

公告本

(此處由本局於收
文時黏貼條碼)

99年6月1日修正替換頁

發明專利說明書

(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：95102734

※ 申請日期：95.1.25

※IPC 分類：H04L 12/18 (2006.01)

一、發明名稱：(中文/英文)

H04L 29/06 (2006.01)

使用單向網路連結之 GAA 功能實行鑑定之方法及系統

Authentication using GAA functionality for unidirectional network connections

二、申請人：(共 1 人)

姓名或名稱：(中文/英文)

諾基亞股份有限公司 / NOKIA CORPORATION

代表人：(中文/英文)

塔格奈堤 維皮 / TOGNETTY, VIRPI

住居所或營業所地址：(中文/英文)

芬蘭艾斯浦·克萊萊登堤 4 號

Keilalahdentie 4, 02150 Espoo, Finland

國 籍：(中文/英文) 芬蘭/FI

三、發明人：(共 1 人)

姓 名：(中文/英文)

佩卡雷笛寧 / Pekka LAITINEN

國 籍：(中文/英文)

芬蘭 FI

四、聲明事項：

☐ 主張專利法第二十二條第二項☐第一款或☐第二款規定之事實，其事實發生日期為： 年 月 日。

☐ 申請前已向下列國家（地區）申請專利：

【格式請依：受理國家（地區）、申請日、申請案號 順序註記】

☐ 有主張專利法第二十七條第一項國際優先權：

1. 歐盟 2005/2/3 05002300.1
2. 美國 2005/4/19 11/108,848

☐ 無主張專利法第二十七條第一項國際優先權：

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號 順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料 【格式請依：寄存機構、日期、號碼 順序註記】

國外生物材料 【格式請依：寄存國家、機構、日期、號碼 順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

五、中文發明摘要：

本發明有關一種方法、一客戶端實體、網路實體、一系統、與一電腦程式產品在一客戶端實體與一網路之間執行鑑定。該網路包括至少一引導伺服器功能實體與一網路應用功能實體。該客戶端實體是不能以雙向方法與兩網路實體通訊。在該客戶端實體與該引導伺服器功能實體之間的 3GPP 標準 Ub 參考點不是用於鑑定目的，例如使用單向網路連接的 GAA 功能之鑑定。

六、英文發明摘要：

Methods, a client entity, network entities, a system, and a computer program product perform authentication between a client and a network. The network includes at least a bootstrapping server function entity and a network application function entity. The client entity is not able to communicate with both of the network entities in a bi-directional manner. The 3GPP standard Ub reference point between the client entity and the bootstrapping server function entity is not utilized for authentication purposes, such as authentication using GAA functionality for unidirectional network connections.

七、指定代表圖：

(一)本案指定代表圖為：第 (5) 圖。

(二)本代表圖之元件符號簡單說明：

無

● **八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：**

九、發明說明：

【發明所屬之技術領域】

本發明有關用以在一客戶端實體與一網路之間鑑定之方法、網路實體、一系統、與一電腦程式產品，其中該客戶端實體不能以雙向方法與網路通訊。特別是，本發明是有關在例如廣播情況中，使用根據一般鑑權架構(GAA與)功能實施鑑定。

【先前技術】

近幾年來，各種不同種類通訊系統，特別是行動及/或以 IP 為主之(IP：網際網路協定)通訊系統、以及在這些系統中所提供的多數服務已發展成。

在此進階通訊系統中，目前在第三代合作夥伴計劃(3GPP)發展下的例如第三代行動通訊網路、有關安全與信賴的部份正扮演越來越重要的角色。

從用戶憑證的觀念，可支援行動操作員提供的服務，且其規定可協助行動操作員，而且是在更一般安全能力的需求的考慮方面，3GPP 標準化工作近來集中在一般鑑權架構(GAA)。圖 1 顯示與一本籍用戶系統 HSS 14、一使用者設備 UE 12、與一網路實體 NE 13 有關的一般鑑權架構環境概述，GAA 11 基本上是由三個子部份所組成。即是，一般引導架構(GBA)11b、用戶憑證 11a、一驗證代理(AP)11c 例如根據安全超媒體傳輸協定(HTTPS)。藉此，一般引導架構(GBA)亦建立供其他子部份的基礎，在於 GBA 可根據一分享的秘密而提供用於各種不同應用的一般鑑權力。通常，

GBA 功能是要引導應用安全的鑑定與主要協議，而且它是根據 IETF RFC 3310 的 HTTP Digest AKA(密鑰確認協定)機制。

圖 2 描述一般引導網路模型。經由一雙向鏈路 Ub 連接的一引導伺服器功能 BSF 13a 與使用者設備 UE 12 是使用 AKA 協定互相鑑定，而且同意會談秘鑰。這些秘鑰然後用於引導會談，並使用在使用者設備 12 與一操作員控制網路應用功能 NAF 13b 之間，而且其中 NAF 13b 經由一雙向鏈路 Ua 而亦連接到使用者設備 12。在下面詳細的引導程序後，使用者設備 12 與網路應用功能 13b 可執行一些應用特殊協定，其中訊息的鑑定將根據在相互鑑定期間所產生的這些會談秘鑰。因此，GAA/GBA 通常可視為 3 方證定情況，其中引導伺服器功能 13a 是進一步連接到一本籍用戶系統 HSS 14，以維持例如使用者安全設定(USS)。

圖 2 的個別實體之間的參考點(介面)是以 Ub、Ua、Zn、和 Zh 表示。介面 Zn 和 Zh 是根據 Diameter(根據在 IETF RFC 3588 中所指定的 Diameter 基頻)，介面 Ub 是根據 HTTP Digest AKA 訊息的再用，且在介面 Ua 上使用的協定是取決於執行的應用。

一般引導架構的利用是被分成兩階段。第一階段，即是(一般)引導程序是如圖 3 的描述；與第二相位，即是一般引導使用程序是在圖 4 描述。

在圖 3 的引導程序中，使用者設備 UE 12 將一 HTTP 請求傳送給引導伺服器功能 BSF 13a(步驟 S31)。在步驟 S32

中，BSF 13 可在來自本籍用戶系統 HSS 14 的 Zh 介面上取回使用者個人資料與挑戰，即是鑒權向量(AV)。然後，在步驟 S33 中，BSF 13a 將鑑定參數 RAND 和 AUTN 轉送給使用者設備 12，為了要求使用者設備 UE 12 對本身進行鑑定。使用者設備 UE 12 可計算訊息鑑定碼(MAC)，如此可確認來自鑑定網路的挑戰，以及計算會談密鑰 CK、IK、和 RES。因此，會談密鑰 CK、IK、和 RES 可使用在 BSF 13a 與使用者設備 UE 12。在步驟 S35 中，使用者設備 UE 12 可將一請求重新傳送給 BSF 13a，且 BSF 13a 會在步驟 S36 檢查接收的參數是否使用 RES 計算，並等於類似使用 XRES 計算的參數，其中 XRES 是在當作來自 HSS 14 的一部分鍵定向量之前已獲得。如果這些參數相等，使用者設備 UE 12 可被鑑定，且 BSF 13a 通過連接會談密鑰 CK 和 IK(步驟 S37)而產生一鑰匙("主鑰")Ks。主鑰 Ks 然後用於確保 Ua 介面。在步驟 S38 中，經由鑑定成功的表示，BSF 13a 可將包括一交易識別符 B-TID 和其他可能資料(例如，主鑰 Ks 的壽命)的一 OK 訊息傳送給使用者設備 UE 12。通過連結會談密鑰 CK 和 IK，用於確保 Ua 介面的主鑰 Ks 然後亦會在使用者設備 UE 12 產生(步驟 S39)。其後，在使用者設備(客戶端)與引導伺服器功能間的一引導連接便已成功開始。

圖 4 描述使用一引導安全聯接的一範例程序。在開始一引導連接(S40a)後，使用者設備 UE 12 可開始與網路應用功能 NAF 13b 通訊。藉此，在使用者設備 UE 12 與在 BSF 13a 的引導程序期間所產生的主鑰 Ks 可用來取得 NAF 特殊主

鑰 K_s_NAF (步驟 S40b)。一應用請求(步驟 S41)包括在引導會談獲得的交易視別符 B-TID，一應用特殊資料組是以 msg 表示，且所有適合性是以 MAC 表示。在步驟 S42 中，NAF13b 可在來自 BSF 13a 的 Zn 介面上請求一個或多個密鑰、與對應使用者設備 UE 12 所供應資訊的使用者個人資料。此一請求可例如根據交易識別符。在步驟 S42 與 S43 之間，NAF 特殊主鑰 K_s_NAF 是在 BSF 實體 13a 中產生。在步驟 S43 中，BSF 13a 是通過將請求的密鑰或一些密鑰(包括 K_s_NAF 、與 Prof 所表示應用特殊部份的使用者個人資料)供應給 NAF 13b 而回應，且 NAF 13b 是直接使用，或 NAF 13b 取得保護在使用者設備 UE 12 的 Ua 介面上所使用協定所需的進一步密鍵，且其是應用特殊功能，且不在 GAA 規格中描述。此一衍生是以與先前使用者設備 UE 12 所做的相同方法執行。

然後，NAF 實體 13b 儲存(步驟 S44)至少參數 K_s_NAF 、Prof、與密鑰的壽命。然後，NAF 13b 通過將一應用回應傳送給 UE 12 而以在 Ua 介面上所使用的協定繼續(步驟 S45)。

若要更多有關一般引導架構的描述，可參考 2004 年 12 月的技術規格 3GPP TS 33.220(版本 6.3.0)。

鑑於前述傳統一般鑑權架構與一般引導架構，下面問題會發生。

概括而言，正常傳統 3GPP GAA 行為是一客戶端，即是一使用者設備，使用一 AKA 鑑權向量的 BSF 實體引導。結果，所謂的 GAA 適合性可獲得，且是由一分享的主鑰 K_s

與一引導交易識別符(B-TID)所組成。這些 GAA 適合性是進一步用來取得一伺服器特殊鑰(Ks_NAF)。NAF 特殊鑰(即是 B-TID 和 Ks_NAF)然後可使用在客戶端 UE 與伺服器 NAF 之間，例如當作在既有協定中的使用者名稱/密碼，此情況是以術語"一般"表示。

傳統引導程序需要客戶具有一雙向連接到 BSF 實體，且在 UE 與 NAF 之間的 NAF 特殊適合性之隨後使用典型亦需要此。因此，問題會存於傳統的 GAA 及/或 GBA 機構不工作。即是不能用於鑑定，在沒有從使用者設備到網路的返回通道。此一情況的範例是廣播網路，例如使用者設備是用於數位視訊廣播的一機上盒(STB；或數位盒)。在此一情況中，當 UE 不能使用 BSF 引導或不能以一雙向方法與 NAF 通訊時，根據先前技術的 GAA 及/或 GBA 是不能使用。

在對 DVB-H (手持式數位視訊廣播)協會與 ETSI(歐洲電信標準學會)的提供中，Vodafone 提出有關用來取得服務保護鑰的機構之一以 USIM 介面為主之元件介面。然而，此協議不適合克服前述問題與相關缺點。

因此，前述問題與缺點的解決對於在未來使用更形重要的情況中提供安全是需要的。

【發明內容】

本發明的一目的是要免除先前技術固有的前述缺點，因此提供改善的方法、網路實體、一系統、與一電腦程式產品。

根據本發明的一第一部份，此目的是例如通過用以在客戶端實體與一網路之間實施鑑定的一方法達成，其中該網路

包含至少一引導伺服器功能實體與一網路應用功能實體，其中該客戶端實體不能以雙向方法與兩網路實體通訊，該方法包含下列步驟：當網路應用功能實體需要將資料安全傳送給客戶端實體時，將用於鑑定資訊的一請求從網路應用功能實體傳送給該引導伺服器功能實體；在該引導伺服器功能實體上處理該請求與取回的鑑定資訊；將包括鑑定資訊的一回應從該引導伺服器功能實體傳送給該網路應用功能實體；將該鑑定資訊與資料從該網路應用功能實體傳送給該客戶端實體；及在客戶端實體上使用鑑定資訊來鑑定網路。

