I524807

(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 I524807 B**

(45)公告日： 中華民國 105 (2016) 年 03 月 01 日

(21)申請案號：102116114 (22)申請日： 中華民國 102 (2013) 年 05 月 06 日

(51)Int. Cl.： *H04W92/18 (2009.01)* *H04W12/06 (2009.01)*
H04L29/02 (2006.01)

(30)優先權：2012/05/07 美國 61/643,383

(71)申請人：財團法人工業技術研究院 (中華民國) INDUSTRIAL TECHNOLOGY RESEARCH INSTITUTE (TW)
新竹縣竹東鎮中興路 4 段 195 號

(72)發明人：王瑞堂 WANG, JUI TANG (TW) ；林咨銘 LIN, TZU MING (TW)

(74)代理人：詹銘文；葉璟宗

(56)參考文獻：

EP 1650915A1 US 2010/0153727A1

審查人員：賴慶仁

申請專利範圍項數：38 項 圖式數：8 共 53 頁

(54)名稱

裝置間通訊的認證系統及認證方法

AUTHENTICATION SYSTEM FOR DEVICE-TO-DEVICE COMMUNICATION AND AUTHENTICATION METHOD THEREFORE

(57)摘要

一種裝置間通訊的認證系統及認證方法。此認證系統包括第一使用者裝置以及認證伺服器。認證伺服器位於第一使用者裝置的通訊範圍內。當第一使用者裝置發出連接請求至所述認證伺服器時，認證伺服器對所述第一使用者裝置進行常規認證並提供金鑰產生信息至第一使用者裝置。認證伺服器依據所述金鑰產生信息以及金鑰衍生程序以產生伺服器金鑰。第一使用者裝置依據金鑰產生信息以及金鑰衍生程序產生裝置金鑰，以獲得裝置間通訊的認證，使第一使用者裝置與獲得裝置間通訊的認證的第二使用者裝置直接進行裝置間通訊，而不需透過認證伺服器。

An authentication system for device-to-device communication and an authentication method therefore are provided. The authentication system includes a first user equipment (UE) and a authentication server within a communication range of the first UE. When the first UE sends a connect request to the authentication server, the authentication server performs a routine certification to the first UE and provides a key derivation information to the first UE. The authentication server produces a server key according to the key derivation information and a key derivation procedure. The first UE produces a device key according to the key derivation information and the key derivation procedure to obtain an authentication for device-to-device communication. Thus, the authenticated first UE can directly communicate with the second UE which is obtained authentication for device-to-device communication without through the authentication server.

指定代表圖：

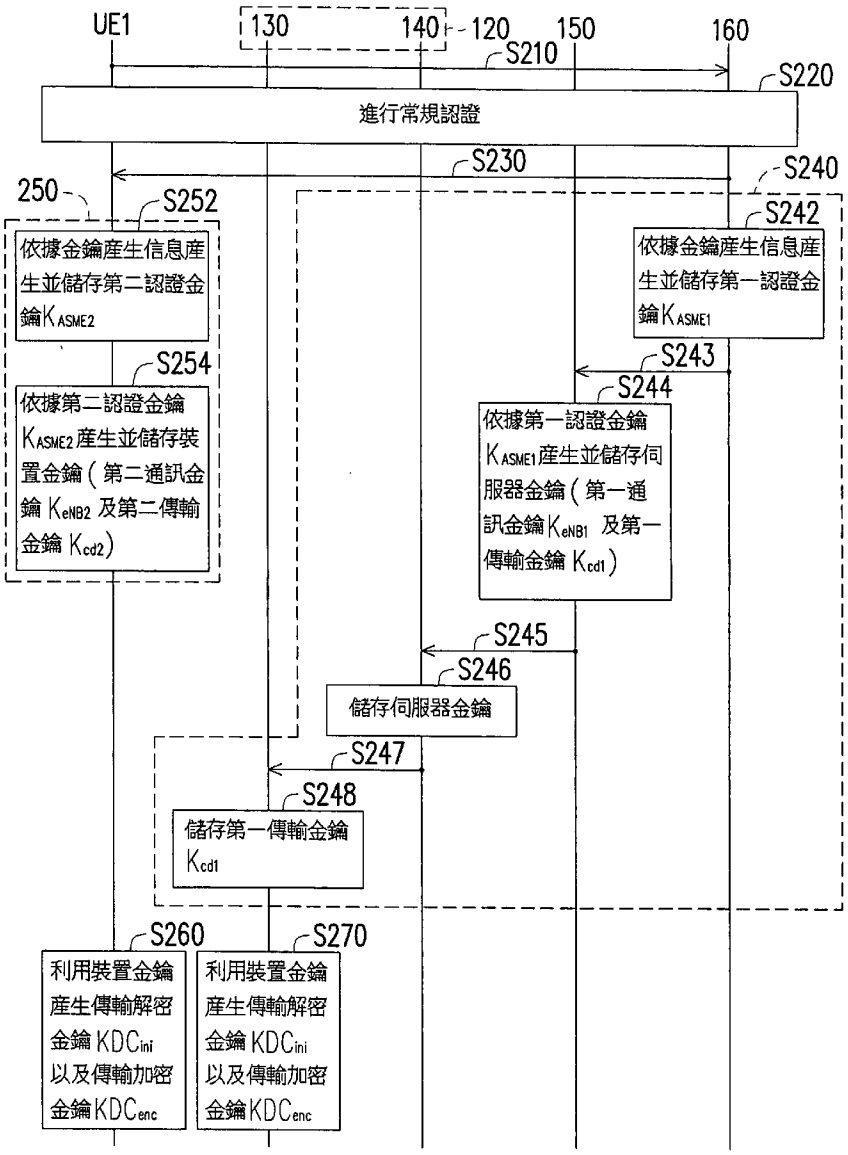

圖2

符號簡單說明：

UE1・・・使用者裝置

120・・・通訊設備

130・・・裝置間通訊控制器

140・・・基地台

150・・・管理單元

160・・・認證單元

S210~S270・・・步驟

I524807

公告本

發明摘要

※ 申請案號：102116114

※ 申請日： 102. 5. 06 ※IPC 分類：H04W 8/18 (2009.01)
H04W 12/06 (2009.01)
H04L 29/07 (2006.01)

【發明名稱】裝置間通訊的認證系統及認證方法

AUTHENTICATION SYSTEM FOR DEVICE-TO-DEVICE COMMUNICATION AND AUTHENTICATION METHOD THEREFORE

【中文】

一種裝置間通訊的認證系統及認證方法。此認證系統包括第一使用者裝置以及認證伺服器。認證伺服器位於第一使用者裝置的通訊範圍內。當第一使用者裝置發出連接請求至所述認證伺服器時，認證伺服器對所述第一使用者裝置進行常規認證並提供金鑰產生信息至第一使用者裝置。認證伺服器依據所述金鑰產生信息以及金鑰衍生程序以產生伺服器金鑰。第一使用者裝置依據金鑰產生信息以及金鑰衍生程序產生裝置金鑰，以獲得裝置間通訊的認證，使第一使用者裝置與獲得裝置間通訊的認證的第二使用者裝置直接進行裝置間通訊，而不需透過認證伺服器。

【英文】

An authentication system for device-to-device communication and an authentication method therefore are provided. The authentication system includes a first user equipment (UE) and a

authentication server within a communication range of the first UE. When the first UE sends a connect request to the authentication server, the authentication server performs a routine certification to the first UE and provides a key derivation information to the first UE. The authentication server produces a server key according to the key derivation information and a key derivation procedure. The first UE produces a device key according to the key derivation information and the key derivation procedure to obtain an authentication for device-to-device communication. Thus, the authenticated first UE can directly communicate with the second UE which is obtained authentication for device-to-device communication without through the authentication server.

【代表圖】

【本案指定代表圖】：圖 2。

【本代表圖之符號簡單說明】：

UE1：使用者裝置

120：通訊設備

130：裝置間通訊控制器

140：基地台

150：管理單元

160：認證單元

S210~S270：步驟

【本案若有化學式時，請揭示最能顯示發明特徵的化學式】：

無

發明專利說明書

（本說明書格式、順序，請勿任意更動）

【發明名稱】裝置間通訊的認證系統及認證方法

AUTHENTICATION SYSTEM FOR DEVICE-TO-DEVICE COMMUNICATION AND AUTHENTICATION METHOD THEREFORE

【技術領域】

【0001】 本揭露是有關於一種通訊與認證技術，且特別是有關於一種裝置間（device-to-device；D2D）通訊的認證系統及認證方法。

【先前技術】

【0002】 行動通訊技術日漸普及，行動裝置中所使用的無線通訊技術通常皆需要連線至基地台（base station；BS）或是無線存取點（access point；AP）以使行動裝置之間相互進行通訊，也就是行動裝置間必須透過 BS 或 AP 來進行通訊，如，通用封包無線服務（General Packet Radio Service；GPRS）技術、分碼多重進接（Code Division Multiple Access；CDMA）技術、WIFI（IEEE 802.11）通訊技術…等。當行動裝置位於訊號不佳的地點或是附近沒有 BS 或無線 AP 時，便無法對其他行動裝置進行通訊。例如，當因爲天災而導致大部分的基地台無法使用時，使用者手中的行動裝置便無法對外通訊。因此，便希望能夠研發出不需要透過 BS 或無線 AP 便可以進行裝置間通訊的技術，也就是所謂的裝置間

（device-to-device；D2D）的直接通訊（direct communication）。

【0003】 裝置間的直接通訊是指各種電子裝置之間透過相應的通訊協定來直接地進行資料傳輸、控制、資料分享、通話…等，而不需要透過 BS 或無線 AP 進行中介管理，例如藍芽協定、WIFI 直連（WIFI direct）協定…等。直接通訊也可以稱爲是裝置間（device-to-device；D2D）通訊、適地應用（proximity-based system）、直接通訊（direct communication）、智慧直接連結（smart direct link）…等技術。目前，第三代合夥專案（Third Generation Partnership Project；3GPP）正在研發的新一代標準化無線通訊技術，如長期演進技術（Long Term Evolution；LTE）、升級版 LTE（LTE Advanced）…等，也希望能夠將直接通訊技術整合在 LTE 中。

【0004】 3GPP 規劃了許多的機制來實現直接通訊的各種應用，例如在裝置間通訊時的裝置相互識別（identify）機制、授權（authenticate）機制、允許（authorize）機制、付費機制及安全機制…等。然而，這些機制仍然在熱烈討論中而未提出任何具體的實現方案。

【發明內容】

【0005】 本揭露提供一種裝置間通訊的認證系統及認證方法，其實現了裝置間通訊的認證機制，並可將此認證機制延伸應用至裝置間通訊的付費、通訊安全等機制。

【0006】 本揭露提出一種裝置間通訊的認證系統。認證系統包括第一使用者裝置以及認證伺服器。認證伺服器位於第一使用者裝置的通訊範圍內。當第一使用者裝置發出連接請求至所述認證伺服器時，認證伺服器對所述第一使用者裝置進行常規認證並提供金鑰產生信息至第一使用者裝置。認證伺服器依據所述金鑰產生信息以及金鑰衍生程序以產生伺服器金鑰。第一使用者裝置依據金鑰產生信息以及金鑰衍生程序產生裝置金鑰，以獲得裝置間通訊的認證，使第一使用者裝置與獲得裝置間通訊的認證的第二使用者裝置直接進行裝置間通訊，而不需透過認證伺服器。

【0007】 從另一角度來看，本揭露提出一種裝置間通訊的認證系統。認證系統包括第一使用者裝置、第二使用者裝置以及認證伺服器。認證伺服器位於第一使用者裝置以及第二使用者裝置的通訊範圍內。當第一使用者裝置及第二使用者裝置分別發出裝置間通訊連接請求至所述認證伺服器時，認證伺服器對所述第一及第二使用者裝置進行常規認證並分別提供第一金鑰產生信息及第二金鑰產生信息至所述第一及第二使用者裝置。認證伺服器依據所述第一及第二金鑰產生信息以及金鑰衍生程序以產生伺服器金鑰。認證伺服器將所述伺服器金鑰分別傳送至所述第一及第二使用者裝置，以使所述第一及第二使用者裝置獲得裝置間通訊的認證並直接進行裝置間通訊，而不需透過所述認證伺服器。

【0008】 從再一角度來看，本揭露提出一種裝置間通訊的認證方法，其適用於通訊系統中的第一使用者裝置。所述通訊系統還包

括認證伺服器以及第二使用者裝置。所述認證方法包括下列步驟。發出連接請求至所述認證伺服器。所述認證伺服器對第一使用者裝置進行常規認證並提供金鑰產生信息，且所述認證伺服器依據所述金鑰產生信息以及金鑰衍生程序以產生伺服器金鑰。以及，依據所述金鑰產生信息以及金鑰衍生程序而產生裝置金鑰，以獲得裝置間通訊的認證，使第一使用者裝置與獲得裝置間通訊的認證的第二使用者裝置能直接進行裝置間通訊，而不需透過所述認證伺服器。

【0009】 從其他角度來看，本揭露提出一種裝置間通訊的認證方法，其適用於通訊系統中的認證伺服器。所述通訊系統還包括第一使用者裝置以及第二使用者裝置。所述認證方法包括下列步驟。接收從該第一使用者裝置發出的連接請求。對所述第一使用者裝置進行常規認證並提供金鑰產生信息至所述第一使用者裝置。依據所述金鑰產生信息以及金鑰衍生程序以產生伺服器金鑰。以及，所述第一使用者裝置依據所述金鑰產生信息以及所述金鑰衍生程序產生裝置金鑰，以獲得裝置間通訊的認證，使所述第一使用者裝置與獲得裝置間通訊的認證的第二使用者裝置直接進行裝置間通訊，而不需透過所述認證伺服器。

【0010】 基於上述，本揭露實施例中的認證系統及認證方法實現了裝置間通訊的認證機制，使用者裝置可以先行通過認證伺服器來進行裝置間通訊的認證並獲得相應的認證金鑰，並在獲得裝置間通訊的認證後與其他已獲得認證的其他使用者裝置進行直接通

訊，而不需再次通過通訊處理裝置（如，基地台或是無線存取點）來進行通訊。透過本揭露所認證的使用者裝置可以依照認證金鑰內部設定的金鑰有效信息來與其他使用者裝置進行裝置間的相互認證（mutual authentication）、裝置間通訊機制、金鑰分配（key distribution）以及金鑰更新，並可於裝置間認證的判定中加入收費及安全機制，藉以保障實現此裝置間通訊系統的廠商利益及使用此裝置間通訊系統的使用者權益。

