(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 201306610 A1
(43)公開日： 中華民國 102 (2013) 年 02 月 01 日

(21)申請案號：101123298 (22)申請日： 中華民國 101 (2012) 年 06 月 28 日
(51)Int. Cl.： *H04W12/06 (2009.01)* *H04L29/06 (2006.01)*
(30)優先權：2011/06/28 美國 61/502,207
2012/01/19 美國 61/588,482
(71)申請人：內數位專利控股公司 (美國) INTERDIGITAL PATENT HOLDINGS, INC. (US)
美國
(72)發明人：車 尹赫 CHA, INHYOK (US)；萊赫 安德魯斯 LEICHER, ANDREAS (DE)；史密特 安德魯斯 SCHMIDT, ANDREAS (DE)；顧吉恩 路易斯 GUCCIONE, LOUIS J. (US)；夏 尤根德拉 SHAH, YOGENDRA C. (GB)；塔爾葛里 優西夫 TARGALI, YOUSIF (US)
(74)代理人：蔡清福
申請實體審查：無 申請專利範圍項數：21 項 圖式數：20 共 106 頁

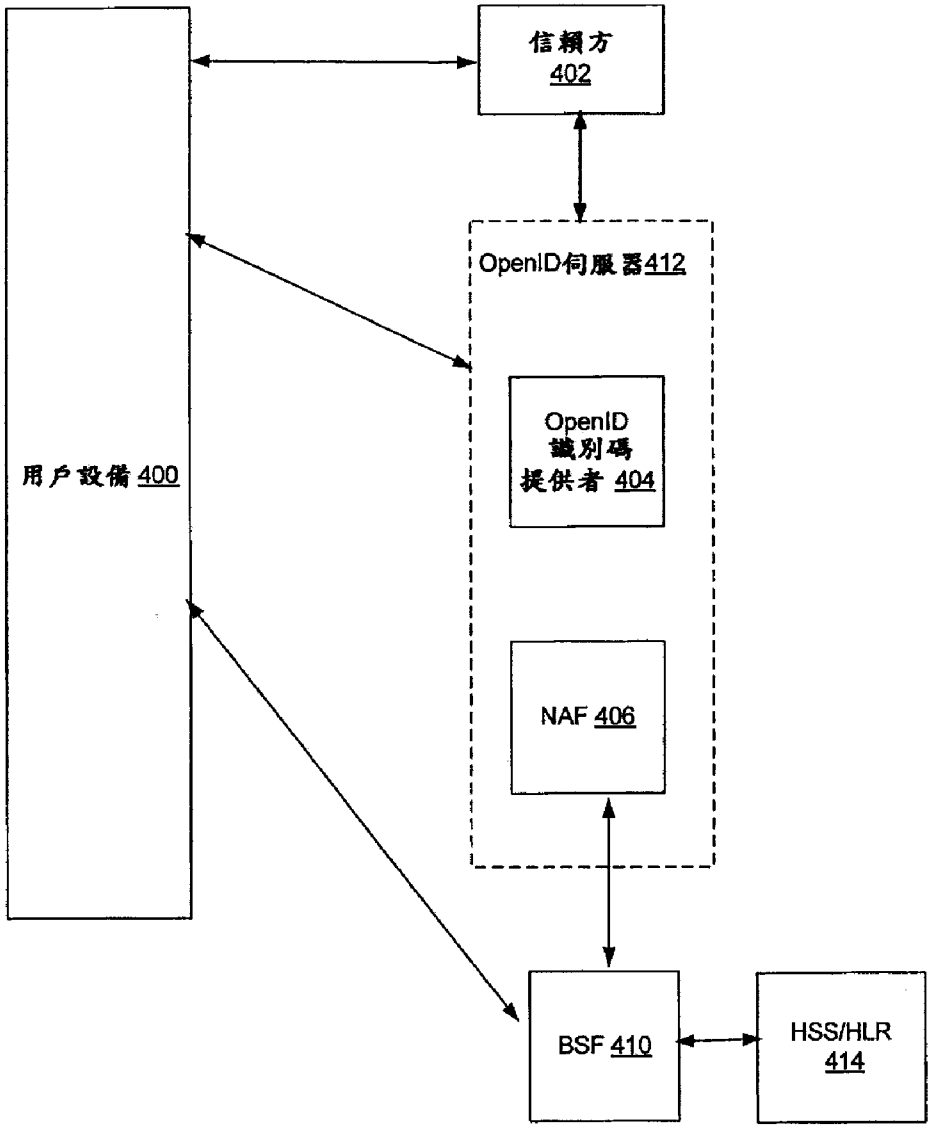
(54)名稱

驗證協定之自動協商及選擇

AUTOMATED NEGOTIATION AND SELECTION OF AUTHENTICATION PROTOCOLS

(57)摘要

無線電信網路可實現各種形式的認證。存在遵循類似網路架構的各種不同的用戶和裝置認證協定，該網路架構涉及各種網路實體，包括使用者設備（UE）、服務供應者（SP）和認證端點（AEP）。為了選取可接受的用於認證用戶或 UE 的認證協定或證書，認證協定協商可在各種網路實體間發生。例如，協商可發生在實現單點登錄（SSO）架構的網路及/或實現通用引導架構（GBA）的網路中。



BSF：引導伺服器功能

HLR：本地暫存器

HSS：本籍用戶伺服器

NAF：網路存取功能

400：用戶設備

402：信賴方

404：OpenID 識別碼提供者

406：網路存取功能

410：引導伺服器功能

412：OpenID 伺服器

414：HSS/HLR

(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 201306610 A1
(43)公開日： 中華民國 102 (2013) 年 02 月 01 日

(21)申請案號：101123298 (22)申請日： 中華民國 101 (2012) 年 06 月 28 日
(51)Int. Cl.： *H04W12/06 (2009.01)* *H04L29/06 (2006.01)*
(30)優先權：2011/06/28 美國 61/502,207
2012/01/19 美國 61/588,482
(71)申請人：內數位專利控股公司 (美國) INTERDIGITAL PATENT HOLDINGS, INC. (US)
美國
(72)發明人：車 尹赫 CHA, INHYOK (US)；萊赫 安德魯斯 LEICHER, ANDREAS (DE)；史密特 安德魯斯 SCHMIDT, ANDREAS (DE)；顧吉恩 路易斯 GUCCIONE, LOUIS J. (US)；夏 尤根德拉 SHAH, YOGENDRA C. (GB)；塔爾葛里 優西夫 TARGALI, YOUSIF (US)
(74)代理人：蔡清福
申請實體審查：無 申請專利範圍項數：21 項 圖式數：20 共 106 頁

(54)名稱

驗證協定之自動協商及選擇

AUTOMATED NEGOTIATION AND SELECTION OF AUTHENTICATION PROTOCOLS

(57)摘要

無線電信網路可實現各種形式的認證。存在遵循類似網路架構的各種不同的用戶和裝置認證協定，該網路架構涉及各種網路實體，包括使用者設備（UE）、服務供應者（SP）和認證端點（AEP）。為了選取可接受的用於認證用戶或 UE 的認證協定或證書，認證協定協商可在各種網路實體間發生。例如，協商可發生在實現單點登錄（SSO）架構的網路及/或實現通用引導架構（GBA）的網路中。

201306610

DTD版本：2.0.0

發明專利說明書

※記號部分請勿填寫

※申請案號：

※IPC分類：H04N 13/00 (2009.01)
H04L 29/06 (2006.01)

※申請日：101.6.28

一、發明名稱：

驗證協定之自動協商及選擇

Automated Negotiation And Selection Of Authentication Protocols

二、中文發明摘要：

無線電信網路可實現各種形式的認證。存在遵循類似網路架構的各種不同的用戶和裝置認證協定，該網路架構涉及各種網路實體，包括使用者設備（UE）、服務供應者（SP）和認證端點（AEP）。為了選取可接受的用於認證用戶或UE的認證協定或證書，認證協定協商可在各種網路實體間發生。例如，協商可發生在實現單點登錄（SSO）架構的網路及/或實現通用引導架構（GBA）的網路中。

三、英文發明摘要：

Wireless telecommunications networks may implement various forms of authentication.There are a variety of different user and device authentication protocols that follow a similar network architecture, involving various network entities such as a user equipment (UE), a service provider (SP), and an authentication endpoint (AEP).To select an acceptable authentication protocol or credential for authenticating a user or UE, authentication protocol negotiations may take place between various network entities.For example, negotiations may take place in networks implementing a single-sign on (SSO) architecture and/or networks implementing a Generic Bootstrapping Architecture (GBA).

四、指定代表圖：

(一)本案指定代表圖為：第4圖

(二)本代表圖之元件符號簡單說明：

BSF、410　引導伺服器功能

HLR　本地暫存器

HSS　本籍用戶伺服器

NAF、406　網路存取功能

400　用戶設備

402　信賴方

404　OpenID識別碼提供者

412　OpenID伺服器

414　HSS/HLR

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

六、發明說明：

【發明所屬之技術領域】

[0001] 相關申請案的交叉引用

本申請案要求2011年6月28日申請的美國臨時專利申請案No. 61/502,207和2012年1月19日申請的美國臨時專利申請案No.61/588,482的權益，每個申請案的內容以完全引用的方式結合於此。

【先前技術】

[0002] 無線電信網路可實現各種形式的認證。存在遵循類似網路架構的各種不同用戶和裝置認證協定，涉及使用者設備（UE）、服務供應者（SP）和認證端點（AEP）。第1圖顯示了這樣的一般架構100。一般架構100包括UE 102、SP 104和AEP 106。UE 102可與諸如網站這樣的SP 104進行通信以存取服務。在允許UE 102存取服務前，SP 104可要求UE 102被認證。AEP 106可為SP 104認證UE 102。實現一般架構100的一個示例架構是聯合識別碼管理（federated identity management）架構，例如OpenID或OpenID連接協定。第2圖顯示了當應用於OpenID的一般架構100。在實施OpenID協定的系統中，AEP可被實施為OpenID識別碼提供者（OP）202，並且SP典型地可被稱為信賴方（relying party，RP）204。OP 202可為RP 204認證UE 102。例如，在使用OP 202認證UE 102後，UE 102可存取由RP 204提供的服務。

也可在實現通用引導架構（Generic Bootstrapping Architecture，GBA）的系統中找到第1圖的一般架構

100。第3圖是一般架構100 的GBA實現的示例圖。在GBA實現中，SP可被實現為網路存取功能（NAF）304，並且AEP可被實現為引導伺服器功能（BSF）302。

存在可被應用於第1、2和3圖所示架構中的各種不同的認證協定。例如，在OpenID架構中，可使用各種協定（例如AKA、EAP或GBA）來認證UE。在主要實現GBA的系統中，存在可被採用的GBA的不同形式（協定）。雖然，各種形式的認證可用於網路，但在網路上的實體可以被限制使用特定形式的認證。例如，使用通用引導架構（GBA）的一些網路實體可以被限制協商認證的形式及/或選取認證的特定形式。此外，網路實體可被限制使用某些類型的證書來認證其他網路實體。

【發明內容】

[0003] 該發明內容被提供來以簡化的形式介紹以下在實施方式中將進一步得以描述的各種概念。該發明內容並不旨在確定所要求保護的主題的關鍵特徵或必要特徵，也不旨在被用於限制所要求保護的主題的範圍。

在此揭露了用於在網路的實體間協商以選取將被用來認證使用者設備（UE）的認證協定及/或證書的方法和裝置。揭露了包括單點登錄（single sign-on，SSO）架構和通用引導架構（GBA）的實施例。

在此描述的實施例可提供包括可經由網路可進行通信的UE、服務供應者（SP）和認證端點（AEP）的系統。UE可為AEP指明和識別該UE所支援的一個或多個認證協定及/或證書。AEP可確定可用於認證UE的一個或多個認證協定及/或證書。UE和AEP可協商以選取SP可接受的認證協

定及/或證書。可使用選取的認證協定或證書來認證UE。在一個示例實施例中，AEP可與SP協商以確定SP可接受的一個或多個認證協定或證書。

在一個示例實施例中，協商和選取認證協定及/或證書的網路可實施通用引導架構（GBA）。例如，在這樣的網路中的SP可包括網路存取功能（NAF），並且AEP可包括引導伺服器功能（BSF）。在另一個示例實施例中，網路可實施GBA和OpenID聯合識別碼管理架構。例如，AEP可包括NAF和例如諸如OpenID IdP（OP）這樣的識別碼提供者（IdP）。服務供應者可包括信賴方（RP）。

【實施方式】

[0004] 在此揭露了用於協商和選取認證協定及/或證書的各種方法和系統。例如，實現第1圖中所示的一般架構100的系統可協商特定認證協定的使用及/或選取認證協定。參考第1圖，例如，使用者設備（UE）102、服務供應者（SP）104和認證端點（AEP）106可經由網路進行通信。UE 102可為AEP 106指明和識別由UE 102支援的一個或多個認證協定及/或證書。AEP 106可確定可被用來認證UE 102的一個或多個認證協定及/或證書。UE 102和AEP 106可協商以選取SP 104可接受的認證協定及/或證書。可使用選取的認證協定及/或證書來認證UE 102。在示例實施例中，AEP 106可與SP 104協商以確定SP 104可接受的一個或多個認證協定或證書。

第2圖闡明了根據另一個示例實施例的示例OpenID架構，其中可以協商和選取認證協定及/或證書。例如，UE 102可向信賴方（RP）204發送存取由RP 204提供的服務的

請求。UE 102可與OpenID識別碼提供者（OP）202協商以選取RP 204可接受並且由UE 102支援的多個認證協定及/或證書中的一者。可使用選取的認證協定及/或證書來認證UE 102。OP 202可向UE 102發送根據選取的認證協定的認證結果的指示。例如，這樣的指示可包括可由UE 102轉發給RP 204的經簽名的判定訊息（signed assertion message）。在示例實施例中，該指示可包括從根據選取的認證協定及/或證書的UE的認證產生的密鑰。

在此處描述的另一個示例實施例中，認證協定及/或證書可在如第3圖所示的實施通用引導架構（GBA）的系統中進行協商和選取。GBA可涉及如在此將進一步解釋的標準化3GPP架構。例如，UE 102可向網路存取功能（NAF）304發送對NAF 304提供的服務進行存取的請求。例如，請求可在用戶代理標頭（user agent header）中包括產品訊標（product token）。這樣的產品訊標可指示UE 102請求使用GBA摘錄協定（GBA Digest protocol）。回應於這樣的請求，UE 102可接收在標頭中包括前綴的碼401回應，其中該前綴指明允許UE 102執行GBA摘錄協定。UE 102可與引導伺服器功能（BSF）304協商以選取NAF 304可接受並且由UE 102支援的多個認證協定及/或證書中的一者。例如，UE 102可向NAF 304提供一個或多個GBA認證協定由UE 102支援的指示。UE 102可從NAF 304接收可接受所支援的GBA認證協定中的至少一者的指示。這樣的可接受GBA認證協定可包括例如基於SIP摘錄的GBA安全關聯。作為另一個示例，UE 102可從

NAF 304接收包括領域屬性（realm attribute）的引導發起訊息。這樣的訊息可觸發UE 102使用選取的認證協定及/或證書來運行引導協定。在一個實施例中，如果沒有由UE 102支援的GBA認證協定為NAF 304可接受，UE 102可接收錯誤訊息，從而終止GBA引導。

在另一個實施例中，在實施OpenID架構的系統中，GBA協定可提供用戶及/或使用者設備（UE）的認證。第4圖顯示了根據示例實施例的在這樣的系統中OpenID和GBA協定可如何協作。在這樣的實施例中，UE 400可向信賴方（RP）402指示其支援基於GBA的認證。如在此使用的那樣，術語UE可涉及用戶裝置本身或可涉及UE的用戶。RP 402可將UE 400重新定向到具有集成的網路存取功能（NAF）406和OpenID識別碼提供者（OP 404）的OpenID伺服器412（在此被稱為NAF/OP）。集成的OpenID伺服器412（NAF/OP）和RP 402可能希望根據OpenID擴展來“協商”例如以確定NAF/OP 412是否可接受由RP 402提供的協定及/或證書。如果協商和選取的協定是GBA協定，UE 400可例如根據安全儲存在UE 400上及/或操作者的策略伺服器（例如本籍用戶伺服器（HSS）/本地暫存器（HLR）414）中的操作者的策略來與BSF 410一起執行GBA引導。在這樣的實施例中，OpenID協定的集成OP伺服器412也可執行GBA協定的NAF 406。第4圖中的AEP可包括OP 404、NAF 406和BSF 410。

SSO架構中認證協定選取/協商的示例實施例

SSO框架描述

以下進一步提供用於在實施第1圖的一般構架100的示例SSO框架的環境中選取及/或協商各種認證協定的使用的方法的實施例細節。在第5圖中更加詳細地示出示例性SSO框架。

如第5圖所示，SSO子系統506可與被配置為存取來自服務供應者（SP）的服務的應用進行通信，例如瀏覽器應用502及/或非瀏覽器應用504。這些應用（瀏覽器應用502和非瀏覽器應用504）可以是用戶可與其互動的應用。使用瀏覽器應用502及/或非瀏覽器應用504，用戶可具有到各種服務（例如網站、銀行服務、用於娛樂事件的售票服務及/或由服務供應者提供的其他服務）的存取。

SSO子系統506可充當SSO過程的集線器。在示例的框架中，SSO子系統506可以是操作者控制的。SSO子系統506可藉由執行用戶認證（例如用戶輔助及/或網路輔助的）來用作網路代理。此外，SSO子系統506可執行後繼的經簽名或可信的用戶識別碼判定及/或認證判定的創建及/或將其提供給服務供應者及/或識別碼提供者，以用於網路輔助的認證。SSO子系統506的一些功能(例如安全儲存和處理)可在安全可信的環境518中執行。

第5圖所示的架構可結合用戶輔助的認證體驗和大量各自獨立的網路輔助認證協定（例如也被稱為SSO技術或SSO協定或SSO代理），其中的一些可使用網路輔助認證來執行用於認證和密鑰交換的引導機制。例如，SSO子系統506可與多個認證模組508、510、512、514及/或516進行通信，認證模組508、510、512、514及/或516中的每一個能夠使用不同的網路輔助認證協定及/或證書以與

服務提供者一起執行網路輔助認證。這些網路輔助認證模組508、510、512、514及/或516可被用來基於諸如數位證書、共享主密鑰（shared master secrets）這樣的預先安裝證書或使用不同的支援認證方案的註冊的任何其他方法，以將安全用戶存取提供到期望服務。例如，認證模組可包括OpenID/SIP摘錄模組508、另一個OpenID模組510、OpenID/GBA模組512、OpenID/ISIM模組514及/或OpenID/AKA模組516。雖然在第5圖中示出的各網路輔助認證模組的實施OpenID網路輔助認證協定，但也可以或者可替代地實施其他類型的網路輔助的認證協定及/或證書。

網路輔助認證模組中的一個或多個可由給定的服務供應者及/或識別碼提供者來支援。每個網路輔助認證模組可被配置為藉由執行其相應的認證協定（例如藉由使用認證演算法）來執行網路輔助的認證。OpenID/GBA模組512、OpenID/ISIM模組514及/或OpenID/AKA模組516可與安全可信環境518進行通信。安全可信環境518例如可包括UICC、智慧卡或其他安全可信環境。在示例實施例中，安全可信環境518可以是UE上的基於硬體的實體、並且可負責安全地儲存敏感資料（例如加密密鑰、用戶證書）和執行敏感功能（加密計算）的安全處理。

第5圖所示的元件中的一個或多個可駐留在行動通信裝置中。雖然第5圖示出了在所描述架構中的功能模組，但第5圖並不意味著要求正如在或不在安全可信環境518上那樣的任何非應用功能的駐留。這些元件及其互動自此將更詳細地描述。雖然將參考OpenID協定來描述認證，但

相同的概念可應用於其他認證協定，例如自由聯盟（Liberty Alliance）。

用戶可使用應用（例如瀏覽器應用502及/或非瀏覽器應用504）來對諸如網路應用服務供應者這樣的服務供應者（例如信賴方（RP））做初始訪問。服務供應者（例如RP）可接收例如可以是OpenID用戶識別符的用戶識別。在OpenID的情況下，在RP發起的發現（discovery）後，用戶可被重新定向（例如發現機制可使用OpenID提供者（OP）識別碼來確定OP的網際網路位址）到基於網路的識別碼管理實體，其例如可以是OP。OP識別碼可被用來向RP提供OP的網際網路地址。然後認證過程可開始。SSO子系統506可提供用於賦能與用戶在應用側與其互動的應用的通信的用戶認證介面和用於網路輔助認證模組508、510、512、514及/或516的網路認證介面。因此，不同的應用（例如瀏覽器應用502及/或非瀏覽器應用504）可基於用戶輸入以向SSO子系統506提供輸入，或者SSO子系統506可向用戶呈現認證螢幕以賦能使用服務供應者的用戶的網路輔助認證及/或使用UE的本地用戶輔助認證。不同的網路輔助認證模組508、510、512、514及/或516（例如認證協定）可被設計以與SSO子系統506互動。策略管理也可由SSO子系統506來執行。

SSO子系統506認證結構可處理兩種類型的用戶認證，用戶輔助認證和網路輔助認證。這兩種類型都可以被分離，使得一個可獨立於另一個地發生，但是這兩者可以互相聯合（例如經由可由SSO子系統產生的判定）並且互相互動（例如用戶輔助認證可觸發網路輔助認證，反之亦

然）。用戶的用戶輔助認證和從用戶到SSO子系統506的證書提供（用於用戶輔助認證）可獨立地發生、並且可與網路輔助認證協定分離。用戶可避免網路輔助認證協定。此透明性，與單一用戶證書組可獨立於服務供應者的事實一起，可產生用戶的無縫SSO體驗。此外，這兩種認證類型可提供用戶經由其證書、生物特徵、密碼、PIN、訊標、其他用戶證書或其組合所要求的識別碼與在UICC中保持的用戶證書或諸如IMSI或IMPI這樣的裝置識別碼的綁定。這樣的綁定，與兩種類型認證的架構分離一起，可由充當中間層的SSO子系統506來實現。如在此描述的那樣，SSO子系統可藉由其本身或藉由調用較低層認證協定中的一者來執行加密綁定。

SSO子系統506可作用為用於外部事件相關者（例如MNO）的網路輔助認證功能的代理、並且可向該外部事件相關者提供關於提供的策略功能的資訊。當用戶發起到服務的存取時（例如經由在網頁瀏覽器上鍵入URL或者開始一個應用），可以發起用戶輔助認證過程。例如，可請求用戶輸入用戶證書，例如生物特徵證書及/或諸如例如PIN這樣的密碼。在示例框架中，行動通信裝置可處理PIN特徵，以存取也可以是用戶證書資訊一部分的裝置本身。例如，UE的用戶介面可將用戶輔助認證證書資訊、正被存取的服務（例如以網頁URL或被啟動的應用的形式）及/或與將使用的服務相關的其他資訊以經由特定的介面傳遞給SSO子系統506。這樣的傳遞可啟動在SSO子系統506中的功能以基於提供的資訊和提供的策略來認證用戶。例如，來自用戶輔助認證的參數可被提供給網路輔

