I514896

(19)中華民國智慧財產局

(12)發明說明書公告本 **(11)證書號數：TW I514896 B**

(45)公告日： 中華民國 104 (2015) 年 12 月 21 日

(21)申請案號：100104273 (22)申請日： 中華民國 100 (2011) 年 02 月 09 日

(51)Int. Cl.： *H04W12/06 (2009.01)* *H04L29/06 (2006.01)*
G06F21/00 (2013.01)

(30)優先權：2010/02/09 美國 61/302,890
2010/05/28 美國 61/396,602

(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)；史密特 安德魯斯 SCHMIDT, ANDREAS (DE)；萊赫 安德魯斯 LEICHER, ANDREAS (DE)；夏 尤根德拉 SHAH, YOGENDRA C. (GB)；顧吉恩 路易斯 GUCCIONE, LOUIS J. (US)；和特 多洛莉絲 HOWRY, DOLORES F. (US)

(74)代理人：蔡清福

(56)參考文獻：

US 2001/0045451A1 US 2006/0155993A1
US 2007/0056025A1

審查人員：黃冠霖

申請專利範圍項數：47 項 圖式數：42 共 174 頁

(54)名稱

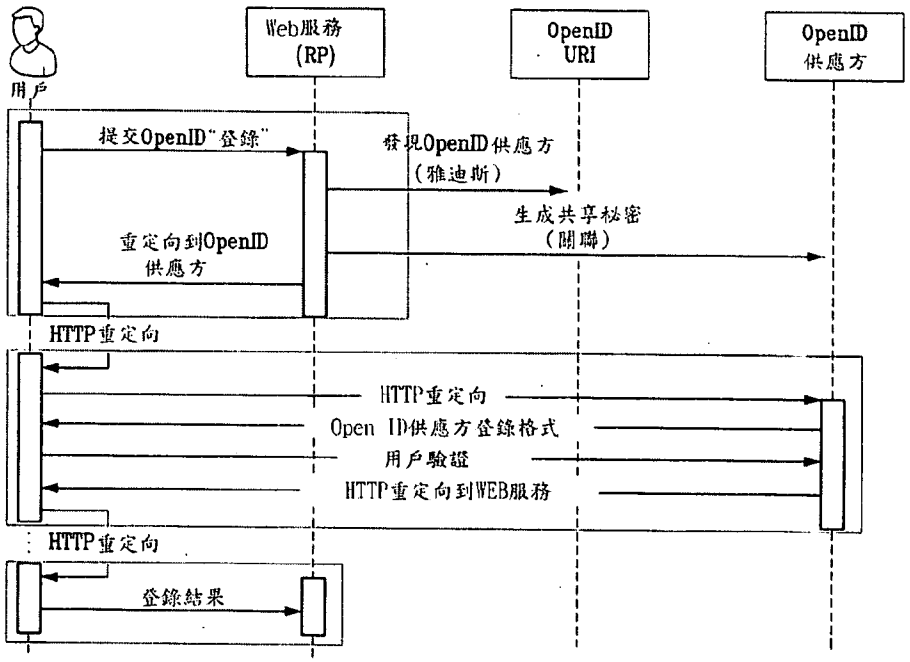
可信賴聯合身份方法及裝置

METHOD AND APPARATUS FOR TRUSTED FEDERATED IDENTITY

(57)摘要

諸如智慧卡、UICC、Java 卡、全球平臺等可信計算環境可以被用作本地主機信任中心和單點登錄(Single Sign-On，SSO)供應方的代理。而這稱為本地 SSO 供應方(OP)。舉例來說，通過執行該處理，可以將驗證業務量保持在本地，並且避免可能對營運商網路造成負擔的空中傳送通信。為了在可信環境中建立 OP 代理，可信環境可以採用多種方式來綁定到 SSO 供應方。例如，SSO 供應方可以與基於 UICC 的 UE 驗證或 GBA 交互操作。這樣一來，使用者設備可以平衡可信環境，以便提供提升的安全性，以及減小 OP 或營運商網路上的空中傳送通信及驗證負擔。

A trusted computing environment, such as a smartcard, UICC, Java card, global platform, or the like may be used as a local host trust center and a proxy for a single-sign on (SSO) provider. This may be referred to as a local SSO provider (OP). This may be done, for example, to keep authentication traffic local and to prevent over the air communications, which may burden an operator network. To establish the OP proxy in the trusted environment, the trusted environment may bind to the SSO provider in a number of ways. For example, the SSO provider may interoperate with UICC-based UE authentication or GBA. In this way, user equipment may leverage the trusted environment in order to provide increased security and reduce over the air communications and authentication burden on the OP or operator network.



第 3 圖

HTTP、HTTPS・・・通信協議

OpenID・・・開放ID

RP・・・可依賴方

web・・・網路

I514896
專利案號：100104273

104年 08月 28日 修正替換頁

申請日： 100年02月09日
IPC分類： H04W 12/06 (2009.01)
H04L 29/06 (2006.01)
G06F 21/00 (2013.01)

公告本

【發明摘要】

【中文發明名稱】 可信賴聯合身份方法及裝置

【英文發明名稱】 Method And Apparatus For Trusted Federated Identity

【中文】

諸如智慧卡、UICC、Java卡、全球平臺等可信計算環境可以被用作本地主機信任中心和單點登錄（Single Sign-On，SSO）供應方的代理。而這稱爲本地SSO供應方（OP）。舉例來說，通過執行該處理，可以將驗證業務量保持在本地，並且避免可能對營運商網路造成負擔的空中傳送通信。爲了在可信環境中建立OP代理，可信環境可以採用多種方式來綁定到SSO供應方。例如，SSO供應方可以與基於UICC的UE驗證或GBA交互操作。這樣一來，使用者設備可以平衡可信環境，以便提供提升的安全性，以及減小OP或營運商網路上的空中傳送通信及驗證負擔。

【英文】

A trusted computing environment, such as a smartcard, UICC, Java card, global platform, or the like may be used as a local host trust center and a proxy for a single-sign on (SSO) provider.This may be referred to as a local SSO provider (OP).This may be done, for example, to keep authentication traffic local and to prevent over the air communications, which may burden an operator network.To establish the OP proxy in the trusted environment,the trusted environment may bind to the SSO provider in a number of ways.For example, the SSO provider may interoperate with UICC-based UE authentication or GBA.In this way, user equipment may leverage the trusted environment in order to provide increased security and reduce over the air communications and authentication burden on the OP or operator network.