【0011】 爲讓本揭露的上述特徵和優點能更明顯易懂，下文特舉實施例，並配合所附圖式作詳細說明如下。

【圖式簡單說明】

【0012】

圖 1 是依照本揭露一實施例之裝置間通訊的認證系統的方塊圖。

圖 2 是依照本揭露第一實施例說明裝置間通訊的認證方法的流程圖。

圖 3 是依照本揭露第二實施例說明裝置間通訊的認證方法的流程圖。

圖 4 是依照本揭露第三實施例說明裝置間通訊的認證方法的流程圖。

圖 5 是依照本揭露第四實施例說明裝置間通訊的認證方法的細節流程圖。

圖 6 是依照本揭露第五實施例說明裝置間通訊的認證方法的細節流程圖。

圖 7 是依照本揭露第六實施例說明裝置間通訊的認證方法的細節流程圖。

圖 8 是依照本揭露第七實施例說明裝置間通訊的認證方法的細節流程圖。

【實施方式】

【0013】 本揭露的認證系統及認證方法實現了裝置間通訊的認證機制，使用者裝置可以先行通過認證伺服器來進行裝置間通訊的認證並獲得相應的認證金鑰，並在獲得裝置間通訊的認證後與其他已獲得認證的其他使用者裝置進行直接通訊，而不需再次通過通訊處理裝置（如，基地台或是無線存取點）來進行通訊。此外，本揭露可在認證程序中加入付費機制，藉以達到使用者付費的理想。

【0014】 圖 1 是依照本揭露一實施例之裝置間通訊的認證系統的方塊圖。本揭露所述的認證系統 100 是符合第三代合夥專案（3GPP）所提出的無線通訊網路協定，因此以下主要以長期演進技術（LTE）配合常用的無線通訊技術（如，CDMA、WIFI…等）作爲裝置間通訊的舉例。然而，應用本揭露的技術人員應可將本案所揭示的認證技術延伸至相關通訊協定及系統當中，例如有關於使用者裝置之間不需通過通訊處理裝置（如，基地台或無線存

取點）而可進行直接通訊，而僅需先行經由認證伺服器獲得裝置間通訊的認證的通訊系統。

【0015】 認證系統 100 包括認證伺服器 110 以及至少一個使用者裝置 UE1~UE3。認證伺服器 110 包括通訊設備 120、管理單元 150 以及認證單元 160。通訊設備 120 則可包括裝置間通訊控制器 130 以及基地台 140。通訊設備 120 的基地台 140 透過符合本揭露實施例的網路協定（如，LTE）以與使用者裝置 UE1~UE3 進行通訊，而裝置間通訊控制器 130 則用來處理位於通訊設備 120 的通訊範圍內的裝置間通訊。於本實施例中，裝置間通訊控制器 130 架設於基地台 140 中以構成通訊設備 120 中的通訊處理裝置，而於其他實施例中，裝置間通訊控制器 130 也可以設置於管理單元 150 和/或認證單元 160 中，或是自行獨立以成爲單獨的實體組件，其實體結構的連接關係並不僅限於圖 1 的繪示。於本實施例中，通訊協定所使用的通訊處理裝置（如，基地台 140）可以是全球互通微波存取（Worldwide Interoperability for Microwave Access；WiMAX）、第三代行動通訊技術（3rd-Generation；3G）所採用的通訊基地台、WIFI 所採用的無線存取點(AP)、或是 LTE 所採用的 eNodeB 設備。使用者裝置 UE1~UE3 可以是符合本案實施例所述通訊協定之行動電話、平板電腦、筆記型電腦…等。管理單元 150 可以是 LTE 中的行動管理實體（Mobile Management Entity；MME），而認證單元 160 則可以是 LTE 中的用戶歸屬伺服器（Home Subscriber Server；HSS）。

【0016】 位於核心網路（Core network）（也就是本揭露所述的網路服務提供者）的認證伺服器 110 爲了管理整個裝置間通訊網路，必須讓每個使用者裝置 UE1~UE3 獲得裝置間通訊的授權。因此，在形成裝置間通訊網路之前，使用者裝置 UE1~UE3 一開始便需對核心網路提出通訊請求以進行裝置間通訊的授權。本揭露在使用者裝置 UE1~UE3 在進行裝置間通訊的授權時，是以 LTE 作爲本案實施例的說明案例，但應用此技術者也可透過 WIFI、CDMA 等無線網路協定來達成。再者，應用本實施例者可以在使用者裝置 UE1~UE3 在進行裝置間通訊的授權時，加入判斷使用者是否付費的相關機制，便可達到使用者付費的目的。在獲得核心網路的裝置間通訊授權之後，使用者裝置 UE1~UE3 再對認證伺服器 110 中的裝置間通訊控制器（D2D communication controller）130 進行裝置間相互通訊的認證及授權，以獲得裝置間通訊的服務。

【0017】 已認證的使用者裝置可以與鄰近並已認證的其他使用者裝置直接建立裝置間通訊，而不需要透過認證伺服器 110 以及裝置間通訊控制器 130。已認證的使用者裝置所獲得的裝置金鑰也可以依照應用本揭露的技術人員的需求而會設定裝置金鑰的使用期限，例如，已認證的使用者裝置在金鑰的使用期限內可以與特定或不特定的其他已認證使用者裝置建立裝置間通訊，並在經過金鑰的使用期限後，使用者裝置必須重新透過認證伺服器 110 來進行認證，否則裝置間通訊控制器 130 可以回收原本提供給已認證使用者裝置的網路資源。此外，認證伺服器 110 也可以協助已認

證的使用者裝置來得知鄰近已認證的其他使用者裝置，或是協助建立與鄰近使用者裝置的裝置間通訊。以下列舉多個實施例說明本揭露之裝置間通訊的認證方法的詳細內容。

【0018】 圖 2 是依照本揭露第一實施例說明裝置間通訊的認證方法的流程圖，特別是，圖 2 是單個使用者裝置 UE1 向認證伺服器 110 進行請求以獲得裝置間通訊的認證。請同時參照圖 1 及圖 2，認證伺服器 110 的通訊設備 120(也就是裝置間通訊控制器 130 以及基地台 140）應位於使用者裝置 UE1 的通訊範圍內。假設使用者裝置 UE1 希望從認證伺服器 110 中獲得裝置間通訊的認證，使用者裝置 UE1 便會發出裝置間通訊的連接請求至認證伺服器 110（步驟 S210)。當使用者裝置 UE1 發出裝置間通訊的連接請求至認證伺服器 110 的基地台 140 時，基地台 140 便將此連接請求傳送到管理單元 150 以及認證單元 160 以進行常規認證(步驟 S220)。此處所指的常規認證可參照相關網路協定所使用的認證流程，如 LTE 的認證程序。舉例來說，使用者裝置 UE1 發出的連接請求中包含國際移動用戶識別碼（International Mobile Subscriber Identity；IMSI)、服務網標誌（Server Network Identity；SN ID）和服務網類型…等信息，而認證單元 160 接收到此連接請求後便會對 SN ID、IMSI 等信息來進行身分驗證。

【0019】 當常規認證成功後，認證單元 160 便會產生對應於使用者裝置 UE1 的金鑰產生信息，並將此金鑰產生信息提供至使用者裝置 UE1（步驟 S230)。金鑰產生信息中可以包含隨機亂數、與使

用者裝置 UE1 有關的序列參數、密碼金鑰（Ciphering key；CK）、完整性金鑰（Integrity key；IK）…等信息區塊。金鑰產生信息的傳送目的是希望使用者裝置 UE1 端以及認證伺服器 110 端皆可產生相同的金鑰並進而確認已經獲得裝置間通訊的認證，因此認證伺服器 110 所產生的金鑰產生信息將等同於使用者裝置 UE1 於步驟 S230 所接收的金鑰產生信息。

【0020】 於步驟 S240 中，認證伺服器中的認證單元 160、管理單元 150 以及通訊設備 120 依據上述的金鑰產生信息以及金鑰衍生（key derivation）程序（或稱爲金鑰衍生功能（key derivation function；KDF））以產生位於認證伺服器 110 端的伺服器金鑰。在此詳述步驟 S240 中的細節步驟。當步驟 S220 的常規認證成功時，認證單元 160 便依據常規認證的結果（例如，密碼金鑰 CK 以及完整性金鑰 IK）來產生第一認證金鑰 K_{ASME1}（步驟 S242），並將此第一認證金鑰 K_{ASME1} 傳送至管理單元 150（步驟 S243）。常規認證的結果也就是上述的金鑰產生信息。管理單元 150 儲存所接收的第一認證金鑰 K_{ASME1}，並依據第一認證金鑰 K_{ASME1} 以分別產生並儲存第一通訊金鑰 K_{eNB1} 以及第一傳輸金鑰 K_{cd1} 以作爲上述的伺服器金鑰（步驟 S244），並將所述伺服器金鑰傳送至通訊設備 120 中的基地台 140（步驟 S245）。基地台 140 儲存伺服器金鑰（也就是，第一通訊金鑰 K_{eNB1} 及第一傳輸金鑰 K_{cd1}）（步驟 S246），並將第一傳輸金鑰 K_{cd1} 傳輸給裝置間通訊控制器 130（步驟 S247）。裝置間通訊控制器 130 則是儲存第一傳輸金鑰 K_{cd1}（步驟 S248），

以作爲使用者裝置 UE1 的裝置間通訊的認證紀錄。

【0021】 繼續參閱圖 2 的步驟 S250，使用者裝置 UE1 依據從步驟 S230 所獲得的金鑰產生信息以及與認證伺服器 110 相同的金鑰衍生程序來產生位於使用者裝置 UE1 的裝置金鑰，從而獲得裝置間通訊的認證。於本實施例的步驟 S252 中，使用者裝置 UE1 依據從步驟 S230 所獲得的金鑰產生信息獲得密碼金鑰 CK 以及完整性金鑰 IK，並將密碼金鑰 CK 以及完整性金鑰 IK 利用金鑰衍生程序來產生並儲存位於使用者裝置 UE1 的第二認證金鑰 K_{ASME2}。理論上，若金鑰產生信息在傳輸中並無發生錯誤的話，第二認證金鑰 K_{ASME2} 將會等同於認證伺服器 110 上的第一認證金鑰 K_{ASME1}。於步驟 S254 中，使用者裝置 UE1 依據第二認證金鑰 K_{ASME2} 並利用金鑰衍生程序來分別產生並儲存第二通訊金鑰 K_{eNB2} 以及第二傳輸金鑰 K_{cd2}，第二通訊金鑰 K_{eNB2} 以及第二傳輸金鑰 K_{cd2} 也可以稱爲是裝置金鑰。理論上，裝置金鑰相會等同於伺服器金鑰。於本實施例中，步驟 S240 及步驟 S250 可以同時執行，也可以先後執行，藉以分別在使用者裝置 UE1 端以及認證伺服器 110 端分別獲得相同的裝置金鑰及伺服器金鑰即可。

【0022】 於步驟 S260 中，使用者裝置 UE1 利用裝置金鑰以及金鑰衍生程序來產生傳輸解密金鑰 KDC_{ini} 以及傳輸加密金鑰 KDC_{enc}。相應地，步驟 S270 則是裝置間通訊控制器 130 利用裝置金鑰以及金鑰衍生程序來產生傳輸解密金鑰 KDC_{ini} 以及傳輸加密金鑰 KDC_{enc}。藉此，透過步驟 S260 及步驟 S270，使用者裝置 UE1 便

可透過上述金鑰 KDC_{ini} 及 KDC_{enc} 與認證伺服器 110 進行通訊，甚至使使用者裝置 UE1 與獲得裝置間通訊之認證的另一個使用者裝置 UE2 直接進行裝置間的相互認證以實現裝置間通訊，而不需透過認證伺服器 110。

【0023】 圖 3 是依照本揭露第二實施例說明裝置間通訊的認證方法的流程圖。圖 3 與圖 2 類似，也是單個使用者裝置 UE1 向引證伺服器 110 進行請求以獲得裝置間通訊的認證。然而，圖 3 與圖 2 不同的是，於圖 2 的步驟 S244 中，管理單元 150 會分別產生第一通訊金鑰 K_{eNB1} 以及第一傳輸金鑰 K_{cd1} 以作爲上述的伺服器金鑰。然而，於圖 3 的步驟 S344 中，管理單元 150 僅會依據第一認證金鑰 K_{ASME1} 產生並儲存基地台 140 需要的第一通訊金鑰 K_{eNB1}（步驟 S344），並將此第一通訊金鑰 K_{eNB1} 傳送給通訊設備 120 中的基地台 140（步驟 S345）。基地台 140 儲存第一通訊金鑰 K_{eNB1}，並依據第一通訊金鑰 K_{eNB1} 以產生並儲存第一傳輸金鑰 K_{cd1}（S346），然後將第一傳輸金鑰 K_{cd1} 傳輸給裝置間通訊控制器 130（步驟 S247）。第一通訊金鑰 K_{eNB1} 以及第一傳輸金鑰 K_{cd1} 合稱爲伺服器金鑰。

【0024】 類似地，圖 3 所揭示的步驟 S354 與步驟 S356 則像是圖 2 的步驟 S254 的拆解，也就是，使用者裝置 UE1 依據第二認證金鑰 K_{ASME2} 並利用金鑰衍生程序來產生並儲存第二通訊金鑰 K_{eNB2}（步驟 S354），然後，依據第二通訊金鑰 K_{eNB2} 並利用金鑰衍生程序來產生並儲存第二傳輸金鑰 K_{cd2}（步驟 S356）。

【0025】 圖 4 是依照本揭露第三實施例說明裝置間通訊的認證方法的流程圖，特別是，圖 4 是當兩個使用者裝置 UE1、UE2 向引證伺服器 110 進行請求以獲得使用者裝置 UE1、UE2 之間的裝置間通訊認證。認證伺服器 110 中的通訊設備 120 應位於使用者裝置 UE1 以及使用者裝置 UE2 的通訊範圍內。與圖 2、圖 3 相較，圖 4 增加使用者裝置 UE2。使用者裝置 UE1 對認證伺服器 110 中的認證單元 160 發出裝置間通訊連接請求（步驟 S410）。認證伺服器 110 中的認證單元 160 便對使用者裝置 UE1 進行常規認證，並提供第一金鑰產生信息至使用者裝置 UE1。相似地，使用者裝置 UE2 對認證伺服器 110 中的認證單元 160 發出裝置間通訊連接請求（步驟 S430）。認證伺服器 110 中的認證單元 160 便對使用者裝置 UE2 進行常規認證，並提供第二金鑰產生信息至使用者裝置 UE2。相關詳細內容請參閱上述實施例，在此不予贅述。

