



(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 I573473 B

(45)公告日：中華民國 106 (2017) 年 03 月 01 日

(21)申請案號：104117238

(22)申請日：中華民國 104 (2015) 年 05 月 28 日

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

H04L9/32 (2006.01)

H04M1/2745 (2006.01)

H04W8/18 (2009.01)

(30)優先權：2014/05/30 美國

62/005,185

(71)申請人：蘋果公司(美國) APPLE INC. (US)

美國

(72)發明人：楊 翔英 YANG, XIANGYING (US) ; 李 莉 LI, LI (US)

(74)代理人：陳長文

(56)參考文獻：

US 2004/0151135A1

US 2012/0260086A1

US 2012/0331292A1

US 2031/0227646A1

審查人員：王紋星

申請專利範圍項數：18 項 圖式數：7 共 37 頁

(54)名稱

在無線通訊裝置中之電子用戶識別模組的安全儲存

SECURE STORAGE OF AN ELECTRONIC SUBSCRIBER IDENTITY MODULE ON A WIRELESS COMMUNICATION DEVICE

(57)摘要

本發明提供一種用於一電子用戶識別模組(eSIM)在一無線通訊裝置上之安全儲存的方法，該無線通訊裝置包括一嵌入式通用積體電路卡(eUICC)及在該 eUICC 外部之一記憶體。該方法可包括該 eUICC 判定包括一 eSIM 之一 eSIM 套件待儲存於該記憶體上。該方法亦可包括回應於判定該 eSIM 套件待儲存於該記憶體上，該 eUICC 維護與該 eSIM 套件相關聯之一單次用工作階段參數以使得能夠在該 eSIM 套件稍後自該記憶體載入至該 eUICC 上之情況下將該 eSIM 安裝於該 eUICC 上。

A method for secure storage of an electronic Subscriber Identity Module (eSIM) on a wireless communication device including an embedded Universal Integrated Circuit Card (eUICC) and a memory external to the eUICC is provided. The method can include the eUICC determining that an eSIM package including an eSIM is to be stored on the memory. The method can also include the eUICC, in response to determining that the eSIM package is to be stored on the memory, maintaining a single-use session parameter associated with the eSIM package to enable installation of the eSIM on the eUICC if the eSIM package is later loaded onto the eUICC from the memory.

指定代表圖：

600

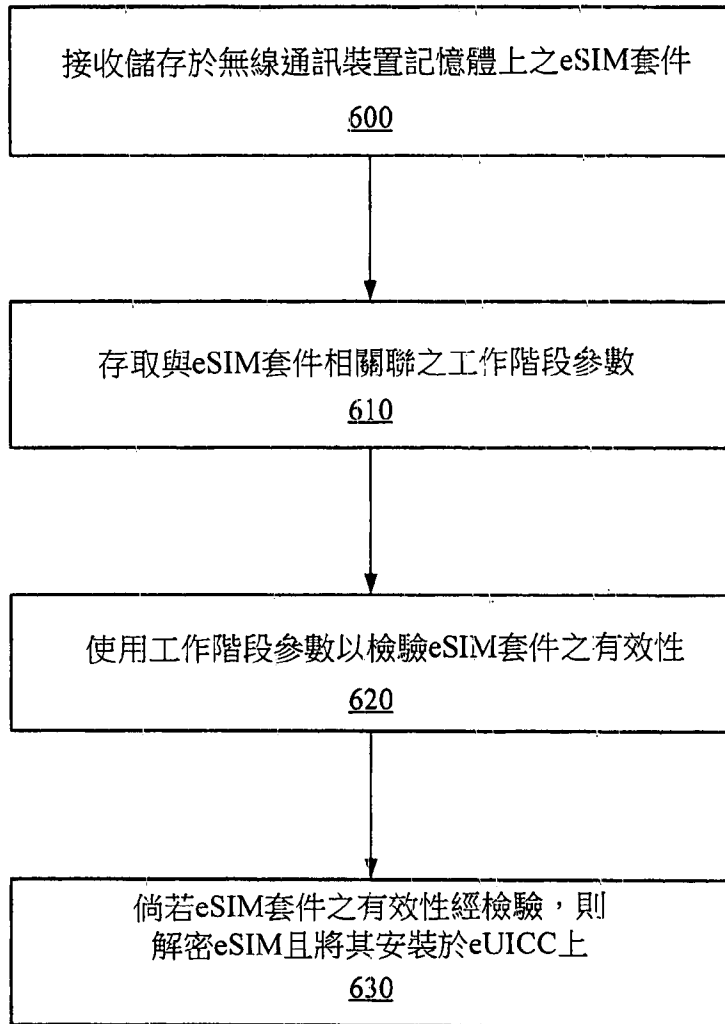
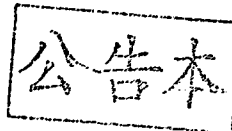


圖6



發明摘要

H04W 12/06 (2009.01)

※ 申請案號：104 117238

H04L 9/32 (2006.01)

※ 申請日：104. 5. 28

※IPC 分類：H04M 1/245 (2006.01)

H04W 8/18 (2009.01)

【發明名稱】

在無線通訊裝置中之電子用戶識別模組的安全儲存

SECURE STORAGE OF AN ELECTRONIC SUBSCRIBER

IDENTITY MODULE ON A WIRELESS COMMUNICATION

DEVICE

【中文】

本發明提供一種用於一電子用戶識別模組(eSIM)在一無線通訊裝置上之安全儲存的方法，該無線通訊裝置包括一嵌入式通用積體電路卡(eUICC)及在該eUICC外部之一記憶體。該方法可包括該eUICC判定包括一eSIM之一eSIM套件待儲存於該記憶體上。該方法亦可包括回應於判定該eSIM套件待儲存於該記憶體上，該eUICC維護與該eSIM套件相關聯之一單次用工作階段參數以使得能夠在該eSIM套件稍後自該記憶體載入至該eUICC上之情況下將該eSIM安裝於該eUICC上。

【英文】

A method for secure storage of an electronic Subscriber Identity Module (eSIM) on a wireless communication device including an embedded Universal Integrated Circuit Card (eUICC) and a memory external to the eUICC is provided. The method can include the eUICC determining that an eSIM package including an eSIM is to be stored on the memory. The method can also include the eUICC, in response to determining that the eSIM package is to be stored on the memory, maintaining a single-use session parameter associated with the eSIM package to enable installation of the eSIM on the eUICC if the eSIM package is later loaded onto the eUICC from the memory.

【代表圖】

【本案指定代表圖】：第（6）圖。

【本代表圖之符號簡單說明】：

無

【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】

在無線通訊裝置中之電子用戶識別模組的安全儲存

SECURE STORAGE OF AN ELECTRONIC SUBSCRIBER

IDENTITY MODULE ON A WIRELESS COMMUNICATION

DEVICE

【技術領域】

所描述實施例大體上係關於無線通訊技術。更特定而言，當前實施例係關於無線通訊裝置上之電子用戶識別模組(eSIM)的安全儲存。

【先前技術】

無線通訊裝置(諸如，智慧型手機)已傳統地經組態以採用提供至無線網路服務之存取的通用積體電路卡(UICC)。UICC通常採用插入至無線通訊裝置中之可移除式小卡(例如，用戶識別模組(SIM)卡)之形式。在大多數情況下，每一UICC係與控制UICC之程式設計及散佈之單一「發行者」(諸如，行動網路業者(MNO))相關聯。

在最近的實施方式中，非可移除式UICC (此處指的是嵌入式UICC)是包含於無線通訊裝置之系統板上。此等eUICC與可移除式UICC相異，相異之處在於：eUICC為非可移除式的，且永久地貼附至無線通訊裝置中之電路板。可使用一或多個eSIM來程式化eUICC，eSIM中之每一者可仿真及複製典型SIM之架構以使包括eUICC之無線通訊裝置能夠存取無線網路服務。

eUICC及eSIM之使用可提供超越傳統UICC之顯著優勢。舉例而言，歸因於缺少設計裝置以適應可移除式UICC之大小及外觀尺寸的需要，因此eUICC之使用可提供裝置設計中之提高之靈活性給裝置製

造商。作為另一實例，在遠端佈建(例如，以空中方式) eSIM之能力可在當組態裝置以存取行動網路業者之無線網路時為消費者及供應商提供便利。

當eUICC及eSIM之使用可提供單一eUICC上之多個eSIM之安裝以及eSIM之遠端佈建之前述的益處時，可限制eUICC中之儲存空間，使得額外eSIM之安裝可能需要自eUICC移除現存之eSIM以便建立所需之儲存空間。用於釋放eUICC上之空間以使得能夠安裝額外eSIM之一個現存之解決方案大體上涉及永久地刪除eSIM，使得被刪除之eSIM不能再次由eUICC使用。另一現存之解決方案涉及自安全eUICC環境將eSIM匯出至遠端佈建伺服器上之安全環境，使得eSIM自eUICC「取消佈建」，且不再在無線通訊裝置處在本端維護。

值得注意的是，前述之解決方案出於各種原因可為不理想的。舉例而言，在某些狀況下，歸因於防止eSIM翻製之安全要求，自eUICC刪除eSIM可為非可逆的。因此，eSIM之刪除不允許eSIM於eUICC上之後續重新安裝，此係因為eSIM不再存在且使用者必須自網路下載另一eSIM，藉此強加成本及責任問題。此外，在匯出至遠端佈建伺服器之情況下，使用者可能未必總是具有網路連接以使得能夠將eSIM匯出至佈建伺服器，及/或可能希望在無線通訊裝置處本端維護裝置eSIM，而非使eSIM在遠端「取消佈建」。

