(19)中華民國智慧財產局
(12)發明說明書公開本 (11)公開編號：TW 201123772 A1
(43)公開日： 中華民國 100 (2011) 年 07 月 01 日

(21)申請案號：100103772 (22)申請日： 中華民國 92 (2003) 年 06 月 20 日
(51)Int. Cl.： *H04L12/28 (2006.01)* *H04W12/00 (2009.01)*
(30)優先權：2002/06/20 美國 10/176,562
(71)申請人：奎康公司 (美國) QUALCOMM INCORPORATED (US)
美國
(72)發明人：徐 雷蒙T S HSU, RAYMOND T-S. (US)
(74)代理人：陳長文
申請實體審查：有 申請專利範圍項數：13 項 圖式數：7 共 34 頁

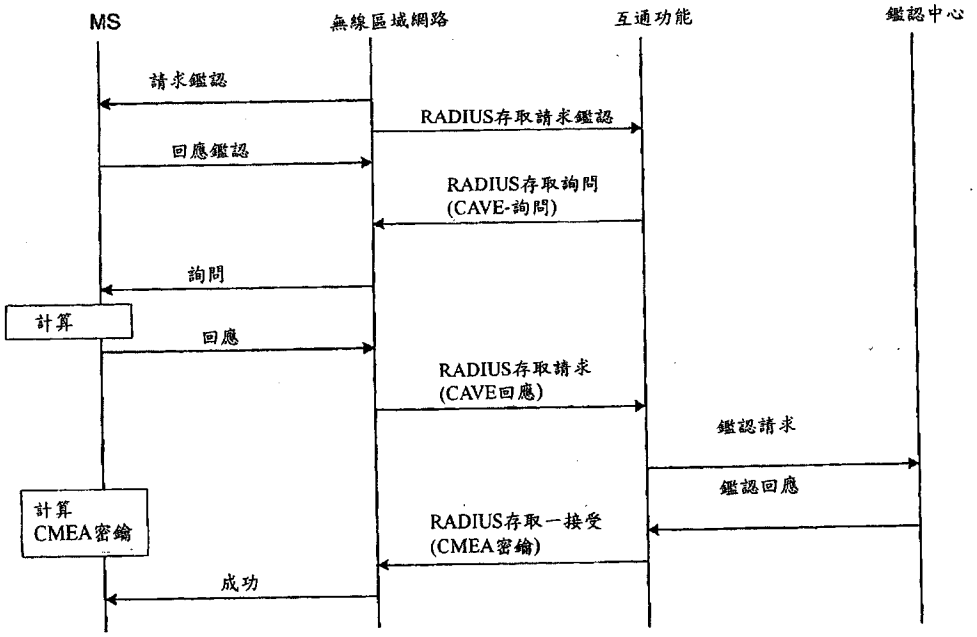
(54)名稱

通信系統之互通功能

INTER-WORKING FUNCTION FOR A COMMUNICATION SYSTEM

(57)摘要

本發明係關於介接一無線區域網路(WLAN)與一通信系統之互通功能(IWF)。IWF 可包含充足資訊以鑑認一用戶存取 WLAN，或者 IWF 係需要請求來自通信系統之鑑認。按一個實例，IWF 可發送一存取詢問至一用戶之 WLAN。IWF 然後將一回應該詢問傳遞給通信系統以供鑑認。IWF 可讓 WLAN 使用通信系統之鑑認能力供本地鑑認。



(19)中華民國智慧財產局
(12)發明說明書公開本 (11)公開編號：TW 201123772 A1
(43)公開日： 中華民國 100 (2011) 年 07 月 01 日

(21)申請案號：100103772 (22)申請日： 中華民國 92 (2003) 年 06 月 20 日
(51)Int. Cl.： *H04L12/28 (2006.01)* *H04W12/00 (2009.01)*
(30)優先權：2002/06/20 美國 10/176,562
(71)申請人：奎康公司 (美國) QUALCOMM INCORPORATED (US)
美國
(72)發明人：徐 雷蒙T S HSU, RAYMOND T-S. (US)
(74)代理人：陳長文
申請實體審查：有 申請專利範圍項數：13 項 圖式數：7 共 34 頁

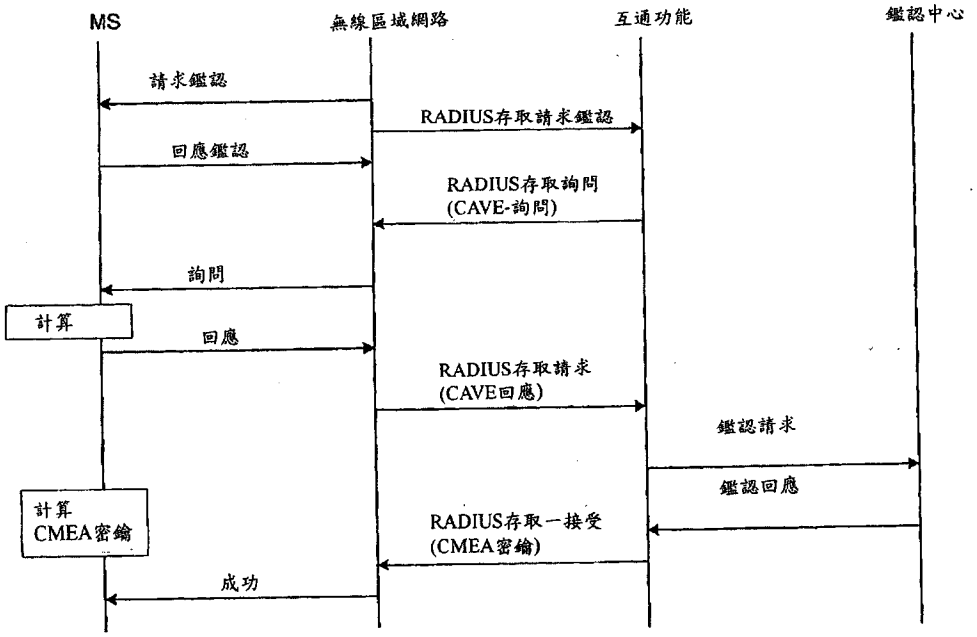
(54)名稱

通信系統之互通功能

INTER-WORKING FUNCTION FOR A COMMUNICATION SYSTEM

(57)摘要

本發明係關於介接一無線區域網路(WLAN)與一通信系統之互通功能(IWF)。IWF 可包含充足資訊以鑑認一用戶存取 WLAN，或者 IWF 係需要請求來自通信系統之鑑認。按一個實例，IWF 可發送一存取詢問至一用戶之 WLAN。IWF 然後將一回應該詢問傳遞給通信系統以供鑑認。IWF 可讓 WLAN 使用通信系統之鑑認能力供本地鑑認。



六、發明說明：

【發明所屬之技術領域】

本發明係關於一通信系統之一種互通功能，尤其是關於經由「無線區域網路」(WLAN)內一互通功能用於共同鑑認及密鑰交換的機構。

【先前技術】

一無線區域網路(WLAN)可讓用戶實際上不受限制存取「網際網路協定」(IP)服務和資料網路。WLAN之使用並非限於膝上型電腦與其他電腦裝置，但正迅速擴大以包括行動電話，個人數位助理器(PDA)，及由一外部網路或載波所支援之其他小型無線裝置。例如，經由一行動通信載波通信之一無線裝置在一電腦化設置或工作空間內漫遊至一WLAN。按此情況，此無線裝置即有通路存取行動通信系統，但希望存取WLAN。WLAN存取需要鑑認。因無線裝置已經獲得存取行動通信系統，進一步鑑認之需要就是冗餘的。因此就有需要一互通功能，它為存取一行動通信系統及存取一WLAN容許一共同鑑認。

【發明內容】

本發明係關於介接一無線區域網路(WLAN)與一通信系統之互通功能(IWF)。IWF可包含充足資訊以鑑認一用戶存取WLAN，或者IWF係需要請求來自通信系統之鑑認。按一個實例，IWF可發送一存取詢問至一用戶之WLAN。IWF然後將一回應該詢問傳遞給通信系統以供鑑認。IWF可讓WLAN使用通信系統之鑑認能力供本地鑑認。

