identifier (Integrated Circuit Card ID, ICCID) is also referred to as a profile ID, and is used to uniquely identify a profile. An eUICC identifier (eUICC-ID, EID) is used to uniquely identify an eUICC. A profile is a set of file structures, data, applications, and the like, and includes one or more network access applications and corresponding network access credentials, for example, an international mobile subscriber identity and a personal key identity (Key Identity, KI). A subscription manager-data preparing (Subscription Manager-Data Preparing, SM-DP, or Subscription Manager Data Preparation+, SM-DP+) server is also referred to as a profile provisioner or a profile download server, and may create, generate, manage, or transmit a profile based on basic subscription information, such as an international mobile subscriber identity (International Mobile Subscriber Identity, IMSI), provided by a mobile network operator (Mobile Network Operator, MNO). After a profile is downloaded to an eUICC, an MNO may send a remote profile management (Remote Profile Management, RPM) command to manage the downloaded profile, for example, perform operations such as activating, deactivating, deleting, and enumerating an installed profile list and updating a profile-related parameter. However, only a profile owner (Profile Owner, PO) has permission to manage the downloaded profile, and whether the MNO is an owner of the profile is not verified. Consequently, a network security problem easily occurs in a network profile management process.

SUMMARY

[0004] This application provides an information verification method and a related device, to resolve a network security problem.

The invention is disclosed according to the independent claims. The dependent claims recite advantageous embodiments of the invention.

[0005] According to a first aspect, an embodiment of this application provides an information verification method, including: first receiving, by a first profile server, a remote profile management request sent by a remote profile management server, and obtaining a second profile owner identifier in profile information; then determining whether a first profile owner identifier is the same as the second profile owner identifier; and sending, by the first profile server, a remote profile management command to user equipment when the first profile owner identifier is the same as the second profile owner identifier. This prevents a third party from maliciously tampering with profile information that is not possessed by the third party, and avoids a loss caused to an operator or a profile owner due to a user's access to an invalid network or random profile unlocking. In addition, the profile server verifies a PO on a network side. In this way, network security can be improved, a bidirectional authentication process between the profile server and a terminal can be reduced, and a waste of network resources can be reduced.

[0006] In a possible design, the first profile server may

obtain the second profile owner identifier in the profile information from a local memory, or read the second profile owner identifier in the profile information from a storage area of another connected server.

[0007] In another possible design, the first profile server may send a first request to the user equipment, where the first request is used to obtain the second profile owner identifier. After receiving the first request, the user equipment sends, to the first profile server, the profile information that carries the second profile owner identifier.

[0008] In another possible design, the first profile server may send a second request to a second profile server, where the second request is used to obtain the second profile owner identifier. After obtaining the second profile owner identifier corresponding to the PO, the second profile server sends, to the first profile server, the profile information that carries the second profile owner identifier.

[0009] In another possible design, after receiving the remote profile management request sent by the remote profile management server, the first profile server may perform verification or identification by using information such as a message header field and an initiator certificate that are in the message sent by the remote profile management server to the first profile server and that are used to identify an initiator, and a PO ID that is carried in the remote profile management request thereby ensuring identity validity of the remote profile management server.

[0010] In another possible design, the first profile server may compare the first profile owner identifier with the second profile owner identifier to verify whether the first profile owner identifier is the same as the second profile owner identifier.

[0011] In another possible design, when the first profile owner identifier is different from the second profile owner identifier, the first profile server sends a response message to the remote profile management server, where the response message is used to notify the remote profile management server of a verification error.

[0012] In another possible design, the first profile owner identifier and the second profile owner identifier each include at least one of the following: a profile owner identifier that is identifiable to the first profile server, or a profile owner identifier that is identifiable to the second profile server.

[0013] In another possible design, when the first profile owner identifier includes only the profile owner identifier that is identifiable to the first profile server, the profile owner identifier that is identifiable to the first profile server in the first profile owner identifier needs to be separately compared with the profile owner identifier that is identifiable to the first profile server in the profile information and the profile owner identifier that is identifiable to the second profile server in the profile information, to verify whether the profile owner identifier that is identifiable to the first profile server in the first profile owner identifier is the same as a profile owner identifier in the profile information. If the profile owner identifier that is identifiable to the first profile server in the first profile owner identifier is the same as a profile owner identifier in the profile information, it is determined that the first profile owner identifier is the same as the second profile owner identifier; or if the profile owner identifier that is identifiable to the first profile server in the first profile owner identifier is different from any profile owner identifier in the profile information, it is determined that the first profile owner identifier is different from the second profile owner identifier. When the first profile owner identifier includes only the profile owner identifier that is identifiable to the second profile server, a verification method is the same as the foregoing method. Details are not described herein again. When the first profile owner identifier includes both the profile owner identifier that is identifiable to the first profile server and the profile owner identifier that is identifiable to the second profile server, the profile owner identifier that is identifiable to the first profile server in the first profile owner identifier and the profile owner identifier that is identifiable to the second profile server in the first profile owner identifier need to be respectively compared with the profile owner identifier that is identifiable to the first profile server in the profile information and the profile owner identifier that is identifiable to the second profile server in the profile information. Only when the profile owner identifier that is identifiable to the first profile server in the first profile owner identifier is the same as the profile owner identifier that is identifiable to the first profile server in the profile information and the profile owner identifier that is identifiable to the second profile server in the first profile owner identifier is the same as the profile owner identifier that is identifiable to the second profile server in the profile information, it is determined that the first profile owner identifier is the same as the second profile owner identifier.

[0014] In another possible design, the first profile server obtains an identifier correspondence list when the first profile owner identifier is different from the second profile owner identifier, where the identifier correspondence list includes a correspondence between a profile server identifier and a profile owner identifier; determines whether a profile owner identifier corresponding to the first profile owner identifier exists in the identifier correspondence list; and sends the remote profile management command to the user equipment when the profile owner identifier corresponding to the first profile owner identifier exists in the identifier correspondence list, to further verify the PO.

[0015] In another possible design, the first profile server obtains the identifier correspondence list from the remote profile management server; obtains the identifier correspondence list from the second profile server; or obtains the identifier correspondence list from the local memory.

[0016] In another possible design, the profile owner identifier includes a profile server identifier and a profile owner identifier.

[0017] In another possible design, because the first

profile owner identifier includes a profile server identifier and a profile owner identifier, the second profile owner identifier that is identifiable to the first profile server in the profile information may be obtained based on an identifier of the first profile server included in the first profile owner identifier. Alternatively, the second profile owner identifier that is identifiable to the second profile server in the profile information is obtained based on an identifier of the second profile server included in the first profile owner identifier.

[0018] In another possible design, the first profile server is a server configured to manage a profile, and the second profile server is a server configured to download the profile.

[0019] According to a second aspect, an embodiment of this application provides an information verification method, including: receiving, by user equipment, a remote profile management command sent by a first profile server, where the remote profile management command includes a first profile owner identifier; obtaining a second profile owner identifier in profile information; then determining whether the first profile owner identifier is the same as the second profile owner identifier; and finally executing the remote profile management command when the first profile owner identifier is the same as the second profile owner identifier. This prevents a third party from maliciously tampering with profile information that is not possessed by the third party, and avoids a loss caused to an operator or a profile owner due to a user's access to an invalid network or random profile unlocking. In addition, the profile server verifies a PO on a network side. In this way, network security can be improved, a bidirectional authentication process between the profile server and a terminal can be reduced, and a waste of network resources can be reduced.

[0020] In a possible design, the user equipment may first search for the second profile owner identifier in the profile information based on an ICCID carried in the remote profile management command, and compare the first profile owner identifier with the second profile owner identifier to verify whether the first profile owner identifier is the same as the second profile owner identifier.

[0021] In another possible design, before receiving the remote profile management command sent by the first profile server, the user equipment receives an update message sent by a remote profile management server or a second profile server, where the update message includes an identifier of the first profile server and a corresponding profile owner identifier.

[0022] In another possible design, after receiving the update request sent by the remote profile management server or the second profile server, the user equipment may perform verification or identification may be performed by using information such as a message header field and an initiator certificate that are in the update message and that are used to identify an initiator, and the PO ID that is carried in the update message, thereby ensuring identity validity of the remote profile management server or the second profile server.

[0023] In another possible design, the first profile owner identifier includes at least one of the following: a profile owner identifier that is identifiable to the first profile server or a profile owner identifier that is identifiable to the second profile server.

[0024] In another possible design, the user equipment obtains an identifier correspondence list when the first profile owner identifier is different from the second profile owner identifier, where the identifier correspondence list includes a correspondence between a profile server identifier and a profile owner identifier; determines whether a profile owner identifier corresponding to the first profile owner identifier exists in the identifier correspondence list; and executes the remote profile management command when the profile owner identifier corresponding to the first profile owner identifier exists in the identifier correspondence list.

[0025] In another possible design, before receiving the remote profile management command sent by the first profile server, the user equipment receives a first request sent by the first profile server, where the first request is used to obtain the second profile owner identifier; and sends, to the first profile server, the profile information that carries the second profile owner identifier.

[0026] In another possible design, the user equipment may send a response message to the first profile server or the remote profile management server when the first profile owner identifier is different from the second profile owner identifier, where the response message is used to notify the remote profile management server of a verification error.

[0027] According to a third aspect, an embodiment of this application provides an information verification method, including: sending, by a remote profile management server, a remote profile management request to a first profile server, where the remote profile management request includes a first profile owner identifier, and the remote profile management request is used to instruct the first profile server to determine whether a second profile owner identifier in profile information is the same as the first profile owner identifier; and sending a remote profile management command to user equipment when the second profile owner identifier is the same as the first profile owner identifier. This prevents a third party from maliciously tampering with profile information that is not possessed by the third party, and avoids a loss caused to an operator or a profile owner due to a user's access to an invalid network or random profile unlocking. In addition, the profile server verifies a PO on a network side. In this way, network security can be improved, a bidirectional authentication process between the profile server and a terminal can be reduced, and a waste of network resources can be reduced.

[0028] In a possible design, the remote profile management server determines whether the first profile server configured to manage a profile and a second profile server previously configured to download the profile are

a same server; and when the first profile server and the second profile server are different servers, the remote profile management server determines a profile owner identifier that is identifiable to the first profile server or a profile owner identifier that is identifiable to the second profile server.

[0029] In another possible design, the remote profile management server may configure information about the first profile server in the profile information in advance, and also configure the profile owner identifier that is identifiable to the first profile server; and after completing the configuration, send an update message to the user equipment, where the update message includes an identifier of the first profile server and a corresponding profile owner identifier.

[0030] In another possible design, the first profile owner identifier includes the identifier of the first profile server and a corresponding profile owner identifier that is identifiable to the first profile server, or an identifier of the second profile server and a corresponding profile owner identifier that is identifiable to the second profile server.

[0031] According to a fourth aspect, an embodiment of this application provides a first profile server. The first profile server is configured to implement the method and the functions that are performed by the first profile server in the first aspect. The first profile server is implemented by using hardware/software. The hardware/software of the first profile server includes units corresponding to the foregoing functions.

[0032] According to a fifth aspect, an embodiment of this application provides user equipment. The user equipment is configured to implement the method and the functions that are performed by the user equipment in the second aspect. The user equipment is implemented by using hardware/software. The hardware/software of the user equipment includes units corresponding to the foregoing functions.

[0033] According to a sixth aspect, an embodiment of this application provides a remote profile management server. The remote profile management server is configured to implement the method and the functions that are performed by the remote profile management server in the third aspect. The remote profile management server is implemented by using hardware/software. The hardware/software of the remote profile management server includes units corresponding to the foregoing functions.

[0034] According to a seventh aspect, this application provides another first profile server, including a processor, a memory, and a communications bus. The communications bus is configured to implement connection and communication between the processor and the memory, and the processor executes a program stored in the memory, to implement the steps in the information verification method provided in the first aspect.

[0035] In a possible design, the profile server provided in this application may include a corresponding module configured to perform behavior of the profile server in the foregoing method design. The module may be software and/or hardware.

[0036] According to an eighth aspect, this application provides other user equipment, including a processor, a memory, and a communications bus. The communications bus is configured to implement connection and communication between the processor and the memory, and the processor executes a program stored in the memory, to implement the steps in the information verification method provided in the second aspect.

[0037] In a possible design, the user equipment provided in this application may include a corresponding module configured to perform behavior of the user equipment in the foregoing method design. The module may be software and/or hardware.

[0038] According to a ninth aspect, this application provides another remote profile management server, including a processor, a memory, and a communications bus. The communications bus is configured to implement connection and communication between the processor and the memory, and the processor executes a program stored in the memory, to implement the steps in the information verification method provided in the third aspect.

[0039] In a possible design, the remote profile management server provided in this application may include a corresponding module configured to perform behavior of the remote profile management server in the foregoing method design. The module may be software and/or hardware.

[0040] According to a tenth aspect, this application provides a computer-readable storage medium, and the computer-readable storage medium stores an instruction. When the instruction runs on a computer, the computer is enabled to perform the methods in the foregoing aspects.

[0041] According to an eleventh aspect, this application provides a computer program product including an instruction. When the computer program product runs on a computer, the computer is enabled to perform the methods in the foregoing aspects.

BRIEF DESCRIPTION OF DRAWINGS

[0042] To describe the technical solutions in the embodiments of this application or in the background more clearly, the following briefly describes the accompanying drawings required for describing the embodiments of this application or the background.

FIG 1 is a schematic structural diagram of an information verification system according to an embodiment of this application;

FIG 2(A) is a schematic flowchart of an information verification method according to an embodiment of this application;

FIG. 2(B) is a schematic flowchart of another information verification method according to an embodiment of this application;

FIG. 3 is a schematic flowchart of an information ver-

ification method according to an embodiment of this application;

FIG. 4 is a schematic flowchart of an information verification method according to another embodiment of this application;

FIG. 5A and FIG. 5B are a schematic flowchart of an information verification method according to still another embodiment of this application;

FIG. 6 is a schematic flowchart of an information verification method according to yet another embodiment of this application;

FIG. 7 is a schematic structural diagram of a first profile server according to an embodiment of this application;

FIG. 8 is a schematic structural diagram of user equipment according to an embodiment of this application;

FIG. 9 is a schematic structural diagram of a remote profile management server according to an embodiment of this application;

FIG. 10 is a schematic structural diagram of another first profile server according to this application;

FIG. 11 is a schematic structural diagram of other user equipment according to this application; and

FIG. 12 is a schematic structural diagram of another remote profile management server according to this application.

DESCRIPTION OF EMBODIMENTS

[0043] The following describes the embodiments of this application with reference to the accompanying drawings in the embodiments of this application.

[0044] FIG. 1 is a schematic structural diagram of an information verification system according to an embodiment of this application. The information verification system includes a profile server, a remote profile management (Remote Profile Management, RPM) server, and user equipment (User Equipment, UE). The profile server may include at least one of a subscription manager-data preparing (Subscription Manager-Data Preparing, SM DP, or Subscription Manager-Data Preparing+, SM-DP+) server and a subscription manager discovery server (Subscription Manager Discovery Server, SM-DS). The SM DP+ is an enhanced release of an SM DP server, and is collectively referred to as the SM DP+ below. The SM-DP+ is mainly configured to generate, based on basic subscription information (for example, an international mobile subscriber identity) provided by the remote profile management server, a profile that can be downloaded to an eUICC, and the SM-DS is mainly configured to provide one or more SM DP+ addresses for the user equipment. The remote profile management server may be an MNO, an MVNO that purchases and uses a profile provided by an MNO, or an enterprise operation and maintenance server that uses a profile provided by an MNO. For example, a company such as BMW Group or State Grid may configure, for a customer or an employee of the company, a profile management service required for connecting a network. The user equipment may include an eUICC and a local profile assistant (Local Profile Assistant, LPA) module. The eUICC may be embedded in the user equipment, or may be a pluggable eUICC inserted into the user equipment. Alternatively, the eUICC may be implemented by using an eUICC that is embedded in a chip and that is accessed by using a bus. The LPA module is configured to manage profile downloading, and provide a UI interface (for example, a profile installation list) for the user equipment, so that a user can manage (activate, deactivate, delete, or unlock) a local profile in the eUICC. In addition, the user equipment may further retrieve an EID and/or an ICCID by using the LPA module. The LPA module may be a virtual logic module, or may be an entity module, for example, a field programmable gate array. The LPA includes a local discovery service (Local Discovery Service, LDS), local profile download (Local Profile Download, LPD), and a local user interface UI interface (Local User Interface, LUI). The LPA in the user equipment and the LPA in the eUICC may each include one or more of the LDS, the LPD, and the LUI.