【0026】 認證伺服器 110 中的認證單元 160 和管理單元 150 其中之一便會依據上述的第一及第二金鑰產生信息以及金鑰衍生程序來產生伺服器金鑰（步驟 S440）。詳言之，認證單元 160 依據常規認證的結果（也就是，第一及第二金鑰產生信息，例如，密碼金鑰 CK 以及完整性金鑰 IK）來產生對應於使用者裝置 UE1 的第一認證金鑰 K_{ASME1} 以及對應於使用者裝置 UE2 的第二認證金鑰 K_{ASME2}（步驟 S442），並將第一及第二認證金鑰 K_{ASME1}、K_{ASME2} 傳輸至管理單元 150（步驟 S443）。管理單元 150 依據第一認證金鑰 K_{ASME1}、第二認證金鑰 K_{ASME2} 以及金鑰衍生程序來產生一組伺

服器金鑰（S444）。

【0027】 認證伺服器 110 便於步驟 S450 中將共同的伺服器金鑰進行計算以產生通訊金鑰 K_{eNB-D}，並將通訊金鑰 K_{eNB-D} 傳送給基地台 140。本案實施例可以是由認證單元 160、管理單元 150 還是基地台 140 其中之一來依據伺服器金鑰而計算產生通訊金鑰 K_{eNB-D}。並且，認證伺服器 110 也會將伺服器金鑰作爲第一及第二實施例中描述的裝置金鑰而傳送至使用者裝置 UE1（步驟 S460）以及使用者裝置 UE2（步驟 S470）中。藉此，使用者裝置 UE1、UE2 便克獲得裝置間通訊的認證，並利用步驟 S260、S270 所計算產生的傳輸解密金鑰 KDC_{ini} 以及傳輸加密金鑰 KDC_{enc} 以直接進行裝置間通訊及加解密等動作，而不需透過認證伺服器 110。

【0028】 上述第一實施例至第三實施例皆爲使用者裝置 UE1~UE3 如何獲得認證伺服器 110 對於裝置間通訊的認證。當完成對於認證伺服器 110 的裝置間通訊認證後，使用者裝置（如 UE1）不一定如上述第三實施例一般已經找尋到要進行裝置間通訊的其他使用者裝置，而通常會透過自行搜尋使用者裝置；或是透過認證伺服器來找尋鄰近的且已認證的使用者裝置之後，再進行裝置間相互認證。本案所述的「裝置搜尋」則是指已完成裝置間通訊之認證的使用者裝置（如，UE1）如何搜尋到鄰近已認證的其他使用者裝置（如，UE2），並確認使用者裝置 UE2 希望進行通訊。本案所述的「裝置間相互認證」是指已完成裝置間通訊之認證的使用者裝置（如，UE1）希望與鄰近已認證的其他使用者裝置（如，UE2）

在確認希望通訊後的相互進行識別、相互認證以及安全性金鑰的傳遞與驗證等動作。

【0029】 圖 5 是依照本揭露第四實施例說明裝置間通訊的認證方法的細節流程圖，特別是說明使用者裝置 UE1 及 UE2 之間的裝置搜尋以及裝置間相互認證。換句話說，本揭露第四實施例可以配合上述第一至第三實施例來實現。在使用者裝置 UE1 與 UE2 皆獲得裝置間通訊的認證之後，如果使用者裝置 UE1 希望對使用者裝置 UE2 進行裝置間通訊的話，使用者裝置 UE1 可對認證伺服器 110 中的裝置間通訊控制器 130 提出對使用者裝置 UE2 的裝置間通訊請求（步驟 S510）。裝置間通訊控制器 130 接收上述的裝置間通訊請求以產生裝置間主要金鑰信息（步驟 S520）。之後，裝置間通訊控制器 130 將所述裝置間主要金鑰信息分別傳送至使用者裝置 UE1（步驟 S530）及使用者裝置 UE2（步驟 S540）。

【0030】 使用者裝置 UE2 在接收所述裝置間主要金鑰信息後，便需決定是否與使用者裝置 UE1 通訊，並且回傳通訊回應至裝置間通訊控制器 130（步驟 S550）。裝置間通訊控制器 130 依據此通訊回應而決定是否同意使用者裝置 UE1、UE2 之間的裝置間通訊。當使用者裝置 UE2 的通訊回應中同意與使用者裝置 UE1 通訊時，裝置間通訊控制器 130 便會通知使用者裝置 UE1 而完成「裝置搜尋」，以讓使用者裝置 UE1、UE2 進行裝置間相互認證（步驟 S560），並在裝置間相互認證成功後進行直接地裝置間通訊（步驟 S580）。

【0031】 於本實施例中，對於使用者裝置 UE1 的裝置間主要金鑰信息主要包括主要金鑰 MK（例如，上述的第一傳輸金鑰 K_{cd1}）及金鑰有效信息 Nonce。金鑰有效信息 Nonce 用以決定此第一傳輸金鑰 K_{cd1} 的使用期限。例如，若認證伺服器 110 提供使用者裝置 UE1 可以使用一個月的裝置間通訊的話，則金鑰有效信息 Nonce 則乘載了「一個月」的信息。

【0032】 在此詳細說明圖 5 的步驟 S560，也就是本揭露所示的「裝置間相互認證」。當使用者裝置 UE2 的通訊回應中同意與使用者裝置 UE1 通訊時（步驟 S550），則進行裝置間相互認證。本揭露所採用的「裝置間相互認證」概略說明如下：第一使用者裝置 UE1 產生第一隨機值 R1 並依據裝置間主要金鑰信息的主要金鑰 MK 以產生第一暫時金鑰 TK1。相應的，第二使用者裝置 UE2 則產生第二隨機值 R2 並依據裝置間主要金鑰信息的主要金鑰 MK 計算第二暫時金鑰 TK2。接著，第一使用者裝置 UE1 以及第二使用者裝置 UE2 相互傳送第一暫時金鑰 TK1 以及第二暫時金鑰 TK2，並依據裝置間要金鑰組的主要金鑰 MK、第一暫時金鑰 TK1 以及第二暫時金鑰 TK2 來相互認證，以使第一使用者裝置 UE1 與第二使用者裝置 UE2 來允許依據裝置間主要金鑰信息進行裝置間通訊的加解密操作。

【0033】 「裝置間相互認證」的詳細步驟流程則如下所述。於步驟 S561 中，使用者裝置 UE1 產生第一隨機值 R1，且依據裝置間主要金鑰信息的主要金鑰 MK 以產生第一暫時金鑰 TK1（步驟

S561)。之後，使用者裝置 UE1 將第一隨機值 R1 送至使用者裝置 UE2（步驟 S562)。使用者裝置 UE2 產生第二隨機值 R2 並依據裝置間主要金鑰信息的主要金鑰 MK 來計算第二暫時金鑰 TK2（步驟 S563)。使用者裝置 UE2 依據所述第二暫時金鑰 TK2 及第一隨機值 R1 以藉由金鑰衍生程序來計算第一中介值 V1(步驟 S564)，並且使用者裝置 UE2 將第一中介值 V1 與第二隨機值 R2 送至使用者裝置 UE1（步驟 S565)。

【0034】 使用者裝置 UE1 在接收第一中介值 V1 與第二隨機值 R2 之後，則依據自身計算出的第一暫時金鑰 TK1 以及第一隨機值 R2 以計算第二中介值 V2，並且判斷所述第一中介值 V1 與第二中介值 V2 是否相同（步驟 S566)。若第一中介值 V1 及第二中介值 V2 相同時，使用者裝置 UE1 便依據第一暫時金鑰 TK1 及第二隨機值 R2 來計算第三中介值 V3（步驟 S567)，並將第三中介值 V3 傳送至使用者裝置 UE2（步驟 S568)。

【0035】 使用者裝置 UE2 在接收到第三中介值 V3 之後，便依據第二暫時金鑰 TK2 及第二隨機值 R2 以計算第四中介值 V4，並判斷第三中介值 V3 與第四中介值 V4 是否相同（步驟 S569)。若第三中介值 V3 與第四中介值 V4 相同時，則使用者裝置 UE2 便允許該使用者裝置 UE1 依據裝置間主要金鑰信息進行裝置間通訊，以及通訊時的加解密操作(步驟 S570)。由上述可知，裝置間相互認證（步驟 S560）以及後續的裝置間通訊（步驟 S580）並不需要透過裝置間通訊控制器 130。

【0036】 第四實施例的圖 5 是使用者裝置 UE1、UE2 皆可以與裝置間通訊控制器 130 進行通訊時的情況，而下述第五實施例的圖 6 則是使用者裝置 UE1 可以與裝置間通訊控制器 130 以及使用者裝置 UE2 進行通訊，但使用者裝置 UE2 無法與裝置間通訊控制器 130 進行通訊且沒有具備裝置間主要金鑰信息的情況。圖 6 是依照本揭露第五實施例說明裝置間通訊的認證方法的細節流程圖。本揭露第五實施例可以同樣可配合上述第一至第三實施例來實現。在使用者裝置 UE1 與 UE2 皆獲得裝置間通訊的認證之後，由於使用者裝置 UE2 並未具有裝置間主要金鑰信息，因此使用者裝置 UE1 可對裝置間通訊控制器 130 提出對使用者裝置 UE2 的裝置間通訊請求（步驟 S510），並且裝置間通訊控制器 130 接收上述的裝置間通訊請求以產生裝置間主要金鑰信息（步驟 S520）之後，裝置間通訊控制器 130 將所述裝置間主要金鑰信息傳送至使用者裝置 UE1（步驟 S630），而無法傳送至使用者裝置 UE2。

【0037】 之後，便進行使用者裝置 UE1、UE2 的裝置間相互認證（步驟 S640）。概略而言，第一使用者裝置 UE1 接收裝置間主要金鑰信息但第二使用者裝置 UE2 並未具有裝置間主要金鑰信息時，第一使用者裝置 UE1 則產生第一隨機值 R1，並將第一隨機值 R1 以及裝置間主要金鑰信息的主要金鑰 MK 傳送到第二使用者裝置 UE2。第二使用者裝置 UE2 產生第二隨機值 R2 並傳送到第一使用者裝置 UE1。第一使用者裝置 UE1 以及第二使用者裝置 UE2 便依據裝置間主要金鑰信息的主要金鑰 MK、第一隨機值 R1 以及

第二隨機值 R2 來相互認證，以使第一使用者裝置 UE1 與第二使用者裝置 UE2 允許依據裝置間主要金鑰信息進行裝置間通訊的加解密操作

【0038】 詳細來說，請參閱圖 6 中的相關步驟 S641~S650，使用者裝置 UE1 產生第一隨機值 R1（步驟 S641），並將第一隨機值 R1 以及裝置間主要金鑰信息的主要金鑰 MK 傳送到使用者裝置 UE2（步驟 S642）。接收到第一隨機值 R1 以及主要金鑰 MK 之後，使用者裝置 UE2 產生第二隨機值 R2，並依據第一隨機值 R1 以及主要金鑰 MK 來計算第一中介值 V1（步驟 S643）。然後，使用者裝置 UE2 將第一中介值 V1 與第二隨機值 R2 傳送至使用者裝置 UE1（步驟 S644）。

【0039】 接收第一中介值 V1 與第二隨機值 R2 之後，使用者裝置 UE1 依據第一隨機值 R1 以及主要金鑰 MK 以計算第二中介值 V2，並判斷第一中介值 V1 與第二中介值 V2 是否相同（步驟 S645）。若第一中介值 V1 與第二中介值 V2 相同時，使用者裝置 UE1 依據第二隨機值 R2 以及主要金鑰 MK 以計算第三中介值 V3（步驟 S646），並將第三中介值 V3 傳送至使用者裝置 UE2（步驟 S647）。

【0040】 在接收第三中介值 V3 之後，使用者裝置 UE2 依據第二隨機值 R2 以及主要金鑰 MK 以計算第四中介值 V4，並判斷第三中介值 V3 與第四中介值 V4 是否相同（步驟 S648）。若第三中介值 V3 與第四中介值 V4 相同時，則使用者裝置 UE2 允許使用者裝

置 UE1 依據裝置間主要金鑰信息以進行裝置間通訊的加解密操作（步驟 S650），並在裝置間相互認證成功後讓使用者裝置 UE1、UE2 進行直接地裝置間通訊（步驟 S580）。

【0041】 圖 7 是依照本揭露第六實施例說明裝置間通訊的認證方法的細節流程圖，特別是說明使用者裝置 UE1 及 UE2 之間的裝置搜尋以及裝置間相互認證。類似於第三實施例，在使用者裝置 UE1、UE2 皆獲得裝置間通訊的認證之後，使用者裝置 UE1、UE2 先奏對認證伺服器 110 中的裝置間通訊控制器 110 提出相互的裝置間通訊請求（步驟 SS710、S720）。裝置間通訊控制器 130 接收這兩個裝置間通訊請求以產生符合使用者裝置 UE1、UE2 的裝置間主要金鑰信息（步驟 S730），並將裝置間主要金鑰信息分別傳送至使用者裝置 UE1（步驟 S740）及使用者裝置 UE2（步驟 S750），以達成裝置搜尋，並進行後續的裝置間相互認證。特別說明的是，圖 7 的裝置間相互認證與上述第四實施例及圖 5 中揭示的步驟 S560~S580 相同，在此不予贅述。

【0042】 再者，請參照圖 7，如果使用者裝置 UE1、UE2 已經先行具備各自的裝置間主要金鑰信息的話，便可不需要進行「裝置搜尋」的步驟（如步驟 S710~S750，而可以直接進入步驟 S560~S580 以進行「裝置間相互認證」以及「裝置間通訊」。「裝置間相互認證」可如圖 5 的步驟 S560 可參閱詳細描述，在此概略說明如下。第一使用者裝置 UE1 產生第一隨機值 R1 並依據裝置間主要金鑰信息的主要金鑰 MK 以產生第一暫時金鑰 TK1。相應的，第二使

用者裝置 UE2 則產生第二隨機值 R2 並依據裝置間主要金鑰信息的主要金鑰 MK 計算第二暫時金鑰 TK2。接著，第一使用者裝置 UE1 以及第二使用者裝置 UE2 相互傳送第一暫時金鑰 TK1 以及第二暫時金鑰 TK2，並依據裝置間要金鑰組的主要金鑰 MK、第一暫時金鑰 TK1 以及第二暫時金鑰 TK2 來相互認證，以使第一使用者裝置 UE1 與第二使用者裝置 UE2 來允許依據裝置間主要金鑰信息進行裝置間通訊的加解密操作。