【實施方式】

本文內使用字彙"典型例"係表示"可用作一範例，實例，或圖例說明"。本文內所述為"典型例"的任一實施例並不一定就構解成比其他實例較佳或較有優勢。

一HDR電話用戶台，本文內係指為一存取終端機(AT)，可為行動或固定，且可與一個或多個HDR基地台通信，本文內係指為數據機集區收發機(MPTs)。一存取終端機經由一個或多個數據機集區收發機可發射及接收資料封包至一HDR基地台控制器，本文內係指為一數據機集區控制器(MPC)。數據機集區收發機與數據機集區控制器係稱為一存取網路中一網路之另件。一存取網路可傳輸在多個存取終端機間之資料封包。存取網路進一步被連接至存取網路外面之額外網路，諸如一共同網內網路或網際網路，且可傳輸在每一存取終端機與這種網外網路間之資料封包。已與一個或多個數據機集區收發機建立之一主動電信頻道連接之一存取終端機係被稱為一主動連接端，且說明其係在一通信狀態。係在與一個或多個數據機集區收發機建立一主動通信頻道連接過程中之一存取終端機說明其係在一連接設定狀態。一存取終端機可為任一資料裝置可經由一無線頻道或經由一連線頻道通信，例如使用纖維光學或同軸纜線通信。一存取終端機更可為眾多型式裝置中任一型包括但不限於PC卡，CF記憶卡，外部或內部數據機，或無線或有線電話。經由存取終端機可發送信號至數據機集區收發機之通信鏈路被稱為一反向鏈路。經由一數據機集區收發機發

送信號至一存取終端機被稱之為正向鏈路。

圖1說明具有多個存取點(APs) 106，108，110之一無線本地區網路(WLAN) 100。一AP係可提供WLAN 100無線側之一星形拓撲控制一集線器或橋接器，以及存取連線網路。

每一AP 106，108，110，以及未圖示之其他AP，可支援連接至一資料服務，諸如網際網路，一工作站102，諸如一膝上型電腦，或其他數位計算裝置，可經由空中介面與一AP通信，因之名詞為無線LAN。此AP然後與一鑑認服務者(AS)或鑑認中心(AC)通信。此AC係供請求進入一網路之裝置執行鑑認服務的一元件。執行包括「遙控鑑認電話撥進用戶服務」(RADIUS)，它係RFC 2138內所述之一網際網路用戶鑑認，1997年4月公佈由C. Rigney et al發明之"遙控鑑認電話撥進用戶服務(RADIUS)"，與其他鑑認，認可及說明(AAA)服務者。

無線網路正顯現為網際網路之一重要層面。根據事實：一無線網路之唯一疆域係無線電信號強度。沒有連線以界定一網路內之一會員資格。沒有實質方法以限制無線電範圍以內之一系統為一無線網路之會員。超過任一其他網路技術之無線網路就需要一鑑認及存取控制之機構。不同團體目前正工作於發展一標準鑑認機構。目前被接受之標準是IEEE 802.11。

一RF為基礎網路之性質係由在發射機範圍內之任一無線電讓其任意截收封包。截收可能發生係藉使用高增益天線遠

超出用戶"工作"範圍。用迅速可用工具，偷聽者並非受限於只收集封包供以後分拆，但實質上能了解相互作用聚集像由一有效無線用戶所觀視之資訊網頁。一偷聽者亦能聽到弱鑑認交換，像某些資訊網站記錄輸入。偷聽者爾後可複製記錄接通與增益存取。

一旦一侵襲者已獲得一WLAN如何控制許可之知識時，他即能夠獲得進入其本身之網路，或者竊取一有效用戶之存取。若該襲擊者能模仿有效用戶之MAC位址且使用其指定IP位址，則偷竊一用戶之存取是簡單的。襲擊者可等待直至有效系統停止使用該網路為止，然後接管其網路內之位置。此可讓一襲擊者直接存取在一網路內所有裝置，或者用該網路以獲致存取較寬之網際網路，始終出現是被襲擊網路之一有效用戶。因此，在執行一WLAN中鑑認及譯密變成最重要關切。

鑑認係證明一個人之身分或在一通信內應用之程序。這種鑑認可讓服務業者確定該實體為一有效用戶且亦確定請求特定服務之用戶。鑑認與認可實質上具有十分特定之意義，雖然此兩名詞常被交互地使用，且實際上常未清楚地加以區別。

鑑認係一用戶建立對身分之一權利的程序-在本質上，使用一名稱之權利。有眾多技術可用以鑑認一用戶-密碼，生物統計學技術，智慧卡，憑證。

一名稱或身分具有與其相關聯之特徵。特徵係密切地受一名稱之影響(例如，在一憑證酬載內)或藉對應於該名稱

之一密鑰可將其儲存在一姓名住址錄或其他資料庫內。特徵會隨時間而改變。

許可係決定是否允許一身分(加上與該身分相關聯之一組特徵)來執行某些行動之程序，諸如存取一資源。注意容許執行一項行動並不保證能執行該行動。注意由不同實體在不同點處可完成鑑認及許可。

在一行動通信網路內，鑑認特徵係可讓行動通信網路確認無線裝置之身分的一網路能力，因而減少未經授權使用行動通信網路。此程序對電話用戶是透明的。當客戶打電話時他不需有任何動作即可鑑認其電話之身分。

鑑認典型上係包括一加密機制，其中服務業者與用戶具有一些共用資訊和一些私人資訊。該共用資訊典型上係指為一"共用秘密"。

A-密鑰

鑑認密鑰(A-密鑰)係一秘密值其對每一個人之行動電話為獨特的。它係與細胞式服務業者被暫存及被儲存在電話與鑑認中心(AC)內。此A-密鑰係由製造商程式設計在電話內。它亦可從無線裝置目錄功能內由用戶手動鍵入，或由在銷售點處一特別終端鍵入。

無線裝置和AC必須有相同之A-密鑰以產生相同計算。A-密鑰之主要功能係被使用為一參數以計算共用秘密資料(SSD)。

共用秘密資料(SSD)

SSD係被使用為在無線裝置及AC內鑑認計算用之一輸

入，且被儲存在兩地點。不像A-密鑰，SSD可透過網路加以修改。AC和無線裝置可共用係從事SSD計算之三個要素：1)電子序號(ESN)；2)鑑認密鑰(A-密鑰)；與3)「共用秘密資料」計算(RANDSSD)之一RANDom號碼。

透過網路及透過空中介面可發射ESN和RANDSSD。當一裝置其第一系統存取時，可更新SSD，且此後定期地予以更新。當計算SSD時，結果是兩個單獨值，SSD-A及SSD-B。使用SSD-A作鑑認用。使用SSD-B作譯密和語音隱密用。

視服務系統之能力而定，在AC與服務行動切換中心(MSC)間可共用或未共用SSD。若共用秘密資料，即表示AC會發送此秘密資料至服務MSC且服務MSC必須能夠執行細胞式鑑認語音譯密(CAVE)。若未共用秘密資料，則AC會保持此資料並執行鑑認。

共用之型式可影響如何進行一鑑認詢問。一鑑認詢問係發送一訊息以詢問無線裝置之身分。基本地，鑑認詢問可發送一些資訊，典型上為隨機數資料，供用戶處理。用戶然後處理此資訊並發送一回應。分析此回應供用戶之鑑認。以共用之秘密資料，在服務MSC處處理一詢問。藉共用秘密資料，此系統可使發送之通信量減至最少且可讓詢問在服務開關處更快發生。

鑑認程序

在一已知系統內，一本方位置暫存器(HLR)藉充當MSC與AC間之中間者就可控制鑑認程序。設定服務MSC即以

行動之HLR來支援鑑認，反之亦然。

若其能夠鑑認，此裝置可藉通知服務MSC即啟始該程序，即藉設定添加信號訊息鏈內之一許可欄位。在回應中，服務MSC用一「鑑認請求」可開始暫存/鑑認過程序。

藉發送該「鑑認請求」，服務MSC即告知HLR/AC是否其能夠執行CAVE計算。AC可控制從現有之該等能力使用服務MSC之能力以及裝置能力中之何者。當服務MSC未具有CAVE能力時，在AC與MSC間不可能共用SSD且因此在AC內可執行所有鑑認程序。

「鑑認請求」(AUTHREQ)之目的係在鑑認電話與請求SSD。AUTHREQ包括鑑認之兩參數，AUTHR和RAND參數。當AC獲得AUTHREQ時，它使用RAND和最後獲知之SSD以計算AUTHR。若它可匹配在AUTHREQ內所發送之AUTHR然後鑑認是成功。若其能共用，回復至AUTHREQ之結果就包含SSD。