【指定代表圖】 第3圖

【代表圖之符號簡單說明】

HTTP、HTTPS　通信協議

OpenID　開放ID

RP　可依賴方

web　網路

【特徵化學式】

【發明說明書】

【中文發明名稱】 可信賴聯合身份方法及裝置

【英文發明名稱】 Method And Apparatus For Trusted Federated Identity

【技術領域】

【0001】 本申請要求根據2010年5月28日申請的名稱爲“Identity Management on a Communications Device（通信設備上的標識管理）”的申請號爲61/396,602的美國臨時專利申請以及2010年2月9日申請的名稱爲“Method and Apparatus for Implementing Local and Mobile OpenID Provider（用於實現本地和行動OpenID供應方的方法和設備）”的申請號爲61/302,890的美國臨時專利申請而享有優先權，其中這些申請的內容在這裏全部引入作爲參考。

【先前技術】

【0002】 網際網路使用者通常具有多個可以用於使用者驗證的使用者名稱和密碼，以便存取多個網站。例如，網際網路使用者可以具有用於存取Facebook之類的社交網站的使用者名稱/密碼組合，以及另一個用於存取諸如Gmail之類的電子郵件站點的使用者名稱/密碼組合。雖然具有多個使用者名稱/密碼組合有可能是使用者驗證所必需的，但是網際網路使用者可能會發現，要想記憶每一個使用者名稱/密碼組合是很麻煩的。例如，網際網路使用者有可能遺忘其在某個網站的使用者名稱/密碼組合，並且無法存取該網站。爲使網際網路使用者的使用者驗證不再那麼麻煩，目前已經提出了諸如OpenID之類的單點登錄（SSO）解決方案。但是，在將SSO作爲網路（web）服務實施的時候存在著一些缺陷。例如，使用者有可能不具有連至基於web的SSO供應方的安全頻道。此外，使用者對SSO供應方的控制有可能是

很有限的。

此外，SSO中的驗證有可能產生經由空中介面的通信，這樣則有可能因爲業務量增大而對網路實體（即OpenID（開放ID）供應方（OP或NAF）以及網路本身產生負擔。另外，行動網路營運商（MNO）可能不得不承擔這個額外業務量和處理的成本。

【發明內容】

【0003】 在本申請中，我們描述了允許在可信環境中實現本地和分散式單點登錄（SSO）供應方的實施方式，所述可信環境例如智慧卡、無線智慧型電話、H(e)NB或其他類型的設備。單點登錄供應方可以是OpenID供應方、自由聯盟供應方、開放認證（OAUTH）供應方等等。本申請提供了很多不同方案及其實施選項的集合。雖然這些描述的概念有可能是在OpenID協議的上下文中，但是這些想法可以擴展到其他的單點登錄（SSO）協定和/或聯合標識協定。

在一個示例實施方式中，使用者環境可用於啓用開放管理安全協定，以使可依賴方（RP）能對使用者進行驗證。該使用者環境可以包括：

使用者介面，該使用者介面使用單點登錄安全協議來與RP進行通信，以便代表使用者來請求存取RP提供的服務，其中RP可以處於使用者環境之外，並且可以與單點登錄證書的可信供應方進行通信，以便起動使用者驗證；以及

處理器，例如可信的計算環境，其在使用者環境內部爲可信供應方驗證使用者，該處理器被配置成在本地執行單點登錄證書的可信供應方的至少一些功能，以便在驗證過程中限制使用者環境以外的通信。

在另一個示例實施方式中，可使用一種方法來保護使用者環境和/或本地斷言（assertion）供應方（LAP），以便在OpenID之類的開放管理安全協議中爲可依賴方驗證使用者。該方法可以包括：

經由使用者介面接收來自RP且表明RP希望對使用者進行驗證的重定向（redirect），該RP能夠與諸如OpenID供應方（OP）之類的單點登錄（SSO）證書的可信供應方進行通信；

通過使用者介面接收來自使用者的使用者證書；

使用接收到的使用者證書來爲RP驗證使用者，以便在本地執行諸如OP之類的SSO證書的可信供應方的至少一些功能，從而在驗證過程中限制使用者環境以外的通信；以及

經由使用者介面來將驗證回應傳送到RP。

本概述是爲了以簡化形式引入眾多概念而被提供的，並且在以下的詳細描述中將會進一步描述這些概念。本概述的目的並不是標識所要求保護的主題的關鍵特徵或基本特徵，也不是用於限制所要求保護的主題的範圍。此外，所要求保護的主題並不受限於那些解決了在本公開的任何部分中指出的任一或所有缺點的實施方式。