【發明內容】

一些實例實施例提供用於一無線通訊裝置上之一eSIM之安全儲存的方法、設備及電腦程式產品。就此而言，一些實例實施例使得一eSIM能夠安全儲存於包括於該無線通訊裝置中且在包括於該無線通訊裝置中之一eUICC外部之一記憶體上。更特定而言，一些實例實施例之該eUICC可經組態以維護與儲存於該無線通訊裝置記憶體上之一加密eSIM套件相關聯之一單次用工作階段參數以供稍後用以支援該eSIM之安裝。若該eSIM套件稍後載入至該eUICC上，則該單次用工

作階段參數可用於驗證該 eSIM 套件，且其中含有之 eSIM 可接著安裝於該 eUICC 上。因此，此等實施例使得一 eSIM 能夠安全地加密且儲存於該無線通訊裝置記憶體上，同時確保該 eUICC 可稍後驗證且安裝該 eSIM。

前述實施例在該 eUICC 上存在不足以使得能夠安裝一額外 eSIM 之儲存空間的情況中可為尤其有益的。舉例而言，可應用一些實施例以使得能夠將一 eSIM 自一 eUICC 安全匯出至本端無線通訊裝置記憶體，同時使得能夠稍後將該 eSIM 重新安裝於該 eUICC 上，且防止該 eSIM 之翻製或其他誤用。作為另一實例，例如，在該 eUICC 上用於該 eSIM 之空間不足的情況下，一些實施例可用於在一佈建工作階段期間將一 eSIM 安全地儲存於該無線通訊裝置記憶體上，而非將該 eSIM 安裝於該 eUICC 上。該 eSIM 可接著稍後載入且安裝於該 eUICC 上。

提供此發明內容僅為概述一些實例實施例以便提供對本發明之一些態樣之基本理解。因此，應瞭解，上述實例實施例僅為實例，且不應解釋為以任何方式窄化本發明之範疇或精神。其他實施例、態樣及優點將結合以實例方式說明所描述實施例之原理的附圖而自以下詳細描述變得顯而易見。

【圖式簡單說明】

藉由結合附圖之以下詳細描述將易理解本發明，在附圖中，相同的參考數字表示相同的結構元件，且其中：

圖1說明根據一些實例實施例之用於 eSIM 佈建的實例系統。

圖2說明根據一些實例實施例之可實施於無線通訊裝置上之設備的方塊圖。

圖3說明根據一些實例實施例之根據用於安全儲存無線通訊裝置記憶體上之 eSIM 之實例方法的流程圖。

圖4說明根據一些實例實施例之根據用於自 eUICC 將 eSIM 安全匯

出至無線通訊裝置記憶體之實例方法的發信圖。

圖5說明根據一些實例實施例之根據用於在佈建工作階段期間將eSIM安全地儲存於無線通訊裝置上之實例方法的發信圖。

圖6說明根據一些實例實施例之根據用於將儲存於無線通訊裝置記憶體上之eSIM安裝於eUICC上的實例方法之流程圖。

圖7說明根據一些實例實施例之根據用於將儲存於無線通訊裝置記憶體上之eSIM安裝於eUICC上的實例方法之發信圖。

【實施方式】

現將詳細參考附圖中所說明之代表性實施例。應理解，以下描述並不意欲將實施例限制為一個較佳實施例。相反地，以下描述意欲涵蓋如可包括於如由所附申請專利範圍界定之所描述實施例之精神及範疇內的替代物、修改及等效物。

一些實例實施例提供在實施於無線通訊裝置上之eUICC外部之無線通訊裝置記憶體上之eSIM的安全儲存。更特定而言，一些實例實施例eUICC可經組態以維護與儲存於無線通訊裝置記憶體上以用於稍後用於支援eSIM之安裝之加密eSIM套件相關聯之單次用工作階段參數，諸如2階(L2)查問及/或其他安全臨時標誌。若eSIM套件稍後載入至eUICC上，則單次用工作階段參數可用於驗證eSIM套件，且其中含有之eSIM可接著安裝於eUICC上。因此，此等實施例使得eSIM能夠安全地加密且儲存於無線通訊裝置記憶體上，同時確保eUICC可稍後驗證且安裝eSIM。本文中所描述之實施例可另外防止翻製儲存於無線通訊裝置記憶體上之eSIM；將儲存於無線通訊裝置記憶體上之eSIM安裝於另一eUICC上，及/或eSIM之其他誤用。

下文參考圖1至圖7論述此等及其他實施例。然而，熟習此項技術者將容易地瞭解，本文中關於此等圖式所給出之詳細描述僅係出於解釋性目的，且不應將其視為限制性的。

圖1說明根據一些實例實施例之用於eSIM佈建的實例系統100。系統100可包括可經由網路104通訊之佈建伺服器102及一或多個無線通訊裝置106。

根據各種實例實施例，佈建伺服器102可體現為一或多個運算裝置，該一或多個運算裝置可經組態以產生eSIM及/或將eSIM佈建至在無線通訊裝置106上實施之eUICC（例如，eUICC 120）。佈建伺服器102可進一步以管理且授權eSIM在一或多個網路內之使用為任務。佈建伺服器102可（例如）包含一或多個實體伺服器、經組態以實施佈建伺服器102之功能性的雲端運算基礎架構（例如，在基礎實體硬體上實施之虛擬運算系統）及/或其他伺服器裝置。在藉由多個實體運算裝置提供佈建伺服器102之功能性之實施例中，運算裝置可共置於共同位置中，或可跨越多個實體位置分散且可經由網路104通訊。佈建伺服器102可由可維護、佈建及/或管理eSIM之集區的任何實體（諸如（藉由非限制性實例），行動網路業者、裝置製造商、裝置供應商或其他此類實體）來代管/操作。

網路104可體現為經組態以支援兩個或兩個以上運算裝置（諸如，佈建伺服器102與無線通訊裝置106）之間的通訊的任何網路或網路之組合。藉由非限制性實例，網路104可包含一或多個有線網路、一或多個無線網路（例如，蜂巢式網路、無線區域網路、無線廣域網路、無線都會區域網路、其某一組合或其類似者），或其組合，且在一些實例實施例中，可包含網際網路。

無線通訊裝置106可體現為可經組態以存取蜂巢式網路的任何運算裝置。藉由非限制性實例，無線通訊裝置106可體現為蜂巢式電話（諸如，智慧型手機）、平板運算裝置、數位媒體播放器裝置、蜂巢式無線熱點裝置、膝上型電腦、其某一組合或其類似者。作為另一實例，無線通訊裝置106可體現為機器對機器(M2M)裝置、可嵌入主機

裝置內或以操作方式與主機裝置耦接以提供主機裝置之網路連接性的裝置，或其可經組態以(例如，經由SIM)存取蜂巢式網路之類似裝置。

無線通訊裝置106可包括亦可稱作「安全元件」之eUICC 120。在一些實施例中，eUICC 120可嵌入(例如，焊接至)無線通訊裝置106之主系統板內。在一些實例實施例中，eUICC 120可包含不能由外部實體直接存取的沙箱化硬體/軟體環境，諸如可在無線通訊裝置106上執行之主要或主機作業系統(OS)。eUICC 120可包括處理電路(諸如，微處理器)及可一起工作以處理命令及進行各種驗證機制的儲存裝置，各種鑑認機制可用於使得無線通訊裝置106能夠存取行動網路業者之網路。eUICC 120之儲存空間可提供用於eUICC 120上之一或多個eSIM (諸如，可藉由佈建伺服器102佈建之eSIM)之安裝的儲存。eUICC 120可經組態以使用eUICC 120上安裝的eSIM來促進用於存取行動業者之網路的網路鑑認。

無線通訊裝置106及因此可藉由佈建伺服器102佈建及/或eUICC 120上安裝之eSIM可經組態以用於使用多種無線電存取技術(RAT)中之任一者存取網路。藉由非限制性實例，根據一些實例實施例之無線通訊裝置106及/或eSIM可支援長期演進(LTE) RAT，諸如藉由第三代合作夥伴計劃(3GPP)指定之LTE標準之各種版本，包括LTE、高級LTE (LTE-A)及/或使用LTE技術之其他現有或未來版本之各種版本。作為另一實例，根據一些實例實施例的無線通訊裝置106及/或eSIM可支援第三代(3G)蜂巢式RAT，諸如寬頻分碼多重存取(WCDMA)或其他通用行動電信系統(UMTS) RAT，諸如時分同步分碼多重存取(TD-SCDMA)、CDMA2000、1xRTT及/或其類似者。作為另一實例，根據一些實例實施例之無線通訊裝置106及/或eSIM可支援第二代(2G)蜂巢式RAT，諸如全球行動通訊系統(GSM) RAT。將瞭解，藉由實例而非

藉由限制來提供前述RAT。就此而言，根據一些實例實施例的無線通訊裝置106及/或eSIM可經組態以經由任何現有或未來開發之蜂巢式RAT (例如，包括正在開發之各種第五代(5G) RAT)通訊。