【0043】 特別說明的是，裝置間主要金鑰信息除了主要金鑰 MK 以及金鑰有效信息 Nonce 以外，還可以包括參數：金鑰索引（index）。金鑰索引是使用來通知使用者裝置 UE1、U2 來進行金鑰分配及金鑰更新所使用的。使用者裝置 UE1 或 UE2 可以藉由相互告知金鑰索引來重新產生裝置間通訊中所需的加密金鑰（Encryption key；EK）以及完整性金鑰（IK），並且讓使用者裝置 UE1、UE2 採用新產生的加密金鑰以及完整性金鑰來進行裝置間通訊。

【0044】 在此利用圖 8 來說明使用者裝置 UE1、UE2 之間如何進行金鑰更新。圖 8 是依照本揭露第七實施例說明裝置間通訊的認證方法的細節流程圖，且第七實施例可同時適用於上述第一至第六實施例。使用者裝置 UE1 可能因爲計數器、使用者請求等情況而觸發並執行金鑰更新事件（步驟 S810）。於步驟 S820 中，使用者裝置 UE1 對使用者裝置 UE2 皆提出金鑰索引更新請求，以使將裝置間主要金鑰信息中的金鑰索引（index）增加一預定值 N（步

驟 S820)。之後，使用者裝置 UE2 便會回傳一個金鑰索引更新回應（步驟 S830)。藉此，使用者裝置 UE1、UE2 便會分別依據裝置間主要金鑰信息中增加後的金鑰索引（也就是 index+N）來重新產生裝置間通訊中所需的加密金鑰 EK 以及完整性金鑰 IK（步驟 S840、S850)。使用者裝置 UE1 及 UE2 將會採用新產生的加密金鑰以及完整性金鑰來進行裝置間通訊（步驟 S860)。

【0045】 綜上所述，本揭露實施例中的認證系統及認證方法實現了裝置間通訊的認證機制，使用者裝置可以先行通過認證伺服器來進行裝置間通訊的認證並獲得相應的認證金鑰，並在獲得裝置間通訊的認證後與其他已獲得認證的其他使用者裝置進行直接通訊，而不需再次通過基地台或是無線存取點來進行通訊。透過本揭露所認證的使用者裝置可以依照認證金鑰內部設定的金鑰有效信息來與其他使用者裝置進行裝置間的相互認證（mutual authentication)、裝置間通訊機制、金鑰分配（key distribution）以及金鑰更新，並可於裝置間認證的判定中加入收費及安全機制，藉以保障實現此裝置間通訊系統的廠商利益及使用此裝置間通訊系統的使用者權益。

【0046】 雖然本發明已以實施例揭露如上，然其並非用以限定本發明，任何所屬技術領域中具有通常知識者，在不脫離本發明的精神和範圍內，當可作些許的更動與潤飾，故本發明的保護範圍當視後附的申請專利範圍所界定者爲準。

【符號說明】

【0047】

100：認證系統

110：認證伺服器

120：通訊設備

130：裝置間通訊控制器

140：基地台

150：管理單元

160：認證單元

UE1~UE3：使用者裝置

S210~S860：步驟

104年 07月 02日 修正替換頁

申請專利範圍

1. 一種裝置間通訊的認證系統，包括：

第一使用者裝置；

認證伺服器，位於該第一使用者裝置的通訊範圍內，其中該認證伺服器包括：

通訊設備，透過網路協定以與該第一使用者裝置進行通訊，並處理位於該通訊設備的通訊範圍內的裝置間通訊；以及

管理單元以及認證單元，當該管理單元及該認證單元透過該通訊設備接收該第一使用者裝置發出的該連接請求後，該認證單元對該第一使用者裝置進行常規認證，

當常規認證成功時，該認證單元依據常規認證結果產生第一認證金鑰（authentication key）並將該第一認證金鑰傳送至該管理單元，該管理單元依據該第一認證金鑰分別產生第一通訊金鑰以及第一傳輸金鑰（transmission key）以作為該伺服器金鑰，並將該伺服器金鑰（server key）傳送並儲存至該通訊設備；

其中，當該第一使用者裝置發出連接請求至該認證伺服器時，該認證伺服器對該第一使用者裝置進行常規認證並提供金鑰產生信息至該第一使用者裝置，

該認證伺服器依據該金鑰產生信息以及金鑰衍生（key derivation）程序以產生伺服器金鑰，以及

該第一使用者裝置依據該金鑰產生信息以及該金鑰衍生程序產生裝置金鑰，以獲得裝置間通訊的認證，使該第一使用者裝置與獲得裝置間通訊的認證的第二使用者裝置直接進行裝置間通訊，而不需透過該認證伺服器。

2. 如申請專利範圍第1項所述的系統，其中該通訊設備包括：

通訊處理裝置，透過網路協定以與該第一使用者裝置進行通訊；以及

裝置間通訊控制器，處理位於該通訊設備的通訊範圍內的裝置間通訊。

3. 如申請專利範圍第1項所述的系統，在該第一使用者裝置獲得裝置間通訊的認證之後，該第一使用者裝置對該認證伺服器中的裝置間通訊控制器提出對該第二使用者裝置的裝置間通訊請求，該裝置間通訊控制器接收該裝置間通訊請求以產生裝置間主要金鑰信息（master key information），並將該裝置間主要金鑰信息分別傳送至該第一使用者裝置及該第二使用者裝置，以使該第一使用者裝置及該第二使用者裝置進行裝置間相互認證以及裝置間通訊。

4. 如申請專利範圍第3項所述的系統，該第二使用者裝置在接收該裝置間主要金鑰信息後，決定是否與該第一使用者裝置通訊，並回傳通訊回應至該裝置間通訊控制器，該裝置間通訊控制器依據該通訊回應而決定是否同意該第一使用者裝置及該第二使用者裝置之間的裝置間通訊。

5. 如申請專利範圍第 4 項所述的系統，當該第二使用者裝置的該通訊回應中同意與第一使用者裝置通訊時則進行該裝置間相互認證，

其中該第一使用者裝置產生第一隨機值並依據該裝置間主要金鑰信息的主要金鑰以產生第一暫時金鑰（temporary key），第二使用者裝置產生第二隨機值並依據該裝置間主要金鑰信息的該主要金鑰計算第二暫時金鑰，該第一使用者裝置以及該第二使用者裝置相互傳送該第一暫時金鑰以及該第二暫時金鑰，並依據該裝置間主要金鑰信息的主要金鑰、該第一暫時金鑰以及該第二暫時金鑰來相互認證，以使該第一使用者裝置與該第二使用者裝置允許依據該裝置間主要金鑰信息進行裝置間通訊的加解密操作。

6. 如申請專利範圍第 5 項所述的系統，其中該第一使用者裝置產生第一隨機值並依據該裝置間主要金鑰信息的主要金鑰以產生第一暫時金鑰（temporary key），並將該第一隨機值送至該第二使用者裝置；

該第二使用者裝置產生第二隨機值並依據該裝置間主要金鑰信息的該主要金鑰計算第二暫時金鑰；

該第二使用者裝置依據該第二暫時金鑰及該第一隨機值以計算第一中介值（intermediary value），並將該第一中介值與該第二隨機值傳送至該第一使用者裝置；

該第一使用者裝置依據該第一暫時金鑰以及該第一隨機值以計算第二中介值，並判斷該第一中介值與該第二中介值是否相同；

若該第一及該第二中介值相同時，該第一使用者裝置依據該第一暫時金鑰及該第二隨機值以計算第三中介值，並將該第三中介值傳送至該第二使用者裝置；

該第二使用者裝置依據該第二暫時金鑰及該第二隨機值以計算第四中介值，並判斷該第三中介值與該第四中介值是否相同；以及

若第三中介值與該第四中介值相同時，則該第二使用者裝置允許該第一使用者裝置依據該裝置間主要金鑰信息進行裝置間通訊的加解密操作。

7. 如申請專利範圍第 3 項所述的系統，其中該裝置間相互認證為，當該第一使用者裝置接收該裝置間主要金鑰信息但該第二使用者裝置並未具有該裝置間主要金鑰信息時，該第一使用者裝置產生第一隨機值，並將該第一隨機值以及該裝置間主要金鑰信息的主要金鑰傳送到該第二使用者裝置；該第二使用者裝置產生該第二隨機值並傳送到該第一使用者裝置，該第一使用者裝置以及該第二使用者裝置依據該裝置間主要金鑰信息的主要金鑰、該第一隨機值以及該第二隨機值來相互認證，以使該第一使用者裝置與該第二使用者裝置允許依據該裝置間主要金鑰信息進行裝置間通訊的加解密操作。

8. 如申請專利範圍第 7 項所述的系統，其中該第一使用者裝置產生第一隨機值，並將該第一隨機值以及該裝置間主要金鑰信息的主要金鑰傳送到該第二使用者裝置；

該第二使用者裝置產生該第二隨機值，依據該第一隨機值以及該主要金鑰計算第一中介值，並將該第一中介值與該第二隨機值傳送至該第一使用者裝置；

該第一使用者裝置依據該第一隨機值以及該主要金鑰以計算第二中介值，並判斷該第一中介值與該第二中介值是否相同；

若該第一中介值與該第二中介值相同時，該第一使用者裝置依據該第二隨機值以及該主要金鑰以計算第三中介值，並將該第三中介值傳送至該第二使用者裝置；

該第二使用者裝置依據該第二隨機值以及該主要金鑰以計算第四中介值，並判斷該第三中介值與該第四中介值是否相同；以及

若該第三中介值與該第四中介值相同時，則該第二使用者裝置允許該第一使用者裝置依據該裝置間主要金鑰信息以進行裝置間通訊的加解密操作。

並依據該裝置間主要金鑰信息的主要金鑰以產生第一暫時金鑰，並將該第一隨機值傳送至該第二使用者裝置；

該第二使用者裝置產生第二隨機值並依據該裝置間主要金鑰信息的該主要金鑰計算一第二暫時金鑰；

該第二使用者裝置依據該第二暫時金鑰及該第一隨機值以計算第一中介值，並將該第一中介值與該第二隨機值送至該第一使用者裝置；

該第一使用者裝置依據該第一暫時金鑰以及該第一隨機值以

計算第二中介值，並判斷該第一中介值與該第二中介值是否相同；

若該第一及該第二中介值相同時，該第一使用者裝置依據該第一暫時金鑰及該第二隨機值以計算第三中介值，並將該第三中介值傳送至該第二使用者裝置；

該第二使用者裝置依據該第二暫時金鑰及該第二隨機值以計算第四中介值，並判斷該第三中介值與該第四中介值是否相同；以及

若第三中介值與該第四中介值相同時，則該第二使用者裝置允許該第一使用者裝置依據該主要金鑰進行裝置間通訊的加解密操作。

9. 如申請專利範圍第 1 項所述的系統，在該第一使用者裝置獲得裝置間通訊的認證之後，該第一使用者裝置與該第二使用者裝置對該認證伺服器中的裝置間通訊控制器提出相互的裝置間通訊請求，該裝置間通訊控制器接收該裝置間通訊請求以產生裝置間主要金鑰信息，並將該裝置間主要金鑰信息分別傳送至該第一使用者裝置及該第二使用者裝置，以使該第一使用者裝置及該第二使用者裝置進行裝置間相互認證以及裝置間通訊。

10. 如申請專利範圍第 9 項所述的系統，其中該裝置間相互認證為，該第一使用者裝置產生第一隨機值並依據該裝置間主要金鑰信息的主要金鑰以產生第一暫時金鑰，第二使用者裝置產生第二隨機值並依據該裝置間主要金鑰信息的該主要金鑰計算第二暫時金鑰，該第一使用者裝置以及該第二使用者裝置相互傳送該

第一暫時金鑰以及該第二暫時金鑰，並依據該裝置間主要金鑰信息的主要金鑰、該第一暫時金鑰以及該第二暫時金鑰來相互認證，以使該第一使用者裝置與該第二使用者裝置允許依據該裝置間主要金鑰信息進行裝置間通訊的加解密操作。

11. 如申請專利範圍第 10 項所述的系統，其中該第一使用者裝置產生第一隨機值並依據該裝置間主要金鑰信息的主要金鑰以產生第一暫時金鑰，並將該第一隨機值送至該第二使用者裝置；

該第二使用者裝置產生第二隨機值並依據該裝置間主要金鑰信息的該主要金鑰計算一第二暫時金鑰；

該第二使用者裝置依據該第二暫時金鑰及該第一隨機值以計算第一中介值，並將該第一中介值與該第二隨機值送至該第一使用者裝置；

該第一使用者裝置依據該第一暫時金鑰以及該第一隨機值以計算第二中介值，並判斷該第一中介值與該第二中介值是否相同；

若該第一及該第二中介值相同時，該第一使用者裝置依據該第一暫時金鑰及該第二隨機值以計算第三中介值，並將該第三中介值傳送至該第二使用者裝置；

該第二使用者裝置依據該第二暫時金鑰及該第二隨機值以計算第四中介值，並判斷該第三中介值與該第四中介值是否相同；

若第三中介值與該第四中介值相同時，則該第二使用者裝置允許該第一使用者裝置依據該裝置間主要金鑰信息進行裝置間通訊的加解密操作。

12. 如申請專利範圍第 1 項所述的系統，其中該第一使用者裝置以及該第二使用者裝置在皆具有裝置間主要金鑰信息後進行該裝置間相互認證，該第一使用者裝置產生第一隨機值並依據該裝置間主要金鑰信息的主要金鑰以產生第一暫時金鑰，第二使用者裝置產生第二隨機值並依據該裝置間主要金鑰信息的該主要金鑰計算第二暫時金鑰，該第一使用者裝置以及該第二使用者裝置相互傳送該第一暫時金鑰以及該第二暫時金鑰，並依據該裝置間主要金鑰信息的主要金鑰、該第一暫時金鑰以及該第二暫時金鑰來相互認證，以使該第一使用者裝置與該第二使用者裝置允許依據該裝置間主要金鑰信息進行裝置間通訊的加解密操作。

13. 如申請專利範圍第 1 項所述的系統，其中該第一使用者裝置及該第二使用者裝置進行裝置間通訊時，依據該裝置間主要金鑰信息中的金鑰索引（index）來重新產生裝置間通訊中所需的加密金鑰（Encryption key；EK）以及完整性金鑰（Integrity key；IK），並且第一使用者裝置及該第二使用者裝置採用新產生的加密金鑰以及完整性金鑰來進行裝置間通訊。

14. 如申請專利範圍第 1 項所述的系統，其中該第一使用者裝置及該第二使用者裝置進行裝置間通訊時，該第一使用者裝置執行金鑰更新事件，對該第二使用者裝置提出金鑰索引更新請求，以使將該裝置間主要金鑰信息中的該金鑰索引增加一預定值，該第一使用者裝置及該第二使用者裝置依據該裝置間主要金鑰信息中增加後的金鑰索引來重新產生裝置間通訊中所需的加密