詢問

鑑認程序係由一詢問與回應對話所組成。若共用SSD，對話即進行在MSC與裝置之間。若未共用SSD，則對話進行在HLR/AC與裝置之間。MSC係能夠作一獨特詢問，一全球詢問，或兩者視開關型式而定。有些MSCs目前並非有能力作全球詢問。獨特詢問係只在打電話嘗試期間所發生之一詢問，因為它使用語音頻道。獨特詢問呈現對在打電話開始與打電話傳送期間一單獨裝置的一鑑認。全球詢

問係在暫存，打電話開始，和打電話傳送期間所發生之一詢問。全球詢問顯現向使用一特殊無線電控制頻道之所有MSs的一鑑認詢問。其被稱為全球詢問因其係在無線電控制頻道上廣播，且由存取該控制頻道之所有電話來使用該詢問。

在一詢問中，該裝置可回應由MSC或AC所提供之一隨機數。該裝置可使用隨機數及在裝置內所儲存之共用秘密資料以計算給MSC之一回應。MSC亦可使用隨機數及共用秘密資料以計算所從裝置之回應。經由CAVE算法可完成此等計算。若回應並非相同，即否定服務。詢問程序並未增加其連接電話所花之時間量。事實上，電話可按某些情況進行，僅當鑑認未能成功時才予拆線。

無線本地區網路(WLANs)已非常普遍作為提供用戶開放存取IP資料網路之一裝置。亦設計第三代(3G)無線網路以提供高速資料存取；雖然其支援之資料率典型上是低於WLAN之資料率，但3G網路透過一甚較寬廣地區可提供資料涵蓋。即使其被視為網路競爭者，但WLAN和3G網路是可以互補：WLAN在公共地區諸如機場接待室和旅館候客廳可提供高容量"高熱點"涵蓋，同時3G網路能提供用戶有雖在進中幾乎無所不在之資料服務。因此，相同載波按一單獨用戶預訂可提供3G與WLAN兩種存取服務。此意示MS可用相同鑑認方法與秘密於兩型式之存取鑑認。

按3G存取鑑認，此鑑認中心(AC)可鑑認MS。AC與MS具有一共用秘密。在網路側上，共同秘密係牢固地儲存在

AC內且並未被分配給任何其他網路實體。在MS側上，共用秘密係牢固地被儲存在穩固記憶體內且未被分配在其外側。AC和MS可使用「細胞式鑑認語音譯密」(CAVE)或者鑑認密鑰協議(AKA)為鑑認算法。經由3G透過空中發送信號訊息與網路發送信號訊息(例如IS-41)在MS與AC之間傳送鑑認參數。

按WLAN存取鑑認，指望使用相同之共同秘密與鑑認算法(AKA或CAVE)可由相同AC來鑑認MS。然而，可使用不同機構以傳送WLAN內之鑑認參數。明確地，經由廣泛鑑認協定(EAP)與一AAA協定(RADIUS或直徑)即可傳送鑑認參數。該詢問係使在3G與WLAN間之傳送機構成網路而使在用於WLAN存取鑑認之MS與AC之間能傳送鑑認參數。

如本文內以上所述，CAVE算法係普遍使用於細胞式通信且因此，它係妥善使用與分配。亦可使用鑑認用之代替算法。明確地在資料通訊內種種不同算法確存在有複雜和應用之變化。為協調此等機構，廣泛鑑認協定(EAP)已發展為可支援多重鑑認和密鑰分配機構之一普遍協定構架。在1998年3月發表，RFC 2284，由L. Blunk et al所著之"PPP廣泛鑑認協定(EAP)"內說明EAP。

在2002年2月發表為一網際網路草案，由J. Arkko et al在"EAP AKA鑑認"內被界定由EAP所支援之一此種機構即係AKA算法。因此有需要擴大以包括細胞式算法CAVE。此乃期望提供新系統與網路之後備相容性。

EAP

廣泛鑑認協定(EAP)係可支援多重鑑認機構之鑑認用的一普遍協定。EAP並非在鏈設定和控制期間選擇一特定鑑認機構，反而可延緩此機構直至鑑認程序開始為止。此可讓鑑認者在決定特定鑑認機構以前要求更多資訊。此鑑認者係被界定為需要鑑認鏈之終端。鑑認者可明定在鏈建立期間內所使用之鑑認協定。

互通功能(IWF)

根據一個實例，一新網路實體係被實行且係指稱為互通功能(IWF)或更明確地，指稱AAA/IS-41互通功能(IWF)。IWF可互通無線網路，諸如3G，與WLAN網路之間鑑認參數(例如CAVE，AKA)之傳送機構。在圖2內說明一IWF 204為一通訊系統200之一部分。系統200包括一WLAN 202，一IWF 204及一AC 206。如圖示，一行動台208目前係在WLAN 202之通信範圍以內。IWF 204可提供在AC 206與WLAN 202之間一介面，容許使用一共同鑑認以讓MS 208獲存取網路。注意MS 208為一無線工作站，一遙控用戶，或係能夠經由WLAN 202以外一網路通信之其他無線裝置，按此情況該網路係其AC 206一部分之網路。

IWF 204係一單向互通功能，即，該鑑認請求係起始於WLAN 202。注意按現行實例及圖示，AAA係輸送在WLAN 202與IWF 204之間鑑認參數之傳送機構。而且，IS-41係輸送在IWF 204與AC 206之間之傳送機構。由此範例之明確，可使用RADIUS為AAA協定。

圖3說明鑑認處理。最初，IWF 204接收一RADIUS存取

一請求訊息其包含執行存取WLAN 202之鑑認所需要之MS 208(或無線工作站)身分。IWF 204係配置有儲存與MS 208相關聯之鑑認能力之一資料庫210，以及經由AC 206目前所暫存之其他MS 208。資料庫210係由每一MS 208身分予以指明。因此，IWF 204可決定MS 208之鑑認能力(例如，AKA及/或CAVE)。

若MS 208只支援CAVE，則IWF 204可執行以下與圖3一致之程序。IWF可發送一RADIUS存取詢問訊息其包括內含一CAVE詢問之一EAP請求訊息。如本文以上所論述，該詢問包含為計算一鑑認回應係由MS 208所使用之一隨機數。IWF 204可接收內含EAP回應訊息(包括CAVE詢問回應)之RADIUS存取請求訊息。CAVE回應包含MS 208鑑認回應，亦即，使用隨機數之計算結果，與對MS 208特定之其他參數。

若IWF 204係不能夠鑑認EAP回應訊息，或明確地不能夠鑑認對CAVE詢問之CAVE回應，IWF 204即發送係一IS-41訊息之AUTHREQ訊息至AC 206。按這種情形，IWF 204並未具有確定詢問回應所必要之資訊。AUTHREQ訊息包括指定給MS 208之IMSI，隨機數(即詢問)，及由MS 208所產生之鑑認回應。具有對MS 208特定之共用秘密知識之AC 206然後確定MS 208之詢問回應。AC 206可回復為一IS-41訊息之AUTHREQ訊息至IWF。AUTHREQ訊息包含鑑認結果。若成功，AUTHREQ訊息亦包含稱為「細胞式訊息譯密算法」(CMEA)密鑰之一密鑰，使用此一密鑰以保

護在WLAN 202內之MS 208通信。若IWF 204在重嘗試一預定數以後係不能接收來自AC 206之AUTHREQ訊息，IWF 204即發送含EAP失敗之RADIUS存取一拒絕訊息至WLAN 202。不能接收一AUTHREQ訊息即指示在IWF 204與AC 206間之網路問題。

若IWF 204係能夠鑑認來自MS 208之詢問回應，且此種鑑認是成功的，則IWF 204即產生CMEA密鑰。若MS 208係成功地被鑑認，IWF 204即發送一RADIUS存取一接受訊息至WLAN 202。此種訊息包括一EAP-成功訊息和CMEA密鑰。若MS 208未能鑑認，IWF 204即發送一含EAP-失敗訊息之RADIUS存取一拒絕訊息至WLAN 202。