[0045] Based on the foregoing architecture of the information verification system, a profile owner (PO) may send a remote profile management command to the SM DP+ or a managing SM DP+ (Managing SM DP+) to manage a downloaded profile. During management of the downloaded profile, it is possible that the profile is previously downloaded by using an SM DP+, and then the profile in the eUICC is managed by using another SM DP+ (Managing SM DP+). If the SM DP+ configured to manage the profile and the SM DP+ configured to download the profile are different servers, an identifier of the managing SM DP+ needs to be first updated to a profile-related parameter, such as profile metadata (Profile Metadata) and profile information (ProfileInfo), and then the managing SM DP+ is permitted to send a remote profile management command.

[0046] As shown in FIG 2(A), when an SM DP+ configured to manage a profile and an SM DP+ configured to download the profile are a same server, the SM DP+ and an eUICC authenticate each other, and the SM DP+ and an MNO authenticate each other. Both an MNO1 and an MNO2 have permission to manage the eUICC. However, it is not verified whether the MNO1 and the MNO2 manage respective profiles in the eUICC, either. As shown in FIG. 2(B), when an SM DP+ configured to manage a profile and an SM DP+ configured to download the profile are different servers, the SM DP+ may assign different PO IDs to a same PO; and the SM DP+ may assign a same PO ID to different POs. For example, an SM DP+ of China Mobile in China assigns a PO ID 46001, and an SM DP+ of China Mobile abroad assigns a PO ID CMCC. Alternatively, T-Mobile assigns a PO ID 23430, and EE also assigns the PO ID 23430. In this case, it is not verified whether an MNO1 and an MNO2 manage respective profiles in an eUICC, either. Because

a PO is not verified, a third party may maliciously tamper with data in a profile. This affects network security. To resolve the problem, the following solutions are proposed.

[0047] FIG. 3 is a schematic flowchart of an information verification method according to an embodiment of this application. In this embodiment of this application, a profile server configured to manage a profile and a profile server configured to download the profile are a same server. The method includes but is not limited to the following steps.

[0048] S301. A remote profile management server sends a remote profile management (RPM) request to a profile server. The RPM request includes a first profile owner identifier (PO ID), and the RPM request further includes at least one of an eUICC identifier (EID), a profile identifier (ICCID), and RPM command-related information.

[0049] The first profile owner identifier may include only a profile owner identifier, or may include a profile server identifier and a profile owner identifier. The profile owner identifier may vary with a specific implementation. For example, an MNO and an SM DP+ may agree on a profile owner identifier in advance, or an MNO and an SM DP+ may use an identifier of a message initiator between the MNO and the SM DP+ as a profile owner identifier. For another example, State Grid, serving as a company, manages a profile purchased by State Grid from the MNO. In this case, the first profile owner identifier may include a PO ID assigned by the MNO or the SM DP+ to State Grid. Alternatively, a mobile virtual network operator (Mobile Virtual Network Operator, MVNO) purchases a profile from the MNO. In this case, the first profile owner identifier may include a PO ID assigned to the MVNO. This ensures that State Grid or the MVNO manages the profile of State Grid or the MVNO by using the MNO.

[0050] Optionally, after receiving the RPM request sent by the RPM server, the profile server may verify identity validity of the RPM server based on a PO ID carried in the RPM request. Specifically, verification or identification may be performed based on at least one type of information such as a message header field and an initiator certificate that are in the message sent by the RPM server to the profile server and that are used to identify an initiator, and the PO ID that is carried in the RPM request. For example, if the PO ID carried in the RPM request is a PO ID of China Mobile, it is verified whether the initiator of the RPM request is China Mobile. If the initiator of the RPM request is not China Mobile, it is verified that an identity of the initiator is invalid. If the initiator of the RPM request is China Mobile, it is verified that the identity of the initiator is valid. This prevents a third party from maliciously using the PO ID of China Mobile to manage the profile. In verification on the identity of the initiator, a verification operation of determining whether the initiator is a valid initiator, a verification operation of judging whether the initiator is a valid initiator, or the like may be performed.

[0051] S302. The profile server obtains a second profile owner identifier in profile information. The following two optional manners are included.

[0052] The first implementation includes the following step:

S302a. The profile server may obtain the second profile owner identifier in the profile information from a local memory, or read the second profile owner identifier in the profile information from a storage area of another connected server. Further, the second profile owner identifier may be obtained by searching, based on a profile ICCID carried in the RPM request, for PO ID information stored in profile-related metadata; or a corresponding profile may be searched for based on the profile ICCID carried in the RPM request, and the second profile owner identifier of the profile is obtained.

[0053] The second implementation includes the following steps.

S302b. The profile server may send a first request to user equipment, where the first request is used to obtain the second profile owner identifier, the first request may be a Get ProfileInfo interface command, and the first request may carry at least one of an identifier of a second profile server, an EID, and an ICCID. Specifically, after a secure channel is established between the profile server and the user equipment, the profile server may send the first request to the user equipment through an ES 8+ or ES 9+ interface between the profile server and the user equipment.

S302c. After receiving the first request, the user equipment searches for the corresponding profile information based on the profile ICCID carried in the RPM request, and after finding the corresponding profile information, the user equipment sends, to the profile server, the profile information that carries the second profile owner identifier.

S303. The profile server determines whether the first profile owner identifier is the same as the second profile owner identifier.

[0054] In specific implementation, the profile server may compare the first profile owner identifier with the second profile owner identifier to verify or determine whether the first profile owner identifier is the same as the second profile owner identifier.

S304. The profile server sends an RPM command to the user equipment when the first profile owner identifier is the same as the second profile owner identifier, where the RPM command carries the first profile owner identifier, the EID, and the ICCID.

S305. The profile server sends a response message to the remote profile management server when the first profile owner identifier is different from the sec-

ond profile owner identifier, where the response message is used to notify the RPM server of a verification error.

S306. After receiving the RPM command, the user equipment determines whether the first profile owner identifier is the same as the second profile owner identifier.

[0055] In specific implementation, the user equipment may first search for the second profile owner identifier in the profile information based on the ICCID carried in the RPM command, and compare the first profile owner identifier with the second profile owner identifier to verify whether the first profile owner identifier is the same as the second profile owner identifier.

[0056] S307. The user equipment executes the RPM command when the first profile owner identifier is the same as the second profile owner identifier. The user equipment may send a response message to the profile server or the RPM server when the first profile owner identifier is different from the second profile owner identifier, where the response message is used to notify the RPM server of a verification error.

[0057] In this embodiment of this application, the profile server, serving as both the server configured to download the profile and the server configured to manage the profile, first receives the RPM request sent by the RPM server, and obtains the second profile owner identifier in the profile information, and then determines whether the first profile owner identifier is the same as the second profile owner identifier. The profile server sends the RPM command to the user equipment when the first profile owner identifier is the same as the second profile owner identifier. This not only prevents a third party from maliciously tampering with profile information that is not possessed by the third party, but also avoids a loss caused to an operator or a profile owner due to a user's access to an invalid network or random profile unlocking. In addition, the profile server verifies a PO on a network side. In this way, network security can be improved, a bidirectional authentication process between the profile server and a terminal can be reduced, and a waste of network resources can be reduced.

[0058] FIG. 4 is a schematic flowchart of an information verification method according to another embodiment of this application. In this embodiment of this application, a first profile server configured to manage a profile and a second profile server configured to download the profile are different servers. The method includes but is not limited to the following steps.

[0059] S401. An RPM server or the second profile server updates profile information to user equipment. This step includes: S401a. The RPM server sends an update message to the user equipment. S401b. The second profile server sends an update message to the user equipment. The update message includes an identifier of the first profile server, and may further include a corresponding profile owner identifier.

[0060] In specific implementation, the RPM server or the second profile server may preconfigure information about the first profile server in the profile information, and preconfigure a profile owner identifier that is identifiable to the first profile server. The information about the first profile server may include the identifier of the first profile server.

[0061] After the foregoing information is configured, the user equipment may be assigned to the first profile server for remote profile management. Therefore, the RPM server or the second profile server may send the update message to the user equipment. The second profile server may assign a same identifier or different identifiers as PO IDs of a same profile owner. Therefore, the PO IDs also need to be updated to the profile information. For example, if a PO ID assigned by a first SM DP+ to China Mobile is 46001, and a PO ID assigned by a second SM DP+ to China Mobile is CMCC, an identifier of the first SM DP+ and the corresponding identifier 46001 of China Mobile are stored in the profile information, and an identifier of the second SM DP+ and the corresponding identifier CMCC of China Mobile are also stored in the profile information, to subsequently search for and verify the PO. After receiving the update message, the user equipment updates the identifier of the first profile server and the corresponding profile owner identifier to the profile information. Optionally, the RPM server may further configure the identifier of the first profile server and the corresponding profile owner identifier in the profile information of the user equipment by using an over-the-air (Over-the-Air, OTA) message.

[0062] Optionally, after receiving the update request sent by the RPM server or the second profile server, the user equipment may verify identity validity of the RPM server or the second profile server based on the PO ID carried in the update request. Specifically, verification or identification may be performed based on information such as a message header field and an initiator certificate that are in the update message and that are used to identify an initiator, and the PO ID that is carried in the update message. For example, if the PO ID carried in the update request is the PO ID of China Mobile, it is verified whether the initiator of the update request is China Mobile. If the initiator of the update request is not China Mobile, it is verified that an identity of the initiator is invalid. If China Mobile is the initiator of the update request, it is verified that the identity of the initiator is valid. Further, the identifier of the first profile server and the corresponding profile owner identifier are updated to the local profile information. This prevents a third party from maliciously using the PO ID of China Mobile to manage the profile. In verification on the identity of the initiator, a verification operation of determining whether the initiator is a valid initiator, a verification operation of judging whether the initiator is a valid initiator, or the like may be performed.

[0063] S402. The RPM server sends an RPM request to the first profile server, where the RPM request includes

a first profile owner identifier (PO ID), and the RPM request further includes at least one of an eUICC identifier (EID), a profile identifier (ICCID), and RPM command-related information, and the first profile owner identifier includes at least one of the following: a profile owner identifier that is identifiable to the first profile server or a profile owner identifier that is identifiable to the second profile server.

[0064] The profile owner identifier may vary with a specific implementation. For example, an MNO and an SM DP+ may agree on a profile owner identifier in advance, or an MNO and an SM DP+ may use an identifier of a message initiator between the MNO and the SM DP+ as a profile owner identifier. For another example, State Grid, serving as a company, manages a profile purchased by State Grid from the MNO. In this case, the first profile owner identifier may include a PO ID assigned by the MNO or the SM DP+ to State Grid. Alternatively, a mobile virtual network operator (Mobile Virtual Network Operator, MVNO) purchases a profile from the MNO. In this case, the first profile owner identifier may include a PO ID assigned to the MVNO. This ensures that State Grid or the MVNO manages the profile of State Grid or the MVNO by using the MNO.

[0065] Optionally, after receiving the RPM request initiated by the RPM server, the first profile server may verify identity validity of the RPM server based on the PO ID carried in the RPM request. Specifically, verification or identification may be performed based on information such as a message header field and an initiator certificate that are in the message sent by the RPM server to the first profile server and that are used to identify an initiator, and the PO ID that is carried in the RPM request. For example, if the PO ID carried in the RPM request is a PO ID of China Mobile, it is verified whether the initiator of the RPM request is China Mobile. If the initiator of the RPM request is not China Mobile, it is verified that the identity of the initiator is invalid. If the initiator of the RPM request is China Mobile, it is verified that the identity of the initiator is valid. This prevents a third party from maliciously using the PO ID of China Mobile to manage the profile.

[0066] S403. The first profile server obtains a second profile owner identifier in profile information, where the second profile owner identifier includes at least one of the following: a profile owner identifier that is identifiable to the first profile server or a profile owner identifier that is identifiable to the second profile server. The following two optional manners are included.

[0067] The first implementation includes the following steps:

S403a. The first profile server may send a first request to the user equipment, where the first request is used to obtain the second profile owner identifier, and the first request may be a Get ProfileInfo interface command, and may carry at least one of an identifier of the second profile server, an EID, and an ICCID. Specifically, after a secure channel is established between the first profile server and the user equipment, the first profile server may send the first request to the user equipment through an ES 8+ or ES 9+ interface between the first profile server and the user equipment.

S403b. After receiving the first request, the user equipment searches for the corresponding profile information based on the profile ICCID carried in the RPM request, and after finding the corresponding profile information, the user equipment sends, to the first profile server, the profile information that carries the second profile owner identifier.

[0068] The second implementation includes the following steps.

S403c. The first profile server may send a second request to the second profile server, where the second request is used to obtain the second profile owner identifier, and the second request may be a Get ProfileInfo interface command, and may carry at least one of an identifier of the second profile server, an EID, and an ICCID. The identifier of the second profile server is used to perform addressing on the corresponding second profile server, and the EID or the ICCID is used to search for a PO to which the corresponding profile belongs, to obtain the PO ID. For example, the PO may be read from the profile information stored in the second profile server, or the second profile server maintains a plurality of profiles of the RPM server, and searches for, based on the ICCID carried in the second request, a PO to which the corresponding profile belongs, to obtain the PO ID.

S403d. After obtaining the second profile owner identifier corresponding to the PO, the second profile server sends, to the first profile server, the second profile owner identifier or the profile information that carries the second profile owner identifier.

S404. The first profile server determines whether the first profile owner identifier is the same as the second profile owner identifier.

[0069] In specific implementation, the first profile server may compare the first profile owner identifier with the second profile owner identifier to verify or determine whether the first profile owner identifier is the same as the second profile owner identifier.

[0070] Further, when the first profile owner identifier includes only the profile owner identifier that is identifiable to the first profile server, the profile owner identifier that is identifiable to the first profile server in the first profile owner identifier needs to be separately compared with the profile owner identifier that is identifiable to the first profile server in the profile information and the profile owner identifier that is identifiable to the second profile server in the profile information, to verify whether the pro-

file owner identifier that is identifiable to the first profile server in the first profile owner identifier is the same as a profile owner identifier in the profile information. If the profile owner identifier that is identifiable to the first profile server in the first profile owner identifier is the same as a profile owner identifier in the profile information, it is determined that the first profile owner identifier is the same as the second profile owner identifier. If the profile owner identifier that is identifiable to the first profile server in the first profile owner identifier is different from any profile owner identifier in the profile information, it is determined that the first profile owner identifier is different from the second profile owner identifier. When the first profile owner identifier includes only the profile owner identifier that is identifiable to the second profile server, a verification method is the same as the foregoing method. Details are not described herein again. When the first profile owner identifier includes the profile owner identifier that is identifiable to the first profile server and the profile owner identifier that is identifiable to the second profile server, the profile owner identifier that is identifiable to the first profile server in the first profile owner identifier and the profile owner identifier that is identifiable to the second profile server in the first profile owner identifier need to be respectively compared with the profile owner identifier that is identifiable to the first profile server in the profile information and the profile owner identifier that is identifiable to the second profile server in the profile information. Only when the profile owner identifier that is identifiable to the first profile server in the first profile owner identifier is the same as the profile owner identifier that is identifiable to the first profile server in the profile information and the profile owner identifier that is identifiable to the second profile server in the first profile owner identifier is the same as the profile owner identifier that is identifiable to the second profile server in the profile information, it is determined that the first profile owner identifier is the same as the second profile owner identifier.

S405. The first profile server sends an RPM command to the user equipment when the first profile owner identifier is the same as the second profile owner identifier, where the RPM command carries the first profile owner identifier, the EID, and the ICCID.

S406. The first profile server sends a response message to the RPM server when the first profile owner identifier is different from the second profile owner identifier, where the response message is used to notify the RPM server of a verification error.

S407. After receiving the RPM command, the user equipment determines whether the first profile owner identifier is the same as the second profile owner identifier.

[0071] In specific implementation, the user equipment may first search for the second profile owner identifier in the profile information based on the ICCID carried in the RPM command, and compare the first profile owner identifier with the second profile owner identifier to verify whether the first profile owner identifier is the same as the second profile owner identifier. A specific verification method is the same as the verification method of the first profile server in S404. Details are not described herein again.

[0072] S408. The user equipment executes the RPM command when the first profile owner identifier is the same as the second profile owner identifier; or the user equipment may send a response message to the first profile server or the RPM server when the first profile owner identifier is different from the second profile owner identifier, where the response message is used to notify the RPM server of a verification error.