助認證協定。這樣的參數例如可包括用戶輔助認證的置信等級、用戶輔助認證的結果（例如通過或失敗）和用戶輔助認證的時間。SSO子系統506可運行可包括諸如被認為足夠用於正被存取的服務的認證的置信（保證）等級和認證的最小新鮮期（minimum freshness）（例如完成時間）這樣的各種認證相關參數的策略功能。例如，為了付賬的目的，用戶可能希望使用銀行服務。在此場景中，提供的策略可以要求用戶輔助認證的強形式（例如多因素），並且提供的策略可要求認證正好在將該用戶導航到該服務之前執行。如果對於服務（例如email存取）需要低等級的安全性，策略可放鬆用戶輔助認證要求。例如，PIN可用於對於低等級安全性的用戶輔助認證。驅動用戶認證的策略可由外部事件相關者及/或服務供應者來執行。例如，策略功能可在服務供應者處（例如在網路上）、在UE處（例如本地）或其組合（例如分散式功能）執行。

在示例SSO框架中，將由SSO子系統506遵循的策略可確定什麼SSO認證協定（例如網路輔助認證模組508、510、512、514及/或516）將被選取用於網路輔助認證。用於網路輔助認證模組（例如，SSO認證協定）選取的標準可基於可用資源及/或將被存取的服務的安全要求。內部策略機制可包括外部事件相關者（例如MNO）提供的、優選認證模組（例如SSO認證協定）的優先性排列的列表。一旦作出策略決策，SSO子系統506可提供用於向外部事件相關者（例如MNO）傳達哪個特定網路輔助認證模組已被選取用於協定交換的機制。可選地，例如如在此參考

第7和8圖描述的那樣，SSO子系統可協商能力並對將使用的認證協定達成一致意見。

第6A和6B圖闡明了使用諸如第1圖所示的一般架構100這樣的SSO框架架構實現的協定的示例實施例。在OpenID的環境中，SSO子系統可以安全的方式執行某些功能，這些功能中的一些在此將參考第6A和6B圖中的調用流來描述。

如第6A和6B圖所示，在614，可以執行用戶輔助認證。例如，用戶證書可以被認證及/或處理。用戶證書可包括與用戶602相關聯的唯一的認證參數（例如用戶PIN、密碼、用戶識別符、生物特徵資訊或摘錄）、及/或其他形式的用戶輔助認證參數。用戶602可在裝置604處本地地或結合諸如外部事件相關者（例如MNO）或識別碼提供者（IdP）（例如OpenID提供者612）這樣的遠端實體被認證。

SSO子系統608可以是被配置為執行用戶602認證的使用者設備604上的本地實體。SSO子系統608可以根據各種框架以使用或不使用本地判定實體（LAE）地執行認證。例如，第6A圖闡明了可使SSO子系統能夠本地執行認證的示例提供協定流，如在此描述的那樣。一旦用戶輔助認證完成，在616，SSO子系統608可產生認證結構，例如認證判定。認證判定可包括諸如例如用戶輔助認證完成的時間和認證置信等級這樣的資料。置信等級可涉及遠端方可對用戶或UE的認證進行保證的等級。用戶輔助認證結果（例如通過或失敗）可安全且本地地儲存在設備604處及/或與網路輔助認證協定一起使用。與用戶輔助

認證相關聯的其他參數也可被儲存及/或用於網路輔助認證。例如，這些參數可包括認證的時間、認證的強度及/或認證參數的類型。這些參數可與認證結果一起被儲存或用於網路輔助認證。例如，SSO子系統可使用該資訊來將認證資料中繼給服務供應者，並且服務供應者可確定認證資料是否足以向用戶提供到服務的存取。614處的用戶輔助認證可在任何時間且如基於各種認證策略（例如期望的安全強度）所建議的頻繁地或不頻繁地發生。在示例實施例中，如果儲存了有效的用戶輔助認證結果，SSO子系統可確定用戶等級的認證不需要被執行。這樣的場景可允許用戶存取多個服務供應者（例如RP），而不再需要用戶再參與認證過程。如果例如為了存取在特定服務供應者處的特定服務策略要求新鮮認證，現有認證資訊的這樣的重新利用可能是不允許的。

在618處，共享密鑰可在RP 610和OP 612之間得以建立。例如，可包括用戶提供的識別符的、用戶的OP登錄請求可從應用606（例如瀏覽器或非瀏覽器應用）傳遞至RP 610，這可觸發共享密鑰的關聯及/或建立。例如，當用戶初始嘗試存取基於網路的服務時，登錄請求可被傳遞至RP 610。基於接收到的登錄請求，可建立OP 612和RP 610間的共享密鑰的關聯可以被執行。在示例SSO框架中，在620處，密鑰（例如從OP 612和RP 610共享密鑰導出的密鑰及/或在網路輔助認證期間導出的密鑰）及/或其他證書可被提供給SSO子系統608。提供的證書可被用於與服務的其他認證中，如在此描述的那樣。

例如，網路輔助認證可在提供後執行，如第6B圖所示。

例如，網路輔助認證可在RP 610重新定向到OP 612之後。該重新定向可由應用606（例如瀏覽器應用或非瀏覽器應用）接收，其可在621處將訊息重新定向至SSO子系統608，以用於選取網路輔助認證模組及/或協定。網路輔助認證模組/協定（例如SSO協定）可由SSO子系統608經由策略實施來選取和使用。此過程可包括引導和共享密鑰建立，如在此進一步描述的那樣。

如第5圖所示，若干網路輔助認證協定方法可由一套網路輔助認證模組（例如SSO協定）暗示。再次參考第6B圖，根據示例實施例，OpenID/SIP摘錄及/或OpenID/GBA可被視為處理GBA結構並採用在第3代合作夥伴計畫（3GPP）技術規範（TS）編號33.220（版本10）中規定的機制。在OpenID GBA中，UICC用戶證書可被用來引導將與網路共享的主對話密鑰（例如表示為Ks）。網路輔助認證可產生從Ks導出的、在OP 612和使用者設備604之間共享的應用特定密鑰Ks_NAF。當使用OP 612進行認證時，應用特定密鑰可被使用者設備604使用作為密碼。例如，其可被使用者設備604用作密碼，如例如在3GPP技術報告（TR）編號33.924（版本9）中描述的那樣。

對於OpenID/SIP摘錄，類似的密鑰結構可經由類似GBA過程來產生。網路輔助認證的這個方法可不基於UICC，並且SIP摘錄證書可被使用，而不是例如UICC證書。OpenID/SIP摘錄的一個示例實施例在3GPP TR 33.914（版本11）中描述。

對於OpenID/AKA，網路輔助認證可不基於GBA，並且使用者設備604和OP 612可直接採用3GPP AKA來認證和共

享密鑰。OpenID/AKA的一個示例實施例在3GPP SA3的阿爾卡特-朗訊（Alcatel-Lucent）pCR S3-100757中描述。

對於傳統的OpenID，SSO子系統608可在網路輔助認證協定中提供接收的用戶證書。

雖然OpenID/GBA、OpenID/SIP摘錄和OpenID/AKA可具有結構差異，但從網路本籍用戶伺務器（HSS）接收的一個類型或另一個類型的認證向量（AV）的應用可以是各種協定的中心。第4圖闡明了HSS如何適合整個架構的示例。附加地，取決於策略和期望的安全強度，在網路輔助認證執行時，可執行用戶（用戶輔助認證）的重新認證。在示例實施例中，在這樣的網路輔助認證期間，可假設裝置已建立網路連接，並且網路輔助認證可被用來使用服務供應者來認證UE。

在成功的網路輔助認證後，SSO子系統608可向應用606提供網路輔助認證成功的指示。例如，SSO子系統（例如經由LAE）可在622處簽名認證判定（例如識別碼判定）、並在624處向RP 610發送判定訊息。從SSO子系統608到RP 610的經簽名的判定訊息可指出成功的認證、並且可由SSO子系統608自主地（autonomously）使用以前提供的證書（例如在第6A圖中620處所示的）來簽名。成功的網路輔助認證的這個通知可在用戶602獲得到在RP 610處期望的服務的存取前執行。在認證過程（例如SSO過程）的早期，可能已執行了關聯以建立OP 612和RP 610之間的共享密鑰。判定訊息可使用此共享密鑰及/或該密鑰的導出來簽名。一旦RP 610及/或使用者設備604

（例如經由應用606）已接收到網路輔助認證成功的指示，使用者設備604（例如經由應用606）可存取在其登錄至的RP 610處的服務。

提供給RP 610的判定訊息可指明對網路和對服務的兩次認證完成，並且在用戶輔助認證中實現的用戶要求的識別碼可被綁定到例如在網路輔助認證中實現的用戶證書，諸如例如IMSI或IMPI。例如，經由瞭解用戶提供的證書和基於UICC的（或SIP摘錄）證書之間連接的機制來執行綁定可以是選取的SSO功能性的一部分。判定訊息可包括指明作為整個SSO協定的一部分的綁定的資訊。同樣地，在示例SSO框架中，判定訊息可提供認證強度或置信等級（例如低、中、高、非常高）。例如，在判定訊息中的低認證強度可指明OP 612對判定的識別碼具有很少或沒有置信度（例如具有用於密碼格式的最少規則的用戶名/密碼的自動插入）；中認證強度可指明OP 612對判定的識別碼有一些置信度（例如具有應用於密碼格式的規則的用戶名/密碼的手動使用）；判定訊息中的高認證強度可指明OP 612對判定的識別碼有高等級的置信度（例如生物特徵或加密網路存取訊標和用戶名/密碼的使用）；以及非常高認證強度可指明OP 612對判定的識別碼具有非常高等級的置信度（例如生物特徵和加密訊標）。在示例實施例中，“低”和“中”等級可指明僅使用了用戶證書，而“高”和“非常高”等級可要求網路輔助互動發生、並且可要求諸如生物特徵和密碼這樣的較強形式的認證。

再次參考第5圖，第5圖闡明了可用於網路控制的引導和

密鑰建立的示例SSO技術（認證協定）。例如，OpenID/ISIM 514和OpenID/AKA 516可以是基於UICC、並且可利用可安全駐留在UICC上的、諸如與網路共享的密鑰這樣的證書。例如取決於與網路共享的證書，OpenID/GBA 212可以是基於或不基於UICC。在示例框架中，OpenID/SIP摘錄508可以是不基於UICC。例如，可使提供OpenID識別碼和密碼的傳統用戶適應。SSO子系統的網路認證介面可允許各種SSO認證協定（例如第5圖中的模組508、510、512、514、516）在單一架構框架中適應。

在示例SSO框架中，用戶可使用兩種認證類型綁定來被驗證。雖然用戶驗證可參考OpenID協定來描述，但相同的概念可被應用於其他認證協定，例如自由聯盟。例如，一旦UE通電，用戶輔助認證可發生。例如，用戶可提供用戶輔助認證證書（例如PIN、生物特徵）來獲取對裝置功能的存取。例如，用戶可提供PIN以獲得對iPhone的存取。這樣的認證機制可在供電時提供一次或者貫穿對話間斷地提供。認證用戶的頻率要求可以是策略驅動的。SSO子系統可驗證用戶提供的PIN、並可以判定的形式儲存結果，從而確認PIN已被輸入並被驗證。這樣的判定可建立用戶輔助認證。在用戶輔助認證被建立後，用戶可經由將網頁瀏覽器定向到RP網頁來嘗試登錄例如可支援OpenID協定的服務供應者（例如RP）。SSO子系統可檢查用戶輔助認證的狀態，並且如果該狀態是有效的，則可將用戶識別碼提供給RP。RP可執行OpenID提供者（OP）的發現，並且這兩個實體可建立關聯。這樣的關聯

可產生共享密鑰。裝置可被重新定向到LAE，LAE可以是在UE本地的、可由SSO子系統執行的OpenID代理功能。在示例實施例中，由SSO執行的策略（例如外部事件相關者的）可要求執行強網路輔助認證（例如GBA、EAP、AKA）。認證模組（例如SSO認證協定及/或證書）可被選取。這樣的選取可由例如在認證協定中的SSO子系統報告給MNO。UE的認證可使用選取的網路輔助認證模組（例如SSO認證協定）來執行。在示例實施例中，選取的認證協定可引起網路輔助認證功能和UE之間共享應用特定密鑰的引導。這樣的密鑰可被用來認證UE。

UE可接收認證完成的指示，並且LAE可簽名至RP的判定訊息(指明強認證已發生)。該判定可指明用戶輔助認證（例如經由初始用戶PIN輸入）和後續的網路輔助認證（例如經由選取的SSO認證協定）之間的綁定。該判定可指明在此描述的認證置信等級中的一者。可使用經由本地SSO代理（例如LAE）和RP之間的關聯建立的密鑰來簽名該判定訊息。RP和LAE可不直接通信，因此OP服務功能（OPSF）可在網路上被創建以便於這兩個實體間的通信。OPSF可以是由就像該功能是OP那樣可與其進行通信的RP以經由公共網際網路可達到的。本地SSO（LAE）代理可經由OPSF密鑰分佈機制來獲得關聯密鑰。OPSF也可根據源於LAE的經簽名的判定來為RP支援簽名驗證。然後，可將用戶無縫地定向到RP網頁。在示例框架中，當用戶隨後希望存取不同的服務供應者時，SSO子系統可檢查用戶輔助認證結果是否已儲存，以及認證是否還有效（例如根據本地儲存的策略）。例如，如果存在有效儲存的結

果，SSO子系統這時可不執行用戶輔助認證。新的服務供應者然後可如在此描述那樣執行識別碼提供者的發現。因此，用戶可存取新的服務供應者，而不用在UE處輸入證書，並且用戶可不被涉及網路輔助認證。根據一個實施例，這樣的場景可構成完全SSO實現。

在示例框架中，用戶可經由偏愛服務及/或應用的註冊來存取偏愛的（例如附屬的）服務。例如，網頁或其他線上應用服務供應者（例如信賴方）可使用服務提供者的選擇的IdP來註冊到基於操作者網路的SSO系統。例如，支付交易供應者可使用OpenID來從特定的IdP獲得授權的認證，這可使支付交易供應者成為附屬的服務。該註冊可由服務供應者（例如RP）、選取的IdP、操作者的SSO系統或服務的終端用戶來發起。另外，該註冊可由存取網頁的用戶或駐留UE的SSO子系統來發起。例如，駐留在UE上的SSO子系統可變得“同步”於基於網路的SSO子系統的資料庫，從而可獲知註冊的、附屬的服務和應用的列表和類型。

可允許RP選取IdP而不顯式地選取SSO認證協定及/或證書。例如，在IdP和將使用的SSO認證協定的選取之間可存在隱式關聯。例如，RP可選擇特定的IdP，因為該IdP可支援諸如OpenID這樣的特定SSO認證協定。

用戶然後可藉由使用UE來存取SSO（例如OpenID）支援的基於網頁的應用服務。UE駐留的SSO子系統可遵從操作者規定的策略、並且可選取註冊的附屬服務/應用及/或偏愛服務/應用。在用戶指明（例如藉由鍵入URL）他或她的偏愛服務後，UE駐留的SSO子系統也可截取（阻礙）

並轉換或替代用戶鍵入的URL為與相同服務的註冊、附屬版本對應的可選服務的URL。這樣的替換服務可由相同的但是可以藉由優先、附屬的基礎呈現和存取的供應者來提供。例如，存取可被限於由與前述服務/應用有前述基於註冊的從屬關係的操作者（例如可提供這樣的服務/應用的IdP和RP）服務的UE的用戶。

根據示例SSO框架，在選取服務/應用後，UE可以透明的及/或無縫的方式以代表用戶來選取偏愛的存取網路輔助認證機制及/或適當的證書。例如，UE可在SSO認證協定中指示選取的存取網路輔助認證機制。網路可識別該選取的偏愛存取網路輔助認證機制、並且可認證用戶。一旦成功認證，剩餘的SSO操作（例如UE重新定向到RP以獲得服務）可發生。

如在此描述的那樣，藉由用操作者的SSO系統而連接到操作者的可信基礎設施，訂閱的附屬服務可有效地獲得由操作者提供的網路輔助認證強度。

更一般地，在此描述的SSO架構可被視為合併了更多形式化功能層次。例如，SSO子系統可管理一個或多個SSO用戶端（例如或本地SSO代理）。如果基礎裝置技術支援多服務供應者配置，那麼大量的SSO用戶端可作為SSO子系統內多服務管理器的子功能運行。該通用架構可提供用來支援具有潛在獨立策略的多個服務的分離。

在這樣的框架中的每個SSO用戶端可管理若干從屬子功能。例如，本地判定子功能可由本地判定實體（LAE）來執行。LAE可涉及執行本地判定的子功能的正式名稱（formal designation）。例如，取決於該實現，一個

或多個LAE可由一個SSO用戶端控制。例如，該配置可涉及SSO用戶端-LAE對（一對一）或一個用戶端控制多個LAE。在任何配置中，SSO用戶端可以是控制實體。在此，SSO認證協定也可被稱為SSO技術。例如，SSO用戶端可控制由選取的SSO認證協定執行的機制的處理。SSO用戶端可管理可確定可使用哪個認證方法的策略執行動作。例如，應用的策略可在諸如MNO這樣的外部事件相關者的控制之下。

根據另一個示例框架，UE可支援作為多服務管理器中子功能運行的多個SSO用戶端的實現。這樣的實現可被視為在不同服務供應者可能需要分離、孤立的SSO用戶端專門地服務該特定供應者，而允許多個可用連接技術的基於策略的管理和由相同供應者同時提供的服務的環境中的功能。例如，ME可具有SSO用戶端A和SSO用戶端B，並且這些SSO用戶端中的每一個可被分離地且互相孤立地來控制。SSO方面可特定於供應者。

與多個SSO用戶端一起，可存在大量的LAE。例如，每個LAE可被實現在UE上的存取技術特定的域中。由於SSO用戶端孤立，可在每孤立的域存在一個LAE。同樣地，例如，根據由該裝置所支援的可用存取技術可構造LAE。相同的存取技術可在不同的LAE間多工，或者不同的存取技術可由LAE同時使用。因此，UE可支援多個LAE。取決於該實現，例如，LAE和SSO用戶端之間的關係可以是一對一或一個SSO用戶端可控制或由多個LAE服務。

如在此描述那樣，在SSO子系統中執行的功能可以各種方式來配置。在UE中，例如，在基於UICC和不基於UICC（

或者替代地安全環境）的架構之間可存在界限（division）。還可劃分UE和MNO網路之間的功能。以下是根據各種實施例的一些可能的配置。

加密AKA功能可駐留在非UICC智慧卡上。這樣的功能可在諸如G&D的MSC這樣的完全可編程的非UICC智慧卡上執行、並且可類似於網路輔助認證（例如AKA），但是該卡可以是可移除的並且在用戶的控制之下。加密功能可駐留在UICC上。這樣的功能可包括在UICC上實現的LAE的基本加密功能，例如密鑰推導和判定簽名。該功能可類似於網路輔助認證（AKA）。並且，可實現到IMSI的綁定和與MNO的用戶註冊。

根據示例SSO框架，LAE功能可駐留在UICC或安全可信環境中。例如，LAE可以是在智慧卡網頁伺服器（SCWS）或其他網頁瀏覽器應用上的OpenID的完全實現。在示例實施例中，網路輔助認證配置可以是為了將LAE（例如本地判定）認證綁定到任何形式的強網路輔助認證（例如本地OpenID/GBA）。強認證可作為附加因素以藉由增加生物特徵或類似的本地認證而應用於強本地用戶輔助認證。例如，任何形式的強本地認證可與網路輔助認證結合和綁定。

在SSO框架中的選取/協商

如此這般描述了示例性SSO框架後，現在將描述在這樣的示例性SSO框架中用於選取和協商各種認證協定的方法和系統的實施例。

第7和8圖闡明了可由在第5圖中示出的SSO框架實現的示例協商和選取。例如，在屬於用戶的UE與單點登錄（SSO

）識別碼提供者（IdP）通信時，可以協商和選取特定的認證協定或特定的證書。一個示例實施例使用OpenID 2.0協定，可在http://openid.net/specs/openid-authentication-2_0.html獲得。例如，協商和選取可利用諸如OpenID提供者授權策略擴展（PAPE）和基於HTTP的認證這樣的標準化協定及/或工具。PAPE在可在http://openid.net/specs/openid-provider-authentication-policy-extension-1_0-01.html獲得的OpenID提供者認證策略交換（PAPE）中描述。基於HTTP的認證在可在http://www.ietf.org/rfc/rfc2616.txt獲得的IETF RFC 2616——超文本傳輸協定HTTP/1.1中、在可在http://www.ietf.org/rfc/rfc2617.txt獲得的IETF RFC 2617——HTTP認證：基礎和摘錄存取認證中以及在可在http://www.ietf.org/rfc/rfc3310.txt獲得的IETF RFC 3310——使用認證和密鑰協商（AKA）的超文本傳輸協定（HTTP）摘錄認證中描述。在IdP由行動網路操作者（MNO）控制時，可以使用附加的機制，例如以最終獲得到諸如RP這樣的網頁服務供應者的存取。

諸如PAPE擴展這樣的OpenID擴展的使用可包括OpenID協定的現有、過去和將來的版本。雖然在此描述的示例實施例集中在基於OpenID的認證流上，但實施例並不這樣受限，並且可使用任何形式的SSO或IdP模式，例如自由聯盟、開放式驗證（OAuth）等。

基於HTTP的認證可在各種實施例中使用。在示例實施例中，可以無需諸如本地OP或本地SSO子系統這樣的本地實

體而實施UE認證。在可選實施例中，SSO IdP的功能可在基於網路的一個（或多個）伺服器和駐留在或連結於UE的本地實體間劃分。

在示例實施例中，IdP可使用可從MNO訂閱蜂巢/無線網路存取服務的裝置（UE）代表諸如信賴方（RP）這樣的網頁服務供應者來監督及/或促進用於用戶的SSO用戶認證協定及/或證書的自動選取。例如，IdP可由行動網路操作者（MNO）來控制（例如MNO/IdP）。在示例實施例中，認證可經由OpenID協定來執行。在這樣的實施例中，IdP可包括OpenID提供者（OP），並且MNO控制的IdP可包括由MNO控制的OP（MNO/OP）。在示例實施例中，OP可根據用戶認證（例如經由PAPE訊息）來接收RP的要求及/或偏好。在另一個示例實施例中，OP可識別特定的RP並從資料庫獲得該RP的要求及/或偏好。這樣的RP要求及/或偏好可與要求及/或偏愛的用戶認證協定、特性及/或證書相關。在這樣的實施例中，OP可識別特定的RP並獲得該RP的要求及/或偏好，而不與RP交換用於這樣的資訊的顯式訊息。