如先前所描述，佈建伺服器102可經組態以經由網路104將eSIM佈建至eUICC 120。此佈建可(例如)使用各種空中方式(OTA)技術實現。另外或替代地，在一些實例實施例中，無線通訊裝置106可經由有線連接連接至網路104及/或直接連接至佈建伺服器102，且eSIM可經由有線連接佈建至eUICC 120。

在一些實例實施例中，佈建伺服器102可另外或替代地經組態以提供用於控制先前佈建之eSIMs之使用的管理服務。舉例而言，在一些實施例中，佈建伺服器102可經組態以授予/拒絕針對根據各種實例實施例的eSIM在無線通訊裝置106之記憶體上之安全儲存(例如，「卡外」SIM儲存)的授權。在一些此等實施例中，為了在eUICC 120外部之無線通訊裝置106之記憶體上儲存eSIM的權限，eUICC 120及/或無線通訊裝置106可經組態以將請求發送至佈建伺服器102。

在一些實例實施例中，佈建伺服器102及eUICC 120可經組態以實施及/或以其他方式支援一或多個邏輯安全層，一或多個邏輯安全層可實施用於佈建程序的安全機制。舉例而言，一些實例實施例之佈建伺服器102可經組態以實施1階(L1)實體110、2階(L2)實體112或3階(L3)實體114中之一或多者。一些實例實施例之eUICC 120可在本端實施對應於佈建伺服器102之邏輯安全實體的邏輯安全層及/或程序(例如，L1、L2及/或L3)。根據一些實例實施例，L1 (例如，L1實體110及eUICC 120上之任何對應L1層/程序)可提供加密服務；L2 (例如，L2實體112及eUICC 120上之任何對應L2層/程序)可提供防翻製服務；且L3 (例如，L3實體114及eUICC 120上之任何對應L3層/程序)可提供授權服務。在一些實例實施例中，L1實體110、L2實體112及L3實體

114中之兩個或兩個以上者可實施為在共同實體伺服器或伺服器之集合上運行之邏輯軟體實體。或者，在一些實例實施例中，個別邏輯安全實體(諸如，L1實體110、L2實體112及/或L3實體114中之個別一者)可在實體伺服器上實施，該(等)實體伺服器與實施另一邏輯安全實體之伺服器分離。

圖2說明根據一些實例實施例之可實施於之無線通訊裝置(諸如，無線通訊裝置106)上的設備200的方塊圖。將瞭解，以下圖2中所說明且關於圖2描述之組件、裝置或元件可並非為強制的，且因此在某些實施例中可忽略一些。另外，一些實施例可包括超出圖2中所說明且關於圖2描述之彼等者的另外或不同組件、裝置或元件。

在一些實例實施例中，設備200可包括根據本文中所揭示之一或多個實例實施例之可經組態以執行動作之處理電路210。就此而言，處理電路210可根據各種實例實施例經組態以執行及/或控制設備200之一或多個功能性之效能，且因此根據各種實例實施例可提供用於執行設備200之功能的構件。處理電路210可根據一或多個實例實施例經組態以執行資料處理、應用程式執行及/或其他處理及管理服務。舉例而言，在一些實施例中，處理電路210可經組態以支援無線通訊裝置之主要主機作業系統之操作。

在一些實施例中，設備200或其部分或組件(諸如，處理電路210)可經由一或多個積體電路實施，該一或多個積體電路中之每一者可包括一或多個晶片。在一些情況下，處理電路210及/或設備200之一或多個另外組件可因此經組態以實施積體電路(例如，作為「系統單晶片」)上之實施例。在一些實例實施例中，當實施於運算裝置上或以其他方式可操作地耦接至運算裝置時，設備200之一或多個組件可實施於能夠使得運算裝置能夠存取網路(諸如，無線網路104)的晶片組上。在一些此等實例實施例中，裝置200可包括蜂巢式基頻晶片組，

蜂巢式基頻晶片組可經組態以使得運算裝置(諸如，無線通訊裝置106)能夠在一或多個蜂巢式網路上操作。

在一些實例實施例中，處理電路210可包括處理器212，且在一些實施例中(諸如，圖2中所說明之實施例)，可進一步包括記憶體214。處理電路210可與通訊介面216及/或使用者介面218通訊或以其他方式控制通訊介面216及/或使用者介面218。

處理器212可以多種形式體現。舉例而言，處理器212可體現為各種基於硬體之處理構件，諸如微處理器、共處理器、控制器或包括積體電路(諸如，ASIC (特殊應用積體電路)、FPGA (場可程式化閘陣列)、其某一組合或其類似者)之各種其他運算或處理裝置。儘管說明為單個處理器，但將瞭解處理器212可包含複數個處理器。該複數個處理器可彼此有效地通訊，且可共同地經組態以執行如本文中所描述之無線通訊裝置106之一或多個功能性。在一些實例實施例中，處理器212可經組態以執行可儲存於記憶體214中或可以其他方式存取至處理器212的指令。因而，不論藉由硬體或藉由硬體與軟體之組合組態，處理器212在相應地組態時都能夠根據各種實施例執行操作。

在一些實例實施例中，記憶體214可包括一或多個記憶體裝置。記憶體214可包括固定式及/或可移除式記憶體裝置。在一些實施例中，記憶體214可提供非暫時性電腦可讀儲存媒體，該非暫時性電腦可讀儲存媒體可儲存可由處理器212執行之電腦程式指令。就此而言，根據一或多個實例實施例，記憶體214可經組態以儲存資訊、資料、應用程式、指令及/或其類似者以用於使得設備200能夠而執行各種功能。根據各種實例實施例，記憶體214可進一步提供在eUICC 220外部之用於安全地儲存eSIM的記憶體。在一些實施例中，記憶體214可經由用於在設備200之組件當中傳遞資訊的一或多個匯流排與處理器212、通訊介面216、使用者介面218或eUICC 220中之一或多者通

訊。

設備200可進一步包括通訊介面216。一些實例實施例之通訊介面216可提供經組態以使得設備200能夠將無線信號發送至一或多個無線網路及自一或多個無線網路接收無線信號之無線通訊介面。舉例而言，一些實例實施例之通訊介面216可經組態以藉由使得能夠與蜂巢式基地台進行無線通訊支援對蜂巢式網路之存取。通訊介面216可因此包括根據一或多個蜂巢式RAT用於使得能夠進行通訊之一或多個收發器及支援硬體及/或軟體。一些實施例之通訊介面216可進一步包括一或多個收發器及/或其他無線電組件以支援一或多個另外之無線通訊技術，諸如Wi-Fi (例如，IEEE 802.11技術)、藍芽及/或其他無線通訊技術。在一些實例實施例中，通訊介面216可另外包括用於支援經由電纜、數位用戶線(DSL)、USB、FireWire、乙太網路、一或多個光學傳輸技術及/或其他有線網路連接方法之通訊的通訊數據機或其他硬體/軟體。

在一些實例實施例中，設備200可包括使用者介面218。然而，將瞭解，在一些實例實施例中，可忽略使用者介面218之一或多個態樣，且在一些實施例中，可完全忽略使用者介面218。使用者介面218可與處理電路210通訊以接收使用者輸入之指示及/或以聽覺、視覺、機械或其他輸出給使用者提供。因而，使用者介面218可包括(例如)鍵盤、滑鼠、操縱桿、顯示器、觸控式螢幕顯示器、麥克風、揚聲器、一或多個生物識別輸入裝置及/或其他輸入/輸出機制。在使用者介面218包含觸控式螢幕顯示器之實施例中，使用者介面218可另外經組態以偵測及/或接收觸控及/或其他移動示意動作之指示或至顯示器之其他輸入。

使用者介面218 可(例如)經組態以顯示使得使用者能夠管理儲存於eUICC 220上之eSIM、儲存於記憶體214上之eSIM及/或可在佈建工

作階段期間藉由佈建伺服器102佈建之eSIM的圖形使用者介面。舉例而言，使用者介面218可根據各種實施例顯示提供可選選項以於記憶體214上儲存卡外eSIM及/或將儲存於記憶體214上之eSIM安裝至eUICC 220之圖形使用者介面。使用者介面218可進一步經組態以根據不同實例實施例提供輸入機制以使得使用者能夠選擇選項(諸如，可呈現於顯示之圖形使用者介面上)，以選擇於記憶體214上儲存卡外eSIM，以將儲存於記憶體214上之eSIM安裝至eUICC 220及/或以其他方式管理eSIM。

設備200可進一步包括eUICC 220，eUICC 220可(例如)包含eUICC 120之實施例。eUICC 220可因此包括處理電路及可經組態以根據各種實例實施例儲存及管理一或多個eSIM，諸如可由佈建伺服器102佈建的儲存裝置。根據各種實施例，eUICC 220可經組態以維護與可儲存於在eUICC 220外部之無線通訊裝置記憶體(例如，記憶體214)上之eSIM套件相關聯之單次用工作階段參數，以使得能夠在eSIM載入至eUICC 220上之情況下進行eSIM之稍後驗證及安裝。

圖3說明根據一些實例實施例之根據用於安全儲存無線通訊裝置記憶體(諸如，記憶體214)上之eSIM之實例方法之流程圖。就此而言，圖3說明根據各種實施例之可藉由諸如eUICC 120及/或eUICC 220之eUICC執行之方法。

操作300可包括eUICC判定包括eSIM之eSIM套件待儲存於無線通訊裝置記憶體上。判定可(例如)基於自無線通訊裝置接收之指令，諸如回應於可經由使用者介面218輸入之使用者命令。