[0073] In this embodiment of this application, when the first profile server configured to manage the profile and the second profile server configured to download the profile are different servers, whether the RPM server that initiates the RPM command specific to the downloaded profile is an owner of the profile is verified; and a PO verification method is provided when different PO IDs are used by the two profile servers to identify a same PO. This not only prevents a third party from maliciously tampering with profile information that is not possessed by the third party, but also avoids a loss caused to an operator or a profile owner due to a user's access to an invalid network or random profile unlocking. In addition, the profile server verifies the PO on a network side. In this way, network security can be improved, a bidirectional authentication process between the profile server and a terminal can be reduced, and a waste of network resources can be reduced.

[0074] FIG. 5A and FIG. 5B are a schematic flowchart of an information verification method according to still another embodiment of this application. In this embodiment of this application, a first profile server configured to manage a profile and a second profile server configured to download the profile are different servers. The method includes but is not limited to the following steps.

[0075] S501. An RPM server or the second profile server updates profile information to user equipment. This step includes: S501a. The RPM server sends an update message to the user equipment. S501b. The second profile server sends an update message to the user equipment. The update message includes an identifier of the first profile server, and may further include a corresponding profile owner identifier.

[0076] In specific implementation, the RPM server or the second profile server may preconfigure information about the first profile server in the profile information, and preconfigure a profile owner identifier that is identifiable to the first profile server. The information about the first profile server may include the identifier of the first profile server.

[0077] After the foregoing information is configured, the user equipment may be assigned to the first profile server for remote profile management. Therefore, the

RPM server or the second profile server may send the update message to the user equipment. PO IDs of a same profile owner may be the same or different. Therefore, the PO IDs also need to be updated to the profile information. For example, if a PO ID assigned by a first SM DP+ to China Mobile is 46001, and a PO ID assigned by a second SM DP+ to China Mobile is CMCC, an identifier of the first SM DP+ and the corresponding identifier 46001 of China Mobile are stored in the profile information, and an identifier of the second SM DP+ and the corresponding identifier CMCC of China Mobile are also stored in the profile information, to subsequently search for and verify the PO. After receiving the update message, the user equipment updates the identifier of the first profile server and the corresponding profile owner identifier to the profile information. Optionally, the RPM server may further configure the identifier of the first profile server and the corresponding profile owner identifier in the profile information of the user equipment by using an over-the-air (Over-the-Air, OTA) message.

[0078] Optionally, after receiving the update request sent by the RPM server or the second profile server, the user equipment may verify identity validity of the RPM server or the second profile server based on the PO ID carried in the update request. Specifically, verification or identification may be performed based on information such as a message header field and an initiator certificate that are in the update message and that are used to identify an initiator, and the PO ID that is carried in the update message. For example, if the PO ID carried in the update request is the PO ID of China Mobile, it is verified whether the initiator of the update request is China Mobile. If the initiator of the update request is not China Mobile, it is verified that an identity of the initiator is invalid. If China Mobile is the initiator of the update request, it is verified that the identity of the initiator is valid. Further, the identifier of the first profile server and the corresponding profile owner identifier are updated to the local profile information. This prevents a third party from maliciously using the PO ID of China Mobile to manage the profile. In verification on the identity of the initiator, a verification operation of determining whether the initiator is a valid initiator, a verification operation of judging whether the initiator is a valid initiator, or the like may be performed.

[0079] S502. The RPM server sends an RPM request to the first profile server, where the RPM request includes a first profile owner identifier (PO ID), and the RPM request further includes at least one of an eUICC identifier (EID), a profile identifier (ICCID), and RPM command-related information, and the first profile owner identifier includes at least one of the following: a profile owner identifier that is identifiable to the first profile server or a profile owner identifier that is identifiable to the second profile server.

[0080] The profile owner identifier may vary with a specific implementation. For example, an MNO and an SM DP+ may agree on a profile owner identifier in advance, or an MNO and an SM DP+ may use an identifier of a message initiator between the MNO and the SM DP+ as a profile owner identifier. For another example, State Grid, serving as a company, manages a profile purchased by State Grid from the MNO. In this case, the first profile owner identifier may include a PO ID assigned by the MNO or the SM DP+ to State Grid. Alternatively, a mobile virtual network operator purchases a profile from the MNO. In this case, the first profile owner identifier may include a PO ID assigned to the MVNO. This ensures that State Grid or the MVNO manages the profile of State Grid or the MVNO by using the MNO.

[0081] Optionally, after receiving the RPM request initiated by the RPM server, the first profile server may verify identity validity of the RPM server based on the PO ID carried in the RPM request. Specifically, verification or identification may be performed based on information such as a message header field and an initiator certificate that are in the message sent by the RPM server to the first profile server and that are used to identify an initiator, and the PO ID that is carried in the RPM request. For example, if the PO ID carried in the RPM request is a PO ID of China Mobile, it is verified whether the initiator of the RPM request is China Mobile. If the initiator of the RPM request is not China Mobile, it is verified that the identity of the initiator is invalid. If the initiator of the RPM request is China Mobile, it is verified that the identity of the initiator is valid. This prevents a third party from maliciously using the PO ID of China Mobile to manage the profile. In verification on the identity of the initiator, a verification operation of determining whether the initiator is a valid initiator, a verification operation of judging whether the initiator is a valid initiator, or the like may be performed.

[0082] S503. The first profile server obtains a second profile owner identifier in profile information, where the second profile owner identifier includes at least one of the following: a profile owner identifier that is identifiable to the first profile server or a profile owner identifier that is identifiable to the second profile server. The following two optional manners are included.

[0083] The first implementation includes the following steps:

S503a. The first profile server may send a first request to the user equipment, where the first request is used to obtain the second profile owner identifier, and the first request may be a Get ProfileInfo interface command, and may carry at least one of an identifier of the second profile server, an EID, and an ICCID. Specifically, after a secure channel is established between the first profile server and the user equipment, the first profile server may send the first request to the user equipment through an ES 8+ or ES 9+ interface between the first profile server and the user equipment.

S503b. After receiving the first request, the user equipment searches for the corresponding profile information based on the profile ICCID carried in the

RPM request, and after finding the corresponding profile information, the user equipment sends, to the first profile server, the profile information that carries the second profile owner identifier.

[0084] The second implementation includes the following steps.

S503c. The first profile server may send a second request to the second profile server, where the second request is used to obtain the second profile owner identifier, and the second request may be a Get ProfileInfo interface command, and may carry at least one of an identifier of the second profile server, an EID, and an ICCID. The identifier of the second profile server is used to perform addressing on the corresponding second profile server, and the EID or the is used to search for a PO to which the corresponding profile belongs, to obtain the PO ID. For example, the PO may be read from the profile information stored in the second profile server, or the second profile server maintains a plurality of profiles of the RPM server, and searches for, based on the ICCID carried in the second request, a PO to which the corresponding profile belongs, to obtain the PO ID.

S503d. After obtaining the second profile owner identifier corresponding to the PO, the second profile server sends, to the first profile server, the second profile owner identifier or the profile information that carries the second profile owner identifier.

S504. The first profile server determines whether the first profile owner identifier is the same as the second profile owner identifier.

[0085] In specific implementation, the first profile server may compare the first profile owner identifier with the second profile owner identifier to verify or determine whether the first profile owner identifier is the same as the second profile owner identifier.

[0086] S505. The first profile server sends an RPM command to the user equipment when the first profile owner identifier is the same as the second profile owner identifier, where the RPM command carries the first profile owner identifier, the EID, and the ICCID.

[0087] It should be noted that the first profile owner identifier includes at least one of the following: a profile owner identifier that is identifiable to the first profile server or a profile owner identifier that is identifiable to the second profile server. The second profile owner identifier also includes at least one of the following: a profile owner identifier that is identifiable to the first profile server or a profile owner identifier that is identifiable to the second profile server. Although the profile owner identifier that is identifiable to the first profile server and the profile owner identifier that is identifiable to the second profile server are PO IDs of a same PO, the profile owner identifier that is identifiable to the first profile server and the profile owner identifier that is identifiable to the second profile server may be different. Therefore, the first profile server may verify that the profile owner identifier that is identifiable to the first profile server and the profile owner identifier that is identifiable to the second profile server are different. Further verification needs to be performed in the following manner.

[0088] S506. The first profile server obtains an identifier correspondence list when the first profile owner identifier is different from the second profile owner identifier.

[0089] In specific implementation, the first profile server may obtain the identifier correspondence list from the RPM server; obtain the identifier correspondence list from the second profile server; or obtain the identifier correspondence list from the local memory. The identifier correspondence list includes a correspondence between a profile server identifier corresponding to a profile owner and a profile owner identifier. For example, if a PO ID assigned by a first SM DP+ to China Mobile is 46001, and a PO ID assigned by a second SM DP+ is CMCC, an identifier of the first SM DP+ and the corresponding identifier 46001 of China Mobile are stored in the identifier correspondence list, and an identifier of the second SM DP+ and the corresponding identifier CMCC of China Mobile are also stored in the identifier correspondence list, to search for and verify the PO.

[0090] S507. The first profile server determines whether a profile owner identifier corresponding to the first profile owner identifier exists in the identifier correspondence list.

[0091] In specific implementation, the profile owner identifier that is identifiable to the first profile server or the profile owner identifier that is identifiable to the second profile server may be separately compared with a profile owner identifier in the identifier correspondence list, to determine whether the profile owner identifier corresponding to the first profile owner identifier exists in the identifier corresponding list.

[0092] S508. The first profile server sends the RPM command to the user equipment when the profile owner identifier corresponding to the first profile owner identifier exists in the identifier correspondence list.

[0093] S509. The first profile server sends a response message to the RPM server when the profile owner identifier corresponding to the first profile owner identifier does not exist in the identifier correspondence list, where the response message is used to notify the RPM server of a verification error.

[0094] S510. After receiving the RPM command, the user equipment determines whether the first profile owner identifier is the same as the second profile owner identifier.

[0095] In specific implementation, the user equipment may first search for the second profile owner identifier in the profile information based on the ICCID carried in the RPM command, and compare the first profile owner identifier with the second profile owner identifier to verify whether the first profile owner identifier is the same as

the second profile owner identifier. A specific verification method is the same as the verification method of the first profile server in S504 to S507. Details are not described herein.

[0096] S511. The user equipment executes the RPM command when the first profile owner identifier is the same as the second profile owner identifier; or the user equipment may send a response message to the first profile server or the RPM server when the first profile owner identifier is different from the second profile owner identifier, where the response message is used to notify the RPM server of a verification error.

[0097] In this embodiment of this application, when the first profile server configured to manage the profile and the second profile server configured to download the profile are different servers, whether the RPM server that initiates the RPM command specific to the downloaded profile is an owner of the profile is verified; and a PO verification method is provided when different PO IDs are used by the two profile servers to identify a same PO. In addition, based on the foregoing embodiment, for the identifier correspondence list maintained by the profile server, when verifying that the first profile owner identifier is different from the second profile owner identifier, the first profile server may further verify, based on the correspondence list, whether the PO IDs belong to a same profile owner. This not only prevents a third party from maliciously tampering with profile information that is not possessed by the third party, but also avoids a loss caused to an operator or a profile owner due to a user's access to an invalid network or random profile unlocking. In addition, the profile server verifies the PO on a network side. In this way, network security can be improved, a bidirectional authentication process between the profile server and a terminal can be reduced, and a waste of network resources can be reduced.

[0098] FIG. 6 is a schematic flowchart of an information verification method according to yet another embodiment of this application. In this embodiment of this application, a first profile server configured to manage a profile and a second profile server configured to download the profile are different servers. The method includes but is not limited to the following steps.

[0099] S601. An RPM server or the second profile server updates profile information to user equipment. This step includes: S601a. The RPM server sends an update message to the user equipment. S601b. The second profile server sends an update message to the user equipment. The update message includes an identifier of the first profile server, and may further include a corresponding profile owner identifier.

[0100] In specific implementation, the RPM server or the second profile server may preconfigure information about the first profile server in the profile information, and preconfigure a profile owner identifier that is identifiable to the first profile server. The information about the first profile server may include the identifier of the first profile server.

[0101] After the foregoing information is configured, the user equipment may be assigned to the first profile server for remote profile management. Therefore, the RPM server or the second profile server may send the update message to the user equipment. PO IDs of a same profile owner may be the same or different. Therefore, the PO IDs also need to be updated to the profile information. For example, if a PO ID assigned by a first SM DP+ to China Mobile is 46001, and a PO ID assigned by a second SM DP+ is CMCC, an identifier of the first SM DP+ and the corresponding identifier 46001 of China Mobile are stored in the profile information, and the identifier of the second SM DP+ and the corresponding identifier CMCC of China Mobile are also stored in the profile information, to subsequently search for and verify the PO. After receiving the update message, the user equipment updates the identifier of the first profile server and the corresponding profile owner identifier to the profile information. Optionally, the RPM server may further configure the identifier of the first profile server and the corresponding profile owner identifier in the profile information of the user equipment by using an over-the-air (Over-the-Air, OTA) message.

[0102] Optionally, after receiving the update request sent by the RPM server or the second profile server, the user equipment may verify identity validity of the RPM server or the second profile server based on the PO ID carried in the update request. Specifically, verification or identification may be performed by using information such as a message header field and an initiator certificate that are in the update message and that are used to identify an initiator, and the PO ID that is carried in the update message. For example, if the PO ID carried in the update request is the PO ID of China Mobile, it is verified whether the initiator of the update request is China Mobile. If the initiator of the update request is not China Mobile, it is verified that an identity of the initiator is invalid. If the initiator of the update request is China Mobile, it is verified that the identity of the initiator is valid. Further, the identifier of the first profile server and the corresponding profile owner identifier are updated to the local profile information. This prevents a third party from maliciously using the PO ID of China Mobile to manage the profile.

[0103] S602. The RPM server may determine whether the first profile server configured to manage the profile and the second profile server previously configured to download the profile are a same server. When the first profile server and the second profile server are different servers, the RPM server determines a profile owner identifier that is identifiable to the first profile server or a profile owner identifier that is identifiable to the second profile server. Although the profile owner identifier that is identifiable to the first profile server and the profile owner identifier that is identifiable to the second profile server are PO IDs of a same PO, the profile owner identifier that is identifiable to the first profile server and the profile owner identifier that is identifiable to the second profile server may be different. Therefore, a correspondence between

the identifier of the first profile server and the profile owner identifier and a correspondence between the identifier of the second profile server and the profile owner identifier are separately established.

[0104] S603. The RPM server sends an RPM request to the first profile server. The RPM request includes a first profile owner identifier (PO ID), and the RPM request further includes at least one of an eUICC identifier (EID), a profile identifier (ICCID), or RPM command-related information.

[0105] The first profile owner identifier includes at least one of the following: a profile owner identifier that is identifiable to the first profile server or a profile owner identifier that is identifiable to the second profile server. Further, the first profile owner identifier may include a profile server identifier and a profile owner identifier, including the identifier of the first profile server and the corresponding profile owner identifier that is identifiable to the first profile server, or the identifier of the second profile server and the corresponding profile owner identifier that is identifiable to the second profile server.

[0106] In addition, the profile owner identifier may vary with a specific implementation. For example, an MNO and an SM DP+ may agree on a profile owner identifier in advance, or an MNO and an SM DP+ may use an identifier of a message initiator between the MNO and the SM DP+ as a profile owner identifier. For another example, State Grid, serving as a company, manages a profile purchased by State Grid from the MNO. In this case, the first profile owner identifier may include a PO ID assigned by the MNO or the SM DP+ to State Grid. Alternatively, a mobile virtual network operator (Mobile Virtual Network Operator, MVNO) purchases a profile from the MNO. In this case, the first profile owner identifier may include a PO ID assigned to the MVNO. This ensures that State Grid or the MVNO manages the profile of State Grid or the MVNO by using the MNO.

[0107] Optionally, after receiving the RPM request initiated by the RPM server, the first profile server may verify identity validity of the RPM server based on the PO ID carried in the RPM request. Specifically, verification or identification may be performed by using information such as a message header field and an initiator certificate that are in the message sent by the RPM server to the first profile server and that are used to identify an initiator, and the PO ID that is carried in the RPM request. For example, if the PO ID carried in the RPM request is a PO ID of China Mobile, it is verified whether the initiator of the RPM request is China Mobile. If the initiator of the RPM request is not China Mobile, it is verified that an identity of the initiator is invalid. If the initiator of the RPM request is China Mobile, it is verified that the identity of the initiator is valid. This prevents a third party from maliciously using the PO ID of China Mobile to manage the profile. In verification on the identity of the initiator, a verification operation of determining whether the initiator is a valid initiator, a verification operation of judging whether the initiator is a valid initiator, or the like may be performed.