附圖說明

更詳細的理解可以從以下結合附圖並借助示例給出的描述中得到，其中：

第1A圖顯示的是可以實施所公開的一個或多個實施方式的示例通信系統。

第1B圖顯示的是可以實施所公開的一個或多個實施方式的示例無線傳輸/接收單元。

第1C圖顯示的是可以實施所公開的一個或多個實施方式的示例系統無線電存取網路。

第2圖顯示的是在標識供應方與服務供應方之間用於交換驗證和資料的SAML協定流程。

第3圖顯示的是允許使用者使用單個IP登錄到不同可依賴方站點的OpenID協定流程。

第4圖顯示的是在可信計算環境上提供具有的集成OP的SSO協定的協定流程

的示例實施方式。

第5圖顯示的是在可信計算環境上提供具有集成OP的SSO協定的協定流程的示例實施方式。

第6圖顯示的是用於以關聯爲基礎的通信的OpenID協定流程。

第7圖顯示的是用於無狀態簽名核驗的OpenID協定流程。

第8圖顯示的是將BONDI與基於關聯的OpenID相集成的示例實施方式。

第9圖顯示的是將BONDI與無狀態簽名核驗相集成的示例實施方式。

第10圖顯示的是啓用分離（split）OP的示例實施方式。

第11圖顯示的是啓用分離OP的另一個示例實施方式。

第12圖顯示的是在GBA架構中使用的BSF功能。

第13圖顯示的是GBA架構概述。

第14圖顯示的是源自3GPP TS 33.220的GBA參考模組。

第15圖顯示的是源自3GPP TS 33.220的用於被存取網路NAF的GBA參考模組。

第16圖顯示的是用於自由（Liberty）/GBA的架構方案。

第17圖顯示的是供用於MMO支援的標識斷言的GBA使用的示例實施方式。

第18圖顯示的是啓用分離OP的另一個示例實施方式。

第19圖顯示的是啓用分離終端/本地OpenId的示例實施方式。

第20圖顯示的是標準的OpenID協定。

第21圖顯示的是來自3GPP TR 33.924 v9.1.0的OpenID/GBA的業務流程。

第22圖顯示的是減小空中傳送業務量的協定流程的示例實施方式。

第23圖顯示的是用於SCWS上的OP的內部路由的示例實施方式。

第24圖顯示的是允許RP使用無狀態模式來執行OpenID驗證的協定流程的示例實施方式。

第25圖顯示的是允許RP使用基於關聯的模式來執行OpenID使用者驗證的協定流程的示例實施方式。

第26圖顯示的是用於改進的無狀態模式的協定流程的示例實施方式。

第27圖顯示的是用於改進的基於關聯的模式的協定流程的示例實施方式。

第28圖顯示的是源自NIST-FIPS PUB 198-1的鍵入式散列（hash）消息驗證碼（HMAC）。

第29圖顯示的是OpenID/GBA的業務流程。

第30圖顯示的是用於基於關聯的通信模式的協定流程的另一個示例實施方式。

第31圖顯示的是用於基於關聯的通信模式的協定流程的另一個示例實施方式。

第32圖顯示的是用於基於關聯的通信模式的協定流程的另一個示例實施方式。

第33圖顯示的是用於無狀態模式的協定流程的另一個示例實施方式。

第34圖顯示的是用於分離終端的協定流程的示例實施方式。

第35圖顯示的是OpenID中的信任關係。

第36圖顯示的是與本地OP的信任關係的示例實施方式。

第37圖顯示的是與MNO的信任關係的示例實施方式。

第38圖顯示的是具有發佈方SD的SD分層的示例實施方式。

第39圖顯示的是具有DM的SD分層的示例實施方式。

第41圖顯示的是作爲GP應用的SCWS的示例實施方式。

第42圖顯示的是在卡的運行時間環境中實施的SCWS的示例實施方式。

【圖式簡單說明】

【0004】 更詳細的理解可以從以下結合附圖並借助示例給出的描述中得到，其中：

第1A圖示出的是可以實施所公開的一個或多個實施方式的例示通信系統。

第1B圖示出的是可以實施所公開的一個或多個實施方式的例示無線發射/接收單元。

第1C圖示出的是可以實施所公開的一個或多個實施方式的例示系統無線電接入網路。

第2圖示出的是在識別供應方與服務供應方之間交換驗證和資料的SAML協定流程。

第3圖示出的是允許使用者使用單個IP登錄到不同可依賴方站點的OpenID協定流程。

第4圖示出的是爲SSO協定提供可信計算環境上的集成OP的協定流程的例示實施方式。

第5圖示出的是爲SSO協定提供可信計算環境上的集成OP的協定流程的例示實施方式。

第6圖示出的是用於以關聯爲基礎的通信的OpenID協定流程。

第7圖示出的是用於無狀態簽名核驗的OpenID協定流程。

第8圖示出的是將BONDI與基於關聯的OpenID相集成的例示實施方式。

第9圖示出的是將BONDI與無狀態簽名核驗相集成的例示實施方式。

第10圖示出的是啓用拆分（split）OP的例示實施方式。

第11圖示出的是啓用拆分OP的另一個例示實施方式。

第12圖示出的是在GBA架構中使用的BSF功能。

第13圖示出的是GBA架構概述。

第14圖示出的是源自3GPP TS 33.220的GBA參考模組。

第15圖示出的是源自3GPP TS 33.220的關於被存取網路的NAF參考模組。

第16圖示出的是用於自由（Liberty）/GBA的架構方案。

第17圖示出的是供用於MMO支援的識別斷言的GBA使用的例示實施方式。

第18圖示出的是啓用拆分OP的另一個例示實施方式。

第19圖示出的是啓用拆分終端/本地OpenId的例示實施方式。

第20圖示出的是標準的OpenID協定。

第21圖示出的是來自3GPP TR 33.924 v9.1.0的OpenID/GBA的業務流程。

第22圖示出的是減小空中傳送業務量的協定流程的例示實施方式。

第23圖示出的是用於SCWS上的OP的內部路由的例示實施方式。

第24圖示出的是允許RP使用無狀態模式來執行OpenID驗證的協定流程的例示實施方式。

第25圖示出的是允許RP使用基於關聯的模式來執行OpenID使用者驗證的協定流程的例示實施方式。

第26圖示出的是用於改進的無狀態模式的協定流程的例示實施方式。

第27圖示出的是用於改進的基於關聯的模式的協定流程的例示實施方式。

第28圖示出的是源自NIST-FIPS PUB 198-1的鍵入式散列（hash）消息驗證碼（HMAC）。

第29圖示出的是OpenID/GBA的業務流程。

第30圖示出的是用於基於關聯的通信模式的協定流程的另一個例示實施方式。

第31圖示出的是用於基於關聯的通信模式的協定流程的另一個例示實施方式。

第32圖示出的是用於基於關聯的通信模式的協定流程的另一個例示實施方式。

第33圖示出的是用於無狀態模式的協定流程的另一個例示實施方式。

第34圖示出的是用於拆分終端的協定流程的例示實施方式。

第35圖示出的是OpenID中的信任關係。

第36圖示出的是與本地OP的信任關係的例示實施方式。

第37圖示出的是與MNO的信任關係的例示實施方式。

第38圖示出的是具有發佈方SD的SD分層的例示實施方式。

第39圖示出的是具有DM的SD分層的例示實施方式。

第41圖示出的是作爲GP應用的SCWS的例示實施方式。

第42圖示出的是在卡的運行時間環境中實施的SCWS的例示實施方式。

【實施方式】

【0005】 在本申請中，我們描述了在可信計算環境，例如使用者設備（UE）、智慧卡、智慧型電話、H(e)NB或其他類型的設備中實施的本地和分散式單點登錄（SSO）供應方的思想和概念。所述單點登錄供應方可以是OpenID供應方、自由聯盟供應方、開放驗證（OAUTH）供應方等等。本申請提供了很多不同的方案及其實施選項。雖然這些概念有可能是在OpenID協議的上下文中描述的，但是這些思想可以擴展到其他的單點登錄（SSO）協定和/或聯合標識協定。