圖4說明按照一個實例之一鑑認程序400，其中MS 208可支援CAVE協定。當MS 208與WLAN 202在步驟402處開始鑑認協商時，程序就開始。亦在此步驟處，WLAN 202發送一含MS 208身分之RADIUS存取請求訊息。如本文上述所示，藉由IMSI或MS 208之其他獨特識別碼即可提供該身分。此程序包括MS 208尋求存取WLAN 202且在回應中，WLAN 202在步驟402處請求自MS 208之鑑認。在此點處，IWF 204可發送一RADIUS存取詢問訊息之WLAN 202，包含在步驟404處之CAVE詢問。為回應此詢問，MS 208可計算一回應並可提供回應至WLAN 202(圖未示)。然後發送此回應至步驟406處在一RADIUS存取回應訊息內之IWF 204。若IWF 204並未具有在決策步驟408處供MS 208之共用秘密知識，則處理持續至驟410其中IWF 204可發送一

AUTHREQ訊息至AC 206。AUTHREQ訊息可請求MS 208之鑑認。若在決策步驟412處獲得一AUTHREQ訊息，處理即持續至決策步驟414以決定是否AUTHREQ訊息係指示成功之鑑認，亦即，鑑認之結果是准予存取WLAN。若在決策步驟412處未接收AUTHREQ訊息，處理即持續至步驟416，其中IWF可發送一RADIUS存取拒絕訊息。

自決策步驟408繼續，若IWF 204具有MS 208共用秘密資訊知識，IWF 204即能決定是否在決策步驟418處鑑認是成功的。成功的鑑認可進行至步驟420以計算CMEA密鑰。然後在步驟424處發送一RADIUS存取接受訊息。注意在步驟414處(供由AC 206鑑認)成功之鑑認亦可進行至步驟420。從決策步驟418處，若鑑認未成功，IWF在步驟422處發送一RADIUS存取拒絕訊息。

在一代替實例中，IWF 204可使用AKA協定供發送一詢問。如圖5所示，若MS 208可支援AKA，IWF 204即執行AKA詢問，且可變更鑑認處理之次序。按此狀況，在一鑑認向量(AV)內可提供足以鑑認一用戶之資訊，諸如MS 208。注意AC 206可發送AV內之共用秘密(SS)資訊至IWF 204。依據本實例，AV包括SS，詢問與一密碼密鑰(CK)。使用CK於譯密MS通信。

若IWF 204未具有鑑認向量(AV)以鑑認MS 208，則IWF 204即發送一AUTHREQ訊息以請求來自AC 206之AV。AUTHREQ訊息包括MS 208之身分，諸如IMSI，及AV之請求。AC 206係用含AV之AUTHREQ訊息來回答。AV係由一

隨機數(RAND)，一預期回應(XRES)，一密碼密鑰(CK)，與一鑑認標誌(AUTN)所組成。AC可提供在AUTHREQ訊息內多重AVs，如此IWF並不需要請求自AC 206之隨後鑑認。

若IWF 204係不能接收自AC 206(其係在有些重試預定數之後)之AUTHREQ訊息，則IWF 204可發送含一EAP-失敗訊息之一RADIUS存取拒絕訊息至WLAN 202，諸如當在IWF 204與AC 206間有網路問題時就如此。

若接收之AUTHREQ並未包括AV，則IWF 204即發送含EAP-失敗訊息之RADIUS存取一拒絕訊息至WLAN 202。例如，當MS 208具有一期滿之預訂時這種情況就顯現。

若IWF 204具有AV，IWF 204即發送一RADIUS存取詢問訊息內含具有一AKA詢問之EAP-請求訊息至WLAN 202。AKA詢問包括AUTN及RAND。AUTN可傳送AC 206證書且係由MS 208予以鑑認。RAND係詢問用以計算一鑑認回應(RES)之MS 208。MS 208可提供RES至WLAN 202。

IWF 204可接收RADIUS存取一請求訊息內含一EAP-回應包括來自WLAN 202之一CAVE詢問。CAVE詢問包含經由WLAN 202接收之MS 208鑑認回應(RES)。IWF 204可比較RES與XRES比較。關於一匹配，MS 208係成功地被鑑認，且IWF 204可發送一RADIUS存取一接受訊息至WLAN 202。此種訊息包含一EAP-成功訊息和一CK。CK係用以保護WLAN 202內之MS 208通信。若MS 208未能鑑認，IWF 204即發送含EAP-失敗訊息之一RADIUS存取一拒絕訊息至

WLAN 202。

圖6說明使用AV之一鑑認程序500。若IWF 204具有AV足以鑑認在決策步驟502處之MS 208，則程序繼續至步驟506，否則處理即繼續至步驟504。在步驟506處IWF 204可發送一RADIUS存取詢問訊息至MS 208之WLAN 202。然後此詢問被轉交至MS 208處理，且提供一回應回至WLAN 202(圖未示)。IWF 204可接收在步驟510處之RADIUS存取請求訊息，且決定是否MS鑑認在決策步驟512處是成功。對一成功之鑑認，IWF 204可在步驟514處發送一RADIUS存取接受訊息，否則IWF 204可在步驟516處發送一RADIUS存取拒絕訊息。

回復至決策步驟502，若IWF 204未具有AV，IWF 204即發送一AUTHREQ訊息至步驟504處之AC 206。在AV接收時，IWF 204繼續處理至步驟506，否則處理可繼續至步驟516。

圖7說明一IWF 600適合於成介面介於一WLAN(圖未示)，且因此能夠執行因通信，鑑認，密鑰交換，及其他與其安全通信所必要之程序，與一AC(圖未示)之間，且能夠執行因通信，鑑認，密鑰交換，及其他與其安全通信所必需之程序。IWF 600包括一WLAN介面單元602，其中可準備，發射，接收，及/或說明與一WLAN通信。同樣，IWF 600包括一AC介面單元604，其中可準備，發射，接收，及/或說明與一AC通信。IWF 600更包括一CAVE程序器608，一EAP程序器610，與一RADIUS程序器612。IWF

600可包括因在一已知系統內互通功能所需之任何數量此種程序器(圖未示)。諸程序器，諸如CAVE程序器608，EAP程序器610及RADIUS程序器612，均可在軟體，硬體，韌體，或其一聯合內予以執行。在IWF 600以內不同模組可經由通信匯流排614通信。

精於技藝之人員會了解：使用任何種種不同之科技及技術即可代表資訊及信號。例如，資料，指示，指令，資訊，信號，位元，符號，及晶片在整個上面說明所指者，均可藉電壓，電流，電磁波，磁場或質粒，光學場或質粒，或其任何聯合代表之。

精於技藝之人員更了解：不同說明性邏輯方塊，模組，電路，及與本文內所揭示實例有關之所述算法步驟均可視為電子硬體，電腦軟體，或兩者之聯合予以執行。為清楚地說明硬體和軟體之此種互換性，不同說明元件，方塊，模組，電路及步驟一般而言就其功能性已說明如上。是否此種功能性係可執行如硬體或軟體端視施加於整個系統上之特殊應用與設計限制而定。精技人員對每一特殊應用可按不同方式執行所述之功能性，但此種實施決算並非解釋為引起偏離本發明之範疇。

不同之說明邏輯方塊，模組，及有關本文內所揭示實例所述之電路均可用一通用處理單元，一數位信號處理單元(DSP)，一專用積體電路(ASIC)，一場可程式製作閘極陣列(FPGA)或其他可程式製作邏輯裝置，分離閘極或電晶體邏輯，分離硬體組成件，或執行本文內所述功能所設計之

其任何組合予以實施或執行。一通用處理單元可為一微處理單元，但在另一選擇上，此處理單元可為任一習用處理單元，控制器，微控制器，或狀態機器。一處理單元亦可被執行為計算裝置之組合，例如一DSP和一微處理單元之組合，眾多微處理單元，一個或多個微處理單元連同一DSP磁圈，或任何其他此種配置。

有關本文內揭示實例所述之一方法或算法之步驟可直接被包含在硬體內，在一由處理單元所執行之軟體模組內，或在兩者之組合內。一軟體模組係存在於RAM記憶體，快閃記憶體，ROM記憶體，EPROM記憶體，EEPROM記憶體，暫存器，硬光碟，一可拆除光碟，一CD-ROM，或技藝內熟知之任何其他形式之儲存媒體。一典型儲存媒體係被耦合至處理單元如此使處理單元可自儲存媒體讀入資訊，且可寫出資訊至儲存媒體。或者，儲存媒體係處理單元所必需的。處理單元和儲存媒體係存在於ASIC。ASIC係存在於一用戶接線端。另一選擇，處理單元和儲存媒體係為各別組成件存在於一用戶接線端。