[0108] S604. The first profile server obtains a second profile owner identifier in profile information. The second profile owner identifier includes at least one of the following: a profile owner identifier that is identifiable to the first profile server or a profile owner identifier that is identifiable to the second profile server. The following two optional manners are included.

[0109] The first implementation includes the following steps:

S604a. The first profile server may send a first request to the user equipment, where the first request is used to obtain the second profile owner identifier, and the first request may be a Get ProfileInfo interface command, and may carry at least one of the identifier of the second profile server, an EID, and an ICCID. Specifically, after a secure channel is established between the first profile server and the user equipment, the first profile server may send the first request to the user equipment through an ES 8+ or ES 9+ interface between the first profile server and the user equipment.

S604b. After receiving the first request, the user equipment searches for the corresponding profile information based on the profile ICCID carried in the RPM request, and after finding the corresponding profile information, the user equipment sends, to the first profile server, the profile information that carries the second profile owner identifier.

[0110] The second implementation includes the following steps.

[0111] S604c. The first profile server may send a second request to the second profile server, where the second request is used to obtain the second profile owner identifier, and the second request may be a Get ProfileInfo interface command, and may carry at least one of the identifier of the second profile server, an EID, and an ICCID. The identifier of the second profile server is used to perform addressing on the corresponding second profile server, and the EID or the is used to search for a PO to which the corresponding profile belongs, to obtain the PO ID. For example, the PO may be read from the profile information stored in the second profile server, or the second profile server maintains a plurality of profiles of the RPM server, and searches for, based on the ICCID carried in the second request, a PO to which the corresponding profile belongs, to obtain the PO ID.

[0112] S604d. After obtaining the second profile owner identifier corresponding to the PO, the second profile server sends, to the first profile server, the profile information that carries the second profile owner identifier.

[0113] In this embodiment of this application, because the first profile owner identifier includes a profile server identifier and a profile owner identifier, the second profile owner identifier that is identifiable to the first profile server in the profile information may be obtained based on the

identifier of the first profile server included in the first profile owner identifier. Alternatively, the second profile owner identifier that is identifiable to the second profile server in the profile information is obtained based on the identifier of the second profile server included in the first profile owner identifier.

[0114] S605. The first profile server determines whether the first profile owner identifier is the same as the second profile owner identifier.

[0115] In specific implementation, the first profile server may compare the first profile owner identifier with the second profile owner identifier to verify or determine whether the first profile owner identifier is the same as the second profile owner identifier.

[0116] S606. The first profile server sends an RPM command to the user equipment when the first profile owner identifier is the same as the second profile owner identifier, where the RPM command carries the first profile owner identifier, the EID, and the ICCID.

[0117] S607. The first profile server sends a response message to the RPM server when the first profile owner identifier is different from the second profile owner identifier, where the response message is used to notify the RPM server of a verification error.

[0118] S608. After receiving the RPM command, the user equipment determines whether the first profile owner identifier is the same as the second profile owner identifier.

[0119] In specific implementation, the user equipment may first search for the second profile owner identifier in the profile information based on the ICCID carried in the RPM command, and compare the first profile owner identifier with the second profile owner identifier to verify or determine whether the first profile owner identifier is the same as the second profile owner identifier. A specific verification method is the same as the verification method of the first profile server in S605. Details are not described herein.

[0120] S609. The user equipment executes the RPM command when the first profile owner identifier is the same as the second profile owner identifier; or the user equipment may send a response message to the first profile server or the RPM server when the first profile owner identifier is different from the second profile owner identifier, where the response message is used to notify the RPM server of a verification error.

[0121] In this embodiment of this application, when the first profile server configured to manage the profile and the second profile server configured to download the profile are different servers, whether the RPM server that initiates the RPM command specific to the downloaded profile is an owner of the profile is verified; and a PO verification method is provided when different PO IDs are used by the two profile servers to identify a same PO. In addition, the RPM server determines the profile owner identifier that is identifiable to the first profile server or the profile owner identifier that is identifiable to the second profile server, so that the first profile server obtains a corresponding profile owner identifier for verification. This not only prevents a third party from maliciously tampering with profile information that is not possessed by the third party, but also avoids a loss caused to an operator or a profile owner due to a user's access to an invalid network or random profile unlocking. In addition, the profile server verifies the PO on a network side. In this way, network security can be improved, a bidirectional authentication process between the profile server and a terminal can be reduced, and a waste of network resources can be reduced.

[0122] The foregoing describes in detail the methods in the embodiments of this application. The following provides apparatuses in the embodiments of this application.

[0123] FIG. 7 is a schematic structural diagram of a first profile server according to an embodiment of this application. The first profile server may include a receiving module 701, an obtaining module 702, a processing module 703, and a sending module 704. Detailed descriptions of the modules are as follows:

[0124] The receiving module 701 is configured to receive an RPM request sent by an RPM server, where the RPM request includes a first profile owner identifier.

[0125] The obtaining module 702 is configured to obtain a second profile owner identifier in profile information.

[0126] The processing module 703 is configured to determine whether the first profile owner identifier is the same as the second profile owner identifier.

[0127] The sending module 704 is configured to send an RPM command to user equipment when the first profile owner identifier is the same as the second profile owner identifier.

[0128] Optionally, the obtaining module 702 is specifically configured to obtain the second profile owner identifier in the profile information from a local memory.

[0129] Optionally, the obtaining module 702 is specifically configured to: send a first request to the user equipment, where the first request is used to obtain the second profile owner identifier; and receive the profile information that is sent by the user equipment and that carries the second profile owner identifier.

[0130] Optionally, the obtaining module 702 is specifically configured to: send a second request to a second profile server, where the second request is used to obtain the second profile owner identifier; and receive the profile information that is sent by the second profile server and that carries the second profile owner identifier.

[0131] Optionally, the first profile owner identifier and the second profile owner identifier each include at least one of the following: a profile owner identifier that is identifiable to the first profile server or a profile owner identifier that is identifiable to the second profile server.

[0132] Optionally, the obtaining module 702 is further configured to obtain an identifier correspondence list when the first profile owner identifier is different from the second profile owner identifier, where the identifier correspondence list includes a correspondence between a

profile server identifier and a profile owner identifier; the processing module 703 is further configured to determine whether a profile owner identifier corresponding to the first profile owner identifier exists in the identifier correspondence list; and the sending module 704 is further configured to send the RPM command to the user equipment when the profile owner identifier corresponding to the first profile owner identifier exists in the identifier correspondence list.

[0133] Optionally, the obtaining module 702 is specifically configured to: obtain the identifier correspondence list from the RPM server; obtain the identifier correspondence list from the second profile server; or obtain the identifier correspondence list from the local memory.

[0134] Optionally, the first profile server is a server configured to manage a profile, and the second profile server is a server configured to download the profile.

[0135] Optionally, the profile owner identifier includes a profile server identifier and a profile owner identifier.

[0136] It should be noted that, for implementation of the modules, refer to corresponding descriptions of the method embodiments shown in FIG. 3 to FIG. 6. The modules perform the methods and the functions performed by the first profile server in the foregoing embodiments.

[0137] FIG. 8 is a schematic structural diagram of user equipment according to an embodiment of this application. The user equipment may include a receiving module 801, an obtaining module 802, a processing module 803, and an execution module 804. Detailed descriptions of the modules are as follows:

[0138] The receiving module 801 is configured to receive an RPM command sent by a first profile server, where the RPM command includes a first profile owner identifier.

[0139] The obtaining module 802 is configured to obtain a second profile owner identifier in profile information.

[0140] The processing module 803 is configured to determine whether the first profile owner identifier is the same as the second profile owner identifier.

[0141] The execution module 804 is configured to execute the RPM command when the first profile owner identifier is the same as the second profile owner identifier.

[0142] Optionally, the receiving module 801 is further configured to receive an update message sent by an RPM server or a second profile server, where the update message includes an identifier of the first profile server and a corresponding profile owner identifier.

[0143] Optionally, the first profile owner identifier includes at least one of the following: a profile owner identifier that is identifiable to the first profile server or a profile owner identifier that is identifiable to the second profile server.

[0144] Optionally, the obtaining module 802 is further configured to obtain an identifier correspondence list when the first profile owner identifier is different from the second profile owner identifier, where the identifier correspondence list includes a correspondence between a profile server identifier and a profile owner identifier; the processing module 803 is further configured to determine whether a profile owner identifier corresponding to the first profile owner identifier exists in the identifier correspondence list; and the execution module 804 is further configured to execute the RPM command when the profile owner identifier corresponding to the first profile owner identifier exists in the identifier correspondence list.

[0145] Optionally, the receiving module 801 is further configured to receive a first request sent by the first profile server, where the first request is used to obtain the second profile owner identifier; and the sending module 805 is configured to send, to the first profile server, the profile information that carries the second profile owner identifier.

[0146] It should be noted that, for implementation of the modules, refer to corresponding descriptions of the method embodiments shown in FIG. 3 to FIG. 6. The modules perform the methods and the functions performed by the user equipment in the foregoing embodiments.

[0147] FIG. 9 is a schematic structural diagram of an RPM server according to an embodiment of this application. The RPM server may include a sending module 901 and a processing module 902. Detailed descriptions of the modules are as follows:

[0148] The sending module 901 is configured to send an RPM request to a first profile server, where the RPM request includes a first profile owner identifier, and the RPM request is used to instruct the first profile server to determine whether a second profile owner identifier in profile information is the same as the first profile owner identifier; and send an RPM command to user equipment when the second profile owner identifier is the same as the first profile owner identifier.

[0149] Optionally, the processing module 902 is configured to: determine whether the first profile server configured to manage a profile and a second profile server previously configured to download the profile are a same server; and when the first profile server and the second profile server are different servers, determine a profile owner identifier that is identifiable to the first profile server or a profile owner identifier that is identifiable to the second profile server.

[0150] It should be noted that, for implementation of the modules, refer to corresponding descriptions of the method embodiments shown in FIG. 3 to FIG. 6. The modules perform the methods and the functions performed by the RPM server in the foregoing embodiments.

[0151] FIG. 10 is a schematic structural diagram of another first profile server according to this application. As shown in the figure, the first profile server may include at least one processor 1001, at least one communications interface 1002, at least one memory 1003, and at least one communications bus 1004.

[0152] The processor 1001 may be a central process-

ing unit, a general-purpose processor, a digital signal processor, an application-specific integrated circuit, a field programmable gate array or another programmable logical device, a transistor logical device, a hardware component, or any combination thereof. The processor 1001 may implement or execute various example logical blocks, modules, and circuits described with reference to content disclosed in this application. Alternatively, the processor may be a combination of processors implementing a computing function, for example, a combination of one or more microprocessors, or a combination of a digital signal processor and a microprocessor. The communications bus 1004 may be a peripheral component interconnect PCI bus, an extended industry standard architecture EISA bus, or the like. The bus may be classified into an address bus, a data bus, a control bus, or the like. For ease of representation, only one thick line is used to represent the bus in FIG. 10, but this does not mean that there is only one bus or only one type of bus. The communications bus 1004 is configured to implement connection and communication between these components. The communications interface 1002 in the device in this embodiment of this application is configured to perform signaling or data communication with another node device. The memory 1003 may include a volatile memory such as a nonvolatile random access memory (Nonvolatile Random Access Memory, NVRAM), a phase change random access memory (Phase Change RAM, PRAM), or a magnetoresistive random access memory (Magetoresistive RAM, MRAM), or may include a nonvolatile memory such as at least one magnetic disk storage device, an electrically erasable programmable read-only memory (Electrically Erasable Programmable Read-Only Memory, EEPROM), a flash storage device such as a NOR flash memory (NOR flash memory) or a NAND flash memory (NAND flash memory), a semiconductor such as a solid state disk (Solid State Disk, SSD), or the like. Optionally, the memory 1003 may be at least one storage apparatus far away from the processor 1001. The memory 1003 stores a group of program code, and the processor 1001 executes a program in the memory 1003 that is executed by the foregoing first profile server.

[0153] An RPM request sent by an RPM server is received by using the communications interface 1002, and the RPM request includes a first profile owner identifier; a second profile owner identifier in profile information is obtained;
it is determined whether the first profile owner identifier is the same as the second profile owner identifier; and
an RPM command is sent by using the communications interface 1002 to user equipment when the first profile owner identifier is the same as the second profile owner identifier.

[0154] Optionally, the processor 1001 is further configured to perform the following operation:
obtaining the second profile owner identifier in the profile information from a local memory.

[0155] Optionally, the processor 1001 is further configured to perform the following operations:

sending a first request to the user equipment by using the communications interface 1002, where the first request is used to obtain the second profile owner identifier; and
receiving, by using the communications interface 1002, the profile information that is sent by the user equipment and that carries the second profile owner identifier.

[0156] Optionally, the processor 1001 is further configured to perform the following operations:

sending a second request to a second profile server by using the communications interface 1002, where the second request is used to obtain the second profile owner identifier; and
receiving, by using the communications interface 1002, the profile information that is sent by the second profile server and that carries the second profile owner identifier.

[0157] The first profile owner identifier and the second profile owner identifier each include at least one of the following: a profile owner identifier that is identifiable to the first profile server or a profile owner identifier that is identifiable to the second profile server.

[0158] Optionally, the processor 1001 is further configured to perform the following operations:

obtaining an identifier correspondence list when the first profile owner identifier is different from the second profile owner identifier, where the identifier correspondence list includes a correspondence between a profile server identifier and a profile owner identifier;
determining whether a profile owner identifier corresponding to the first profile owner identifier exists in the identifier correspondence list; and
when a profile owner identifier corresponding to the first profile owner identifier exists in the identifier correspondence list, sending the RPM command to the user equipment by using the communications interface 1002.

[0159] Optionally, the processor 1001 is further configured to perform the following operations:

obtaining the identifier correspondence list from the RPM server;
obtaining the identifier correspondence list from the second profile server; or
obtaining the identifier correspondence list from the local memory.

[0160] The first profile server is a server configured to manage a profile, and the second profile server is a server

configured to download the profile.

[0161] The profile owner identifier includes a profile server identifier and a profile owner identifier.

[0162] Further, the processor may further cooperate with the memory and the communications interface to perform the operations of the first profile server in the foregoing embodiments of this application.

[0163] FIG. 11 is a schematic structural diagram of other user equipment according to this application. As shown in the figure, the user equipment may include at least one processor 1101, at least one communications interface 1102, at least one memory 1103, and at least one communications bus 1104.

[0164] The processor 1101 may be the various types of processors mentioned above. The communications bus 1104 may be a peripheral component interconnect PCI bus, an extended industry standard architecture EISA bus, or the like. The bus may be classified into an address bus, a data bus, a control bus, or the like. For ease of representation, only one thick line is used to represent the bus in FIG. 11, but this does not mean that there is only one bus or only one type of bus. The communications bus 1104 is configured to implement connection and communication between these components. The communications interface 1102 in the device in this embodiment of this application is configured to perform signaling or data communication with another node device. The memory 1103 may be the various types of memories mentioned above. Optionally, the memory 1103 may be at least one storage apparatus far away from the processor 1101. The memory 1103 stores a group of program code, and the processor 1101 executes a program in the memory 1103 that is executed by the foregoing user equipment.

[0165] An RPM command sent by a first profile server is received by using the communications interface 1102, where the RPM command includes a first profile owner identifier;
a second profile owner identifier in profile information is obtained;
it is determined whether the first profile owner identifier is the same as the second profile owner identifier; and
the RPM command is executed when the first profile owner identifier is the same as the second profile owner identifier.

[0166] Optionally, the processor 1101 is further configured to perform the following operation:
receiving, by using the communications interface 1102, an update message sent by an RPM server or a second profile server, where the update message includes an identifier of the first profile server and a corresponding profile owner identifier.

[0167] The first profile owner identifier includes at least one of the following: a profile owner identifier that is identifiable to the first profile server or a profile owner identifier that is identifiable to the second profile server.

[0168] Optionally, the processor 1101 is further configured to perform the following operation:
obtaining an identifier correspondence list when the first profile owner identifier is different from the second profile owner identifier, where the identifier correspondence list includes a correspondence between a profile server identifier and a profile owner identifier;
determining whether a profile owner identifier corresponding to the first profile owner identifier exists in the identifier correspondence list; and
executing the RPM command when the profile owner identifier corresponding to the first profile owner identifier exists in the identifier correspondence list.