根據進一步有利發展，下列至少之一可應用：

- 傳輸請求的步驟是由不同於客戶端實體的一裝置所觸發；
- 該請求包含客戶端實體、與該網路應用功能實體的一識別符之至少一個人識別；
- 該取回鑑定資訊的步驟包含從一本籍用戶系統拾取該鑑定資訊的步驟；
- 該鑑定資訊包含至少一任意挑戰參數與一網路鑑定參數；
- 該回應進一步包含該網路應用功能實體的一密鑰；
- 該傳輸鑑定資訊的步驟進一步包含傳送該網路應用功能實體識別的一步驟；
- 該鑑網路的步驟進一步包含在該客戶端實體上產生該網路應用功能實體的一密鑰的步驟；
- 該執行的鑑定是根據一般鑑權架構的一般鑑定；

- 該取回鑑定資訊的步驟進一步包含建立引導會談資料的步驟；
- 該鑑定資訊包含至少一任意挑戰參數、一網路鑑定參數、與引導會談資料；
- 該回應進一步包含該網路應用功能實體的一密鑰；
- 該傳輸鑑定資訊的步驟進一步包含傳輸該網路應用功能實體識別的一步驟；
- 該鑑定網路的步驟進一步包含在該客戶端實體上產生該網路應用功能實體的一密鑰的步驟；
- 該鑑定網路的步驟進一步包含在該客戶端實體與該引導伺服器功能實體之間建立一引導會談的步驟；
- 該建立一引導會談的步驟是根據從該網路應用功能實體傳送的該鑑定資訊；
- 該鑑定網路的步驟進一步包含在該客戶端實體上儲存該引導會談資料的一步驟；
- 在該客戶端實體與該引導伺服器功能實體之間存在一有效的引導會談；
- 一有效引導會談是永久存在；
- 該處理請求的步驟進一步包含觸發該客戶端實體以建立一有效引導會談的一步驟；
- 該鑑定資訊包含至少引導會談資料；
- 該回應進一步包含該網路應用功能實體的一密鑰；
- 該鑑定網路的步驟進一步包含在該客戶端實體上產生該網路應用功能實體的一密鑰的步驟；

- 該方法進一步包含一步驟，其中該客戶端實體開始接觸該網路應用功能實體，並傳送它的個人識別；
- 該網路應用功能實體可觸發該客戶端實體以建立一有效的引導會談；
- 該網路應用功能實體可觸發該引導伺服器功能實體，如此使用該客戶端實體觸發未被請求的引導程序；
- 該方法進一步包含使用它的密鑰將在該網路應用功能實體上傳送的資料予以加密的一步驟；及
- 該方法進一步包含使用該網路應用功能實體的密鑰將在該客戶端實體上的加密資料予以解碼的步驟。

根據本發明的一第二部份，此目的可例如通過下列達成：一方法，用以執行在一客戶端實體與包含至少一引導伺服器功能實體與一網路應用功能實體的一網路之間的鑑定，其中該客戶端實體不能以一雙向方法而與兩網路實體通訊，該方法包含下列步驟：當該網路應用功能實體需要將資料安全傳送給客戶端實體時，將鑑定資訊的一請求從該網路應用功能實體傳送給該引導伺服器功能實體；在該引導伺服器功能實體上處理請求及取回該鑑定資訊，包括從一本籍用戶系統拾取該鑑定資訊的一步驟；將包括該鑑定資訊的一回應從該引導伺服器功能實體傳送給該網路應用功能實體，其包含至少一任意挑戰參數、一網路鑑定參數、與網路應用功能實體的一密鑰；傳送該鑑定資訊，該網路應用功能實體的一識別，與從該網路應用功能實體傳送給該客戶端實體的資料；及使用該鑑定資訊來鑑定網路，並在該客戶端實體上產

生該網路應用功能實體的一密鑰。

根據本發明的一第三部份，此目的可例如通過一方法達成，其中該方法用於執行在一客戶端實體與包含至少一引導伺服器功能實體與一網路應用功能實體的一網路之間的鑑定，其中該客戶端實體不能以一雙向方法而與兩網路實體都通訊，該鑑定是根據一般鑑權架構的一般鑑定，該方法包含下列步驟：當該網路應用功能實體需要將資料安全傳送給客戶端實體時，將鑑定資訊的一請求從該網路應用功能實體傳送給該引導伺服器功能實體；在該引導伺服器功能實體上處理請求及取回該鑑定資訊，其包括建立引導會談資料的一步驟；將包括該鑑定資訊的一回應從該引導伺服器功能實體傳送給網路應用功能實體，其包含至少一任意挑戰參數、一網路鑑定參數、引導會談資料、與該網路應用功能實體的一密鑰；傳送該鑑定資訊、該網路應用功能實體的一識別、與從該網路應用功能實體傳送給該客戶端實體的資料；及使用該鑑定資訊來鑑定網路，並在該客戶端實體與該引導伺服器功能實體之間建立一引導會談。

根據本發明的一第四部份，此目的可例如通過一方法達成，其中該方法用以在一客戶端實體與包含至少一引導伺服器功能實體與一網路應用功能實體的一網路之間執行鑑定，其中該客戶端實體不能以一雙向方法而與兩網路實體通訊，其中在該客戶端實體與該引導伺服器功能實體之間存在一有效的引導會談，該方法包含下列步驟：當該網路應用功能實體需要將資料安全傳送給客戶端實體時，將鑑定資訊的

一請求從該網路應用功能實體傳送給該引導伺服器功能實體；在該引導伺服器功能實體上處理請求及取回該鑑定資訊；將包括該鑑定資訊的一回應從該引導伺服器功能實體傳送給該網路應用功能實體，且其包含至少引導會談資料與該網路應用功能實體的一密鑰；傳送該鑑定資訊與從該網路應用功能實體傳送給該客戶端實體的資料；及使用該鑑定資訊來鑑定網路，並在該客戶端實體上產生該網路應用功能實體的一密鑰。

根據本發明的一第五部份，此目的可例如通過下列達成：使用在一鑑權架構的一客戶端實體，用以在該客戶端實體與一網路之間執行鑑定；該包含接收裝置的客戶端實體，用以從網路接收傳輸；與鑑定裝置，以使用接收的鑑定資訊來鑑定網路。

根據本發明的一第六部份，此目的可例如通過使用在一鑑權架構的一客戶端實體達成，以在該客戶端實體與一網路之間執行鑑定，該網路包含至少一引導伺服器功能實體與一網路應用功能實體，而且在此架構中，該客戶端實體不能以一雙向方法而與兩網路實體通訊，該客戶端實體包含：接收裝置，用以從該網路應用功能實體接收傳輸；及鑑定裝置，以使用該接收的鑑定資訊來鑑定網路。

根據進一步有利發展，下列之至少一者可應用：

- 該客戶端實體進一步包含密鑰產生裝置，用以產生該網路應用功能實體的一密鑰；

- 該客戶端實體進一步包含建立裝置，用以在該客戶端

實體與該引導伺服器功能實體之間建立一引導會談；

- 該客戶端實體進一步包含儲存裝置，用以儲存引導會談資料；

- 該客戶端實體進一步包含解碼裝置，以供使用該網路應用功能實體的一密鑰將從該網路應用功能實體接收的加密資料予以解密；

- 該客戶端實體進一步包含處理及控制裝置，用以處理資料及信令，及用以控制該客戶端實體及其構成裝置；及

- 該客戶端實體包含至少一使用者設備，並可連接到一全球用戶識別模組。

根據第五或第六部份的進一步有利發展，下列之至少一者可應用：

- 該客戶端實體是一機上盒；

- 該鑑定裝置配置成存取在該客戶端實體上可獲得的使用者識別資訊；及/或

- 該使用者識別資訊是儲存在連接到該客戶端實體的一智慧卡。

根據本發明的一第七部份，此目的可例如通過使用在一鑑權架構的一網路實體達成，用以在一客戶端實體與一網路之間執行鑑定，其中該網路包含至少網路實體，且其是一網路應用功能實體與一引導伺服器功能實體，而且在此架構中，該客戶端實體不能以雙向方法而與兩網路實體通訊，該網路實體包含收發器裝置，用以將傳輸傳送給該客戶端實體，及用以從該引導伺服器功能實體傳送及接收，其中該收

發器裝置配置成當該網路應用功能實體需要將資料安全傳送給客戶端實體時，將鑑定資訊的一請求傳送給該引導伺服器功能實體；用以從該引導伺服器功能實體接收包括該鑑定資訊的一回應；及用以傳送該鑑定資訊及傳送給該客戶端實體的資料。

根據進一步有利發展，下列之至少一者可應用：

- 該收發器進一步配置成將該網路應用功能實體的一識別傳送給該客戶端實體；

- 該網路實體進一步包含加密裝置，以使用該網路應用功能實體的密鑰將傳送給該客戶端實體的資料予以加密；及

- 該網路實體配置成廣播傳輸。

根據本發明的一第八部份，此目的可例如通過使用在一鑑權架構中的一網路實體達成，用以在一客戶端實體與網路之間執行鑑定，其中該網路包含至少網路實體，且其是一引導伺服器功能實體與一網路應用功能實體，而且在此架構中，該客戶端實體不能以雙向方法而與兩網路實體都通訊，該網路實體包含收發器裝置，用以從該網路應用功能實體接收及傳送；及處理和取回裝置，用以處理從該網路應用功能實體接收一請求，及用以取回該鑑定資訊，其中該收發器裝置配置成用以從該網路應用功能實體接收請求，及用以將該鑑定資訊傳送給該網路應用功能實體。

根據進一步有利發展，下列之至少一者可應用：

- 該網路實體進一步包含拾取裝置，用以從一本籍用戶系統拾取該鑑定資訊；

- 該網路實體進一步包含建立裝置，用以建立引導會談資料；

- 該網路實體進一步包含觸發裝置，用以觸發該客戶端實體以建立一有效的引導會談；及/或

- 該網路是一廣播網路。

根據本發明的一第九部份，此目的可例如通過一鑑權架構系統達成，用以在一客戶端實體與一網路之間執行鑑定，其中該網路包含至少一引導伺服器功能實體與一網路應用功能實體，而且在此架構中，該客戶端實體不能以一雙向方法而與兩網路實體通訊，該系統包含根據第五或第六部份的至少一客戶端實體、根據第七部份的至少一網路應用功能實體、與根據第八部份的至少一引導伺服器功能實體。

根據一進一步有利發展，該鑑權架構系統的客戶端實體是一機上盒。

根據本發明的第十部份，此目的可例如通過一電腦程式產品達成，該電腦程式產品可載入一數位處理裝置的一記憶體，且包含軟體碼部分，用以當該產品在該數位處理裝置上執行時，可根據第一對第四部份之任一者執行該方法的步驟。

根據本發明的另一有利技術解決，根據前述部份之任一者的網路是一廣播網路。

本發明的一優點是一解決的提供是 3GPP GAA 觀念如何使用在客戶端未將一通道送回網路的情況。

隨著本發明的實施例，在客戶端與引導伺服器功能之間

的引導階段基本上可被移除。此外，有利是此引導階段是部分與在網路應用功能與客戶端間的前置協定(或單一訊息)組合。

本發明的另一優點是鑑定與密鑰協議的引導是允許用於缺乏一回傳通道的情況，即是缺乏與網路的雙向連接。

經由本發明，GAA/GBA 觀念如此可在它應用的區域中變寬。

【實施方式】

本發明是在此經由參考特殊非限制範例情況的實施例描述。熟諳此技者可了解到本發明並未侷限於這些範例，而且可更廣泛應用。

本發明及其實施例是針 GAA 及/或 GBA 環境的情況，其中一客戶端或使用者設備沒有網路的一回傳通道。隨著網路包含至少一網路應用功能實體與一引導伺服器功能實體，此表示一使用者設備(客戶端實體)不能以一雙向方法而與兩網路實體通訊。換句話說陳述，此表示使用者設備(客戶端實體)缺乏與網路應用功能實體或引導伺服器功能實體、或這兩實體的一雙向連接，即是一回傳通道。

