I886265

(19)中華民國智慧財產局

(12)發明說明書公告本 **(11)證書號數：TW I886265 B**

(45)公告日： 中華民國 114 (2025) 年 06 月 11 日

(21)申請案號：110115569 (22)申請日： 中華民國 110 (2021) 年 04 月 29 日

(51)Int. Cl.： ***H04W12/04 (2021.01)*** ***H04W12/06 (2021.01)***
H04W12/08 (2021.01)

(30)優先權：2020/10/16 中國大陸 202011111639.9

(71)申請人：大陸商中興通訊股份有限公司 (中國大陸) ZTE CORPORATION (CN)
中國大陸

(72)發明人：游世林 YOU, SHI-LIN (CN) ；蔡繼燕 CAI, JI-YAN (CN) ；林兆驥 LIN, ZHAO-JI (CN) ；彭錦 PENG, JIN (CN) ；劉宇澤 LIU, YU-ZE (CN) ；邢真 XING, ZHEN (CN) ；王繼剛 WANG, JI-GANG (CN) ；劉敏 LIU, MIN (CN)

(74)代理人：李有財

(56)參考文獻：

CN 102754486B EP 3673674A1

WO 2020/031157A1 WO 2020/173863A1

網路文獻 Samsung, " Support AKMA context Deregistration option in AKMA", 3GPP, S3-201968, 2020-08-07。

網路文獻 3GPP;Technical Specification Group Service and System Aspects; "Authentication and Key Management for Application (AKMA) Based on 3Gpp credenticls in 5G system (5Gs)(Release 16)" 3rd Generation Partnership Project; 2020-09-25

審查人員：程敦睿

申請專利範圍項數：17 項 圖式數：15 共 32 頁

(54)名稱

用戶資料更新方法、節點和儲存媒體

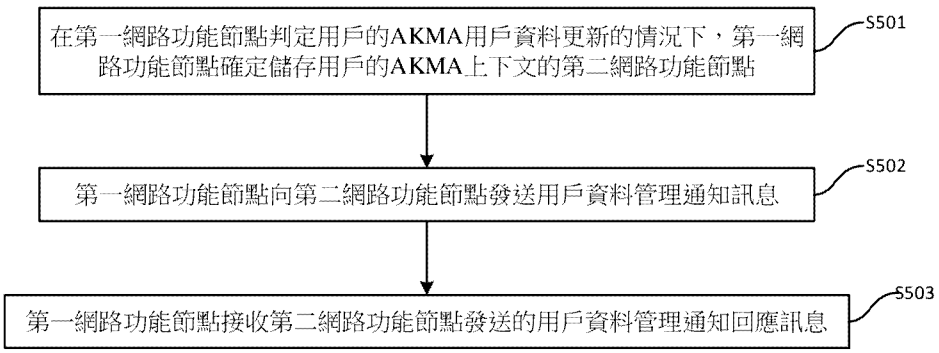
(57)摘要

本文公開一種用戶資料更新方法、裝置、節點和儲存媒體。該用戶資料更新方法包括在第一網路功能節點確定用戶的 AKMA 架構的用戶資料更新的情況下，第一網路功能節點確定儲存用戶的 AKMA 上下文的第二網路功能節點；第一網路功能節點向第二網路功能節點發送用戶資料管理通知訊息；第一網路功能節點接收第二網路功能節點發送的用戶資料管理通知回應訊息；其中，用戶資料管理通知回應訊息是第二網路功能節點根據用戶資料管理通知訊息刪除用戶的 AKMA 上下文後發送的。

The present invention provides a method for updating subscriber data, and apparatus, node and storage medium. The method comprising: when a first network function node determines that a subscriber data under an AKMA structure is updated, the first network function node determining a second network function node which stores the subscriber's AKMA context; the first network function node transmitting a subscriber data management notification message to the second network function node; the first network function node receiving an acknowledgement message from the second network node function; wherein, the

acknowledgement message is transmitted by the second network function node after deleting the subscriber's AKMA context according to the subscriber data management notification message.

指定代表圖：



【圖 5】

符號簡單說明：

S501, S502, S503:步驟

I886265

【發明摘要】

【中文發明名稱】用戶資料更新方法、節點和儲存媒體

【英文發明名稱】METHOD FOR UPDATING SUBSCRIBER DATA, AND NODE, AND STORAGE MEDIUM

【中文】

本文公開一種用戶資料更新方法、裝置、節點和儲存媒體。該用戶資料更新方法包括在第一網路功能節點確定用戶的 AKMA 架構的用戶資料更新的情況下，第一網路功能節點確定儲存用戶的 AKMA 上下文的第二網路功能節點；第一網路功能節點向第二網路功能節點發送用戶資料管理通知訊息；第一網路功能節點接收第二網路功能節點發送的用戶資料管理通知回應訊息；其中，用戶資料管理通知回應訊息是第二網路功能節點根據用戶資料管理通知訊息刪除用戶的 AKMA 上下文後發送的。

【英文】

The present invention provides a method for updating subscriber data, and apparatus, node and storage medium. The method comprising: when a first network function node determines that a subscriber data under an AKMA structure is updated, the first network function node determining a second network function node which stores the subscriber's AKMA context; the first network function node transmitting a subscriber data management notification message to the second network function node; the first network function node receiving an acknowledgement message from the second network node function; wherein, the acknowledgement message is transmitted by the

second network function node after deleting the subscriber's AKMA context according to the subscriber data management notification message.

【指定代表圖】

圖5

【代表圖之符號簡單說明】

S501, S502, S503: 步驟

【發明說明書】

【中文發明名稱】用戶資料更新方法、節點和儲存媒體

【英文發明名稱】 METHOD FOR UPDATING SUBSCRIBER DATA, AND NODE, AND STORAGE MEDIUM

【技術領域】

【0001】本說明書涉及無線通訊技術領域，例如涉及一種用戶資料更新方法、裝置、節點和儲存媒體。

【先前技術】

【0002】根據第三代合作夥伴計畫（3rd Generation Partnership Project，3GPP）標準工作組的定義，第五代移動通訊技術（5th generation wireless systems，5G）系統包括 5G 無線接入網（5G Radio Access Network，5G RAN）子系統、5G 核心網（5G Core network，5GC）子系統。如圖 1 所示，5G 系統的架構包括多個網路功能（Network Function，NF），其中，5G 無線接入網子系統包括新一代無線（New Radio，NR）基站，即（無線）接入點（(Radio) Access Node，(R)AN）。5G 核心網子系統包括統一資料管理（Unified Data Management，UDM）功能、接入管理功能（Access Management Function，AMF）、會話管理功能（Session Management Function，SMF）、用戶面功能（User Plane Function，UPF）、策略控制功能（Policy Control Function，PCF）、安全錨點功能（Security Anchor Function，SEAF）、認證伺服器功能（Authentication Server Function，AUSF）和身份驗證憑據儲存庫和處理功能（Authentication Credential Repository and Processing Function，ARPF）。5G 網路中包括有用戶隱藏識別碼（Subscription Concealed Identifier，SUCI）和用戶永久識別碼（Subscription Permanent Identifier，SUPI），

其中，SUPI 可以包括國際移動用戶識別碼（International Mobile Subscriber Identification Number，IMSI）或網路接入識別碼（Network Access Identifier，NAI）。

【0003】圖 2 是基於服務化架構的應用的身份認證和金鑰管理架構（Architecture for Authentication and Key Management for Applications，AKMA）的示意圖，其相對於 5G 網路系統引入了新的網路功能—AKMA 錨定功能（AKMA Anchor Function，AAnF），AAnF 位於歸屬網路，主要用於產生用戶設備（User Equipment，UE）與應用功能（Application Function，AF）之間的會話秘鑰，以及維護 AAnF 與 UE 之間的安全上下文。AAnF 與通用引導認證機制（General Bootstrapping Architecture，GBA）中的自舉服務功能（Bootstrapping Server Function，BSF）功能類似，同時 UE 與 AF 之間的介面 Ua*也與 GBA 中的 Ua 介面近似，另外，圖 2 中的 Nnef、Nausf、Naanf 和 Namf 分別為網路開放功能（Network Exposure Function，NEF）、AUSF、AAnF 和 AMF 的基於服務化介面。

【0004】圖 3 是應用的身份認證和金鑰管理系統的金鑰推衍架構的示意圖，UE 接入 5G 網路，透過 w 和金鑰協商（Authentication and Key Agreement，AKA），即 5G-AKA，或者可擴充認證協議（Extensible Authentication Protocol）-AKA’，即 EAP-AKA’，認證成功後，AUSF 和 UE 產生金鑰 K_{AUSF}，同時由金鑰 K_{AUSF} 推衍出 AKMA 錨定金鑰 K_{AKMA}，移動設備（Mobile Equipment，ME）和 AAnF 由金鑰 K_{AKMA} 推衍出應用金鑰 K_{AF}，其中 AUSF 和 AAnF 均在歸屬網路中。