[0169] Optionally, the processor 1101 is further configured to perform the following operations:
receiving, by using the communications interface 1102, a first request sent by the first profile server, where the first request is used to obtain the second profile owner identifier; and
sending, to the first profile server by using the communications interface 1102, the profile information that carries the second profile owner identifier.

[0170] Further, the processor may further cooperate with the memory and the communications interface to perform the operations of the user equipment in the foregoing embodiments of this application.

[0171] FIG. 12 is a schematic structural diagram of another RPM server according to this application. As shown in the figure, the RPM server may include at least one processor 1201, at least one communications interface 1202, at least one memory 1203, and at least one communications bus 1204.

[0172] The processor 1201 may be the various types of processors mentioned above. The communications bus 1204 may be a peripheral component interconnect PCI bus, an extended industry standard architecture EISA bus, or the like. The bus may be classified into an address bus, a data bus, a control bus, or the like. For ease of representation, only one thick line is used to represent the bus in FIG. 12, but this does not mean that there is only one bus or only one type of bus. The communications bus 1204 is configured to implement connection and communication between these components. The communications interface 1202 in the device in this embodiment of this application is configured to perform signaling or data communication with another node device. The memory 1203 may be the various types of memories mentioned above. Optionally, the memory 1203 may be at least one storage apparatus far away from the processor 1201. The memory 1203 stores a group of program code, and the processor 1201 executes a program in the memory 1203 that is executed by the foregoing RPM server.

[0173] An RPM request is sent to a first profile server by using the communications interface 1202, where the RPM request includes a first profile owner identifier, and

the RPM request is used to instruct the first profile server to determine whether a second profile owner identifier in profile information is the same as the first profile owner identifier; and an RPM command is sent to user equipment when the second profile owner identifier is the same as the first profile owner identifier.

[0174] Optionally, the processor 1201 is further configured to perform the following operations:

determining whether the first profile server configured to manage a profile and a second profile server previously configured to download the profile are a same server; and

when the first profile server and the second profile server are different servers, determining a profile owner identifier that is identifiable to the first profile server or a profile owner identifier that is identifiable to the second profile server.

[0175] Further, the processor may further cooperate with the memory and the communications interface to perform the operations of the RPM server in the foregoing embodiments of this application.

[0176] All or some of the foregoing embodiments may be implemented by using software, hardware, firmware, or any combination thereof. When software is used to implement the embodiments, all or some of the embodiments may be implemented in a form of a computer program product. The computer program product includes one or more computer instructions. When the computer program instructions are loaded and executed on a computer, the procedure or functions according to the embodiments of this application are all or partially generated. The computer may be a general-purpose computer, a dedicated computer, a computer network, or other programmable apparatuses. The computer instructions may be stored in a computer-readable storage medium or may be transmitted from a computer-readable storage medium to another computer-readable storage medium. For example, the computer instructions may be transmitted from a website, computer, server, or data center to another website, computer, server, or data center in a wired (for example, a coaxial cable, an optical fiber, or a digital subscriber line (DSL)) or wireless (for example, infrared, radio, or microwave) manner. The computer-readable storage medium may be any usable medium accessible by a computer, or a data storage device, such as a server or a data center, integrating one or more usable media. The usable medium may be a magnetic medium (for example, a floppy disk, a hard disk, or a magnetic tape), an optical medium (for example, a DVD), a semiconductor medium (for example, a solid state disk Solid State Disk (SSD)), or the like.

[0177] The objectives, technical solutions, and beneficial effects of the present invention have been described in more detail with reference to the foregoing specific embodiments. Any modification, equivalent replacement, or improvement made without departing from the principle of the present invention shall fall within the protection scope of the present invention.

Claims

1. An information verification method, wherein the method comprises:

   receiving (S301, S402, S502, S603), by a first profile server, a remote profile management request sent by a remote profile management server, wherein the remote profile management request comprises a first profile owner identifier;
   obtaining (S302, S403, S503, S604), by the first profile server, a second profile owner identifier in profile information;
   determining (S303, S404, S504, S605), by the first profile server, whether the first profile owner identifier is the same as the second profile owner identifier; and
   sending (S304, S405, S505, S606), by the first profile server, a remote profile management command to a user equipment when the first profile owner identifier is the same as the second profile owner identifier;
   characterized in that
   the first profile owner identifier and the second profile owner identifier each comprise at least one of the following: a profile owner identifier that is identifiable to the first profile server or a profile owner identifier that is identifiable to the second profile server;
   and in that the method further comprises:

      obtaining (S506), by the first profile server, an identifier correspondence list when the first profile owner identifier is different from the second profile owner identifier, wherein the identifier correspondence list comprises a correspondence between a profile server identifier and a profile owner identifier;
      determining (S507), by the first profile server, whether a profile owner identifier corresponding to the first profile owner identifier exists in the identifier correspondence list; and
      sending (S508), by the first profile server, the remote profile management command to the user equipment when the profile owner identifier corresponding to the first profile owner identifier exists in the identifier correspondence list.

2. The method according to claim 1, wherein the obtaining, by the first profile server, a second profile owner identifier in the profile information comprises:
   obtaining (S302), by the first profile server, the sec-

ond profile owner identifier in the profile information from a local memory.

3. The method according to claim 1, wherein the obtaining, by the first profile server, a second profile owner identifier in the profile information comprises:

sending (S302b, S403a, S503a, S604a) by the first profile server, a first request to the user equipment, wherein the first request is used to obtain the second profile owner identifier; and
receiving (S302c, S403b, S503b, S604b) by the first profile server, the profile information that is sent by the user equipment and that carries the second profile owner identifier.

4. The method according to claim 1, wherein the obtaining, by the first profile server, a second profile owner identifier in the profile information comprises:

sending (S403c, S503c, S604c) by the first profile server, a second request to a second profile server, wherein the second request is used to obtain the second profile owner identifier; and
receiving (S403d, S503d, S604d), by the first profile server, the profile information that is sent by the second profile server and that carries the second profile owner identifier.

5. The method according to claim 1, wherein the obtaining, by the first profile server, an identifier correspondence list comprises:

obtaining, by the first profile server, the identifier correspondence list from the remote profile management server;
obtaining, by the first profile server, the identifier correspondence list from the second profile server; or
obtaining, by the first profile server, the identifier correspondence list from the local memory.

6. The method according to any one of claims 1 to 5, wherein the first profile server is a server configured to manage a profile, and the second profile server is a server configured to download the profile.

7. An information verification method, wherein the method comprises:

receiving (S304, S405, S505 or S508, S606), by a user equipment, a remote profile management command sent by a first profile server, wherein the remote profile management command comprises a first profile owner identifier;
obtaining, by the user equipment, a second profile owner identifier in profile information;
determining (S306, S407, S510, S608), by the user equipment, whether the first profile owner identifier is the same as the second profile owner identifier; and
executing (S307, S408, S511, S609) by the user equipment, the remote profile management command when the first profile owner identifier is the same as the second profile owner identifier;
characterized in that
the first profile owner identifier comprises at least one of the following: a profile owner identifier that is identifiable to the first profile server or a profile owner identifier that is identifiable to a second profile server;
and in that the method further comprises:

obtaining, by the user equipment, an identifier correspondence list when the first profile owner identifier is different from the second profile owner identifier, wherein the identifier correspondence list comprises a correspondence between a profile server identifier and a profile owner identifier;
determining, by the user equipment, whether a profile owner identifier corresponding to the first profile owner identifier exists in the identifier correspondence list; and
executing, by the user equipment, the remote profile management command when the profile owner identifier corresponding to the first profile owner identifier exists in the identifier correspondence list.

8. The method according to claim 7, before the receiving, by the user equipment, a remote profile management command sent by a first profile server, further comprising:
receiving (S401, S501, S601), by the user equipment, an update message sent by a remote profile management server or the second profile server, wherein the update message comprises an identifier of the first profile server and a corresponding profile owner identifier.

9. The method according to claims 7 or 8, before the receiving, by user equipment, a remote profile management command sent by a first profile server, further comprising:

receiving, by the user equipment, a first request sent by the first profile server, wherein the first request is used to obtain the second profile owner identifier; and
sending, by the user equipment to the first profile server, the profile information that carries the second profile owner identifier.

10. A first profile server, comprising a memory, a com-

munications bus, and a processor, wherein the memory is configured to store program code that, when executed by the processor, cause the first profile server to implement the method according to any one of claims 1-6.

11. A user equipment, comprising a memory, a communications bus, and a processor, wherein the memory is configured to store program code, that, when executed by the processor, cause the user equipment to implement the method according to any one of claims 7-9.

Patentansprüche

1. Verfahren zur Informationsüberprüfung, wobei das Verfahren Folgendes umfasst:

Empfangen (S301, S402, S502, S603) einer von einem Remote-Profilverwaltungsserver gesendeten Remote-Profilverwaltungsanforderung durch einen ersten Profilserver, wobei die Remote-Profilverwaltungsanforderung eine erste Profilinhaberkennung umfasst;
Erhalten (S302, S403, S503, S604) einer zweiten Profilinhaberkennung in Profilinformationen durch den ersten Profilserver;
Bestimmen (S303, S404, S504, S605) durch den ersten Profilserver, ob die erste Profilinhaberkennung mit der zweiten Profilinhaberkennung identisch ist; und
Senden (S304, S405, S505, S606) eines Remote-Profilverwaltungsbefehls an eine Benutzerausrüstung durch den ersten Profilserver, wenn die erste Profilinhaberkennung mit der zweiten Profilinhaberkennung identisch ist;
dadurch gekennzeichnet, dass:

die erste Profilinhaberkennung und die zweite Profilinhaberkennung jeweils mindestens eines der folgenden umfassen: eine Profilinhaberkennung, die für den ersten Profilserver identifizierbar ist, oder eine Profilinhaberkennung, die für den zweiten Profilserver identifizierbar ist;
und dadurch, dass das Verfahren ferner Folgendes umfasst:

Erhalten (S506) einer Kennungsübereinstimmungsliste durch den ersten Profilserver, wenn sich die erste Profilinhaberkennung von der zweiten Profilinhaberkennung unterscheidet, wobei die Kennungsübereinstimmungsliste eine Übereinstimmung zwischen einer Profilserverkennung und einer Profilinhaberkennung umfasst;

Bestimmen (S507) durch den ersten Profilserver, ob eine Profilinhaberkennung, die mit der ersten Profilinhaberkennung übereinstimmt, in der Kennungsübereinstimmungsliste vorhanden ist; und
Senden (S508) des Remote-Profilverwaltungsbefehls an die Benutzerausrüstung durch den ersten Profilserver, wenn die Profilinhaberkennung, die mit der ersten Profilinhaberkennung übereinstimmt, in der Kennungsübereinstimmungsliste vorhanden ist.

2. Verfahren nach Anspruch 1, wobei das Erhalten einer zweiten Profilinhaberkennung in den Profilinformationen durch den ersten Profilserver Folgendes umfasst:
Erhalten (S302) der zweiten Profilinhaberkennung in den Profilinformationen von einem lokalen Speicher durch den ersten Profilserver.

3. Verfahren nach Anspruch 1, wobei das Erhalten einer zweiten Profilinhaberkennung in den Profilinformationen durch den ersten Profilserver Folgendes umfasst:

Senden (S302b, S403a, S503a, S604a) einer ersten Anforderung an die Benutzerausrüstung durch den ersten Profilserver, wobei die erste Anforderung verwendet wird, um die zweite Profilinhaberkennung zu erhalten; und
Empfangen (S302c, S403b, S503b, S604b) der Profilinformationen, die von der Benutzerausrüstung gesendet werden und die die zweite Profilinhaberkennung enthalten, durch den ersten Profilserver.

4. Verfahren nach Anspruch 1, wobei das Erhalten einer zweiten Profilinhaberkennung in den Profilinformationen durch den ersten Profilserver Folgendes umfasst:

Senden (S403c, S503c, S604c) einer zweite Anforderung an einen zweiten Profilserver durch den ersten Profilserver, wobei die zweite Anforderung verwendet wird, um die zweite Profilinhaberkennung zu erhalten; und
Empfangen (S403d, S503d, S604d) der Profilinformationen, die von dem zweiten Profilserver gesendet werden und die die zweite Profilinhaberkennung enthalten, durch den ersten Profilserver.

5. Verfahren nach Anspruch 1, wobei das Erhalten einer Kennungsübereinstimmungsliste durch den ersten Profilserver Folgendes umfasst:

Erhalten der Kennungsübereinstimmungsliste von dem Remote-Profilverwaltungsserver durch den ersten Profilserver;
Erhalten der Kennungsübereinstimmungsliste von dem zweiten Profilserver durch den ersten Profilserver; oder
Erhalten der Kennungsübereinstimmungsliste von dem lokalen Speicher durch den ersten Profilserver.

6. Verfahren nach einem der Ansprüche 1 bis 5, wobei der erste Profilserver ein Server ist, der zum Verwalten eines Profils konfiguriert ist, und der zweite Profilserver ein Server ist, der zum Herunterladen des Profils konfiguriert ist.

7. Verfahren zur Informationsüberprüfung, wobei das Verfahren Folgendes umfasst:

Empfangen (S304, S405, S505 oder S508, S606) eines von einem ersten Profilserver gesendeten Remote-Profilverwaltungsbefehls durch eine Benutzerausrüstung, wobei der Remote-Profilverwaltungsbefehl eine erste Profilinhaberkennung umfasst;
Erhalten einer zweiten Profilinhaberkennung in Profilinformationen durch die Benutzerausrüstung;
Bestimmen (S306, S407, S510, S608) durch die Benutzerausrüstung, ob die erste Profilinhaberkennung mit der zweiten Profilinhaberkennung identisch ist; und
Ausführen (S307, S408, S511, S609) des Remote-Profilverwaltungsbefehls durch die Benutzerausrüstung, wenn die erste Profilinhaberkennung mit der zweiten Profilinhaberkennung identisch ist;
dadurch gekennzeichnet, dass:

die erste Profilinhaberkennung mindestens eines der Folgenden umfasst: eine Profilinhaberkennung, die für den ersten Profilserver identifizierbar ist, oder eine Profilinhaberkennung, die für einen zweiten Profilserver identifizierbar ist;
und dadurch, dass das Verfahren ferner Folgendes umfasst:

Erhalten einer Kennungsübereinstimmungsliste durch die Benutzerausrüstung, wenn sich die erste Profilinhaberkennung von der zweiten Profilinhaberkennung unterscheidet, wobei die Kennungsübereinstimmungsliste eine Übereinstimmung zwischen einer Profilserverkennung und einer Profilinhaberkennung umfasst;
Bestimmen durch die Benutzerausrüstung, ob eine Profilinhaberkennung, die mit der ersten Profilinhaberkennung übereinstimmt, in der Kennungsübereinstimmungsliste vorhanden ist; und
Ausführen des Remote-Profilverwaltungsbefehls durch die Benutzerausrüstung, wenn die Profilinhaberkennung, die mit der ersten Profilinhaberkennung übereinstimmt, in der Kennungsübereinstimmungsliste vorhanden ist.

8. Verfahren nach Anspruch 7, das vor dem Empfangen eines von einem ersten Profilserver gesendeten Remote-Profilverwaltungsbefehls durch die Benutzerausrüstung, ferner Folgendes umfasst:

Empfangen (S401, S501, S601) einer von einem Remote-Profilverwaltungsserver oder einem zweiten Profilserver gesendeten Aktualisierungsnachricht durch die Benutzerausrüstung,
wobei die Aktualisierungsnachricht eine Kennung des ersten Profilservers und eine entsprechende Profilinhaberkennung umfasst.

9. Verfahren nach den Ansprüchen 7 oder 8, das vor dem Empfangen eines von einem ersten Profilserver gesendeten Remote-Profilverwaltungsbefehls durch eine Benutzerausrüstung, ferner Folgendes umfasst:

Empfangen einer ersten von dem ersten Profilserver gesendeten Anforderung durch die Benutzerausrüstung, wobei die erste Anforderung verwendet wird, um die zweite Profilinhaberkennung zu erhalten; und
Senden der Profilinformationen, die die zweite Profilinhaberkennung enthalten, an den ersten Profilserver durch die Benutzerausrüstung.