如在此所述那樣，服務供應者（例如RP）和諸如例如OP這樣的認證端點（AEP）可管理細粒度的協商以選取用於認證用戶及/或UE的認證協定及/或證書。作為對高級策略的擴展，RP和OP可協商及/或提供在OpenID範圍內的要求或偏愛的認證協定（或認證協定的特性）的指示。在示例實施例中，OP可使用其自己的策略來預先選取及/或確定從UE請求哪個認證協定。在另一個示例實施例中，UE可使用由MNO/OP所配置的策略來選取及/或確定使

用哪個認證協定、並且可相應地回應於MNO/OP。例如，OP可在預先配置的時間訊框中發送多個請求認證的訊息，並且UE可基於儲存的策略來選取認證協定。策略可以是基於一個標準或各種標準（例如OP最偏愛的、最安全的、最小OTA流量、最小電池消耗等）。在示例實施例中，OP及/或服務供應者（例如RP）可定義其自己的策略、並且可指明（以信號發送）其細粒度認證協定選取偏好。

第7圖闡明了用於協商和選取用戶認證協定及/或證書的協定流的示例實施例。第7圖闡明了OpenID SSO，雖然實施例不如此受限。例如，OpenID供應者（OP）702（例如網頁伺服器）可被稱為認證端點（AEP）、並且可由其他識別碼提供者來實現，RP 704（例如應用伺服器）可由與各種協定一致的其他服務供應者來實現。

參考第7圖，用戶（例如UE 700）可在706嘗試登錄RP 704。例如，用戶可瀏覽RP 704、並且可向RP 704提供他的OpenID識別符。在708，RP 704例如可基於策略及/或基於用戶請求存取的服務來選取認證協定。例如，RP 704可確定（例如基於提供的OpenID識別符）RP可能要求及/或偏愛的一個或多個用戶認證協定及/或證書。在示例實施例中，RP 704可確定RP 704可能要求及/或偏愛的一般特性。一個或多個認證協定及/或證書可包括這樣的特性。在710，RP 704可發起OpenID協定，並且OP 702和RP 704可建立關聯。在712，RP可將UE 700重新定向到OP 702。在712，RP 704可經由諸如例如PAPE這樣的擴展來向UE 700發送用於期望的認證協定及/或證書

的請求。在714，UE 700可經由諸如PAPE這樣的擴展來向OP 702發送重新定向請求，該請求可包括期望的認證協定及/或證書。在716，RP 704和OP 702可協商期望的認證協定及/或證書是否可以實現。例如，OP 702和RP 704可根據諸如PAPE這樣的OpenID擴展來聯合確定期望的協定是否可以實現。例如，OP 702可提出（promote）哪些協定被支援，RP然後可要求支援的協定中的一者。在718，OP 702可與UE/用戶 700一起參與OpenID。

例如，在718，OP 702可質詢（challenge）UE 700以進行認證，並且該質詢可包括期望的認證協定及/或證書的指示。在720，UE 700和OP 702可協商認證協定及/或證書（例如經由HTTP標頭）。例如，OP 702及/或UE 700可確定UE是否支援期望的認證協定。在示例實施例中，OP 702可能知道UE 700支援哪些認證協定及/或證書。UE 700還可通知OP 702該UE支援哪些認證協定及/或證書。在722，UE 700例如使用聯合確定的（例如選取的）協定及/或證書來向OP 702認證其本身。UE 700可使用諸如例如OpenID/GBA或摘錄AKA認證這樣的各種協定來認證其本身。

在724，OP可判定識別碼、並使用經簽名的判定訊息（在726）將UE/用戶700重新定向回RP 704。該判定訊息可包括認證協定及/或證書、以及諸如例如上一次認證的時間等這樣的各種其他資訊。在728，RP 704可確定報告的（接收的）協定及/或證書是否匹配請求的（期望的）認證協定及/或證書，或者在OP 702和UE 700之間的協

定期間是否選取了另一個認證協定及/或證書。

在示例實施例中，用於協商和選取用戶認證協定及/或證書的協定流（第7圖中所示）可包括作為OP 702的MNO/OP。參考第7圖，用戶（例如UE 700）在706可嘗試登錄RP 704。例如，用戶可瀏覽RP 704、並且可向RP 704提供他的OpenID識別符。RP可發起與MNO/OP的OpenID協定。該RP可藉由使用PAPE來指明認證方法或其要求或偏愛的這樣的方法的特性。在708，RP 704可例如基於策略及/或基於用戶請求存取的服務來選取認證協定。例如，RP 704可確定（例如基於提供的OpenID識別符）RP可能要求及/或偏愛的一個或多個用戶認證協定及/或證書。在示例實施例中，RP 704可確定RP 704可能要求及/或偏愛的一般特性。一個或多個認證協定及/或證書可包括這樣的特性。

可選地，根據示例實施例，RP 704可不提供要求或偏愛的認證協定或特性的指示。例如，MNO/OP可獲取與認證協定/特性及/或證書對應的RP的特定要求及/或偏好。MNO/OP可從其可存取及/或其自己的資料庫獲取這樣的資訊。例如，MNO/OP可具有與RP的先驗關係（prior relationship）和RP的知識（例如藉由將RP登記到其資料庫）。MNO/OP可確定關於用於特定RP的認證協定/特性的特定要求及/或偏好，而無需從RP接收指示。

在716，RP 704和MNO/OP可協商RP的期望的（或偏愛的）認證協定及/或證書是否可實現。例如，MNO/OP和RP 704可根據諸如PAPE這樣的OpenID擴展來聯合確定期望的協定是否可實現。例如，MNO/OP可提出支援哪些協定

，並且RP然後可要求支援的協定中的一者。在718，MNO/OP可發起與UE/用戶700的OpenID認證。

例如，在720，UE 700和MNO/OP可協商認證協定及/或證書（例如經由HTTP標頭）。例如，MNO/OP及/或UE 700可協商以確定UE是否支援期望的認證協定。在這樣的協商中，UE可通知MNO/OP其支援哪些認證協定。在協商後，最後的認證協定可被選取。可控制協商和最後選取，使得MNO/OP的策略得以滿足。在示例實施例中，MNO/OP可能知道UE支援哪些認證協定及/或證書，及/或MNO/OP可指示其自己選取的認證。這樣的選取的認證協定及/或證書可根據MNO/OP的策略來選取。

在722，例如UE 700可使用協商的及/或選取的協定及/或證書來向MNO/OP認證其自己。UE 700可使用諸如例如OpenID/GBA或摘錄AKA認證這樣的各種協定來認證其自己。

在724，MNO/OP可判定識別碼並使用經簽名的判定訊息以將UE/用戶700重新定向回RP 704（在726）。MNO/OP可指明RP（例如經由PAPE）執行的認證協定及/或證書、以及諸如例如上一次認證的時間等這樣的附加資訊。在728，RP 704可確定經報告的（接收的）協定及/或證書是否匹配請求的（期望的）認證協定/特性及/或證書。例如，基於該確定，RP 704可確定是否授權UE 700存取請求的服務。例如，如果RP 704確定接收到的協定匹配期望的認證協定及/或包括期望的特性，RP 704可允許UE 700存取由RP 704提供的服務。

如在此描述的那樣，服務供應者（例如RP）和諸如例如

OP這樣的認證端點（AEP）可協商AEP和UE使用的認證協定及/或證書。例如，充當RP的銀行（bank）可偏愛使用強認證協定。服務供應者可基於各種確定來選取認證協定。

例如，如果OP具有與RP的先驗關係及/或RP的知識（例如藉由將RP登記到其資料庫），OP可能已經知道與特定RP對應的用於認證協定/特性的特定要求/偏好。OP可從其擁有及/或其可存取的資料庫獲取這樣的資訊。在這樣的實施例中，其中OP具有RP的先驗知識（prior knowledge），RP和OP可確定認證而無需互相協商。在可選的實施例中，OP可經由從資料庫獲取、經由直接的（例如經排程的）與RP聯繫帶外更新資料庫資訊或其組合來獲取與RP的要求及/或偏好相關聯的資訊。

在其中AEP是由MNO運行的OP（MNO/OP）的示例實施例中，MNO可具有與可由裝置及/或用戶支援的特定認證協定及/或證書相關聯的知識。在示例實施例中，MNO可向RP公佈每個用戶可支援的特定認證協定及/或證書。這樣的公告可允許RP在期望的認證協定及/或證書上做出細粒度的決策。在示例實施例中，服務供應者（例如RP）可代替指定期望的認證協定來提供期望的高等級策略配置檔。在這樣的實施例中，MNO/OP可選取可獲得的最強的認證協定及/或證書。例如，MNO/OP可使用GBA_U替代GBA_ME。可選地，MNO/OP可基於例如環境及/或可能要求使用較低強度認證協定的附加策略來選取較低強度的認證協定。例如，可影響認證協定選取的策略參數包括諸如例如電池狀態、信號狀態、裝置的漫遊狀態、裝置

的位置等這樣的參數。在其中MNO不使用最強認證協定的實施例中，MNO可在例如判定訊息中向RP信號發送認證協定。

在服務供應者（例如RP）和AEP（例如OP）協商期間，或在AEP從AEP可存取的資料庫獲取服務供應者的要求及/或偏好資訊期間，關於用戶認證的要求或偏好資訊可經由特定認證協定（例如OpenID/SIP摘錄、OpenID/GBA等）的指示及/或經由顯著特性（broad characteristics）的指示來提供。可能要求及/或偏愛將這樣的特性作為特定認證協定及/或證書的一部分來包括。例如，特性可指明認證證書應當是最少128位元強及/或被保護在防篡改環境中。根據示例實施例，多因素認證可作為認證協定的特性。在其中認證要求或偏好可根據特性來指定的示例實施例中，OP在獲取（例如，經由OP-RP協商或經由資料庫獲取）要求或偏愛的“用戶認證的特性”後，可將指定的特性轉換為特定支援的認證協定及/或證書的選取。

OP和UE可對使用的認證協定及/或證書達成一致。在示例實施例中，用戶可已向OP（例如MNO）註冊OpenID識別符，OP可知道（例如，基於在發現和關聯期間從RP接收的用戶的OpenID識別符）哪個用戶可認證。在這樣的實施例中，MNO可查找關於與給定用戶對應的支援的認證協定及/或證書的資訊。例如，基於在其中認證證書可被賦能的登記（例如使用BSF的引導可在GBA實現中發生，SIP密碼可在SIP摘錄實現中創建），MNO可確定哪些認證協定及/或證書可由裝置支援、並且可相應地更新此資

訊。例如，所支援的認證協定及/或證書可儲存在OP處的資料庫中及/或在MNO處的資料庫（例如SSO子系統）中。這樣的資料庫可儲存用戶識別符和所支援的及/或賦能的認證協定及/或證書之間的映射。表1顯示了用於儲存認證協定的示例資料庫。OP可選取可最適合RP要求及/或偏好的認證協定。OP可使用可以是適當的並且可與選取的認證協定（例如適用於摘錄AKA、HTTP摘錄等）對應的認證請求來質詢UE。在示例實施例中，認證協定可以偏愛的優先性按順序列出，或者可包括偏愛使用順序列表。

表1

用戶 ID	認證協定	上一次登錄	…
openid.mno.com/joe	HTTP 摘錄 AKA、GBA、用戶名/密碼 …	10.20pm 03-05-2011	附加數據
openid.mno.com/jane	SIP 摘錄、用戶名/密碼	9.15am 03-05-2011	
…			

在示例實施例中，UE可經由在HTTP請求訊息中的標頭資訊來通知AEP（例如OP）支援的認證方法。這樣的標頭的一個示例可包括正文字串，例如“openid-gba”、“openid-aka”、“openid-sip-digest”、“openid-eap”等。例如，HTTP用戶代理標頭可被使用、並且可包括至NAF的支援GBA形式的指示。

認證協定協商可經由修改或無修改的工具和標準來實現。雖然在此的協商通常在OpenID環境下進行描述，但實施例並不這樣受限。例如，RP可涉及服務供應者的實施例，並且OP可涉及AEP的示例實施例。在此描述的協商可包括UE和RP、UE和OP及/或RP和OP之間的互動。

對OpenID的提供者認證策略交換（PAPE）擴展可使RP能夠在認證用戶時請求將由OP應用的特定認證策略。RP可

請求由OP應用的以前達成一致的認證策略。OP可通知RP曾使用什麼認證策略。

作為擴展，PAPE可不需要改變OpenID認證協定、並且可與各種OpenID認證版本一起使用，例如版本1.1和2.0。表2顯示了根據示例實施例的XRDS文件。如所示那樣，以粗體突出的部分指示支援PAPE擴展（防網路釣魚（phishing resistant））。在Yadis發現過程期間，OP在用戶的XRDS文件中公佈支援的認證策略。RP可從可用認證策略中的一者選取。藉由將策略添加為OpenID <xrd:Service>元素的<xrd:Type>元素的值，該策略可被公佈在XRDS文件中。

表2

```
<?xml version="1.0" encoding="UTF-8"?>
<xrds:XRDS
    xmlns:xrds="xri://$xrds"
    xmlns="xri://$xrd*($v*2.0)">
<XRD>

<Service priority="0">
<Type>http://specs.openid.net/auth/2.0/signon</Type>
<Type>http://openid.net/signon/1.0</Type>
<Type>http://schemas.openid.net/pape/policies/2007/06/phishing-resistant</Type>
<URI>http://openid.novalyst.de/openidserver</URI>
<LocalID>http://openid.novalyst.de/id/joe</LocalID>

</Service>

</XRD>
</xrds:XRDS>
```

可存在在PAPE中指定的預先定義的策略及/或策略識別符。在示例實施例中，RP可定義其自己的PAPE策略及/或策略識別符。例如，RP可藉由在其網站上公佈PAPE策略及/或策略識別符及/或藉由與單獨的OP的私有介面（例如頻道）來指明這樣的PAPE策略及/或策略識別符。例如包括期望的認證協定及/或證書的策略可由RP來定義。這樣的

策略可類似於MNO可定義的策略。在示例實施例中，RP可將策略定義上傳給其自己的URL（例如www.example.com/policies/policy1）。在上傳後，RP可在PAPE請求中包括該URL（到自定義的策略）。在示例實施例中，RP可顯式地指明策略要求及/或偏好。例如，RP可經由使用PAPE以每一對話為基礎來指明策略要求及/或偏好。在可選的實施例中，策略要求及/或偏好可與RP與其具有關係的OP共享，並且OP可維護一個或多個資料庫來記錄這樣的策略要求及/或策略偏好。與多個RP相關聯的多個策略識別符（ID）可被儲存在這樣的資料庫中，並且與多個RP相關聯的策略資訊可被儲存並且可經由資料查找來獲取。RP和OP可理解策略和策略識別符、並且具有以前達成一致的策略。表3列出了可在PAPE中定義的示例策略。

表3

名稱	策略識別符	策略描述
防網路釣魚認證	http://schemas.openid.net/pape/policies/2007/06/phishing-resistant	其中端用戶不向潛在地在信賴方的控制下的一方提供共享密鑰的認證機制。(注意，潛在惡意信賴方控制用戶代理被重新定向的地方，且因此可能不將其發送給端用戶真實的 OpenID 提供者)。
多因素認證	http://schemas.openid.net/pape/policies/2007/06/multi-factor	其中端用戶藉由提供多於一個認證因素來向 OpenID 提供者進行認證的認證機制。通用的認證因素可以是你知道的、你有的和你是的。一個示例可以是使用密碼和軟體訊標或數位證書的認證。
實體多因素認證	http://schemas.openid.net/pape/policies/2007/06/multi-factor-physical	其中端用戶藉由提供多於一個認證因素來向 OpenID 提供者進行認證的認證機制，其中這些因素的至少一個是諸如硬體裝置或生物特徵這樣的實體因素。通用的認證因素可以是你知道的、你有的和你是的。一個示例可以是使用密碼和硬體訊標的認證。

根據示例實施例，包括用於用戶認證的特定和細粒度要求的策略配置檔可被定義。表4包括示例協定的定義和分類的示例。例如，如果OP由MNO操作，則OP可具有到行動網路和裝置特定認證機制（例如，諸如GBA來認證UE）、

及/或能夠從安全記憶體獲取和採用證書（例如，以本地認證用戶）的瀏覽器（或非瀏覽器）應用和用戶端的存取。

表4

協定	用戶認證	裝置（UE）認證	手動認證	認證強度
GBA 摘錄	X		X	中
GBA (GBA_U, GBA_ME)		X	X	高
EAP-SIM		X	X	高
EAP-AKA, EAP-AKA'		X	X	高

表5顯示了根據示例實施例的用於策略配置檔的認證協定的示例分類（特性）。

表5

協定	防網路釣魚	多因素	實體多因素
經由 HTTP 的密碼			
經由 HTTP 的 PIN 和數位證書	X	X	
經由 HTTP 的 PIN 和“軟”OTP 訊標	X	X	
經由 HTTP 的 PIN 和“硬”OTP 訊標	X	X	X
經由 HTTP 的 PIN 和“硬”加密訊標	X	X	X

在示例實施例中，RP可在OpenID認證請求中包括認證協定及/或證書的偏好，例如藉由在該請求中包括附加參數。這樣的參數的示例在表7中示出。RP可請求最後啟動的用戶認證在指定時間訊框內（例如在與運行的目前認證協定相關的若干秒數內）發生。表6根據示例實施例提供了請求參數及其在PAPE中由RP使用的示例概覽。

表6

名稱	值
openid.ns.pape	如果將使用 PAPE 則需要“http://specs.openid.net/extensions/pape/1.0”
openid.pape.max_auth_age	如果端用戶在以符合請求的策略的方式指定的秒數內沒有主動向 OP 進行認證，OP 可針對該請求認證端用戶。 值：以秒為單位的大於或等於零的數值。 OP 應當認識到不堅持（adhering to）用於重新認證的請求最可能意味著端用戶將不被允許存取由 RP 提供的服務。

Openid.pape.preferred_auth_policies	OP 在認證用戶時可遵循的零個或更多個認證策略 URI。如果請求了多個策略，OP 將要嘗試盡力滿足盡可能多的。如果沒有請求策略，RP 對諸如認證壽命（age）這樣的其他資訊感興趣。 值：認證策略 URI 的空間分離的列表

表7包括根據示例實施例的附加（例如，除在表6中示出的示例請求參數之外的）示例請求參數。

表7

名稱	值
openid.pape.last_auth_time	（可選的）如果端用戶在從以符合請求的策略的方式指定的時間以來沒有主動向 OP 進行認證，OP 認證與該請求參數相關聯的端用戶。 值：上次認證的時間。 OP 可認識到不堅持用於重新認證的請求最可能意味著端用戶將不被允許存取由 RP 提供的服務。
Openid.pape.max_auth_age_by_device	（可選的）如果端用戶在秒數內或可選地在從以符合請求的策略的方式指定的時間以來沒有主動藉由使用者設備被認證，OP 認證與該請求相關聯的端用戶。 值：以秒為單位的或可選地以認證的時間為單位的大於或等於零的數值。 OP 應當認識到不堅持用於重新認證的請求最可能意味著端用戶將不被允許存取由 RP 提供的服務。

在示例實施例中，用於在指定嘗試次數內認證的請求可被包括在PAPE的擴展中。如在此所述的，OP可從RP接收用戶認證要求及/或偏好策略資訊。OP的認證回應可包括關於例如在其自己和用戶/UE之間採用的認證協定的資訊。該認證回應可在用戶認證後被發送給RP。OP可傳遞與被應用的認證策略相關聯的資訊。例如，新鮮度資訊（例如用戶上次被認證的時間）和關於認證強度的資訊（例如NIST保證等級）可以被傳遞。諸如例如指明在兩次最近成功的認證之間的嘗試次數的參數這樣的附加參數可被擴展在PAPE協定中。表8顯示了根據示例實施例的在PAPE中的示例OP回應參數。

表 8

名稱	值
openid.ns.pape	如果使用 PAPE 則需要 "http://specs.openid.net/extensions/pape/1.0"
openid.pape.auth_policies	OP 在認證端用戶時可遵循的一個或多個認證策略 URI。該參數可包括認證策略 URI 的空間分離的列表。 示例： openid.pape.auth_policies= http://schemas.openid.net/pape/policies/2007/06/multi-factor http://schemas.openid.net/pape/policies/2007/06/multi-factor-physical http://www.3gpp.org/auth-specs/multi-factor-physical-gba-u 以上示例可讓 RP 知道 GBA UICC 已被用於認證，其可實現多因素實體認證的性質（例如其是多因素認證）。在示例實施例中，如果沒有策略被滿足並且 OP 希望在回應中傳遞其他資訊，該參數可被包括有空值。
openid.pape.auth_time	端用戶以符合判定策略的方式主動向 OP 進行認證時的最近時間戳。 值：該時間戳可如在[RFC3339]的 5.6 節規定的那樣被格式化，並且可根據在用 "Z" 指示的 UTC 時間區域中的以下限制來格式化。根據示例，時間可不包括小數秒（fractional second）。
openid.pape.auth_level.ns.<cust>	用於由諸如國家或行業特定標準機構這樣的各種機構或者其他組織或個人定義的客戶（custom）保證等級的名稱空間。 值：表示該保證等級的 URL。
openid.pape.auth_level.<cust>	如由以上標準機構、組織或個人定義的保證等級對應於由 OP 在認證端用戶時採用的認證協定和策略。客戶保證等級定義可定義在其名稱空間內表示的附加子參數值，雖然為了簡潔的原因，這可被避免。 值：根據該保證等級定義的字串。

RP可確定（例如基於從OP接收的資料）用於登錄的要求是否滿足。基於該確定（例如，如果登錄要求被滿足），RP可授權對服務的存取。在示例實施例中，如果RP確定要求沒有被滿足，RP可拒絕對服務的存取。確定用於登錄的要求是否被滿足的方式可具體根據RP的需要來實現。