金鑰以及完整性金鑰，並且第一使用者裝置及該第二使用者裝置採用新產生的加密金鑰以及完整性金鑰來進行裝置間通訊。

15. 一種裝置間通訊認證系統，包括：

第一使用者裝置以及第二使用者裝置；以及

認證伺服器，位於該第一使用者裝置以及該第二使用者裝置的通訊範圍內，其中該認證伺服器包括：

通訊設備，透過網路協定以與該第一使用者裝置進行通訊並處理位於該通訊設備的通訊範圍內的裝置間通訊；以及

管理單元以及認證單元，當該管理單元及該認證單元透過該通訊設備接收該第一使用者裝置發出的該連接請求後，該認證單元對該第一使用者裝置進行常規認證，

當常規認證成功時，該認證單元依據常規認證結果產生第一認證金鑰並將該第一認證金鑰傳送至該管理單元，該管理單元依據該第一認證金鑰分別產生第一通訊金鑰以及第一傳輸金鑰以作為該伺服器金鑰，並將該伺服器金鑰傳送並儲存至該通訊設備；

其中，當該第一使用者裝置及該第二使用者裝置分別發出裝置間通訊連接請求至該認證伺服器時，該認證伺服器對該第一及該第二使用者裝置進行常規認證並分別提供第一金鑰產生信息及第二金鑰產生信息至該第一及該第二使用者裝置，

該認證伺服器依據該第一及第二金鑰產生信息以及金鑰衍生程序以產生伺服器金鑰，以及

該認證伺服器將該伺服器金鑰分別傳送至該第一及該第二使用者裝置，以使該第一及該第二使用者裝置獲得裝置間通訊的認證並直接進行裝置間通訊，而不需透過該認證伺服器。

16. 如申請專利範圍第 15 項所述的系統，其中當該第一使用者裝置發出連接請求至該認證伺服器時，該認證伺服器對該第一使用者裝置進行常規認證並提供金鑰產生信息至該第一使用者裝置該認證伺服器依據該金鑰產生信息以及金鑰衍生程序以產生伺服器金鑰，以及，該第一使用者裝置依據該金鑰產生信息以及該金鑰衍生程序產生裝置金鑰，以獲得裝置間通訊的認證，使該第一使用者裝置與獲得裝置間通訊的認證的第二使用者裝置直接進行裝置間通訊，而不需透過該認證伺服器。

17. 如申請專利範圍第 16 項所述的系統，其中該通訊設備包括：

通訊處理裝置，透過網路協定以與該第一使用者裝置進行通訊；以及

裝置間通訊控制器，處理位於該通訊設備的通訊範圍內的裝置間通訊。

18. 如申請專利範圍第 15 項所述的系統，在該第一使用者裝置獲得裝置間通訊的認證之後，該第一使用者裝置對該認證伺服器中的裝置間通訊控制器提出對該第二使用者裝置的裝置間通訊請求，該裝置間通訊控制器接收該裝置間通訊請求以產生裝置間主要金鑰信息，並將該裝置間主要金鑰信息分別傳送至該第一使

用者裝置及該第二使用者裝置，以使該第一使用者裝置及該第二使用者裝置進行裝置間相互認證以及裝置間通訊。

19. 如申請專利範圍第 18 項所述的系統，該第二使用者裝置在接收該裝置間主要金鑰信息後，決定是否與該第一使用者裝置通訊，並回傳通訊回應至該裝置間通訊控制器，該裝置間通訊控制器依據該通訊回應而決定是否同意該第一使用者裝置及該第二使用者裝置之間的裝置間通訊。

20. 如申請專利範圍第 19 項所述的系統，當該第二使用者裝置的該通訊回應中同意與第一使用者裝置通訊時則進行該裝置間相互認證，

其中該第一使用者裝置產生第一隨機值並依據該裝置間主要金鑰信息的主要金鑰以產生第一暫時金鑰（temporary key），第二使用者裝置產生第二隨機值並依據該裝置間主要金鑰信息的該主要金鑰計算第二暫時金鑰，該第一使用者裝置以及該第二使用者裝置相互傳送該第一暫時金鑰以及該第二暫時金鑰，並依據該裝置間主要金鑰信息的主要金鑰、該第一暫時金鑰以及該第二暫時金鑰來相互認證，以使該第一使用者裝置與該第二使用者裝置允許依據該裝置間主要金鑰信息進行裝置間通訊的加解密操作。

21. 如申請專利範圍第 20 項所述的系統，其中該第一使用者裝置產生第一隨機值並依據該裝置間主要金鑰信息的主要金鑰以產生第一暫時金鑰，並將該第一隨機值送至該第二使用者裝置；

該第二使用者裝置產生第二隨機值並依據該裝置間主要金鑰

信息的該主要金鑰計算一第二暫時金鑰；

該第二使用者裝置依據該第二暫時金鑰及該第一隨機值以計算第一中介值，並將該第一中介值與該第二隨機值送至該第一使用者裝置；

該第一使用者裝置依據該第一暫時金鑰以及該第一隨機值以計算第二中介值，並判斷該第一中介值與該第二中介值是否相同；

若該第一及該第二中介值相同時，該第一使用者裝置依據該第一暫時金鑰及該第二隨機值以計算第三中介值，並將該第三中介值傳送至該第二使用者裝置；

該第二使用者裝置依據該第二暫時金鑰及該第二隨機值以計算第四中介值，並判斷該第三中介值與該第四中介值是否相同；以及

若第三中介值與該第四中介值相同時，則該第二使用者裝置允許該第一使用者裝置依據該裝置間主要金鑰信息進行裝置間通訊的加解密操作。

22. 如申請專利範圍第 18 項所述的系統，其中該裝置間相互認證為，當該第一使用者裝置接收該裝置間主要金鑰信息但該第二使用者裝置並未具有該裝置間主要金鑰信息時，該第一使用者裝置產生第一隨機值，並將該第一隨機值以及該裝置間主要金鑰信息的主要金鑰傳送到該第二使用者裝置；該第二使用者裝置產生該第二隨機值並傳送到該第一使用者裝置，該第一使用者裝置以及該第二使用者裝置依據該裝置間主要金鑰信息的主要金鑰、

該第一隨機值以及該第二隨機值來相互認證，以使該第一使用者裝置與該第二使用者裝置允許依據該裝置間主要金鑰信息進行裝置間通訊的加解密操作。

23. 如申請專利範圍第 22 項所述的系統，其中該第一使用者裝置產生第一隨機值，並將該第一隨機值以及該裝置間主要金鑰信息的主要金鑰傳送到該第二使用者裝置；

該第二使用者裝置產生該第二隨機值，依據該第一隨機值以及該主要金鑰計算第一中介值，並將該第一中介值與該第二隨機值傳送至該第一使用者裝置；

該第一使用者裝置依據該第一隨機值以及該主要金鑰以計算第二中介值，並判斷該第一中介值與該第二中介值是否相同；

若該第一中介值與該第二中介值相同時，該第一使用者裝置依據該第二隨機值以及該主要金鑰以計算第三中介值，並將該第三中介值傳送至該第二使用者裝置；

該第二使用者裝置依據該第二隨機值以及該主要金鑰以計算第四中介值，並判斷該第三中介值與該第四中介值是否相同；以及

若該第三中介值與該第四中介值相同時，則該第二使用者裝置允許該第一使用者裝置依據該裝置間主要金鑰信息以進行裝置間通訊的加解密操作。

並依據該裝置間主要金鑰信息的主要金鑰以產生第一暫時金鑰，並將該第一隨機值傳送至該第二使用者裝置；

該第二使用者裝置產生第二隨機值並依據該裝置間主要金鑰信息的該主要金鑰計算一第二暫時金鑰；

該第二使用者裝置依據該第二暫時金鑰及該第一隨機值以計算第一中介值，並將該第一中介值與該第二隨機值送至該第一使用者裝置；

該第一使用者裝置依據該第一暫時金鑰以及該第一隨機值以計算第二中介值，並判斷該第一中介值與該第二中介值是否相同；

若該第一及該第二中介值相同時，該第一使用者裝置依據該第一暫時金鑰及該第二隨機值以計算第三中介值，並將該第三中介值傳送至該第二使用者裝置；

該第二使用者裝置依據該第二暫時金鑰及該第二隨機值以計算第四中介值，並判斷該第三中介值與該第四中介值是否相同；以及

若第三中介值與該第四中介值相同時，則該第二使用者裝置允許該第一使用者裝置依據該主要金鑰進行裝置間通訊的加解密操作。

24. 如申請專利範圍第 15 項所述的系統，在該第一使用者裝置獲得裝置間通訊的認證之後，該第一使用者裝置與該第二使用者裝置對該認證伺服器中的裝置間通訊控制器提出相互的裝置間通訊請求，該裝置間通訊控制器接收該裝置間通訊請求以產生裝置間主要金鑰信息，並將該裝置間主要金鑰信息分別傳送至該第一使用者裝置及該第二使用者裝置，以使該第一使用者裝置及該

第二使用者裝置進行裝置間相互認證以及裝置間通訊。

25. 如申請專利範圍第 24 項所述的系統，其中該裝置間相互認證為，該第一使用者裝置產生第一隨機值並依據該裝置間主要金鑰信息的主要金鑰以產生第一暫時金鑰，第二使用者裝置產生第二隨機值並依據該裝置間主要金鑰信息的該主要金鑰計算第二暫時金鑰，該第一使用者裝置以及該第二使用者裝置相互傳送該第一暫時金鑰以及該第二暫時金鑰，並依據該裝置間主要金鑰信息的主要金鑰、該第一暫時金鑰以及該第二暫時金鑰來相互認證，以使該第一使用者裝置與該第二使用者裝置允許依據該裝置間主要金鑰信息進行裝置間通訊的加解密操作。

26. 如申請專利範圍第 15 項所述的系統，其中該第一使用者裝置以及該第二使用者裝置在皆具有裝置間主要金鑰信息後進行該裝置間相互認證，該第一使用者裝置產生第一隨機值並依據該裝置間主要金鑰信息的主要金鑰以產生第一暫時金鑰，第二使用者裝置產生第二隨機值並依據該裝置間主要金鑰信息的該主要金鑰計算第二暫時金鑰，該第一使用者裝置以及該第二使用者裝置相互傳送該第一暫時金鑰以及該第二暫時金鑰，並依據該裝置間主要金鑰信息的主要金鑰、該第一暫時金鑰以及該第二暫時金鑰來相互認證，以使該第一使用者裝置與該第二使用者裝置允許依據該裝置間主要金鑰信息進行裝置間通訊的加解密操作。

27. 如申請專利範圍第 15 項所述的系統，其中該第一使用者裝置及該第二使用者裝置進行裝置間通訊時，依據該裝置間主要

金鑰信息中的金鑰索引（index）來重新產生裝置間通訊中所需的加密金鑰（Encryption key；EK）以及完整性金鑰（Integrity key；IK），並且第一使用者裝置及該第二使用者裝置採用新產生的加密金鑰以及完整性金鑰來進行裝置間通訊。

28. 如申請專利範圍第 15 項所述的系統，其中該第一使用者裝置及該第二使用者裝置進行裝置間通訊時，該第一使用者裝置執行金鑰更新事件，對該第二使用者裝置提出金鑰索引更新請求，以使將該裝置間主要金鑰信息中的該金鑰索引增加一預定值，該第一使用者裝置及該第二使用者裝置依據該裝置間主要金鑰信息中增加後的金鑰索引來重新產生裝置間通訊中所需的加密金鑰以及完整性金鑰，並且第一使用者裝置及該第二使用者裝置採用新產生的加密金鑰以及完整性金鑰來進行裝置間通訊。

29. 一種裝置間通訊及認證方法，適用於該通訊系統中的第一使用者裝置，其中該通訊系統還包括認證伺服器以及第二使用者裝置，該認證方法包括：

發出連接請求至該認證伺服器；

該認證伺服器對該第一使用者裝置進行常規認證並提供金鑰產生信息，且該認證伺服器依據該金鑰產生信息以及金鑰衍生程序以產生伺服器金鑰；以及

依據該金鑰產生信息以及該金鑰衍生程序產生裝置金鑰，以獲得裝置間通訊的認證，使該第一使用者裝置與獲得裝置間通訊的認證的第二使用者裝置直接進行裝置間通訊，而不需透過該認

證伺服器，其中該認證伺服器包括：

通訊設備，透過網路協定以與該第一使用者裝置進行通訊並處理位於該通訊設備的通訊範圍內的裝置間通訊；以及

管理單元以及認證單元，當該管理單元及該認證單元透過該通訊設備接收該第一使用者裝置發出的該連接請求後，該認證單元對該第一使用者裝置進行常規認證，

當常規認證成功時，該認證單元依據常規認證結果產生第一認證金鑰並將該第一認證金鑰傳送至該管理單元，該管理單元依據該第一認證金鑰分別產生第一通訊金鑰以及第一傳輸金鑰以作為該伺服器金鑰，並將該伺服器金鑰傳送並儲存至該通訊設備。

30. 如申請專利範圍第 29 項所述的方法，在該第一使用者裝置獲得裝置間通訊的認證之後更包括：

對該認證伺服器中的裝置間通訊控制器提出對該第二使用者裝置的裝置間通訊請求；以及

從該裝置間通訊控制器接收由該裝置間通訊控制器產生的該裝置間主要金鑰信息，以使該第一使用者裝置及該第二使用者裝置利用該裝置間主要金鑰信息進行裝置間相互認證以及裝置間通訊。

31. 如申請專利範圍第 29 項所述的方法，利用該裝置間主要金鑰信息進行裝置間相互認證包括下列步驟：

接收從該裝置間通訊控制器依據由第二使用者裝置所決定是否與該第一使用者裝置通訊的通訊回應；以及

依據該通訊回應而決定是否進行該第一以及該第二使用者裝置之間的該裝置間相互認證。

32. 如申請專利範圍第 29 項所述的方法，進行該第一以及該第二使用者裝置之間的該裝置間相互認證更包括下列步驟：

產生第一隨機值並依據該裝置間主要金鑰信息的主要金鑰以產生第一暫時金鑰，並將該第一隨機值送至該第二使用者裝置；

接收從該第二使用者裝置產生的第二隨機值以及第一中介值，其中該第一中介值是該第二使用者裝置依據第二暫時金鑰及該第一隨機值而計算產生，該第二暫時金鑰是該第二使用者裝置依據該裝置間主要金鑰信息的該主要金鑰而計算產生；