10. Erster Profilserver, der einen Speicher, einen Kommunikationsbus und einen Prozessor umfasst, wobei der Speicher dazu konfiguriert ist, Programmcode zu speichern, der, wenn er von dem Prozessor ausgeführt wird, den ersten Profilserver veranlasst, das Verfahren gemäß einem der Ansprüche 1-6 umzusetzen.

11. Benutzerausrüstung, die einen Speicher, einen Kommunikationsbus und einen Prozessor umfasst, wobei der Speicher dazu konfiguriert ist, Programmcode zu speichern, der, wenn er von dem Prozessor ausgeführt wird, die Benutzerausrüstung veranlasst, das Verfahren gemäß einem der Ansprüche 7-9 umzusetzen.

Revendications

1. Procédé de vérification d'informations, dans lequel le procédé comprend :

   la réception (S301, S402, S502, S603), par un premier serveur de profil, d'une requête de gestion de profil à distance envoyée par un serveur de gestion de profil à distance, dans lequel la requête de gestion de profil à distance comprend un premier identifiant de propriétaire de profil ;
   l'obtention (S302, S403, S503, S604), par le premier serveur de profil, d'un second identifiant de propriétaire de profil dans les informations de profil ;
   le fait de déterminer (S303, S404, S504, S605), par le premier serveur de profil, si le premier identifiant de propriétaire de profil est le même que le second identifiant de propriétaire de profil ; et
   l'envoi (S304, S405, S505, S606), par le premier serveur de profil, d'une commande de gestion de profil à distance à un équipement utilisateur lorsque le premier identifiant de propriétaire de profil est le même que le second identifiant de propriétaire de profil ;
   caractérisé en ce que
   le premier identifiant de propriétaire de profil et le second identifiant de propriétaire de profil comprennent chacun au moins l'un : d'un identifiant de propriétaire de profil qui peut être identifié par le premier serveur de profil ou d'un identifiant de propriétaire de profil qui peut être identifié par le second serveur de profil ;
   et en ce que le procédé comprend en outre :

      l'obtention (S506), par le premier serveur de profil, d'une liste de correspondance d'identifiant lorsque le premier identifiant de propriétaire de profil est différent du second identifiant de propriétaire de profil, dans lequel la liste de correspondance d'identifiant comprend une correspondance entre un identifiant de serveur de profil et un identifiant de propriétaire de profil ;
      le fait de déterminer (S507), par le biais du premier serveur de profil, si un identifiant de propriétaire de profil correspondant au premier identifiant de propriétaire de profil est présent dans la liste de correspondance d'identifiants ; et
      l'envoi (S508), par le premier serveur de profil, de la commande de gestion de profil à distance à l'équipement utilisateur lorsque l'identifiant de propriétaire de profil correspondant au premier identifiant de propriétaire de profil est présent dans la liste de correspondance d'identifiants.

2. Procédé selon la revendication 1, dans lequel l'obtention, par le premier serveur de profil, d'un second identifiant de propriétaire de profil dans les informations de profil comprend :
   l'obtention (S302), par le premier serveur de profil, du second identifiant de propriétaire de profil dans les informations de profil à partir d'une mémoire locale.

3. Procédé selon la revendication 1, dans lequel l'obtention, par le premier serveur de profil, d'un second identifiant de propriétaire de profil dans les informations de profil comprend :

   l'envoi (S302b, S403a, S503a, S604a), par le premier serveur de profil, d'une première requête à l'équipement utilisateur, dans lequel la première requête est utilisée pour obtenir le second identifiant de propriétaire de profil ; et
   la réception (S302c, S403b, S503b, S604b), par le premier serveur de profil, des informations de profil qui sont envoyées par l'équipement utilisateur et qui contiennent le second identifiant de propriétaire de profil.

4. Procédé selon la revendication 1, dans lequel l'obtention, par le premier serveur de profil, d'un second identifiant de propriétaire de profil dans les informations de profil comprend :

   l'envoi (S403c, S503c, S604c), par le premier serveur de profil, d'une seconde requête à un second serveur de profil, dans lequel la seconde requête est utilisée pour obtenir le second identifiant de propriétaire de profil ; et
   la réception (S403d, S503d, S604d), par le premier serveur de profil, des informations de profil qui sont envoyées par le second serveur de profil et qui contiennent le second identifiant de propriétaire de profil.

5. Procédé selon la revendication 1, dans lequel l'obtention, par le premier serveur de profil, d'une liste de correspondance d'identifiants comprend :

   l'obtention, par le premier serveur de profil, de la liste de correspondance d'identifiants à partir du serveur de gestion de profil à distance ;
   l'obtention, par le premier serveur de profil, de la liste de correspondance d'identifiants à partir du second serveur de profil ; ou
   l'obtention, par le premier serveur de profils, de la liste de correspondance d'identifiants à partir de la mémoire locale.

6. Procédé selon l'une quelconque des revendications

1 à 5, dans lequel le premier serveur de profil est un serveur configuré pour gérer un profil, et le second serveur de profil est un serveur configuré pour télécharger le profil.

7. Procédé de vérification d'informations, dans lequel le procédé comprend :

la réception (S304, S405, S505 ou S508, S606), par un équipement utilisateur, d'une commande de gestion de profil à distance envoyée par un premier serveur de profil, dans lequel la commande de gestion de profil à distance comprend un premier identifiant de propriétaire de profil ;
l'obtention, par l'équipement utilisateur, d'un second identifiant de propriétaire de profil dans les informations de profil ;
le fait de déterminer (S306, S407, S510, S608), par le biais de l'équipement utilisateur, si le premier identifiant de propriétaire de profil est le même que le second identifiant de propriétaire de profil ; et
l'exécution (S307, S408, S511, S609) par l'équipement utilisateur, de la commande de gestion de profil à distance lorsque le premier identifiant de propriétaire de profil est le même que le second identifiant de propriétaire de profil ;
caractérisé en ce que
le premier identifiant de propriétaire de profil comprend au moins l'un : d'un identifiant de propriétaire de profil qui peut être identifié par le premier serveur de profil ou d'un identifiant de propriétaire de profil qui peut être identifié par un second serveur de profil ;
et en ce que le procédé comprend en outre :

l'obtention, par l'équipement utilisateur, d'une liste de correspondance d'identifiants lorsque le premier identifiant de propriétaire de profil est différent du second identifiant de propriétaire de profil, dans lequel la liste de correspondance d'identifiants comprend une correspondance entre un identifiant de serveur de profil et un identifiant de propriétaire de profil,
le fait de déterminer, par le biais de l'équipement utilisateur, si un identifiant de propriétaire de profil correspondant au premier identifiant de propriétaire de profil est présent dans la liste de correspondance d'identifiants ; et
l'exécution, par l'équipement utilisateur, de la commande de gestion de profil à distance lorsque l'identifiant de propriétaire de profil correspondant au premier identifiant de propriétaire de profil est présent dans la liste de correspondance d'identifiants.

8. Procédé selon la revendication 7, avant la réception, par l'équipement utilisateur, d'une commande de gestion de profil à distance envoyée par un premier serveur de profil, comprenant en outre :
la réception (S401, S501, S601), par l'équipement utilisateur, d'un message de mise à jour envoyé par un serveur de gestion de profil à distance ou le second serveur de profil, dans lequel le message de mise à jour comprend un identifiant du premier serveur de profil et un identifiant de propriétaire de profil correspondant.

9. Procédé selon les revendications 7 ou 8, avant la réception, par un équipement utilisateur, d'une commande de gestion de profil à distance envoyée par un premier serveur de profil, comprenant en outre :

la réception, par l'équipement utilisateur, d'une première requête envoyée par le premier serveur de profil, dans lequel la première requête est utilisée pour obtenir le second identifiant de propriétaire de profil ; et
l'envoi, par l'équipement utilisateur au premier serveur de profil, des informations de profil qui contiennent le second identifiant de propriétaire de profil.

10. Premier serveur de profil, comprenant une mémoire, un bus de communications et un processeur, dans lequel la mémoire est configurée pour stocker un code de programme qui, lorsqu'il est exécuté par le processeur, amène le premier serveur de profil à mettre en œuvre le procédé selon l'une quelconque des revendications 1 à 6.

11. Équipement utilisateur, comprenant une mémoire, un bus de communications et un processeur, dans lequel la mémoire est configurée pour stocker un code de programme qui, lorsqu'il est exécuté par le processeur, amène l'équipement utilisateur à mettre en œuvre le procédé selon l'une quelconque des revendications 7 à 9.

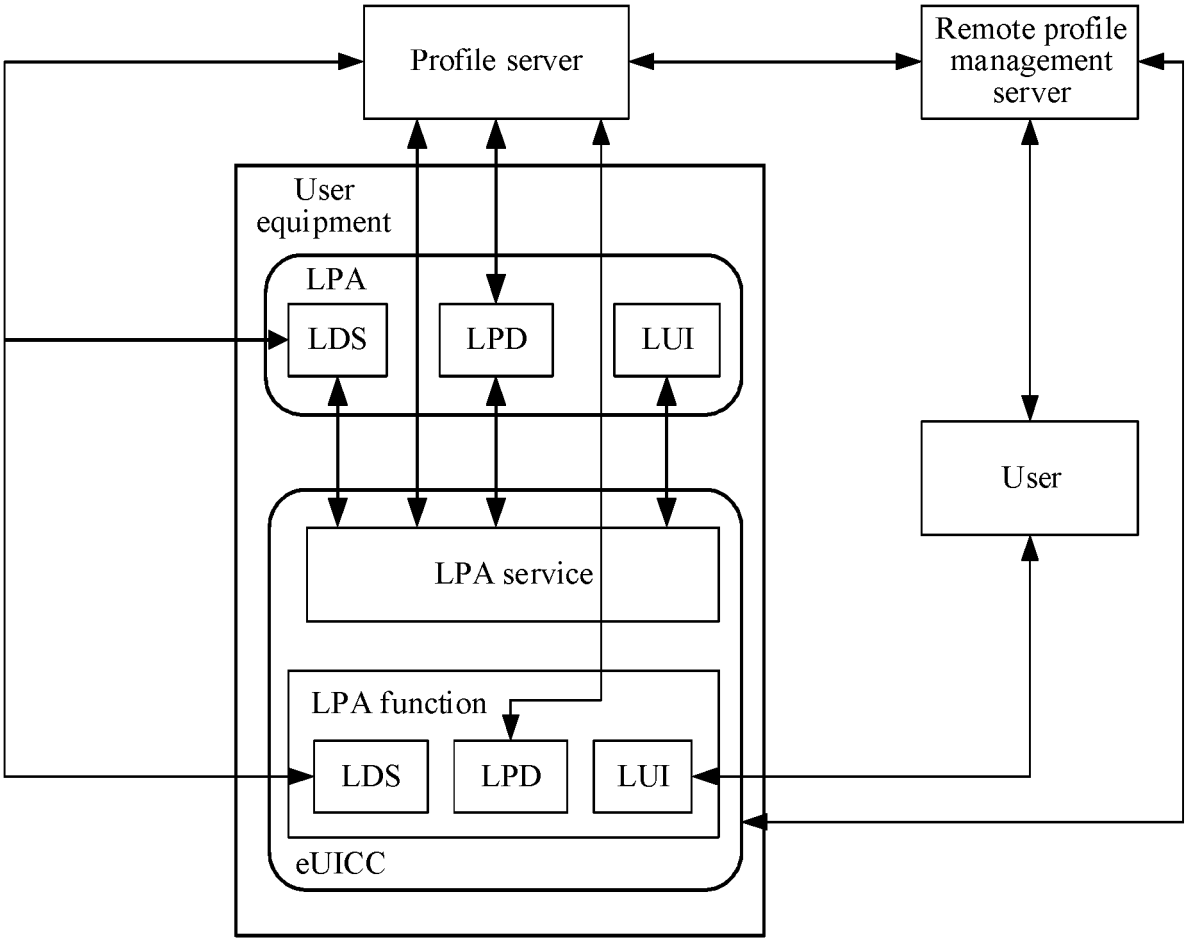
Profile server
Remote profile management server
User equipment
LPA
LDS
LPD
LUI
User
LPA service
LPA function
LDS
LPD
LUI
eUICC

FIG. 1

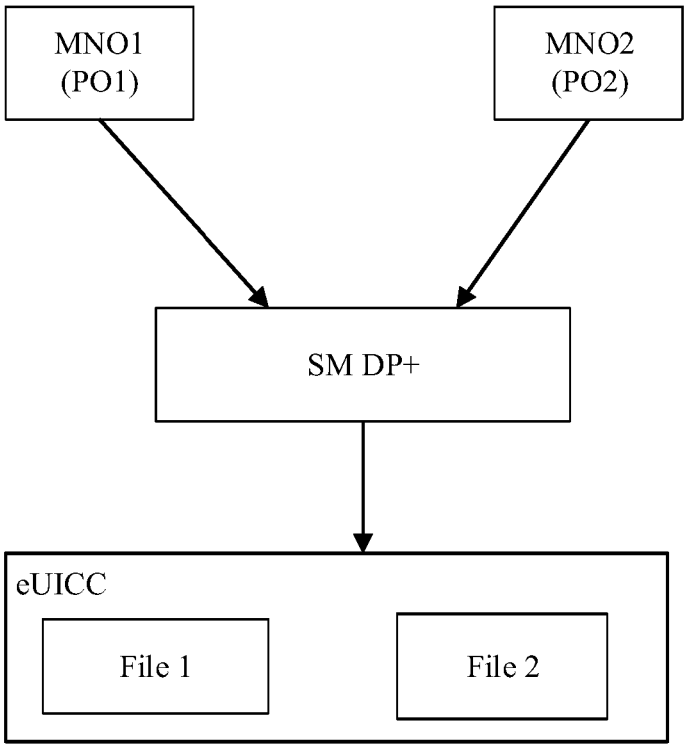
MNO1
(PO1)
MNO2
(PO2)
SM DP+
eUICC
File 1
File 2

FIG. 2(A)

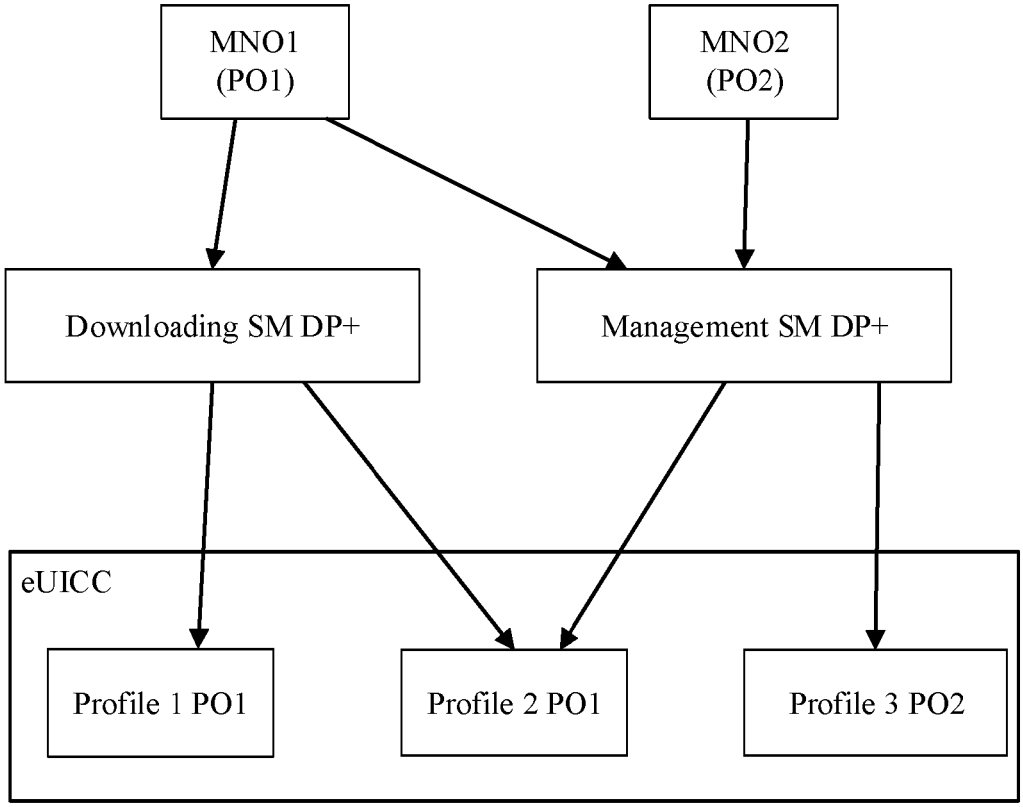
MNO1
(PO1)
MNO2
(PO2)
Downloading SM DP+
Management SM DP+
eUICC
Profile 1 PO1
Profile 2 PO1
Profile 3 PO2