諸如本地行動OpenID之類的本地行動SSO協議是允許位於本地的模組或實體來執行作爲諸如OpenID協定之類的SSO或標識管理協定的一部分的標識驗證/斷言功能的概念。位於本地的模組可以是智慧卡、SIM、UICC、Java卡、啓用智慧卡web伺服器（SCWS）的智慧卡、智慧型電話之類的無線設備等等。

本地行動SSO是用於統指那些可以藉以將部分或是所有那些通常由基於web的SSO伺服器執行的單點登錄（single sign-on，SSO）及相關標識管理功能改由基於本地的實體和/或模組執行的方法的術語，其中所述實體和/或模組是通信設備本身的一部分或是全部，或者此類實體/模組在物理和/或邏輯上位於通信設備和/或其使用者附近（也就是位於本地）。例如，實體/模組可以嵌入到設備中；附著到設備；或者通過本地介面、線路或短距離無線裝置連接到設備。

本地OpenID也可以用作術語來指示本地行動SSO方法的子集，由此，所述SSO或標識管理方法是以OpenID協議爲基礎的。例如，本地OpenID可以用於指示那些可以由位於本地的實體/模組執行的OpenID標識供應方（簡寫成OP或OpenID IdP）的功能。

本地IdP是用於指示執行了OpenID伺服器的功能的實體或模組的術語。字首組合詞OPloc可以用於表示本地IdP。本地IdP的一個主要功能可以是通過關於使用者和/或設備標識的一個或多個斷言來促成使用者和/或設備的驗證。這種斷言可以從本地IdP發送到在設備上運行的瀏覽器代理（BA），然後，瀏覽器代理可以將該斷言轉發給外部的可依賴方（RP）。如果將本地IdP提供的一種或多種功能限制成提供這種標識斷言，那麼可以將本地IdP稱爲本地斷言供應方（LAP）。

本地IdP可以處理、創造、管理或者發送斷言消息至一個或多個外部接收方。這些斷言消息可以斷言與使用者和/或設備相關的一個或多個標識的核驗狀態。例如在OpenID協議中，稱爲可依賴方（RP）的第三方實體可以是斷言消息的接收方之一。本地IdP還可以使用簽名、加密密鑰、密碼等等來對斷言消息進行簽名。

本地OpenID方法可以使用一個或多個密碼密鑰，例如根會話密鑰。根會話密鑰可以用Krp來表示，並且可以是在RP與OP之間要使用的會話密鑰。Krp還可以充當RP與能夠得到其他密鑰的OP之間的根會話密鑰。本地OpenID方法還可以使用斷言密鑰，該斷言密鑰可以用Kasc表示。Kasc可以是用於對一個或多個斷言消息進行簽名以進行使用者驗證的簽名密鑰。Kasc可以從Krp中推導得到。

本地OpenId方法還可以使用稱爲OpenID伺服器功能（OPSF）的服務，其作用可以是生成、共用以及分佈那些可以供本地IdP和/或可依賴方（RP）使用的秘密（secret）。外部RP可以將OPSF和本地IdP視爲單個實體。OPSF

還能夠核驗本地OpenID發佈的簽名，並且RP可以直接與之取得聯繫，例如借助公共網際網路來取得聯繫。通過修改設備上的本地DNS解析快取來將OPSF的位址映射到本地IdP，可以將設備上的瀏覽器重定向到本地IdP。本地OpenID方法還可以使用一種用OP-agg表示的服務，其作用可以是便於代表RP來發現本地IdP。

1 通信系統

第1A圖是可以實施所公開的一個或多個實施方式的示例通信系統100的圖示。通信系統100可以是爲多個無線使用者提供語音、資料、視訊、消息傳遞、廣播等內容的多重存取系統。該通信系統100能使多個無線使用者通過共用包括無線帶寬在內的系統資源來存取這些內容。舉例來說，通信系統100可以使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）等等。

如第1A圖所示，通信系統100可以包括無線傳輸/接收單元（WTRU）102a、102b、102c、102d，無線電存取網路（RAN）104，核心網路106，公共交換電話網絡（PSTN）108，網際網路110以及其他網路112，但是應該瞭解，所公開的實施方式設想了任意數量的WTRU、基地台、網路和/或網路元件。WTRU 102a、102b、102c、102d中的每一個可以是被配置成在無線環境中工作和/或通信的任何類型的設備。例如，WTRU 102a、102b、102c、102d可以被配置成傳輸和/或接收無線信號，並且可以包括使用者設備（UE）、行動站、行動節點、固定或行動使用者單元、尋呼機、行動電話、個人數位助理（PDA）、智慧型電話、膝上型電腦、筆記型電腦、個人電腦、無線感測器、消費類電子設備等等。

通信系統100還可以包括基地台114a和基地台114b。基地台114a、114b中的每一個可以是被配置成通過與WTRU 102a、102b、102c、102d中的至少

一個形成無線介面來促成針對一個或多個通信網路的存取的任何類型的設備，其中舉例來說，該網路可以是核心網路106、網際網路110和/或網路112。舉個例子，基地台114a、114b可以是基地收發器（BTS）、節點-B、e節點B、家庭節點B、家庭e節點B、站點控制器、存取點（AP）、無線路由器等等。雖然每一個基地台114a、114b都被描述成單個元件，但是應該瞭解，基地台114a、114b可以包括任何數量的互連基地台和/或網路元件。

