I475899

(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 I475899 B**

(45)公告日： 中華民國 104 (2015) 年 03 月 01 日

(21)申請案號：101111723 (22)申請日： 中華民國 101 (2012) 年 04 月 02 日

(51)Int. Cl.： ***H04W12/06 (2009.01)***

(30)優先權：2011/04/05 美國 61/472,109

2011/04/25 美國 13/093,722

(71)申請人：蘋果公司 (美國) APPLE INC. (US)

美國

(72)發明人：海格帝 大衛 HAGGERTY, DAVID T. (US)；凡豪克 傑諾德 VON HAUCK, JERROLD (US)；麥克萊夫林 凱文 MCLAUGHLIN, KEVIN (US)

(74)代理人：陳長文

(56)參考文獻：

EP 2282442A1 US 2008/0253564A1

US 2009/0205028A1 US 2010/0306107A1

US 2010/0310076A1

審查人員：葉昌倫

申請專利範圍項數：20 項 圖式數：5 共 46 頁

(54)名稱

用以儲存電子存取用戶之設備及方法

APPARATUS AND METHODS FOR STORING ELECTRONIC ACCESS CLIENTS

(57)摘要

本發明揭露用以儲存和控制存取控制用戶之設備及方法。於一實施例中，傳輸及接收裝置確保其於任何時刻僅有 eSIM 之一副本為有效的。明確地，各轉移之 eSIM 係針對目的地裝置而加密；來自來源裝置之 eSIM 被刪除、撤銷、或者除此之外使其變為不可用。亦描述網路設施之各種形態，包括電子通用積體電路卡(eUICC)器具、及行動裝置。亦揭露用於 eSIM 之轉移的各種情境。

Apparatus and methods for storing and controlling access control clients. In one embodiment, transmitting and receiving devices ensure that only one copy of an eSIM is active at any time. Specifically, each transferred eSIM is encrypted for the destination device; the eSIM from the source device is deleted, deactivated, or otherwise rendered unusable. Various aspects of network infrastructure are also described, including electronic Universal Integrated Circuit Card (eUICC) appliances, and mobile devices. Various scenarios for transfer of eSIMs are also disclosed.

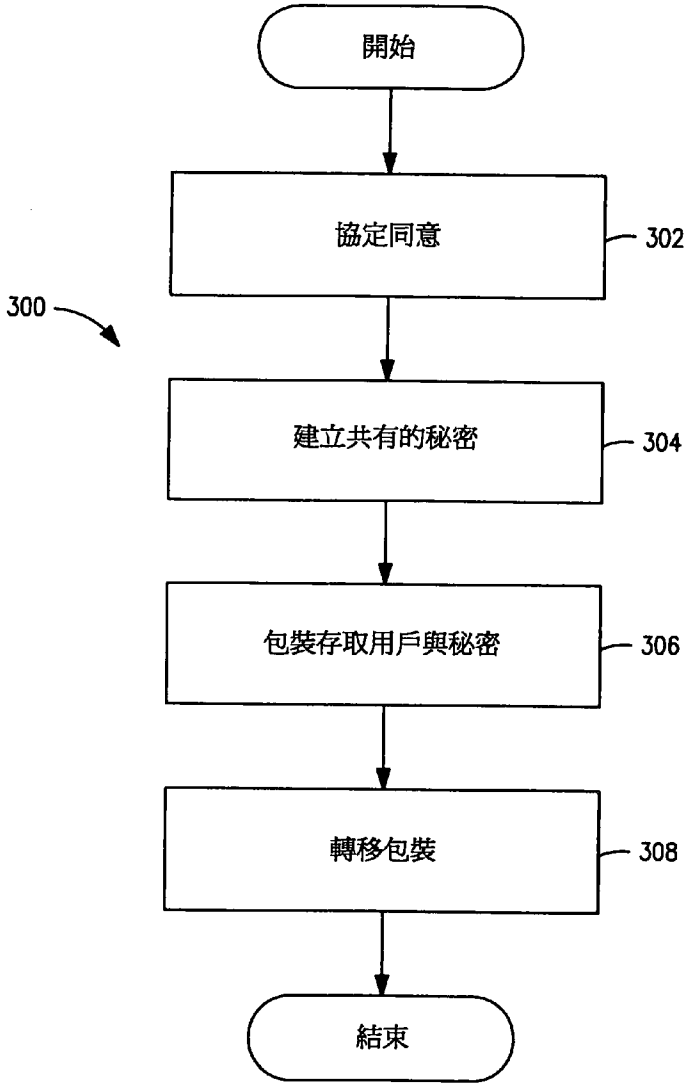

圖3

公告本

發明專利說明書

（本申請書格式、順序，請勿任意更動，※記號部分請勿填寫）

※申請案號：101111723

※申請日：101 年 04 月 02 日　※IPC 分類：H04W 12/06 (2009.01)

一、發明名稱：（中文／英文）

用以儲存電子存取用戶之設備及方法

Apparatus and methods for storing electronic access clients

二、中文發明摘要：

本發明揭露用以儲存和控制存取控制用戶之設備及方法。於一實施例中，傳輸及接收裝置確保其於任何時刻僅有 eSIM 之一副本爲有效的。明確地，各轉移之 eSIM 係針對目的地裝置而加密；來自來源裝置之 eSIM 被刪除、撤銷、或者除此之外使其變爲不可用。亦描述網路設施之各種形態，包括電子通用積體電路卡（eUICC）器具、及行動裝置。亦揭露用於 eSIM 之轉移的各種情境。

三、英文發明摘要：

Apparatus and methods for storing and controlling access control clients. In one embodiment, transmitting and receiving devices ensure that only one copy of an eSIM is active at any time. Specifically, each transferred eSIM is encrypted for the destination device; the eSIM from the source device is deleted, deactivated, or otherwise rendered unusable. Various aspects of network infrastructure are also described, including electronic Universal Integrated Circuit Card (eUICC) appliances, and mobile devices. Various scenarios for transfer of eSIMs are also disclosed.

四、指定代表圖：

（一）本案指定代表圖為：第（3）圖。

（二）本代表圖之元件符號簡單說明：無

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：無

六、發明說明：

【發明所屬之技術領域】

本發明一般而言是有關通訊系統之領域，而更明確地於一範例形態中係有關儲存和分配存取控制用戶至裝置。

【先前技術】

存取控制是大部分習知技術無線無線電通訊系統中之安全通訊所必要的。例如，一種簡單的存取控制技術可包括：（i）驗證（verifying）之一通訊方之身分、及（ii）准予一與該已驗證身分相稱之存取等級（level）。於範例蜂巢式系統（例如，全球行動通訊系統（UMTS））之背景下，存取控制係由一執行在實體全球積體電路卡（UICC）上之存取控制用戶（稱之爲全球訂戶識別模組（USIM））來管理。USIM 存取控制用戶鑑別訂戶以進入 UMTS 蜂巢式網路。在成功的鑑別（authentication）之後，容許訂戶對蜂巢式網路存取。於下文中使用時，術語「存取控制用戶」一般指的是邏輯實物（entity），無論是內嵌於硬體或軟體中，其適於控制第一裝置之存取至網路。存取控制用戶之共同範例包括前述的 USIM、CDMA 訂戶識別模組（CSIM）、IP 多媒體服務識別模組（ISIM）、訂戶識別模組（SIM）、可移動式使用者識別模組（RUIM）、等等。

傳統上，USIM（或更一般地「SIM」）係執行眾所週知的鑑別及金鑰協定（AKA）程序，其係將應用資料及程

式驗證和解密以確保安全的初始化。明確地，USIM 必須（i）成功地回答一遠端詰問（challenge）以對網路業者證明其識別；及（ii）發送詰問以驗證網路之識別。

雖然傳統的 SIM 解決方案被實施於可移動式積體電路卡（ICC）（亦稱爲「SIM」卡），其專利權人之初期研究係導向在一執行於行動裝置中之軟體用戶內虛擬化 SIM 操作。虛擬化的 SIM 操作可減小裝置尺寸，增加裝置功能性，及提供較大的彈性。

不幸地，虛擬化的 SIM 操作也爲網路業者（operator）及裝置製造商帶來多重新的挑戰。例如，傳統的 SIM 卡係由一受信賴的 SIM 供應商（vendor）來製造及保固。這些傳統的 SIM 卡係執行其已被永久地「燒」入 SIM 卡之軟體的單一安全版本。一旦燒入後，該卡即無法被篡改（除非同時破壞該 SIM 卡）。

反之，行動裝置係由廣大範圍的裝置製造商所製造，且可執行由多數或甚至未知的第三方軟體供應商所提供之軟體。此外，行動裝置被頻繁地「修補」軟體，其可能同時地修正現存的錯誤並引入新的錯誤。任何軟體均可能產生惡化、破壞、及/或誤用。此外，雖然實體 SIM 卡極難以複製，但軟體可輕易地被複製、重製，等等。因爲各 SIM 係代表對有限網路資源之存取量的合約，所以虛擬化的 SIM 之非法使用可大大地影響網路操作及使用者經驗。