【0005】在相關技術中，通常以重用 5G 主認證流程（即上述 5G-AKA 或 EAP-AKA’）的方式產生金鑰 K_{AKMA}，當認證成功後，UE 和 AUSF 由金鑰 K_{AUSF} 推衍產生 AKMA 錨定金鑰 K_{AKMA}，在產生金鑰 K_{AKMA} 的同時也產生金鑰 K_{AKMA} 的相關金鑰識別碼 A-KID，那麼金鑰 K_{AKMA} 也只能透過 5G 主認證流程進行更新。而 AKMA 技術為 5G 網路用戶提供了用戶到應用的端到端的安全保護，若用戶資

料發生更新，則將會影響 AKMA 服務的使用，若 AAnF 繼續保留 AKMA 相關的安全上下文，那麼存在 AKMA 相關的安全上下文被攻擊者濫用的可能性。

【發明內容】

【0006】本說明書提供一種用戶資料更新方法、裝置、節點和儲存媒體，旨在用戶資料發生更新的情況下，使第二網路功能節點不保留 AKMA 相關的上下文，從而避免 AKMA 相關的上下文被攻擊者濫用的情況。

【0007】本說明書實施例提供了一種用戶資料更新方法，包括：

【0008】在第一網路功能節點確定用戶的 AKMA 用戶資料更新的情況下，第一網路功能節點確定儲存用戶的 AKMA 上下文的第二網路功能節點；第一網路功能節點向第二網路功能節點發送用戶資料管理通知訊息；第一網路功能節點接收第二網路功能節點發送的用戶資料管理通知回應訊息；其中，用戶資料管理通知回應訊息是所述第二網路功能節點根據用戶資料管理通知訊息刪除用戶的 AKMA 上下文後發送的。

【0009】本說明書實施例還提供了一種用戶資料更新方法，包括：

【0010】第三網路功能節點接收第一網路功能節點發送的查詢訊息；第三網路功能節點根據查詢訊息確定第二網路功能節點；第三網路功能節點向第一網路功能節點發送查詢回應訊息，查詢回應訊息中攜帶有第二網路功能節點的識別碼或地址。

【0011】本說明書實施例還提供了一種用戶資料更新方法，該方法包括：

【0012】第四網路功能節點確定第二網路功能節點；第四網路功能節點向第一網路功能節點發送訊息；訊息中攜帶有第二網路功能節點的識別碼或地址。

【0013】本說明書實施例還提供了一種用戶資料更新裝置，該裝置包括：

【0014】確定模組，用於在確定用戶的 AKMA 用戶資料更新的情況下，確定儲存用戶的 AKMA 上下文的第二網路功能節點；發送模組，用於向第二網路功能節點發送用戶資料管理通知訊息；接收模組，用於接收第二網路功能節點發送的用戶資料管理通知回應訊息；其中，用戶資料管理通知回應訊息是第二網路功能節點根據用戶資料管理通知訊息刪除用戶的 AKMA 上下文後發送的。

【0015】本說明書實施例還提供了一種用戶資料更新裝置，該裝置包括：

【0016】接收模組，用於接收第一網路功能節點發送的查詢訊息；確定模組，用於根據查詢訊息確定第二網路功能節點；發送模組，用於向第一網路功能節點發送查詢回應訊息，查詢回應訊息中攜帶有第二網路功能節點的識別碼或地址。

【0017】本說明書實施例還提供了一種用戶資料更新裝置，該裝置包括：

【0018】確定模組，用於確定第二網路功能節點；發送模組，用於向第一網路功能節點發送訊息；訊息中攜帶有所述第二網路功能節點的識別碼或地址。

【0019】本說明書實施例還提供了一種網路功能節點，該節點包括處理器，當程式被處理器執行時實作本說明書實施例提供的用戶資料更新方法。

【0020】本說明書實施例還提供了一種可讀寫儲存媒體，用於電腦儲存，儲存媒體儲存有一個或者多個程式，該一個或者多個程式可被一個或者多個處理器執行，以實作本說明書實施例提供的用戶資料更新方法。

【0021】本說明書實施例提供了一種用戶資料更新方法、裝置、節點和儲存媒體，該方法包括在第一網路功能節點確定用戶的 AKMA 用戶資料更新的情況下，第一網路功能節點確定儲存用戶的 AKMA 上下文的第二網路功能節點；第一網路功能節點向第二網路功能節點發送用戶資料管理通知訊息；第一網路功能節點接收第二網路功能節點發送的用戶資料管理通知回應訊息；其中，用戶資料管理通知回應訊息是第二網路功能節點根據用戶資料管理通知訊息刪除用戶的 AKMA 上下文後發送的。透過這樣的設計方式，在用戶資料發生更新的情況下，

第二網路功能節點不保留 AKMA 相關的上下文，從而避免了 AKMA 相關的上下文被攻擊者濫用的情況。

【圖式簡單說明】

圖1是相關技術中的5G系統架構的示意圖；

圖2是相關技術中的應用的身份認證和金鑰管理系統架構的示意圖；

圖3是相關技術中的應用的身份認證和金鑰管理系統的金鑰推衍架構的示意圖；

圖4是相關技術中的AKMA錨定金鑰產生方法的流程示意圖；

圖5是本說明書實施例提供的一種用戶資料更新方法的流程圖；

圖6是本說明書實施例提供的一種用戶資料更新方法的信令交互示意圖；

圖7是本說明書實施例提供的一種用戶資料更新方法的信令交互示意圖；

圖8是本說明書實施例提供的一種用戶資料更新方法的信令交互示意圖；

圖9是本說明書實施例提供的一種用戶資料更新方法的信令交互示意圖；

圖10是本說明書實施例提供的一種用戶資料更新方法的流程圖；

圖11是本說明書實施例提供的一種用戶資料更新方法的流程圖；

圖12是本說明書實施例提供的一種用戶資料更新裝置的結構示意圖；

圖13是本說明書實施例提供的一種用戶資料更新裝置的結構示意圖；

圖14是本說明書實施例提供的一種用戶資料更新裝置的結構示意圖；

圖15是本說明書實施例提供的一種網路功能節點的結構示意圖。

【實施方式】

【0022】下文中將結合附圖對本說明書的實施例進行說明。

【0023】另外，在本說明書實施例中，“可選地”或者“示例性地”等詞用於表示作例子、例證或說明。本說明書實施例中被描述為“可選地”或者“示例性地”的任何實施例或設計方案不應被解釋為比其它實施例或設計方案更優選或更具優勢。確切而言，使用“可選地”或者“示例性地”等詞旨在以具體方式呈現相關概念。

【0024】為了便於理解本說明書實施例提供的方法，對本說明書實施例以及附圖中所涉及的網路功能節點功能等相關概念進行解釋：

【0025】UDM 用於永久存放用戶資料，位於用戶的歸屬網；ARPF 儲存用於認證的長期安全憑證，並使用長期安全憑證作為輸入執行金鑰運算。UDM 和 ARPF 位於運營商或者協力廠商系統的安全環境中，不會暴露給非授權的物理接入。另外，ARPF 和 AUSF 之間可以進行交互。

【0026】AMF 用於對用戶接入到網路的需求進行管理，負責終端到網路的非接入層（Non-Access Stratum，NAS）信令管理、用戶移動性管理等功能。AMF 具有 SEAF，SEAF 與 AUSF 以及 UE 交互，接收為 UE 認證程式而建立的中間金鑰。針對基於全球用戶識別卡（Universal Subscriber Identity Module，USIM）的認證方式，AMF 從 AUSF 獲取安全相關資料。

【0027】AUSF 具有與 ARPF 交互的認證功能，並可以終止來自 SEAF 的要求。AUSF 位於運營商或協力廠商系統的安全環境中，不會暴露給未授權的物理接入。

【0028】SMF 用於管理用戶的分組資料單元（Packet Data Unit，PDU）會話、服務品質（Quality of Service，QoS）流，為 UPF 制定包檢測和轉發規則等。

【0029】UPF 負責網際協議（Internet Protocol，IP）資料、非 IP 資料的路由和轉發、用量上報等功能。

【0030】PCF 負責為 AMF、SMF 提供各級別策略規則。

【0031】資料網路（Data Network，DN），包括例如運營商服務，網路接入，協力廠商服務等網路。

【0032】AF用於對AF會話進行管理。

【0033】SUCI包括六部分：

【0034】（1）SUPI型別（SUPI Type），取值為0-7，其中0為國際移動用戶識別碼（International Mobile Subscriber Identity，IMSI），1為網路接入識別碼（Network Access Identifier，NAI），其他保留。

【0035】（2）歸屬網路識別碼（Home Network Identifier），識別碼歸屬網路用戶，當SUPI為IMSI時，由移動國家碼（Mobile Country Code，MCC）和移動網路碼（Mobile Network Code，MNC）組成；當SUPI為NAI時，NAI由標準網際網路工程任務組要求評論（The Internet Engineering Task Force Request For Comments，IETF RFC）7542中的2.2章節定義。

【0036】（3）路由指示（Routing Indicator，RID），由歸屬網路運營商分配，配置在手機卡（USIM）中，和歸屬網路識別碼共同指示網路信令到服務用戶的AUSF和UDM。

【0037】（4）保護方案識別碼（Protection Scheme Identifier），表示無保護（null-scheme）或者有保護（non-null-scheme）兩種之一。