基地台114a可以是RAN 104的一部分，其中該RAN還可以包括其他基地台和/或網路元件（未顯示），例如基地台控制器（BSC）、無線電網路控制器（RNC）、中繼節點等等。基地台114a和/或基地台114b可以被配置成在稱爲胞元（未顯示）的特定地理區域內部傳輸和/或接收無線信號。所述胞元可以進一步分成胞元磁區。例如，與基地台114a相關聯的胞元可以分成三個磁區。因此，在一個實施方式中，基地台114a可以包括三個收發器，即每一個收發器對應於胞元的一個磁區。在另一個實施方式中，基地台114a可以使用多輸入多輸出（MIMO）技術，由此可以爲胞元中的每個磁區使用多個收發器。

基地台114a、114b可以經由空中介面116來與一個或多個WTRU 102a、102b、102c、102d進行通信，該空中介面可以是任何適當的無線通信鏈路（例如無線頻率（RF）、微波、紅外線（IR）、紫外線（UV）、可見光等等）。空中介面216可以用任何適當的無線電存取技術（RAT）來建立。

更具體地說，如上所述，通信系統100可以是多存取系統，並且可以使用一種或多種頻道存取方案，例如CDMA、TDMA、FDMA、OFDMA、SC-FDMA等等。舉例來說，RAN 104中的基地台114a與WTRU 102a、102b、102c可以實施通用行動電信系統（UMTS）陸地無線電存取（UTRA）之類的無線電技術，該技術可以使用寬頻CDMA（WCDMA）來建立空中介面116。WCDMA可以包

括高速封包存取（HSPA）和/或演進型HSPA（HSPA+）之類的通信協議。HSPA可以包括高速下行鏈路封包存取（HSDPA）和/或高速上行鏈路封包存取（HSUPA）。

在另一個實施方式中，基地台114a和WTRU 102a、102b、102c可以實施演進型UMTS陸地無線電存取（E-UTRA）之類的無線電技術，該無線電技術可以使用長期演進（LTE）和/或先進LTE（LTE-A）來建立空中介面116。

在其他實施方式中，基地台114a與WTRU 102a、102b、102c可以實施IEEE 802 .16（全球互通微波存取（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）、用於GSM演進的增強型資料速率（EDGE）、GSM EDGE（GERAN）等無線電存取技術。

第1A圖中的基地台114b可以是無線路由器、家庭節點B、家庭e節點B或存取點，並且可以使用任何適當的RAT來促成營業場所、住宅、交通工具、校園等局部區域中的無線連接。在一個實施方式中，基地台114b和WTRU 102c、102d可以通過實施IEEE 802.11之類的無線電技術來建立無線區域網路（WLAN）。在另一個實施方式中，基地台114b和WTRU 102c、102d可以實施IEEE 802.15之類的無線電技術來建立無線個人區域網路（WPAN）。在另一個實施方式中，基地台114b和WTRU 102c、102d可以通過使用基於胞元的RAT（例如WCDMA、CDMA2000、GSM、LTE、LTE-A等等）來建立微微胞元或毫微微胞元。如第1A圖所示，基地台114b可以直接連接到網際網路110。因此，基地台114b可以不需要經由核心網路106來存取網際網路110。

RAN 104可以與核心網路106進行通信，所述核心網路106可以是被配置成向WTRU 102a、102b、102c、102d中的一個或多個提供語音、資料、應用和/或借助網際協定的語音（VoIP）服務的任何類型的網路。例如，核心網

路106可以提供呼叫控制、計費服務、基於行動位置的服務、預付費呼叫、網際網路連接、視訊分佈等等，和/或執行使用者驗證之類的高級安全功能。雖然第1A圖中沒有顯示，但是應該瞭解，RAN 104和/或核心網路106可以直接或間接地和其他那些與RAN 104使用相同RAT或不同RAT的RAN進行通信。例如，除了連接到可以使用E-UTRA無線電技術的RAN 104之外，核心網路106還可以與使用GSM無線電技術的另一個RAN（未顯示）通信。

核心網路106還可以充當供WTRU 102a、102b、102c、102d存取PSTN 108、網際網路110和/或其他網路112的閘道。PSTN 108可以包括提供普通老式電話服務（POTS）的電路交換電話網絡。網際網路110可以包括使用公共通信協定的全球性互聯電腦網路設備系統，該協定可以是TCP/IP互連網協定族中的傳輸控制協定（TCP）、使用者資料報協定（UDP）以及網際協議（IP）。網路112可以包括由其他服務供應商擁有和/或營運的有線或無線通信網路。例如，網路112可以包括與一個或多個RAN相連的另一個核心網路，其中所述一個或多個RAN既可以與RAN 104使用相同RAT，也可以使用不同RAT。

通信系統100中的一些或所有WTRU 102a、102b、102c、102d可以包括多模式能力，換言之，WTRU 102a、102b、102c、102d可以包括在不同無線鏈路上與不同無線網路通信的多個收發器。例如，第1A圖所示的WTRU 102c可以被配置成與使用基於胞元的無線電技術的基地台114a通信，並且可以與使用IEEE 802無線電技術的基地台114b通信。

第1B圖是示例WTRU 102的系統圖示。如第1B圖所示，WTRU 102可以包括處理器118、收發器120、傳輸/接收元件122、揚聲器/麥克風124、數位鍵盤126、顯示器/觸控板128、不可拆卸記憶體130、可拆卸記憶體132、電源134、全球定位系統（GPS）晶片組136以及其他週邊設備138。應該瞭解的是，在保持符合實施方式的同時，WTRU 102可以包括前述元件的任何子

組合。

處理器118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核心關聯的一個或多個微處理器、控制器、微控制器、專用積體電路（ASIC）、現場可程式化閘陣列（FPGA）電路、其他任何類型的積體電路（IC）、狀態器等等。處理器118可以執行信號編碼、資料處理、功率控制、輸入/輸出處理和/或其他任何能使WTRU 102在無線環境中工作的功能。處理器118可以耦合至收發器120，收發器120可以耦合至傳輸/接收元件122。雖然第1B圖將處理器118和收發器120描述成是獨立組件，但是應該瞭解，處理器118和收發器120可以一起集成在電子封裝或晶片中。