此外，需要新的解決方案以提供虛擬化的 SIM 之保護及特性，其特性通常係類似於傳統「硬式」SIM 之特性。

更一般地，需要增進的解決方案來儲存及分配虛擬化的存取控制用戶。理想地，此等解決方案應提供傳統存取控制用戶操作之優點，而具有虛擬化操作之額外能力。

【發明內容】

本發明係藉由提供（除了別的事項之外）用以儲存和分配存取控制用戶至裝置的設備及方法來滿足上述需求。

於本發明之一形態中，揭露一種用以儲存一或更多存取資料元件之設備。於一實施例中，安全設備包括一適於儲存複數使用者存取資料元件之安全元件，各使用者存取資料元件係針對該安全元件而加密。安全設備進一步包括一處理器；及一資料通連與該處理器之儲存裝置，該儲存裝置包括電腦可執行指令，其係組態成，當由該處理器執行時：從一同級（peer）裝置接收針對一或更多存取資料元件之請求；驗證該同級裝置；解密該一或更多請求之存取資料元件；針對該同級裝置再加密該解密的一或更多存取資料元件；及將該一或更多再加密的資料元件轉移至該已驗證的同級裝置，該轉移致使該一或更多存取資料元件移除自該安全元件。

於一變異中，該使用者存取資料元件爲電子訂戶識別模組（eSIM）。

於第二變異中，該驗證包括檢查與該同級裝置相關的憑證，並產生詰問回應。

於第三變異中，電腦可執行指令額外地包括指令，其

係組態成，當由該處理器執行時：協商一轉移協定。於一範例中，該解密的一或更多存取資料元件之再加密係至少部分地根據該轉移協定。於另一範例中，該轉移協定包括交握（handshaking）之一或更多元件。於又另一此類範例中，該協商的轉移協定包括由該設備及該同級裝置所支援之轉移協定的識別。

於第四變異中，該設備包括硬體安全性模組（HSM）。

於第五變異中，該設備係實施於行動電話中。

於又第六變異中，該設備係實施於實體卡形狀因數中。

於另一實施例中，該設備包括一適於儲存複數使用者存取資料元件之安全元件，各使用者存取資料元件係針對該安全元件而加密。安全設備進一步包括一處理器、及一資料通連與該處理器之儲存裝置，該儲存裝置包括電腦可執行指令，其係組態成，當由該處理器執行時：從一已驗證的同級裝置請求一或更多存取資料元件；從該已驗證的同級裝置接收該一或更多請求的存取資料元件；驗證其針對該安全元件而加密之該一或更多請求的存取資料元件；儲存該一或更多加密的存取資料元件於該安全元件中；及於一鑑別協定期間解密該一或更多加密的存取資料元件。

於一變異中，該使用者存取資料元件爲電子訂戶識別模組（eSIM）。

於第二變異中，該設備係實施於行動電話中。

於第三變異中，該設備係實施於實體卡形狀因數中，以用行動電話中使用。

於第四變異中，該驗證包括檢查由可靠的認證機構所發送之憑證。

於第五變異中，該驗證包括詰問與回應密碼交換之完成。

於第六變異中，該同級裝置包括 SIM 提供服務（SPS）。

於第七變異中，該同級裝置包括 eUICC 器具。

於第八變異中，該同級裝置包括操作性通連與行動應用程式商店之桌上型電腦。

於本發明之第三形態中，揭露一種用以轉移一或更多存取資料元件之方法。於一實施例中，該一或更多存取資料元件具有一與其相關之獨特識別符，且該方法包括：同意介於裝置與同級裝置之間的轉移協定；從該同級裝置接收該一或更多存取資料元件；驗證該轉移的一或更多存取資料元件，該一或更多存取資料元件及獨特識別符係針對該裝置而加密；及儲存該轉移的一或更多存取資料元件。

於第一變異中，該使用者存取資料元件包括電子訂戶識別模組（eSIM）。

於第二變異中，該轉移的一或更多存取資料元件之該獨特識別符係由該裝置所決定。

於第三變異中，該轉移的一或更多存取資料元件之該獨特識別符被提供至該同級裝置。

於第四變異中，該方法額外地包括通知該同級裝置有關該一或更多存取資料元件之成功的接收。

於第五變異中，該轉移的一或更多存取資料元件之該獨特識別符被提供至該同級裝置。

於本發明之第四形態中，揭露一種電腦可讀式設備。於一實施例中，該設備包括儲存有至少一電腦程式之儲存媒體，該電腦程式係組態成，當執行時：藉由至少如下步驟以轉移一或更多存取資料元件：同意與一同級裝置之轉移協定；及從該同級裝置接收該一或更多存取資料元件。

本發明之進一步特徵、其本質和各種優點將從後附圖形及以下詳細說明變爲更清楚明白。

【實施方式】

現在參考圖形，其中全文中類似的數字係指示類似的部件。

概觀

本發明係提供（除了別的事項之外）用以儲存和分配存取控制用戶至諸如（例如）行動裝置或「智慧型手機」的方法及設備。於本發明之第一形態中，用於轉移存取控制用戶（例如，eSIM）之裝置藉由確認該轉移僅以一可靠裝置來執行以實施用戶之獨特性及保存。於一實施例中，揭露一 eUICC 器具，其被實施於硬體安全性模組（HSM）內。各 HSM 可儲存大量 eSIM 以協助其儲存及分配，諸如

用於零售服務。所描述的 eUICC 器具首先驗證其同級 eUICC 器具正依據已同意並可靠的協定而操作。假如 eUICC 器具兩者均同意，接著，當來源 eUICC 器具轉以其 eSIM 時，該 eUICC 器具將刪除其 eSIM（或者否則使其本身的 eSIM 無效）。目的地 eUICC 器具將僅保留有效的 eSIM。

於本發明之第二形態，當存取控制用戶從一個移至另一個時，接收裝置發送一詰問或獨特識別符。於一實施例中，傳送裝置係使用接收裝置之公共金鑰以加密存取控制用戶並加入一獨特識別符或詰問，該加密的存取控制用戶及獨特識別符或詰問被進一步簽署。在傳輸之後，傳送裝置刪除其存取控制用戶。接收裝置驗證加密的存取控制用戶、及獨特的識別符；假如爲有效的，則加密的存取控制用戶及獨特的識別符被儲存以供未來使用。

於範例組態中，存取控制用戶僅被轉移於其符合標準可靠關係的裝置之間。以此方式，因爲兩裝置均依據一同意的協定而操作，所以存取控制用戶可於整個轉移期間保持獨特並保存的。再者，藉由確認其存取控制用戶僅對目的地裝置加密並從目前裝置刪除，介於其間的有害方無法破壞或擊敗轉移程序。

於此亦詳細地描述用於存取控制用戶之轉移的各種其他情境。

範例實施例之詳細描述

現在詳細地描述本發明之範例實施例和形態。雖然主要在 GSM、GPRS/EDGE、或 UMTS 蜂巢式網路的訂戶識別模組（SIM）之情境中討論這些實施例及形態，具有通常知識者將認知到本發明不如此受限。事實上，本發明之各種形態對可用於能受益自將存取控制用戶儲存和分配至裝置的任何網路中（無論是無線蜂巢式、或其他）。

亦將認知到雖在此使用術語「訂戶識別模組」（如 eSIM），此術語並不一定意味著或要求（i）由訂戶本身使用（亦即，本發明可由訂戶或非訂戶實行）；（ii）單一個體的識別（亦即，可替一群的個體（諸如家庭）或無形或虛構實物（諸如企業）實行本發明）；或（iii）任何有形「模組」設備或硬體。

先前技術訂戶身份模組（SIM）操作-

在先前技術 UMTS 蜂巢式網路的情境中，使用者設備（UE）包括行動裝置及通用訂戶識別模組（USIM）。USIM 爲儲存在實體通用積體電路卡（UICC）上或從其執行之邏輯軟體實物。各種資訊儲存在 USIM 中，諸如訂戶資訊，還有用於與網路業者鑑別以獲得無線網路服務的金鑰及演算法。於一實施例中，USIM 軟體係基於 Java Card 編程語言。Java Card 是 Java 編程語言之子集，其已被修改以用於嵌入式「卡」型裝置（諸如前述的 UICC）。其他實施方式可包括所謂的「本質」軟體實施方式，及/或其爲私有的實施方式，等等。

一般而言，在訂戶分配前先以 USIM 編程 UICC；預先編程或「個人化」爲每一個網路業者所特定的。例如，在佈署前，USIM 與一國際行動訂戶識別（IMSI）、一獨特積體電路卡識別符（ICC-ID）及一特定鑑別金鑰（K）關聯。網路業者將該關聯儲存在包含在網路的鑑別中心（AuC）內的註冊表中。在個人化之後，可分配 UICC 給訂戶。

現在參考圖 1，詳細地說明使用前述先前技術 USIM 之一範例鑑別及金鑰協定（AKA）程序。於正常鑑別程序期間，UE 從 USIM 獲取國際行動訂戶識別（IMSI）。UE 將 IMSI 傳遞至網路業者之服務網路（SN）或受訪的核心網路。SN 將鑑別請求遞送至家用網路（HN）之 AuC。HN 將所接收的 IMSI 比較與 AuC 之註冊表並獲得適當的 K。HN 產生一隨機數字（RAND）並使用一演算法而以 K 簽署之，來產生預期得回應（XRES）。HN 進一步產生加密金鑰（CK）及完整性金鑰（IK）以用於加密及完整性保護、還有一使用各種演算法之鑑別符記（AUTN）。HN 將一由 RAND、XRES、CK、及 AUTN 所組成之鑑別向量傳送至 SN。SN 儲存該鑑別向量以供僅用於一次性鑑別程序。SN 將 RAND 及 AUTN 傳遞至 UE。

一旦 UE 接收到 RAND 及 AUTN，USIM 驗證該接收的 AUTN 是否爲有效。假如是的話，則 UE 便使用該接收的 RAND 來計算其本身的回應（RES），其係使用所儲存的 K 及產生 XRES 的相同演算法。UE 將 RES 傳遞回至 SN。