【0038】（5）歸屬網路公開金鑰識別碼（Home Network Public Key Identifier），表示一個歸屬網路提供的為保護SUPI的公開金鑰的識別碼，當無保護情況下，值為0。

【0039】（6）保護方案輸出（Scheme Output），當無保護時，Scheme Output為IMSI的移動用戶識別號碼（Mobile Subscriber Identification Number，MSIN）部分或者NAI；當有保護時，Scheme Output為使用橢圓曲線加密MSIN和NAI的值。

【0040】例如，當 IMSI 為 234150999999999，即 MCC=234，MNC=15 和 MSIN=0999999999，路由指示為 678，歸屬網路公開金鑰識別碼為 27 時，無保護的 SUCI 為 0、234、15、678、0、0 和 0999999999，有保護的 SUCI 為 0、234、15、678、1、27、<橢圓曲線密碼學（Elliptic Curve Cryptography，EEC）臨時公開金鑰值（EEC ephemeral public key value）>、<加密 0999999999>和<媒體接入控制（Medium Access Control，MAC）識別碼值（MAC tag value）>。

【0041】如圖 4 所示，5G 主認證程式如下：

【0042】S401、AUSF 與 UDM 交互，獲取認證資訊。例如，認證憑證（AKA 認證向量(Authentication Vector，AV)），認證方法使用 Nudm_UEAuthentication_Get Request 服務操作。

【0043】S402、在回應訊息中，UDM 可以向 AUSF 指示是否需要為 UE 產生 AKMA 金鑰。

【0044】S403、如果 AUSF 收到 UDM 的 AKMA 指示，則 AUSF 儲存 K_{AUSF}，並在主認證成功後基於 K_{AUSF} 產生 AKMA 錨定金鑰 K_{AKMA} 和 A-KID。在 UE 啟動與 AKMA 應用伺服器的通訊之前，UE 基於 K_{AUSF} 產生 AKMA 錨定金鑰 K_{AKMA} 和 A-KID。

【0045】S404、AUSF 產生 AKMA 金鑰材料後，使用 Naanf_AKMA_KeyRegistration Request 服務操作將用戶的 SUPI、產生的 A-KID 和 K_{AKMA} 發送到 AAnF。AAnF 儲存 AUSF 發送的最新金鑰材料。

【0046】S405、AAnF 使用 Naanf_AKMA_KeyRegistration Response 服務操作，將回應發送給 AUSF。

【0047】本說明書實施例提供了一種用戶資料更新方法，該方法流程圖如圖 5 所示，包括但不限於以下步驟：

【0048】S501、在第一網路功能節點確定用戶的AKMA用戶資料更新的情況下，第一網路功能節點確定儲存用戶的 AKMA 上下文的第二網路功能節點。

【0049】在本說明書實施例中，可以將本步驟中的第一網路功能節點理解為UDM，將第二網路功能節點理解為 AAnF。

【0050】本步驟中用戶的 AKMA 用戶資料更新的情況可以包括但不限於以下幾種情況：一、用戶退網，在 UDM 中刪除用戶訊息；二、用戶不使用 AKMA 服務，刪除 AKMA 用戶資訊；三、由於欠費等各種原因，用戶不能使用服務。

【0051】也即本步驟可以理解為在用戶的 AKMA 用戶資料發生更新的情況下，UDM 需要確認儲存用戶的 AKMA 上下文的 AAnF。

【0052】S502、第一網路功能節點向第二網路功能節點發送用戶資料管理通知訊息。

【0053】第一網路功能節點確定第二網路功能節點後，向第二網路功能節點發送用戶資料管理通知訊息時，可以在訊息中攜帶用戶識別碼 SUPI。可選地，也可以在該訊息中攜帶用戶的 AKMA 用戶指示。

【0054】S503、第一網路功能節點接收第二網路功能節點發送的用戶資料管理通知回應訊息。

【0055】第二網路功能節點接收到第一網路功能節點發送的用戶資料管理通知訊息後，可以根據訊息中攜帶的用戶識別碼 SUPI，刪除其儲存的該用戶的 AKMA 上下文，例如，SUPI、A-KID 和 K_{AKMA}，進而向第一網路功能節點發送用戶資料管理通知回應訊息。

【0056】本說明書實施例提供了一種用戶資料更新方法，該方法包括在第一網路功能節點確定用戶的 AKMA 用戶資料更新的情況下，第一網路功能節點確定儲存用戶的 AKMA 上下文的第二網路功能節點；第一網路功能節點向第二網路功能節點發送用戶資料管理通知訊息；第一網路功能節點接收第二網路功能節

點發送的用戶資料管理通知回應訊息；其中，用戶資料管理通知回應訊息是第二網路功能節點根據用戶資料管理通知訊息刪除用戶的 AKMA 上下文後發送的。透過這樣的設計方式，在使用者用戶資料發生更新的情況下，第二網路功能節點不保留 AKMA 相關的上下文，從而避免 AKMA 相關的上下文被攻擊者濫用的情況。

【0057】在一種實施例中，上述步驟 S501 的實作方式可以包括但不限於以下幾種情況：

【0058】第一種情況，第一網路功能節點根據本地配置確定第二網路功能節點；第二種情況，第一網路功能節點透過第三網路功能節點確定第二網路功能節點；第三種情況，第一網路功能節點透過第四網路功能節點確定第二網路功能節點。

【0059】如圖 6 所示，上述第一種情況的實作方式可以包括，第一網路功能節點根據用戶識別碼的部分欄位元確定第二網路功能節點。

【0060】示例性地，上述部分欄位元可以包括 MCC 或者 MNC 等。

【0061】如圖 7 所示，上述第二種情況的實作方式可以包括以下程式：第一網路功能節點向第三網路功能節點發送查詢訊息；第一網路功能節點接收第三網路功能節點根據查詢訊息發送的查詢回應訊息，該查詢回應訊息中攜帶有第二網路功能節點的識別碼或地址；第一網路功能節點根據查詢回應訊息確定第二網路功能節點。

【0062】示例性地，上述查詢訊息中可以攜帶有網路功能名（例如，AAnF）和/或網路型別（例如，AAnF 型別），以及，用戶識別碼 SUPI 和/或第一網路功能節點的位置資訊。上述第三網路功能節點可以為網路儲存庫功能（Network Repository Function，NRF），即 NRF 根據查詢訊息中的 SUPI 和/或 UDM 位置資訊，以及 AAnF 網路功能名和/或 AAnF 網路型別查詢儲存用戶 AKMA 上下文的 AAnF，進而向 UDM 發送查詢回應訊息。

【0063】如圖 8 所示，在一種實施例中，上述第三種情況的實作方式可以包括以下程式：第一網路功能節點向第四網路功能節點發送用戶改變要求訊息；第一網路功能節點接收第四網路功能節點發送的用戶改變要求回應訊息，用戶改變要求回應訊息攜帶有第二網路功能節點的識別碼或地址；第一網路功能節點根據用戶改變要求回應訊息確定第二網路功能節點。

【0064】示例性地，上述第四網路功能節點可以為 AUSF，上述用戶改變要求中可以攜帶有網路功能名（例如，AAnF）和/或網路型別（例如，AAnF 型別），以及，用戶識別碼 SUPI 和/或第一網路功能節點的位置資訊。即 AUSF 根據 SUPI 和/或 UDM 位置資訊，以及 AAnF 網路功能名和/或 AAnF 網路型別查詢儲存用戶 AKMA 上下文的 AAnF，並將查詢結果以用戶改變要求回應訊息的方式發送至 UDM。

【0065】如圖 9 所示，在一種實施例中，上述第三種情況的實作方式還可以包括以下程式：第一網路功能節點接收第四網路功能節點發送的用戶資料管理用戶訊息，用戶資料管理用戶訊息攜帶第二網路功能節點的識別碼或地址；第一網路功能節點根據用戶資料管理用戶訊息儲存第二網路功能節點的識別碼或地址；第一網路功能節點根據儲存的第二網路功能節點的識別碼或地址確定第二網路功能節點。

【0066】可選地，第一網路功能節點接收第四網路功能節點發送的用戶資料管理用戶訊息後，還可以向第四網路功能節點發送用戶資料管理用戶回應訊息。

【0067】在第一網路功能節點接收第四網路功能節點發送的用戶資料管理用戶訊息之前，第一網路功能節點還可以透過第四網路功能節點執行主認證程式，該主認證程式即為本說明書圖 4 所提供的實作方式。結合圖 4 可以看出，AUSF 產生 AKMA 金鑰材料後，將這一內容發送至 AAnF，由 AAnF 進行儲存。這樣，

在用戶的 AKMA 用戶資料更新的情況下，UDM 可以根據儲存的 AAnF 的識別碼或位址向 AAnF 發送用戶管理通知訊息。

【0068】圖 10 是本說明書實施例提供的一種用戶資料更新方法的流程圖，如圖 10 所示，該方法可以包括但不限於以下步驟：

【0069】S1001、第三網路功能節點接收第一網路功能節點發送的查詢訊息。

【0070】本說明書實施例中的第三網路功能節點可以為 NRF，第一網路功能節點可以為 UDM，第一網路功能節點發送的查詢訊息中可以攜帶有網路功能名和/或網路型別，以及，用戶識別碼和/或第一網路功能節點的位置資訊。