傳輸/接收元件122可以被配置成經由空中介面116來傳輸至基地台（例如基地台114a）或或來自基地台的信號。舉個例子，在一個實施方式中，傳輸/接收元件122可以是被配置成傳輸和/或接收RF信號的天線。在另一個實施方式中，舉例來說，傳輸/接收元件122可以是被配置成傳輸和/或接收IR、UV或可見光信號的傳輸器/檢測器。在再一個實施方式中，傳輸/接收元件122可以被配置成傳輸和接收RF和光信號。應該瞭解的是，傳輸/接收元件122可以被配置成傳輸和/或接收無線信號的任何組合。

此外，雖然在第1B圖中將傳輸/接收元件122描述成了單個元件，但是WTRU 102可以包括任何數量的傳輸/接收元件122。更具體地說，WTRU 102可以使用MIMO技術。因此，在一個實施方式中，WTRU 102可以包括兩個或多個經由空中介面116來傳輸和接收無線電信號的傳輸/接收元件122（例如多個天線）。

收發器120可以被配置成對傳輸/接收元件122將要傳輸的信號進行調製，以及對傳輸/接收元件122接收的信號進行解調。如上所述，WTRU 102可以具有多模式能力。因此，收發器120可以包括允許WTRU 102借助UTRA和

IEEE 802.11之類的多種RAT來進行通信的多個收發器。

WTRU 102的處理器118可以耦合至揚聲器/麥克風124、數位鍵盤126和/或顯示器/觸控板128（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），並且從中接收使用者輸入資料。處理器118還可以向揚聲器/麥克風124、數位鍵盤126和/或顯示器/觸控板128輸出使用者資料。此外，處理器118可以從不可拆卸記憶體130和/或可拆卸記憶體132之類的任何適當的記憶體中存取資訊，以及將資訊存入這些記憶體。所述不可拆卸記憶體130可以包括隨機存取記憶體（RAM）、唯讀記憶體（ROM）、硬碟或是其他任何類型的記憶儲存設備。可拆卸記憶體132可以包括使用者標識模組（SIM）卡、記憶卡、安全數位（SD）記憶卡等等。在其他實施方式中，處理器118可以從那些並非實際位於WTRU 102的記憶體存取資訊，以及將資料存入這些記憶體，其中舉例來說，所述記憶體可以位於伺服器或家庭電腦上（未顯示）。

處理器118可以接收來自電源134的電力，並且可以被配置分佈和/或控制用於WTRU 102中的其他組件的電力。電源134可以是爲WTRU 102供電的任何適當的設備。例如，電源134可以包括一個或多個乾電池組（如鎳鎘（Ni-Cd）、鎳鋅（Ni-Zn）、鎳氫（NiMH）、鋰離子（Li-ion）等等）、太陽能電池、燃料電池等等。

處理器118還可以與GPS晶片組136耦合，該GPS晶片組136可以被配置成提供與WTRU 102的當前位置相關的位置資訊（例如經度和緯度）。作爲來自GPS晶片組136的資訊的補充或替換，WTRU 102可以經由空中介面116接收來自基地台（例如基地台114a、114b）的位置資訊，和/或根據從兩個或多個附近基地台接收的信號定時來確定其位置。應該瞭解的是，在保持符合實施方式的同時，WTRU 102可以借助任何適當的定位方法來獲取位置資訊。

處理器118還可以耦合到其他週邊設備138，這些週邊設備可以包括提供額外特徵、功能和/或有線或無線連接的一個或多個軟體和/或硬體模組。例如，週邊設備138可以包括加速度計、電子指南針、衛星收發器、數位相機（用於照片和視訊）、通用串列匯流排（USB）埠、振動設備、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、電視遊樂器模組、網際網路瀏覽器等等。

第1C圖是根據一個實施方式的RAN 104和核心網路106的系統圖示。如上所述，RAN 104可以使用E-UTRA無線電技術並且經由空中介面116來與WTRU 102a、102b、102c進行通信。並且該RAN 104還可以與核心網路106通信。

RAN 104可以包括e節點-B 140a、140b、140c，但是應該瞭解，在保持與實施方式相符合的同時，RAN 104可以包括任何數量的e節點-B。每一個e節點-B 140a、140b、140c都可以包括一個或多個收發器，以便經由空中介面116來與WTRU 102a、102b、102c通信。在一個實施方式中，e節點-B 140a、140b、140c可以實施MIMO技術。因此舉例來說，e節點-B 140a可以使用多個天線來向WTRU 102a傳輸無線信號，以及接收來自WTRU 102a的無線信號。

每一個e節點-B 140a、140b、140c都可以與特定胞元（未顯示）關聯，並且可以被配置成處理無線電資源管理決策、切換決定、上行鏈路和/或下行鏈路中的使用者調度等等。如第1C圖所示，e節點-B 140a、140b、140c彼此可以經由X2介面來進行通信。

第1C圖所示的核心網路106可以包括行動性管理閘道（MME）142、服務閘道144以及封包資料網路（PDN）閘道146。雖然每一個前述元件都被描述成是核心網路106的一部分，但是應該瞭解，這其中的任一元件都可以由核心網路營運商之外的其他實體擁有和/或營運。

MME 142可以經由S1介面來與RAN 104中的e節點B 140a、140b、140c中的每一個相連，並且可以充當控制節點。例如，MME 142可以負責驗證WTRU 102a、102b、102c的使用者，啓動/去啓動承載，在WTRU 102a、102b、102c的初始附著過程中選擇特定服務閘道等等。MME 142還可以提供控制平面功能，以便在RAN 104與使用諸如GSM或WCDMA之類的其他無線電技術的其他RAN（未顯示）之間進行切換。

服務閘道144可以經由S1介面而與RAN 104中的e節點-B 140a、140b、140c中的每一個相連。該服務閘道144通常可以路由至WTRU102a、102b、102c和轉發來自WTRU 102a、102b、102c的使用者資料封包。該服務閘道144還可以執行其他功能，例如在e節點-B間的切換過程中錨定使用者平面，在下行鏈路數據可供WTRU 102a、102b、102c使用時觸發尋呼，管理和儲存WTRU 102a、102b、102c的上下文等等。

服務閘道144還可以連接到PDN閘道146，該PDN閘道可以爲WTRU 102a、102b、102c提供針對網際網路之類的封包交換網路的存取，以便促成WTRU 102a、102b、102c與IP啓用的設備之間的通信。