SN 將 XRES 與該接收的 RES 做比較而假如其吻合的話，則 SN 便授權 UE 使用業者之無線網路服務。

圖 1 之前述程序被實施於 SIM 卡之實體媒體內。先前技術 SIM 卡具有至少兩（2）顯著且理想的特性：（i）SIM 卡提供 SIM 資料（例如，帳戶資訊、加密金鑰，等）之密碼安全的儲存，及（ii）SIM 卡無法被輕易地複製。

先前技術 SIM 卡包括形成於實體通用積體電路卡（UICC）中之處理器及記憶體。SIM 卡可用環氧樹脂填充以防止 UICC 上之資料信號的外部探測。假如想要的話，其他的干預防護結構可被包括於 UICC 中（例如，屏蔽層、遮罩層，等等）。SIM 卡具有通至處理器之一安全介面，且處理器具有通至記憶體之一內部介面。UICC 從外部裝置接收電力，其致能處理器執行來自記憶體組件之碼。記憶體組件本身非直接可存取的（亦即，內部檔案系統被隱藏自使用者），且必須經由處理器來存取。

於正常操作期間，處理器接受有限數目的指令。每一指令僅爲條件性可存取的。存取條件被侷限於指令之執行以防止未授權的存取。存取條件可以是或可以不是階層式的，例如，針對某一層級之授權不一定自動准予針對另一層級之授權。例如，一組存取條件可包括：（i）永遠可存取、（ii）永遠不可存取、（iii）可存取第一帳戶、（iv）可存取第二帳戶，等等。條件性存取僅在一適當安全性協定之成功完成後被准予。用以驗證識別之常見方法可包括密碼或個人識別數字（PIN）、共有秘密之詰問，等

等。

條件性存取、有限的指令集、及受保護的記憶體空間確保其 SIM 卡內所儲存之資訊是安全的不被外部存取。複製 SIM 卡將需要實體卡之建構、及內部檔案系統和資料之建構。這些特徵之結合使得實體 SIM 卡不受實際僞造企圖所影響。

電子訂戶識別模組（eSIM）操作-

附帶一提，此處所使用之術語「保存」、「保存」及「保存的」係指稱一無法被簡單地增加或縮減的元件（無論是實體或虛擬的）。例如，一被保存的 eSIM 無法被拷貝或複製於正常操作期間。

此外，如此處所使用的，應用於一元件（無論是實體或虛擬的）之術語「獨特性」係指稱其使該元件爲具有一特定性質及/或特性之唯一元件的性質。例如，獨特的 eSIM 無法具有複製的 eSIM。

如此處所使用的，術語「安全性」係一般地指稱資料及/或軟體之保護。例如，存取控制資料安全性確保其關聯與一存取控制用戶之資料及/或軟體被保護以防被未授權的活動、及/或惡意第三方所竊盜、濫用、毀損、公開及/或篡改。

此外，如此處所使用者，術語「授權」通常指的是其指明使用者對於資源之存取。附帶一提，利用先前技術的實體 SIM 卡，使用者授權係以實體 SIM 卡擁有來實施；

實體卡代表對於存取網路資源之使用者的授權。例如，當實體 SIM 卡係從第一電話移動至第二電話時，假設其移動係由使用者所執行（且由使用者所暗示地授權）。於 eSIM 操作之背景下，需要類似的能力以供 eSIM 轉移之使用者授權。特別地，eSIM（以及網路）之「所有人」需確保其 eSIM 僅被轉移至合法的裝置。

一般而言，應理解其軟體較硬體更有彈性；例如，軟體易於複製、修改、及散佈。此外，相較於硬體同等物，軟體常可被製成較低價、電力效率更高、及實體上更小。因此，雖然傳統的 SIM 卡操作係利用諸如卡（UICC）等實體形狀因數，但目前研究領域係集中朝向軟體內之虛擬化 SIM 操作。然而，SIM 資料（例如，訂戶特定資訊，等）之敏感本質需要特殊的考量。例如，SIM 資料之各種部分對訂戶而言是獨特的，且應被小心地保護以防止惡意的第三方。再者，如先前所述，各 SIM 代表對於有限的網路資源之存取量的合約；因此，SIM 之複製、破壞、及/或回收利用需被管理以防止網路資源之利用的超過及/或不足、以及服務提供者費用或收入之轉移。因此，虛擬化的 SIM 應滿足下列性質：（i）安全性、（ii）獨特性、及（iii）保存。此外，此類性質應被理想地提供以一比得上現存網路設施之價格。

SIM 操作之起初解決方案係將一 UICC 模擬爲一虛擬的或電子的實物，諸如（例如）軟體應用程式，於下文中稱之爲電子通用積體電路卡（eUICC）。eUICC 能夠儲存

及管理一或更多 SIM 元件，於下文中稱之爲電子訂戶識別模組（eSIM）。然而，對於虛擬化 eSIM 操作之解決方式需提供對於已由先前技術 UICC 所提供之現有安全性能力的同等（假如非增進）安全性。此外，現存的設施需要用以實施虛擬化 eSIM 之保存的適當方法，以使得虛擬化 eSIM 之數目在整個網路中受控制（亦即，虛擬化 eSIM 不被複製、遺失，等等）。

考量圖 2 中所示之系統；系統 200 包括（i）數個 SIM 供應商 202、（ii）數個 SIM 提供伺服器（SPS）204（諸如那些共同擁有且同時審查中之 2010 年十一月 22 日所提出申請而案名爲「無線網路鑑別設備和方法」的美國專利申請案編號 12/952,082、及 2010 年十一月 22 日所提出申請而案名爲「用以供應訂戶識別資料於無線網路中之設備和方法」的美國專利申請案編號 12/952,089，其被併入於此以供參考）、及（iii）使用者設備（UE）206 之總數，其中各 UE 含有一安全 eUICC。下列討論描述用以從 SIM 供應商分配 eSIM 至安全 eUICC 之不同技術。

於第一技術中，UE 206 從任何 SPS 204 請求一 eSIM，且 SPS 從諸如 SIM 供應商 202（或者於其他情況下行動網路業者（MNO）、可靠服務管理者（TSM），等等）之可靠實物擷取一適當的 eSIM。於此方式中，SIM 供應商可輕易地控制 eSIM 之分配；每一新請求的 eSIM 僅由 SIM 供應商所確認。然而，因爲 SIM 供應商爲可散佈 eSIM 之唯一方，所以假如在短時期內有大量訂戶對 SIM 供應商提

出請求，則 SIM 供應商可能產生「瓶頸」（如暢銷產品釋出時所常見的）。類似地，SIM 供應商爲失敗的單一點。因此，於災難之情況，eSIM 發送將被完全地停止。

於第二技術中，各 SPS 204 從 SIM 供應商 202 擷取 eSIM 池，並將該 eSIM 池儲存於各 SPS 內（該 eSIM 池係針對各 SPS 而被複製）。之後，SPS 依請求而將 eSIM 分配至 UE 206。eSIM 僅可由安全 eUICC 所解密並使用。此分配的 SPS 伺服器模型不會被 SIM 供應商所壅塞。然而，此第二技術需要實質上更多的設施。明確地，SPS 之總數確保其並無複製的 eSIM 被分配。因此，每當 SPS 准許一 eSIM，則其他 SPS 需經由通訊鏈結 208 被告知以撤銷其複製的 eSIM。如此確保 eSIM 是獨特的（亦即，並無複製的 eSIM 已被分配）。用以保存介於 SPS 間之 eSIM 狀態資訊同步化的通訊爲網路設施上之主要流量。此外，緩慢網路連接或網路分裂可能進一步造成「競賽情況」。於電腦網路連接之情境下，競賽情況通常指的是由網路實物同步化之間的傳遞延遲所導致的資料危機。例如，不完美的同步化可能造成兩個（2）SPS 同時輸出相同的 eSIM（產生競賽情況）；此將導致 eSIM 被意外地仿製。

於又第三技術（未顯示）中，SPS 204 和 SIM 供應商 206 設施以某種方式結合。例如，SIM 供應商和 SPS 網路可被一起裝入一共同設備中並任意地彼此存取，或者被邏輯地編結。編結的設施之成功的操作需要介於 SIM 供應商與 SPS 網路業者之間的可靠商業關係，其可能是不受歡迎

的（例如，在商業利益衝突之情況下、由於法律上的反壟斷法，等等）。

每一前述技術需要極高的通訊管理費用以於轉移期間同步化各個網路實物。例如，當 eSIM 從 SPS 被成功地轉移至行動裝置時，各 SPS 需被告知其 eSIM 無法被再次轉移（以防止相同 eSIM 之多重傳遞，如前文所述者）。

方法 -

因此，本發明之各個形態有利地致能虛擬化的存取控制用戶操作及分配，其提供與先前技術解決方案（例如，基於實體卡的存取控制用戶）同等的及/或增進的能力。於一範例實施例中，自含的 SIM 提供服務（SPS）實物可配合其他同級 SPS 裝置而操作，其致能 SIM 提供之分配的同級模型（不同於從集中資料庫追蹤 eSIM 之集中模型、或者需要同級裝置間之同步化的分配技術）。此外，如此處更詳細地描述，本發明之實施例並非專用於任何特定的網路設施，且可彈性地適應差不多任何組態。