在示例實施例中，行動網路可定義行動網路特定策略。例如，行動網路特定策略可允許認證性質及/或特性的細粒度定義。表9列出了根據示例實施例的示例策略名稱、

識別符和描述。這樣的策略可經由PAPE來實現。

表9

名稱	策略識別符	策略描述
多因素認證—cert	http://schemas.openid.net/pape/policies/2007/06/multi-factor-cert	其中端用戶可藉由提供認證因素，例如使用安全儲存在使用者設備上的證書，來向OpenID提供者進行認證的認證機制。
實體多因素認證—GBA	http://www.3gpp.org/auth-specs/multi-factor-physical-gba-u	其中端用戶可藉由提供多於一個認證因素來向OpenID提供者進行認證的認證機制。例如，使用密碼和在使用GBA-U的行動電話上的UICC中的證書的認證。
實體多因素認證—GBA	http://www.3gpp.org/auth-specs/multi-factor-physical-gba-me	其中端用戶可藉由提供認證因素來向OpenID提供者進行認證的認證機制。例如，使用密碼和在使用GBA-ME的行動電話上的UICC中的證書的認證。
實體多因素認證—EAP-SIM	http://www.3gpp.org/auth-specs/multi-factor-physical-eap-sim	其中端用戶可藉由提供認證因素來向OpenID提供者進行認證的認證機制。例如，使用密碼和在使用EAP-SIM的行動電話上的SIM卡中的證書的認證。
實體多因素認證—ISIM	http://www.3gpp.org/auth-specs/multi-factor-physical-isim	其中端用戶可藉由提供認證因素來向OpenID提供者進行認證的認證機制。例如，使用密碼和在行動電話上的UICC上的ISIM功能中的證書的認證。

分離的策略的不同之處可在於不同的認證協定及/或證書可由行動裝置（UE）及/或行動網路來提供。在另一個示例實施例中，前述認證協定（例如在表9中涉及的）可被定義為客戶保證等級名稱空間。由於在表9中的示例行動網路特定策略定義較大策略中的一者的特性（例如其落入多因素或實體多因素認證的集合），對於要求多因素或實體多因素認證的標準化配置檔和定義包括例如關於諸如GBA、AKA、EAP-SIM等這樣的協定是否已被用作實際的基礎認證協定的細節的客戶保證等級名稱空間是足夠的。例如，客戶保證等級名稱空間可被定義為http://3gpp.org/auth/types。在這樣的定義中，根據示例實施例，實際的認證變數的細節可如在表10中描述的那樣來定義。

表 10

認證等級	描述
cert	依靠安全儲存在使用者設備上的證書的認證
gba-u	使用在使用 GBA_U 的行動電話上的 UICC 中的證書的認證
gba-me	使用在使用 GBA_ME 的行動電話上的 UICC 中的證書的認證
eap-sim	使用在使用 EAP-SIM 的行動電話上的 SIM 卡中的證書的認證
eap-aka	使用在使用 EAP-AKA 的行動電話上的 SIM 卡中的證書的認證
isim	使用在行動電話上的 UICC 上的 ISIM 功能中的證書的認證

OP可藉由公佈用於其用戶的XRDS文件來公佈支援名稱空間，例如：

```
<xrd>
<Service>
<Type>http://specs.openid.net/auth/2.0/signon</Type>
<Type>
  http://3gpp.org/auth/types
</Type>
<Type>
  http://schemas.openid.net/pape/policies/2007/06/multi-factor
</Type>
<Type>
  http://schemas.openid.net/pape/policies/2007/06/multi-factor-physical
</Type>
<URI>https://example.com/server</URI>
</Service>
</xrd>
```

在公佈支援名稱空間後，RP可請求使用特定保證等級來應用多因素認證策略。例如，這樣的請求可經由如表11所示的那樣設置參數來實現。

表 11

參數	值
openid.ns.pape	http://specs.openid.net/extensions/pape/1.0
openid.pape.max_auth_age	自最後一次認證以來的最大可接受秒數
openid.pape.preferred_auth_policies	http://schemas.openid.net/pape/policies/2007/06/multi-factor-physical （例如為了請求實體多因素認證）
openid.pape.auth_level.ns.3gpp	http://3gpp.org/auth/types （例如為了請求使用 3GPP 名稱空間）
openid.pape.preferred_auth_level_types	3gpp

在成功的用戶認證後，OP可報告（例如在回應訊息中）可能已經使用的認證等級。例如，表12示出了可指示GBA-U得以使用的參數的示例。

表 12

參數	值
openid.ns.pape	http://specs.openid.net/extensions/pape/1.0
openid.pape.auth_policies	http://schemas.openid.net/pape/policies/2007/06/multi-factor-physical 為了請求實體多因素認證
openid.pape.auth_time	最近認證的時間戳
openid.pape.auth_level.ns.3gpp	http://3gpp.org/auth/types 為了信號發送 3GPP 名稱空間的使用
openid.pape.auth_level.3gpp	gba-u 為了信號發送 GBA-U 已被用作基礎認證機制

AEP（例如OP）和UE可使用HTTP標頭來選取認證協定及/或證書。例如，OP可選取UE/用戶可使用的特定認證協定。對於基於HTTP的認證機制（例如HTTP基礎認證和摘錄認證、SIP摘錄和摘錄AKA），可使用具有回應碼“401未授權”的HTTP訊息來請求認證。WWW認證標頭可以信號發送將被使用的認證協定。WWW認證可包括認證質詢和諸如例如領域（其可允許向用戶顯示使用哪個用戶名）、指定保護空間的域、將使用的演算法等這樣的附加資訊。認證質詢可能需要的參數可包括在從OP到UE的401 HTTP回應中，如在IETF RFC 2617的3.2.1節中所描述的。

在其中HTTP摘錄AKA可實現的示例實施例中，用戶端可被指向使用AKA用於認證而替代標準用戶名/密碼系統。例如，摘錄認證的演算法指令（directive）（在例如RFC 2617中所描述的）可經由設置演算法= AKAv1-MD5來重寫（例如在IETF RFC 3310的3.1節中所描述的）。為了傳輸附加的AKA特定認證質詢參數，RFC 2617的現時（nonce）指令可藉由將其設定為AKA認證質詢RAND、AKA AUTN訊標及/或一些伺服器特定資料（例如在IETF RFC 3310的3.2節中所描述的）的串聯的Base64編碼來

擴展。

表13顯示了攜帶401未授權訊息的示例伺服器回應。OP伺服器可在單一的HTTP 401認證訊息中發送多個質詢，並且每個質詢可使用不同的認證方案（例如在RFC 2617的4.6節中所描述的）。這允許協商，例如因為OP伺服器可指明多個認證方案，並且UE用戶端然後可選擇在用戶端側支援的方案，例如最強認證方案（例如在RFC 2617的4.6節中所描述的）。HTTP訊息可允許在來自伺服器的訊息中呈現的多個WWW認證質詢（例如在相同的WWW認證標頭中或經由在相同回應中的多個WWW認證標頭）。例如，OP可在一個訊息標頭或藉由使用多個標頭以在單一的訊息中發送多個質詢。根據示例實施例，多個質詢可使用認證協定識別符來發送。例如，來自伺服器的多標頭回應可包括WWW認證：3gpp-gba-uicc、WWW認證：3gpp-gba-me、WWW認證：3gpp-aka和WWW認證：sip-digest。在示例實施例中，來自伺服器的單一標頭回應可包括WWW認證：3gpp-gba-uicc、3gpp-gba-me和sip-digest。攜帶401未授權訊息的伺服器回應的示例在表13中示出。

表 13

```
HTTP/1.1 401 Unauthorized
WWW-Authenticate: Digest
        realm="testrealm@host.com",
        qop="auth,auth-int",
        nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093",
        opaque="5ccc069c403ebaf9f0171e9517f40e41"
```

OP例如可藉由設計（shape）其可發送給UE的請求來影響UE可選取哪個認證協定。例如，基於其自己的UE認證能力的記錄的資料庫，OP可知道或猜想UE可能能夠支援

特定的不同認證。MNO可查找其自己的關於如何選取認證協定的策略、並可發送可包括用於選取認證協定的請求的HTTP 401認證訊息。OP可採用策略，由此其從多個可能的認證協定中選取最安全的認證協定。可選地，OP的策略可要求可最小化空氣下載（over the air）流量及/或（例如，佔用OTA頻道的）時間、最小化延遲或潛時、最小化電池功率消耗或這些及/或其他最佳化因素的任何組合的用戶認證協定的選取。表4和5顯示了因素的示例。

在根據示例實施例的OP-UE認證中，UE及/或UE的瀏覽器代理可偵測其是否可支援可由OP要求的認證協定。例如，UE可指明這樣的偵測的結果、並且可支援要求的認證協定。如果在來自OP伺服器的401訊息中發送了多個認證協定，UE例如作為用戶端可選取適當的認證協定。例如，適當的認證協定可以是提供最強等級認證的認證協定。

例如，UE可包括訂閱也是MNO的特殊OP（MNO/OP）的電話。該MNO/OP可經由提供及/或遠端配置來配置UE。例如，MNO/OP可配置UE可如何選取認證協定。這樣的配置可支援由OP及/或RP偏愛的協定。

例如，UE可包括策略資訊。這樣的策略資訊可控制UE如何答覆來自MNO/OP的多個可能的HTTP 401認證訊息。這樣的訊息的每一個可包括對認證的請求，例如使用特定用戶認證協定。例如，這樣的UE配置策略可命令UE在其獲得用於SSO認證的HTTP 401認證訊息時，等待預先配置長度的時間以在該指定的時間期間接收後續的HTTP

401認證訊息。每個後續的訊息可由其自己的SSO認證命令組成。UE可被進一步的命令以根據預先配置選取標準（例如“最安全”、“最小OTA流量”、“最小電池消耗”等）在多個所接收的HTTP 401認證訊息中被指出的多個協定中選取認證協定。

預先配置策略的示例可以是UE答覆包括UE可支援的認證協定的請求的第一個HTTP 401認證訊息。預先配置策略的另一個示例可以是UE將HTTP 401認證訊息看作以優先性為順序的偏愛的認證協定的列表，並且UE可被命令以開始從第一個到最後一個的檢查，當到達其支援的認證協定時停止，並且然後使用認證的該協定。另一個示例性預先配置策略可命令UE基於預先配置策略而無需認證協定的HTTP 401認證訊息列表來使用認證協定。

UE和MNO/OP之間的成功協商（例如達到可接受的認證協定）可使用智慧瀏覽器來實現。第8圖顯示了用於UE 800和MNO/OP 802之間的協商的示例訊息交換。例如，如果藉由使用多個訊息伺服器（MNO/OP）802和UE 800知道他們想協商，UE在804可請求站點。在806，UE 800可接收從伺服器返回的401（未經授權的）訊息，其中WWW認證標頭可包括用於首次提出的認證協定的首次質詢。在808，在來自UE 800的回應中，UE可向HTTP訊息的認證標頭增加資訊，例如以請求將被提出的不同的認證協定。在810，在回應中，伺服器可發送具有不同WWW認證標頭的另一個401，該另一個401可包括用於與UE的和RP的所請求的認證協定（812）匹配的認證協定的質詢。

參考第8圖，對認證請求的回應可使用HTTP請求來發送給

OP，其中認證標頭行可包括證書資訊。表14顯示了攜帶認證資訊的示例回應。

表 14

```
授權:
Digest username="Mufasa",
       realm="testrealm@host.com",
       nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093",
       uri="/dir/index.html",
       qop=auth,
       nc=00000001,
       cnonce="0a4f113b",
       response="6629fae49393a05397450978507c4ef1",
       opaque="5ccc069c403ebaf9f0171e9517f40e41"
```

在其中UE不能實現所請求的認證協定的示例實施例中，UE可如在例如RFC 2617的3.4節中所描述的“優雅地失敗（fail gracefully）”。在使用HTTP摘錄AKA的示例實施例中，可使用上述訊息。例如，當UE接收到摘錄AKA認證質詢時，UE可從“現時(nonce)”參數中擷取RAND和AUTN、並且可存取由伺服器提供的AUTN訊標。如果UE使用AUTN成功地認證了伺服器並確定用於產生該質詢的SQN在期望的範圍內，AKA演算法可使用RAND質詢和共享密鑰K來運行。當計算RFC 2617的回應指令時，產生的AKA RES參數可被作為“密碼”（例如在RFC 3310中所描述的）。

在瀏覽代理和計算AKA摘錄的智慧卡上的ISIM應用之間的通信在RFC 3310中未規定。例如，在HTTP摘錄AKA上建立的GBA在3GPP TS 33.220 v10.0.0的4.2.4節中總結這些功能。如所述的那樣，從UE要求的功能是：支援HTTP摘錄AKA協定、在引導中使用USIM和ISIM兩者的能力、當有USIM和ISIM兩者存在時選取將用於引導的USIM或ISIM的能力、ME上Ua應用指出在ME上GBA功能用於引

導的UICC應用的類型或名稱的能力（參見條款4.4.8）、從CK和IK以經由Ua介面導出將與協定一起使用的新密鑰材料的能力、支援NAF特定應用協定（例如參見TS 33.221）。

表15顯示了根據示例實施例的當使用HTTP摘錄AKA時協定步驟的示例。

表 15

1) 初始請求 REGISTER sip:home.mobile.biz SIP/2.0
2) 包括質詢的回應 SIP/2.0 401 Unauthorized WWW-Authenticate: Digest realm="RoamingUsers@mobile.biz", nonce="CjPk9mRqNuT25eRkajM09uTl9nM09uTl9nMz5OX25PZz==", qop="auth,auth-int", opaque="5ccc069c403ebaf9f0171e9517f40e41", algorithm=AKAv1-MD5
3) 包括證書的請求 REGISTER sip:home.mobile.biz SIP/2.0 Authorization: Digest username="jon.dough@mobile.biz", realm="RoamingUsers@mobile.biz", nonce="CjPk9mRqNuT25eRkajM09uTl9nM09uTl9nMz5OX25PZz==", uri="sip:home.mobile.biz", qop=auth-int, nc=00000001, cnonce="0a4f113b", response="6629fae49393a05397450978507c4ef1", opaque="5ccc069c403ebaf9f0171e9517f40e41"
4) 成功回應 SIP/2.0 200 OK Authentication-Info: qop=auth-int, rspauth="6629fae49393a05397450978507c4ef1", cnonce="0a4f113b", nc=00000001
在 AKA 同步失敗的情況下，伺服器在步驟 4 發送新的質詢： SIP/2.0 401 Unauthorized WWW-Authenticate: Digest realm="RoamingUsers@mobile.biz", qop="auth,auth-int", nonce="9uQzNPbk9jM05Pbl5Pbl5DIz9uTl9uTl9jM0NTHk9uXk==", opaque="dcd98b7102dd2f0e8b11d0f600bfb0c093", algorithm=AKAv1-MD5

在示例實施例中，在從UE到OP的HTTP請求中（例如在從RP到OP的重新定向中），UE可藉由使用GBA技術以向OP信號發送其能力（例如支援的認證協定及/或證書）。例

如，藉由將作為產品訊標的固定字串附加至請求中的用戶代理標頭上（如在RFC 2616中的3.8節和14.43節所規定的），UE可向OP傳遞資訊。在GBA中，UE可藉由例如附加用於基於UE的GBA的“3gpp-gba”或藉由附加用於基於UICC的GBA的“3gpp-gba-uicc”來與NAF進行通信（例如，在3GPP 33.222中的5.3節所描述的）。表16顯示了具有修改的用戶代理標頭的示例HTTP GET請求（HTTP 獲取請求）。

表 16

```
GET / HTTP/1.1
User-Agent: curl/7.19.7 (x86_64-pc-linux-gnu) 3gpp-gba-uicc
Host: example.com
Accept: */*
```

附加的產品訊標可被定義以藉由例如對用戶代理標頭附加定義的固定字串來將關於支援的認證協定的資訊從UE傳遞至OP。可為可支援多個認證協定的裝置連結多個字串。3GPP特定認證的示例固定字串可在諸如3GPP 33.222這樣的規範中定義。其他字串根據示例實施例進行定義。例如，表18顯示了示例字串。在可選實施例中，Prgama標頭可被用來將關於支援的認證協定的資訊從UE傳遞至OP。例如，Pragma標頭可由代理和閘道保持完整和未改變（例如參見RFC 2616，14.32節）。表17顯示了Pragma標頭的示例語法。

表 17

```
Pragma              = "Pragma" ":" 1#pragma-directive
pragma-directive    = "no-cache" | extension-pragma
extension-pragma    = token [ "=" ( token | quoted-string ) ]
```

在可使用Pragma標頭的示例實施例中，UE的瀏覽器例如可增加“Pragma: 3gpp-gba-uicc 3gpp-gba-me”以

在該標頭訊息中指明其支援基於UE和ME的GBA認證協定。雖然在此描述的示例實施例在OpenID的環境下實施，但應當理解上述技術可應用於任何數目的單點登錄安全協定，例如自由聯盟。並且，雖然各種實施例結合各種圖式來描述，但應當理解其他類似的實施例可被使用，或者可對描述的實施例作出修改和增加以執行各種實施例的相同功能，而不脫離於此。因此，實施例不應當受限於任何單獨的實施例，而應當根據所附加的申請專利範圍的廣度和範圍來構造。

在示例GBA系統中認證協定的選取和協商

第9-19圖闡明了在其中認證協定協商和選取方法可在實現通用引導架構（GBA）的系統中採用的示例實施例。在一個實施例中，GBA可為用於應用安全的認證和密鑰協定（agreement）提供引導機制（例如，用於2G及/或3G的3GPP AKA機制）、並且可支援在基於UICC及/或非UICC的證書的UE中及/或GBA網路元件中的認證協定協商。例如，網路元件可基於由UE支援的認證類型和基於應用的策略及/或MNO的策略來選取基於UICC的證書、基於非UICC的證書或其組合。在此描述的實施例可支援用於GBA知道的（GBA aware）及/或GBA不知道的（GBA unaware）UICC智慧卡的認證協定協商。

在示例實施例中，HSS/HLR可包括MNO主資料庫。這樣的資料庫可包括用戶配置檔和UE可支援的不同認證協定（例如AKA、SIP摘錄等）。在示例實施例中，GBA架構可假設UE使用一個認證協定（例如用於GBA引導的基於UICC的證書（2G或3G AKA））。在這樣的實施例中，

HSS可以是決策作出者。例如，HSS可產生AKA認證向量並回應於多媒體認證請求（MAR）發送這些向量（例如經由BSF和HSS之間的Zh介面）。在可選實施例中，例如，其中在HSS中的UE配置檔指明支援多個認證協定，UE可能想將這些協定中的一者用於GBA引導。例如，UE可支援AKA和SIP摘錄，並且UE可能想使用基於SIP摘錄的GBA引導。在這樣的實施例中，可能需要認證協定協商，並且HSS可能不是認證協定決定作出者。例如，認證協定的選取可由UE及/或GBA網路元件（例如NAF及/或BSF）來執行。

在在此描述的示例GBA系統中，在一個實施例中，認證協定可由UE和GBA實體（諸如例如NAF、BSF及/或HSS/HLR）協商並達成一致。例如，使用者設備（UE）可向服務供應者或應用伺服器（例如NAF）發送可指定可由該UE支援的認證協定及/或通信協定的資料。UE可接收可包括NAF可接受的經選取的認證協定的GBA訊息。UE可使用選取的GBA引導協定來引導與引導伺服器功能（BSF）的共享密鑰。UE可使用與BSF共享的GBA引導密鑰來導出用於與NAF進行認證的證書，並且UE可基於GBA創建的證書來建立與NAF的安全頻道。

根據在此描述的實施例，可涉及諸如例如使用者設備（UE）、BSF及/或網路存取功能（NAF）之類的實體的協定流（如第18圖所示）可以被實現。這樣的協定流可覆蓋用於達到互相可接受的認證協定及/或用於包括關聯的引導及/或繼續認證的協商。這樣的協定可實現可包括UE和NAF之間協商的GBA協定。在其他示例協定流中，協商

可在UE和BSF之間發生。

根據示例實施例，例如，諸如NAF實體這樣的服務供應者可接收指明了可由UE支援的GBA認證協定的資訊。該NAF可從支援的GBA認證協定中選取可用的GBA認證協定，並且該NAF向UE發送可包括選取的認證協定的GBA訊息。例如，如果沒有UE支援的認證方法可接受，該NAF可產生適當的錯誤訊息。示例NAF可基於選取的認證協定與UE一起運行GBA協定。

在此描述的各種實施例可由BSF來實現。例如，BSF可接收指明了可由UE支援的GBA認證協定的資訊。BSF可選取可接受的GBA認證協定。BSF可例如從操作者的策略伺服器（例如HSS/HLR）獲取與選取的協定對應的適當的認證向量（AV）。BSF可引導與運行在UE上的GBA應用的共享密鑰。BSF可基於互相的預先共享密鑰來導出應用特定密鑰。BSF可將這樣的導出密鑰及/或相關的用戶安全設定（USS）發送給請求的NAF。

根據示例實施例，各種GBA實體（例如BSF、NAF、Zn代理）及/或各種參考點（例如Ua、Ub、Zn、Zn’、Zh）可支援基於UICC及/基於非UICC的認證協定的協商。例如，至Ua參考點的UE和NAF協商可包括可附註可能的認證協定的經擴展的訊息。根據一個實施例，在至NAF的針對服務訊息的UE的請求中，用戶代理標頭欄位可包括由UE支援的認證協定的列表。在從NAF到UE的401“未授權”回應中，例如WWW認證標頭可在領域屬性中包括具有格式“3GPP-gba-type-bootstrapping@”的若干可能的前綴。前綴可指明可能需要引導安全關聯，及/或前綴可提

供選取的認證協定。例如，該通信可涉及使用兩個實體間的多訊息協商。在示例實施例中，NAF可使用演算法欄位來指明選取的認證協定及/或證書。

擴展的訊息可被用於例如使UE和BSF協商適應於Ub參考點。擴展的訊息可附註可能的認證協定。所描述的實施例可使用可附註可能的認證協定的擴展訊息來例如使BSF和NAF協商適應於Zn和Zn’參考點。擴展訊息可被用來附註可能的認證方法以例如使BSF和HSS協商適應於Zh參考點。根據示例實施例，GBA實體和GBA參考點可被用來支援自動認證協定（及/或證書）協商和選取。一些實施例為單點登錄（SSO）場景提供認證協定的協商和選取，其中用戶例如可與用作SSO識別碼提供者（IdP）及/或AEP的NAF通信。

GBA系統（協定）例如可藉由使用在本地暫存器（HLR）及/或本籍用戶伺服器（HSS）上的用戶的有效識別碼來賦能用戶認證。第9圖示出了GBA元件的示例。例如，GBA認證可藉由使網路元件質詢在UE 900中的UICC來發生、並且可以對應答類似於由HLR/HSS 902所預測的一者進行驗證。GBA可代表預先共享密鑰認證協定。根據示例實施例，引導伺服器功能（BSF）906可以是充當兩個端點（例如UE 902和NAF 904）之間的仲介的MNO網路實體。例如，BSF 906可使端點能夠建立共享密鑰。這樣的共享密鑰可在壽命方面受限。

第10圖闡明了GBA元件間的示例訊息流。參考第10圖，在1處，用戶或UE 900可請求存取NAF 904。在2處，BSF 906可傳達（mediate）GBA引導。在3處，HSS/HLR

902可由BSF 906查詢。HSS/HLR 902可在3處使用GBA引導回應來回應。在4處，UE 900和BSF 906可經歷互相認證、並可建立NAF密鑰。在5處，NAF 904可從BSF 906獲得NAF密鑰和USS。在6處，UE 900可存取NAF 904。