核心網路106可以促成與其他網路的通信。例如，核心網路106可以爲WTRU 102a、102b、102c提供針對PSTN 108之類的電路交換網路的存取，以便促成WTRU 102a、102b、102c與傳統的陸線通信設備之間的通信。舉例來說，核心網路106可以包括IP閘道（例如IP多媒體子系統（IMS）伺服器）或與之通信，其中該IP閘道充當的是核心網路106與PSTN 108之間的介面。此外，核心網路106可以爲WTRU 102a、102b、102c提供針對網路112的存取，該網路112可以包括其他服務供應商擁有和/或營運的其他有線或無線網路。

2.3 標識管理和可用安全性

當使用者開始在行動設備上存取資訊時，他們面臨著爲一個接一個的web服

務處理過多使用者證書的困境。使用者面對的是記憶這些證書以及在每次存取web服務時輸入登錄和密碼資訊的煩瑣任務。雖然設備有可能記憶這些證書，但是設備有可能會被丟失或盜竊，並且有可能最終落在不該擁有的人的手裏。

所提供的可以是一種將本地使用者驗證與透明的網路驗證組合在一起的牢固的驗證解決方案。例如，多種密碼或權杖項和/或生物測定（biometric）驗證技術可以與問候式的無縫網路驗證方案結合使用，其中所述方案是與web服務入口合作的。這些方案可以被稱爲單點登錄（SSO）或聯合標識。

行動平臺可以包括UE，它可以支援多種專用處理器架構和作業系統。這樣爲軟體/韌體開發人員創造了一個零散的市場，並且迫使營運商通過與OEM協商來引入並支持諸如存取控制和驗證之類的常見技術。以下部分討論的是在行動平臺上提供SSO協定的實施方式。

在一個示例實施方式中，可以通過使用使用者環境來啓用開放管理安全協議，以使可依賴方（RP）能夠驗證使用者。該開放管理安全協定可以是單點登錄協定（SSO），例如OpenID協定、自由聯盟協定、開放驗證（OAUTH）協定、安全斷言標記語言、標識保證框架等等。可依賴方可以是希望驗證或核驗使用者證書的一方。

使用者環境可以包括使用者介面和/或處理器，例如可信計算環境。

使用者介面可以在UE與使用者之間提供介面。例如，該使用者介面可以是web瀏覽器、網頁、應用等等。使用者介面還可以接收使用者證書。該使用者證書可以是使用者名稱、密碼、PIN碼、密鑰、權杖、生物測定標識等等的組合。

使用者介面可以提供介面和/或使用OpenID之類的SSO協議來與RP進行通信，以便代表使用者來請求存取RP提供的服務。例如，使用者可以使用web瀏

覽器之類的使用者介面代理來存取RP，並且可以使用OpenID來選擇進行登錄。該使用者介面還可以從RP接收表明該RP希望對使用者進行驗證的指示。例如，使用者介面可以接收來自RP的重定向消息，其中該消息指示使用者介面使用可信計算環境來對使用者進行驗證。

使用者介面還可以通過與SSO證書的可信供應方進行通信來發起使用者驗證。例如，RP可以將使用者介面重定向到可與可信供應方相關聯的可信計算環境。該可信供應方可以是使用者證書供應方。例如，可信供應方有可能知道使用者，並且能夠通過使用者提供的證書來驗證使用者。

處理器可以是通用處理器，專用處理器，常規處理器，數位信號處理器（DSP），多個微處理器，與DSP核相關聯的一個或多個微處理器，控制器，微控制器，專用積體電路（ASIC），現場可程式化閘陣列（FPGA）電路，任何其他類型的積體電路（IC），狀態機等等。此外，處理器

在一個示例實施方式中，處理器可以是可信的計算環境，例如UMTS積體電路卡（UICC），使用者標識模組（SIM），機器對機器（M2M）設備，智慧卡，Java卡，全球平臺智慧卡，安全集成晶片卡（ICC）等等。該可信計算環境可以使用智慧卡web伺服器（SCWS）來實現。

該可信計算環境可以在使用者環境內部爲可信供應方驗證使用者。爲了驗證使用者，可信計算環境可以在本地執行單點登錄證書的可信供應方的至少一些功能，以便在驗證處理過程中限制使用者環境以外的通信。例如，使用者可以通過PIN碼、生物測定標識、權杖等等或是其組合（即PIN碼和生物測定標識）而在可信計算環境本地執行驗證。可信計算環境可以生成驗證回應。該可信計算環境可以使用重定向消息來將使用者介面代理重定向到RP，其中該重定向消息可以包括使用者被驗證的斷言。然後，使用者介面可以被重定向到RP，並且使用者可以在RP核驗了來自可信計算環境的斷言之後登錄。

在一個示例實施方式中，可信計算環境可以計算一個簽名，例如base64（基本64位元）編碼的HMAC簽名，並且可以將該簽名經由使用者介面提供給RP。舉例來說，通過執行該處理，可以允許RP核驗可信計算環境的證書。可信環境可以基於該可信計算環境與可能關聯於MNO或OP的可信供應方之間的共用秘密來核算簽名。該共用秘密可以是通過使用者介面而在可信計算環境與可信供應方之間建立的。該簽名可以用於對從RP接收的參數列表進行簽名。

可依賴方（RP）可以是服務、網站、資料庫、應用等等。在一個示例實施方式中，RP可以處於使用者環境以外。例如，RP可以是在使用者環境以外的伺服器上託管的網站，其中該使用者環境可以是例如使用者用於存取網站的行動電話或其他UE。RP有可能必須建立一個連接，例如使用行動網路營運商（MNO）提供的針對web服務實體的公共網際網路通信來建立連接。舉例來說，該處理可以在可依賴方（RP）無法直接與可信計算環境通信的時候進行。MNO可以具有與可信計算環境形成介面的遠端管理介面，以及諸如SMS之類的額外通信頻道，這樣可以允許MNO與UE和/或可信計算環境進行通信。MNO可以充當RP與可信計算環境上的OP之間的協商橋樑。