圖 5 是根據本發明的一第一實施例描述的一方法的信令圖。圖 5 描述客戶端實體或使用者設備 UE 12 沒有網路回傳通道的情況，即是客戶端實體不能以一雙向方法而與網路應用通訊功能(NAF)實體 13b 與引導伺服器功能(BSF)實體 13a 通訊。因此，客戶端實體不能與 BSF 實體執行一引導程序。此一情況的範例可為具有全球積體電路卡(UICC)卡讀

卡機的一機上盒(STB；或數位盒)。

一方法用以在客戶端實體與網路之間執行鑑定，如此使用 GAA 功能是在下面描述。

在步驟 S51 中，NAF 實體 13b 需要將一些資料(例如，廣播密鑰)傳遞給客戶端 UE 12。NAF 實體 13b 知道用戶的個人識別，即是用戶的 IMPI(IP 多媒體核心網路子系統個人識別)、與需要遞傳送給 UE 12 的資料。在步驟 S52 中，NAF 實體 13b 是在 Zn 參考點上將包括用戶 IMTI 的一請求、它自己的識別 NAF_ID(即是，NAF 主機名稱)、或者一個或多個 GSIDs(用於請求 NAF 特殊使用者安全設定的 GAA 服務識別符)傳送給引導伺服器功能(BSF)實體 13a。

注意，(步驟 2)的請求傳輸可通過不同於客戶端實體的一裝置而觸發。例如，在 DVB-H 情況中，鑑定(引導)程序或此需要是在網路(例如在 NAF 實體本身)中通過更新終端機實體的廣播密鑰的需要而觸發。

只要從 NAF 實體 13b 接收請求，BSF 實體 13a 會在步驟 S53 檢查 NAF 實體 13b 是否授權請求鑑定資訊，例如一網路鑑定元件(AUTN)與一任意挑戰(RAND)。如果是如此，BSF 實體 13a 可從一本籍用戶系統 HSS 14 拾取鑑定向量，根據 NAF 實體的識別 NAF_ID 和其他密鑰衍生參數而計算 NAF 實體密鑰。它亦可從用戶的 GBA 使用者安全設定(GUSS)擷取該請求的使用者安全設定 USSs(如有任何存在)。

在第四步驟 S54 中，BSF 實體 13a 然後將參數 AUTN、

RAND、Ks_NAF、Ks_NAF 的壽命、與請求的 USSs(如有任何存在)傳送給 NAF 實體 13b。NAF 13b 使用密鑰 Ks_NAF 將傳送給客戶端實體 12 的資料予以加密(或予以保護)(步驟 S55)。或者，在 UICC 致能 GBA(即是 GBA_U)的情況中，密鑰 Ks_int_NAF 和 Ks_ext_NAF 的任一者可於於此目的。然而，加密的功能(以及下列解密)是選擇性。

在步驟 S56 中，NAF 實體 13b 使用在本身與 UE 12 之間的廣播通道將參數 AUTN、RAND、NAF_UD、與加密的資料傳送給 UE 12。AUTN、RAND、NAF_ID、與加密的資料本身可進一步使用其他已知裝置保護(例如，使用 UE 的裝置認證公眾金鑰)。當 UE 12 從 NAF 13b 接收資料時，它會先使用參數 AUTN 與 RAND 來鑑定網路。如果此成功，它將會從會談密鑰 CK 和 IK 取得引導密鑰(Ks)，並使用 Ks、NAF_ID、與其他密鑰衍生參數來持續取得 NAF 特殊密鑰 Ks_NAF。它能然後使用密鑰 Ks_NAF 將資料解碼，並將資料(例如，廣播密鑰)使用在 UE 12。

結果，Ub 參考點未全然使用在展現的方法。

圖 6 根據本發明的一第二實施例描述一方法的信令圖。再次描述客戶端實體 UE 12 沒有網路回傳通道的情況，如此不能與 BSF 13a 實體直接執行一引導程序。最好是，該引導是在 NAF 實體的輔助下發生。因此，此一程序可視為相反引導。

根據目前實施例的一相反引導程序是經由一網路應用功能實體 BSF 13b 而在客戶端實體 UE 12 與引導伺服器功

能實體 NAF 13a 之間發生。該程序是在下面描述。

在步驟 S61 中，NAF 實體 13b 需要將一些資料(例如，廣播密鑰)傳遞給客戶端 UE 12。NAF 實體 13b 知道用戶的識別，亦即用戶的 IMPI (參考上面)、與需要傳遞給 UE 12 的資料。根據傳統程序，在 NAF 實體 13b 可從 BSF 實體 13a 請求對應的 GBA 密鑰前，UE 12 始終具有連接到 NAF 實體 13b，並傳遞一引導交易識別符 B-TID。

在根據目前實施例的方法中，NAF 實體 13b 可被一些其他裝置觸發以拾取 GBA 資料。

在步驟 S62 中的 NAF 實體 13b 可在 Zn 參考點上將用戶的 IMPI、它自己的 NAF_ID(即是，NAF 主機名稱)、或者一個或多個 GSIDs (用於請求 NAF 特殊使用者安全設定的 GAA 服務識別符)傳送給 BSF 實體 13a。根據傳統程序，識別符 B-TID 是用來從 BSF 13a 拾取 GBA 密鑰。對照下，在此的 NAF 實體 13b 使用用戶的 IMPI 從 BSF 13a 拾取 GBA 資料。

只要從 NAF 實體 13b 接收請求，在步驟 S63 的 BSF 13a 會檢查 NAF 實體 13b 是否授權請求類似 AUTN 和 RAND 的授權資訊，而且是根據目前實施例的一部份相反引導程序。如果是如此，BSF 實體 13a 便從一本籍用戶系統 HSS 14 拾取鑑定向量，根據識別 NAF_ID 及其他密鑰衍生參數來計算密鑰 $Ks_{NA.F}$ 。它亦從用戶 GUSS 擷取請求的使用者安全設定 USSs(如有任何存在)。然後，仍然在步驟 S63，BSF 實體 13a 可建立可供用戶稍後與其他 NAFs 13b 使用的引導會談

資料。

根據先前技術的程序，BSF 實體 13a 應該包含既有的引導會談資料(通過引導交易識別符 B-TID 識別)，及如前述計算密鑰 K_s_NAF 。對照下，根據此實施例的 BSF 實體 13a 可建立未與客戶端實體 UE 12 通訊的引導會談資料，並可用於 K_s_NAF 的計算與 USSa 的選擇。在步驟 S64 中，BSF 實體 13a 可將參數 AUTN、RAND、B-TID、 K_s_NAF 、 K_s_NAF 的壽命、與請求的 USSs(如有任何存在)傳送給 NAF。而且，AUTN、RAND、和 B-TID 是傳回給 NAF。NAF 然後(在步驟 5)選擇性使用密鑰 K_s_NAF 將傳送的資料予以加密(或保護)。根據目前的規格，此是 NAF 特殊功能。(注意，GBA 規格對於在 NAF 13b 的發生是沒有限制，及 NAF13b 如何使用 GBA 密鑰)。如前述，將傳送的資料加密(與解碼)功能在執行鑑定的結構是純選擇性。

在步驟 S66 中，NAF 實體使用在它本身與 UE 12 之間的(單向)廣播通道將參數 AUTN、RAND、B-TID、NAF_ID、與加密的資料傳送給 UE 12。AUTN、RAND、NAF_ID、與加密的資料本身可進一步使用其他裝置(例如，通過 OMA DRM 2.0 及通過使用 UE 12 的裝置認證公眾金鑰)保護。

根據目前的先前標準，識別符 B-TID 是從 UE 12 傳送給 NAF 13b。此在一正常 GBA 程序中是在步驟 S61 之前發生。根據目前實施例，識別符 B-TID 以及參數 AUTN 和 RAND 是從 NAF 實體 13b 傳送給客戶端 UE 12。

當 UE 從 NAF 13b 接收資料(步驟 S67)時，它先使用參

數 AUTN 與 RAND 來鑑定網路。如果此成功，它可從會談密鑰 CK 和 IK 取得引導密鑰(Ks)，並使用 Ks、NAF_ID、和其他密鑰衍生參數持續取得 NAF 特殊密鑰 Ks_NAF。然後使用密鑰 Ks_NAF 將資料予以解密，並將資料(例如，廣播密鑰)使用在 UE 12。UE 12 亦配置成可儲存引導會談資料，以稍後與另一 NAF13 b 使用。UE 12 然後經由接收的參數 B-TID、AUTN、和 RAND 以建立一引導會談。而且，在目前實施例中，密鑰衍生是在此程序階段(當引導會談變成有效)處理。只要會談有效或一引導會談建立，UE 12 亦能使用與另一 NAFs 13b 的一新建立的引導會談。

而且在此，Ub 參考點未使用在展現的方法。

圖 7 是根據本發明的一第三實施例描述一進一步方法的信令圖。其描述客戶端 UE 12 沒有 NAF 實體 13b 的回傳通道，但是確實具有到例如 BSF 13a 的其他網路元件的一雙向連接的情況。即是，類似前述的情況，客戶端實體 UE 12 不能以一雙向方法而與相關的網路元件 NAF 13b 和 BSF 13a 通訊。然而，在目前情況中，客戶端可與 BSF 實體 13a 執行一引導程序。此一情況的範例可為具有例如 IP 連接的 3G 功能之一行動終端機，但是它亦具有一設施以接收例如手持式終端機的數位視訊廣播，即是 DVB-H 致能。

此情況假設 UE 12 始終具有與 BSF 13a 的一有效引導會談(此在 UE 12 可為一組態選項)，或 BSF 13a 可觸發 UE 12 以執行引導會談建立(例如，通過使用會談開始協定(SIP))。目前方法是利用下述的 GAA 功能。

在步驟 S71 中，NAF 實體 13b 需要教一些資料(例如，廣播密鑰)傳遞給客戶端實體 UE 12。它知道用戶的識別(即是他的 IMPI)、與需要傳遞給 UE 12 的資料。NAF 實體 13b 然後在 Zn 參考點上傳送用戶的 IMPI、它的 NAF_ID(即是，NAF 主機名稱)、與選擇性一個或多個 GSIDs(用於請求 NAF 特殊使用者安全設定的 GAA 服務識別符)(步驟 S72)。直到此刻，該方法是相當類似前述第二實施例之一。

只要從 NAF 實體 13b 接收請求，BSF 實體 131 會在步驟 S73 檢查用戶是否具有一有效的引導會談，並可在它的資料庫中找到。如果它未提供，BSF 實體 13 會表示 NAF 實體 13b 的錯誤，或觸發客戶端實體 UE 12 以執行一引導建立程序。NAF 實體 13a 然後根據識別 NAF_ID 及其他密鑰衍生參數來計算密鑰 Ks_NAF。它亦從用戶的 GUSS 擷取請求的使用者安全設定 USSs(如有任何存在)。BSF 實體 13a 將參數 B-TID、Ks_NAF、Ks_NAF 的壽命、請求的 USSs(如有任何存在)傳送給 NAF 實體 13b。因此，當 BSF 實體 13b 從 BSF 實體 13a 接收此時，NAF 實體 13b 會學習有效的引導交易識別符 B-TID。在第五步驟中，NAF 實體 13b 可選擇性使用它的密鑰 Ks_NAF 將傳送的資料予以加密(或保護)。NAF 實體 13b 使用在它本身與 UE 12 之間的廣播通道將參數 B-TID、NAF_ID、與加密的資料傳送給客戶端實體 UE。參數 B-TID、NAF_ID、與加密資料本身可進一步使用其他裝置(例如，通過 OMA DRM 2.0 與通過使用 UE 12 的裝置認證公眾金鑰)保護。