【0071】S1002、第三網路功能節點根據查詢訊息確定第二網路功能節點。

【0072】第三網路功能節點根據查詢訊息中的網路功能名和/或網路型別，以及，用戶識別碼和/或第一網路功能節點的位置資訊查詢第二網路功能節點。其中，該第二網路功能節點可以為 AAnF，AAnF 用於儲存用戶的 AKMA 上下文。

【0073】S1003、第三網路功能節點向第一網路功能節點發送查詢回應訊息。

【0074】第三網路功能節點發送的查詢回應訊息中攜帶有第二網路功能節點的識別碼或地址。

【0075】本說明書實施例提供了一種用戶資料更新方法，該方法包括第三網路功能節點接收第一網路功能節點發送的查詢訊息；第三網路功能節點根據查詢訊息確定第二網路功能節點；第三網路功能節點向第一網路功能節點發送查詢回應訊息，查詢回應訊息中攜帶有第二網路功能節點的識別碼或地址。透過上述方案可以有效確定第二網路功能節點，進而可以在用戶資料發生更新的情況下，實作第一網路功能節點向第二網路功能節點發送用戶資料管理通知訊息，以使得第二網路功能節點不保留 AKMA 相關的上下文，從而避免 AKMA 相關的上下文被攻擊者濫用的情況。

【0076】圖 11 是本說明書實施例提供的一種用戶資料更新方法的流程圖，如圖 11 所示，該方法可以包括但不限於以下步驟：

【0077】S1101、第四網路功能節點確定第二網路功能節點。

【0078】本說明書實施例中的第四網路功能節點可以為 AUSF，第二網路功能節點可以為 AAnF，AAnF 用於儲存用戶的 AKMA 上下文。

【0079】示例性地，本步驟的實作方式可以包括：第四網路功能節點接收第一網路功能節點發送的用戶改變要求訊息，該用戶改變要求訊息中攜帶用戶識別碼；第四網路功能節點根據用戶識別碼查詢第二網路功能節點。其中，上述第一網路功能節點可以為 UDM，即 AUSF 接收 UDM 發送的用戶改變要求訊息後，AUSF 根據該訊息中的用戶識別碼查詢儲存用戶的 AKMA 上下文的 AAnF。

【0080】S1102、第四網路功能節點向第一網路功能節點發送訊息。

【0081】第四網路功能節點發送的訊息中可以攜帶有第二網路功能節點的識別碼或位址。

【0082】本說明書實施例提供了一種用戶資料更新方法，該方法包括第四網路功能節點確定第二網路功能節點，第四網路功能節點向第一網路功能節點發送訊息，該訊息中攜帶有第二網路功能節點的識別碼或地址。透過上述方案可以實作第一網路功能節點確定第二網路功能節點，進而在用戶資料發生更新的情況下，由第一網路功能節點向第二網路功能節點發送用戶資料管理通知訊息，以使得第二網路功能節點不保留 AKMA 相關的上下文，從而避免 AKMA 相關的上下文被攻擊者濫用的情況。

【0083】圖 12 是本說明書實施例提供的一種用戶資料更新裝置，如圖 12 所示，該裝置可以包括：確定模組 1201、發送模組 1202、接收模組 1203；其中，確定模組 1202，用於在所述裝置確定用戶的 AKMA 用戶資料更新的情況下，確定儲存用戶的 AKMA 上下文的第二網路功能節點；發送模組 1202，用於向第二網路

功能節點發送用戶資料管理通知訊息；接收模組 1203，用於接收第二網路功能節點發送的用戶資料管理通知回應訊息；其中，用戶資料管理通知回應訊息是第二網路功能節點根據用戶資料管理通知訊息刪除用戶的 AKMA 上下文後發送的。

【0084】在一種示例中，上述確定模組 1201 用於根據本地配置確定第二網路功能節點；或者，透過第三網路功能節點確定第二網路功能節點；或者，透過第四網路功能節點確定第二網路功能節點。

【0085】在一種示例中，確定模組 1201，可以根據用戶識別碼的部分欄位元確定第二網路功能節點。

【0086】在一種示例中，確定模組 1201 可以包括通訊單元和確定單元；通訊單元，用於向第三網路功能節點發送查詢訊息，以及接收第三網路功能節點根據查詢訊息發送的查詢回應訊息，該查詢回應訊息中攜帶有第二網路功能節點的識別碼或地址；確定單元，用於根據查詢回應訊息確定第二網路功能節點。

【0087】在一種示例中，確定模組 1201，可以包括通訊單元和確定單元；通訊單元，用於向第四網路功能節點發送用戶改變要求訊息，以及接收第四網路功能節點發送的用戶改變要求回應訊息，該用戶改變要求回應訊息攜帶有第二網路功能節點的識別碼或地址；確定單元，用於根據用戶改變要求回應訊息確定第二網路功能節點。

【0088】上述查詢訊息可以攜帶網路功能名和/或網路型別，以及，用戶識別碼和/或第一網路功能節點的位置資訊；上述用戶改變要求訊息可以攜帶網路功能名和/或網路型別，以及，用戶識別碼和/或第一網路功能節點的位置資訊。

【0089】在一種示例中，上述確定模組 1201，可以包括通訊單元、儲存單元和確定單元；通訊單元，用於接收第四網路功能節點發送的用戶資料管理用戶訊息，用戶資料管理用戶訊息攜帶第二網路功能節點的識別碼或地址；儲存單元，用於

根據用戶資料管理用戶訊息儲存第二網路功能節點的識別碼或地址；確定單元，用於根據儲存的第二網路功能節點的識別碼或地址確定第二網路功能節點。

【0090】在一種示例中，上述裝置還可以包括認證模組，用於透過第四網路功能節點執行主認證程式。

【0091】本實施例提供的用戶資料更新裝置用於實作圖 5、圖 6、圖 7、圖 8、圖 9 所示實施例的用戶資料更新方法，其實作原理和技術效果類似，此處不再贅述。

【0092】圖 13 是本說明書實施例提供的一種用戶資料更新裝置，如圖 13 所示，該裝置可以包括：接收模組 1301、確定模組 1302、發送模組 1303；其中，接收模組 1301，用於接收第一網路功能節點發送的查詢訊息；確定模組 1302，用於根據查詢訊息確定第二網路功能節點；發送模組 1303，用於向第一網路功能節點發送查詢回應訊息，查詢回應訊息中攜帶有第二網路功能節點的識別碼或地址。

【0093】其中，上述查詢訊息攜帶有網路功能名和/或網路型別，以及，用戶識別碼和/或第一網路功能節點的位置資訊。

【0094】本實施例提供的用戶資料更新裝置用於實作圖 10 所示實施例的用戶資料更新方法，其實作原理和技術效果類似，此處不再贅述。

【0095】圖 14 是本說明書實施例提供的一種用戶資料更新裝置，如圖 14 所示，該裝置可以包括：確定模組 1401、發送模組 1402；其中，確定模組 1401，用於確定第二網路功能節點；發送模組 1402，用於向第一網路功能節點發送訊息，該訊息中攜帶有第二網路功能節點的識別碼或地址。

【0096】可選地，上述確定模組 1401 可以包括通訊單元，以及查詢單元；通訊單元，用於接收第一網路功能節點發送的用戶改變要求訊息，用戶改變要求訊息中攜帶有用戶識別碼；查詢單元，用於根據用戶識別碼查詢第二網路功能節點。

【0097】本實施例提供的用戶資料更新裝置用於實作圖 11 所示實施例的用戶資料更新方法，其實作原理和技術效果類似，此處不再贅述。

【0098】圖 15 為本說明書實施例提供的一種網路節點的結構示意圖，如圖 15 所示，該網路節點包括處理器 1501 和記憶體 1502；網路節點中處理器 1501 的數量可以是一個或多個，圖 15 中以一個處理器 1501 為例；網路節點中的處理器 1501 和記憶體 1502 可以透過匯流排或其他方式連接，圖 15 中以透過匯流排連接為例。

【0099】記憶體 1502 作為一種電腦可讀儲存媒體，可用於儲存軟體程式、電腦可執行程式以及模組，如本說明書圖 5 至圖 11 任一實施例中的方法對應的程式指令/模組。處理器 1501 透過執行儲存在記憶體 1502 中的軟體程式、指令以及模組實作上述的圖 5 至圖 11 實施例中的方法。

【0100】記憶體 1502 可主要包括儲存程式區和儲存資料區，其中，儲存程式區可儲存作業系統、至少一個功能所需的應用程式；儲存資料區可儲存根據機上盒的使用所創建的資料等。此外，記憶體 1502 可以包括高速接入隨機接入記憶體，還可以包括非易失性記憶體，例如至少一個磁碟記憶體件、快閃記憶體器件、或其他非易失性固態記憶體件。