提供揭示實例之前述說明以使精於技藝人員能完成或使用本發明。此等實例之不同修改對精於技藝人員是顯而易見，且本文內所界定之一般原則可被應用於其他實例而沒有違背本發明之精神或範圍。因此，本發明並非欲限定本文內所示之實例，但係符合與本文內所揭露原則及特徵一致之最廣範圍。

【圖式簡單說明】

圖1係包括一無線區域網路(WLAN)之一通信系統。

圖2係具有一互通功能(IWF)器之一通信系統。

圖3係在一通信系統內之一鑑認程序之時序圖。

圖4係一鑑認程序之流程圖。

圖5係在一通信系統內之一鑑認程序之時序圖。

圖6係在一通信系統內在一IWF處一鑑認程序之一流程圖。

圖7係在一行動台處鑑認處理之一流程圖。

【主要元件符號說明】

100, 202	無線區域網路
102	工作站
106, 108, 111, 208	存取點
204	互通功能
602	WLAN介面
604	AC介面
606	中央處理單元
608	CAVE程序
610	EAP程序
612	RADIUS程序

201123772

分割子案

發明專利說明書　中文說明書

分割案

（本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫）

※ 申請案號：100103772

※ 申請日：92.6.20　※IPC 分類：H04L 12/28 (2006.01)

H04W 12/00 (2006.01)

原申請案號：092116827

一、發明名稱：（中文/英文）

通信系統之互通功能

INTER-WORKING FUNCTION FOR A COMMUNICATION SYSTEM

二、中文發明摘要：

本發明係關於介接一無線區域網路(WLAN)與一通信系統之互通功能(IWF)。IWF可包含充足資訊以鑑認一用戶存取WLAN，或者IWF係需要請求來自通信系統之鑑認。按一個實例，IWF可發送一存取詢問至一用戶之WLAN。IWF然後將一回應該詢問傳遞給通信系統以供鑑認。IWF可讓WLAN使用通信系統之鑑認能力供本地鑑認。

三、英文發明摘要：

Inter-Working Function (IWF) for interfacing between a Wireless Local Area Network (WLAN) and a communication system. The IWF may contain sufficient information to authenticate a user access to the WLAN, or the IWF may need to request authentication from the communication system. In one embodiment, the IWF sends an access challenge to the WLAN for a user. The IWF may then pass a response to the challenge on to the communication system for authentication. The IWF allows the WLAN to use the authentication capability of the communication system for local authentication.

七、申請專利範圍：

1. 一種與一無線區域網路(WLAN)及具有一無線裝置之一蜂巢式通信網路通信之互通功能(IWF)裝置，該IWF裝置包含：

一WLAN介面，以自該無線裝置接收一認證存取請求以用於存取該WLAN，該認證存取請求由該無線裝置基於一預定認證金鑰產生；及

一存取控制(AC)介面，以傳輸該認證存取請求至該蜂巢式通信網路，及以接收由該蜂巢式通信網路基於該預定認證金鑰所產生之一認證存取回應，其中其決定該IWF是否持有認證該無線裝置所需之資訊以用於存取該WLAN，其中若該IWF未持有認證該無線裝置所需之該資訊以用於存取該WLAN，該認證存取請求被傳輸至該蜂巢式通信網路，及其中若其決定該IWF已經持有認證該無線裝置所需之該資訊以用於存取該WLAN，該認證存取請求不會被傳輸至該蜂巢式通信網路。

2. 如請求項1之IWF裝置，其包含：

一資料庫，其與該WLAN與該等AC介面通信以儲存對應於該無線裝置之認證資訊；及

一處理器，其與該資料庫、該WLAN與該等AC介面通信。

3. 如請求項1之IWF裝置，該認證資訊包含對應於該無線裝置之至少一認證能力及認證程序指令。

4. 如請求項1之IWF裝置，該認證請求包含一認證訊息。

5. 如請求項4之IWF裝置，該認證訊息包含至少一蜂巢式認證聲音加密(CAVE)訊息及認證金鑰協議(AKA)訊息。

6. 如請求項1之IWF裝置，該IWF裝置以透過一第一傳輸埠與該WLAN通信，以及透過一第二傳輸埠與該蜂巢式通信網路通信。

7. 如請求項4之IWF裝置，其中該預定認證金鑰對應至該認證訊息。

8. 一種用於藉由一蜂巢式通信網路認證一無線裝置以用於存取一無線區域網路(WLAN)，該方法包含：

由該無線裝置基於一預定認證金鑰產生一認證存取請求；

透過與該無線裝置及該蜂巢式通信網路通信之一互通功能(IWF)裝置中該WLAN自該無線裝置接收該認證存取請求；

若該IWF未持有認證該無線裝置所需之資訊以用於存取該WLAN，由該IWF傳輸已接收之該認證存取請求至該蜂巢式通信網路，其中其決定該IWF是否持有認證該無線裝置所需之資訊以用於存取該WLAN，及其中若其決定該IWF已經持有認證該無線裝置所需之該資訊以用於存取該WLAN，該認證存取請求不會被傳輸至該蜂巢式通信網路；及

若該IWF未已經持有認證該無線裝置所需之資訊以用於存取該WLAN：

由該蜂巢式通信網路基於該預定認證金鑰認證該認證

存取請求；及

接收由該蜂巢式通信網路基於該預定認證金鑰所產生之一認證存取回應。

9. 如請求項8之網路，進一步包含：

若該蜂巢式通信網路認證基於該預定認證金鑰該認證存取請求，藉由該WLAN同意無線裝置存取該WLAN。

10. 如請求項8之網路，該認證存取請求透過一第一傳輸協定接收於該IWF裝置。

11. 如請求項8之網路，該認證存取請求透過一第二傳輸協定被傳輸至該蜂巢式通信網路。

12. 一種與一無線區域網路(WLAN)通信及與一無線裝置通信之一蜂巢式通信網路通信之互通功能(IWF)裝置，該IWF裝置包含：

產生構件，其用於由該無線裝置基於一預定認證金鑰產生一認證存取請求；

接收構件，其用於透過與該無線裝置及該蜂巢式通信網路通信之一互通功能(IWF)裝置中該WLAN自該無線裝置接收該認證存取請求；

傳輸構件，用於由該IWF傳輸已接收之該認證存取請求至該蜂巢式通信網路，其中其決定該IWF是否持有認證該無線裝置所需之資訊以用於存取該WLAN，其中若該IWF未持有認證該無線裝置所需之該資訊以用於存取該WLAN，該認證存取請求被傳輸至該蜂巢式通信網路，及其中若其決定該IWF已經持有認證該無線裝置所

需之該資訊以用於存取該WLAN，該認證存取請求不會被傳輸至該蜂巢式通信網路；

認證構件，其用於藉由該蜂巢式通信網路基於該預定認證金鑰認證該認證存取請求；及

接收回應構件，其用於接收由該蜂巢式通信網路基於該預定認證金鑰所產生之一認證存取回應。

13. 一種用於藉由一蜂巢式通信網路認證一無線裝置以用於存取一無線區域網路(WLAN)之電腦程式產品，該電腦程式產品包含具有指令於其上之一電腦可讀取儲存媒體，該等指令包含：

用於由該無線裝置基於一預定認證金鑰產生一認證存取請求之程式碼；

用於透過與該無線裝置及該蜂巢式通信網路通信之一互通功能(IWF)裝置中該WLAN自該無線裝置接收該認證存取請求之程式碼；

用於由該IWF傳輸已接收之該認證存取請求至該蜂巢式通信網路之程式碼，其中其決定該IWF是否持有認證該無線裝置所需之資訊以用於存取該WLAN，其中若該IWF未持有認證該無線裝置所需之該資訊以用於存取該WLAN，該認證存取請求被傳輸至該蜂巢式通信網路，及其中若其決定該IWF已經持有認證該無線裝置所需之該資訊以用於存取該WLAN，該認證存取請求不會被傳輸至該蜂巢式通信網路；