於本發明之一形態中，存取控制用戶僅可一次被儲存及轉移至一安全元件。於一實施例中，安全元件僅儲存從其他具有相同或相當的協定之安全元件所接收的存取控制用戶（稍後被更詳細地描述於此）。類似地，安全元件將存取控制用戶之轉移限制於其他具有相同或相當的協定之安全元件。例如，安全元件可將異動（transaction）限制於其他滿足安全性要求之安全元件。某些行動網路業者（

MNO）可用其裝置實施較其他 MNO 更高的安全性。於各個實施例中，安全元件可被認證以不同位準且存取控制用戶可能需要某一認證位準。於轉移程序期間，裝置移除其本身的存取控制用戶（或使其無效）。藉由確保其涉及轉移之兩用戶爲可靠實物並認同相同的協定，則存取控制用戶不會於轉移時被複製或消失。

附帶一提，安全元件可被實施爲執行來自受保護的儲存媒體之軟體的處理器或處理設備。於某些變異中，受保護的儲存媒體被加密以排除未授權的存取或篡改。此外，安全元件可被實體地硬化或保護以防存取至儲存媒體及/或安全處理器。實體硬化之常見範例可包括一實體殼或其他機構，其係準備來在未授權的存取嘗試之情況下自行破壞或者使裝置無法存取；及/或將電路嵌入樹脂或其他材料中以防外部的探查。

於某些實施例中，本發明之安全元件組態成進一步限制及/或監督/標記異常的存取。例如，於一實施例中，存取控制用戶之轉移或儲存至安全元件需要詰問回應及/或獨特識別符。不適當的詰問回應或不正確的識別符可能指示異常的/詐騙的活動。類似地，介於安全元件之間的異動被加密；因此不當加密的異動亦可能標記可疑的行爲。

現在參考圖 3，顯示一種依據本發明以儲存並轉移存取控制用戶之集中方法 300 的實施例。於一實施方式中，至少一裝置爲實施於硬體安全性模組（HSM）中之 eUICC 器具，該 HSM 可管理一或更多 eSIM 之儲存。於某些實施

例中，HSM 本地地儲存加密的 eSIM，或者替代地，加密 eSIM 以供儲存於遠端媒體（於某些情況下，不安全的檔案系統）上。於一替代實施方式中，至少一裝置爲實施於實體 SIM 卡形狀因數中之 eUICC 器具（例如，致能舊有形狀因數插座再使用）。於又另一替代方案中，至少一裝置爲硬化裝置，諸如包括一實施於安全元件中之 eUICC 器具的行動電話（亦即，安全元件無法被移除自該裝置而不破壞或者犧牲裝置之完整性）。

於方法 300 之步驟 302，來源裝置與目的地裝置同意一協定。於一實施例中，協定型式係根據（例如）以普通文字所識別之軟體的版本。於其他實施例中，協定型式是以其他方式編碼的初始通訊所固有的。例如，加密的 256 位元詰問可固有地指明一特定協定或一組協定，而未加密的詰問可固有地指明一不同的協定。於另其他實施例中，協定可根據復原程序。例如，於某些變異中，裝置可被登錄以一目錄服務，其中登錄包括諸如識別符、網路位址、支援的協定型式等資訊。

於一範例實施例中，協定型式是由互相信任的發送者機構所發送之簽署憑證來決定。數位憑證可包括（但不限定於）例如：（i）序號（用以獨特地識別憑證）、（ii）裝置被認證、（iii）用以產生簽名之簽名演算法、（iv）驗證資訊並簽署憑證之發送者、（v）有效性範圍（例如，有效自、有效直到，等等）、（vi）加密金鑰、及/或（vii）指印或驗證散列（用以驗證憑證之合法性）。數位憑

證是相關技術中眾所周知的，且將不會進一步描述。

於一此類變異中，互相信任的發送者機構爲啓動機構，例如，行動網路業者（MNO）、鑑別中心（AuC）。於其他變異中，互相信任的發送者機構爲可靠的第三方，例如，SIM 供應商、裝置製造商，等等。互相信任的發送者機構不需對兩裝置爲相同的。例如，於某些實施例中，系統可具有多數可靠的實物（例如，多數接受的 MNO、多數可靠的裝置製造商，等等）。此外，於某些系統中，可靠的實物可爲另一未知實物之信任的根源（例如，可靠的實物提供確認其未知實物亦可被信任）。此信任「鏈」可延伸跨越任意數目的中間裝置；各中間裝置被鏈接至其前任者之信任位準，其延伸至可靠的根源實物。

於其他範例中，eUICC 器具可支援其符合標準化規格等之任何器具裝置。類似地，爲了確保向後的相容性，eUICC 器具之未來化身亦可支援舊有的 eUICC 器具，等等。

可用裝置及/或可用裝置之已接受的協定可被儲存（例如）於一查找目錄服務中。此目錄服務型式應用是網路設施技術中所常見的。例如，多數器具陣列可被進一步匹配與一目錄服務伺服器，其係組態成提供每一該些器具之連接資訊。一請求者方（來源或目的地）可請求來自目錄服務之資訊。

於某些實施例中，協定係依據軟體版本或修訂版而被編碼。例如，裝置可驗證其他裝置爲一可接受的軟體版本

或修訂版。替代地，來源和目的地裝置可同意一非正式協定；例如，裝置可被要求動態地協商或決定一協定。於又其他實施例中，無須協定協商（亦即，僅支援單一轉移協定之系統）。

轉移協定可於轉移期間指明（尤其）詰問回應協定之型式、獨特識別符區段、轉移加密、存取控制用戶管理（例如，刪除程序、通知程序，等等）。如先前所述，爲了確保存取控制用戶之保存和獨特性性質被保留於轉移期間，存取控制用戶係針對目的地裝置而被加密，並刪除自該轉移裝置。例如，轉移協定可指明：（i）接收之通知是否需要、（ii）當傳輸失敗時是否允許再傳輸、（iii）再嘗試之可接受數目、及/或（iv）於何種條件下來源裝置可刪除加密的存取控制用戶。

應理解來源裝置可於任何時刻及/或於任何條件下刪除及/或撤銷加密的存取控制用戶，以便可能於各種情境下爲便利的或需要的。於某些實施例中，刪除可發生於轉移後之某時刻。此類實施例可特別用於大量轉移。另一方面，存取控制用戶可於轉移前之某被撤銷。類似地，於其他實施例中，亦可指明「有效性窗」以供轉移，以致可於一段被視爲有效的指定時間窗內完成一特定的轉移。

其他考量包括（尤其）裝置考量、及/或存取控制用戶考量。例如，某些裝置僅可允許接收或（傳輸）一存取控制用戶。於一此類實施方式中，行動裝置可被限制爲僅接收一 eSIM（一旦指定後，其無法被返回，等等）。另

一方面，某些裝置可僅被使用爲「一次」轉移（例如，用以提供 eSIM 一次的可拋棄式裝置）。於某些情況下，裝置可爲較同級裝置更加（或更不）安全的。例如，於一範例實施例中，使用者設備可具有較 eUICC 器具更強的安全性需求；eUICC 器具可經由其他措施（例如，安全設施等等）而被保護。安全的使用者設備亦可將 eSIM 轉移至較不安全的 eUICC 器具，假設其較不安全的 eUICC 器具實施最低位準的安全性。類似地，於某些情況下，存取控制用戶具有轉移限制，包括（但不限定於）（i）所允許的轉移總數、（ii）目的地裝置限制，等等。

此外，應理解其通訊方法對於轉移協定考量可能具有顯著的影響。網路設施轉移可使用高帶寬的協定及媒體（例如，T3、T1、Sonet（同步光學網路）、Gigabit Ethernet 等等），而基於消費者的轉移可被執行於較低的帶寬連接（例如，蜂巢式存取、WLAN（無線局部區域網路）、Ethernet 等等）。不同的使用情境亦可具有針對交握、轉移時間需求等不同的需求。例如，SIM 供應商可將大量 eSIM 轉移至 eUICC 器具（例如，諸如用以協助 SIM 傳遞或其他功能）。類似地，於另一範例中，eSIM 之一集中的大型貯藏庫可被任意地轉移於數個 eUICC 器具之間。eUICC 器具可任意地從器具至器具轉移 eSIM，以協助負載管理，等等。這些大量轉移情境之交握需求較不重要，因爲 eSIM 並非在流通中（可於轉移結束時將通知歸併在一起，而非僅針對各單獨的 eSIM）。

消費者應用可具有更低的轉移率，但交握是更重要的，因爲 eSIM 應被健全地傳遞，並立即可供使用。於某些變異中，無法完成交握程序將自動地觸發一再嘗試。例如，eUICC 器具、SIM 供應伺服器（SPS）、或類似實物可直接地轉移一 eSIM 以服務一來自使用者設備（UE）之即興 eSIM 請求、或者一執行來自桌上型或可攜式電腦之應用程式。於另一此類範例中，基於消費者之應用程式可執行一能夠儲存一或更多 eSIM（例如，一個用於工作、一個用於個人使用、數個用於漫遊存取，等等）之小型內化器具，其致能消費者將 eSIM 轉移於其各個裝置之間。

於圖 3 之方法 300 的步驟 304，來源和目的地裝置建立一共有的秘密。於一範例實施例中，裝置係藉由檢查數位簽名以驗證同級裝置識別，而假如該簽名爲有效，則交換（或同意交換）詰問、獨特識別符、或其他安全性符記，以供加密與存取控制用戶。

例如，裝置可利用一詰問及回應型式交握；其中任何可靠裝置知道一共同秘密（例如，共同金鑰、一組金鑰，等等），其可被用以產生數個詰問和相關的回應。裝置可信任一未知的裝置，假設其可產生適當的詰問、及/或適當的回應。