當驗步驟 S77 的 UE 12 從 NAF 實體 13b 接收資料時，它可使用 B-TID 和 NAF_ID 以取得使用 Ks(通過 B-TID 識別)、NAF_ID、與其他密鑰衍生參數的 NAF 特殊密鑰 Ks_NAF。如果加密，它然後可使用 Ks_NAF 將資料予以解碼，並將資料(例如，廣播密鑰)使用在 UE 12。有關在 UE 12 的 GBA 密鑰使用(如在 NAF 13b，參考步驟 S75)的功能是特殊的 NAF。密鑰衍生是在此程序階段處理。

當根據本發明實施例之任一者實施方法時，根據先前技術在一 GBA 結構中的延伸/修改如下所示：

- NAF 13b 可通過使用用戶個人識別(例如 IMPI 或 IMSI)而不是 B-TID 來請求從 CK 和 IK(即是例如 Ks_NAF)取得的 AUTN 和 RAND(而不是 RES、CK、IK)和 GBA 密鑰；

- BSF 13a 可根據 AUTN 和 RAND 的 NAF 請求而建立一用戶的引導會談資料；

- 除了從 BSF 13a 傳回的正常資料之外，AUTN 和 RAND 亦會傳回(而不是 RES、CK、IK)；

- UE 12 可根據從 NAF 13b 接收的 AUTN、RAND、B-TID、與密鑰壽命來建立一引導會談資料；及

- NAF 13b 可通過使用用戶的 IMPI 而請求引導會談資料(B-TID、特殊 NAF 等)。

如本發明的一進一步實施例，可想像該客戶端實體 12 不能夠到達 BSF 13a 的情況，但是具有與 NAF 13b 的一雙向通道。例如，此是當 UE 12 使用用於存取鑑定的 GBA 的情況。因為 NAF 13b 不知道 UE 12 用戶的 IMPI，所以不

能使用基本的反向 GBA 協定。此一情況亦可能例如在一無線區域網路(WLAN)情況中出現，其中客戶端實體 12 需要鑑定，但是只具有與在此一情況可如同 NAF 實體 13b 操作的一 EAP(可擴充式驗證協定)伺服器之一連接。

因此，客戶端實體 UE 12 可經由 NAF 實體 13b(與 BSF 實體 13a)執行一引導程序。除了在第一步驟之前的 UE 12 接觸 NAF 實體 13b 並傳它的個人識別 IMPI 之外，信令是類似前述程序。

一仍然進一步實施例存在於 NAF 實體 13b 只具有與 UE 12 的一單向通道，但是 BSF 13a 具與 UE 12 的一雙向通道情況。

在此實施例中，可能

(1) NAF 實體 13b 觸發 UE 12 建立一有效的引導會談；
或

(2) NAF 實體 13b 觸發 BSF 實體 13a，如此可與客戶端實體 UE 12 觸發一未被請求的引導程序。

根據本發明的進一步實施例，提供一客戶端實體、一網路應用功能實體、一引導伺服器功能實體、與用以在該客戶端實體與網路之間執行鑑定之一方法、與根據本發明任一方法的網路。

圖 8 是根據本發明的一實施例描述一客戶端實體方塊圖。

根據一實施例的客戶端實體 12 包含：接收裝置 87，用以從該網路應用功能 NAF 實體 13b 接收傳輸；及鑑定裝置

81，其可通過使用該接收的鑑定資訊來鑑定網路。

根據進一步實施例，該客戶端實體 UE 12 選擇性進一步包含下列之一個或多個(可從圖 8 獲知)：

- 密鑰產生裝置 82，用以產生該網路應用功能實體的一密鑰(例如 K_s_NAF)；
- 建立裝置 84，用以在該客戶端實體 12 與該引導伺服器功能實體 13a 之間建立一引導會談；
- 儲存裝置 85，用以儲存該引導會談資料；及/或
- 解密裝置 83，其可通過使用該網路應用功能實體 13b 的一密鑰而將從該網路應用功能實體 13b 接收的加密資料予以解密，而且其中該網路應用功能實體 13b 的一密鑰是從密鑰產生裝置供應。

根據圖 8 顯示實施例的客戶端實體 12 進一步包含處理和控制裝置 86，其配置成可處理資料和信令，且整體上可控制客戶端實體 12 及它元件，例如建立裝置 84。對於此目的而言，處理和控制裝置 86 具有與顯示構成裝置任一者的雙向資料及/或控制連接。

根據目前實施例的客戶端實體進一步包含至少一使用者設備、及/或根據例如 3GPP 標準而可連接到一全球用戶識別模組。

此外，根據仍然本發明另一實施例的客戶端實體是一機上盒(或數位盒)。如果是如此，此一機上盒的客戶端實體可配置成根據任何適當的已知技術來操作，例如根據 DVB-H 標準。

在前述實施例中，客戶端實體的鑑定裝置 81 是被配置成存取在客戶端實體上可獲得的使用者識別資訊。除了接收的鑑定資訊之外，此使用者識別資訊可例如用於鑑定目的。這些使用者識別資訊是例如儲存在可連接到客戶端實體的一智慧卡，例如一 UICC，一全球用戶識別模組(USIM)、或可根據 DVB-H 標準使用的一智慧卡。

圖 9 是根據本發明的一實施例描述一網路應用功能實體的方塊圖。

根據一實施例，特別是一網路應用功能實體 13b 的一網路實體包含收發器裝置 91，其配置成可將傳輸傳送給客戶端實體 12，並從該引導伺服器功能實體 13a 傳送及接收。該收發器裝置 91 是例如配置成當該網路應用功能實體 13b 需要將資料安全傳送給客戶端實體 12 時，將用於鑑定資訊的一請求傳送給該引導伺服器功能實體 13a，以從該引導伺服器功能實體 13a 接收包括該鑑定資訊的一回應，並傳送該鑑定資訊與傳送給該客戶端實體 12 的資料。

根據進一步實施例，該網路應用功能 NAF 實體 13b 選擇性進一步包含加密裝置 92，其可通過使用該網路應用功能實體 13b 本身的密鑰而將傳送給該客戶端實體 12 的資料予以加密。根據圖 9，傳送的資料可通過標示 DATA 93 的一資料庫符號表示。

此外，該收發器裝置 91 可配置用於教該網路應用功能實體 13b 的一識別傳送給該客戶端實體 12。此一識別亦可儲存在相同資料庫資料 93，當作要傳送的日期。

根據本發明的一進一步實施例的網路實體可配置成將傳輸例如廣播給客戶端實體 UE。

圖 10 是根據本發明的一實施例描述一引導伺服器功能實體的方塊圖。

根據一實施例，網路實體(特別是一引導伺服器功能 BSF 實體 13a)包含：收發器裝置 101，用以從該網路應用功能實體 13b 傳送及接收；及處理和取回裝置 102，用以處理從該網路應用功能實體 13b 接收的一請求，及用以取回鑑定資訊。在目前實施例中，收發器裝置 101 是特別配置成用以從該網路應用功能實體 13b 接收請求，及用以將該鑑定資訊傳送給該網路應用功能 13b 實體。

根據進一步實施例，該引導伺服器功能實體 BSF 13a 選擇性進一步包含下列之一個或多個(可從圖 10 獲得)：

- 拾取裝置 105，用以從一本籍用戶系統 HSS 14 拾取鑑定資訊；
- 建立裝置 104，用以建立引導會談資料；及/或
- 觸發裝置 103，用以觸發該客戶端實體 12 以建立一有效的引導會談。

根據圖 8 至 10，根據本發明的一系統包含至少一客戶端實體 12(或者為一機上盒)、至少一網路應用功能實體 13b、與至少一引導伺服器功能實體 13。

注意，在圖 8 至 10 中，只有這些裝置和功能元件的描述是與本發明有關。為了簡化，省略在他們傳統結構中形成任何部分描述裝置的熟諳此技者所已知的其他裝置與功能

元件。

大體上，注意，只要配置成執行相對部分的描述功能，前述功能元件(亦即根據本發明的 UE、BSF、和 NAF、及其元件)可通過任何已知的方法、或分別以硬體及/或軟體實施。例如，客戶端實體的鑑定裝置可通過任何資料處理單元實施，例如微處理器，其配置可根據本發明的方法使用接收的鑑定資訊來鑑定網路。前述部分亦能以個別的功能方塊或個別裝置實施，或者一個或多個前述部分可以單一的功能方塊或單一裝置實施。因此，圖 8 至 10 的前述例證只是說明而不是限制本發明的實施。

簡言知，揭示的方法、一客戶端實體、網路實體、一系統、與一電腦程式產品是用以在一客戶端實體與一網路之間執行鑑定，該網路包含至少一引導伺服器功能實體與一網路應用功能實體，而且其中該客戶端實體不能以一雙向方法而與兩網路實體都通訊，其中在該客戶端實體與該引導伺服器功能實體之間的標準 Ub 參考點不是用於鑑定目的。簡言之，本發明揭示通過使用供單向網路連接的 GAA 功能的鑑定。

根據本發明的一有利部份，該網路是一廣播網路。

即使本發明的描述是根據附圖的範例，可清楚知道本發明並未侷限於此。最好是，對於熟諳此技者顯然的是本發明能以許多方法修改，而不致脫離如文後申請專利範圍所揭示的創作觀念的範圍。

【圖式簡單說明】

- 圖 1 係一般鑑權架構環境的概述；
 圖 2 顯示一般引導的網路模型；
 圖 3 顯示先前技術描述一般引導程序；
 圖 4 顯示先前技術描述一般引導使用程序；
 圖 5 係本發明之第一實施例中方法的信令圖；
 圖 6 係本發明之第二實施例中方法的信令圖；
 圖 7 係本發明之第三實施例中方法的信令圖；
 圖 8 係本發明之實施例中客戶端實體的方塊圖；
 圖 9 係本發明之實施例中網路應用功能實體的方塊圖；及
 圖 10 係本發明之具體實例中引導伺服器功能實體的方塊圖。

【主要元件符號說明】

- | | |
|----------------|-----------------|
| 11a 用戶憑證 | 11b 引導架構(GBA) |
| 11c 驗證代理(AP) | 12 使用者設備 UE |
| 13 網路實體 NE | 13a 引導伺服器功能 BSF |
| 13b 網路應用功能 NAF | |
| 14 本籍用戶系統 HSS | |
| 81 鑑定裝置 | 83 解密裝置 |
| 84 建立裝置 | 85 儲存裝置 |
| 86 控制裝置 | 91 收發器裝置 |
| 93 資料庫資料 | 103 觸發裝置 |
| 104 建立裝置 | 105 拾取裝置 |

101年12月7日修正本

十、申請專利範圍：

1. 一種用以在一客戶端實體(UE)與包含一引導伺服器功能實體(BSF)和一網路應用功能實體(NAF)的一網路之間實施鑑定之方法，其中該客戶端實體(UE)具有缺乏自該客戶端實體至該引導伺服器功能實體(BSF)及/或該網路應用功能實體(NAF)之一返回頻道的一單向網路連接，該鑑定之方法包含下列步驟：

當該網路應用功能實體需要將資料安全傳送給該客戶端實體時，將用於鑑定資訊的一請求從該網路應用功能實體傳送(S62)給該引導伺服器功能實體，該請求包含該客戶端實體之一個人識別；