在一些實施例中，諸如圖4中說明且下文關於圖4進一步描述，操作300之判定可包括判定儲存於eUICC上之eSIM待匯出至無線通訊裝置記憶體。舉例而言，eSIM可自eUICC匯出至無線通訊裝置記憶體以為另一eSIM釋放eUICC上之儲存空間。

在一些實施例中，諸如圖5中所說明且下文關於圖5進一步描述，操作300之判定可包括在佈建工作階段(例如，具有佈建伺服器102之佈建工作階段)期間判定佈建至eUICC之eSIM將儲存於無線通訊裝置記憶體上而非載入且安裝於eUICC上。舉例而言，eUICC上可不存在用於eSIM之充足的儲存空間，且eSIM可儲存於無線通訊裝置記憶體上而非中斷佈建工作階段。就此而言，eSIM可臨時儲存於無線通訊裝置記憶體上，且eSIM之安裝可暫停直至已清除eUICC上之空間以容納新eSIM。在一些此等實例實施例中，可經由使用者介面(例如，使用者介面218)提示無線通訊裝置使用者eUICC上之空間不足以安裝eSIM，且使用者可選擇繼續佈建工作階段且於裝置記憶體上臨時儲存eSIM。

方法可進一步包括回應於操作300之判定，eUICC執行操作310。操作310可包括eUICC維護與eUICC上之eSIM套件相關聯之單次用工作階段參數以使得能夠在eSIM套件稍後自記憶體載入至eUICC上之情況下將eSIM安裝於eUICC上。工作階段參數可(例如)包含可由eUICC使用以驗證及/或以其他方式鑑認eSIM套件以便防止eSIM之翻製或其他誤用的安全臨時標誌。舉例而言，在一些實施例中，可在操作310中維護之工作階段參數可包括可被產生及用於單一eSIM及/或eSIM佈建工作階段之L2安全值，諸如L2查問。

就此而言，工作階段參數可經維持以用於稍後之使用而非被丟棄。因此，即使在eSIM套件自記憶體載入至eUICC上之前產生後續工作階段參數以用於介入佈建工作階段或其他eSIM操作，若eSIM套件載入至eUICC上以用於安裝，則可稍後使用經維護之工作階段參數。

在一些實例實施例中，eUICC可維護另外之工作階段內容脈絡參數以用於儲存於無線通訊裝置記憶體上之eSIM。舉例而言，與佈建工作階段相關聯之工作階段識別符、eSIM識別符及/或可用於唯一地

識別eSIM套件之其他識別符可維持與工作階段參數相關聯，使得在eSIM套件稍後自無線通訊裝置記憶體載入至eUICC上之情況下，eUICC可存取及使用適當之工作階段參數及/或其他工作階段內容脈絡資訊以用於驗證及安裝。

工作階段參數及/或藉由eUICC維護之其他工作階段內容脈絡資訊可在eUICC之非揮發性記憶體(諸如，非揮發性隨機存取記憶體(NVRAM))中維護。因此，若在安裝eSIM之前存在動力循環，則eUICC將仍具有對工作階段內容脈絡資訊之存取以使得能夠驗證及安裝eSIM。

在實施例中，諸如圖4中所說明且下文關於圖4進一步描述，其中儲存於eUICC上之eSIM待匯出至無線通訊裝置記憶體，可在在操作310中維持之工作階段參數可藉由eUICC產生以支援匯出，且可用於製備eSIM套件以用於匯出。在實施例中，諸如圖5中說明且下文關於圖5進一步描述，其中正佈建至eUICC之eSIM將儲存於無線通訊裝置記憶體上，而非載入且安裝於eUICC上，可在操作310中維持之工作階段參數可為待用於佈建工作階段中之eSIM驗證的工作階段參數。

在一些實例實施例中，諸如圖5中說明且下文關於圖5進一步描述，其中正佈建至eUICC之eSIM將儲存於無線通訊裝置記憶體上，而非載入且安裝於eUICC上，在eSIM成功地本端儲存於無線通訊裝置記憶體上之後，eUICC及/或無線通訊裝置可將指示提供至成功下載eSIM之佈建伺服器。在一些此等實施例中，訊息可簡單地為相同於可在佈建工作階段期間回應於成功eSIM安裝而發送之訊息的「確定(OK)」訊息。或者，在一些此等實施例中，訊息可具體地指示eSIM已儲存於無線通訊裝置記憶體中，且eUICC上之安裝已推遲直至稍後某一時間。

圖4說明根據一些實例實施例之根據用於自eUICC將eSIM安全匯

出至無線通訊裝置記憶體之實例方法的發信圖。更特定而言，圖4說明根據一些實例實施例之可彼此之間交換的發信及藉由eUICC 402、無線通訊裝置404及L3卡外授權實體406執行以支援eSIM自eUICC至無線通訊裝置記憶體之安全匯出的操作。

eUICC 402可實施於無線通訊裝置404上。在一些實施例中，eUICC 402可包含eUICC 120及/或eUICC 220之實施例。

無線通訊裝置404可為無線通訊裝置106之實施例。設備200可實施於無線通訊裝置404上。因而，處理電路210、處理器212、記憶體214、通訊介面216或使用者介面218中之一或多者可(例如)提供用於執行無線通訊裝置404之功能性的構件。

在一些實例實施例中，L3卡外授權實體406可為經組態以提供L3安全服務之網路伺服器實體。舉例而言，在一些實施例中，L3卡外授權實體406可為L3實體114及/或經組態以提供L3安全服務之佈建伺服器之其他實體的實施例。另外或替代地，在一些實例實施例中，L3卡外授權實體406之態樣可由可本端儲存於無線通訊裝置404之記憶體上(例如，在記憶體214上)之使用者憑證提供。

無線通訊裝置404及/或eUICC 402可判定儲存於eUICC 402上之eSIM待匯出至無線通訊裝置404之記憶體(例如，至記憶體214)。就此而言，eSIM可基本上自eUICC 402匯出至其自身以用於無線通訊裝置404之記憶體上的卡外儲存。舉例而言，可回應於可自無線通訊裝置404之使用者接收之指令而進行此判定(例如，經由使用者介面218)。

參考圖4，操作410可包括無線通訊裝置404將指令傳遞至eUICC 402以製備用於儲存於記憶體上之eSIM。舉例而言，無線通訊裝置404可傳遞「prepareeSIM」指令，該「prepareeSIM」指令包括識別eSIM ((例如，「eSIM ID」)及指示操作類型為「儲存」之參數。

操作420可包括eUICC 402將「signedIdentityMap」訊息傳遞至無

線通訊裝置404，以使得能夠獲得用於eSIM之卡外儲存之L3授權。無線通訊裝置404可之後在操作430處自L3卡外授權實體406請求L3授權。操作440可包括L3卡外授權實體406授予用於儲存操作之授權。

操作450可包括eUICC 402產生新L2工作階段參數(諸如，L2查問)以支援eSIM之匯出。就此而言，由於現存之用於eUICC 402之當前L2工作階段參數可與用於未來的eSIM佈建工作階段之網路預共享，可產生新L2工作階段參數。由於eUICC 402可知其將為經製備以用於匯出之eSIM套件之未來接收者，eUICC 402可維護新L2工作階段參數。

操作460可包括eUICC 402格式化eSIM套件。eSIM套件可包括eSIM之加密複本。eSIM加密可(例如)經由可防止除eUICC 402外之實體在匯出至無線通訊裝置404之記憶體之後解密eSIM的任何適當之L1加密技術而處理。

舉例而言，在一些實施例中，eSIM可用與eUICC 402相關聯之公開-私密金鑰對之公開金鑰加密。因此，eSIM可僅用僅eUICC 402已知之私密金鑰解密，使得(除非eUICC 402之金鑰被破解)當匯出至無線通訊裝置404之記憶體時，eSIM不能藉由其他實體解密。

作為另一實例，在一些實施例中，eSIM可用對稱金鑰(例如，AES128金鑰)加密。若eSIM套件隨後自無線通訊裝置404之記憶體載入回至eUICC 402上，則對稱金鑰可藉由eUICC 402秘密地維護以用於稍後用於解密eSIM。另外或替代地，在一些此等實施例中，對稱金鑰可經加密(例如，用eUICC 402之公開金鑰)，且可包括於用於匯出至無線通訊裝置404之記憶體之eSIM套件中。因此，若eSIM套件稍後自無線通訊裝置404之記憶體載入回至eUICC 402上，則eUICC 402可使用私密金鑰以解密對稱金鑰，且接著使用經解密之對稱金鑰以解密eSIM。

eSIM套件可另外包括在操作450中產生之L2工作階段參數之複

本。舉例而言，eSIM套件可用L2工作階段參數簽署。在一些實例實施例中，可包括於eSIM套件中之L2工作階段參數之複本可連同eSIM加密以提供防止誤用之額外保護，諸如在其中eUICC 402不區分所有卡內查問之實施例中。

如操作470所說明，在已製備eSIM套件之後，eUICC 402可刪除eUICC 402上之現存eSIM以防止翻製。

操作480可包括將eSIM套件匯出至無線通訊裝置404。在操作480之後，eSIM（例如，eSIM之任何複本及/或含有eSIM之套件）可自eUICC 402完全移除。eSIM套件可接著在無線通訊裝置404之記憶體（例如，記憶體214）中維護，eSIM套件可稍後自記憶體載入回至eUICC 402，諸如圖6至圖7中說明且下文關於圖6至圖7進一步描述。