【0101】在一種示例中，在可能的情況下，上述節點中的處理器 1501 也可以透過其內部的邏輯電路、門電路等硬體電路實作上述的用戶資料更新方法。

【0102】本說明書實施例還提供了一種可讀寫儲存媒體，用於電腦儲存，儲存媒體儲存有一個或者多個程式，在一個或者多個程式可被一個或者多個處理器執行時，可以實作如圖 5 至圖 11 任一實施例所提供的方法。

【0103】上文中所公開方法中的全部或一些步驟、設備中的功能模組/單元可以被實施為軟體、韌體、硬體及其適當的組合。

【0104】在硬體實施方式中，在以上描述中提及的功能模組/單元之間的劃分不一定對應於物理元件的劃分；例如，一個物理元件可以具有多個功能，或者一個功能或步驟可以由多個物理元件合作執行。一些物理元件或所有物理元件可以被實施為由處理器，如中央處理器、數位訊號處理器或微處理器執行的軟體，或者被實施為硬體，或者被實施為積體電路，如專用積體電路。這樣的軟體可以分佈在電腦可讀媒體上，電腦可讀媒體可以包括電腦儲存媒體（或非暫時性媒體）和通訊媒體（或暫時性媒體）。術語電腦儲存媒體包括在用於儲存資訊（諸如電腦可讀指令、資料結構、程式模組或其他資料）的任何方法或技術中實施的易失性和非易失性、可移除和不可移除媒體。電腦儲存媒體包括但不接入限於隨機接入記憶體（Random Access Memory，RAM）、唯讀記憶體（Read-Only Memory，ROM）、帶電可擦可程式唯讀記憶體（Electrically Erasable Programmable Read-Only Memory，EEPROM）、快閃記憶體或其他記憶體技術、光碟唯讀記憶體（Compact Disc Read-Only Memory，CD-ROM）、數位多功能盤（Digital Versatile Disc，DVD）或其他光碟儲存、磁盒、磁帶、磁片儲存或其他磁儲存裝置、或者可以用於儲存期望的資訊並且可以被電腦接入的任何其他的媒體。通訊媒體通常包含電腦可讀指令、資料結構、程式模組或者諸如載波或其他傳輸機制之類的調變資料信號中的其他資料，並且可包括任何資訊遞送媒體。

【符號說明】

S401, S402, S403, S404, S405:步驟

S501, S502, S503, S1001, S1002, S1003, S1101, S1102:步驟

1201: 確定模組

1202: 發送模組

1203: 接收模組

1301: 接收模組

1302: 確定模組

1303: 發送模組

1401: 確定模組

1402: 發送模組

1501: 處理器

1502: 記憶體

【發明申請專利範圍】

【請求項1】一種用戶資料更新方法，包括：

一第一網路功能節點根據一本地配置確定儲存一用戶的應用身份認證和金鑰管理架構（AKMA）上下文的一第二網路功能節點；或者，該第一網路功能節點透過一第三網路功能節點確定儲存該用戶的AKMA上下文的該第二網路功能節點；

該第一網路功能節點向該第二網路功能節點發送一用戶資料管理通知訊息；

該第一網路功能節點接收該第二網路功能節點發送的一用戶資料管理通知回應訊息；

其中，該用戶資料管理通知回應訊息是該第二網路功能節點根據該用戶資料管理通知訊息刪除該用戶的AKMA上下文後發送的。

【請求項2】如請求項1所述的方法，其中，該第一網路功能節點根據該本地配置確定儲存該用戶的AKMA上下文的該第二網路功能節點，包括：

該第一網路功能節點根據一用戶識別碼的部分欄位確定該第二網路功能節點，該部分欄位包括一移動國家碼（Mobile Country Code，MCC）或者一移動網路碼（Mobile Network Code，MNC）。

【請求項3】如請求項1所述的方法，其中，該第一網路功能節點透過該第三網路功能節點確定儲存該用戶的AKMA上下文的該第二網路功能節點，包括：

該第一網路功能節點向該第三網路功能節點發送一查詢訊息；

該第一網路功能節點接收該第三網路功能節點根據該查詢訊息發送的一查詢回應訊息，該查詢回應訊息攜帶該第二網路功能節點的一識別碼或一地址；

該第一網路功能節點根據該查詢回應訊息確定該第二網路功能節點。

【請求項4】如請求項1所述的方法，其中，該第一網路功能節點透過該第三網路功能節點確定儲存該用戶的AKMA上下文的該第二網路功能節點，包括：

該第一網路功能節點向該第三網路功能節點發送一用戶改變要求訊息；

該第一網路功能節點接收該第三網路功能節點發送的一用戶改變要求回應訊息，該簽約改變要求回應訊息攜帶該第二網路功能節點的一識別碼或一地址；

該第一網路功能節點根據該用戶改變要求回應訊息確定該第二網路功能節點。

【請求項5】如請求項3所述的方法，其中，該查詢訊息攜帶以下至少之一：該第二網路功能節點的一網路功能名、該第二網路功能節點的一網路型別、一用戶識別碼、該第一網路功能節點的一位置資訊。

【請求項6】如請求項4所述的方法，其中，該用戶改變要求訊息攜帶該第二網路功能節點的該網路功能名和該第二網路功能節點的該網路型別中的至少之一種，以及，該用戶識別碼和該第一網路功能節點的該位置資訊中的至少一種。

【請求項7】如請求項1所述的方法，其中，該第一網路功能節點透過該第三網路功能節點確定儲存該用戶的AKMA上下文的該第二網路功能節點，包括：

該第一網路功能節點接收該第三網路功能節點發送的一用戶資料管理簽約訊息，該用戶資料管理簽約訊息攜帶該第二網路功能節點的一識別碼或一地址；

該第一網路功能節點根據該用戶資料管理簽約訊息儲存該第二網路功能節點的該識別碼或該地址；

該第一網路功能節點根據該第一網路功能節點儲存的該第二網路功能節點的該識別碼或該地址確定該第二網路功能節點。

【請求項8】如請求項7所述的方法，其中，在該第一網路功能節點接收該第三網路功能節點發送的該用戶資料管理簽約訊息之前，該方法還包括：

該第一網路功能節點透過該第三網路功能節點執行一主認證程式。

【請求項9】一種第一網路功能節點，包括用於儲存一電腦指令的一記憶體以及與該記憶體通訊的一處理器，其中，當該處理器執行該電腦指令時，該處理器被配置為使該第一網路功能節點：

根據一本地配置確定儲存一用戶的應用身份認證和金鑰管理架構（AKMA）上下文的一第二網路功能節點；或者透過一第三網路功能節點確定儲存該用戶的AKMA上下文的該第二網路功能節點；

向該第二網路功能節點發送一用戶資料管理通知訊息；

接收該第二網路功能節點發送的一用戶資料管理通知回應訊息；

其中，該用戶資料管理通知回應訊息是該第二網路功能節點根據該用戶資料管理通知訊息刪除該用戶的AKMA上下文後發送的。

【請求項10】如請求項9所述的第一網路功能節點，其中，當該處理器被配置為使該第一網路功能節點根據該本地配置確定儲存該用戶的AKMA上下文的該第二網路功能節點時，該處理器被配置為使該第一網路功能節點：

根據一用戶識別碼的部分欄位確定該第二網路功能節點，該部分欄位包括一移動國家碼（Mobile Country Code，MCC）或者一移動網路碼（Mobile Network Code，MNC）。

【請求項11】如請求項9所述的第一網路功能節點，其中，當該處理器被配置為使該第一網路功能節點透過該第三網路功能節點確定儲存該用戶的AKMA上下文的該第二網路功能節點時，該處理器被配置為使該第一網路功能節點：

向該第三網路功能節點發送一查詢訊息；

接收該第三網路功能節點根據該查詢訊息發送的一查詢回應訊息，該查詢回應訊息攜帶該第二網路功能節點的一識別碼或一地址；

根據該查詢回應訊息確定該第二網路功能節點。

【請求項12】如請求項9所述的第一網路功能節點，其中，當該處理器被配置為使該第一網路功能節點透過該第三網路功能節點確定儲存該用戶

的AKMA上下文的該第二網路功能節點時，該處理器被配置為使該第一網路功能節點：

向該第三網路功能節點發送一用戶改變要求訊息；

接收該第三網路功能節點發送的一用戶改變要求回應訊息，該用戶改變要求回應訊息攜帶該第二網路功能節點的一識別碼或一地址；

根據該用戶改變要求回應訊息確定該第二網路功能節點。

【請求項13】如請求項11所述的第一網路功能節點，其中，該查詢訊息攜帶以下至少之一：該第二網路功能節點的一網路功能名、該第二網路功能節點的一網路型別、一用戶識別碼和該第一網路功能節點的一位置資訊。

【請求項14】一種儲存媒體，該儲存媒體儲存有一電腦可讀指令，當該電腦可讀指令由一第一網路功能節點中的一處理器執行時，使得該處理器：

根據一本地配置確定儲存一用戶的應用身份認證和金鑰管理架構（AKMA）上下文的一第二網路功能節點；或者透過一第三網路功能節點確定儲存該用戶的AKMA上下文的該第二網路功能節點；