在該引導伺服器功能實體上處理(S63)請求及取回該鑑定資訊，其中該取回包含建立引導會談資料；

將包括包含用於該客戶端實體之該引導會談資料之該鑑定資訊的一回應從該引導伺服器功能實體傳送(S64)給該網路應用功能實體；

將該包含用於該客戶端實體之該引導會談資料之鑑定資訊和資料從該網路應用功能實體傳送傳送(S66)給該客戶端實體；及

在客戶端實體上使用該包含用於該客戶端實體之該引導會談資料之鑑定資訊以鑑定(S67)該網路，其中該鑑定包含依據一通用鑑定架構來實施包括一通用鑑定之一鑑定。

2. 如申請專利範圍第 1 項之方法，其中該傳輸請求步

驟是通過不同於該客戶端實體的一裝置觸發。

3. 如申請專利範圍第 1 項之方法，其中該請求進一步包含該網路應用功能實體的識別。

4. 如申請專利範圍第 1 項之方法，其中該處理請求及取回鑑定資訊的步驟包含從一本籍用戶系統(HSS)拾取該鑑定資訊。

5. 如申請專利範圍第 1 項之方法，其中該鑑定資訊進一步包含至少一任意挑戰參數或一網路鑑定參數。

6. 如申請專利範圍第 5 項之方法，其中該回應進一步包含該網路應用功能實體的一密鑰。

7. 如申請專利範圍第 1 項之方法，其中該傳輸鑑定資訊的步驟進一步包含傳送該網路應用功能實體識別的步驟。

8. 如申請專利範圍第 1 項之方法，其中該鑑定網路的步驟進一步包含在客戶端實體上產生該網路應用功能實體的一密鑰之步驟。

9. 如申請專利範圍第 1 項之方法，其中該鑑定網路的

步驟進一步包含在該客戶端實體與該引導伺服器功能實體間建立一引導會談之步驟。

10. 如申請專利範圍第 9 項之方法，其中該建立一引導會談的步驟是根據傳送來自該網路應用功能實體的該鑑定資訊。

11. 如申請專利範圍第 1 項之方法，其中該鑑定網路的步驟進一步包含在該客戶端實體上儲存該引導會談資料的步驟。

12. 如申請專利範圍第 1 項之方法，進一步包含判斷一有效的引導會談資料是否存在該客戶端實體與該引導伺服器功能實體之間。

13. 如申請專利範圍第 12 項之方法，其中該有效的引導會談是永續性。

14. 如申請專利範圍第 12 項之方法，其中該處理請求的步驟進一步包含觸發該客戶端實體以建立有效引導會談之步驟。

15. 如申請專利範圍第 12 項之方法，其中該回應進一

步包含該網路應用功能實體的一密鑰。

16. 如申請專利範圍第 12 項之方法，其中該鑑定網路的步驟進一步包含在該客戶端實體上產生該網路應用功能實體的一密鑰之步驟。

17. 如申請專利範圍第 1 項之方法，進一步包含開始接觸該網路應用功能實體，並傳送該客戶端實體的一個人識別。

18. 如申請專利範圍第 1 項之方法，進一步包含通過該網路應用功能實體觸發該客戶端實體，以建立一有效的引導會談。

19. 如申請專利範圍第 1 項之方法，進一步包含通過該網路應用功能實體觸發該引導伺服器功能實體，以觸發與該客戶端實體的一未被請求引導程序。

20. 如申請專利範圍第 1 項之方法，進一步包含使用該網路應用功能的一密鑰將在該網路應用功能實體上傳送的資料予以加密之步驟。

21. 如申請專利範圍第 20 項之方法，進一步包含使用該網路應用功能實體的密鑰將在該客戶端實體上的資料予

以解碼之步驟。

22. 如申請專利範圍第 1 項之方法，其中該網路包含一廣播網路。

23. 一種在一電腦可讀式媒體上實現的一電腦程式，該電腦程式係組配來載入至一數位處理裝置之一記憶體中並控制該數位處理裝置實施依據申請專利範圍第 1 至 22 項中任一項之方法。

24. 一種操作為使用在一鑑定架構中以在該客戶端實體(UE)與一網路之間執行鑑定之客戶端實體之裝置，該網路包含至少一引導伺服器功能實體(BSF)與一網路應用功能實體(NAF)，其中該客戶端實體(UE)係可操作為具有缺乏自該客戶端實體至該引導伺服器功能實體(BSF)及/或該網路應用功能實體(NAF)之一返回頻道的一單向網路連接，該裝置包含：

接收裝置(87)，用以從一網路應用功能實體接收將從該網路應用功能實體傳送至該客戶端實體之鑑定資訊與資料，該鑑定資訊包含用於該客戶端實體之引導會談資料；及

鑑定裝置(81)，其可使用該接收的包含用於該客戶端實體之引導會談資料之鑑定資訊來鑑定網路，其中該鑑定包含依據一通用鑑定架構來實施包括一通用鑑定之一鑑

定。

25. 如申請專利範圍第 24 項之裝置，進一步包含該密鑰產生裝置(82)，用以產生該網路應用功能實體的一密鑰。

26. 如申請專利範圍第 24 項之裝置，進一步包含該建立裝置(84)，用以在該客戶端實體與該引導伺服器功能實體之間建立一引導會談。

27. 如申請專利範圍第 24 項之裝置，進一步包含該儲存裝置(85)，用以儲存該引導會談資料。

28. 如申請專利範圍第 24 項之裝置，進一步包含該解密裝置(83)，其可使用該網路應用功能實體的一密鑰而將從該網路應用功能實體接收的加密資料予以解密。

29. 如申請專利範圍第 24 項之裝置，進一步包含處理和控制裝置(86)，用以處理資料及信令，及用以控制該裝置及其構成裝置。

30. 如申請專利範圍第 25 項之裝置，其中該裝置包含至少一使用者設備，並可連接到一全球用戶識別模組。

31. 如申請專利範圍第 24 項之裝置，其中該客戶端實

體包含一機上盒。

32. 如申請專利範圍第 31 項之裝置，其中該鑑定裝置係組配來存取使用者。

33. 如申請專利範圍第 32 項之裝置，其中該使用者識別資訊係儲存在可連接至該客戶端實體之一智慧卡中。

34. 一種在一客戶端實體(UE)與一網路之間執行鑑定之方法，該網路包含至少一引導伺服器功能實體(BSF)與一網路應用功能實體(NAF)，其中該客戶端實體(UE)具有缺乏從該客戶端實體至該引導伺服器功能實體(BSF)及/或該網路應用功能實體(NAF)之一返回頻道的一單向網路連接，該鑑定包含：

從該網路應用功能實體接收(S66)來自該引導伺服器功能之鑑定資訊與將從該網路應用功能實體傳送之資料，該鑑定資訊包含用於該客戶端實體之引導會談資料，以及

使用接收的包含用於該客戶端實體之該引導會談資料的該鑑定資訊來鑑定該網路，其中該鑑定包含依據一通用鑑定架構來實施包括一通用鑑定之一鑑定。

35. 如申請專利範圍第 34 項之方法，其進一步包含產生該網路應用功能實體之一密鑰。

36. 如申請專利範圍第 34 項之方法，其進一步包含在該客戶端實體與該引導伺服器功能實體之間建立一引導會談。

37. 如申請專利範圍第 34 項之方法，其進一步包含該儲存該引導會談資料。

38. 如申請專利範圍第 34 項之方法，其進一步包含使用該網路應用功能實體的一密鑰而將從該網路應用功能實體接收的加密資料予以解密。

39. 如申請專利範圍第 34 項之方法，其進一步包含處理資料及信令，及用以控制該裝置及其構成裝置。

40. 一種在一電腦可讀式媒體上實現的一電腦程式，該電腦程式係組配來載入至一數位處理裝置之一記憶體中並控制該數位處理裝置實施依據申請專利範圍第 34 至 39 項中任一項之方法。

41. 一種操作為使用在一鑑權架構中以在一客戶端實體(UE)與一網路之間執行鑑定之網路應用功能實體之裝置，該網路包含至少操作為一網路應用功能實體之該裝置，且其具有一網路應用功能實體(NAF)與一引導伺服器功能實體(BSF)，而且其中該客戶端實體(UE)係可操作為具有

缺乏從該客戶端實體至該引導伺服器功能實體(BSF)及/或該網路應用功能實體(NAF)之一返回頻道的一單向網路連接，該裝置包含：

收發器裝置，用以傳送至該客戶端實體，及用以從一引導伺服器功能實體傳送及接收；

其中該收發器裝置適用於當該網路應用功能實體需要將資料安全傳送給該客戶端實體時，將鑑定資訊的一請求傳送給該引導伺服器功能實體，該請求包含該客戶端實體之一個人識別；

從該引導伺服器功能實體接收包括包含用於該客戶端實體之引導會談資料之該鑑定資訊的一回應；及

傳送包含用於該客戶端實體之該引導會談資料之該鑑定資訊與傳送給該客戶端實體的資料，

其中該鑑定資訊適用於包括依據一通用鑑定架構之一通用鑑定之一鑑定。

42. 如申請專利範圍第 41 項之裝置，其中該收發器裝置(91)配置成可將該網路應用功能實體的一識別傳送給該客戶端實體。

43. 如申請專利範圍第 41 項之裝置，進一步包含該加密裝置(92)，其可通過使用該網路應用功能實體的一密鑰而將傳送給客戶端實體的資料予以加密。

44. 如申請專利範圍第 41 項之裝置，其中該裝置係組配來廣播傳輸。

45. 一種用以在一客戶端實體(UE)與包含一引導伺服器功能實體(BSF)和一網路應用功能實體(NAF)的一網路之間實施鑑定之方法，其中該客戶端實體(UE)具有缺乏從該客戶端實體至該引導伺服器功能實體(BSF)及/或該網路應用功能實體(NAF)之一返回頻道的一單向網路連接，該鑑定之方法包含下列步驟：

當該網路應用功能實體需要將資料安全傳送給該客戶端實體時，該請求包含該客戶端實體之一個人識別，將用於鑑定資訊的一請求傳送(S62)給該引導伺服器功能實體；

接收(S64)包括該鑑定資訊的一回應，該鑑定資訊包含來自該引導伺服器功能實體的用於該客戶端實體之引導會談資料，以及

傳送(S66)包含用於該客戶端實體之引導會談資料之該鑑定資訊與將傳送給該客戶端實體的資料，

其中該鑑定資訊適用於包括依據一通用鑑定架構之一通用鑑定之一鑑定。

46. 如申請專利範圍第 45 項之方法，其進一步包含傳送該網路應用功能實體之一識別至該客戶端實體。

47. 如申請專利範圍第 45 項之方法，其進一步包含利

用該網路應用功能實體之一密鑰將被傳送至該客戶端實體之資料加密。

48. 一種在一電腦可讀式媒體上實現的一電腦程式，該電腦程式係組配來載入至一數位處理裝置之一記憶體中並控制該數位處理裝置實施依據申請專利範圍第 45 至 47 項中任一項之方法。

49. 一種操作為使用在一鑑權架構中以在一客戶端實體與一網路之間執行鑑定之引導伺服器功能實體之裝置，該網路包含至少操作為一引導伺服器功能實體(BSF)與一網路應用功能實體(NAF)之該裝置，其中該客戶端實體(UE)係可操作為具有缺乏從該客戶端實體至該引導伺服器功能實體(BSF)及/或該網路應用功能實體(NAF)之一返回頻道的一單向網路連接；該裝置包含：

收發器裝置(101)，用以從一網路應用功能實體傳送及接收；及

處理和取回裝置(102)，用以處理從該網路應用功能實體接收的一請求，該請求包含該客戶端實體的一個人識別，及用以取回該鑑定資訊，該處理與取回裝置進一步包含用來建立用於客戶端實體之引導會談資料的建立裝置；