於藉由該蜂巢式通信網路基於該預定認證金鑰認證該

認證存取請求之程式碼；及

於接收由該蜂巢式通信網路基於該預定認證金鑰所產生之一認證存取回應之程式碼。

八、圖式：

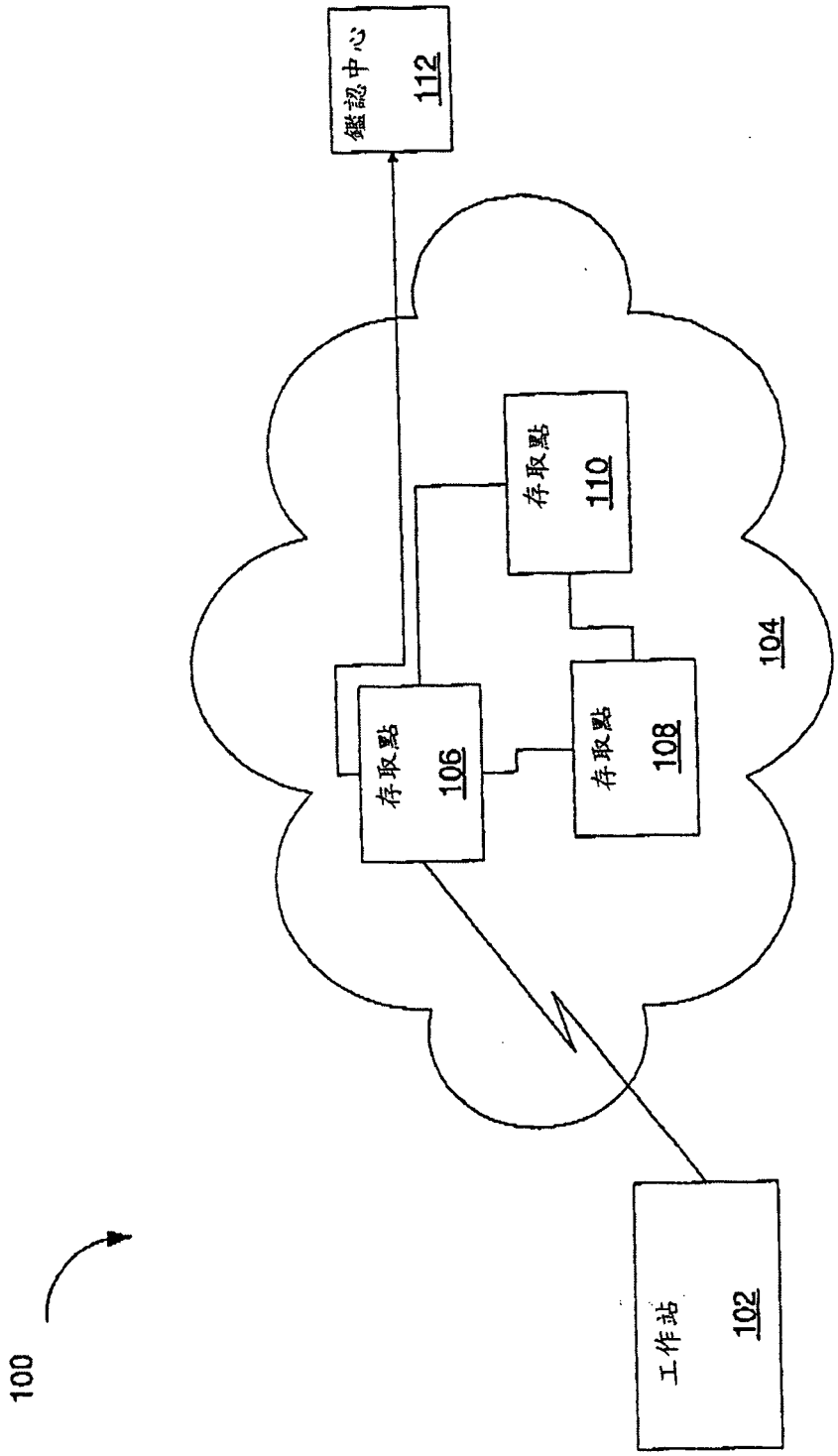


圖 1

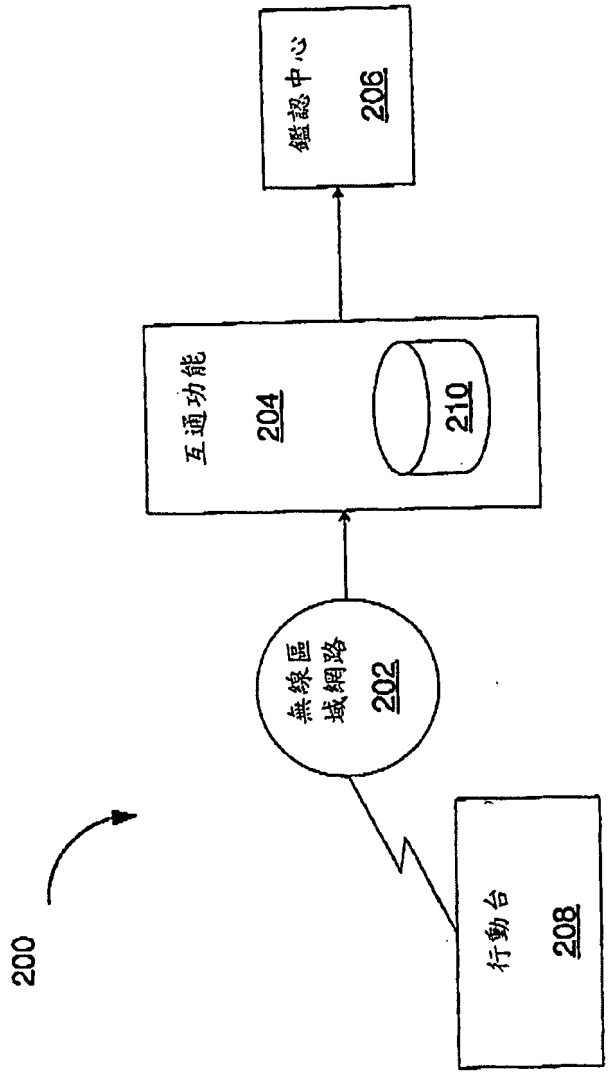


圖 2

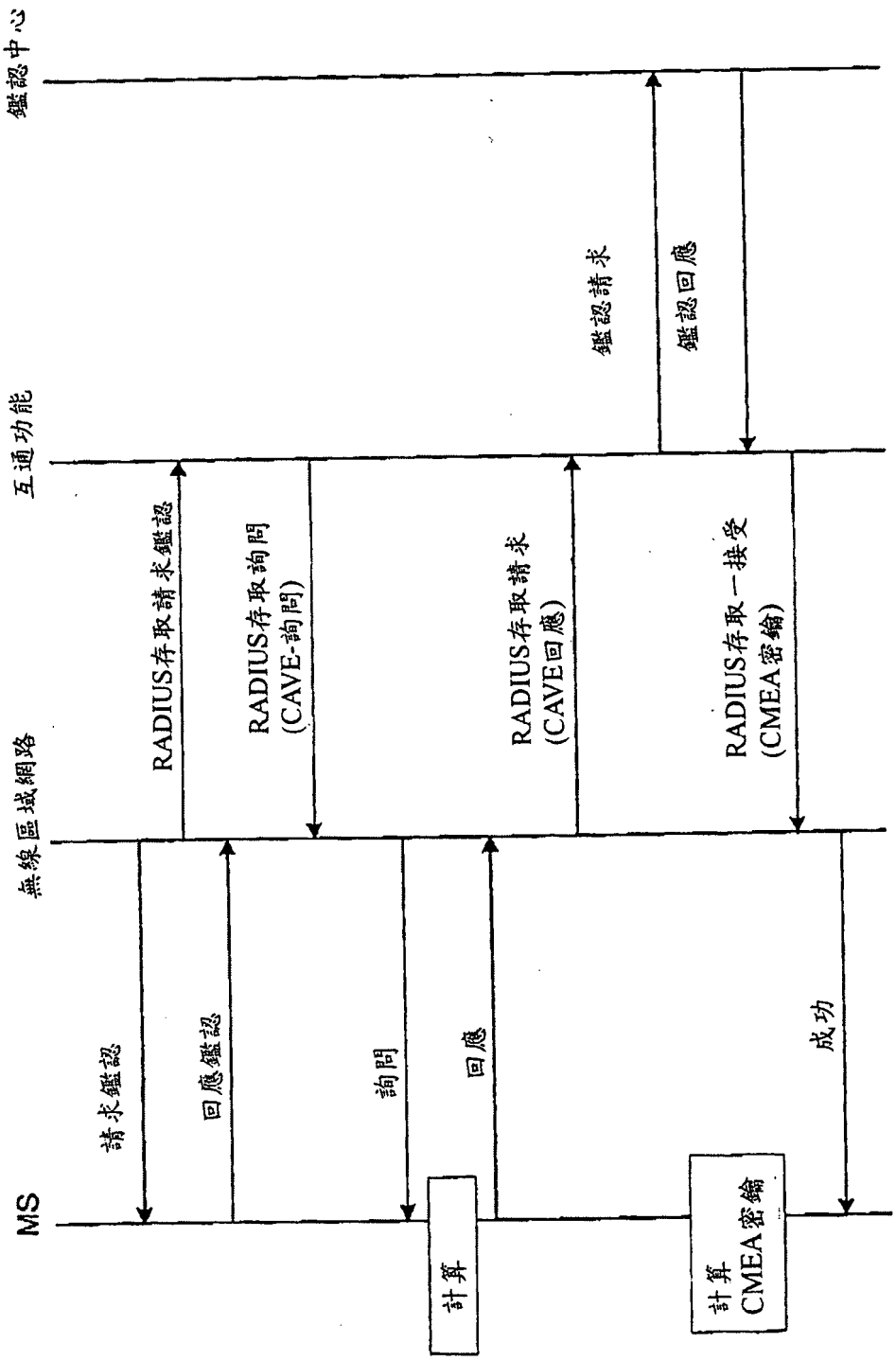

鑑認中心
互通功能
無線區域網路
MS
RADIUS存取請求鑑認
RADIUS存取詢問
(CAVE-詢問)
RADIUS存取請求
(CAVE回應)
RADIUS存取－接受
(CMEA密鑰)
鑑認請求
鑑認回應
請求鑑認
回應鑑認
詢問
回應