向該第二網路功能節點發送一用戶資料管理通知訊息；

接收該第二網路功能節點發送的一用戶資料管理通知回應訊息；

其中，該用戶資料管理通知回應訊息是該第二網路功能節點根據該用戶資料管理通知訊息刪除該用戶的AKMA上下文後發送的。

【請求項15】如請求項14所述的儲存媒體，其中，當該電腦可讀指令使該處理器根據該本地配置確定儲存該用戶的AKMA上下文的該第二網路功能節點時，該電腦可讀指令使該處理器：

根據一用戶識別碼的部分欄位確定該第二網路功能節點，該部分欄位包括一移動國家碼（Mobile Country Code，MCC）或者一移動網路碼（Mobile Network Code，MNC）。

【請求項16】如請求項14所述的儲存媒體，其中，當該電腦可讀指令使該處理器透過該第三網路功能節點確定儲存該用戶的AKMA上下文的該第二網路功能節點時，該電腦可讀指令使該處理器：

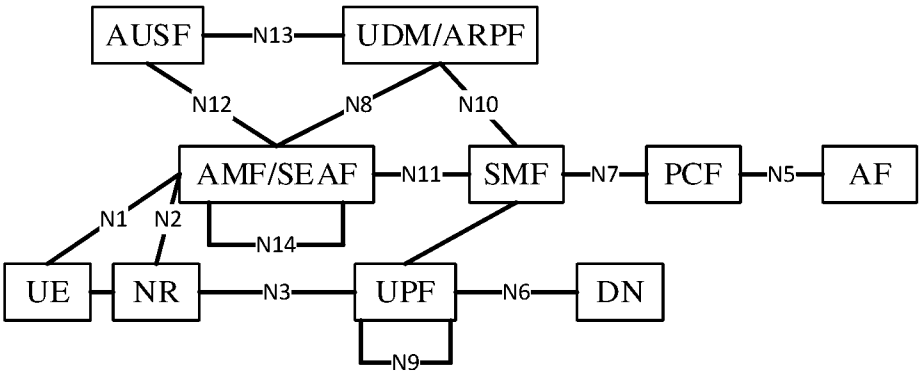
向該第三網路功能節點發送一查詢訊息；

接收該第三網路功能節點根據該查詢訊息發送的一查詢回應訊息，該查詢回應訊息攜帶該第二網路功能節點的一識別碼或一地址；

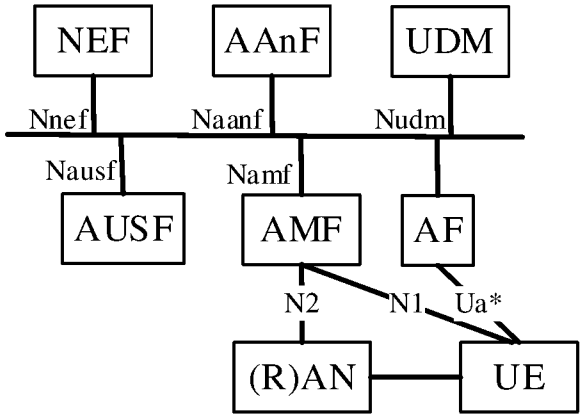
根據該查詢回應訊息確定該第二網路功能節點。

【請求項17】如請求項16所述的儲存媒體，其中，該查詢訊息攜帶以下至少之一：該第二網路功能節點的一網路功能名、該第二網路功能節點的一網路型別、一用戶識別碼和該第一網路功能節點的一位置資訊。