依據該第一暫時金鑰以及該第一隨機值以計算第二中介值，並判斷該第一中介值與該第二中介值是否相同；

若該第一及該第二中介值相同時，依據該第一暫時金鑰及該第二隨機值以計算第三中介值，並將該第三中介值傳送至該第二使用者裝置；以及

該第二使用者裝置依據該第二暫時金鑰及該第二隨機值以計算第四中介值，並在判斷該第三中介值與該第四中介值相同時，該第二使用者裝置允許該第一使用者裝置依據該裝置間主要金鑰信息進行裝置間通訊的加解密操作。

33. 如申請專利範圍第 29 項所述的方法，利用該裝置間主要金鑰信息進行裝置間相互認證包括下列步驟：

當該第一使用者裝置接收該裝置間主要金鑰信息但該第二使

用者裝置並未具有該裝置間主要金鑰信息時，產生第一隨機值，並將該第一隨機值以及該裝置間主要金鑰信息的主要金鑰傳送到該第二使用者裝置；

接收從該該第二使用者裝置產生的第二隨機值以及第一中介值，其中該第一中介值是該第二使用者裝置依據第二暫時金鑰及該第一隨機值而計算產生，該第二暫時金鑰是該第二使用者裝置依據該裝置間主要金鑰信息的該主要金鑰而計算產生；

依據該第一暫時金鑰以及該第一隨機值以計算第二中介值，並判斷該第一中介值與該第二中介值是否相同；

若該第一及該第二中介值相同時，依據該第一暫時金鑰及該第二隨機值以計算第三中介值，並將該第三中介值傳送至該第二使用者裝置；以及

該第二使用者裝置依據該第二暫時金鑰及該第二隨機值以計算第四中介值，並在判斷該第三中介值與該第四中介值相同時，該第二使用者裝置允許該第一使用者裝置依據該裝置間主要金鑰信息進行裝置間通訊的加解密操作。

34. 一種裝置間通訊的認證方法，適用於該通訊系統中的認證伺服器，其中該通訊系統還包括第一使用者裝置以及第二使用者裝置，該認證方法包括：

接收從該第一使用者裝置發出的連接請求；

對該第一使用者裝置進行常規認證並提供金鑰產生信息至該第一使用者裝置；

依據該金鑰產生信息以及金鑰衍生程序以產生伺服器金鑰；

以及

該第一使用者裝置依據該金鑰產生信息以及該金鑰衍生程序產生裝置金鑰，以獲得裝置間通訊的認證，使該第一使用者裝置與獲得裝置間通訊的認證的第二使用者裝置直接進行裝置間通訊，而不需透過該認證伺服器，

其中該認證伺服器包括：

通訊設備，透過網路協定以與該第一使用者裝置進行通訊並處理位於該通訊設備的通訊範圍內的裝置間通訊；以及

管理單元以及認證單元，當該管理單元及該認證單元透過該通訊設備接收該第一使用者裝置發出的該連接請求後，該認證單元對該第一使用者裝置進行常規認證，

當常規認證成功時，該認證單元依據常規認證結果產生第一認證金鑰並將該第一認證金鑰傳送至該管理單元，該管理單元依據該第一認證金鑰分別產生第一通訊金鑰以及第一傳輸金鑰以作為該伺服器金鑰，並將該伺服器金鑰傳送並儲存至該通訊設備。

35. 一種裝置間通訊的認證系統，包括：

第一使用者裝置；

認證伺服器，位於該第一使用者裝置的通訊範圍內，其中該認證伺服器包括：

通訊設備，透過網路協定以與該第一使用者裝置進行通訊並處理位於該通訊設備的通訊範圍內的裝置間通訊；以及

管理單元以及認證單元，當該管理單元及該認證單元透

過該通訊設備接收該第一使用者裝置發出的該連接請求後，該認證單元對該第一使用者裝置進行常規認證，

當常規認證成功時，該認證單元依據常規認證結果產生第一認證金鑰並將該第一認證金鑰傳送至該管理單元，該管理單元依據該第一認證金鑰產生第一通訊金鑰，並將該第一通訊金鑰傳送至該通訊設備，該通訊設備儲存該第一通訊金鑰並依據該第一通訊金鑰以產生第一傳輸金鑰，其中該第一通訊金鑰以及該第一傳輸金鑰稱為該伺服器金鑰；

其中，當該第一使用者裝置發出連接請求至該認證伺服器時，該認證伺服器對該第一使用者裝置進行常規認證並提供金鑰產生信息至該第一使用者裝置，

該認證伺服器依據該金鑰產生信息以及金鑰衍生（key derivation）程序以產生伺服器金鑰，以及

該第一使用者裝置依據該金鑰產生信息以及該金鑰衍生程序產生裝置金鑰，以獲得裝置間通訊的認證，使該第一使用者裝置與獲得裝置間通訊的認證的第二使用者裝置直接進行裝置間通訊，而不需透過該認證伺服器。

36. 一種裝置間通訊認證系統，包括：

第一使用者裝置以及第二使用者裝置；以及

認證伺服器，位於該第一使用者裝置以及該第二使用者裝置的通訊範圍內，其中該認證伺服器包括：

通訊設備，透過網路協定以與該第一使用者裝置進行通

訊並處理位於該通訊設備的通訊範圍內的裝置間通訊；以及

管理單元以及認證單元，當該管理單元及該認證單元透過該通訊設備接收該第一使用者裝置發出的該連接請求後，該認證單元對該第一使用者裝置進行常規認證，

當常規認證成功時，該認證單元依據常規認證結果產生第一認證金鑰並將該第一認證金鑰傳送至該管理單元，該管理單元依據該第一認證金鑰產生第一通訊金鑰，並將該第一通訊金鑰傳送至該通訊設備，該通訊設備儲存該第一通訊金鑰並依據該第一通訊金鑰以產生第一傳輸金鑰，其中該第一通訊金鑰以及該第一傳輸金鑰稱為該伺服器金鑰，

其中，當該第一使用者裝置及該第二使用者裝置分別發出裝置間通訊連接請求至該認證伺服器時，該認證伺服器對該第一及該第二使用者裝置進行常規認證並分別提供第一金鑰產生信息及第二金鑰產生信息至該第一及該第二使用者裝置，

該認證伺服器依據該第一及第二金鑰產生信息以及金鑰衍生程序以產生伺服器金鑰，以及

該認證伺服器將該伺服器金鑰分別傳送至該第一及該第二使用者裝置，以使該第一及該第二使用者裝置獲得裝置間通訊的認證並直接進行裝置間通訊，而不需透過該認證伺服器。

37. 一種裝置間通訊及認證方法，適用於該通訊系統中的第一使用者裝置，其中該通訊系統還包括認證伺服器以及第二使用者裝置，該認證方法包括：

發出連接請求至該認證伺服器；

該認證伺服器對該第一使用者裝置進行常規認證並提供金鑰產生信息，且該認證伺服器依據該金鑰產生信息以及金鑰衍生程序以產生伺服器金鑰；以及

依據該金鑰產生信息以及該金鑰衍生程序產生裝置金鑰，以獲得裝置間通訊的認證，使該第一使用者裝置與獲得裝置間通訊的認證的第二使用者裝置直接進行裝置間通訊，而不需透過該認證伺服器，

其中該認證伺服器包括：

通訊設備，透過網路協定以與該第一使用者裝置進行通訊並處理位於該通訊設備的通訊範圍內的裝置間通訊；

管理單元以及認證單元，當該管理單元及該認證單元透過該通訊設備接收該第一使用者裝置發出的該連接請求後，該認證單元對該第一使用者裝置進行常規認證；

當常規認證成功時，該認證單元依據常規認證結果產生第一認證金鑰並將該第一認證金鑰傳送至該管理單元，該管理單元依據該第一認證金鑰產生第一通訊金鑰，並將該第一通訊金鑰傳送至該通訊設備，該通訊設備儲存該第一通訊金鑰並依據該第一通訊金鑰以產生第一傳輸金鑰，其中該第一通訊金鑰以及該第一傳輸金鑰稱為該伺服器金鑰。

38. 一種裝置間通訊的認證方法，適用於該通訊系統中的認證伺服器，其中該通訊系統還包括第一使用者裝置以及第二使用

者裝置，該認證方法包括：

接收從該第一使用者裝置發出的連接請求；

對該第一使用者裝置進行常規認證並提供金鑰產生信息至該第一使用者裝置；

依據該金鑰產生信息以及金鑰衍生程序以產生伺服器金鑰；以及

該第一使用者裝置依據該金鑰產生信息以及該金鑰衍生程序產生裝置金鑰，以獲得裝置間通訊的認證，使該第一使用者裝置與獲得裝置間通訊的認證的第二使用者裝置直接進行裝置間通訊，而不需透過該認證伺服器，

其中該認證伺服器包括：

通訊設備，透過網路協定以與該第一使用者裝置進行通訊並處理位於該通訊設備的通訊範圍內的裝置間通訊；

管理單元以及認證單元，當該管理單元及該認證單元透過該通訊設備接收該第一使用者裝置發出的該連接請求後，該認證單元對該第一使用者裝置進行常規認證；

當常規認證成功時，該認證單元依據常規認證結果產生第一認證金鑰並將該第一認證金鑰傳送至該管理單元，該管理單元依據該第一認證金鑰產生第一通訊金鑰，並將該第一通訊金鑰傳送至該通訊設備，該通訊設備儲存該第一通訊金鑰並依據該第一通訊金鑰以產生第一傳輸金鑰，其中該第一通訊金鑰以及該第一傳輸金鑰稱為該伺服器金鑰。