在示例實施例中，可以實現可賦能用戶/裝置認證協定的協商和選取的GBA系統。例如，NAF 1100（在第11圖中示出）可選取基於UICC及/或非UICC的證書。例如，UE 1102可宣稱其支援特定類型的證書，及/或其可宣稱其支援基於UICC及/或非UICC的證書。NAF 1100可支援特定類型的證書，或者其可支援基於UICC和非UICC的證書。第11圖闡明了可在本籍操作者場景下實現的示例GBA架構的方塊圖，並且第12圖闡明了可在漫遊場景下實現的示例GBA架構的方塊圖。使用本籍操作者的用戶/裝置認證方法協商及/或選取。在此描述的GBA實現（例如在第11圖和第12圖中所示）可賦能認證協定協商及/或選取、並且可支援基於UICC和非UICC的證書。在此描述的用於賦能這樣的認證協定協商及/或選取的各種實施例可包括改進的Ua參考點、Ub參考點、Zh參考點、Zn參考點、Zn'參考點、BSF功能、NAF功能及/或Zn代理功能。

參考第11圖和第12圖，Ua參考點1104可賦能UE 1102和NAF 1100之間的認證協定的協商。第13圖闡明了根據示例實施例在UE和NAF之間的示例GBA訊息流。參考第13圖，例如，UE 1102可開始與NAF 1100的通信（例如經由參考點Ua 1104）。例如，在1300，通信可指明可支援的GBA認證協定。在1302，NAF 1100可使用其可接受的

選取的GBA引導認證協定來回覆。如果沒有UE 1102支援的GBA認證協定可被NAF 1100接受，GBA引導可用錯誤訊息來終止。任何應用協定可經由Ua參考點1104（例如，HTTP、SIP）來使用。例如，在此描述的是可經由基於HTTP的Ua參考點用於認證協定協商的實施例，雖然實施例可不限於基於HTTP的協定。

在可經由Ua參考點利用HTTP協定來賦能UE和NAF協商的實施例中，HTTP摘錄認證可與GBA引導安全關聯一起使用。在此描述的Ua介面的實施例可使UE和NAF能夠在GBA引導期間協商將被使用的認證協定。術語引導協定可被用來代表認證協定。例如，引導協定可相應於認證協定。在示例實施例中，UE可藉由例如在“用戶代理”標頭中包括“產品”訊標來向NAF指明其可支援的GBA引導協定。示例“產品”訊標可採用通用形式“3gpp-gba-type”。根據各種配置，若干GBA協定可以被支援。在一個示例實施例中，UE可包括GBA不知道的UICC、並且可使用GBA_ME協定。在這樣的實施例中，示例產品訊標可包括：“3gpp-gba-me-sim”（例如使用SIM AKA）、“3gpp-gba-me-usim”（例如使用USIM AKA）和“3gpp-gba-me-isim”（例如使用ISIM AKA）。在另一個支援的GBA協定中，UE可包括GBA知道的UICC、並且可使用GBA_U。在其中UE可包括GBA知道的UICC的這樣的實施例中，示例產品訊標可包括：“3gpp-gba-uicc-sim”（例如使用SIM AKA）、“3gpp-gba-uicc-usim”（例如使用USIM AKA）和“3gpp-gba-uicc-isim”（例如使用ISIM AKA）。在另一個支援的GBA協定中，UE

可能沒有UICC智慧卡、或者可以有UICC，但是不能存取。在這樣的實施例中，示例產品訊標可包括“3gpp-gba-sip-digest”（例如用於使用SIP摘錄的非UICC證書）和“3gpp-gba-http-digest”（例如用於使用HTTP摘錄的非UICC證書）。

在“產品”訊標中包括由UE支援的認證協定列表的用戶代理標頭欄位可根據UE及/或操作者配置的策略來排序、及/或可被添加到例如輸出（outgo）的HTTP請求。一旦接收到此“產品”訊標，NAF可決定並且可選取其接受用於認證UE的認證協定中的一者，例如使用基於GBA的認證協定。第14圖顯示了當使用HTTP摘錄認證時根據示例實施例的Ua介面1402的示例協定堆疊1400。

根據示例實施例，NAF可使用領域屬性以向UE提供指示。NAF例如可藉由發送具有碼401“未經授權”的HTTP回應來向UE指示引導安全關聯可被實現。該回應也可包括WWW認證標頭。“領域”屬性可包括在此描述的示例前綴，該實例前綴可觸發UE使用例如通用格式“3GPP-gba-type-bootstrapping@”的選取的認證協定來經由Ub介面運行引導協定。示例前綴可包括：“3GPP-gba-me-usim-bootstrapping@”（例如，如果UICC是GBA不知道的，則使用USIM AKA GBA引導安全關聯）、“3gpp-gba-me-isim-bootstrapping@”（例如，如果UICC是不知道的，則使用ISIM AKA GBA引導安全關聯）、“3gpp-gba-me-sim-bootstrapping@”（例如，如果UICC是GBA不知道的，則使用SIM AKA GBA引導安全關聯）、“

3gpp-gba-uicc-usim-bootstrapping@”（例如，如果UICC是GBA知道的，則使用USIM AKA GBA引導安全關聯）、“3gpp-gba-uicc-isim-bootstrapping@”（例如，如果UICC是GBA知道的，則使用ISIM AKA GBA引導安全關聯）、“3gpp-gba-uicc-sim-bootstrapping@”（例如，如果UICC是GBA知道的，則使用SIM AKA GBA引導安全關聯）、“3gpp-gba-sip-digest-bootstrapping@”（例如，用於使用了使用SIP摘錄的非UICC證書的GBA類型引導安全關聯）和“3gpp-gba-http-digest-bootstrapping@”（例如，用於使用了使用HTTP摘錄的非UICC證書的GBA類型引導安全關聯）。在示例實施例中，NAF也可決定沒有UE支援的認證協定可接受。在這樣的場景下，可提供用於指示的適當錯誤訊息。

在可選示例實施例中，NAF可使用演算法欄位來提供指示。演算法欄位可以是替代的使用用戶代理欄位。例如，演算法欄位可由NAF用來指明將使用的認證協定。NAF可在至UE的HTTP 401未經授權訊息的演算法欄位中包括期望的協定。訊息（1）示出了這樣的訊息的一個示例：

訊息（1）：

HTTP/1.1 401 Unauthorized

WWW-Authenticate: Digest

realm=” service1.home1.net”,

nonce=” base64 (RAND)”,

qop=” auth,auth-int”,

opaque=" 6dae728da9089dab9112373c9f0a9731",
algorithm=ALGORITHM-VALUE

參考訊息（1），在訊息（1）中的ALGORITHM-VALUE可採取各種形式，例如所描述的格式“3GPP-gba-type-bootstrapping@”的變型中的一者。

第15圖闡明了根據示例實施例的用於GBA的示例性認證協定流。第15圖中的協定流可包括協同經由Ub的引導經由Ua的在UE（例如經由瀏覽器1504）和NAF 1510之間的協商。

在1512，對服務訊息的HTTP請求可被發送至NAF 1510。對服務訊息的請求可使用摘錄標頭或無需摘錄標頭來發送。例如，如果使用HTTP，則可發送訊息而無標頭。可假設UE網頁瀏覽器1504知道可包括其FQDN的NAF的ID。在請求中，瀏覽器1504可在例如“用戶代理”標頭欄位中增加一個或多個可指明其支援的GBA引導協定的產品訊標（例如，使用格式“3gpp-xxx-xxx-bootstrapping”）。例如，該產品訊標可指明UE請求使用GBA摘錄協定。該產品訊標也可指明UE支援諸如例如HTTP摘錄這樣的認證協定。UE可向NAF 1510提供該UE可支援一個或多個GBA認證協定的指示。表18闡明了包括在請求訊息中的GBA協定的示例。

表18

GBA Type Chart
• 3gpp-gba-me-usim-bootstrapping
• 3gpp-gba-me-isim-bootstrapping
• 3gpp-gba-me-sim-bootstrapping (2G GBA with SIM card)
• 3gpp-gba-uicc-usim-bootstrapping
• 3gpp-gba-uicc-isim-bootstrapping
• 3gpp-gba-uicc-sim-bootstrapping (2G GBA)
• 3gpp-gba-SIP digest-bootstrapping

在1514，NAF 1510可注意到在請求中的URL可識別可能

需要認證的服務。NAF 1510可檢查用戶代理標頭及/或可識別UE的GBA類型能力。NAF 1510可發送可指示可能需要認證的回應（例如HTTP）。在這樣的回應中，NAF 1510可增加領域值（例如使用格式“3gpp-xxxx-bootstrapping@www.naf.org”）及/或可以使用演算法欄位來指明一個或多個可接受的GBA協定。例如，UE可接收包括前綴標頭的碼401回應，並且該前綴標頭可指明允許UE執行其已請求的GBA摘錄協定。NAF 1510例如可向UE提供一個或多個GBA認證協定可被接受的指示，並且可接受的GBA認證協定可包括基於SIP摘錄的安全關聯。例如，如果指明了多於一個協定，NAF 1510可按優先性排列該列表。根據一個實施例，當瀏覽器1504接收到NAF回應時，其可檢查領域及/或演算法欄位指示的前綴值。如果沒有指示引導，瀏覽器1504例如可提示用戶輸入用戶名及/或密碼。如果前綴指示了引導，例如，UE可檢查以確定其能力是否滿足NAF 1510的要求。如果能力不滿足NAF 1510的要求，例如UE可終止該協定。在可選實施例中，可不終止協定，且瀏覽器1504例如可藉由向NAF 1510重新發送請求訊息來重新發起協定以重新協商互相可接受的引導協定。

如果UE能夠執行NAF 1510可接受的引導協定，其可在1516建構NAF_ID。例如，UE可經由NAF 1510來接收包括領域屬性的引導發起訊息，以觸發UE使用選取的認證協定及/或證書來運行引導協定。在1516建構的NAF_ID可以是FQDN和可識別Ua安全協定的5個8位元長字串的串聯。瀏覽器1504可向GBA模組1502發送可包括NAF_ID的

對引導的NAF特定密鑰的請求。在1516的訊息中，例如，瀏覽器可指明可與請求的對話密鑰相關聯的GBA類型。

在1518，GBA模組1502可執行涉及證書的引導。例如，證書可以在UICC及/或ME（例如在SIP摘錄實現中）上。例如，當使用基於卡的用戶證書時，引導可擴展到智慧卡。引導可使用BSF 1506及/或HSS/HLR 1508來建立主對話密鑰（例如Ks）。GBA模組1502可檢查請求NAF特定密鑰的應用是否被授權而做出這樣的請求。與UE和NAF協商相比，選取的引導協定在此被進一步地描述。例如，引導協定的選取可預設為UE可能夠的最高安全等級。

在1520，GBA模組1502可導出NAF特定密鑰（例如Ks_NAF）、並且可將這樣的密鑰傳遞至瀏覽器1504。與密鑰一起包括的可以是B-TID、密鑰壽命及/或指明GBA類型的資訊。NAF特定密鑰（或多個密鑰）可從Ks、可由瀏覽器提供的NAF_ID及/或諸如例如私有識別碼IMPI（例如，如果使用USIM證書，根據IMSI重格式化的）和RAND這樣的其他參數來導出。當實現（執行）GBA_U協定時，可在UICC上計算Ks_int_NAF和Ks_Ext_NAF，並且Ks_Ext_NAF可被傳遞至GBA模組1502。

在1522，在從GBA模組1502接收引導材料後，瀏覽器1504可準備對質詢（來自於1514）的摘錄回應。瀏覽器1504可使用在“授權”標頭中具有計算的摘錄回應參數的原服務請求訊息。該計算可使用B-TID作為用戶名、並且使用NAF特定的密鑰作為密碼。

在1524，可能已接收到B-TID的NAF 1510例如可向BSF 1506發送該B-TID和其NAF_ID，以請求NAF特定密鑰。

NAF 1510可使用GAA服務識別符來請求用戶安全設定（USS）、並且可指出其是否是GBA知道的。BSF 1506可使用B-TID來取回密鑰。BSF 1506可使用B-TID、NAF_ID及/或其他參數來計算NAF特定密鑰。

在1526，BSF 1506可檢查來看請求NAF特定密鑰的NAF 1510是否被授權使用接收的NAF_ID。如果是，BSF 1506可定位可由B-TID識別的主對話密鑰Ks，並且其可如在步驟1520中那樣繼續計算NAF特定密鑰。BSF 1506可將計算的密鑰發送給NAF 1510。根據一個實施例，BSF 1506也可使用USS來發送IMPI及/或服務特定用戶識別碼。USS可包括例如由操作者規定的密鑰使用要求。這樣的使用要求例如可要求使用Ks_int_NAF。如果這樣的密鑰要求未發佈，可使用來自步驟1512及/或1514的協商的密鑰。

在步驟1528，NAF 1510例如可經由使用從BSF 1506接收的NAF特定密鑰來證實摘錄回應。摘錄回應例如可在步驟1520已由瀏覽器1504發送。在一個實施例中，一旦成功認證用戶，NAF 1510可向瀏覽器1504發送可指明認證成功及/或授權用戶存取服務的200 OK。該訊息也可包括諸如例如B-TID和摘錄領域這樣的認證資訊。

在示例實施例中，Ub參考點可賦能UE和BSF之間的認證協商。第16圖闡明了根據示例實施例的用於協商認證協定的示例訊息流。

參考第16圖，在步驟1606，UE 1600可向BSF 1602發送HTTP請求。在一些實施例中，當與使用的IMIP相關聯的TMPI可在UE 1600上獲得時，UE 1600可將該TMPI包括

在“用戶名”參數中。當TMPI不可獲得時，UE可包括IMPI。UE 1600例如可藉由在“用戶代理”標頭中包括“產品”訊標來（例如向BSF 1602）指明支援的認證協定。該“產品”訊標格式可以是“3gpp-gba-type”。在1608，BSF 1602可識別（例如根據“用戶名”參數的結構）是否發送TMPI及/或IMPI。如果發送了TMPI，BSF 1602可查找相應的IMPI（例如在其本地資料庫中）。如果BSF 1602沒有找到與接收的TMPI對應的IMPI，其可向UE 1600返回適當的錯誤訊息。UE 1600可刪除該TMIP，並例如使用IMPI來重新嘗試該請求。BSF 1602可選取（例如基於來自UE支援的GBA協定列表的操作者的策略引導協定）並可獲取GBA用戶安全設定及/或用於選取協定的一個或多個認證向量的完整集合。該安全設定及/或認證向量可經由參考點Zh從操作者的策略伺服器1604（例如，HSS/HLR）中獲取。如果BSF 1602不能選取認證協定，其可依賴由策略伺服器1604（例如HSS/HLR）選取的協定。如果沒有UE 1600支援的GBA認證協定可被BSF 1602接受，例如可使用適當的錯誤訊息來終止GBA引導。HSS/HLR例如可結合用戶訂閱以基於其策略來確定使用哪個AV。例如，在其中UE可裝備有包括SIM和USIM應用的UICC的實施例中，其可預設USIM。在其中UICC可以是GBA知道的的實施例中，其可自動運行GBA_U。

在步驟1610，BSF 1602可將401訊息轉發給UE 1600。該訊息可包括選取的協定及/或現時(nonce)質詢。該訊息可要求UE 1600認證其自己。在1612，UE 1600可運

行選取的認證協定及/或可檢查現時(nonce)，例如，以驗證該質詢可來自於經授權的網路。根據一個實施例，UE 1600也可計算對話密鑰及/或RES。步驟1612可在BSF 1602及/或UE 1600中產生對話密鑰。在步驟1614，UE 1600可向BSF 1602發送包括（例如，使用RES計算的）摘錄回應的另一個HTTP請求。BSF 1602例如可經由驗證該摘錄回應來認證UE 1600（步驟1616）。在步驟1618，BSF 1602可基於從HSS/HLR接收的AV產生密鑰材料（Ks）（例如Ks =CK||IK）。B-TID值可以NAI的格式來產生，例如以綁定密鑰材料和UE識別碼。在步驟1620，BSF 1602可向UE 1600發送200 OK訊息（例如包括B-TID）。該訊息可指出認證的成功。BSF 1602可在200 OK訊息中提供密鑰Ks的壽命。密鑰材料Ks可在UE中產生（例如Ks =CK||IK）。在步驟1622，UE 1600及/或BSF 1602例如可使用Ks來導出密鑰材料Ks_NAF，該密鑰材料Ks_NAF可用於保護參考點Ua。UE 1600和BSF 1602可與關聯的B-TID一起儲存密鑰Ks以便將來使用，直到Ks的壽命期滿、直到更新密鑰Ks及/或直到滿足刪除條件。

根據在此描述的實施例，UE可經由Ub參考點例如根據在“用戶代理”標頭中包括“產品”訊標來向BSF指明支援的認證協定。“產品”訊標可採用以下字串值，例如：“3gpp-gba-me-usim”（例如，UICC不是GBA知道的，並且UE使用USIM AKA）、“3gpp-gba-me-isim”（例如UICC不是GBA知道的，並且UE使用ISIM AKA）、“3gpp-gba-me-sim”（例如UICC不是GBA知道的，並且

UE使用SIM AKA）、“3gpp-gba-uicc-usim”（例如UICC是GBA知道的，並且UE使用USIM AKA）、“3gpp-gba-uicc-isim”（例如UICC是GBA知道的，並且UE使用ISIM AKA）、“3gpp-gba-uicc-sim”（例如UICC是GBA知道的，並且UE使用SIM AKA）、“3gpp-gba-sip-digest”（例如使用SIP摘錄的非UICC證書）和“3gpp-gba-http-digest”（例如使用HTTP摘錄的非UICC證書）。具有在“產品”訊標中的由UE支援的認證協定列表的用戶代理標頭欄位可根據UE及/或操作者配置的策略來排列。在一個實施例中，一旦接收到“產品”訊標，應用伺服器（例如，BSF）可決定並且可選取使用的認證協定，例如，以使用基於GBA的認證協定來認證UE。在示例引導協定中的Ub介面1202的示例協定堆疊1200在第17圖中示出。

如在此描述那樣，UE和NAF之間的初始協商的協定可相對於可被採用的（例如，經由用戶訂閱及/或網路策略）引導來解決。例如，NAF可包括指明其是否接受用戶使用SIP摘錄證書的策略。在一些實施例中，例如，如果這樣的認證協定與策略不一致，用戶訂閱及/或網路策略可代替可在UE和BSF之間協商的認證協定。這樣的代替可取決於實現的整體決策結構。

Zn參考點可在BSF和NAF之間實現。根據第18圖所示的實施例，Zn介面1808可賦能GBA引導協定協商及/或選取。第18圖顯示了GBA引導協定協商的示例實施例。在步驟1810，UE 1800例如可經由發送其識別碼（UE-Id）及/或按優先性排列的所支援的GBA引導協定列表來開始協定

Ua 1806。如果這些協定中的一個或多個可被NAF 1802接受，在步驟1812，NAF 1802例如可經由發送UE-Id、NAF-Id及/或UE支援的GBA協定列表來開始與BSF 1804的協定Zn 1808。NAF可（例如，如果其能接受在列表上的所有GBA協定）發送完整的列表、或者其可發送GBA協定及/或其接受的協定（例如，來自接收到的列表）的列表。如果在列表上的協定不被NAF 1802接受，其可向UE 1800發送適當的錯誤訊息，並且該協定可被終止。在1814，BSF 1804可檢查由NAF 1802提供的UE-Id、NAF-Id及/或GBA認證協定列表。BSF 1804可選取（例如，基於操作者的策略）GBA認證協定。在1816，BSF 1804可向NAF 1802發送（例如，經由Zn介面1808）包括私有UE識別碼（IMPI）及/或選取的GBA認證協定的訊息。在其中在列表上的GBA協定不被BSF 1804接受的示例實施例中，BSF 1804可向NAF 1802發送適當的錯誤訊息。在1818，NAF 1802例如可經由向UE 1800指明可接受的GBA認證協定來與UE 1800繼續協定Ua 1806。在其中沒有GBA認證協定可被接受的實施例中，適當的錯誤訊息可被返回。如在此描述的那樣，UE 1800和NAF 1802之間的初始協商協定可相對於可採用的引導來解決。在一些實施例中，用戶訂閱及/或網路策略可替代可在NAF和BSF之間協商的認證方法。這樣的替代可取決於實現的整體決策結構。

Zh介面可在BSF和操作者的策略伺服器（例如，HSS/HLR）之間實現。第19圖闡明了根據在其中Zh介面1908可賦能與HSS 1904的GBA引導協定協商及/或選取的實施例的

示例調用流。在1910，UE 1900例如可經由發送其識別碼（IMPI）及/或按優先性排列的所支援的GBA引導協定列表來開始協定Ub 1906。在1912，BSF 1902可經由發送IMPI及/或選取的GBA認證協定來開始與HSS 1904的協定Zh 1908。在其中BSF 1902不能選取GBA協定的實施例中，其可將協定設定為“未知”及/或可依賴HSS 1904來選取協定。例如，HSS 1904可基於儲存在HSS 1904中的用戶配置檔來選取協定。根據一個實施例，HSS 1904可基於用戶識別碼及/或網路策略以獲知使用哪個協定。在其中BSF 1902指明協定是“未知的”且HSS 1904不選取協定的這樣的實施例中，BSF 1902可向UE 1900發送適當的錯誤訊息。在1914，HSS 1904可為選取的GBA認證協定產生AV。在1916中，HSS 1904可提供（例如向BSF 1902）所請求的認證向量及/或GUSS（例如，如果有的話）。在1918，BSF 1902可儲存為IMPI接收的AV資訊。在步驟1920，BSF 1902可向UE 1900指明可接受的GBA協定。在1922，UE 1900和BSF 1902可經由Ub介面1906繼續引導協定。

根據示例實施例，在此描述的協商的結果可潛在地互相衝突。因此，在示例實施例中，衝突可被調解及/或避免。例如，配置可從最高到最低安全評級。基於通用行動安全考慮，示例評級順序可以是：（1）UE具有GBA知道的UICC；（2）UE具有GBA不知道的UICC；和（3）UE沒有UICC，或者UE有UICC但不可用。

在示例實施例中，選取可要求有效的策略，例如，規定選取的引導協定與NAF允許的至少最小安全等級相關聯。

例如，這樣的策略可根據用戶及/或操作者等級或從在認證中涉及的實體（例如UE、BSF、NAF、HSS）中的一者的等級是可實施的。在使用這樣的策略的實施例中，UE-NAF協商可最終確定可使用什麼進行引導。在一個示例場景中，由NAF允許的最小安全等級可低於或等於UE的能力。例如，如果UE能夠包括GBA知道的UICC且NAF允許UE沒有UICC（或者有UICC但不可用），則UE和NAF可根據任何上述可能的UE能力自由地協商。例如，在這樣的場景中，GBA_U、GBA_ME或GBA_Digest（GBA_摘錄）可以是可能。可選地，如果NAF堅持與包括GBA知道的UICC的UE相關聯的安全等級，則可要求GBA_U。