成功
計算
計算
CMEA密鑰

圖 3

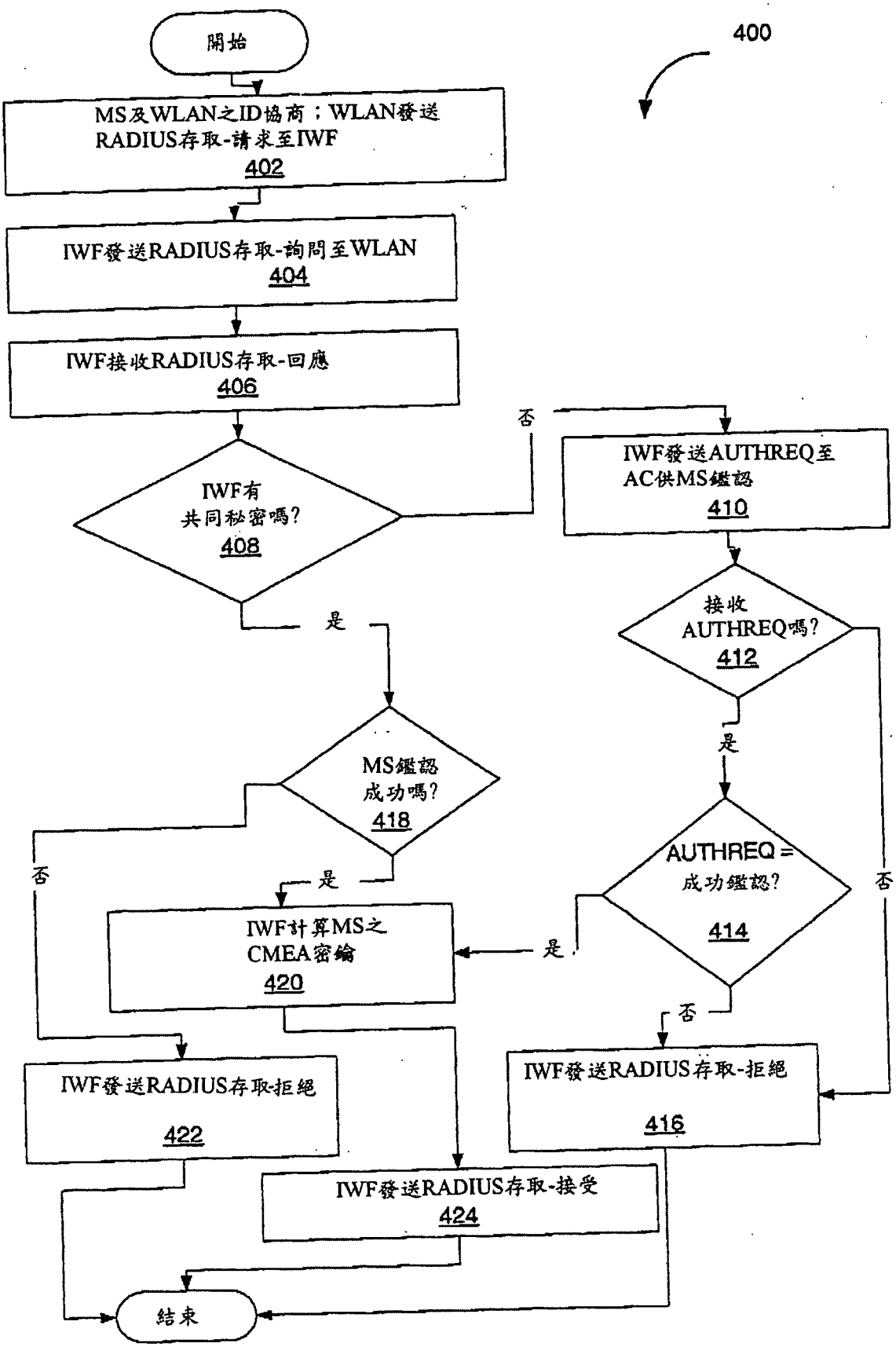

開始
400
MS及WLAN之ID協商；WLAN發送RADIUS存取-請求至IWF
402
IWF發送RADIUS存取-詢問至WLAN
404
IWF接收RADIUS存取-回應
406
IWF有共同秘密嗎?
408
否
是
IWF發送AUTHREQ至AC供MS鑑認
410
接收AUTHREQ嗎?
412
是
否
AUTHREQ=成功鑑認?
414
是
否
MS鑑認成功嗎?
418
否
是
IWF計算MS之CMEA密鑰
420
IWF發送RADIUS存取-拒絕
422
IWF發送RADIUS存取-拒絕
416
IWF發送RADIUS存取-接受
424
結束