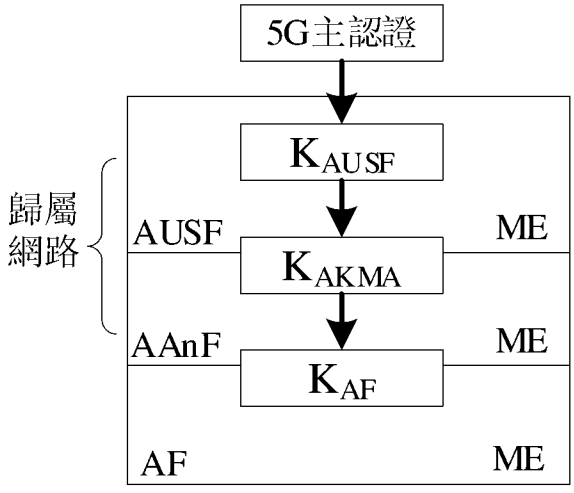
【發明圖式】


AUSF
N13
UDM/ARPF
N12
N8
N10
AMF/SEAF
N11
SMF
N7
PCF
N5
AF
N1
N2
N14
UE
NR
N3
UPF
N6
DN
N9

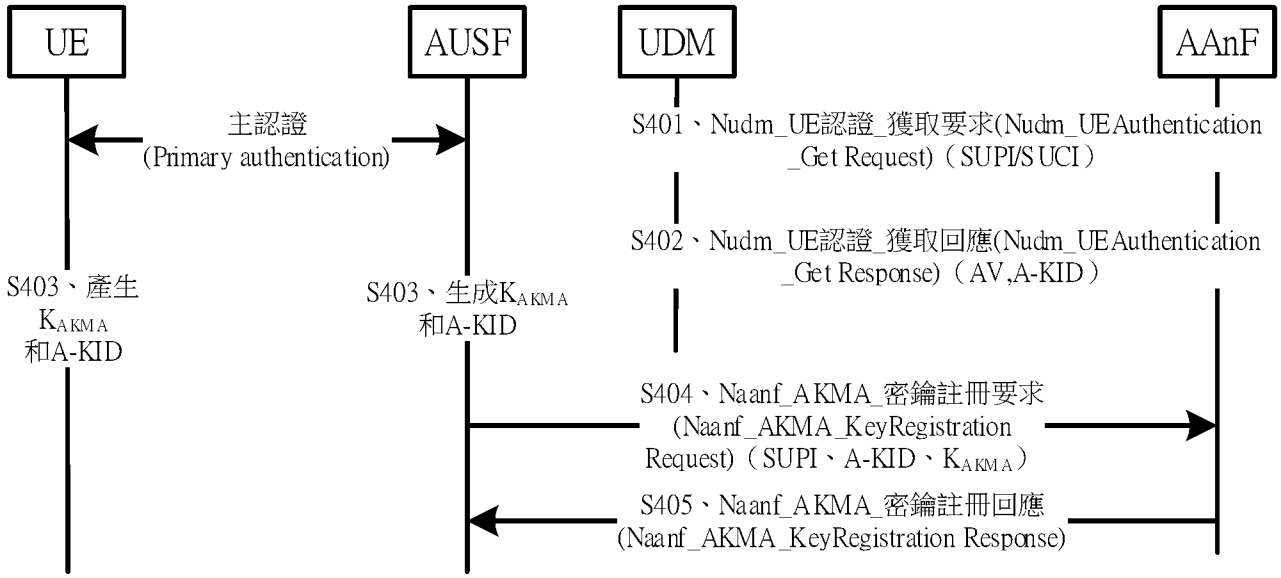
【圖 1】


NEF
AAnF
UDM
Nnef
Naanf
Nudm
Nausf
Namf
AUSF
AMF
AF
N2
N1
Ua*
(R)AN
UE

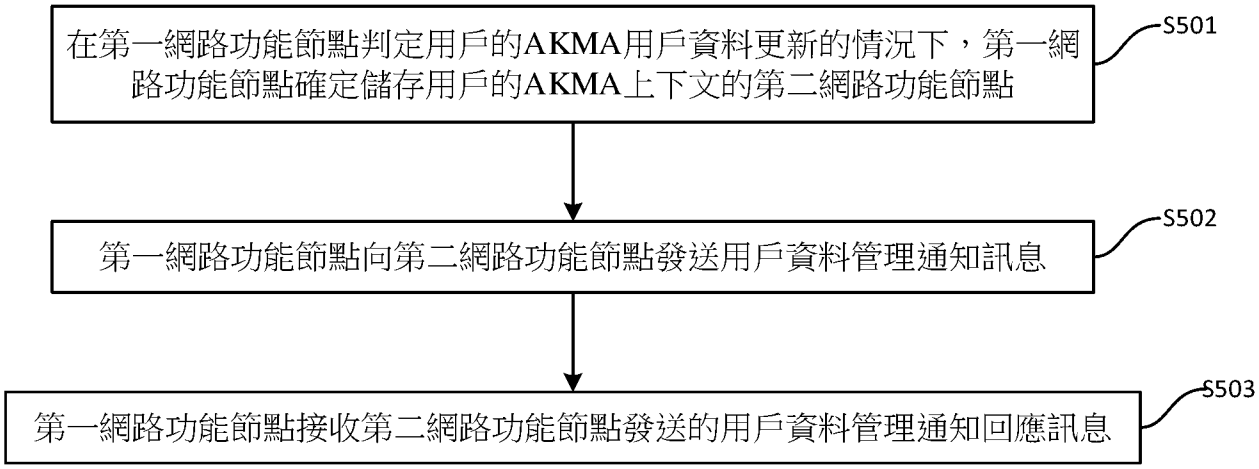
【圖 2】


5G主認證
K_{AUSF}
歸屬網路
AUSF
ME
K_{AKMA}
AAnF
ME
K_{AF}
AF
ME

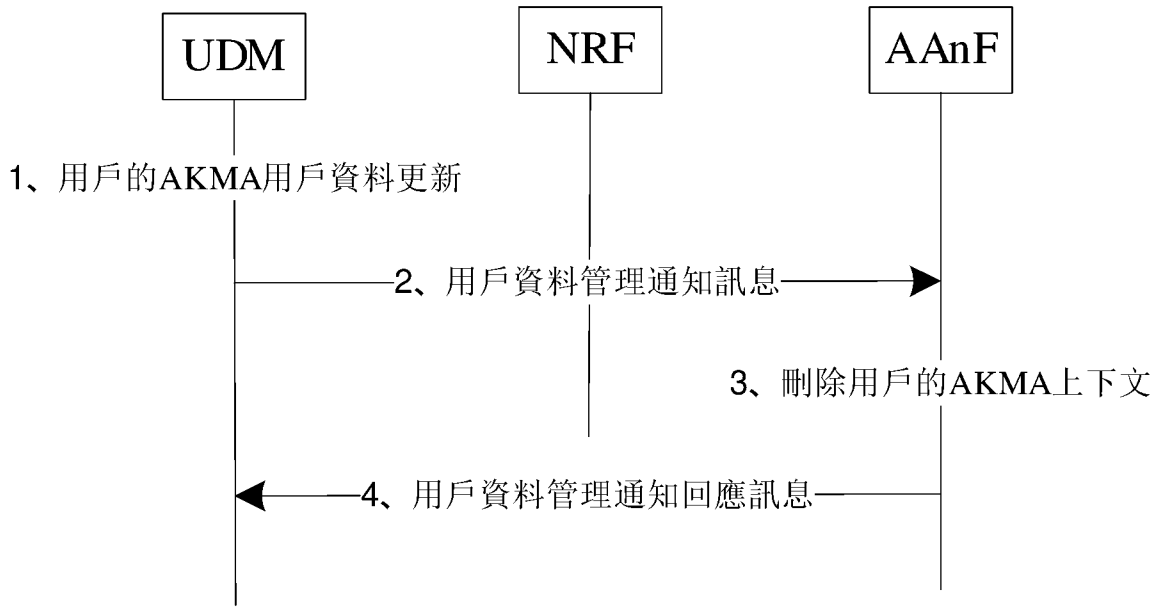
【圖 3】


UE
AUSF
UDM
AAnF
主認證
(Primary authentication)
S401、Nudm_UE認證_獲取要求(Nudm_UEAuthentication_Get Request)（SUPI/SUCI）
S402、Nudm_UE認證_獲取回應(Nudm_UEAuthentication_Get Response)（AV,A-KID）
S403、產生 K_{AKMA} 和A-KID
S403、生成 K_{AKMA} 和A-KID
S404、Naanf_AKMA_密鑰註冊要求 (Naanf_AKMA_KeyRegistration Request)（SUPI、A-KID、K_{AKMA}）
S405、Naanf_AKMA_密鑰註冊回應 (Naanf_AKMA_KeyRegistration Response)

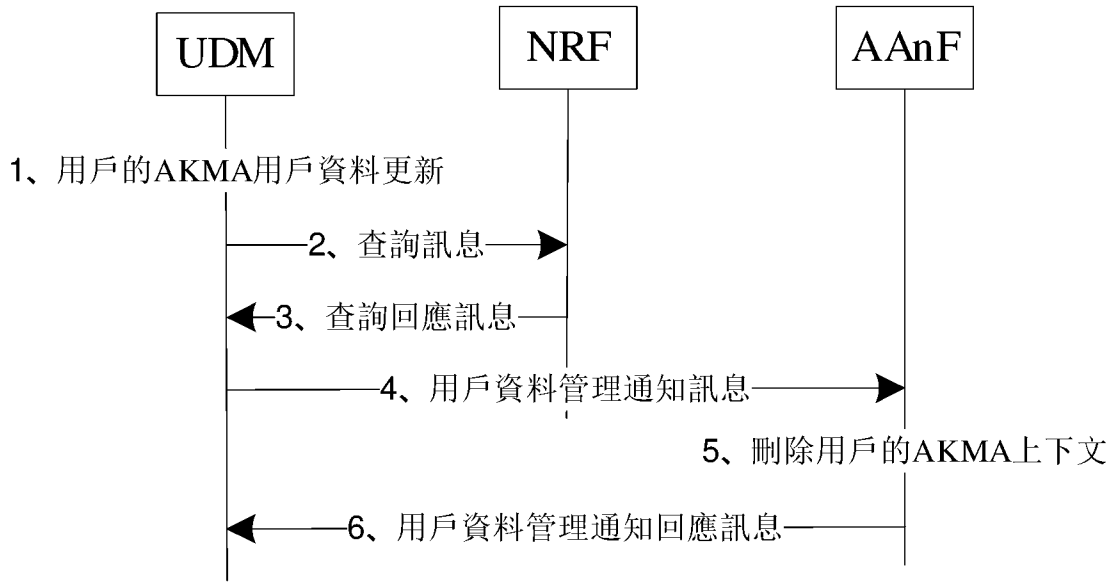
【圖 4】


在第一網路功能節點判定用戶的AKMA用戶資料更新的情況下，第一網路功能節點確定儲存用戶的AKMA上下文的第二網路功能節點
S501
第一網路功能節點向第二網路功能節點發送用戶資料管理通知訊息
S502
第一網路功能節點接收第二網路功能節點發送的用戶資料管理通知回應訊息
S503