在另一個示例場景中，由NAF允許的最小安全等級可比UE能力大。在這樣的場景中，例如，錯誤訊息將作為初始協商的一部分從NAF發送給UE，並且沒有引導可發生。

以上討論的示例實施例可避免解決潛在的衝突，該衝突當兩個或多個協商（例如BSF-NAF、UE-BSF等）在給定的認證協定中發生時可能產生。在示例實施例中，UE-NAF協商可被考慮。例如，如果允許多個協商發生，則可需要選取方法更複雜的調解。涉及例如在BSF中的決策智慧化的調解可解決協商衝突。這樣的決策智慧化可駐留在HSS、NAF、UE、BSF或其組合中。

如前在本文中討論的，第7圖闡明了用於單獨登錄（SSO）場景的用戶認證協定及/或證書的協商和選取的協定流的示例實施例。在示例實施例中，NAF可用作SSO識別碼提供者（IdP）。例如，在該場景中NAF可被表示為NAF/IdP及/或OP（例如，在OpenID的環境中）。例如

，協商可使用諸如OpenID提供者授權策略擴展（PAPE）及/或HTTP這樣的標準協定及/或工具。雖然在此參考OpenID協定來描述，但也可參考其他諸如自由聯盟的協定。對於第7圖考慮的配置可包括UE、NAF/IdP（網頁伺服器）及/或可被稱為信賴方（RP）的服務供應者。各種條件可強加於這些實體。例如，UE可以是行動網路操作者（MNO）的無線服務的用戶。例如NAF/IdP可在若干變型下實現認證選取。

在示例實施例中，NAF/IdP可在MNO的策略控制下運行。在另一個示例實施例中，NAF/IdP可作用為OP、並且可以處於或者不處於MNO的策略控制下。OP和RP可使用OpenID協定擴展（例如，使用PAPE訊息）來傳達認證偏好。在請求UE可使用特定協定來認證時，OP可應用其自己的策略。

參考第7圖，闡明了示例SSO協定流（例如，使用OpenID）。在706，UE/用戶700可瀏覽RP 704且可向RP 704提供OpenID識別符，並且UE/用戶700可指明其支援基於GBA的認證。在708，RP 704可基於提供的OpenID識別符和GBA認證提示來決定RP 704可能偏愛哪些用戶認證的特定協定及/或RP 704可能偏愛哪些認證協定特性。在步驟712和714，RP 704將UE 700重新定向到具有集成NAF的OpenID伺服器702（NAF/OP），例如，以發起與NAF/OP的OpenID協定。RP 704可使用PAPE來請求期望的認證協定及/或證書。在716，NAF/OP 702和RP 704可能想根據OpenID擴展來進行“協商”，例如以確定由RP 704提供的協定是否可被NAF/OP 702接受。如果多

於一個協定是可接受的，GBA認證協定協商可被執行（例如，如在此描述的），並且可選取協定（例如，經由策略）。如果沒有協定是可接受的，例如，NAF可向RP 704發送錯誤訊息，並且RP 704可通知UE/用戶700（例如，和OpenID SSO）不再繼續。在718，NAF/OP 702可參與與UE/用戶700的OpenID認證（例如，使用選取的協定）。在認證中，NAF/OP 702和UE 700例如可能想根據UE 700是否支援該協定來重新協商選取的認證協定。例如，NAF/OP 702可知道哪些協定可被支援，及/或UE 700可能想通知NAF/OP 702該UE支援哪些認證協定。在步驟720，UE 700可使用選取的協定或協商的協定及/或證書來進行認證。在722，OP可判定識別碼、並可將用戶重新定向回RP 704。該訊息可包括經簽名的判定訊息且可包括（例如基於OpenID擴展）認證協定及/或諸如例如上一次認證的時間這樣的附加資訊。在步驟724，RP 704可決定經報告的協定是否匹配請求的協定。RP 704也可確定是否在OP 702和UE 700之間已選取了另一個協定。

第20A圖在其中可以實施一個或多個揭露的實施例的示例通信系統2000的圖。通信系統2000可以是向多個無線用戶提供諸如語音、資料、視訊、訊息、廣播等這樣的內容的多重存取系統。通信系統2000可使多個無線用戶能夠經由共享包括無線頻寬的系統資源來存取這樣的內容。例如，通信系統2000可採用一種或多種頻道存取方法，例如分碼多重存取（CDMA）、分時多重存取（TDMA）、分頻多重存取（FDMA）、正交FDMA（OFDMA）、單載

波FDMA（SC-FDMA）等。

如第20A圖所示，通信系統2000可包括無線傳輸/接收單元（WTRU）2002a、2002b、2002c、2002d、無線電存取網路（RAN）2004、核心網路2006、公共交換電話網路（PSTN）2008、網際網路2010和其他網路2012，但是將理解揭露的實施例設想任何數目的WTRU、基地台、網路及/或網路元件。WTRU 2002a、2002b、2002c、2002d的每一個可以是被配置為在無線環境中操作及/或通信的任何類型的裝置。以示例的方式，WTRU 2002a、2002b、2002c、2002d可被配置為發送及/或接收無線信號、並且可包括使用者設備（UE）、行動站、固定或行動用戶單元、呼叫器、蜂巢式電話、個人數位助理（PDA）、智慧型電話、膝上型電腦、迷你筆記型電腦、個人電腦、無線感測器、消費電子產品等。

通信系統2000亦可包括基地台2014a和基地台2014b。基地台2014a、2014b的每一個可以是被配置為與WTRU 2002a、2002b、2002c、2002d的至少一個進行無線介面連接的任何類型的裝置，以便於存取一個或多個諸如核心網路2006、網際網路2010及/或網路2012這樣的通信網路。以示例的方式，基地台2014a、2014b可以是基地台收發站（BTS）、節點B、e節點 B、家用節點 B、家用e節點 B、站點控制器、存取點（AP）、無線路由器等。雖然基地台2014a、2014b每一個被描述為單一元件，但應理解基地台2014a、2014b可包括任何數目的互連基地台及/或網路元件。

基地台2014a可以是RAN 2004的一部分，RAN 2004也可

包括其他基地台及/或網路元件（未示出），例如基地台控制器（BSC）、無線電網路控制器（RNC）、中繼節點等。基地台2014a及/或基地台2014b可被配置為在可被稱為胞元（未示出）的特定地理區域內發送及/或接收無線信號。胞元可進一步被劃分為胞元扇區。例如，與基地台2014a相關聯的胞元可被劃分為3個扇區。因此，在一個實施例中，基地台2014a可包括3個收發器，即針對所述胞元的每個扇區都有一個收發器。在另一個實施例中，基地台2014a可採用多輸入多輸出（MIMO）技術，因此可針對胞元的每個扇區使用多個收發器。

基地台2014a、2014b可經由空氣介面2016與WTRU 2002a、2002b、2002c、2002d的一個或多個進行通信，空氣介面2016可以是任何適當的無線通信鏈路（例如射頻（RF）、微波、紅外（IR）、紫外（UV）、可見光等）。空氣介面2016可使用任何適當的無線電存取技術（RAT）來建立。

更具體地，如上所述，通信系統2000可以是多重存取系統、並且可採用一種或多種頻道存取方案，例如CDMA、TDMA、FDMA、OFDMA、SC-FDMA等。例如，RAN 2004中的基地台2014a和WTRU 2002a、2002b、2002c可實現諸如通用行動通信系統（UMTS）陸地無線電存取（UTRA）這樣的無線電技術，其可使用寬頻CDMA（WCDMA）來建立空氣介面2016。WCDMA可包括諸如高速封包存取（HSPA）及/或演進型HSPA（HSPA+）這樣的通信協定。HSPA可包括高速下鏈封包存取（HSDPA）及/或高速上鏈封包存取（HSUPA）。

在另一個實施例中，基地台2014a和WTRU 2002a、2002b、2002c可實現諸如演進型UMTS陸地無線電存取（E-UTRA）這樣的無線電技術，其可使用長期演進（LTE）及/或高級LTE（LTE-A）來建立空氣介面2016。

在其他實施例中，基地台2014a和WTRU 2002a、2002b、2002c可實現諸如IEEE 802.16（即全球微波互通存取（WiMAX））、CDMA2000、CDMA2000 1X、CDMA2000 EV-DO、臨時標準2000（IS-2000）、臨時標準95（IS-95）、臨時標準856（IS-856）、全球行動通信系統（GSM）、增強型資料速率GSM演進（EDGE）、GSM EDGE（GERAN）等這樣的無線電技術。

第20A圖中的基地台2014b可以是例如無線路由器、家用節點 B、家用e節點 B或存取點、並且可使用任何適當的RAT以促進局部區域中的無線連接，例如商業地點、家庭、車輛、校園等。在一個實施例中，基地台2014b和WTRU 2002c、2002d可實現諸如IEEE 802.11這樣的無線電技術，以建立無線區域網路（WLAN）。在另一個實施例中，基地台2014b和WTRU 2002c、2002d可實現諸如IEEE 802.15這樣的無線電技術，以建立無線個人區域網路（WPAN）。在又一個實施例中，基地台2014b和WTRU 2002c、2002d可使用基於蜂巢的RAT（例如WCDMA、CDMA2000、GSM、LTE、LTE-A等）來建立微微胞元（picocell）或毫微微胞元（femtocell）。如第20A圖所示，基地台2014b可與網際網路2010有直接連接。因此，基地台2014b不需要經由核心網路2006來存取網際網路2010。

RAN 2004可與核心網路2006通信，核心網路2006可以是任何類型的、被配置為向WTRU 2002a、2002b、2002c、2002d的一個或多個提供語音、資料、應用及/或網際協定上的語音（VoIP）服務的網路。例如，核心網路2006可提供呼叫控制、計費服務、基於移動位置的服務、預付費呼叫、網際網路連接、視訊發佈等，及/或執行諸如用戶認證這樣的高級安全功能。雖然未在第20A圖中示出，但應理解RAN 2004及/或核心網路2006可與採用與RAN 2004相同RAT或不同RAT的其他RAN直接或間接通信。例如，除了與可採用E-UTRA無線電技術的RAN 2004連接之外，核心網路2006也可與採用GSM無線電技術的另一個RAN（未示出）通信。

核心網路2006也可作為閘道，以用於WTRU 2002a、2002b、2002c、2002d存取PSTN 2008、網際網路2010及/或其他網路2012。PSTN 2008可包括提供普通老式電話服務（POTS）的電路交換電話網路。網際網路2010可包括使用公共通信協定的互連電腦網路和裝置的全球系統，例如TCP/IP網際網路協定系列中的傳輸控制協定（TCP）、用戶資料報協定（UDP）和網際網路協定（IP）。網路2012可包括由其他服務供應者擁有及/或操作的有線或無線通信網路。例如，網路2012可包括與可採用與RAN 2004相同RAT或不同RAT的一個或多個RAN相連接的另一個核心網路。

在通信系統2000中的WTRU 2002a、2002b、2002c、2002d的一些或所有可包括多模能力，例如WTRU 2002a、2002b、2002c、2002d可包括用於經由多個無線鏈路

來與不同無線網路進行通信的多個收發器。例如，第20A圖中示出的WTRU 2002c可被配置為與可採用基於蜂巢的無線電技術的基地台2014a和與可採用IEEE 802無線電技術的基地台2014b進行通信。

第20B圖是闡明示例WTRU 2002的系統圖。如第20B圖所示，WTRU 2002可包括處理器2018、收發器2020、傳輸/接收元件2022、揚聲器/麥克風2024、鍵盤2026、顯示器/觸控板2028、不可移式記憶體2030、可移式記憶體2032、電源2034、全球定位系統（GPS）碼片組2036和其他週邊裝置2038。應理解，WTRU 2002可包括前述元件的任何子組合，而與實施例保持一致。

處理器2018可以是通用處理器、專用處理器、傳統處理器、數位信號處理器（DSP）、多個微處理器、與DSP核相關聯的一或多個微處理器、控制器、微控制器、專用積體電路（ASIC）、現場可編程閘陣列（FPGA）電路、任何其他類型的積體電路（IC）、狀態機等。處理器2018可執行信號編碼、資料處理、功率控制、輸入/輸出處理及/或使WTRU 2002能夠在無線環境中操作的任何其他功能。處理器2018可與收發器2020耦合，收發器2020可與傳輸/接收元件2022耦合。雖然第20B圖將處理器2018和收發器2020描述為分離的元件，但將理解處理器2018和收發器2020可被一起集成在電子封裝或晶片中。

傳輸/接收元件2022可被配置為經由空氣介面2016向基地台（例如基地台2014a）發送信號或從基地台（例如基地台2014a）接收信號。例如，在一個實施例中，傳輸/接收元件2022可以是被配置為發送及/或接收RF信號的天

線。在另一個實施例中，傳輸/接收元件2022可以是被配置為例如發送及/或接收IR、UV或可見光信號的發光體/偵測器。在又一個實施例中，傳輸/接收元件2022可以被配置為發送和接收RF和光信號兩者。將理解，傳輸/接收元件2022可被配置為發送及/或接收無線信號的任何組合。

此外，雖然傳輸/接收元件2022在第20B圖中被描述為單一元件，但WTRU 2002可包括任何數目的傳輸/接收元件2022。更具體地，WTRU 2002可採用MIMO技術。因此，在一個實施例中，WTRU 2002可包括用於經由空氣介面2016發送和接收無線信號的兩個或更多個傳輸/接收元件2022（例如多個天線）。

收發器2020可被配置為調變將由傳輸/接收元件2022發送的信號並解調由傳輸/接收元件2022接收的信號。如上所述，WTRU 2002可具有多模能力。因此，收發器2020可包括多個收發器，以例如用於使WTRU 2002能夠經由諸如UTRA和IEEE 802.11這樣的多個RAT進行通信。

WTRU 2002的處理器2018可與揚聲器/麥克風2024、鍵盤2026及/或顯示器/觸控板2028（例如液晶顯示器（LCD）顯示單元或有機發光二極體（OLED）顯示單元）耦合、並可從其接收用戶輸入資料。處理器2018也可以向揚聲器/麥克風2024、鍵盤2026及/或顯示器/觸控板2028輸出用戶資料。此外，處理器2018可從諸如不可移式記憶體2030及/或可移式記憶體2032這樣的任何類型的適當記憶體存取資訊、並將資料儲存在其中。不可移式記憶體2030可包括隨機存取記憶體（RAM）、唯讀記憶

體（ROM）、硬碟或任何其他類型的記憶體裝置。可移式記憶體2032可包括用戶身份模組（SIM）卡、記憶條、安全數位（SD）記憶卡等。在其他實施例中，處理器2018可從實體上不位於WTRU 2002上（例如在伺服器或家用電腦（未示出）上）的記憶體存取資訊，並將資料儲存在其中。

處理器2018可從電源2034接收功率、並可被配置為分配及/或控制至WTRU 2002中其他元件的功率。電源2034可以是用於向WTRU 2002供電的任何適當的裝置。例如，電源2034可包括一個或多個乾電池（例如鎳鎘（NiCd）、鎳鋅（NiZn）、鎳氫（NiMH）、鋰離子（Li-ion）等）、太陽能電池、燃料電池等。

處理器2018也可以與可被配置為提供關於WTRU 2002目前位置的位置資訊（例如經度和緯度）的GPS碼片組2036耦合。附加於或替代來自GPS碼片組2036的資訊，WTRU 2002可經由空氣介面2016從基地台（例如基地台2014a、2014b）接收位置資訊、及/或基於信號從兩個或更多個附近基地台接收的時序來確定其位置。將理解，WTRU 2002可以用任何適當的位置確定方法來獲取位置資訊而與實施例保持一致。

處理器2018可進一步與其他週邊裝置2038耦合，其他週邊裝置2038可包括提供附加特徵、功能及/或有線或無線連接的一個或多個軟體及/或硬體模組。例如，週邊裝置2038可包括加速計、電子羅盤、衛星收發器、數位照相機（用於相片或視訊）、通用串列匯流排（USB）埠、振動裝置、電視收發器、免持耳機、藍芽®模組、調頻（FM

）無線電單元、數位音樂播放器、媒體播放器、視訊遊戲播放器模組、網際網路瀏覽器等。

第20C圖是根據實施例的RAN 2004和核心網路2006的系統圖。如上所述，RAN 2004可採用E-UTRA無線電技術來經由空氣介面2016與WTRU 2002a、2002b、2002c進行通信。RAN 2004亦與核心網路2006進行通信。

RAN 2004可包括e節點B 2040a、2040b、2040c，雖然將理解RAN 2004可包括任何數目的e節點B而與實施例保持一致。e節點B 2040a、2040b、2040c每一個可包括用於經由空氣介面116與WTRU 2002a、2002b、2002c進行通信的一個或多個收發器。在一個實施例中，e節點B 2040a、2040b、2040c可實施MIMO技術。因此e節點B 2040a例如可使用多個天線來向WTRU 2002a發送無線信號並從其接收無線信號。

e節點B 2040a、2040b、2040c的每一個可與特定的胞元（未示出）相關聯、並且可被配置為處理無線電資源管理決策、切換決策、排程在上鏈及/或下鏈中的用戶等。如第20C圖所示，e節點B 2040a、2040b、2040c可經由X2介面互相通信。

第20C圖中示出的核心網路2006可包括行動管理閘道（MME）2042、服務閘道2044和封包資料網路（PDN）閘道2046。雖然上述元件被描述為核心網路2006的一部分，但將理解這些元件的任何一個可由除核心網路操作者以外的實體擁有及/或操作。

MME 2042可經由S1介面以與RAN 2004中的e節點B 2040a、2040b、2040c的每一個進行連接、並且可作為

控制節點。例如，MME 2042可負責認證WTRU 2002a、2002b、2002c的用戶、承載啟動/止動、在WTRU 2002a、2002b、2002c初始連結期間選取特定的服務閘道等。MME 2042也可提供用於在RAN 2004和採用諸如GSM或WCDMA這樣的其他無線電技術的其他RAN（未示出）之間切換的控制平面功能。

服務閘道2044可經由S1介面以與RAN 2004中的e節點B 2040a、2040b、2040c的每一個進行連接。服務閘道2044通常可路由用戶資料封包至WTRU 2002a、2002b、2002c/轉發來自WTRU 2002a、2002b、2002c的用戶資料封包。服務閘道2044也可以執行其他功能，例如在e節點 B間切換期間錨定用戶平面、當下鏈資料對WTRU 2002a、2002b、2002c可用時觸發傳呼、管理和儲存WTRU 2002a、2002b、2002c的上下文等。

服務閘道2044也可與PDN閘道2046連接，PDN閘道2046可向WTRU 2002a、2002b、2002c提供到諸如網際網路2010這樣的封包交換網路的存取，以便於WTRU 2002a、2002b、2002c和賦能IP的裝置之間的通信。

核心網路2006可促進與其他網路的通信。例如，核心網路2006可向WTRU 2002a、2002b、2002c提供到諸如PSTN 2008這樣的電路交換網路的存取，以促進WTRU 2002a、2002b、2002c和傳統陸線通信裝置之間的通信。例如，核心網路2006可包括作為核心網路2006和PSTN 2008之間的介面的IP閘道（例如IP多媒體子系統（IMS）伺服器）或與之通信。此外，核心網路2006可向WTRU 2002a、2002b、2002c提供到網路2012的存取，網路

2012可包括由其他服務提供者擁有及/或操作的其他有線或無線網路。

雖然在此描述的示例實施例在OpenID的環境下得以執行，但上述技術可被應用於任何數目的單點登錄安全協定，例如自由聯盟。並且各個實施例與各個圖式相關地進行描述，但應當理解其他類似的實施例可被使用，或者可對描述的實施例作出修改和增加，以執行各個實施例相同的功能，而不脫離於此。因此，實施例不應當受限於任何單一實施例，相反應當根據所附加的申請專利範圍的廣度和範圍來建構。

此外，以上以特定的組合描述了特徵和元素，並且每個特徵或元素可以單獨地或與其它的特徵和元素任何組合地使用。應當理解所有在此描述的系統、方法和過程可以儲存在電腦可讀儲存媒體上的電腦或處理器可執行指令（即程式碼、軟體及/或韌體）的形式來實施，這些指令在由諸如處理器這樣的機器執行時執行及/或實現在此描述的系統、方法和過程。具體地，在此描述的任何步驟、操作或功能可以這樣的可執行指令的形式來實現。電腦可讀儲存媒體包括以任何用於儲存資訊的方法或技術實現的揮發和非揮發、可移式和不可移式媒體。電腦可讀儲存媒體的示例包括但不限制為RAM、ROM、EEPROM、快閃記憶體或其他儲存技術、CDROM、數位光碟（DVD）或其他光碟儲存、盒式磁帶、磁帶、磁碟記憶體或其他磁儲存裝置或者任何其他可被用來儲存期望資訊並且可由電腦或處理器存取的媒體。