在一些實施例中，eUICC 402可維護用於已匯出至無線通訊裝置404之記憶體的經刪除之eSIM的旗標或其他標號器，此可指示eSIM已儲存於卡外。可使用此旗標以促進eSIM管理，諸如將指示經由eSIM存在且已儲存於eUICC 402外部之無線通訊裝置404之記憶體上之使用者介面提供至使用者，且使得使用者能夠選擇於eUICC 402上重新安裝eSIM。

圖5說明根據一些實例實施例之根據用於在佈建工作階段期間將eSIM安全地儲存於無線通訊裝置上之實例方法的發信圖。更特定而言，圖5說明可彼此之間交換的發信及可藉由eUICC、無線通訊裝置508及佈建伺服器執行以支援佈建工作階段期間無線通訊裝置508之記憶體上之eSIM之安全儲存的動作。

eUICC可實施於無線通訊裝置508上，且可（例如）對應於eUICC 120及/或eUICC 220之實施例。eUICC可實施多個邏輯安全層，包括可提供加密服務之eUICC L1 502、可提供防翻製服務之eUICC L2 504及可提供授權服務之eUICC L3 506。

無線通訊裝置508可為無線通訊裝置106之實施例。設備200可實施於無線通訊裝置508上。因而，處理電路210、處理器212、記憶體214、通訊介面216或使用者介面218中之一或多者可(例如)提供用於執行無線通訊裝置508之功能性的構件。

佈建伺服器可(例如)包含佈建伺服器102之實施例，且可包括包括伺服器L3 510、伺服器L2 512及伺服器L1 514之複數個邏輯安全實體。伺服器L3 510可(例如)對應於L3實體114之實施例，且可提供授權服務。伺服器L2 512可(例如)對應於L2實體112之實施例，且可提供防翻製服務。伺服器L1 514可(例如)對應於L1實體110之實施例，且可提供加密服務。

佈建工作階段之階段1 518可包括查詢可用之eSIM操作的無線通訊裝置508，如操作520及522中所說明且關於操作520及522描述。在操作520處，無線通訊裝置508可自eUICC L3 506擷取eUICC CSN及簽章。無線通訊裝置508可接著與伺服器L3 510通訊以得到用於eUICC之可用的eSIM選項(例如，經由「geteSIMOptions」訊息)。

歸因於儲存侷限性，eUICC上之eSIM之載入及安裝可能不能夠繼續進行。然而，使用者可需要繼續eSIM下載，但使安裝稍後在准許(例如，藉由佈建伺服器)時進行。操作524可包括無線通訊裝置508得到用於本端eSIM儲存之授權。此授權之獲得可包括與伺服器L3 510(例如，在操作522中)通訊及/或接收使用者選擇以下載及經由無線通訊裝置508之使用者介面(例如，使用者介面218)本端儲存eSIM。然而，將瞭解，所說明之操作524之時序為非限制性的，且操作524可根據各種實施例在eSIM之本端儲存之前在佈建工作階段內出現於其他點處。

佈建工作階段之階段2 526可包括可關於用於佈建工作階段之鑑認步驟的操作528至操作542。操作528可包括無線通訊裝置508將指令

傳遞至 eUICC L3 506 以用伺服器 L3 510 创建工作階段。在傳遞至 eUICC L2 504 上之前，eUICC L3 506 可執行指令之 L3 檢驗。

如操作 530 所說明，eUICC L2 504 可產生可經由 eUICC L3 506 傳遞至無線通訊裝置 508 之工作階段請求。操作 532 可包括無線通訊裝置 508 將工作階段初始化請求訊息發送至伺服器 L3 510，工作階段初始化請求訊息可包括由 eUICC L2 504 產生之作為參數之工作階段請求。

伺服器 L3 510 可執行請求之 L3 檢驗，且，倘若請求經檢驗，則可將可包括藉由 eUICC L2 504 產生之作為參數之工作階段請求的 `verifySession` 訊息傳遞至伺服器 L2 512。伺服器 L2 512 可執行工作階段請求之 L2 檢驗，且可產生經簽署之工作階段回應 (`sessionResponse`)，在操作 538 處，工作階段回應可經由伺服器 L3 510 發送至無線通訊裝置 508。

在操作 540 處，無線通訊裝置 508 可將指令 (`prepareeSIMOperationRequest`) 傳遞至 eUICC，該指令可包括來自伺服器 L2 512 之工作階段回應。在操作 542 處，eUICC L2 504 可檢驗工作階段回應。

倘若工作階段回應以適當方式檢驗，則可包括佈建工作階段之操作 546 至操作 566 的階段 3a 544 可開始。階段 3a 544 可包括用於佈建工作階段之 eSIM 傳輸操作。

操作 546 可包括 eUICC L2 504 將用於 eSIM 佈建之參數之 (諸如，用於工作階段之 L2 查問、eUICC 公開金鑰及 eUICC 憑證) 傳遞至無線通訊裝置 508。在操作 548 中，無線通訊裝置 508 可依次將彼等參數發送至伺服器 L3 510 (例如，在「`performeSIMOperation`」訊息中)。

在操作 550 處，伺服器 L3 510 可檢驗來自無線通訊裝置 508 之請求。在操作 552 處，倘若請求經檢驗，則伺服器 L3 510 可將 eUICC 參數 (例如，L2 查問、eUICC 公開金鑰及 eUICC 憑證) 傳遞至伺服器 L2

512。在操作554處，伺服器L2 512可依次執行請求之L2檢驗。

操作556可包括伺服器L2 512將包括用於佈建工作階段之異動ID之異動資訊發送至無線通訊裝置508。在操作558處，伺服器L2 512可另外將包括eUICC參數(例如，L2攻擊、eUICC公開金鑰及eUICC憑證)之personalizeeSIM命令發送至伺服器L1 514。在操作560處，伺服器L1 514可製備包括加密eSIM (例如，具備eUICC公開金鑰)之eSIM套件，且可將eSIM套件發送至伺服器L2 512。伺服器L2 512可簽署eSIM套件，且將eSIM套件提供至伺服器L3 510。

在操作562處，無線通訊裝置508可請求伺服器L3 510經由參考先前提供之異動ID的「geteSIM」訊息發送eSIM套件。操作564可包括伺服器L3 510將eSIM套件發送至無線通訊裝置508。操作566可包括無線通訊裝置508於eUICC外部之記憶體上本端儲存eSIM套件566。

在一些實例實施例中，eUICC及/或無線通訊裝置508可提供成功下載及儲存eSIM之確認給佈建伺服器(例如，伺服器L3 510)。

階段3b可包括將eSIM套件載入eUICC上及在eUICC上安裝eSIM。可推遲載入及安裝直至稍後某一時間，諸如在已釋放eUICC上之足夠的儲存空間之後。可(例如)根據圖6及圖7中所說明且下文中關於圖6及圖7所論述之技術而執行載入及安裝。

圖6說明根據一些實例實施例之根據用於將儲存於無線通訊裝置記憶體上之eSIM安裝於eUICC (諸如，eUICC 120及/或eUICC 220)上的實例方法之流程圖。就此而言，圖6說明(諸如)根據關於圖3至圖5所論述之方法的可藉由eUICC執行以安裝安全地儲存於無線通訊裝置記憶體(例如，記憶體214)上之eSIM的操作。圖6之方法可(例如)藉由無線通訊裝置106及/或其使用者(例如，經由使用者介面218)回應於安裝之初始化而執行。

操作600可包括eUICC接收儲存於無線通訊裝置記憶體上之eSIM

套件。在操作610處，eUICC可存取與eSIM套件相關聯之所儲存之工作階段參數。所儲存之工作階段參數可為如上文所描述之可用於驗證eSIM套件且提供防翻製保護的單次用工作階段參數，諸如L2查問及/或其他L2安全值。在一些實例實施例中，eUICC可使用可包括於eSIM套件上及/或藉由無線通訊裝置106以其他方式傳遞至eUICC以存取用於eSIM套件之適當工作階段參數的工作階段ID及/或eSIM ID。

操作620可包括eUICC使用工作階段參數以檢驗eSIM套件之有效性。在一些實施例中，在檢驗eSIM套件之有效性之後，eUICC可刪除工作階段參數。倘若eSIM套件之有效性經檢驗，則操作630可包括eUICC解密含於eSIM套件中之eSIM且將其安裝於eUICC上。

可伴隨圖6之方法之執行而自無線通訊裝置記憶體刪除eSIM套件。就此而言，自無線通訊裝置記憶體之刪除可確保在給定時間僅存在eSIM之一個複本。

在一些實施例中，無線通訊裝置106及/或eUICC 120可經組態以通知佈建伺服器102伴隨圖6之方法由eUICC 120之執行而已將eSIM安裝於eUICC 120上。

圖7說明根據一些實例實施例之根據用於將儲存於無線通訊裝置記憶體上之eSIM安裝於eUICC上的實例方法之發信圖。更特定而言，諸如根據關於圖3至圖5所論述之各種技術，圖7說明可彼此之間交換的發信及可藉由eUICC 702及無線通訊裝置704執行以用於安裝儲存於無線通訊裝置702之記憶體上之eSIM的操作。

eUICC 702可在無線通訊裝置704上實施。在一些實施例中，eUICC 702可包含eUICC 120及/或eUICC 220之實施例。eUICC 702可實施多個邏輯安全層，包括可提供加密服務之eUICC L1 706、可提供防翻製服務之eUICC L2 708及可提供授權服務之eUICC L3 710。