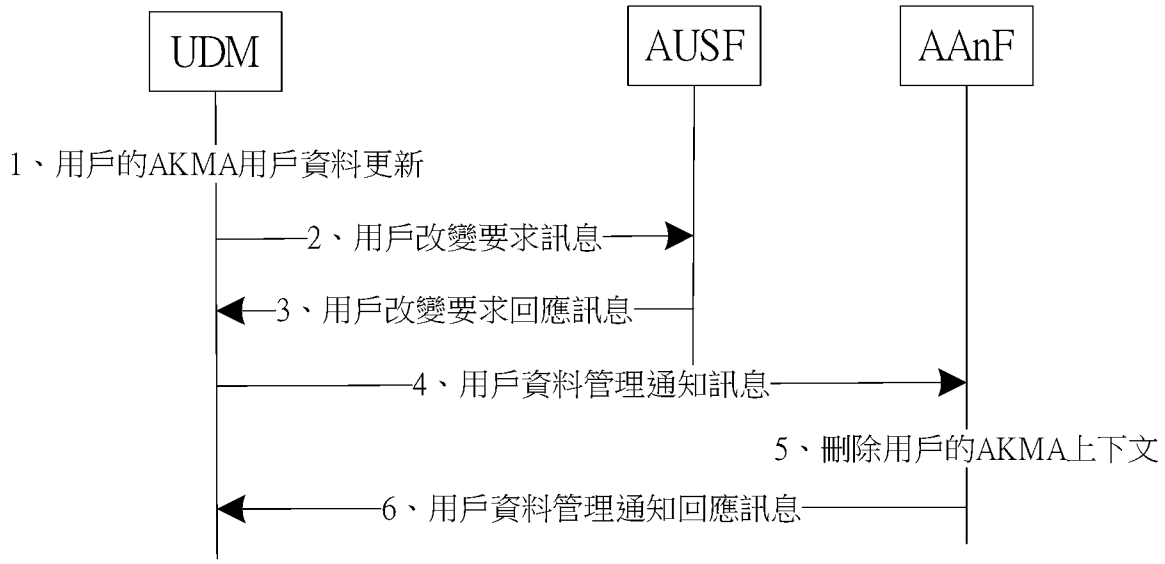
【圖 5】


UDM
NRF
AAnF
1、用戶的AKMA用戶資料更新
2、用戶資料管理通知訊息
3、刪除用戶的AKMA上下文
4、用戶資料管理通知回應訊息

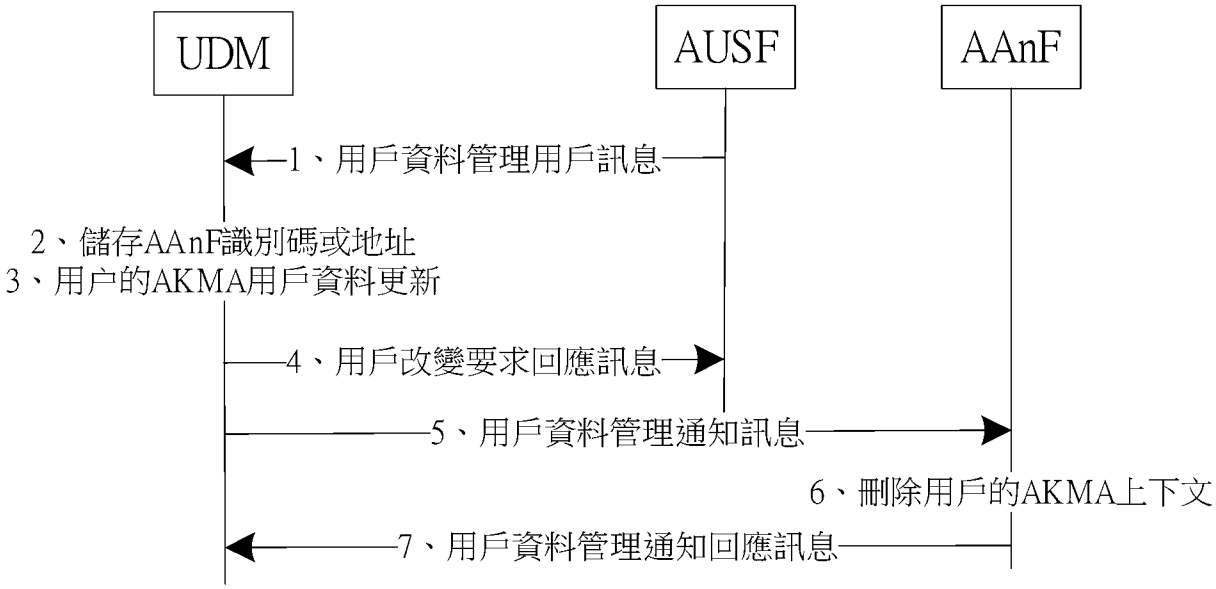
【圖 6】


UDM
NRF
AAnF
1、用戶的AKMA用戶資料更新
2、查詢訊息
3、查詢回應訊息
4、用戶資料管理通知訊息
5、刪除用戶的AKMA上下文
6、用戶資料管理通知回應訊息

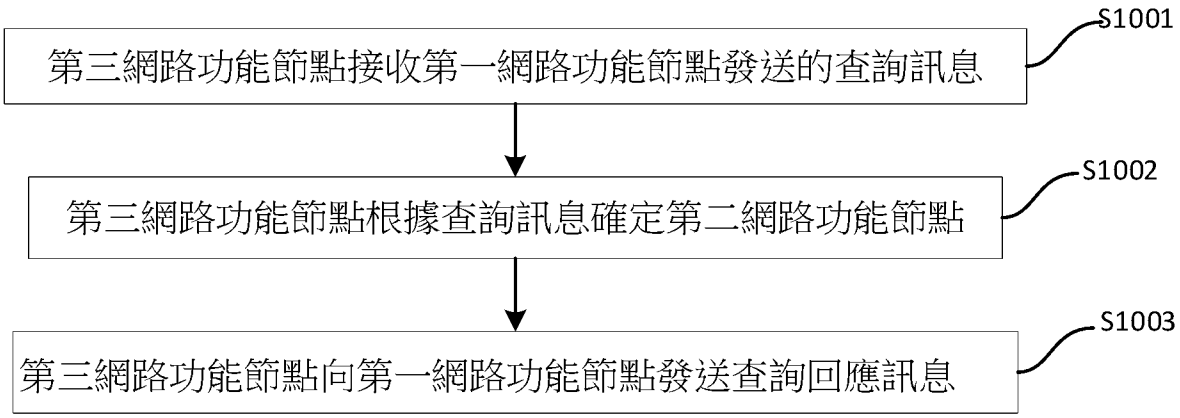
【圖 7】


UDM
AUSF
AAnF
1、用戶的AKMA用戶資料更新
2、用戶改變要求訊息
3、用戶改變要求回應訊息
4、用戶資料管理通知訊息
5、刪除用戶的AKMA上下文
6、用戶資料管理通知回應訊息

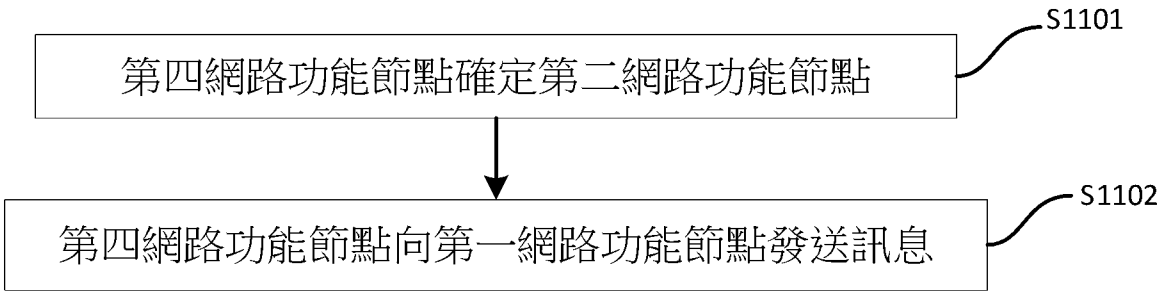
【圖 8】


UDM
AUSF
AAnF
1、用戶資料管理用戶訊息
2、儲存AAnF識別碼或地址
3、用户的AKMA用戶資料更新
4、用戶改變要求回應訊息
5、用戶資料管理通知訊息
6、刪除用戶的AKMA上下文
7、用戶資料管理通知回應訊息

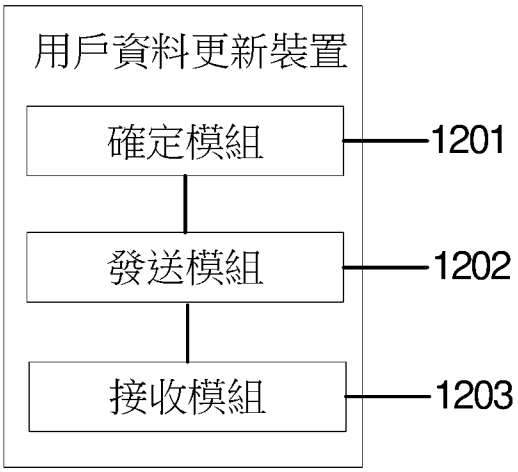
【圖 9】


第三網路功能節點接收第一網路功能節點發送的查詢訊息
S1001
第三網路功能節點根據查詢訊息確定第二網路功能節點
S1002
第三網路功能節點向第一網路功能節點發送查詢回應訊息
S1003

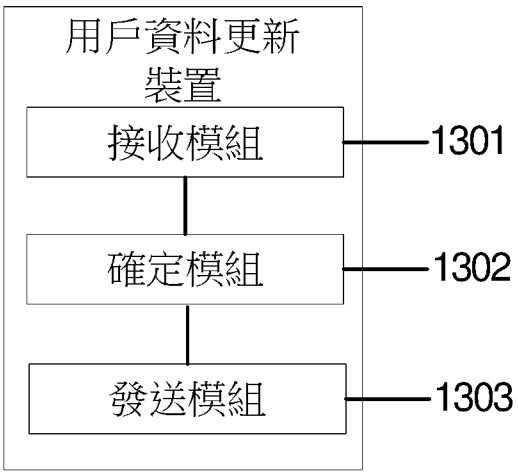
【圖 10】


第四網路功能節點確定第二網路功能節點
S1101
第四網路功能節點向第一網路功能節點發送訊息
S1102

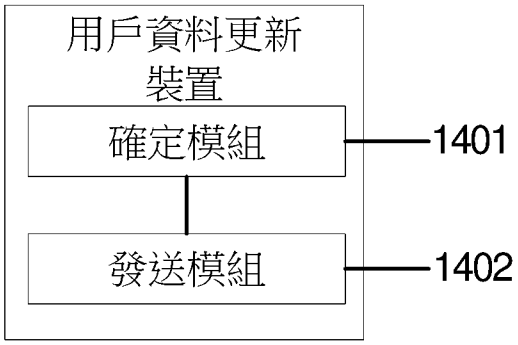
【圖 11】


用戶資料更新裝置
確定模組
1201
發送模組
1202
接收模組
1203

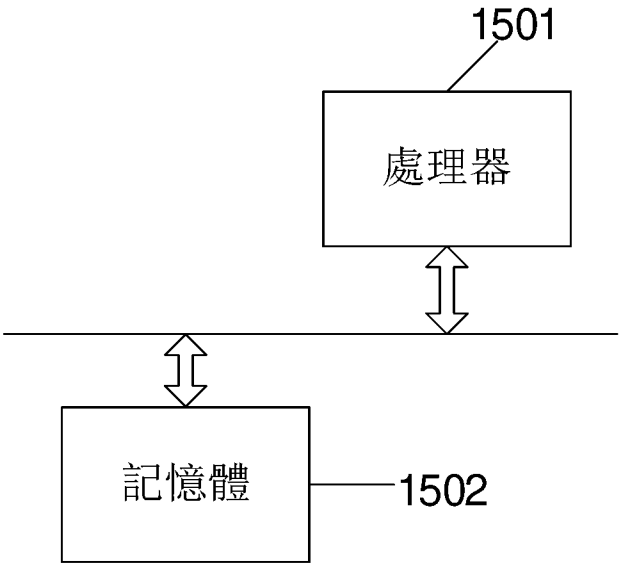
【圖 12】


用戶資料更新裝置
接收模組
1301
確定模組
1302
發送模組
1303

【圖 13】


用戶資料更新裝置
確定模組
1401
發送模組
1402

【圖 14】


1501
處理器
記憶體
1502

【圖 15】