其中該收發器裝置(101)配置成從該網路應用功能實體接收該請求，並將包含用於該客戶端實體之該建立的引導會談資料之該鑑定資訊傳送給該網路應用功能實體，

其中該鑑定資訊適用於包括依據一通用鑑定架構之一通用鑑定的一鑑定。

50. 如申請專利範圍第 49 項之裝置，進一步包含該拾取裝置(105)，用以從一本籍用戶系統拾取該鑑定資訊(HSS)。

51. 如申請專利範圍第 49 項之裝置，進一步包含該觸發裝置(103)，用以觸發該客戶端實體以建立一有效的引導會談。

52. 如申請專利範圍第 49 項之裝置，其中該網路包含一廣播網路。

53. 一種用以在一客戶端實體(UE)與包含一引導伺服器功能實體(BSF)和一網路應用功能實體(NAF)的一網路之間實施鑑定之方法，其中該客戶端實體(UE)具有缺乏從該客戶端實體至該引導伺服器功能實體(BSF)及/或該網路應用功能實體(NAF)之一返回頻道的一單向網路連接，該鑑定之方法包含下列步驟：

自該網路應用功能實體接收(S62)用於鑑定資訊的一請求，該請求包含該客戶端實體的一個人識別，

處理(S63)自該網路應用功能實體接收之一請求並取回鑑定資訊，其進一步包含建立用於該客戶端實體之引導

會談資料，

傳送(S64)包括包含該建立的用於該客戶端實體之引導會談資料之該鑑定資訊之一回應至該網路應用功能實體，

其中該鑑定資訊適用於包括依據一通用鑑定架構之一通用鑑定的一鑑定。

54. 如申請專利範圍第 53 項之方法，其進一步包含從一本籍用戶系統(HSS)拾取該鑑定資訊。

55. 如申請專利範圍第 53 項之方法，其進一步包含觸發該客戶端實體以建立一有效的引導會談。

56. 一種在一電腦可讀式媒體上實現的一電腦程式，該電腦程式係組配來載入至一數位處理裝置之一記憶體中並控制該數位處理裝置實施依據申請專利範圍第 53 至 55 項中任一項之方法。