無線通訊裝置704可為無線通訊裝置106之實施例。設備200可實

施於無線通訊裝置704上。因而，處理電路210、處理器212、記憶體214、通訊介面216或使用者介面218中之一或多者可(例如)提供用於執行無線通訊裝置704之功能性的構件。無線通訊裝置704可具有本端儲存於裝置記憶體(例如，記憶體214)上之eSIM套件。

操作720可包括無線通訊裝置704將eSIM套件傳遞至eUICC 702。無線通訊裝置704可另外傳遞異動資訊，諸如可由eUICC 702使用以擷取用於驗證eSIM套件之適當之工作階段內容脈絡的異動ID。操作720可(例如)回應於來自無線通訊裝置704之使用者的指令而執行以安裝eSIM。

eUICC 702可接收eSIM套件。諸如關於圖6之操作600至操作620之以上描述，eUICC L2 708可存取用於eSIM套件之所儲存之L2查問，且使用所儲存之L2查問以檢驗eSIM套件之有效性。

在操作730處，倘若檢驗L2查問及/或可為安全目的而檢驗之任何其他異動資訊，則eUICC L2 708可將eSIM套件提供至eUICC L1，且授權eSIM之安裝。

操作735可包括eUICC L1 706解密包括於eSIM套件中之eSIM。eSIM之解密可(例如)使用實施例中(其中eSIM使用eUICC之公開金鑰加密)之eUICC之私密金鑰執行。或者，作為另一實例，eSIM可用可能已用於加密eSIM之對稱金鑰解密。

操作740可包括eUICC L1 706將eSIM安裝於eUICC 702上。在操作745處，eUICC 708可另外刪除L2 查問，此係因為出於驗證eSIM套件之目的，單次用參數不再被需要或不再有效。

操作750可包括eUICC 702向無線通訊裝置704通知eSIM成功安裝於eUICC 702上。在一些實例實施例中，無線通訊裝置704可將指示傳遞至佈建伺服器(例如，佈建伺服器102)以指示已安裝及啟動eSIM。

將瞭解，當各種實施例已描述於eUICCs之內容脈絡中時，本文

中所描述之技術經必要修改後可應用於其他形式之UICC，諸如傳統SIM卡(eSIMs可安裝於其上)。另外，本文中所描述之技術已關於eSIM而描述，亦已知為電信設定檔，電信設定檔可用於為存取行動網路服務提供鑑認。將瞭解，本文中所描述之技術經必要修改後可應用於可儲存於eUICC及/或其他安全元件上之其他類型之設定檔，諸如用於轉移服務之設定檔、用於儲備服務之設定檔及/或類似之設定檔。

可單獨地或以任何組合形式使用各種態樣、實施例、實施方案或所描述之實施例之特徵。所描述實施例之各種態樣可藉由軟體、硬體或硬體與軟體之組合實施。所描述實施例亦可體現為儲存電腦可讀程式碼之電腦可讀媒體(或若干媒體)，該電腦可讀程式碼包括可由一或多個運算裝置執行之指令。電腦可讀媒體可與可儲存此後可由電腦系統讀取之資料的任何資料儲存裝置相關聯。電腦可讀媒體之實例包括唯讀記憶體、隨機存取記憶體、CD-ROM、HDD、DVD、磁帶及光學資料儲存裝置。電腦可讀媒體亦可分散於網路耦接之電腦系統上，以使得電腦可讀程式碼可以分散式方式儲存且執行。

在前述之詳細描述中，參考隨附圖式，該等隨附圖式形成描述之一部分，且其中藉由說明而展示根據所描述實施例之特定實施例。儘管此等實施例經足夠詳細地描述以使得熟習此項技術者能夠實踐所描述之實施例，但應理解，此等實例為非限制性的；使得可使用其他實施例，且在不脫離所描述之實施例之精神及範疇之情況下可進行變化。舉例而言，將瞭解，流程圖中所說明之操作的排序為非限制性的，使得流程圖中所說明及關於流程圖所描述之兩個或兩個以上操作的排序可根據一些實例實施例而改變。作為另一實例，將瞭解，在一些實施例中，流程圖中所說明且關於流程圖所描述之一或多個操作可為可選的，且可忽略。

另外，出於解釋之目的，前述之描述使用特定命名法以提供對所描述實施例之澈底理解。然而，熟習此項技術者將顯而易見，不需要特定細節以便實踐所描述實施例。因此，出於說明及描述之目的呈現特定實施例之前述描述。單獨提供前述描述中所呈現之實施例的描述及關於該等實施例所揭示之實例以添加上下文且輔助理解所描述實施例。該描述並不意欲為窮盡性的或將所描述實施例限制為所揭示之精確形式。一般熟習此項技術者將顯而易見，鑒於上文教示，許多修改、替代應用及變化係可能的。就此而言，一般熟習此項技術者將容易理解，可在無此等特定細節中之一些或全部的情況下實踐所描述實施例。另外，在一些情況下，未詳細描述熟知處理步驟以便避免不必要地模糊所描述實施例。

【符號說明】

100	系統
102	佈建伺服器
104	無線網路
106	無線通訊裝置
110	1階(L1)實體
112	2階(L2)實體
114	3階(L3)實體
120	嵌入式通用積體電路卡(eUICC)
200	設備
210	處理電路
212	處理器
214	記憶體
216	通訊介面
218	使用者介面

220	嵌入式通用積體電路卡(eUICC)
402	嵌入式通用積體電路卡(eUICC)
404	無線通訊裝置
406	L3卡外授權實體
502	嵌入式通用積體電路卡(eUICC) L1
504	嵌入式通用積體電路卡(eUICC) L2
506	嵌入式通用積體電路卡(eUICC) L3
508	無線通訊裝置
510	伺服器L3
512	伺服器L2
514	伺服器L1
518	階段1
526	階段2
544	階段3a
702	嵌入式通用積體電路卡(eUICC)
704	無線通訊裝置
706	嵌入式通用積體電路卡(eUICC) L1
708	嵌入式通用積體電路卡(eUICC) L2
710	嵌入式通用積體電路卡(eUICC) L3

申請專利範圍

105年11月18日修正
對照頁(本)

1. 一種用於將一電子用戶識別模組(eSIM)安全地儲存於一無線通訊裝置中之方法，該無線通訊裝置包括(i)一嵌入式通用積體電路卡(eUICC)及(ii)該eUICC外部之一記憶體，該方法包含：

在該eUICC處進行以下操作：

判定包含一eSIM之一eSIM套件待儲存於該記憶體上，其中該判定發生在該eUICC及一與一佈建伺服器之間的一eSIM佈建工作階段期間；及

維護與該eSIM套件相關聯之一單次用工作階段參數，其中當該eSIM套件自該記憶體載入至該eUICC上時，該單次用工作階段參數使得能夠進行該eSIM於該eUICC上之一安裝。

2. 如請求項1之方法，其中該單次用工作階段參數包含一2階(L2)安全值。

3. 如請求項1之方法，其進一步包含：

接收儲存於該記憶體上之該eSIM套件；

使用該單次用工作階段參數以檢驗該eSIM套件之一有效性；

及

當該eSIM套件之該有效性經檢驗時進行以下操作：

將該eSIM安裝於該eUICC上。

4. 如請求項3之方法，其進一步包含：

在檢驗該eSIM套件之該有效性之後，自該eUICC刪除該單次用工作階段參數。

5. 如請求項3之方法，其進一步包含：

自該記憶體刪除該eSIM套件。

6. 如請求項1之方法，其進一步包含：在該判定之前，得到用於本

端eSIM儲存之一授權。

7. 如請求項1之方法，其進一步包含：

回應於該eUICC上用於該eSIM之足夠儲存空間的一缺乏而判定將該eSIM套件儲存於該記憶體上；

將該eSIM套件儲存於該記憶體上；及

向該eUICC通知該eSIM套件儲存於該記憶體上。

8. 如請求項1之方法，其進一步包含：

回應於該eSIM套件之一成功下載及在該記憶體上之儲存而提供該eSIM套件之該成功下載之一確認給該佈建伺服器。

9. 一種無線通訊裝置，其包含：

一嵌入式通用積體電路卡(eUICC)；及

該eUICC外部之一記憶體，其中該eUICC經組態以進行包括以下各者之步驟：

判定包含一電子用戶識別模組(eSIM)之一eSIM套件待儲存於該記憶體上，其中該判定發生在該eUICC及一與一佈建伺服器之間的一eSIM佈建工作階段期間；及

維護與該eSIM套件相關聯之一單次用工作階段參數，其中當該eSIM套件自該記憶體載入至該eUICC上時，該單次用工作階段參數使得能夠進行該eSIM於該eUICC上之一安裝。