【圖式簡單說明】

[0005] 第1圖闡明了使用認證的一般架構的示例實施例；

第2圖闡明了實施OpenID協定的一般架構的示例實施例；

第3圖闡明了實施通用引導架構（GBA）協定的一般架構的示例實施例；

第4圖闡明了實施OpenID和GBA的架構的示例實施例；

第5圖闡明了為了使用具有多個認證協定及/或證書的單點登錄（SSO）的架構框架的示例實施例；

第6A和6B圖闡明了用於SSO框架架構的協定流的示例實施例；

第7圖闡明了用於協商和選取用戶認證協定及/或證書的協定流的示例實施例；

第8圖顯示了用於UE和行動網路操作者（MNO）控制的OpenID識別碼提供者（OP）之間的協商的示例訊息交換；

第9圖闡明了GBA網路元件的示例方塊圖；

第10圖闡明了根據示例實施例的GBA元件間的示例訊息流；

第11圖闡明了可在本籍操作者場景中實施的示例GBA架構的方塊圖；

第12圖闡明了可在漫遊場景中實施的示例GBA架構的方塊圖；

第13圖闡明了UE和網路存取功能（NAF）之間的示例GBA訊息流；

第14圖顯示了Ua介面的示例協定堆疊；

第15圖闡明了根據示例實施例的GBA的示例性認證協定流；

第16圖闡明了根據示例實施例的用於協商認證協定的示例訊息流；

第17圖顯示了Ub介面的示例性協定堆疊；

第18圖闡明了用於GBA引導協定協商的訊息流的示例實施例；

第19圖闡明了用於GBA引導協定協商的訊息流的另一個示例實施例；

第20A圖是在其中可以實施一個或多個揭露的實施例的示例通信系統的系統圖；

第20B圖是可在第20A圖所示的通信系統中使用的示例無線傳輸/接收單元（WTRU）的系統圖；

第20C圖是可在第20A圖所示的通信系統中使用的示例無線電存取網路和示例核心網路的系統圖。

【主要元件符號說明】

[0006] AV　認證向量

BSF、302、410、906、1506、1602、1804、1902　引導伺服器功能

GBA　通用引導架構

GPS　全球定位系統

HLR　本地暫存器

HSS、1904　本籍用戶伺服器

HTTP　超文本傳輸協定

IMPI　私有UE識別碼

IP　網際網路協定

Ks　密鑰

MME、2042　行動管理閘道

MNO　行動網路操作者

NAF、304、406、904、1100、1510、1802　網路存取功能

OP、202、404、612、702　OpenID識別碼提供者

PAPE　提供者授權策略擴展

PDN　封包資料網路

RAN、2004　無線電存取網路

RP、204、402、610、704　信賴方

SSO　實現單點登錄

TCP　傳輸控制協定

UE、800、900、1102、1600、1800、1900　使用者設備

USS　用戶安全設定

WTRU、2002、2002a、2002b、2002c、2002d　無線傳輸/接收單元

100　一般架構

102、400、700　用戶設備

104　服務供應者

106　認證端點

116、2016　空氣介面

3gpp　第3代合作夥伴計畫

412　OpenID伺服器

414、902、1508　HSS/HLR

502　瀏覽器應用

504　非瀏覽器應用

506、608　SSO子系統

508、510、512、514、516　認證模組

518　安全可信環境

602　用戶

604　裝置

606　應用

802　MNO/OP

1104　Ua參考點

1400　示例協定堆疊

1402　Ua介面

1502　GBA模組

1504　瀏覽器

1604　策略伺服器

1806　Ua

1808　Zn介面

1906　Ub

1908　Zh

2000　示例通信系統

2006　核心網路

2008　PSTN

2010　網際網路

2012　其他網路

2014b　基地台

2018　處理器

2020　收發器

2022　傳輸/接收元件

2024　揚聲器/麥克風

2026 鍵盤

2028 顯示器/觸控板

2030 不可移式記憶體

2032 可移式記憶體

2034 電源

2036 全球定位系統碼片組

2038 週邊裝置

2040a、2040b、2040c e節點B

2044 服務閘道

2046 PDN閘道

七、申請專利範圍：

1．一種在包括經由一網路進行通信的一使用者設備（UE）、一服務供應者（SP）和一認證端點（AEP）的一系統中由該AEP認證該UE的方法，該方法包括在該AEP處：

確定能被用來認證該UE的一個或多個認證協定或證書；

與該UE協商以選取該SP可接受的該多個認證協定或證書中的一者；以及

使用所選取的認證協定或證書來認證該UE。

2．如申請專利範圍第1項所述的方法，該方法更包括：

確定該SP可接受的一個或多個認證協定或證書，其中確定該SP可接受的該一個或多個協定或證書包括與該SP協商以確定該可接受的協定或證書。

3．如申請專利範圍第2項所述的方法，其中確定該SP可接受的一個或多個認證協定或證書包括：

從該SP接收一個或多個特性；以及

確定包括該一個或多個特性的該可接受的協定或證書。

4．如申請專利範圍第2項所述的方法，其中確定該SP可接受的一個或多個認證協定或證書包括從對該AEP可存取的一資料庫獲取該可接受的協定或證書，該資料庫為一個或多個服務供應者儲存關於多個可接受的協定或證書的一資訊。

5．如申請專利範圍第1項所述的方法，該方法更包括：

從該UE接收由該UE支援的一個或多個認證協定或證書的一識別。

6．如申請專利範圍第1項所述的方法，其中該網路實施一

OpenID聯合識別碼管理架構，並且其中該SP包括一信賴方（RP），以及該AEP包括該聯合識別碼管理架構中的一識別碼提供者（IdP）。

7．如申請專利範圍第1項所述的方法，其中該網路實施一通用引導架構（GBA），並且其中該SP包括一網路存取功能（NAF），以及該AEP包括一引導伺服器功能（BSF）。

8．如申請專利範圍第7項所述的方法，該方法更包括在該BSF處：

從該UE接收運行一GBA摘錄協定的一請求；以及

回應於該請求，從一策略伺服器請求並獲取一認證向量。

9．如申請專利範圍第8項所述的方法，其中該NAF包括指明是否接受使用一SIP摘錄證書的一用戶的一策略。

10．如申請專利範圍第1項所述的方法，其中該網路實施一通用引導架構（GBA）和一OpenID聯合識別碼管理架構，並且其中該AEP包括一網路存取功能（NAF）和一識別碼提供者（IdP）。

11．一種在包括經由一網路進行通信的一使用者設備（UE）、一服務供應者（SP）和一認證端點（AEP）的一系統中由一AEP認證該UE的方法，該方法包括在該SP處：

從該UE接收存取由該SP提供的一服務的一請求；

確定將被用於認證該UE的一個或多個認證協定或證書；

向該AEP提供關於該SP可接受的該認證協定或證書的一資訊；

根據一選取的認證協定或證書，從該UE接收指明該UE的認證的一經簽名的判定訊息。

12．一種在包括經由一網路進行通信的一使用者設備（UE）、

一服務供應者（SP）和一認證端點（AEP）的一系統中認證該UE的方法，該方法包括在該UE處：

向該SP發送用於存取由該SP提供的一服務的一請求；

與該AEP協商以選取該SP可接受的且由該UE支援的多個認證協定或證書中的一者；以及

根據該選取的多個認證協定或證書，從AEP接收多個UE的一認證結果的一指示。

13．如申請專利範圍第12項所述的方法，其中該指示包括一經簽名的判定訊息，該經簽名的判定訊息包括根據該選取的認證協定或證書的該UE的該認證結果，該方法更包括：

由該UE將該經簽名的判定訊息轉發給該SP。

14．如申請專利範圍第12項所述的方法，其中來自該AEP的該指示包括一密鑰，該密鑰從根據該選取的認證協定及/或證書的該UE的一認證產生。

15．如申請專利範圍第12項所述的方法，其中該網路實施一通用引導架構（GBA），並且其中該SP包括一網路存取功能（NAF），以及該AEP包括一引導伺服器功能（BSF）。

16．如申請專利範圍第12項所述的方法，其中該網路實施一通用引導架構（GBA）和一OpenID聯合識別碼管理架構，並且其中該AEP包括一網路存取功能（NAF）和一識別碼提供者（IdP）。

17．如申請專利範圍第15項所述的方法，該方法更包括：

經由該NAF接收包括一領域屬性的一引導發起訊息，以觸發該UE使用該選取的認證協定及/或證書來運行一引導協定。

18．如申請專利範圍第15項所述的方法，該方法更包括在該

UE處：

向該NAF提供一指示，該指示表明由該UE支援一個或多個GBA認證協定；以及

從該NAF接收該一個或多個GBA認證協定中的一者可接受的一指示，其中該可接受的GBA認證協定包括一基於SIP摘錄的GBA安全關聯。

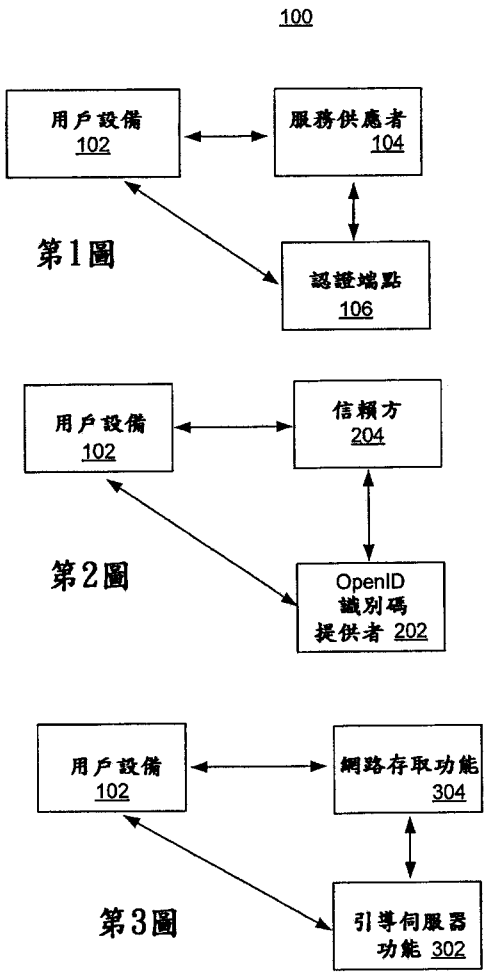
19．如申請專利範圍第17項所述的方法，該方法更包括：

如果由該UE支援的該一個或多個GBA認證協定中沒有GBA認證協定是該NAF可接受的，則在該UE處接收一錯誤訊息，從而終止GBA引導。

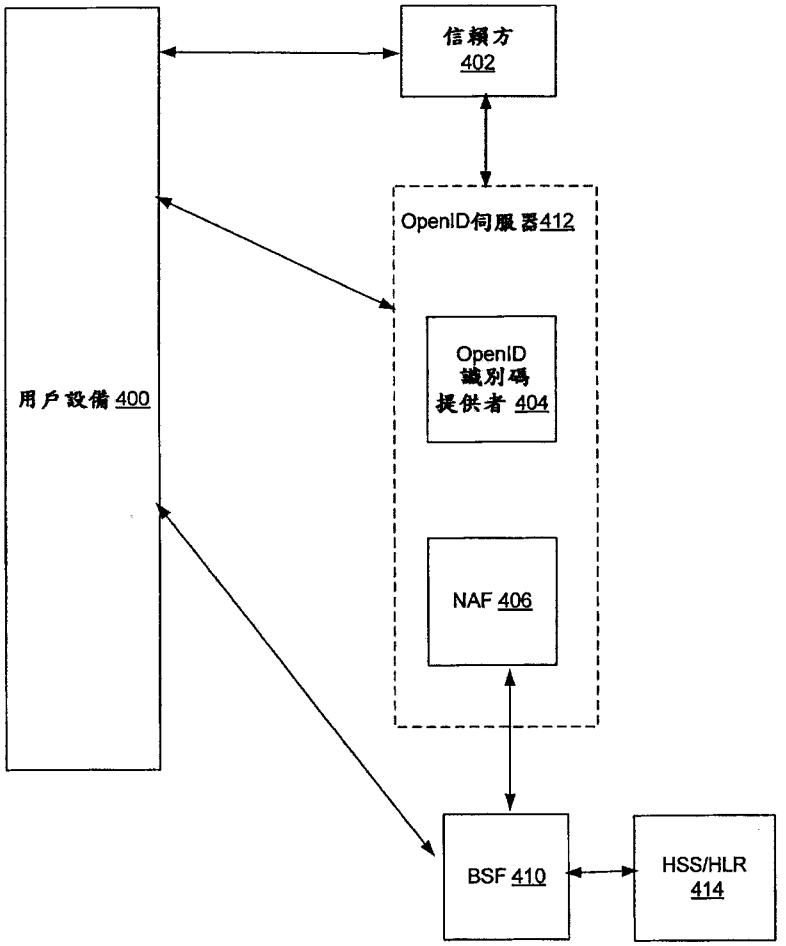
20．如申請專利範圍第18項所述的方法，其中用於存取一服務的該請求在一用戶代理標頭中包括一產品訊標，其中該產品訊標指明該UE請求使用一GBA摘錄協定。

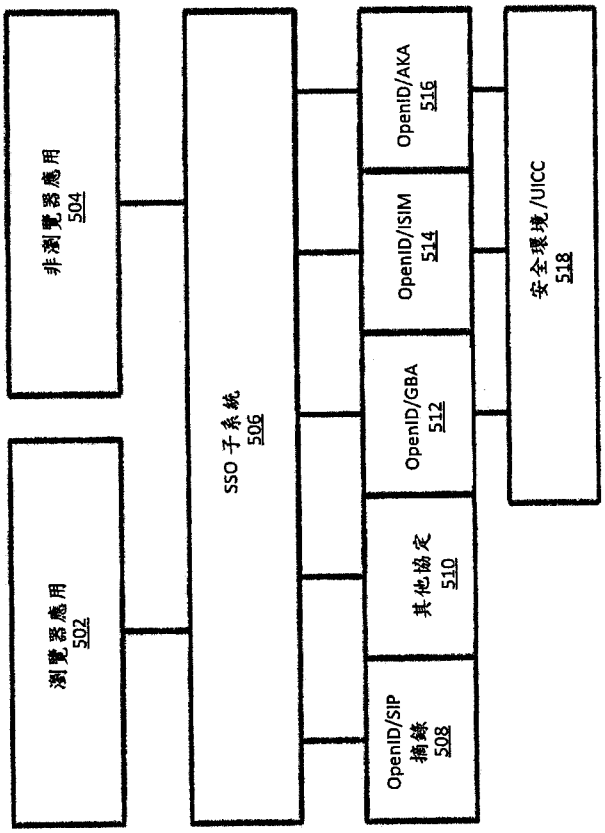
21．如申請專利範圍第20項所述的方法，其中回應於用於存取的該請求，接收一碼401回應，其中該碼401回應在一標頭中包括一前綴，其中該前綴指明該UE被允許執行該GBA摘錄協定。

八、圖式：

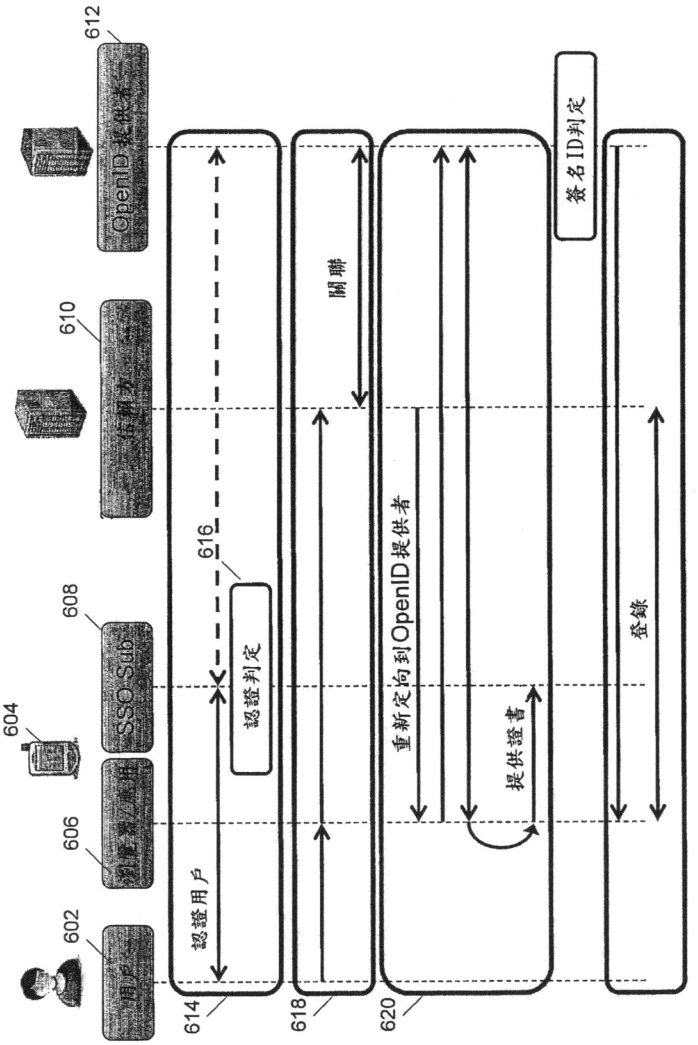

100
用戶設備
102
服務供應者
104
認證端點
106
第1圖
用戶設備
102
信賴方
204
OpenID
識別碼
提供者 202
第2圖
用戶設備
102
網路存取功能
304
引導伺服器
功能 302
第3圖

第4圖

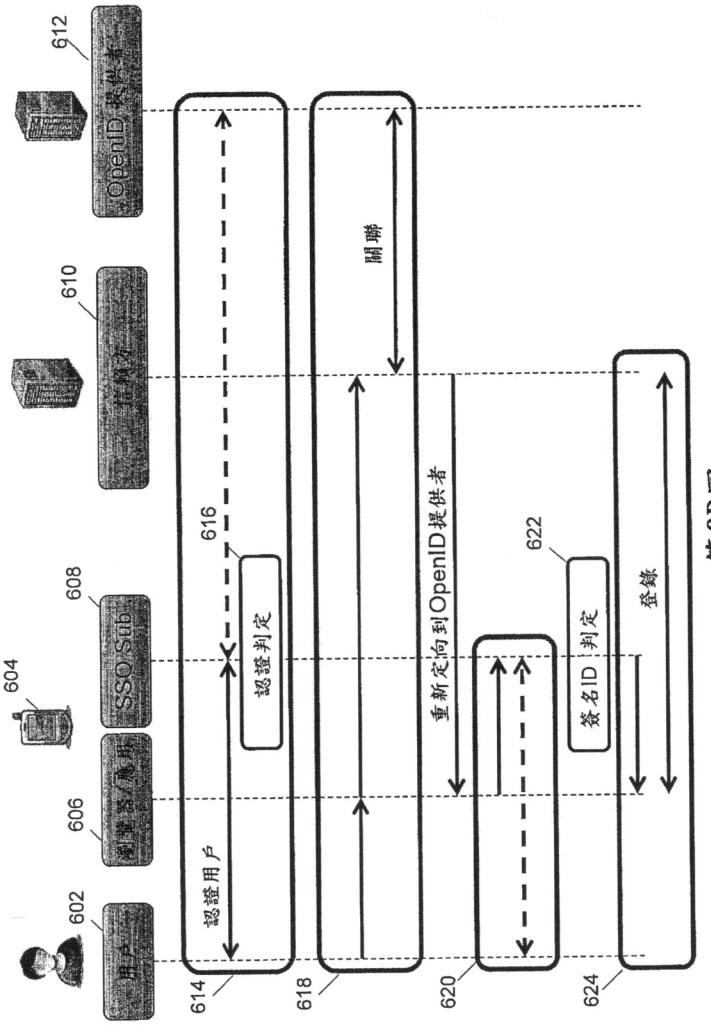

信賴方
402
OpenID伺服器412
OpenID
識別碼
提供者 404
用戶設備 400
NAF 406
BSF 410
HSS/HLR
414


非瀏覽器應用
504
瀏覽器應用
502
SSO 子系統
506
OpenID/AKA
516
OpenID/ISIM
514
OpenID/GBA
512
其他協定
510
OpenID/SIP
摘錄
508
安全環境/UICC
518

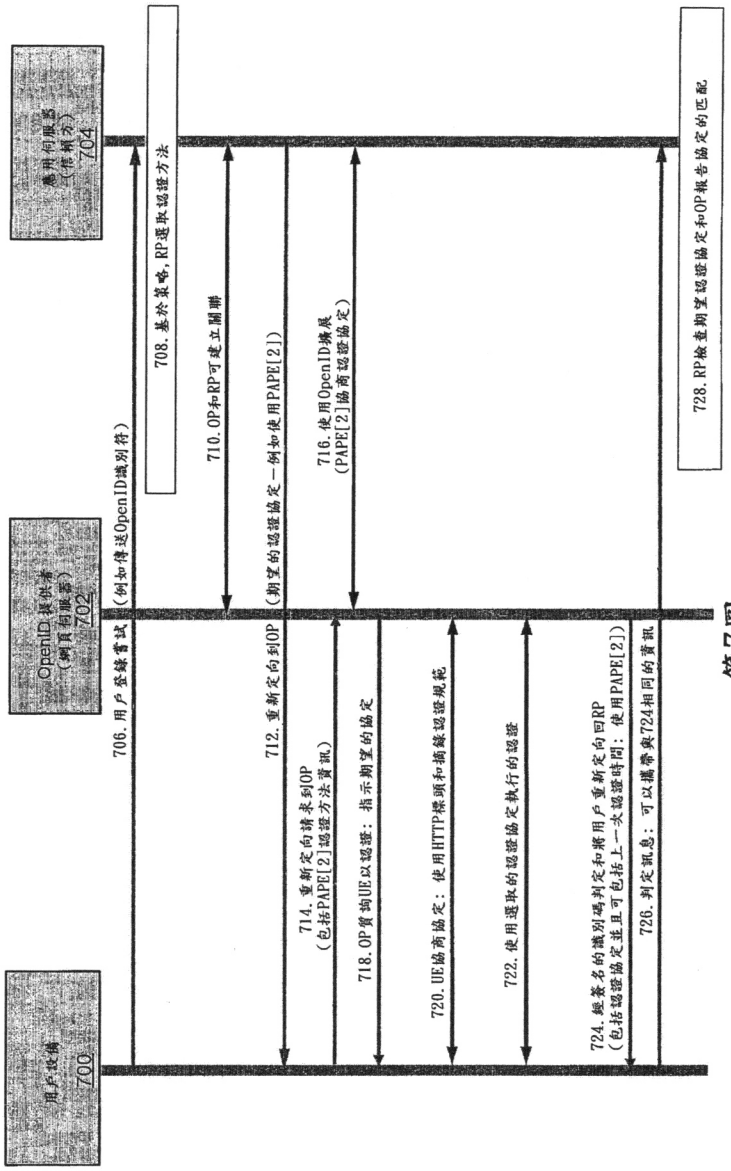
第5圖


612
OpenID 提供者
610
信賴方
608
SSO Stub
604
606
602
用戶
認證用戶
616
認證判定
614
閒聊
618
重新定向到OpenID提供者
提供證書
620
簽名ID判定
登錄

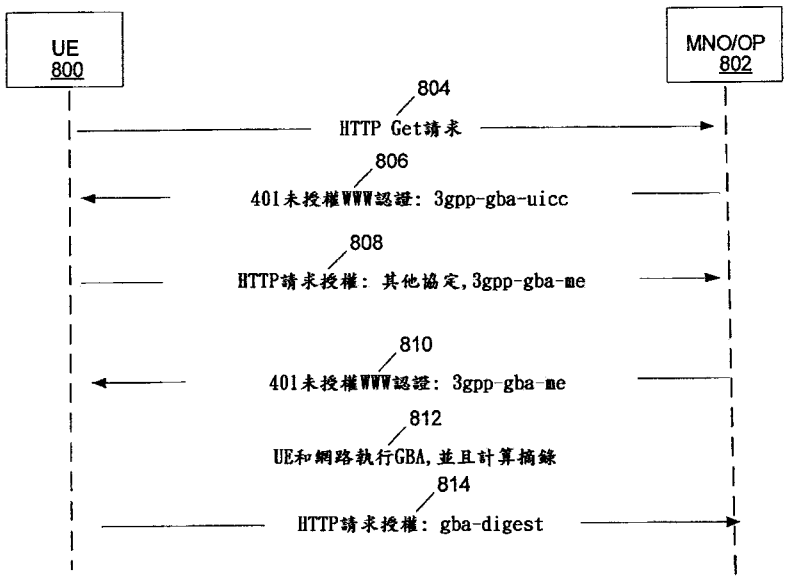
第6A圖


612
OpenID 提供者
610
608
SSO Sub
604
606
602
用戶
認證用戶
614
616
認證判定
618
關聯
重新定向到OpenID提供者
620
622
簽名ID 判定
624
登錄

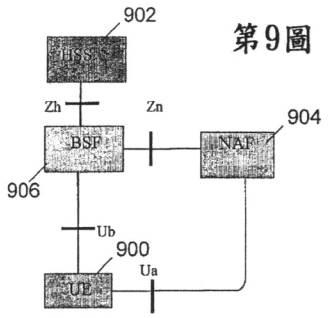
第6B圖


用戶收情
700
OpenID 提供者
(網頁伺服器)
702
應用伺服器
(信賴方)
704
706. 用戶登錄嘗試
(例如傳送OpenID識別符)
708. 基於策略, RP選取認證方法
710. OP和RP可建立關聯
(期望的認證協定－例如使用PAPE[2])
712. 重新定向到OP
714. 重新定向請求到OP
(包括PAPE[2]認證方法資訊)
716. 使用OpenID模具
(PAPE[2]協商認證協定)
718. OP質詢UE以認證：指示期望的協定
720. UE協商協定：使用HTTP標頭和摘錄認證規範
722. 使用選取的認證協定執行的認證
724. 經簽名的識別碼判定和將用戶重新定向回RP
(包括認證協定並且可包括上一次認證時間：使用PAPE[2])
726. 判定訊息：可以攜帶與724相同的資訊
728. RP檢查期望認證協定和OP報告協定的匹配