於另一範例中，裝置可利用由具有存取控制用戶請求之目的地裝置所產生的獨特識別符。來源裝置包括具有存取控制用戶之獨特識別符以識別該服務的請求。

於又其他實施例中，裝置可用一可靠的第三方來驗證

其同級裝置（例如，可靠的第三方提供一對話金鑰給每一裝置）。此關係可被直接或間接地驗證。例如，同級裝置可在執行轉移之前直接地詢問可靠的第三方，或者另一方面各裝置可提呈一由靠的第三方所簽署之憑證。

在本發明之背景下，熟悉本項技術人士將理解利用本發明之又其他型式的密碼配置及信任情境。

於步驟 306，來源裝置將存取控制用戶與秘密（例如，詰問、獨特識別符、或其他安全性符記）包裝在一起。於一範例實施例中，該包裝係使用目的地裝置之公共金鑰而被額外地加密。於一變異中，來源裝置需首先以其本身的私人金鑰來解密該存取控制用戶，於再加密該存取控制用戶之前。

一旦以目的地裝置之公共金鑰來加密後，僅有該目的地裝置可解密該存取控制用戶以供使用。用以轉移存取控制用戶之公共及私人金鑰加密的一範例係描述於 2010 年十月 28 日所提出申請而案名爲「用於存取控制用戶之儲存及執行的方法和設備」的美國臨時申請案編號 61/407，866（併入於此以供參考）。例如，各 eUICC 器具具有一獨特的裝置公共/私人金鑰對及背書憑證。公共/私人金鑰對係根據一秘密私人金鑰、及一可公開的公共金鑰。公共/私人金鑰技術被視爲「非對稱」，由於用以加密與解密之金鑰不同，而因此加密器與解密器並未共用相同的金鑰。

進一步瞭解其步驟 306 和 304（尤其）可被進一步結

合、次分割、及/或反轉。例如，於一實施例中，來源裝置決定一對話金鑰，並以該對話金鑰加密該存取控制用戶，所得的包裝被進一步包覆以目的地裝置之公共金鑰。於一此類變異中，對話金鑰係由目的地裝置於接收之時刻所決定。

此外，於某些實施例中，包裝被進數位地簽署以提供來源裝置之進一步驗證。目的地裝置可檢查該數位簽名，以驗證其包裝（例如，存取控制用戶及獨特識別符，等等）是源自來源裝置。此外，已輕易理解其數位簽名僅爲電子簽名之一子集，因此可類似地利用其他形式的來源驗證，包括（但不限定於）：使用者識別（密碼、生物辨識系統，等等）、電子識別，等等。

於步驟 308，已包裝的存取控制用戶係從來源被轉移至目的地裝置。目的地裝置驗證共有的秘密，而假如驗證成功，則儲存加密的存取控制用戶以供未來使用。於一實施例中，存取控制用戶被刪除、撤銷、或者除此之外使其變爲不可用，於來源裝置上，在致能目的地裝置之存取控制用戶前（例如，在轉移前、在完成轉移前、在通知轉移成功前，等等）。

範例操作-

當作依據本發明之典型操作的一範例，於初始化期間，SIM 供應商提供 eSIM 之集合或「批（lot）」給 eUICC 器具。注意：多數 SIM 供應商（及）可獨立地提供 eSIM

；在 SIM 供應商方面並無必要的合作（雖然此合作亦可被使用，假如需要的話）。SIM 供應商進一步以針對 eUICC 器具之一詰問或獨特識別符來加密每一 eSIM。

如先前所述，各 eSIM 包括一虛擬的 SIM 和獨特的金鑰關聯與能力以執行前述的鑑別及金鑰協定（AKA）技術，來爲蜂巢式網路鑑別一行動裝置（參見前述**先前技術訂戶識別模組（SIM）操作**之討論）。此外，各 eSIM 係獨特地關聯與一依每次轉移而改變的詰問或識別符。詰問或識別符之典型的實施方式可包括密碼材料、計數器、僞隨機序列、大型狀態機器，等等。

考量下列操作-第一 eUICC 器具起始 eSIM 轉移（其目前是針對第一 eUICC 器具而加密）至第二 eUICC 器具。第一 eUICC 器具起始安全通訊至第二 eUICC 器具。於一情境中，第一和第二 eUICC 器具均根據由一或更多互相信任的第三方所簽署之憑證而同意該轉移。第二 eUICC 器提供獨特識別符給第一 eUICC 器具。第一 eUICC 器具以其本身的私人金鑰來解密該 eSIM，並接著以第二 eUICC 之公共金鑰來再加密該 eSIM（公共金鑰是由第二 eUICC 所任意地分配）。獨特識別符與再加密之 eSIM 的組合係由第一 eUICC 器具所簽署（該簽名係驗證第一 eUICC 器具之識別）。該簽署的組合被包裝給第二 eUICC。現在，僅有第二 eUICC 可解密該 eSIM，且該簽署的組合證明其加密的 eSIM 包裝係相應於獨特識別符。第一 eUICC 器具將新加密的 eSIM 傳輸至第二 eUICC 器具。

於一實施例中，獨特識別符被用以保護不受重播攻擊。例如，各 eSIM 轉移被獨特地識別，因此異動無法被「複製」及播放（例如，由惡意的第三方）。例如，當從器具 A 轉移 eSIM 至器具 B 時，且接著從器具 B 轉移至器具 C，則介於器具 A 至器具 B 之間的轉移無法被重播而 eSIM 仍於器具 C 之上。

類似地，考量從第一 eUICC 器具轉移 eSIM 至行動裝置。行動裝置以一詰問發送針對一 eSIM 之請求、及其公共金鑰。第一 eUICC 器具以其本身的私人金鑰解密 eSIM，並產生一適當的詰問回應。eSIM 係以行動裝置之公共金鑰來被再加密。再加密的 eSIM 被結合與一詰問回應，並接著簽署。行動裝置驗證該詰問回應（其識別第一 eUICC 器具爲一合法來源），而假如成功便解密該 eSIM 以供使用。即使一惡意的第三方可攔截加密的 eSIM，其將無法使用或篡改該 eSIM（因爲該 eSIM 已被加密）。

最後，考量從第一行動裝置轉移 eSIM 至第二行動裝置。第一行動裝置推出一請求以將其 eSIM 轉移至第二行動裝置。於一情境下，第一或第二行動裝置之任一者的使用者需手動地接受該轉移。假如接受的話，第二行動裝置便傳輸一詰問至第一行動裝置。第一行動裝置以其本身的私人金鑰來解密其儲存之加密的 eSIM，接著以第二行動裝置之公共金鑰來再加密該 eSIM（第二行動裝置之公共金鑰爲永遠可得的），包括適當的回應。該組合被簽署，並傳輸。第二行動裝置驗證該詰問回應（其識別第一行動

裝置爲一合法來源），並解密該 eSIM 以供使用。

設備 -

現在詳細地描述可配合上述方法而使用的各種設備。

eUICC 器具

圖 4 說明依據本發明之 eUICC 器具 400 的一範例實施例。eUICC 器具可包含一獨立實物，或結合與其他網路實物（例如，服務供應服務（SPS），等等）。如圖所示，eUICC 器具 400 一般包括一網路介面 402，用以交流與通訊網路、處理器 404、及一儲存設備 408。網路介面係顯示爲連接至 MNO 設施，以提供對於其他 eUICC 器具之存取、及對於一或更多行動裝置之直接或間接存取，雖然其他的組態及功能可被取代。

於一組態中，eUICC 器具爲硬體安全性模組（HSM）。HSM 包括一或更多安全元件，用以管理數個存取控制用戶。於某些實施例中，存取控制用戶被直接地儲存於 HSM 上。另一方面，存取控制用戶被加密並儲存於外部儲存中。於此外部（例如，遠端）儲存實施例中，加密確保其存取控制用戶是安全的，即使當儲存於實體上不安全的媒體上時。

HSM 被組態成致能存取控制用戶之轉移至和自另一 HSM，同時維持存取控制用戶之獨特及保存。此外，於本實施例中存取控制用戶至另一 HSM 之轉移造成本地儲存

之存取控制用戶的撤銷及/或刪除。HSM 亦可被組態成假如被篡改的話便自行毀損。

於圖 4 所示之實施例中，eUICC 器具 400 包括至少一運行於處理器 404 上之 SIM 資料庫 410。雖顯示爲運行於 eUICC 器具上之單一應用程式，應理解其前述資料庫功能性可包含一運行於彼此間資料通訊之複數裝置上的分散式應用程式。

SIM 資料庫應用程式處理包括如下之請求：（i）儲存 eSIM 之請求、（ii）轉移目前儲存之 eSIM 的請求。資料庫應用程式亦負責驗證請求以確保其通訊係接收自一被授權做出此一請求之實物（參見步驟 304，如前文所討論的）。

於一實施例中，SIM 資料庫應用程式被組態成執行詰問及回應安全性協定。詰問/回應安全性協定被組態成驗證由未知的第三方所做出之請求，根據詰問及/或回應之適當產生。另一方面，於另一實施例中，安全元件可驗證一由可靠管理機構所簽署的數位憑證。

如圖所示，儲存設備 408 適於儲存存取控制用戶之陣列。於一實施例中，eUICC 器具儲存 eSIM 之陣列。於一此類實施方式中，各 eSIM 包括小型檔案系統，其包括電腦可讀式指令（eSIM 程式）及相關資料（例如，密碼金鑰、完整性金鑰，等等）。此外，各 eSIM 係額外地以 eUICC 器具之公共金鑰來加密。因此，各 eUICC 僅可由 eUICC 器具所解密。於某些實施例中，各加密的 eSIM 被