10. 如請求項9之無線通訊裝置，其中該單次用工作階段參數包含一2階(L2)安全值。

11. 如請求項9之無線通訊裝置，其中該等步驟進一步包括：

接收儲存於該記憶體上之該eSIM套件；

使用該單次用工作階段參數以檢驗該eSIM套件之一有效性；

及

當該eSIM套件之該有效性經檢驗時進行以下操作：

將該eSIM安裝於該eUICC上。

12. 如請求項11之無線通訊裝置，其中該等步驟進一步包括：

在檢驗該eSIM套件之該有效性之後，自該eUICC刪除該單次用工作階段參數。

13. 如請求項11之無線通訊裝置，其中該等步驟進一步包括：

自該記憶體刪除該eSIM套件。

14. 如請求項9之無線通訊裝置，其中該eUICC經組態以進行的步驟更進一步包括：

在該判定之前，得到用於本端eSIM儲存之一授權。

15. 如請求項9之無線通訊裝置，其中該等步驟進一步包括：

回應於該eUICC上用於該eSIM之足夠儲存空間的一缺乏而判定將該eSIM套件儲存於該記憶體上；

將該eSIM套件儲存於該記憶體上；及

向該eUICC通知該eSIM套件儲存於該記憶體上。

16. 如請求項9之無線通訊裝置，其中該等步驟進一步包括：

回應於該eSIM套件之一成功下載及在該記憶體上之儲存而提供該eSIM套件之該成功下載之一確認給該佈建伺服器。

17. 一種非暫時性電腦可讀儲存媒體，其經組態以儲存在由包括於一無線通訊裝置中之一嵌入式通用積體電路卡(eUICC)執行時使該eUICC進行包括以下各者之步驟的指令：

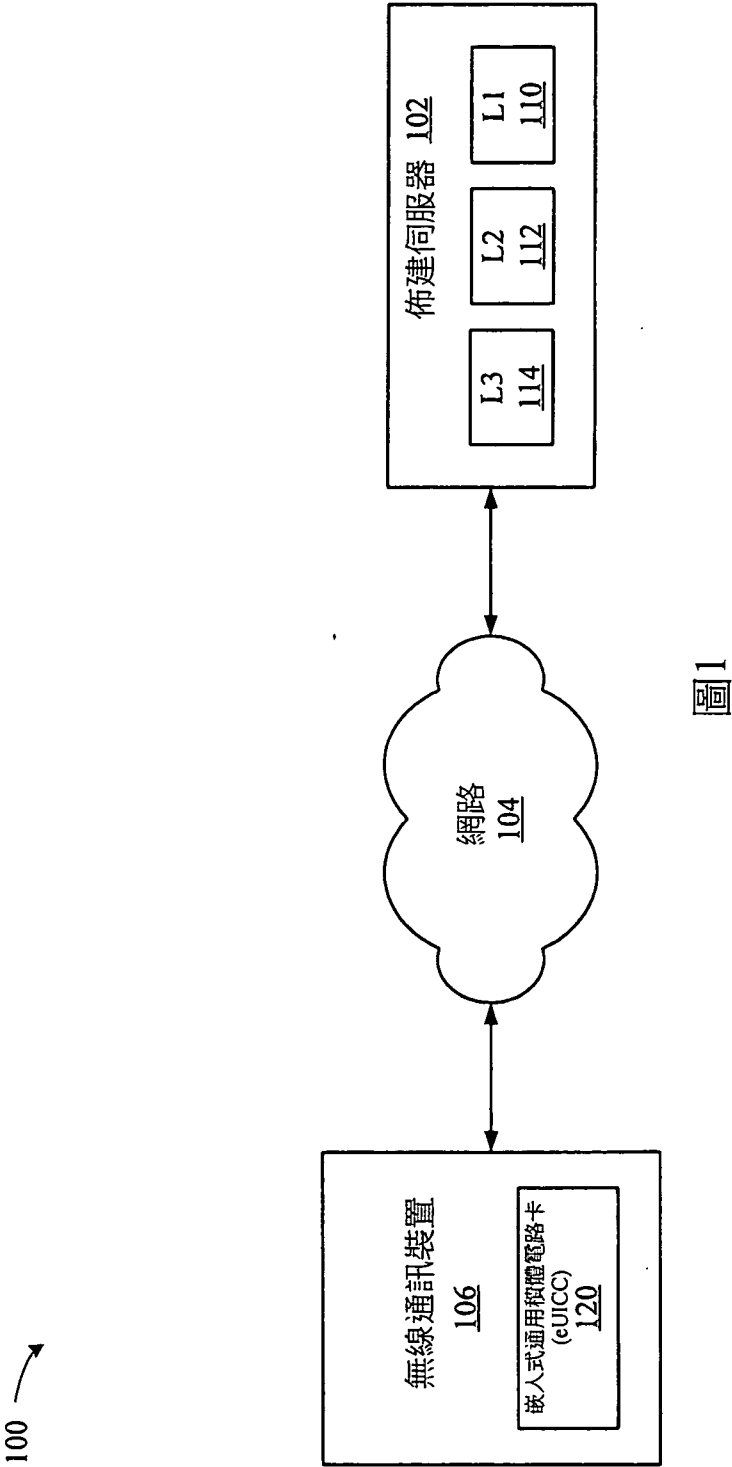
判定包含一電子用戶識別模組(eSIM)之一eSIM套件待儲存於一記憶體上，該記憶體在該eUICC外部且包括於該無線裝置中，其中該判定發生在該eUICC及一與一佈建伺服器之間的一eSIM佈建工作階段期間；及

維護與該 eSIM 套件相關聯之一單次用工作階段參數，其中當該 eSIM 套件自該記憶體載入至該 eUICC 上時，該單次用工作階段參數使得能夠進行該 eSIM 於該 eUICC 上之一安裝。