FIG. 2(B)

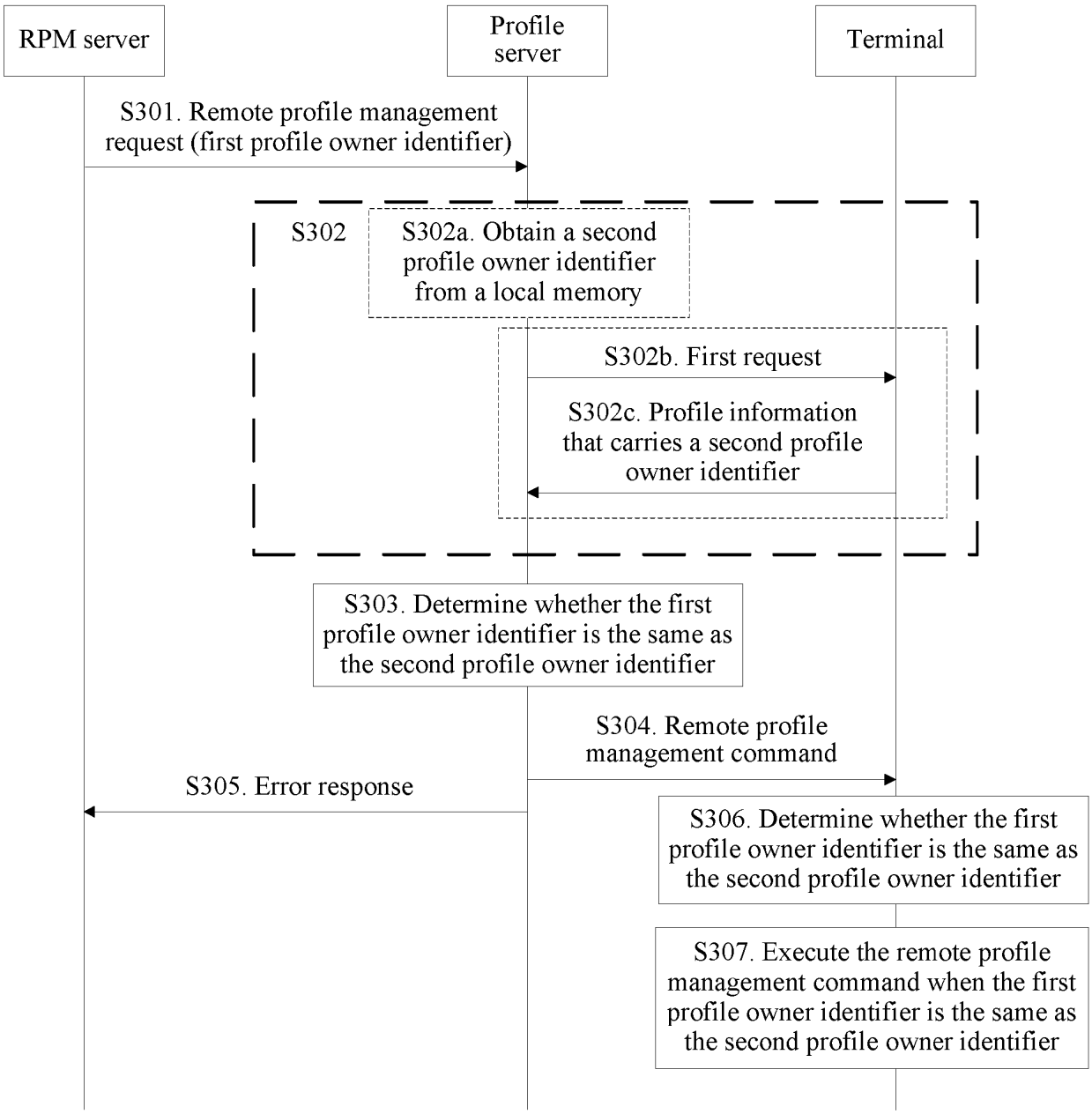
RPM server
Profile server
Terminal
S301. Remote profile management request (first profile owner identifier)
S302
S302a. Obtain a second profile owner identifier from a local memory
S302b. First request
S302c. Profile information that carries a second profile owner identifier
S303. Determine whether the first profile owner identifier is the same as the second profile owner identifier
S304. Remote profile management command
S305. Error response
S306. Determine whether the first profile owner identifier is the same as the second profile owner identifier
S307. Execute the remote profile management command when the first profile owner identifier is the same as the second profile owner identifier

FIG. 3

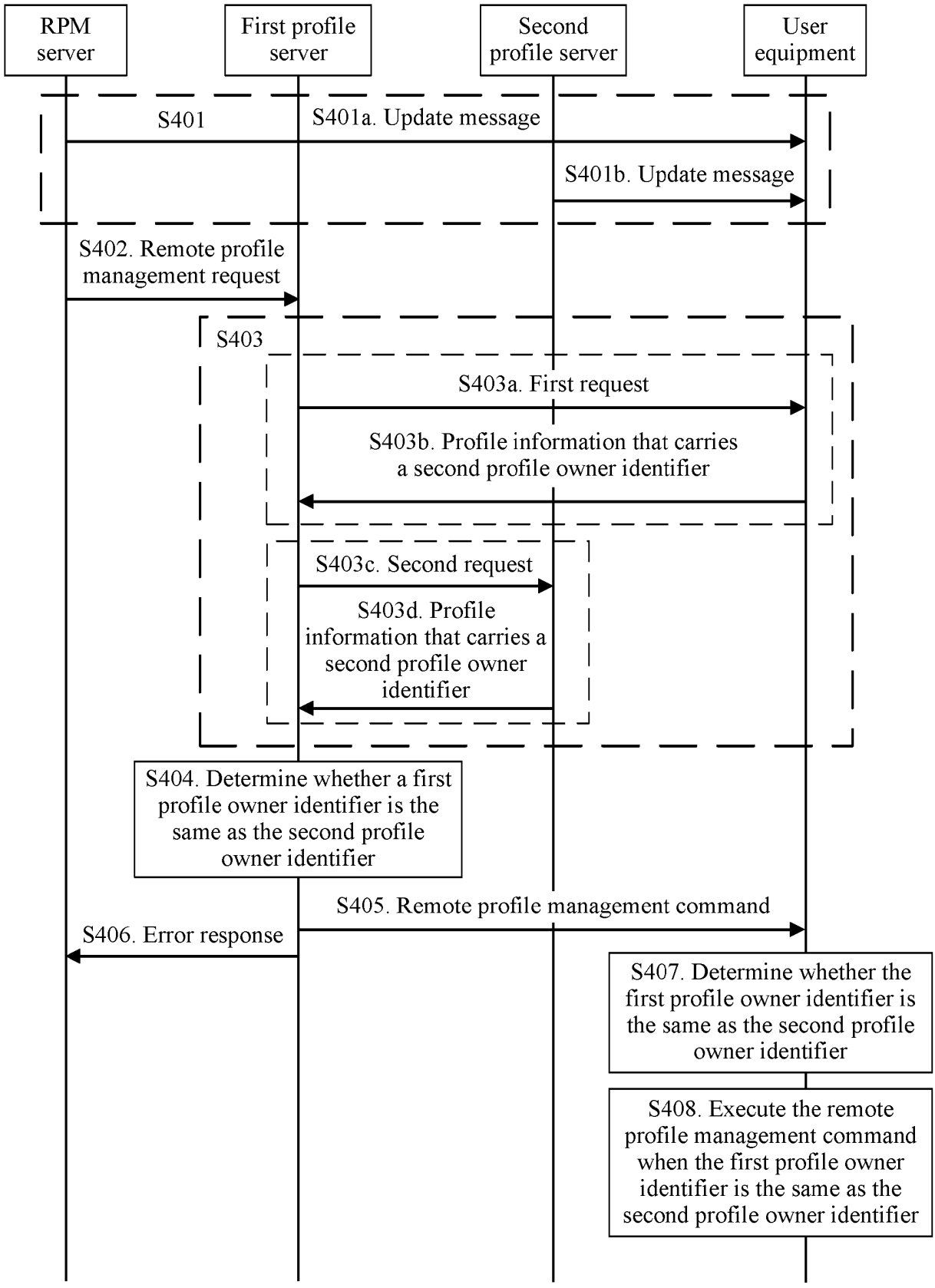
RPM server
First profile server
Second profile server
User equipment
S401
S401a. Update message
S401b. Update message
S402. Remote profile management request
S403
S403a. First request
S403b. Profile information that carries a second profile owner identifier
S403c. Second request
S403d. Profile information that carries a second profile owner identifier
S404. Determine whether a first profile owner identifier is the same as the second profile owner identifier
S405. Remote profile management command
S406. Error response
S407. Determine whether the first profile owner identifier is the same as the second profile owner identifier
S408. Execute the remote profile management command when the first profile owner identifier is the same as the second profile owner identifier

FIG. 4

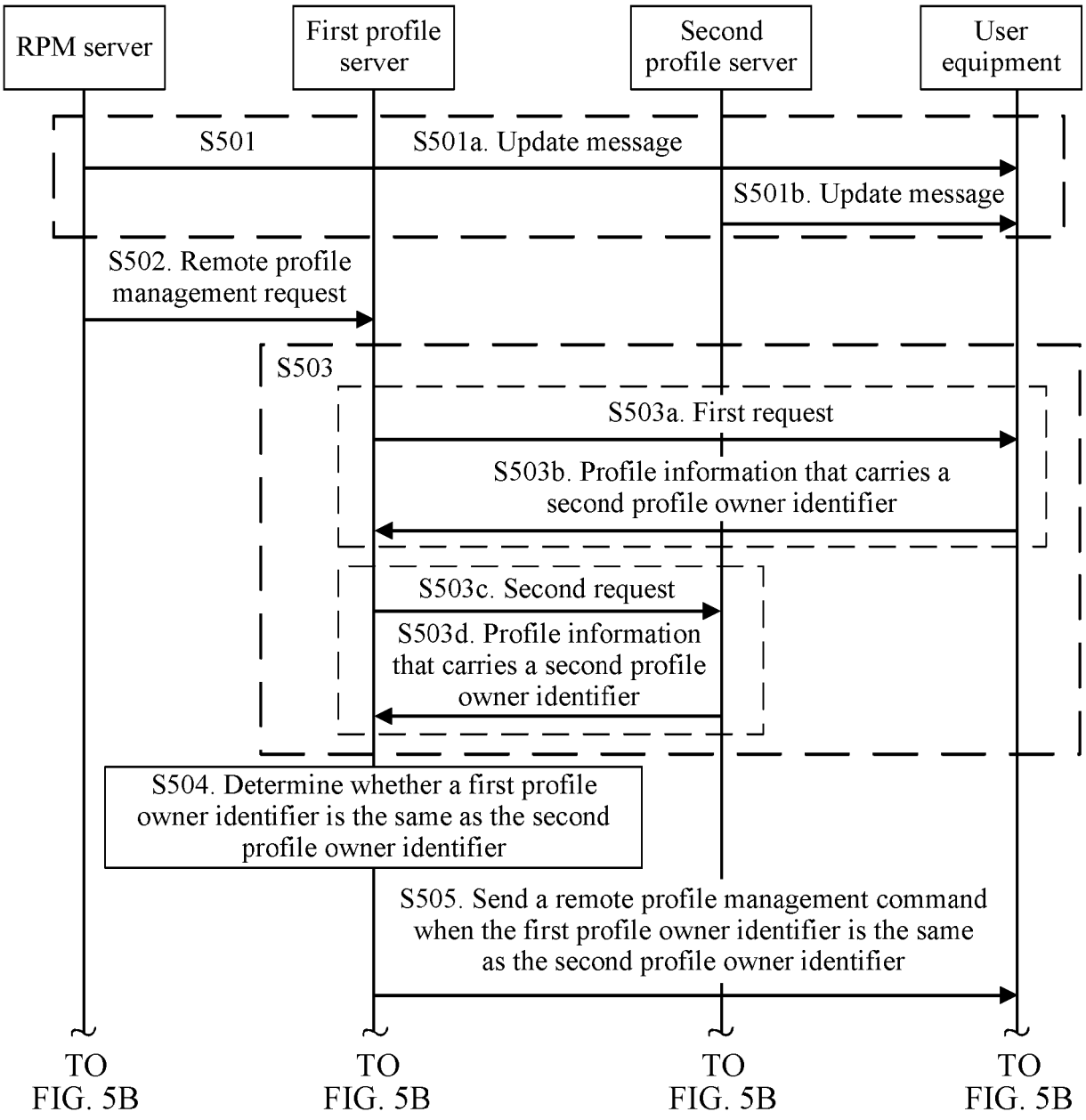
RPM server
First profile server
Second profile server
User equipment
S501
S501a. Update message
S501b. Update message
S502. Remote profile management request
S503
S503a. First request
S503b. Profile information that carries a second profile owner identifier
S503c. Second request
S503d. Profile information that carries a second profile owner identifier
S504. Determine whether a first profile owner identifier is the same as the second profile owner identifier
S505. Send a remote profile management command when the first profile owner identifier is the same as the second profile owner identifier
TO FIG. 5B
TO FIG. 5B
TO FIG. 5B
TO FIG. 5B

FIG. 5A

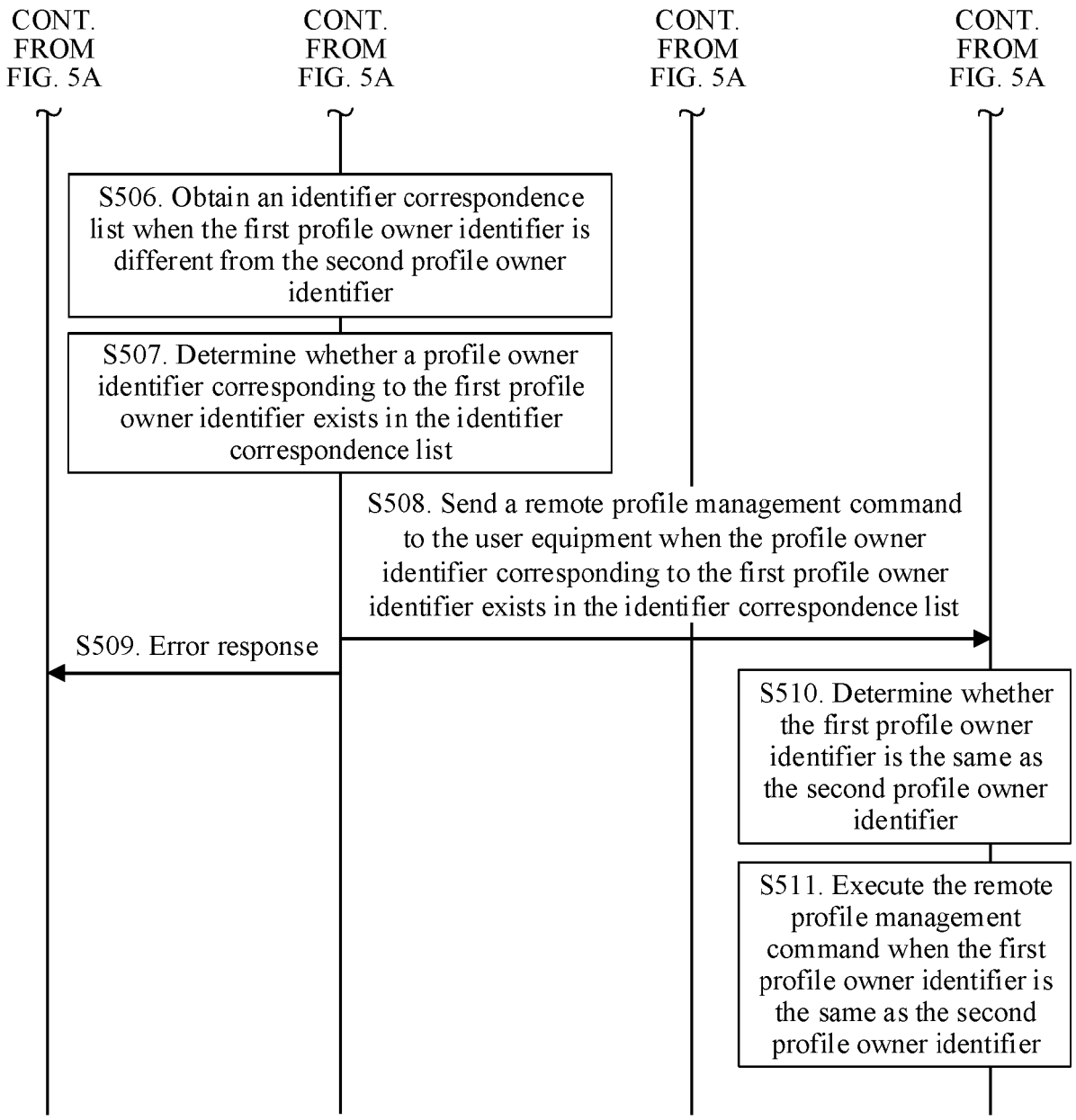
CONT. FROM FIG. 5A
CONT. FROM FIG. 5A
CONT. FROM FIG. 5A
CONT. FROM FIG. 5A
S506. Obtain an identifier correspondence list when the first profile owner identifier is different from the second profile owner identifier
S507. Determine whether a profile owner identifier corresponding to the first profile owner identifier exists in the identifier correspondence list
S508. Send a remote profile management command to the user equipment when the profile owner identifier corresponding to the first profile owner identifier exists in the identifier correspondence list
S509. Error response
S510. Determine whether the first profile owner identifier is the same as the second profile owner identifier
S511. Execute the remote profile management command when the first profile owner identifier is the same as the second profile owner identifier