進一步以一獨特識別符、詰問、或詰問回應來加密。於某些實施例中，加密的組件被進一步儲存爲二進制大型物件（BLOB）。

SIM 資料庫應用程式被組態成管理可用的 eSIM。如圖 4 中所示，資料庫可提供關於特定 eSIM BLOB 之資訊、被授權可使用 eSIM 之裝置、eSIM 之目前狀態、及/或 eSIM 之目前狀況（「可用」、「不可用」、「過時」等等）。亦可維持額外的資訊。資料庫應用程式被組態成更新或改變資料庫中所儲存之資訊。

當另一裝置從 eUICC 器具 400 請求一 eSIM 時，資料庫應用程式便擷取所請求之 eSIM 的目前狀態。此資訊可被用以判斷該請求之 eSIM 是否可被提供。此有效性檢查可被執行於啓動服務上、於 eUICC 器具上、被共用、或者發生於其他位置；例如，藉由將啓動服務上之狀態比較與 eUICC 器具上之最後已知狀態。類似地，當另一裝置將一 eSIM 轉移至 eUICC 器具 400 時，資料庫應用程式便負責更新該轉移之 eSIM 的目前狀態。

使用者設備-

現在參考圖 5，說明依據本發明之各個形態的使用者設備 500（例如，UE）。

圖 5 之範例 UE 設備爲具有處理器子系統 502（諸如數位信號處理器、微處理器、場可編程閘陣列、或安裝於一或更多基底上之複數處理組件）之無線裝置。處理子系

統亦可包含一內部快取記憶體。處理子系統係通連與一包括記憶體之記憶體子系統 504，其可（例如）包含 SRAM、快閃、及/或 SDRAM 組件。記憶體子系統可實施一或更多 DMA 型的硬體，以協助資料存取，如本技術中眾所週知的。記憶體子系統含有其可由處理器子系統所執行的電腦可執行指令。

於一範例實施例中，裝置可包括一或更多適於連接至一或更多無線網路的無線介面 506。藉由實施適當的天線和數據機子系統，多種無線介面可支援不同的無線電科技，諸如 GSM、CDMA、UMTS、LTE/LTE-A、WiMAX、WLAN、藍牙，等等。

使用者介面子系統 508 包括任何數目的已知 I/O，包括（不限定於）：鍵盤、觸控螢幕（例如，多點觸控介面）、LCD 顯示、背光、揚聲器、及/或麥克風。然而，已瞭解於某些應用中，可將一或更多這些組件排除。例如，PCMCIA 卡型式的用戶實施例可能缺乏使用者介面（因爲其可裝附於實體地及/或電氣地耦合至主機裝置之使用者介面上）。

於所示之實施例中，裝置包括安全元件 510，其含有及操作 eUICC 應用程式。eUICC 能夠儲存並存取複數存取控制用戶以用於與網路業者之鑑別。安全元件包括（於本實施例中）執行安全媒體中所儲存之軟體的安全處理器。安全媒體無法被所有其他組件（除了安全處理器之外）所存取。此外，安全元件可被進一步硬化以防止篡改（例如

，封入樹脂內），如先前所描述者。

安全元件 510 能夠接收並儲存一或更多存取控制用戶。於一實施例中，安全元件儲存複數與一使用者相關的 eSIM 之陣列（例如，一個用於工作、一個用於個人、數個用於漫遊存取，等等），及/或依據另一邏輯技術或關係（例如，一個用於家庭或商業實物之多數成員的每一者、一個用於該家庭之成員的個人及工作使用之每一者，等等）。各 eSIM 包括一小型檔案系統，其包括電腦可讀式指令（eSIM 程式）、及相關資料（例如，密碼金鑰、完整性金鑰，等等）。

安全元件進一步適於致能 eSIM 之轉移至及/或自行動裝置。於一實施例中，行動裝置提供 GUI 基的確認以起始 eSIM 之轉移。

再者，範例實施例之各種實現包括指令，其（當執行時）開始詰問/回應安全性協定。詰問回應安全性協定組態成驗證由未知的第三方所做出的請求，根據詰問及/或回應之適當產生。另一方面，於一範例實施例中，安全元件可驗證由可靠管理機構所簽署的數位憑證。

此外，於一實施例中，安全元件維持所儲存之存取控制用戶的表列或清單。清單可包括關於所儲存之存取控制用戶的目前狀態之資訊；此資訊可包括（例如）可用性、完成、有效性、及/或先前經歷的錯誤。清單可被進一步鏈結或耦合至使用者介面，以致能可用的存取控制用戶之使用者選擇。

於一範例實施例中，安全元件具有相關的裝置密碼金鑰。這些裝置金鑰被用以確保存取控制用戶之交換。於一此類變異中，加密金鑰爲非對稱公共/私人金鑰對。公共金鑰可被任意地分配而無需犧牲私人金鑰之完整性。例如，裝置可被指定（或內部地產生）一 RSA 公共/私人金鑰；公共金鑰被變得可用於後部署通訊。

應理解雖以方法的步驟之特定序列描述本發明之某些形態，這些說明僅爲本發明之較廣義方法的例示而已，且可隨特定應用所需而修改。在某些情況下某些步驟可能變得不必要或選擇性。額外地，可添加某些步驟或功能至揭露的實施例，或可置換兩或更多個步驟的履行順序。所有這種變異視爲包括在於此所揭露及主張專利權的本發明內。

雖然上述詳細說明已顯示、描述、及指出應用至各種實施例的本發明之新穎特徵，將可了解到可由熟悉此技藝人士做出所解釋之裝置或程序的形式及細節上的各種省略、替代、及改變而不背離本發明。上述說明爲目前認爲係進行本發明之最佳模式。此說明絕不意爲限制性，而應視爲本發明之通用原則的例示。應參照申請專利範圍來判定本發明之範圍。