圖 4

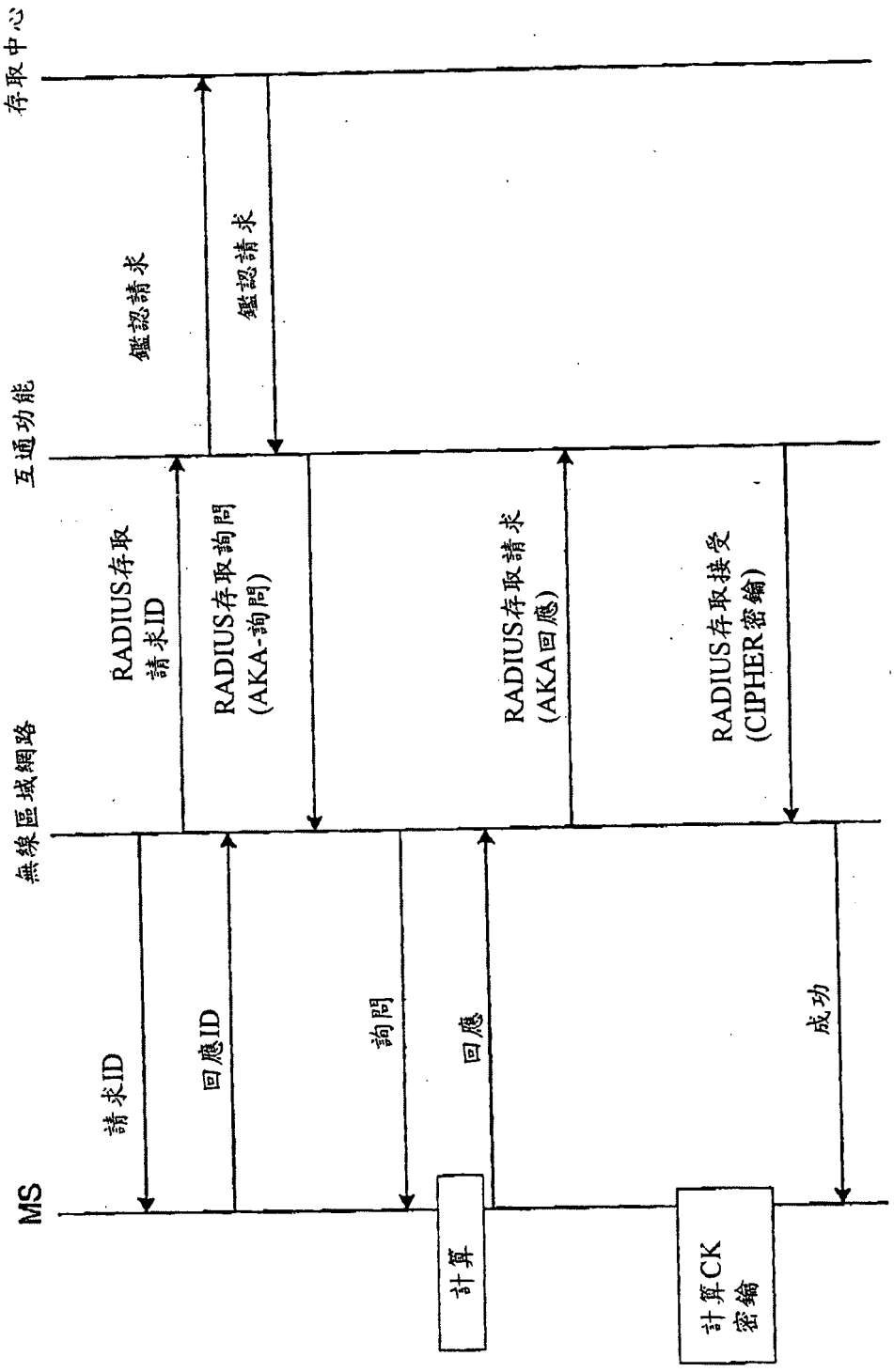

MS
無線區域網路
互通功能
存取中心
請求ID
回應ID
RADIUS存取
請求ID
鑑認請求
鑑認請求
詢問
RADIUS存取詢問
(AKA-詢問)
回應
RADIUS存取請求
(AKA回應)
成功
RADIUS存取接受
(CIPHER密鑰)
計算
計算CK
密鑰

圖 5

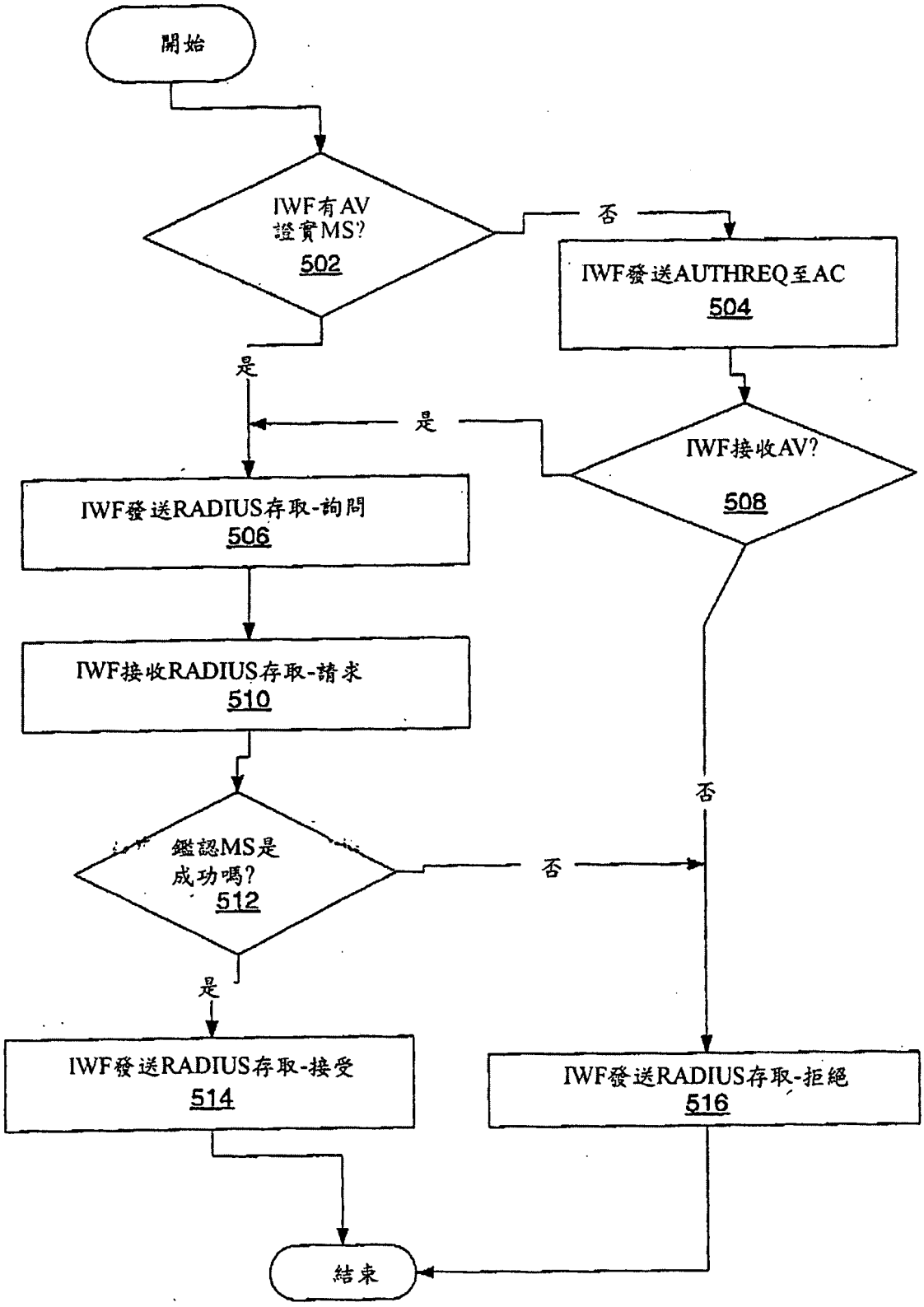

開始
IWF有AV證實MS?
502
否
IWF發送AUTHREQ至AC
504
是
是
IWF接收AV?
508
IWF發送RADIUS存取-詢問
506
IWF接收RADIUS存取-請求
510
否
鑑認MS是成功嗎?
512
否
是
IWF發送RADIUS存取-接受
514
IWF發送RADIUS存取-拒絕
516
結束

圖 6

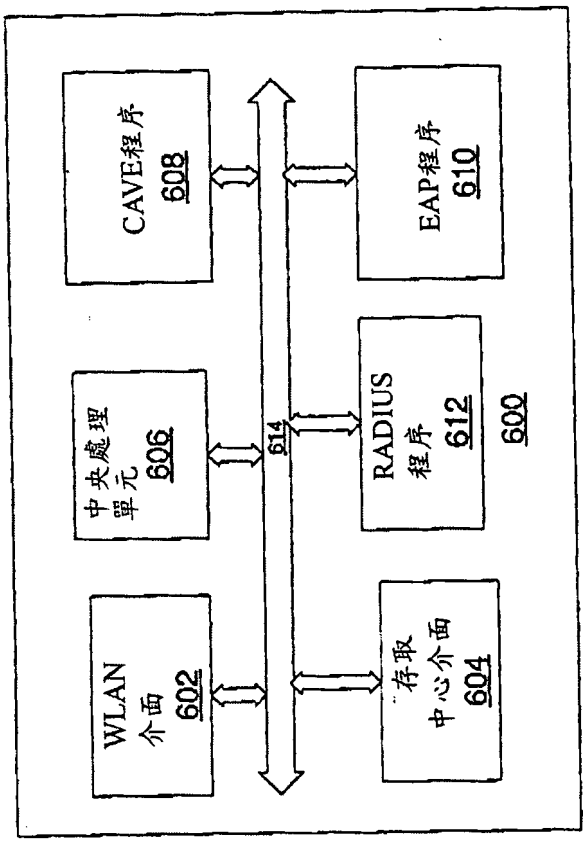

CAVE程序
608
EAP程序
610
中央處理
單元
606
614
RADIUS
程序
612
600
WLAN
介面
602
存取
中心介面
604

圖 7

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：

(無元件符號說明)

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)