FIG. 5B

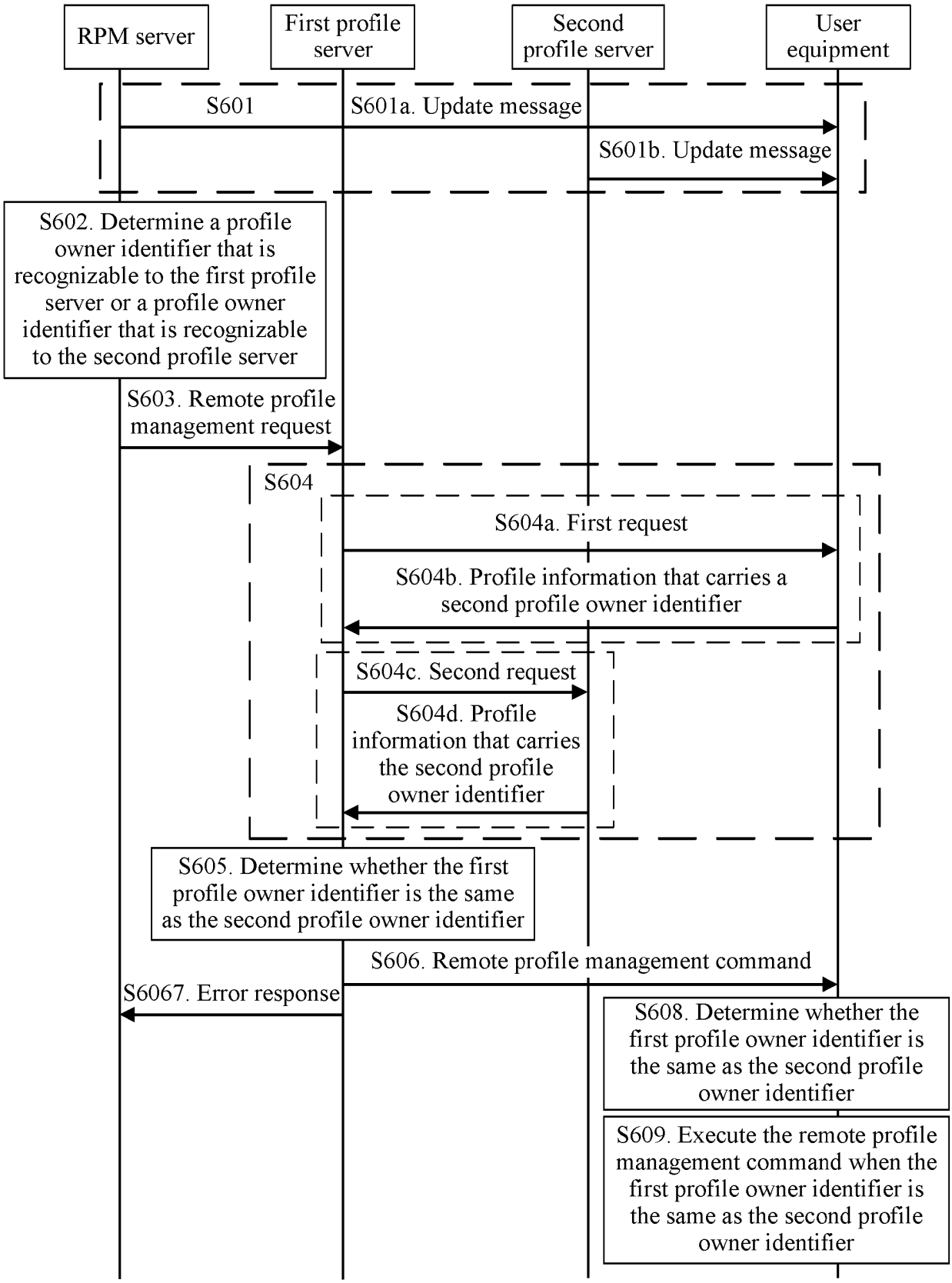
RPM server
First profile server
Second profile server
User equipment
S601
S601a. Update message
S601b. Update message
S602. Determine a profile owner identifier that is recognizable to the first profile server or a profile owner identifier that is recognizable to the second profile server
S603. Remote profile management request
S604
S604a. First request
S604b. Profile information that carries a second profile owner identifier
S604c. Second request
S604d. Profile information that carries the second profile owner identifier
S605. Determine whether the first profile owner identifier is the same as the second profile owner identifier
S606. Remote profile management command
S6067. Error response
S608. Determine whether the first profile owner identifier is the same as the second profile owner identifier
S609. Execute the remote profile management command when the first profile owner identifier is the same as the second profile owner identifier

FIG. 6

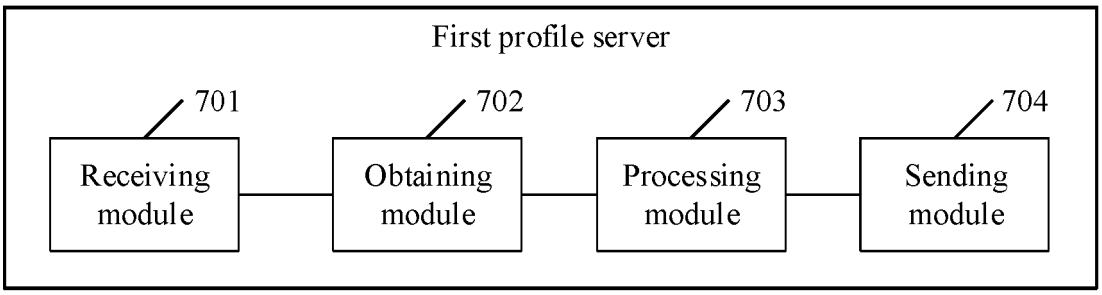

FIG. 7

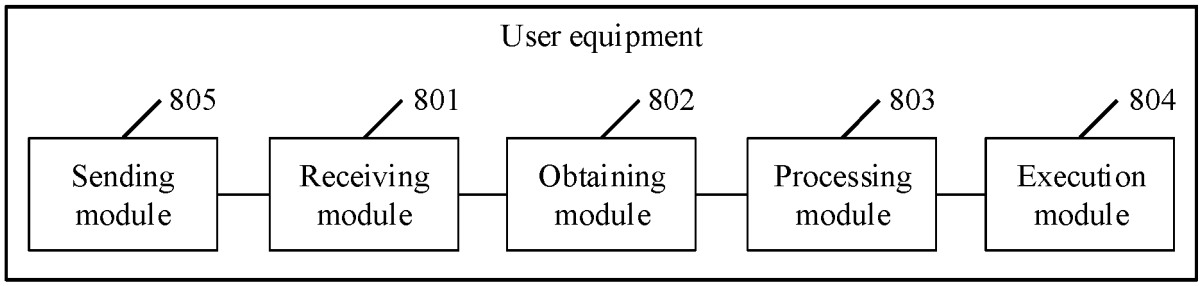

FIG. 8

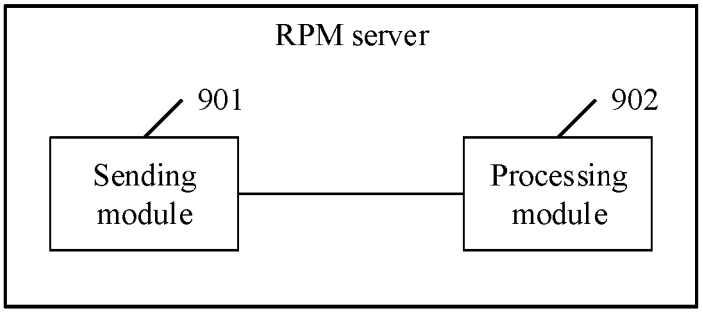

FIG. 9

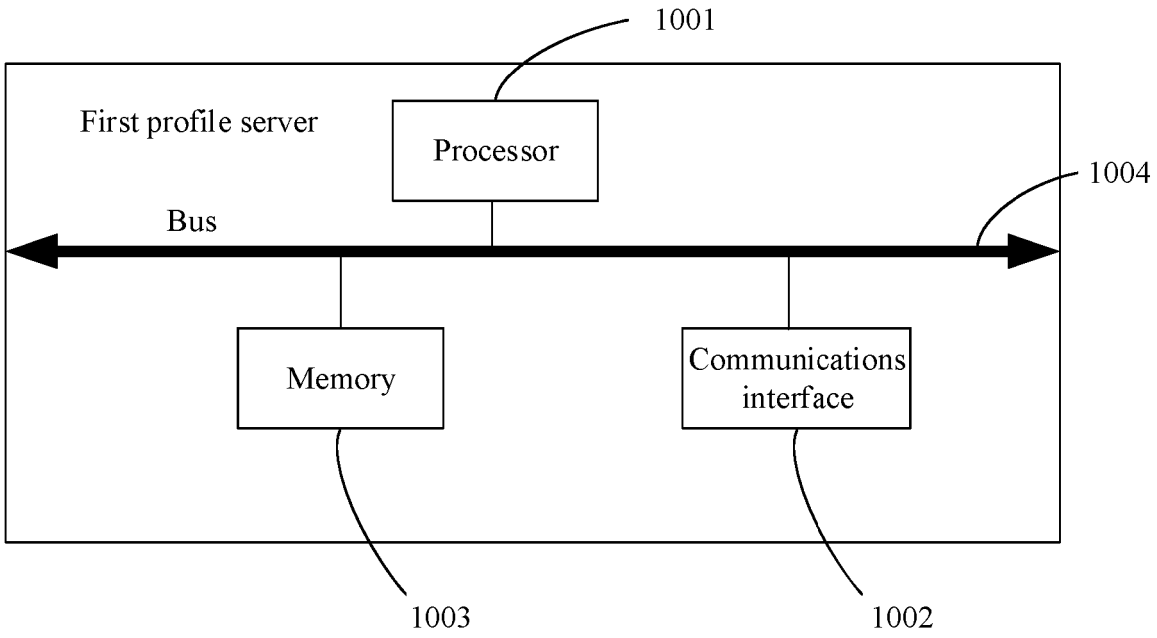
1001
First profile server
Processor
1004
Bus
Memory
Communications interface
1003
1002

FIG. 10

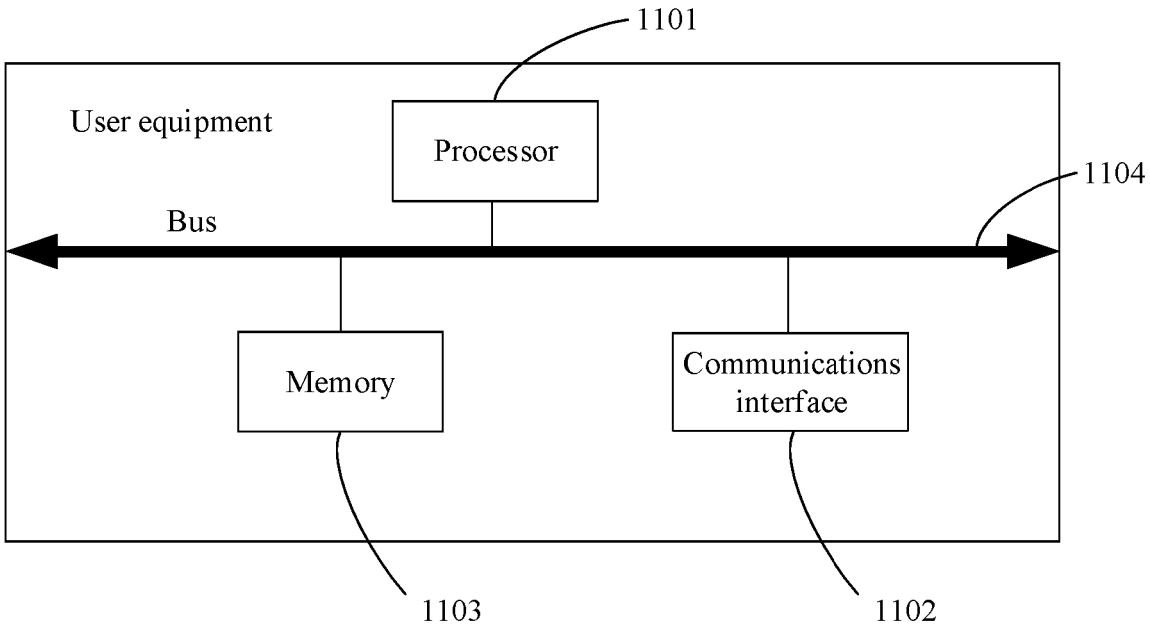
1101
User equipment
Processor
1104
Bus
Memory
Communications interface
1103
1102

FIG. 11

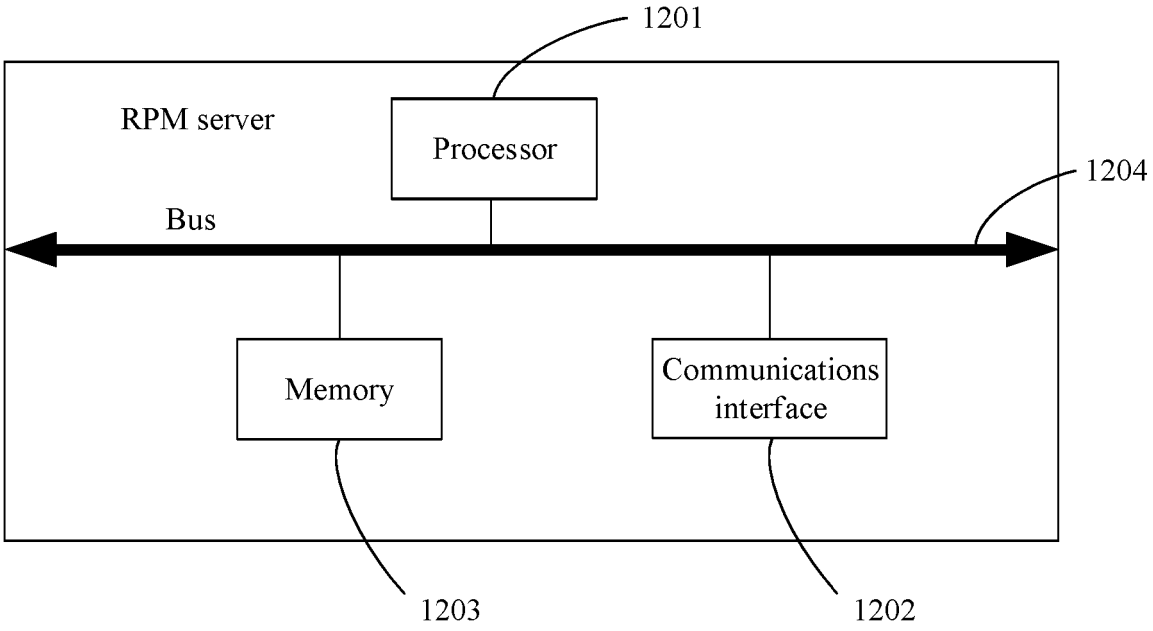
1201
RPM server
Processor
1204
Bus
Memory
Communications interface
1203
1202

FIG. 12

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- EP 3073770 A1 **[0002]**