【圖式簡單說明】

圖 1 係圖示地說明使用先前技術 USIM 之範例鑑別及金鑰協定（AKA）程序。

圖 2 係一可用於分配存取控制用戶的範例網路架構之方塊圖。

圖 3 係一邏輯流程圖，其說明一種依據本發明以將存取控制用戶轉移至裝置的一般性方法之一實施例。

圖 4 係一方塊圖，其說明依據本發明之一 eUICC 器具的一實施例，該 eUICC 器具適於儲存一或更多存取控制用戶。

圖 5 係一方塊圖，其說明依據本發明之一行動裝置的一實施例，該行動裝置適於儲存並使用一或更多存取控制用戶。

【主要元件符號說明】

200：系統

202：SIM 供應商

204：SIM 提供伺服器

206：使用者設備

208：通訊鏈結

400：eUICC 器具

402：網路介面

404：處理器

408：儲存設備

410：SIM 資料庫

500：使用者設備

502：處理器子系統

504：記憶體子系統

506：無線介面

508：使用者介面子系統

510：安全元件

103. 9. 25

年 月 日修正替換頁

七、申請專利範圍：

1. 一種經組態以提供存取資料元件至同級裝置之設備，包含：

一適於儲存複數個存取資料元件之第一安全元件；及

一處理器，其中該處理器經組態以：

從一同級裝置接收該複數個存取資料元件之至少一存取資料元件的一請求，其中該請求包括：

一公共金鑰，其對於包括於該同級裝置中之一第二安全元件係獨特的，及

一獨特識別符，其係藉由與該請求相關聯之該同級裝置而產生；

從該第一安全元件獲得該至少一存取資料元件；

產生包括該至少一存取資料元件及該獨特識別符之一包裝(package)；

使用該公共金鑰加密該包裝；及

將該經加密的包裝轉移至該同級裝置。

2. 如請專利範圍第 1 項之設備，其中該複數個存取資料元件之每一存取資料元件係與一行動網路業者(MNO)關聯。

3. 如申請專利範圍第 1 項之設備，其中該複數個存取資料元件之每一存取資料元件係與一使用者關聯。

4. 如申請專利範圍第 1 項之設備，其中該複數個存取資料元件之每一存取資料元件係與相同使用者之一不同使用情況關聯。

5. 如申請專利範圍第 1 項之設備，其中該處理器進一步經組態以在從該同級裝置接收該請求之前與該同級裝置協商一轉移協定。

6. 如申請專利範圍第 5 項之設備，其中該處理器進一步經組態以基於該經協商之轉移協定加密該經加密之包裝。

7. 如申請專利範圍第 6 項之設備，其中協商該轉移協定包含識別該轉移協定係由該設備及該同級裝置所支援。

8. 如申請專利範圍第 1 項之設備，其中該處理器進一步經組態以識別該至少一存取資料元件已在不同的裝置之間轉移之次數。

9. 如申請專利範圍第 8 項之設備，其中該處理器進一步經組態以在驗證該次數滿足一預定臨限值之後，立即轉移該經加密之包裝。

10. 如申請專利範圍第 1 項之設備，其中該複數個存取資料元件之每一存取資料元件係一電子訂戶識別模組（eSIM）。

11. 如申請專利範圍第 1 項之設備，其中該設備係一硬體安全性模組（HSM）。

12. 一種行動裝置，包含：

一安全元件；及

一處理器，其中該處理器經組態以：

發送複數個存取資料元件之至少一存取資料元件

的一請求至一種經組態以儲存該複數個存取資料元件之設備，其中該請求包括：

一公共金鑰，其對於該安全元件係獨特的，及

一獨特識別符，其係與發送該請求相關聯而產生；及

回應該請求：

從該設備接收一包裝，其中使用該公共金鑰加密該包裝，且該包裝包括該至少一存取資料元件及該獨特識別符。

13. 如申請專利範圍第 12 項之行動裝置，其中在該設備驗證該至少一存取資料元件已經轉移之次數滿足一特定臨限值之後，從該設備接收該包裝。

14. 如申請專利範圍第 12 項之行動裝置，其中該複數個存取資料元件之每一存取資料元件係一電子訂戶識別模組（eSIM）。

15. 一種用以轉移存取資料元件至同級裝置之方法，包含：

在包括儲存複數個存取資料元件之一第一安全元件之一設備處：

從一同級裝置接收該複數個存取資料元件之至少一存取資料元件的一請求，其中該請求包括：

一公共金鑰，其對於包括於該同級裝置中之一第二安全元件係獨特的，及

一獨特識別符，其係藉由與該請求相關聯之該同

級裝置而產生；

從該第一安全元件獲得該至少一存取資料元件；

產生包括該至少一存取資料元件及該獨特識別符之一包裝；

使用該公共金鑰加密該包裝；及

將該經加密的包裝轉移至該同級裝置。

16. 如申請專利範圍第 15 項之方法，其中該複數個存取資料元件之每一存取資料元件係與一行動網路業者(MNO)關聯。

17. 如申請專利範圍第 15 項之方法，其中進一步包含在從該同級裝置接收該請求之前與該同級裝置協商一轉移協定。

18. 如申請專利範圍第 15 項之方法，進一步包含識別該至少一存取資料元件已在不同的裝置之間轉移之次數。

19. 如申請專利範圍第 18 項之方法，其中在驗證該次數滿足一預定臨限值之後，立即轉移該經加密之包裝。

20. 如申請專利範圍第 15 項之方法，其中進一步包含識別與該同級裝置關聯之裝置限制。

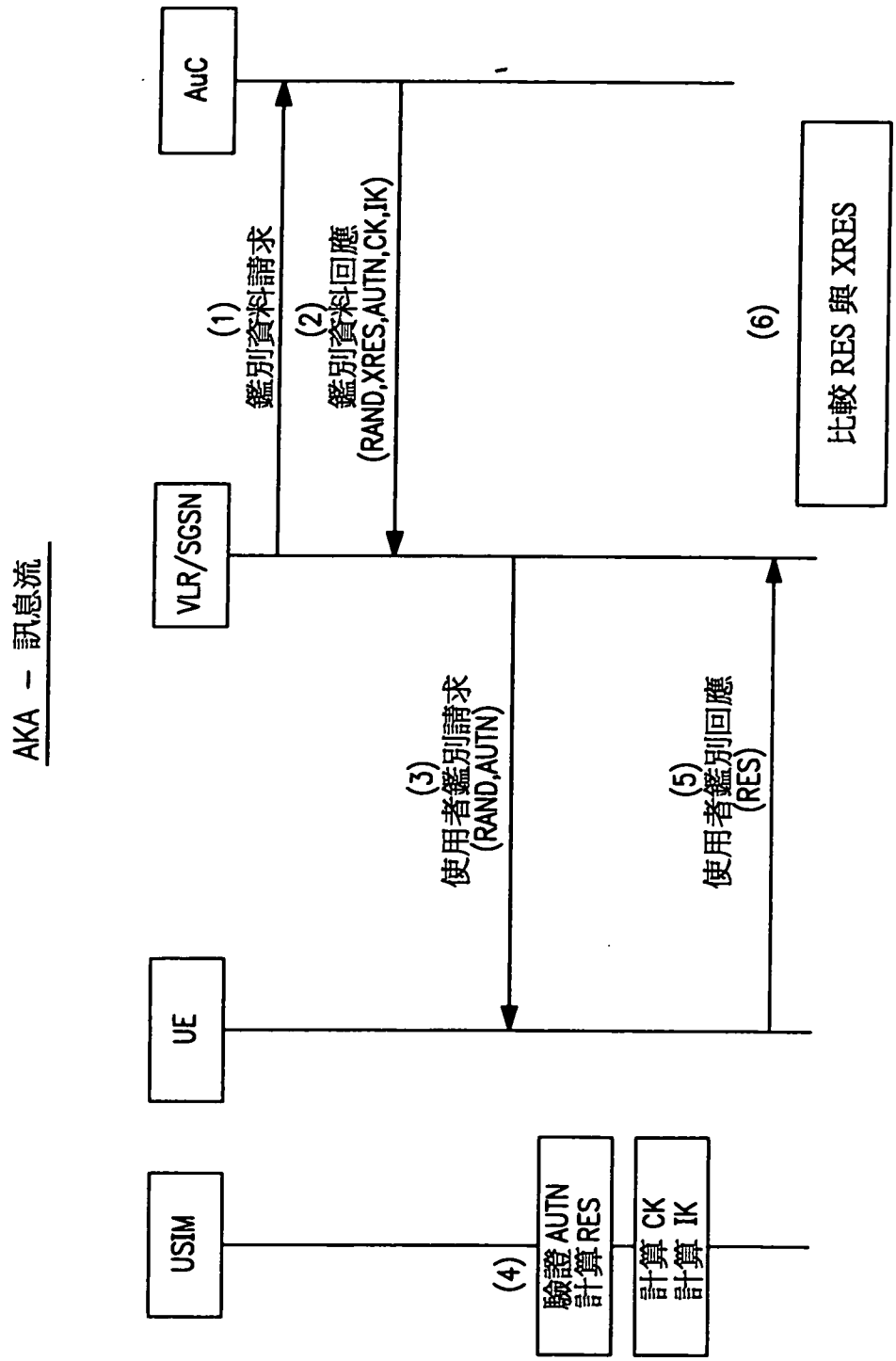
AKA – 訊息流
AuC
VLR/SGSN
UE
USIM
(1)
鑑別資料請求
(2)
鑑別資料回應
(RAND,XRES,AUTN,CK,IK)
(3)
使用者鑑別請求
(RAND,AUTN)
(4)
驗證 AUTN
計算 RES
計算 CK
計算 IK
(5)
使用者鑑別回應
(RES)
(6)
比較 RES 與 XRES