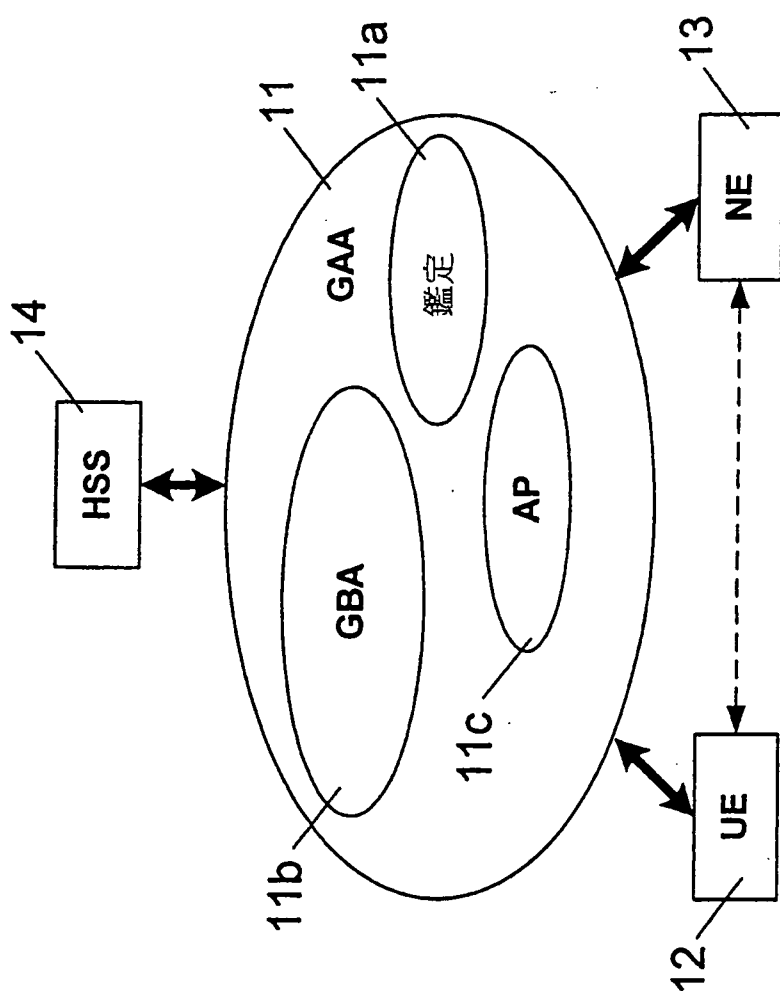


圖 1

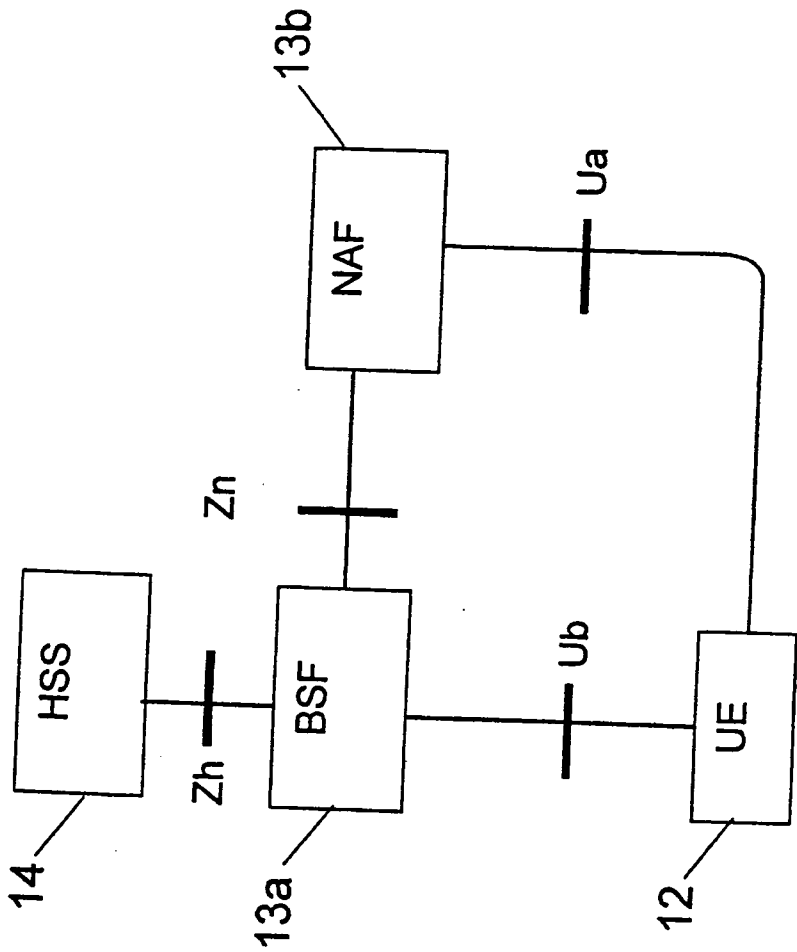


圖 2

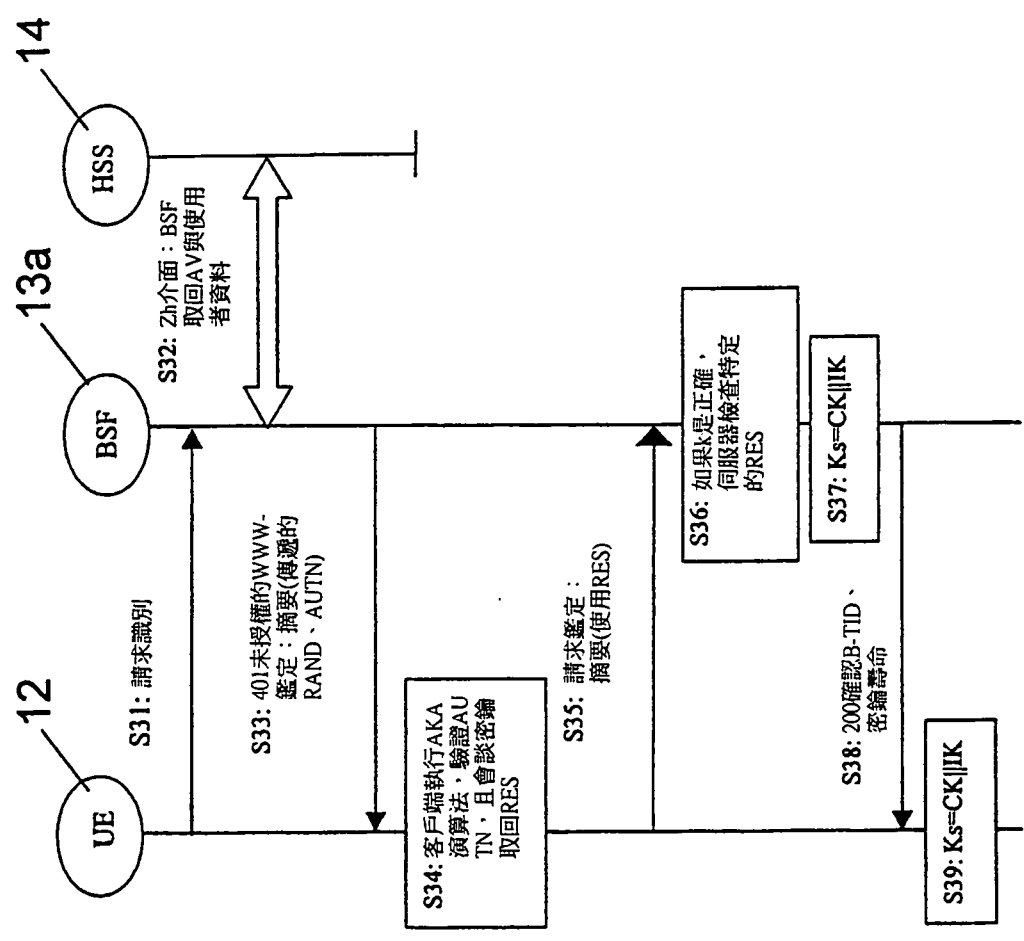


圖 3

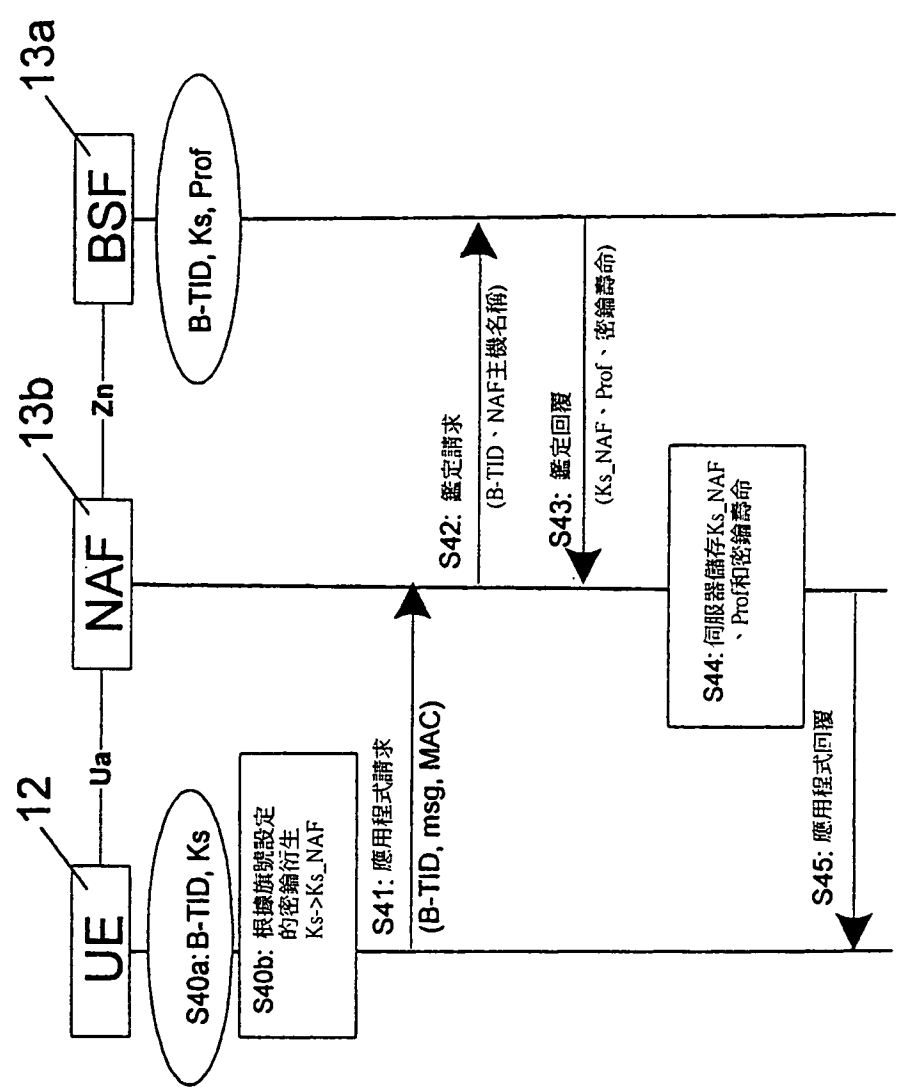


圖 4

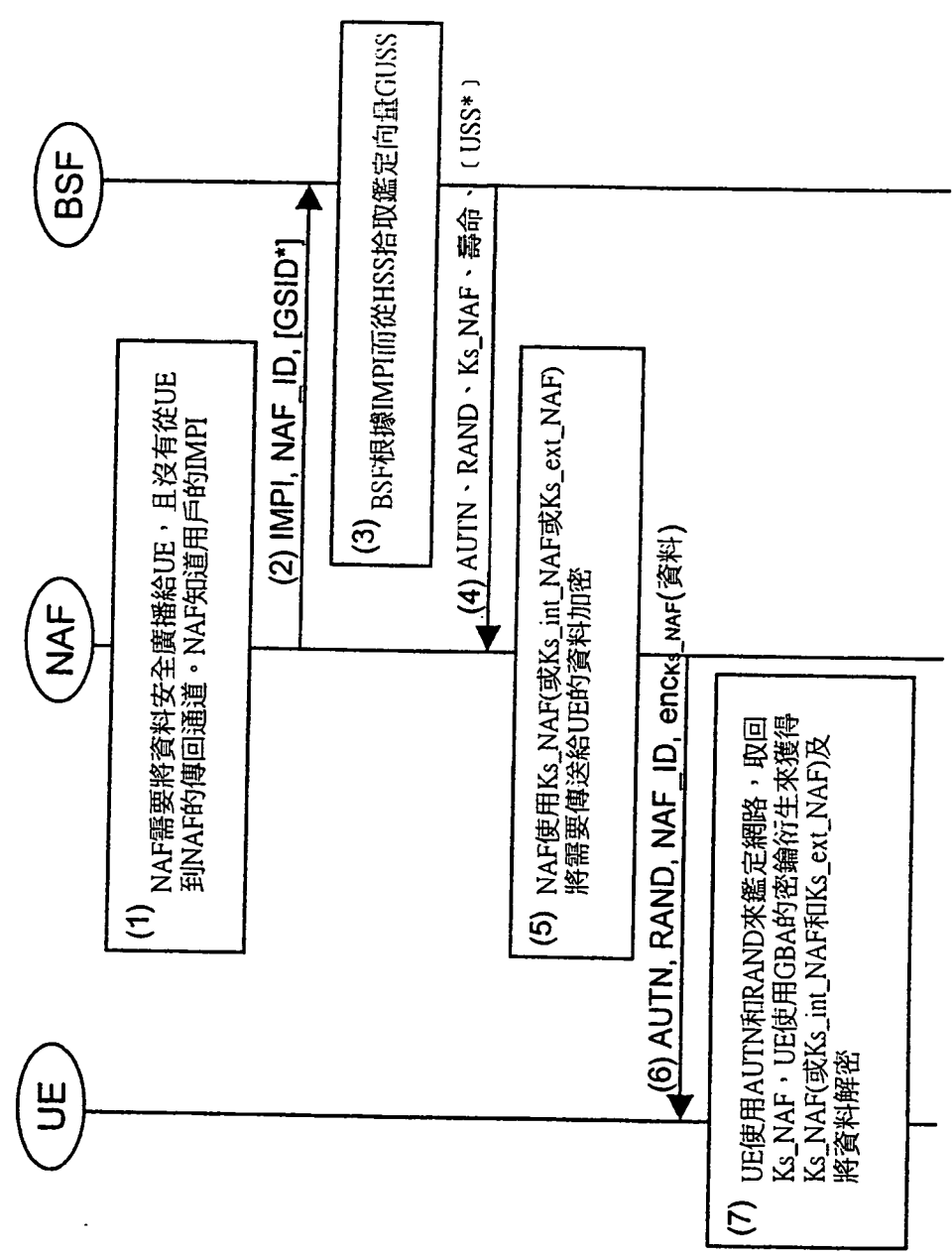


圖 5