18. 如請求項 17 之非暫時性電腦可讀儲存媒體，其中該等指令更進一步使得該 eUICC 進行以下步驟：

在該判定之前，得到用於本端 eSIM 儲存之一授權。

圖式



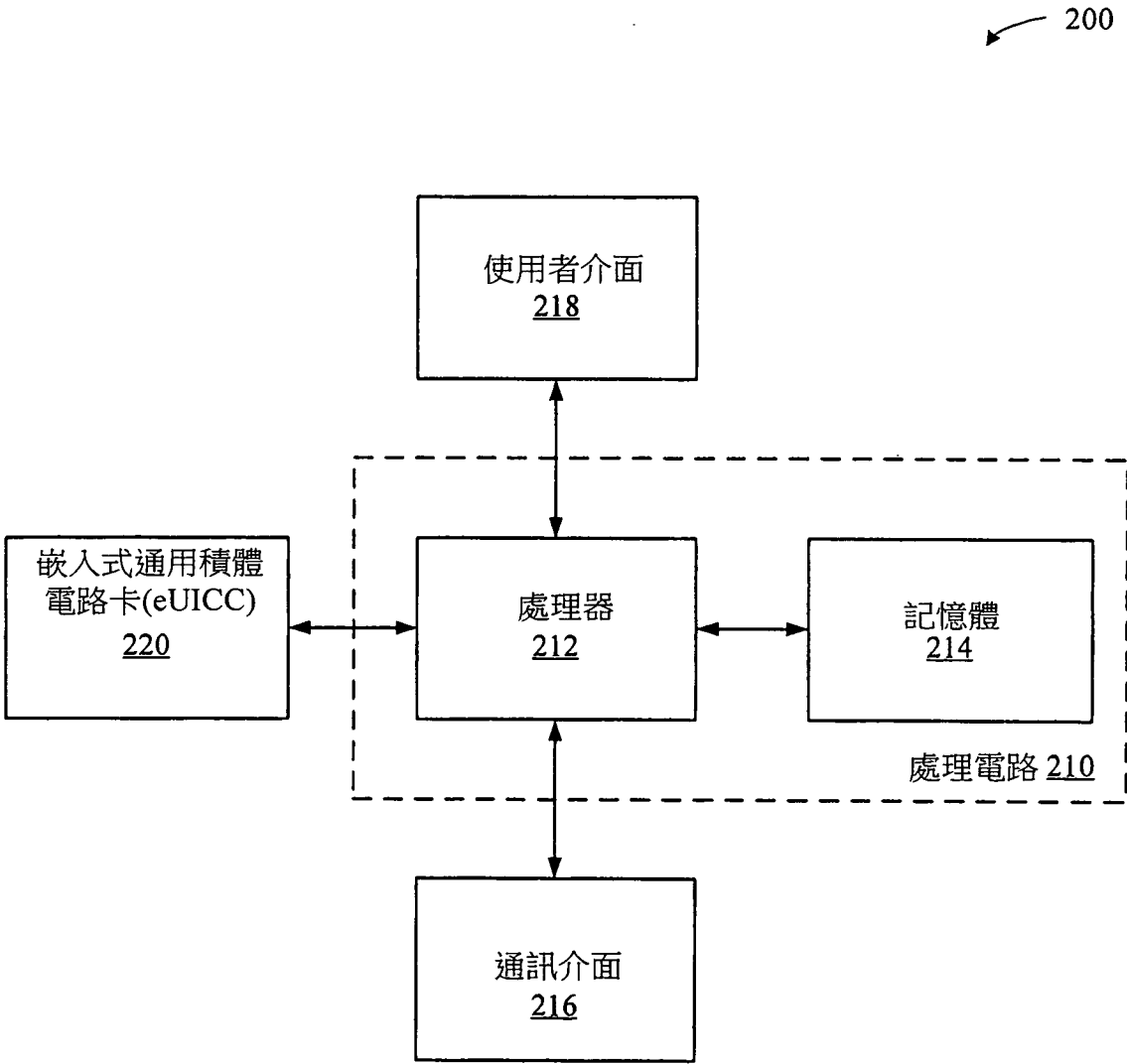


圖2

300

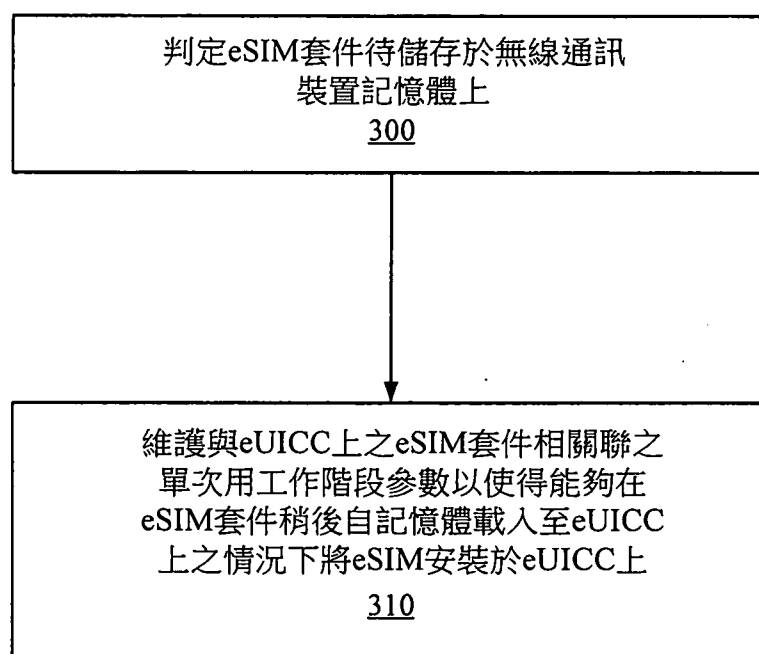


圖3

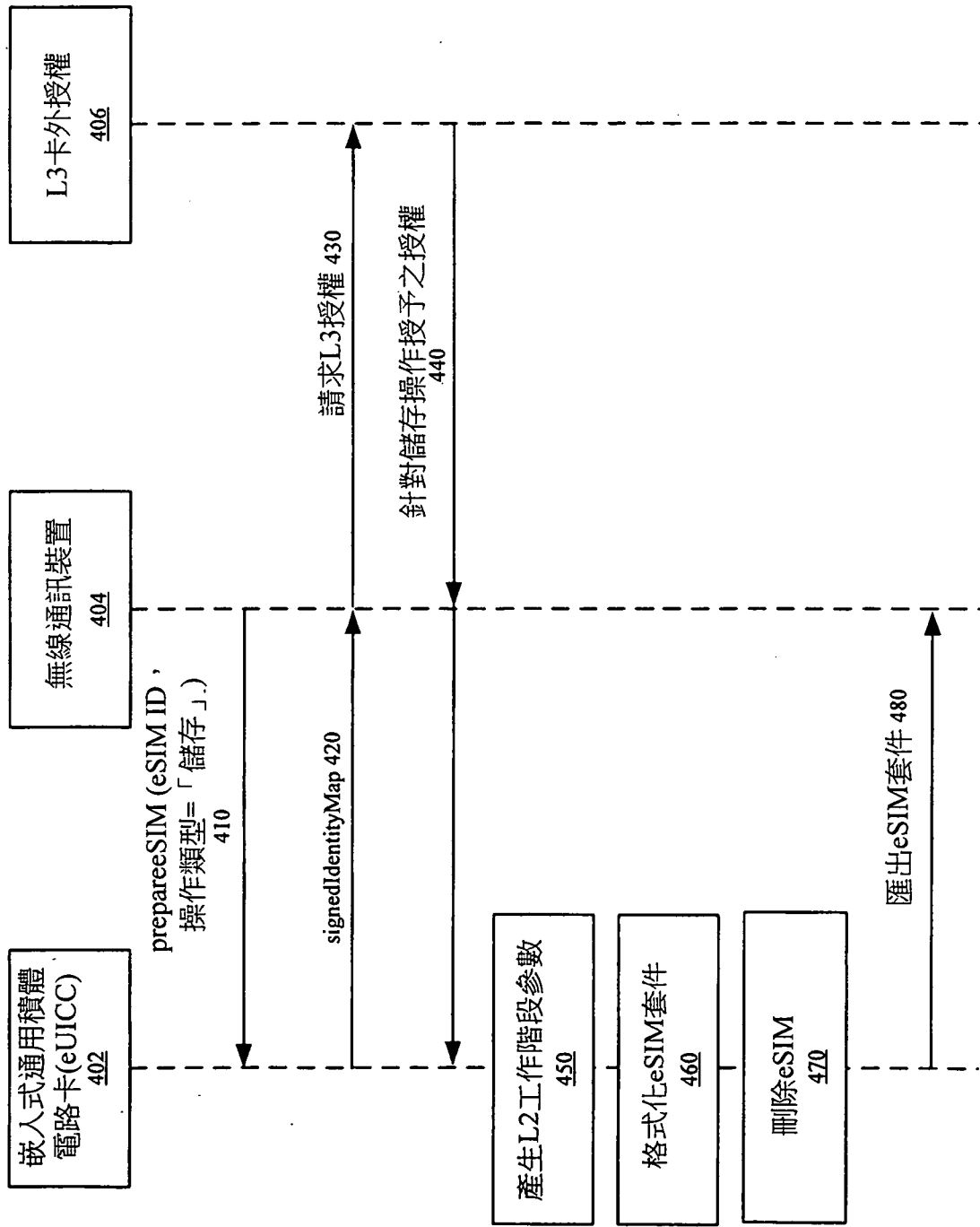


圖4



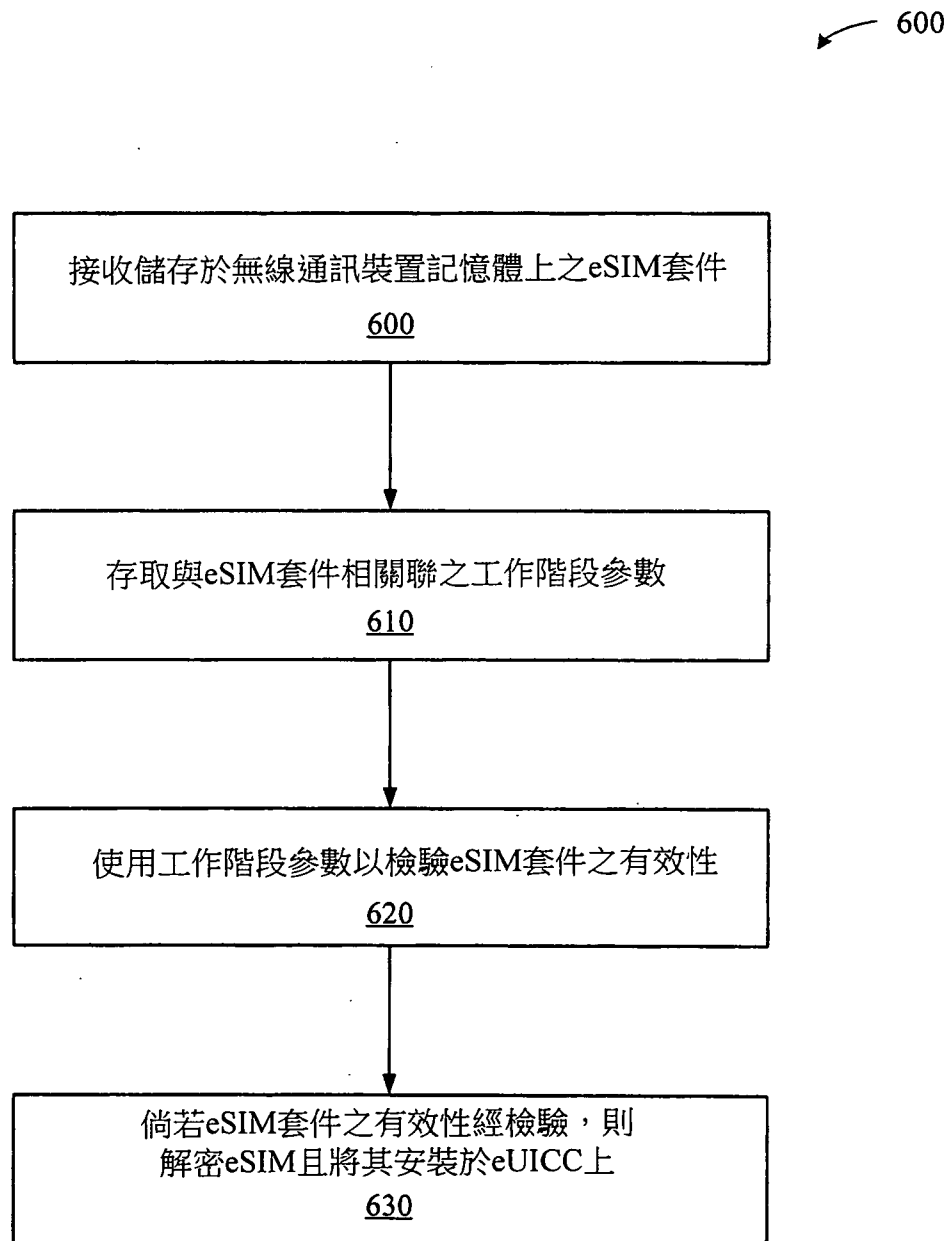


圖6