圖 1
（先前技術）

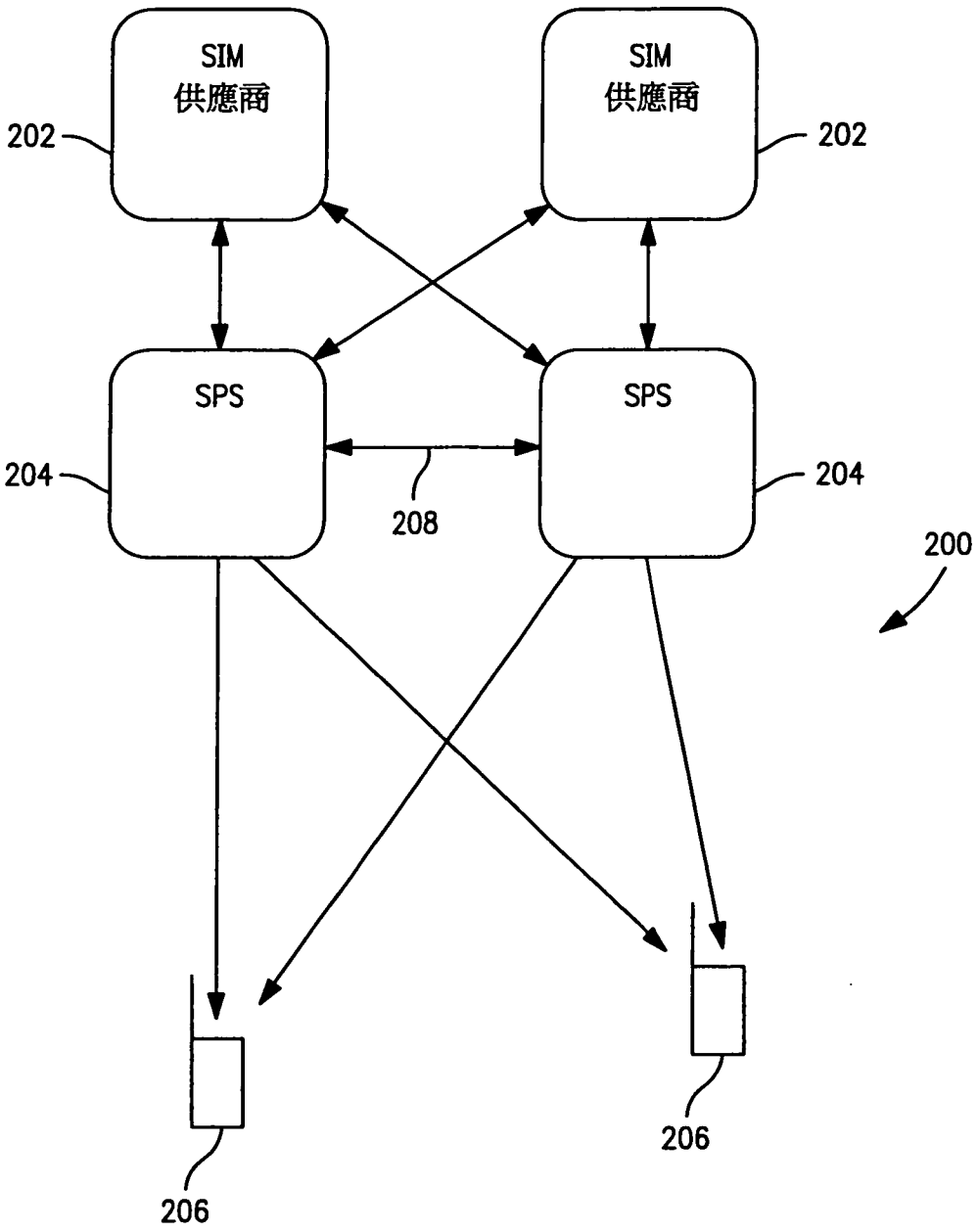

圖2

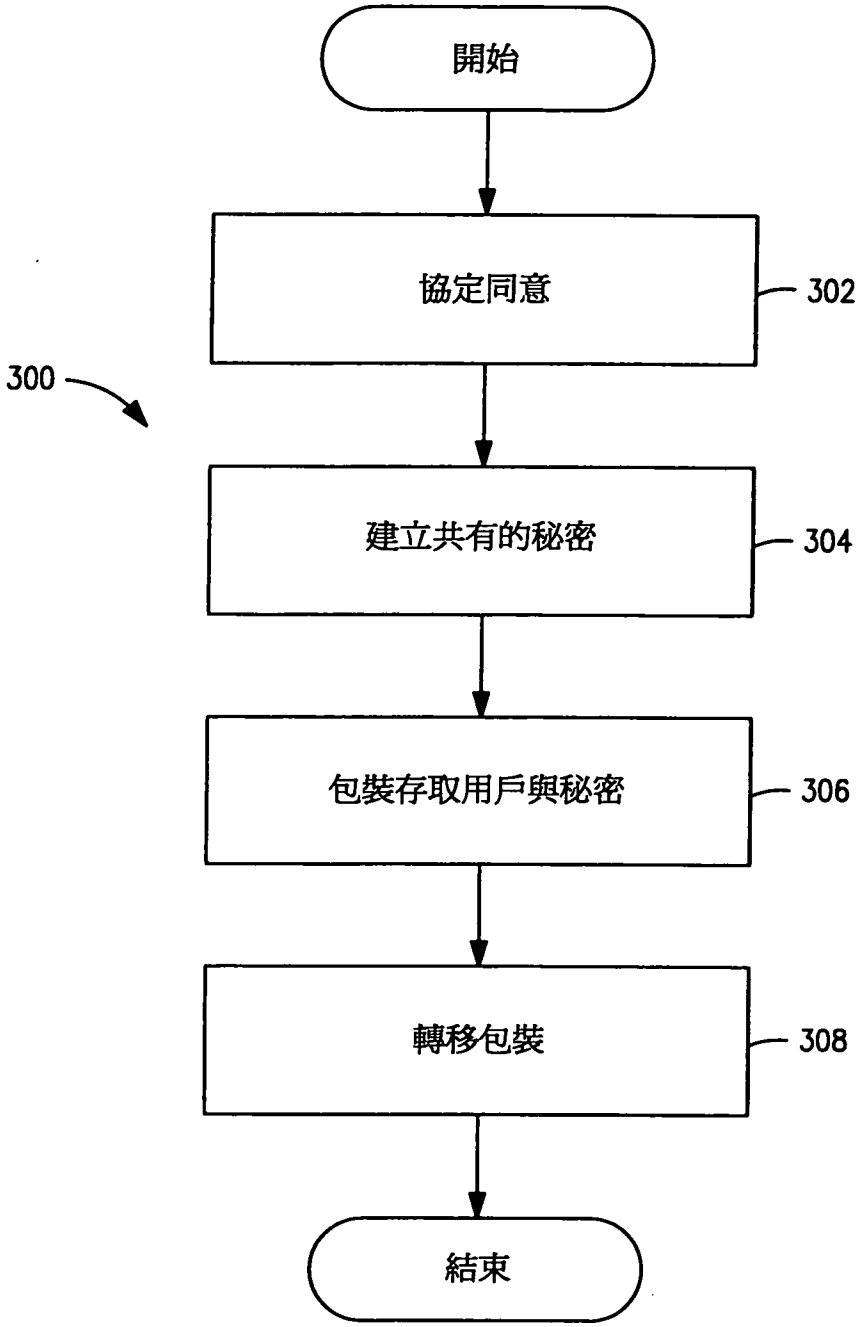

圖3

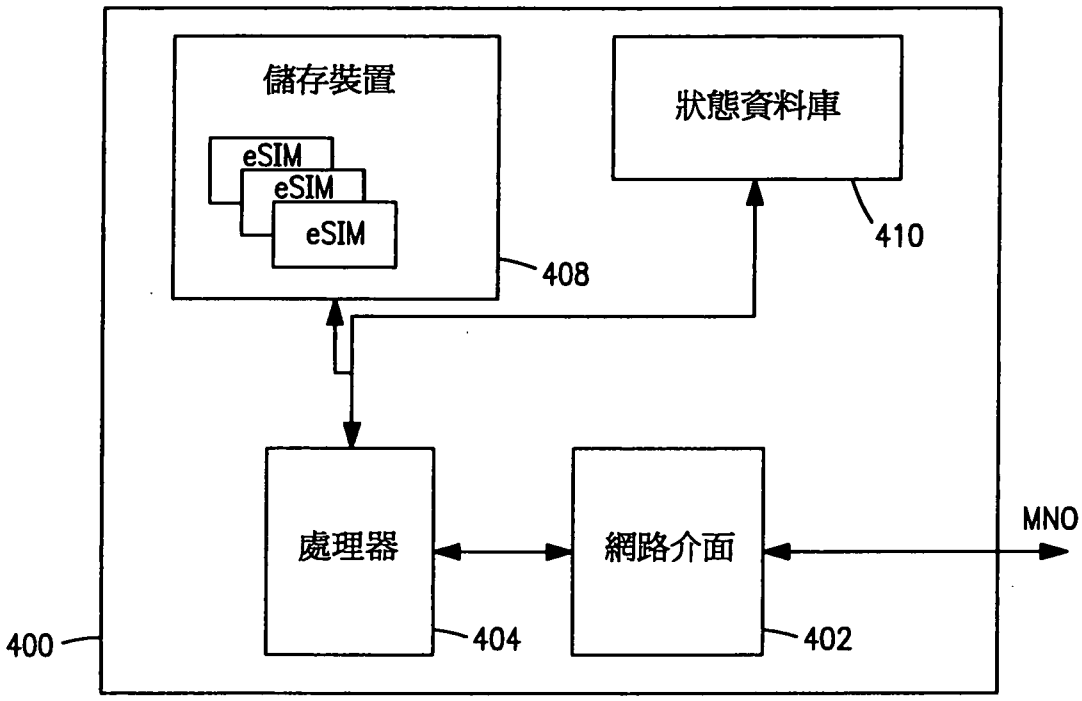

圖4

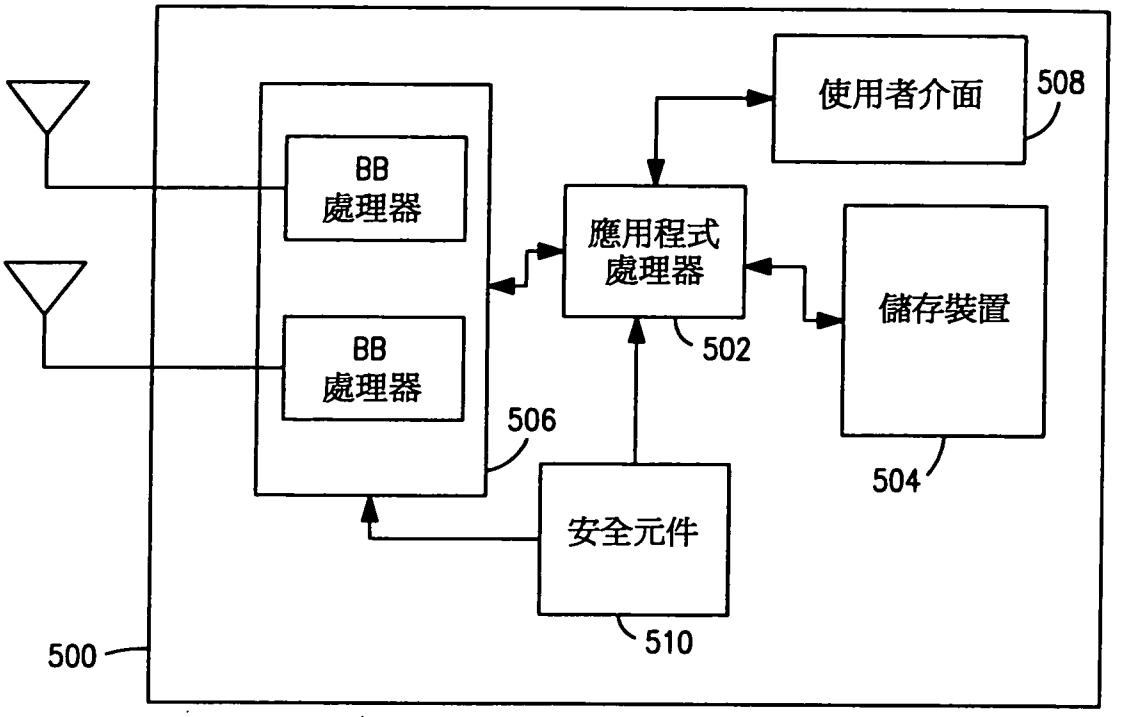

圖5