圖式

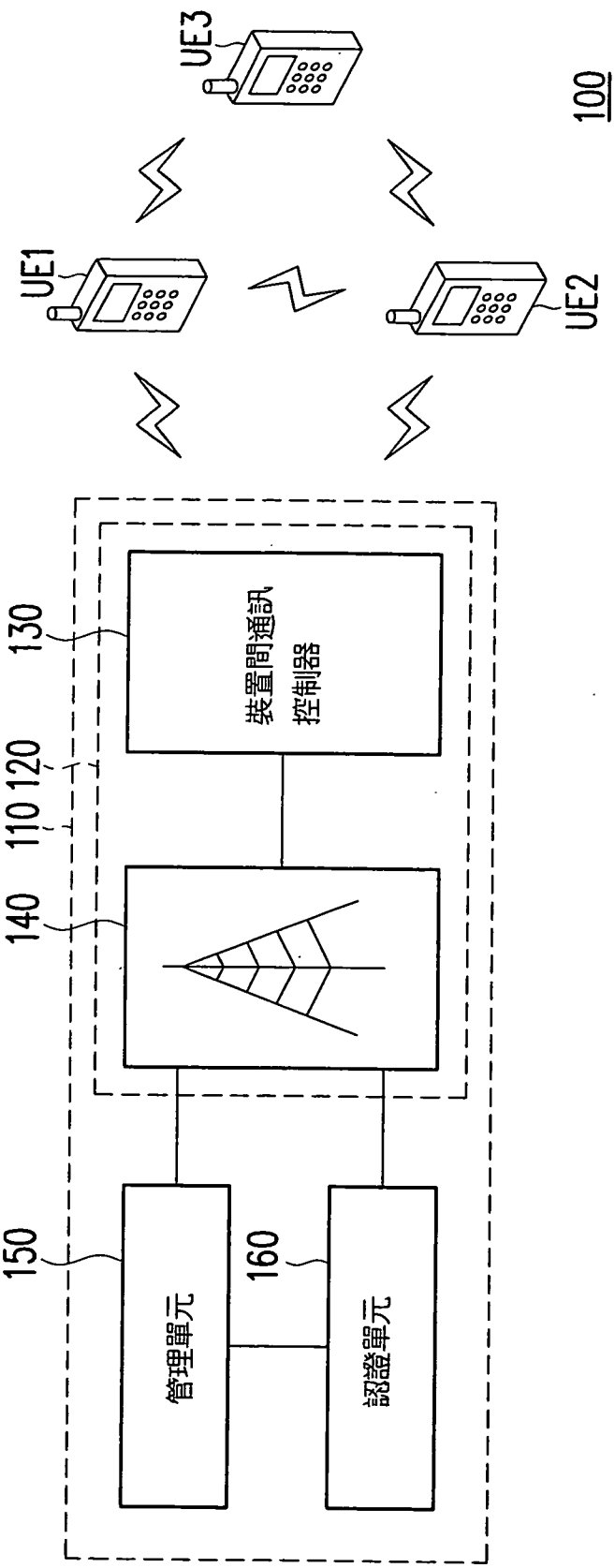

圖 1

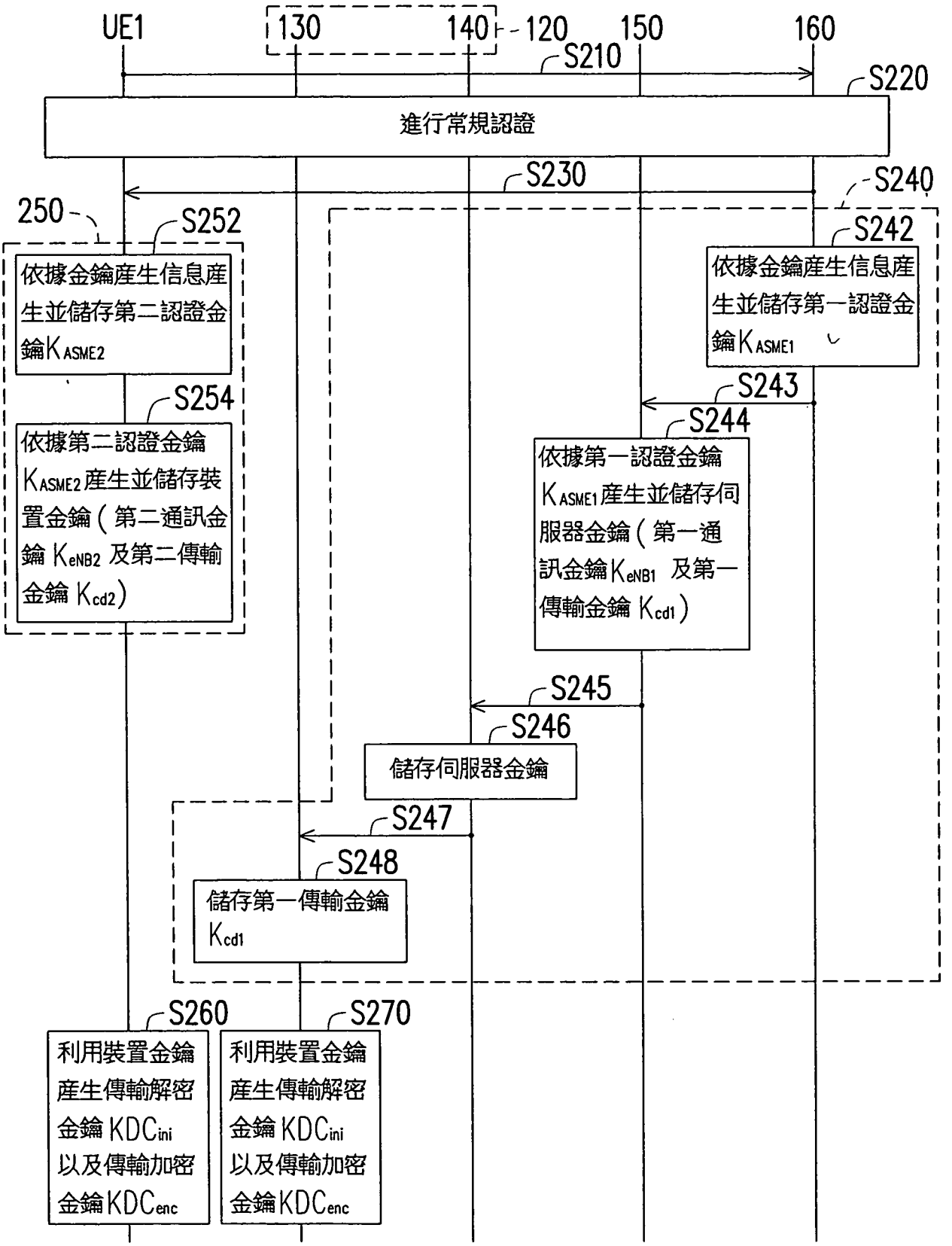
UE1
130
140
120
150
160
S210
S220
進行常規認證
S230
S240
250
S252
依據金鑰產生信息產生並儲存第二認證金鑰 K_{ASME2}
S242
依據金鑰產生信息產生並儲存第一認證金鑰 K_{ASME1}
S254
依據第二認證金鑰 K_{ASME2} 產生並儲存裝置金鑰（第二通訊金鑰 K_{eNB2} 及第二傳輸金鑰 K_{cd2}）
S243
S244
依據第一認證金鑰 K_{ASME1} 產生並儲存伺服器金鑰（第一通訊金鑰 K_{eNB1} 及第一傳輸金鑰 K_{cd1}）
S245
S246
儲存伺服器金鑰
S247
S248
儲存第一傳輸金鑰 K_{cd1}
S260
利用裝置金鑰產生傳輸解密金鑰 KDC_{ini} 以及傳輸加密金鑰 KDC_{enc}
S270
利用裝置金鑰產生傳輸解密金鑰 KDC_{ini} 以及傳輸加密金鑰 KDC_{enc}

圖2

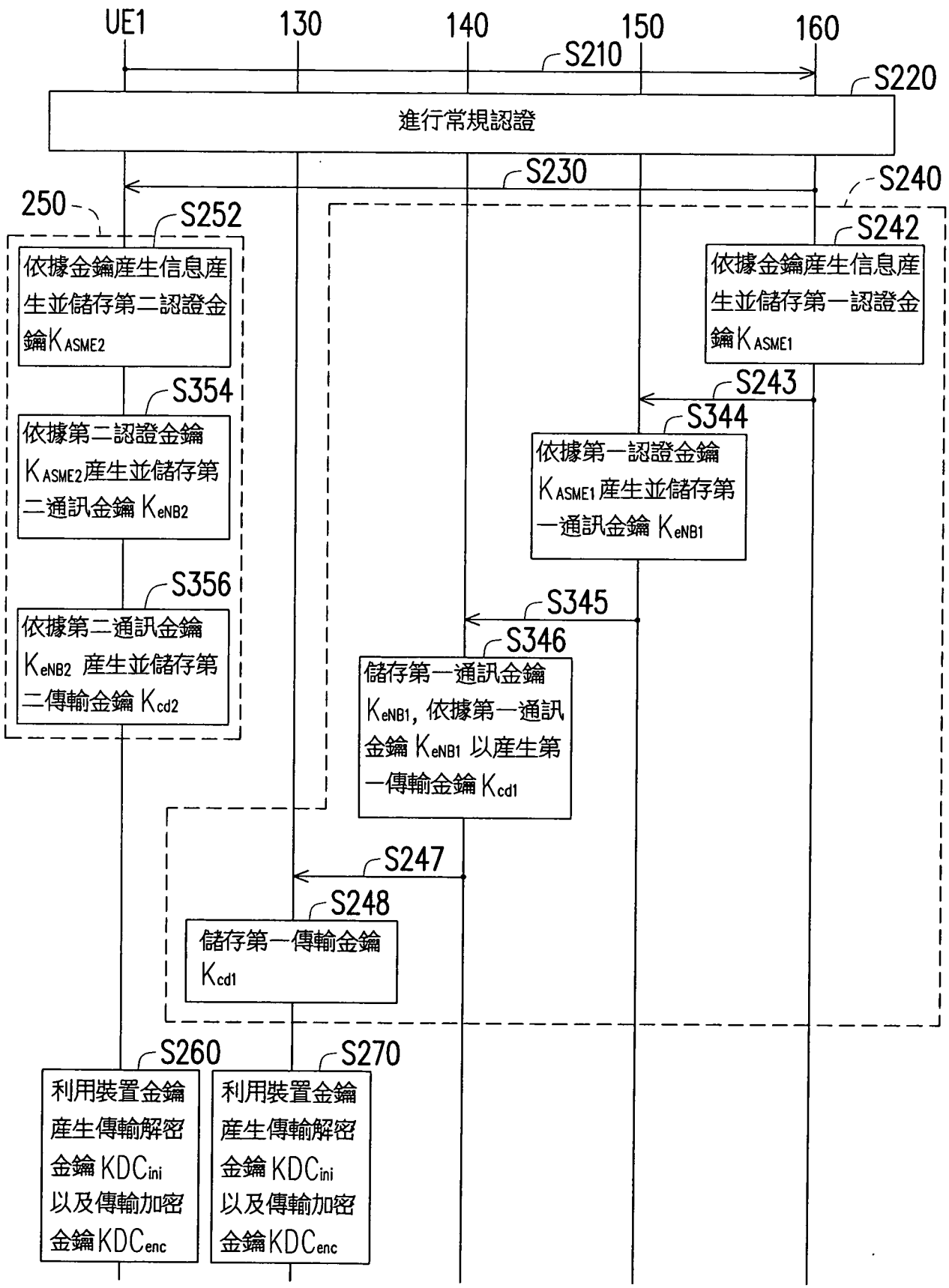
UE1
130
140
150
160
S210
S220
進行常規認證
S230
S240
250
S252
依據金鑰產生信息產生並儲存第二認證金鑰 K_{ASME2}
S242
依據金鑰產生信息產生並儲存第一認證金鑰 K_{ASME1}
S243
S354
依據第二認證金鑰 K_{ASME2} 產生並儲存第二通訊金鑰 K_{eNB2}
S344
依據第一認證金鑰 K_{ASME1} 產生並儲存第一通訊金鑰 K_{eNB1}
S356
依據第二通訊金鑰 K_{eNB2} 產生並儲存第二傳輸金鑰 K_{cd2}
S345
S346
儲存第一通訊金鑰 K_{eNB1}，依據第一通訊金鑰 K_{eNB1} 以產生第一傳輸金鑰 K_{cd1}
S247
S248
儲存第一傳輸金鑰 K_{cd1}
S260
S270
利用裝置金鑰產生傳輸解密金鑰 KDC_{ini} 以及傳輸加密金鑰 KDC_{enc}
利用裝置金鑰產生傳輸解密金鑰 KDC_{ini} 以及傳輸加密金鑰 KDC_{enc}

圖3

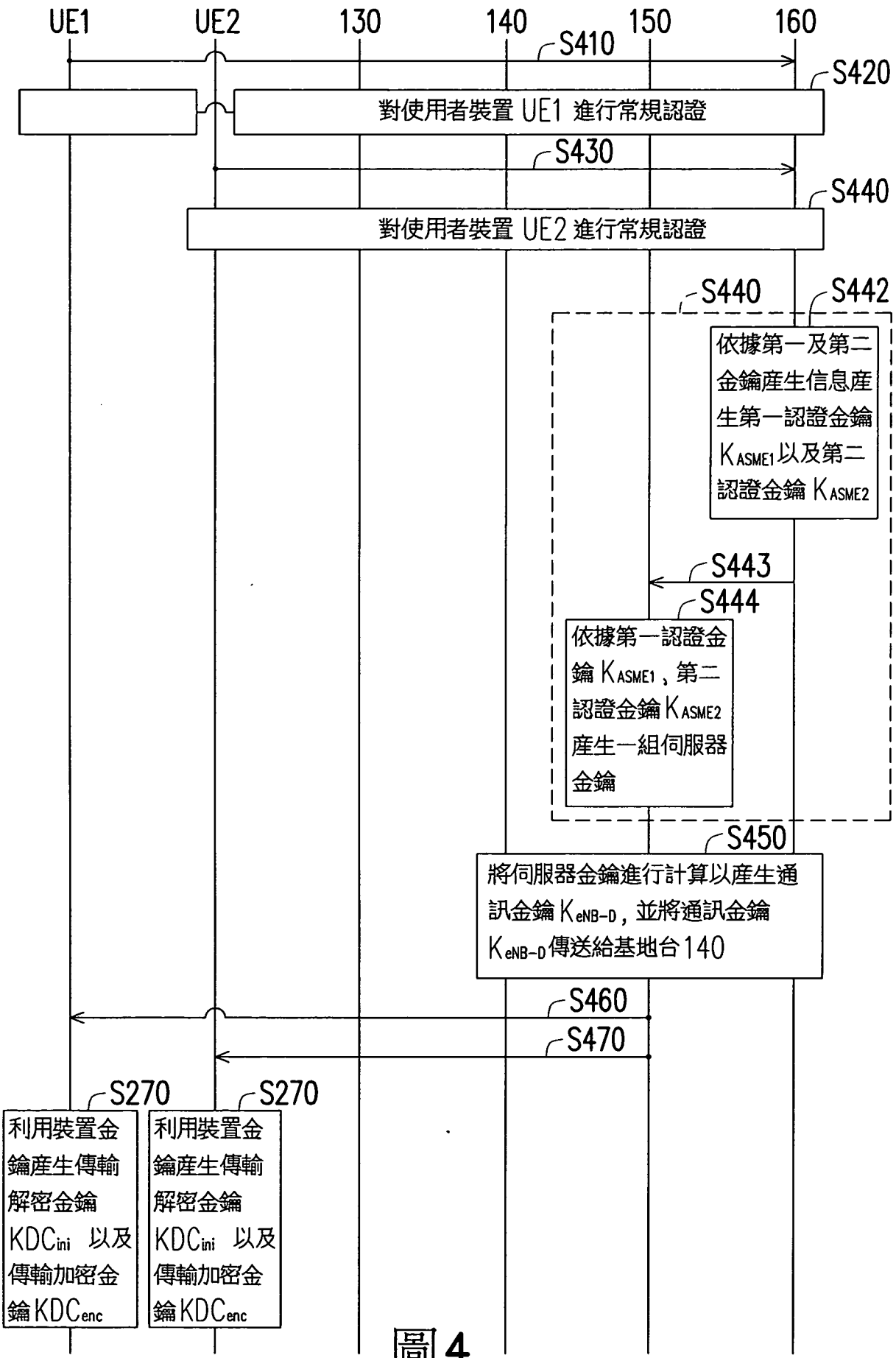
UE1
UE2
130
140
150
160
S410
S420
對使用者裝置 UE1 進行常規認證
S430
S440
對使用者裝置 UE2 進行常規認證
S440
S442
依據第一及第二金鑰產生信息產生第一認證金鑰 K_{ASME1} 以及第二認證金鑰 K_{ASME2}
S443
S444
依據第一認證金鑰 K_{ASME1}，第二認證金鑰 K_{ASME2} 產生一組伺服器金鑰
S450
將伺服器金鑰進行計算以產生通訊金鑰 K_{eNB-D}，並將通訊金鑰 K_{eNB-D} 傳送給基地台140
S460
S470
S270
S270
利用裝置金鑰產生傳輸解密金鑰 KDC_{ini} 以及傳輸加密金鑰 KDC_{enc}
利用裝置金鑰產生傳輸解密金鑰 KDC_{ini} 以及傳輸加密金鑰 KDC_{enc}

圖 4

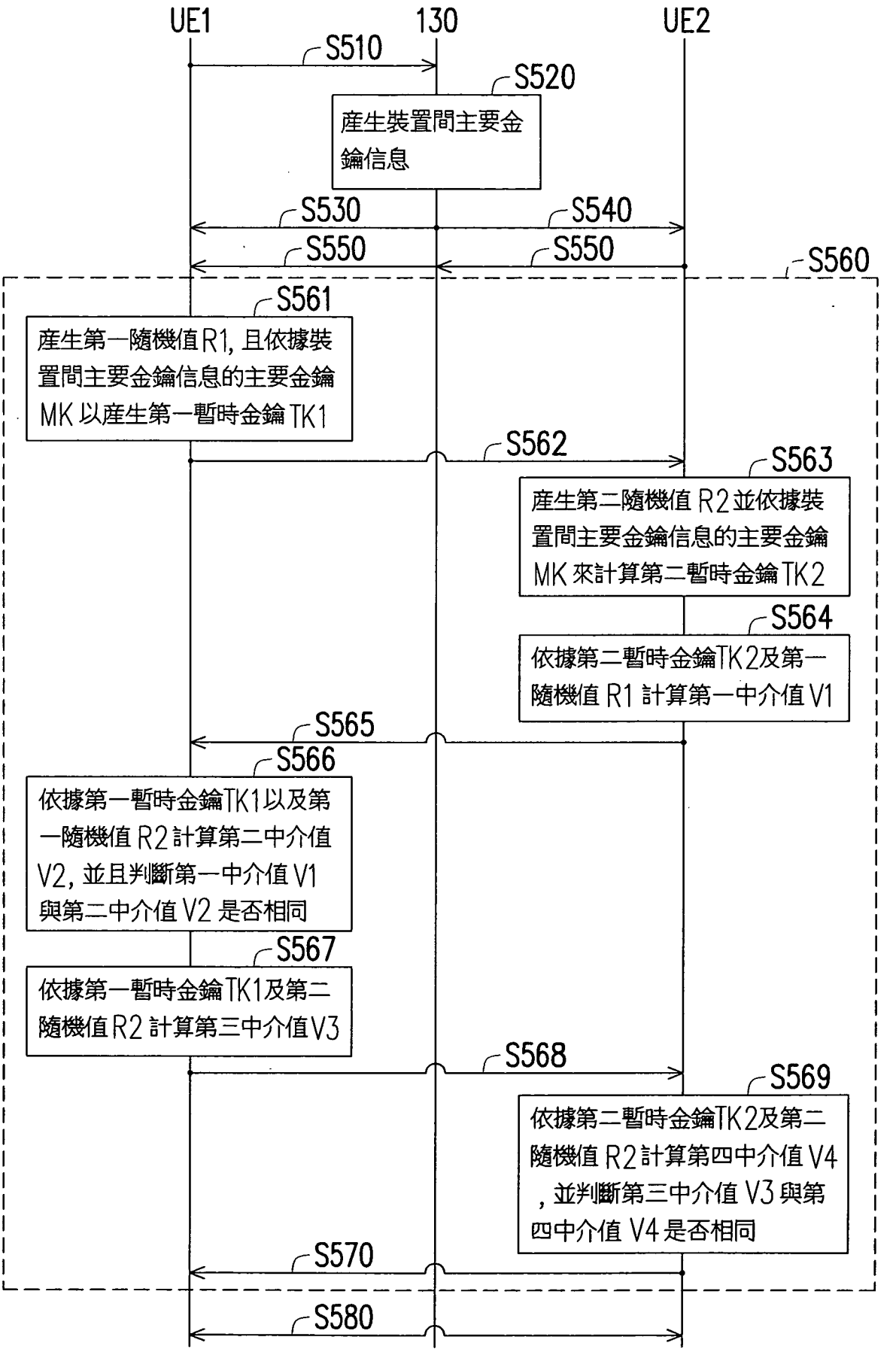
UE1
130
UE2
S510
S520
產生裝置間主要金鑰信息
S530
S540
S550
S550
S560
S561
產生第一隨機值R1, 且依據裝置間主要金鑰信息的主要金鑰MK 以產生第一暫時金鑰TK1
S562
S563
產生第二隨機值 R2並依據裝置間主要金鑰信息的主要金鑰MK 來計算第二暫時金鑰TK2
S564
依據第二暫時金鑰TK2及第一隨機值 R1 計算第一中介值V1
S565
S566
依據第一暫時金鑰TK1以及第一隨機值 R2 計算第二中介值V2, 並且判斷第一中介值 V1與第二中介值 V2 是否相同
S567
依據第一暫時金鑰TK1及第二隨機值R2 計算第三中介值V3
S568
S569
依據第二暫時金鑰TK2及第二隨機值 R2計算第四中介值 V4, 並判斷第三中介值 V3 與第四中介值 V4 是否相同
S570
S580