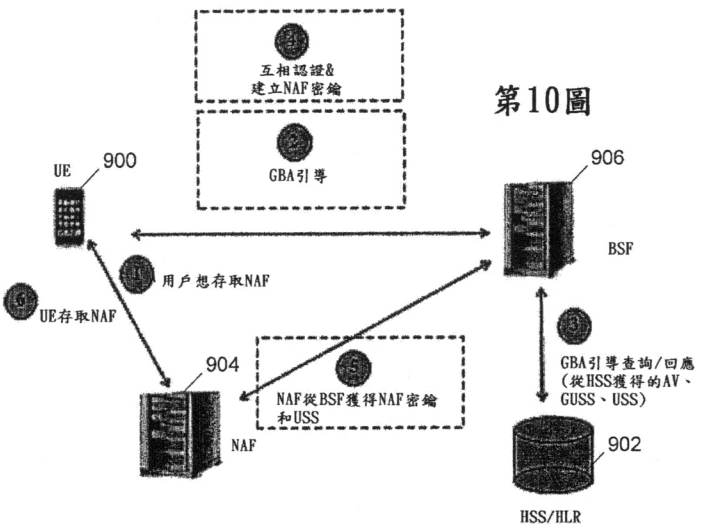
第7圖


UE
800
MNO/OP
802
804
HTTP Get請求
806
401未授權WWW認證: 3gpp-gba-uicc
808
HTTP請求授權: 其他協定,3gpp-gba-me
810
401未授權WWW認證: 3gpp-gba-me
812
UE和網路執行GBA,並且計算摘錄
814
HTTP請求授權: gba-digest

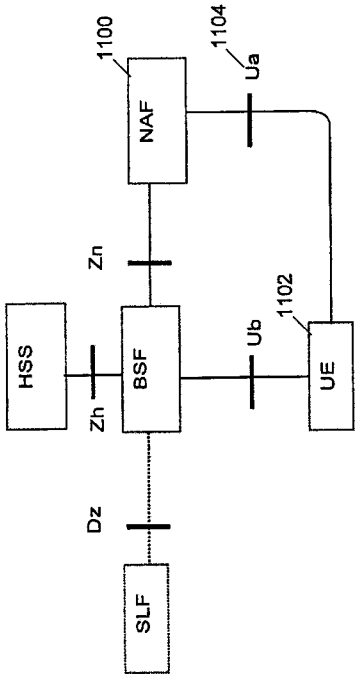
第8圖


902
HSS
Zh
Zn
904
BSF
NAF
906
Ub
900
Ua
UE

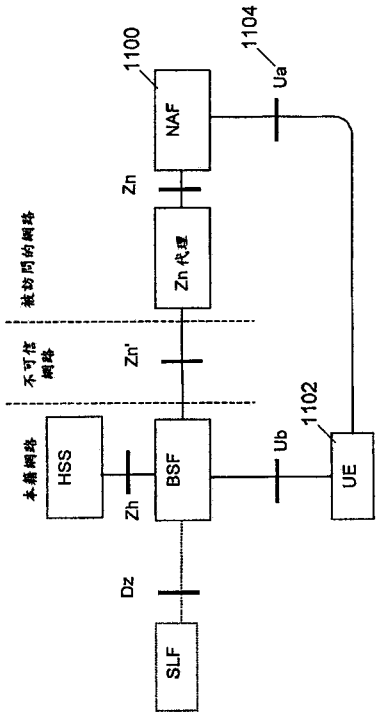
第9圖


互相認證&
建立NAF密鑰
GBA引導
UE
900
906
BSF
用戶想存取NAF
UE存取NAF
904
NAF從BSF獲得NAF密鑰
和USS
NAF
GBA引導查詢/回應
(從HSS獲得的AV、
GUSS、USS)
902
HSS/HLR

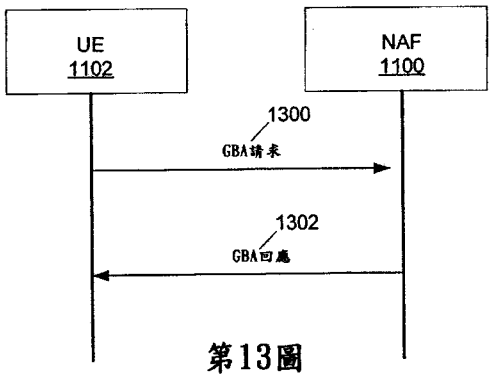
第10圖



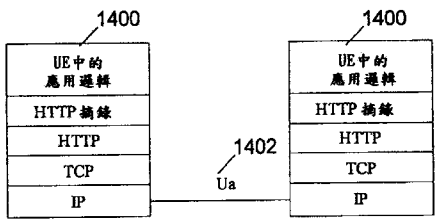
第11圖


1100
NAF
1104
Ua
Zn
Zn代理
被訪問的網絡
不可信網絡
Zn'
1102
本籍網絡
HSS
Zh
BSF
Ub
UE
Dz
SLF

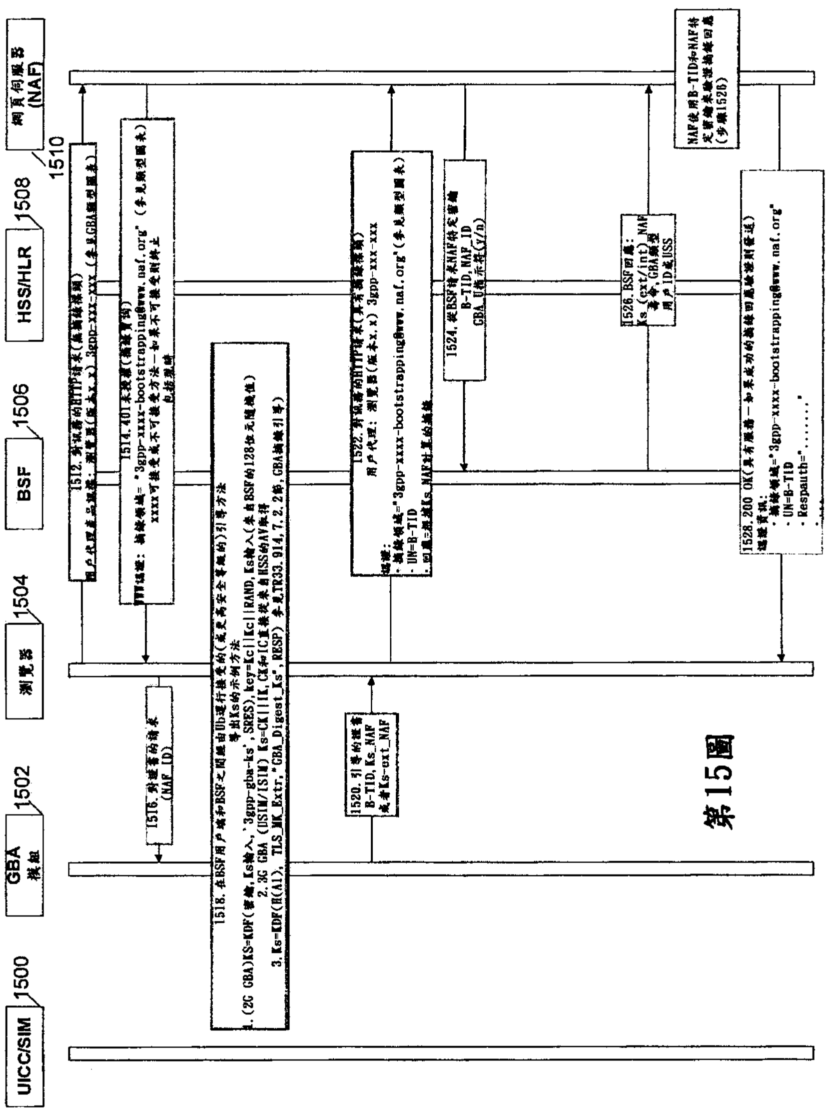
第12圖


UE
1102
NAF
1100
1300
GBA請求
1302
GBA回應

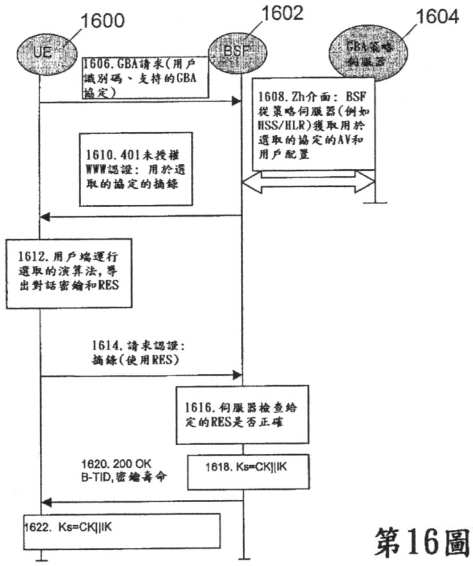
第13圖


1400
UE中的
應用邏輯
HTTP摘錄
HTTP
TCP
IP
1402
Ua
1400
UE中的
應用邏輯
HTTP摘錄
HTTP
TCP
IP

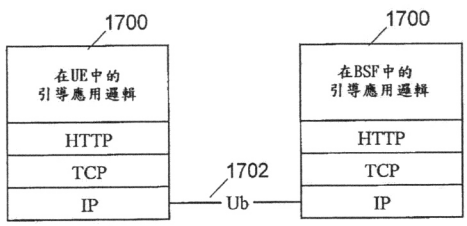
第14圖


UICC/SIM
1500
GBA 模組
1502
瀏覽器
1504
BSF
1506
HSS/HLR
1508
網頁伺服器 (NAF)
1510

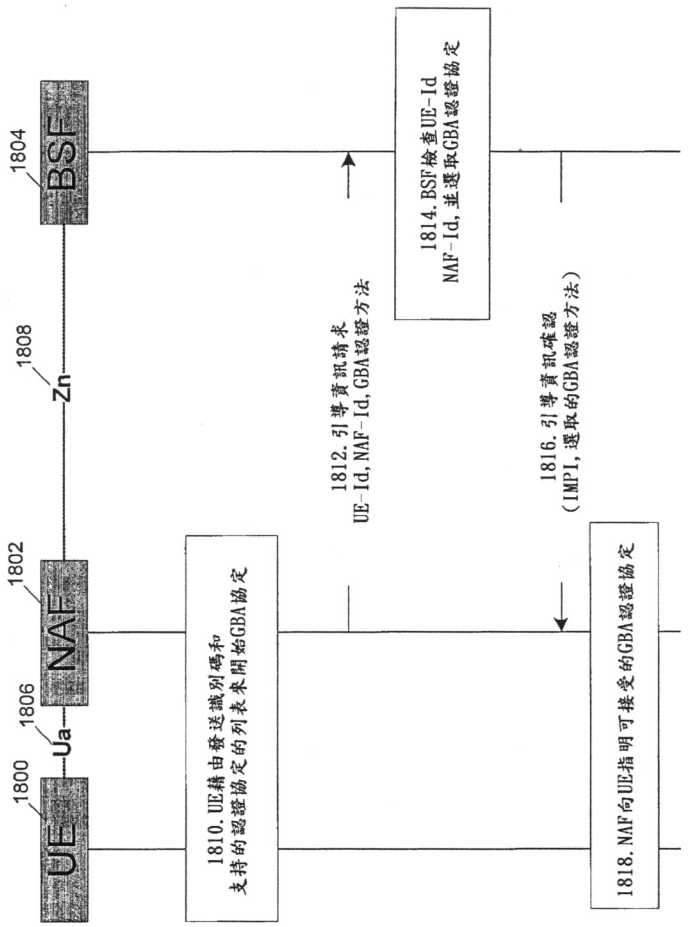
第15圖


1600
1602
1604
UE
BSF
1606. GBA請求(用户識別碼、支持的GBA協定)
1608. Zh介面：BSF從策略伺服器(例如HSS/HLR)獲取用於選取的協定的AV和用户配置
1610. 401未授權WWW認證：用於選取的協定的摘錄
1612. 用户端運行選取的演算法，導出對話密鑰和RES
1614. 請求認證：摘錄(使用RES)
1616. 伺服器檢查給定的RES是否正確
1618. Ks=CK||IK
1620. 200 OK B-TID,密鑰壽命
1622. Ks=CK||IK

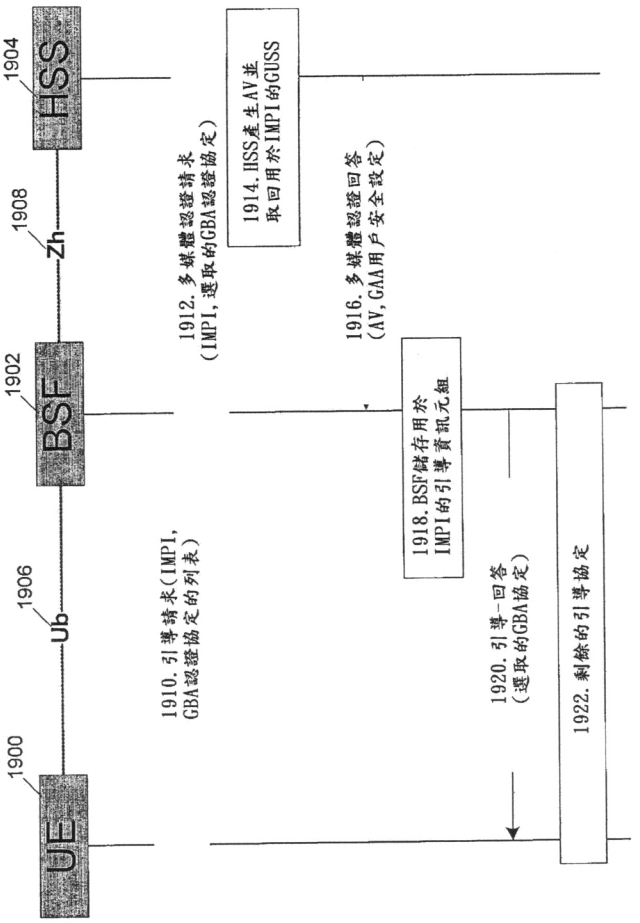
第16圖


1700
1700
在UE中的引導應用邏輯
在BSF中的引導應用邏輯
HTTP
TCP
IP
1702
Ub
HTTP
TCP
IP

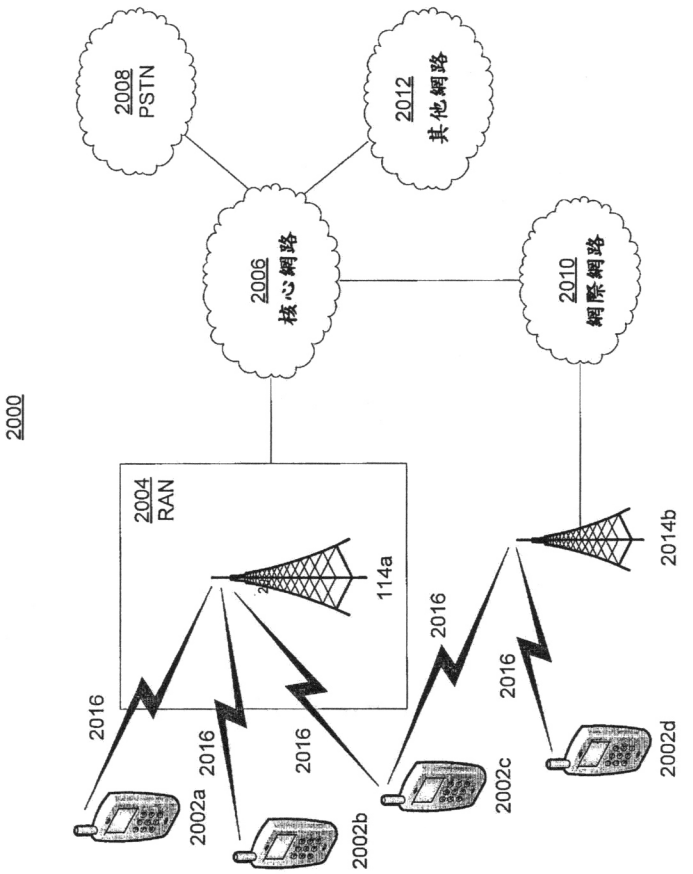
第17圖


1800
UE
1806
Ua
1802
NAF
1808
Zn
1804
BSF
1810. UE藉由發送識別碼和
支持的認證協定的列表來開始GBA協定
1812. 引導資訊請求
UE-Id, NAF-Id, GBA認證方法
1814. BSF檢查UE-Id
NAF-Id, 並選取GBA認證協定
1816. 引導資訊確認
(IMPI, 選取的GBA認證方法)
1818. NAF向UE指明可接受的GBA認證協定

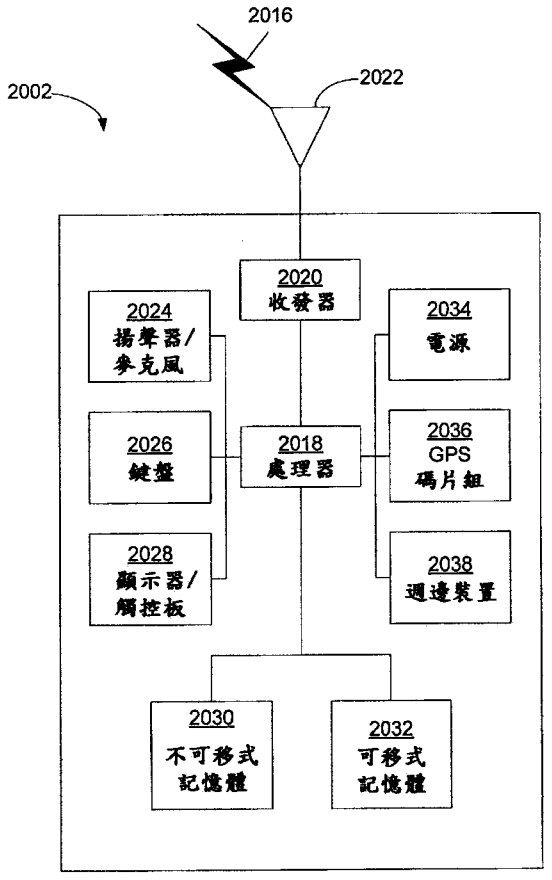
第18圖


1900
UE
1906
Ub
1902
BSF
1908
Zh
1904
HSS
1910. 引導請求(IMPI, GBA認證協定的列表)
1912. 多媒體認證請求 (IMPI, 選取的GBA認證協定)
1914. HSS產生AV並 取回用於IMPI的GUSS
1916. 多媒體認證回答 (AV, GAA用戶安全設定)
1918. BSF儲存用於 IMPI的引導資訊元組
1920. 引導-回答 (選取的GBA協定)
1922. 剩餘的引導協定

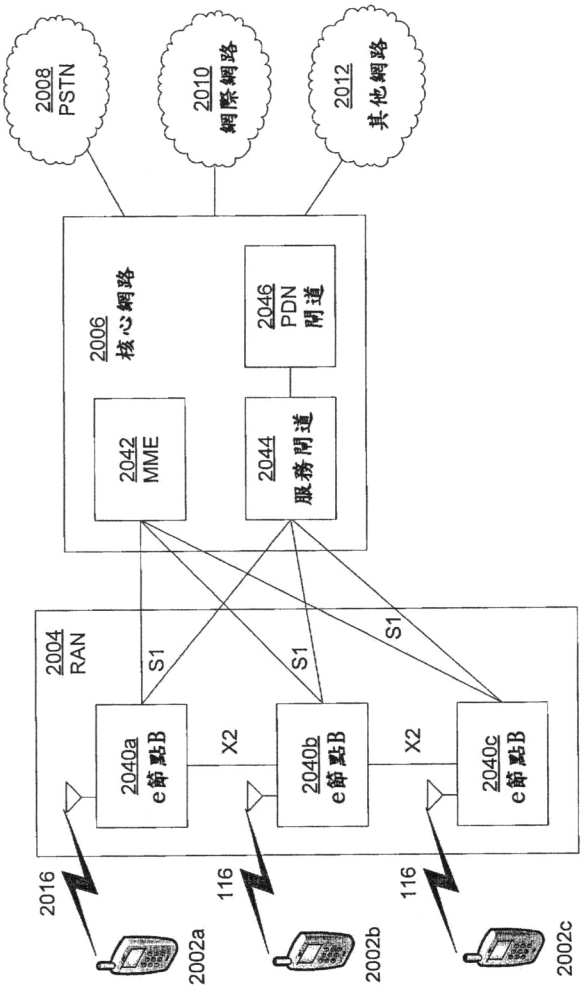
第19圖


2000
2008 PSTN
2012 其他網路
2006 核心網路
2010 網際網路
2004 RAN
114a
2014b
2016
2002a
2002b
2002c
2002d

第20A圖


2016
2022
2002
2020
收發器
2024
揚聲器/
麥克風
2034
電源
2026
鍵盤
2018
處理器
2036
GPS
碼片組
2028
顯示器/
觸控板
2038
週邊裝置
2030
不可移式
記憶體
2032
可移式
記憶體

第20B圖


2008
PSTN
2010
網際網路
2012
其他網路
2006
核心網路
2042
MME
2044
服務閘道
2046
PDN
閘道
2004
RAN
S1
S1
S1
2040a
e節點B
2040b
e節點B
2040c
e節點B
X2
X2
2016
116
116
2002a
2002b
2002c

第20C圖