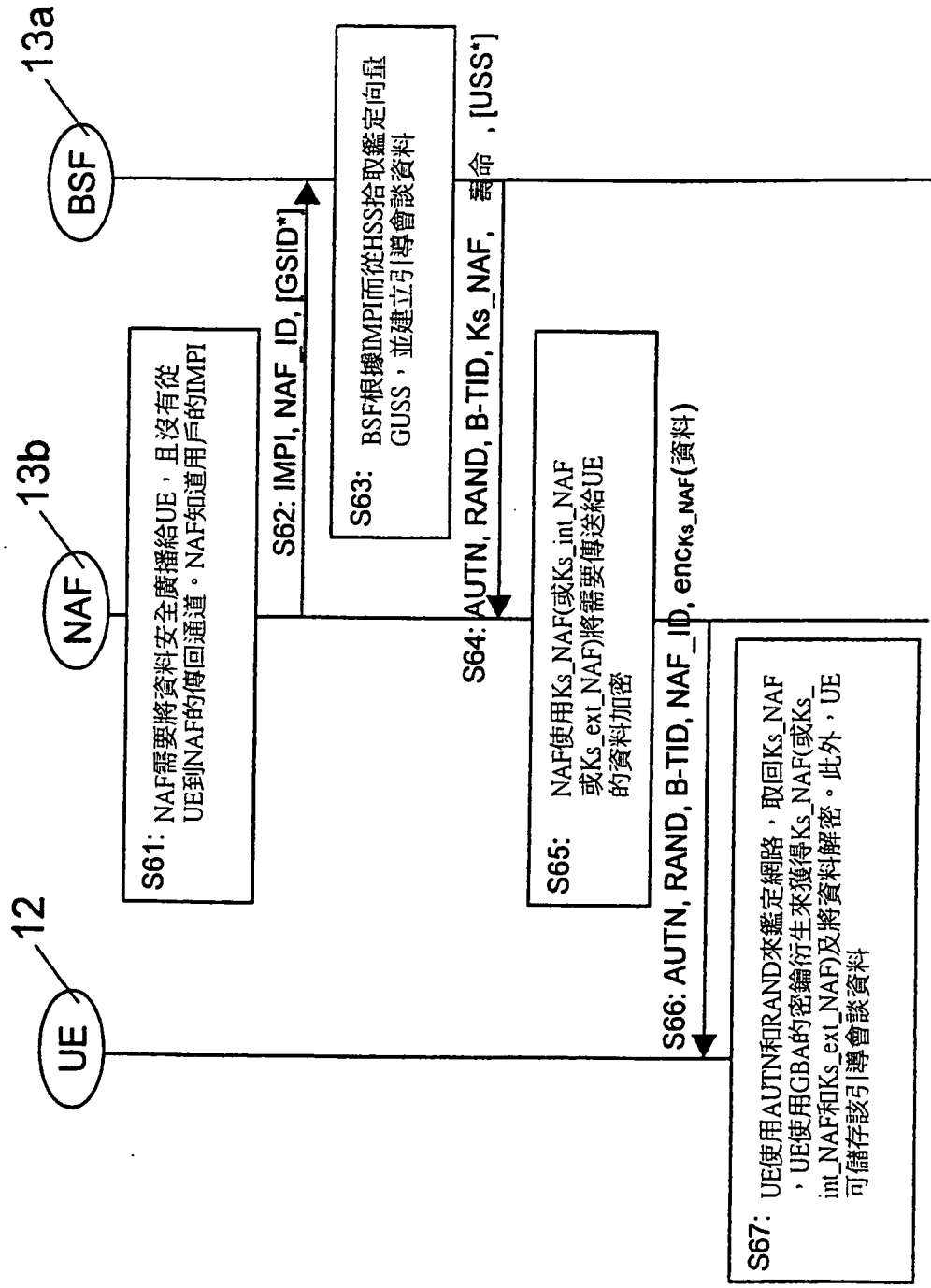


圖 6

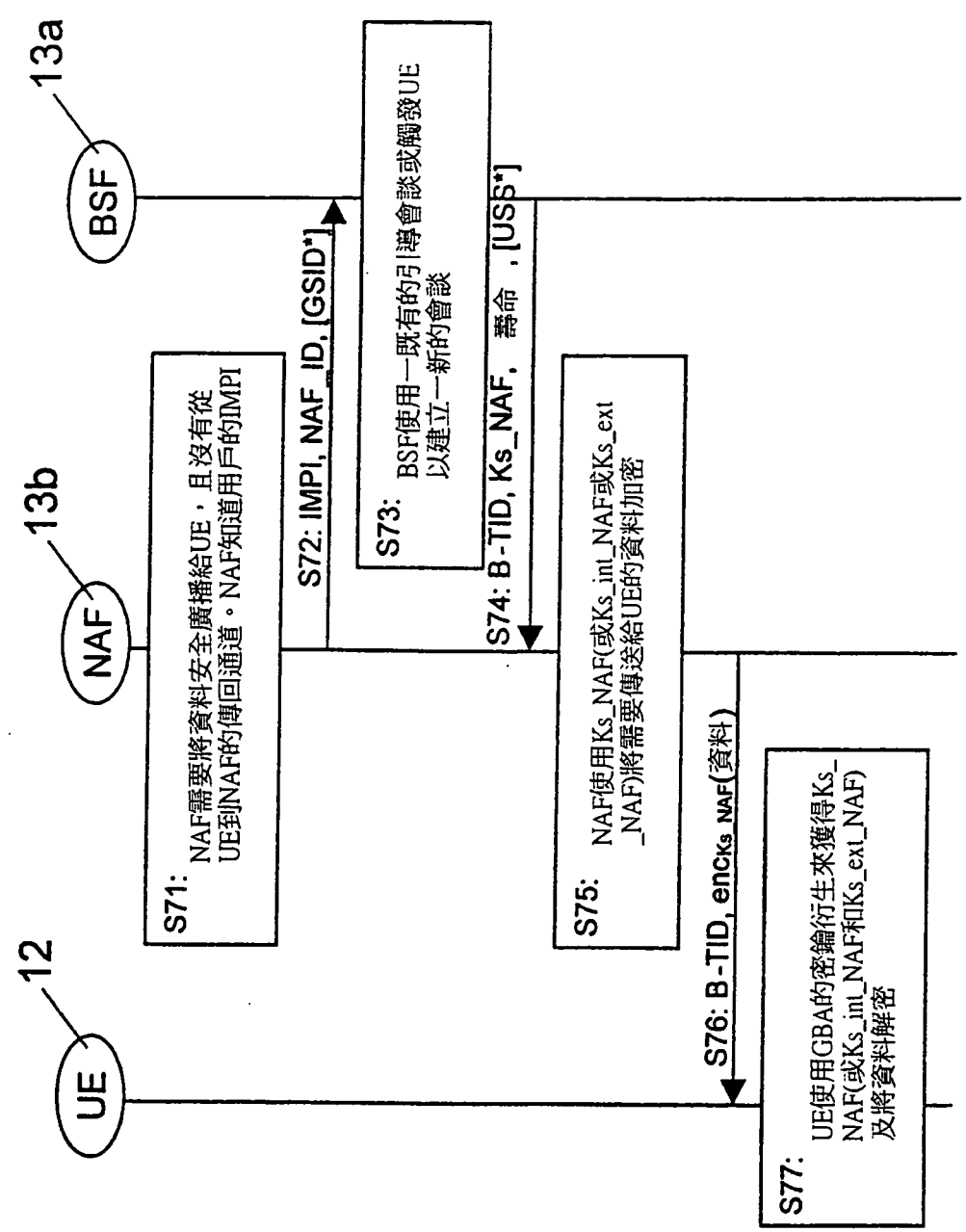


圖 7

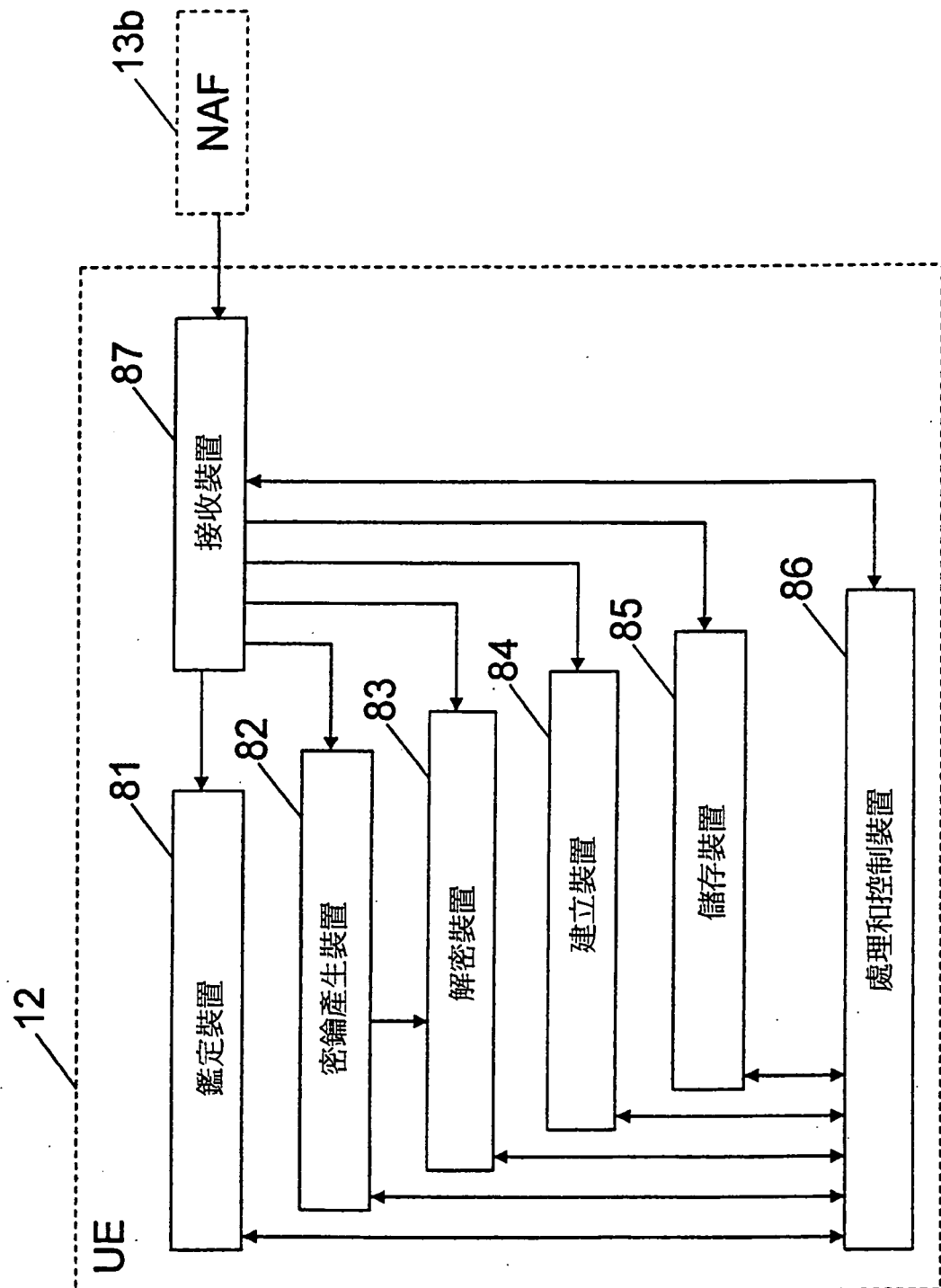


圖 8

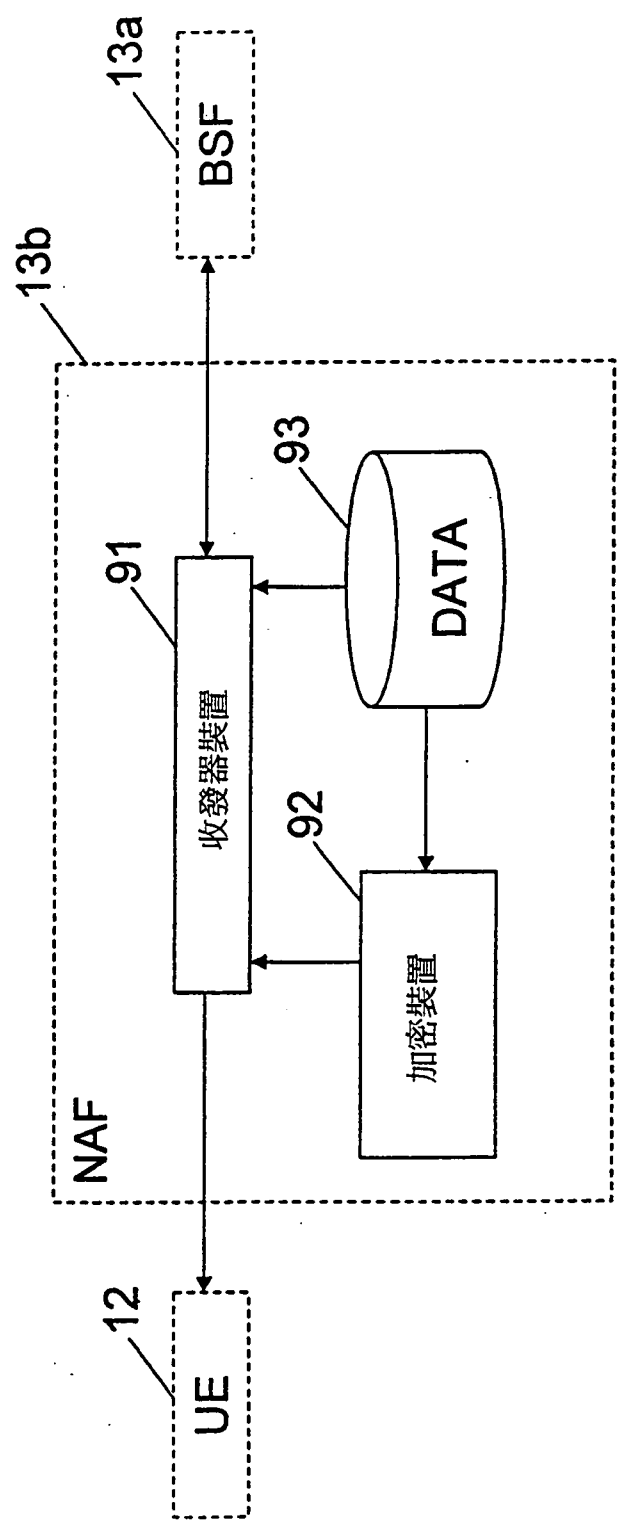


圖 9

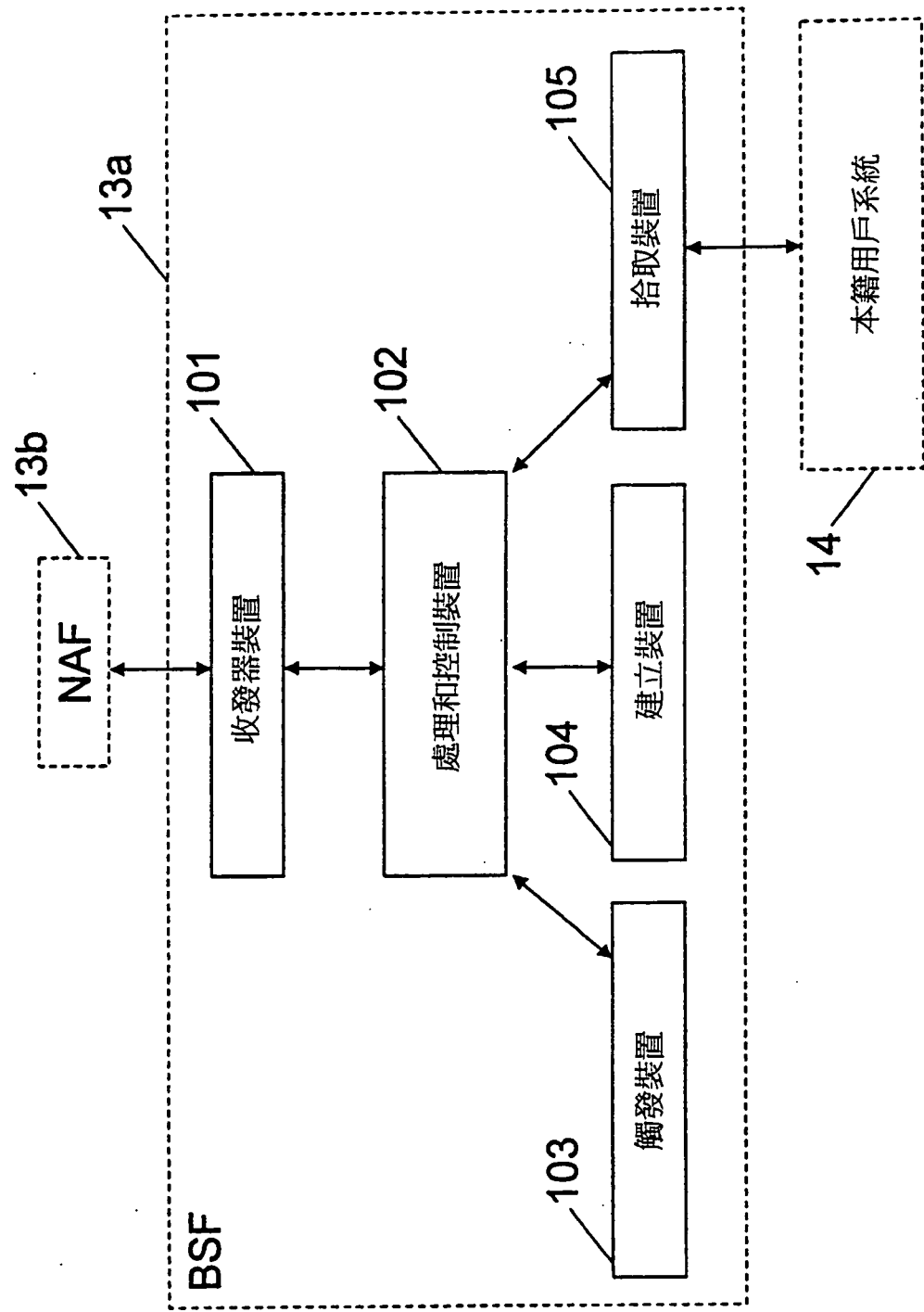


圖 10