圖5

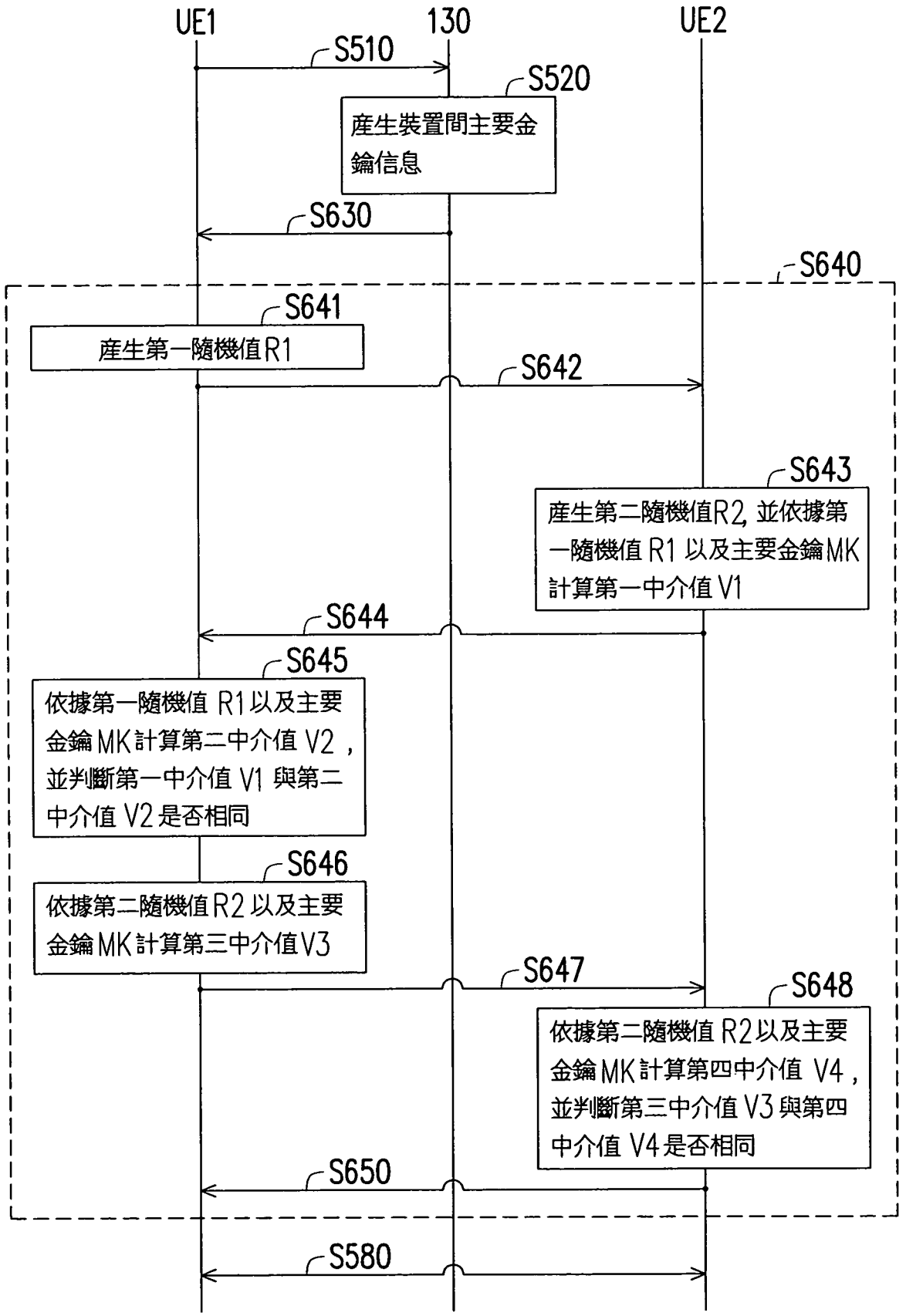
UE1
130
UE2
S510
S520
產生裝置間主要金鑰信息
S630
S640
S641
產生第一隨機值R1
S642
S643
產生第二隨機值R2, 並依據第一隨機值 R1 以及主要金鑰MK計算第一中介值 V1
S644
S645
依據第一隨機值 R1以及主要金鑰MK計算第二中介值 V2，並判斷第一中介值 V1 與第二中介值 V2是否相同
S646
依據第二隨機值R2 以及主要金鑰MK計算第三中介值V3
S647
S648
依據第二隨機值 R2以及主要金鑰MK計算第四中介值 V4，並判斷第三中介值 V3與第四中介值 V4是否相同
S650
S580

圖6

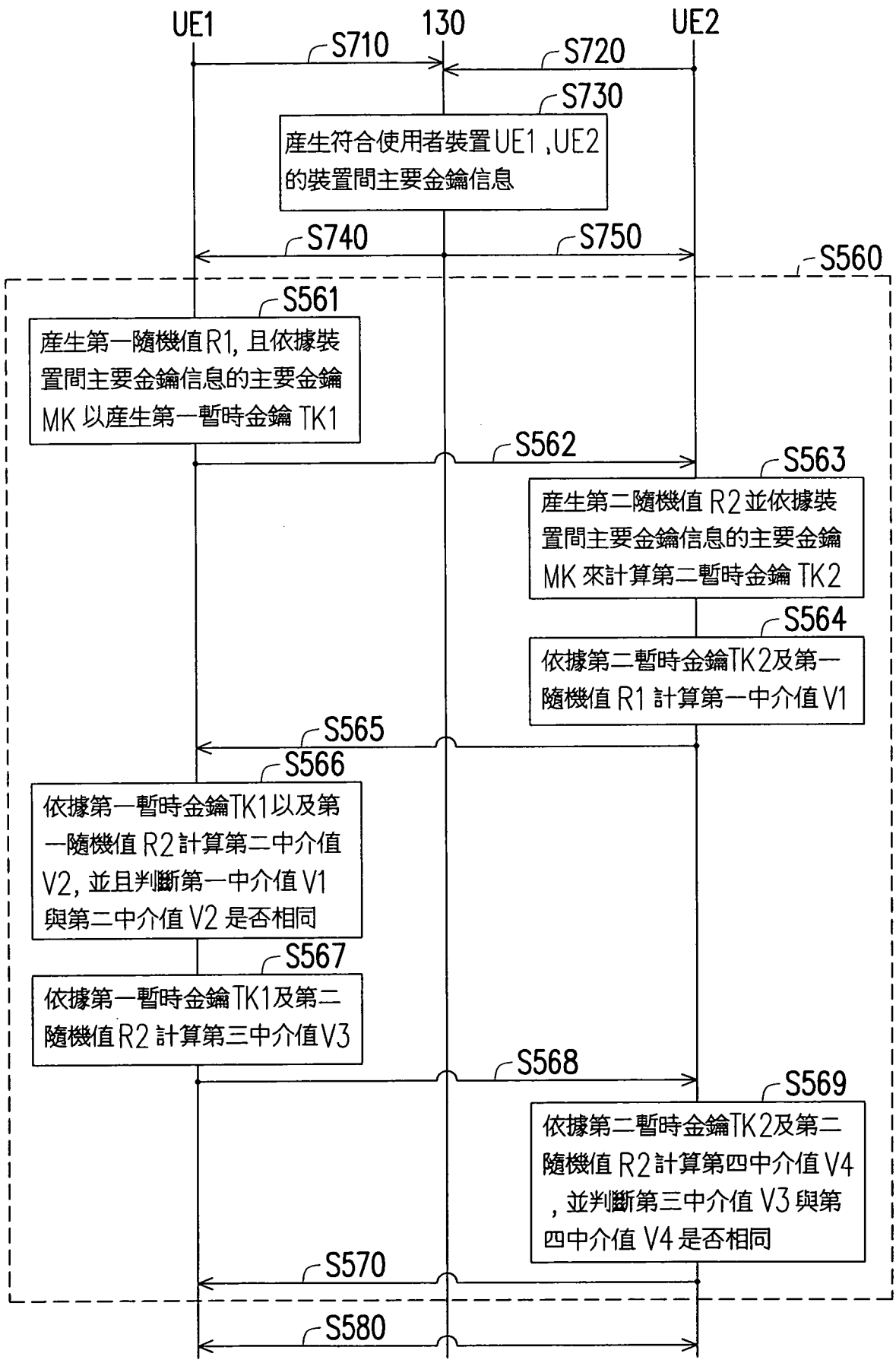
UE1
130
UE2
S710
S720
S730
產生符合使用者裝置UE1,UE2的裝置間主要金鑰信息
S740
S750
S560
S561
產生第一隨機值R1,且依據裝置間主要金鑰信息的主要金鑰MK以產生第一暫時金鑰TK1
S562
S563
產生第二隨機值R2並依據裝置間主要金鑰信息的主要金鑰MK來計算第二暫時金鑰TK2
S564
依據第二暫時金鑰TK2及第一隨機值R1計算第一中介值V1
S565
S566
依據第一暫時金鑰TK1以及第一隨機值R2計算第二中介值V2,並且判斷第一中介值V1與第二中介值V2是否相同
S567
依據第一暫時金鑰TK1及第二隨機值R2計算第三中介值V3
S568
S569
依據第二暫時金鑰TK2及第二隨機值R2計算第四中介值V4,並判斷第三中介值V3與第四中介值V4是否相同
S570
S580

圖7

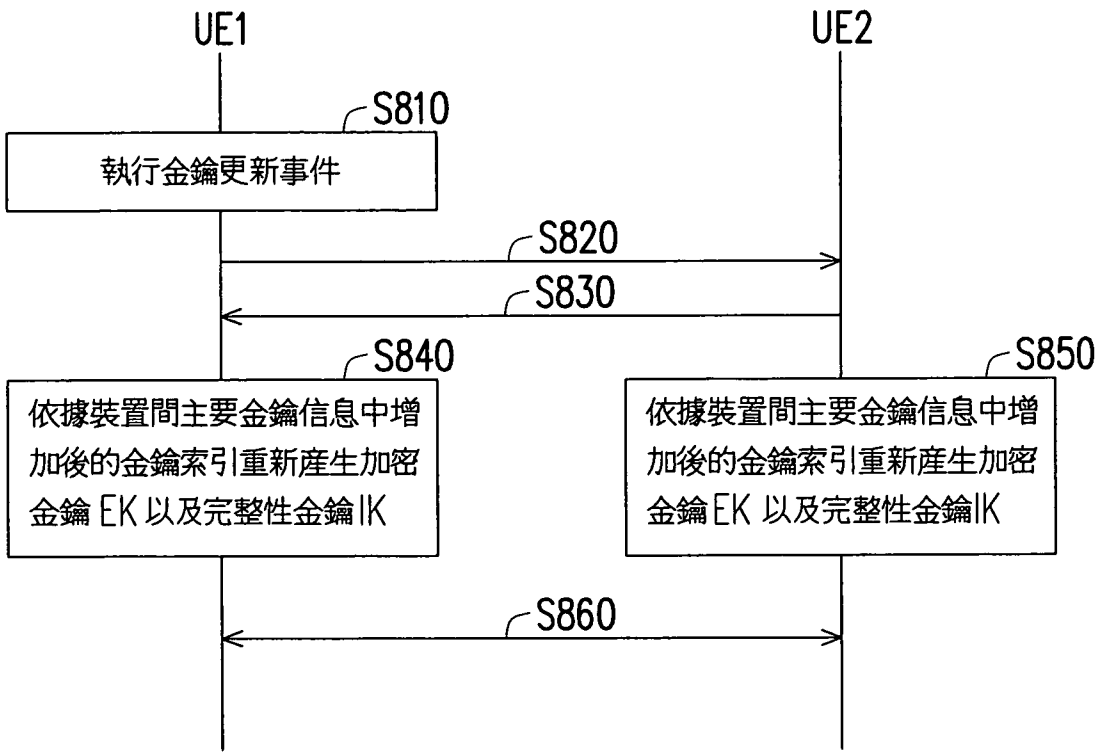
UE1
UE2
S810
執行金鑰更新事件
S820
S830
S840
依據裝置間主要金鑰信息中增加後的金鑰索引重新產生加密金鑰 EK 以及完整性金鑰 IK
S850
依據裝置間主要金鑰信息中增加後的金鑰索引重新產生加密金鑰 EK 以及完整性金鑰 IK
S860

圖8