在另一個示例實施方式中，RP可以處於使用者環境內。例如，RP可以位於可包含使用者介面和可信計算環境的UE的內部。

在一個示例實施方式中，RP可以被配置成傳送驗證請求，以便允許RP核驗可信計算環境的證書。使用者介面可以接收來自RP的驗證請求。該驗證請求可以包括關聯控制。使用者介面可以將這個關聯控制提供給可信計算環境。該可信計算環境可以基於共用秘密來生成簽名，並且可以生成包含簽名和關聯控制的驗證響應。使用者介面或可信計算環境可以將可信環境生成的驗證回應提供給RP。

在一個示例實施方式中，使用者環境可以處於使用者設備（UE）內部。例

如，使用者介面和可信計算環境可以包含在單個UE內部。在另一個示例實施方式中，使用者環境可以採用分離終端配置來部署，其中使用者介面和可信計算環境可以駐留在分離的UE中。例如，使用者介面可以是在屬於使用者的行動電話上，而可信計算環境則可以存在於屬於使用者的銀行卡或UICC上。另舉一例，使用者介面可以是在屬於使用者的個人電腦上的，而可信計算環境則有可能在屬於使用者的行動電話上。

在一個示例實施方式中，通過提供一種用於保護使用者環境和/或本地斷言供應方（LAP）的方法，可以在開放管理安全協議中爲可依賴方（RP）驗證使用者。在一個示例實施方式中，LAP可以處於處理器內部，例如處於可信計算環境以內。來自RP的指示可以經由使用者介面而被接收，其中該指示表明RP希望對使用者進行驗證。RP可以處於使用者環境以外，並且能夠與單點登錄（SSO）證書的可信供應方進行通信。使用者證書可以是通過使用者介面而從使用者那裏接收的。所述使用者可以用接收到的使用者證書來驗證。例如，可信計算環境之類的處理器可以使用接收到的使用者證書來爲RP驗證使用者，以便在本地執行SSO證書的可信供應方的至少一些功能，從而在驗證處理過程中限制使用者環境以外的通信。驗證可以通過使用智慧卡web伺服器（SCWS）來進行。

驗證回應可以經由使用者介面傳送到RP。例如，該驗證回應可以在使用者已被驗證的時候傳送。

從RP接收的指示可以是重定向消息。該重定向消息可以指示使用者介面使用可信計算環境來驗證使用者。例如，重定向消息可以指示瀏覽器在本地驗證使用者，而不是由可信供應方來進行驗證。

簽名可以是例如base64編碼的HMAC簽名，該簽名可被核算並經由使用者介面提供給RP。例如，通過執行該處理，可以允許RP核驗可信計算環境的證書。可信計算環境可以基於該可信計算環境與諸如OpenID供應方這類可能

關聯於MNO的可信供應方之間的共用秘密來核驗證書。該共用秘密可以是通過使用者介面而在可信計算環境與可信供應方之間建立的。

在一個示例實施方式中，驗證請求可以是從RP接收的，這樣可以允許RP核驗可信計算環境的證書。例如，使用者介面可以接收來自RP的驗證請求。該驗證請求可以包括關聯控制。使用者介面可以將關聯控制提供給可信計算環境。可以生成基於共用秘密的簽名。此外還可以生成包含了所述簽名和關聯控制的驗證響應。然後，該驗證回應可被提供給RP。

2.3.2 使用OpenID和SCWS的單點登錄的實施方式

OpenID可以爲營運商提供一個輕鬆的角色，以便以最小的努力和風險向可依賴方（RP）提供OpenID供應方（OP）中的信任。OpenID可以與先前已有的驗證方法協作，由此營運商可以使用自己的AAA和在UICC中預先提供的AKA證書或其他驗證方法來支援針對OP的驗證過程，這其中包括但不侷限於PKI、預共用密鑰、SIP-摘要證書、TLS等等。

OpenID與智慧卡的組合提供了一條通向令人關注的價值主張的途徑。智慧卡Web伺服器（SCWS）提供了基於IP的全新服務，該服務可以爲使用者提供豐富得多且非常安全的Web體驗。Web伺服器的基本功能是使用HTTP協定來遞送網頁。這一點對駐留在智慧卡或UICC上的SCWS來說也是一樣的。SCWS可以是將UICC作爲網路節點集成在行動電話供應商的IP網路中的第一步。

在一個示例實施方式中，UICC可被用作營運商的本地信任中心和代理。例如，通過執行該處理，可以將驗證業務量保持在本地，並且避免加重營運商網路的負擔。OP能夠通過縮放驗證強度來啓用多種用於將OpenID證書綁定到UICC和/或設備和/或使用者標識和/或使用者的方法。例如，OpenID可以與基於UICC的UE驗證AKA證書、GBA或其他形式的驗證機制進行交互操作，其中所述驗證機制可以是基於證書的驗證機制。在這裏公開的實施方

式中，UE可以爲設備上的OP代理對營運商的信任和聲譽提供制衡作用，以便借助標準的OpenID協定來提供更高的安全性。

2.3.3 智慧卡上的OP

在以下的第4節中描述了若干實施方式，這些實施方式描述的是將OP集成在智慧卡上。例如，其中一個實施方式描述的是駐留有智慧卡web伺服器（SCWS）的智慧卡上的OpenID。另一個實施方式描述的是對SCWS上的OpenID的改進。

從這裏描述的實施方式中得到的益處可以包括：

·使用OpenID時的使用者行動性

·改進了對證書進行的使用者控制（增強的安全保護），這是因爲這個重要資訊現在是在卡上而不是在雲中

·減小了對於使用GBA的需要，由此顯著減小了網路資源的負擔

·驗證業務量被限制在網路實體之間的公共網際網路上，而不需要空中傳送—對於SCWS上的OpenID的改進協議來說，這一點是很明顯的

3 標準化前景

有很多正式和事實上的（產業）標準化團體組織從事的是標識管理（IdM）；但是，這其中的大多數組織將重點放在IdM在桌面機環境中的運用。這裏公開的實施方式是通過本地和/或分散式SSO供應方來提供IdM的，這些供應方既可以在智慧卡之類的可信環境中實施，也可以在能夠包含可信計算環境的平臺上實施，例如智慧型電話、H(e)NB或其他類型的設備。單點登錄供應方可以由標準化組織提供，例如自由聯盟供應方、SAML供應方、Kantara Initiative（發起）供應方、OpenID供應方等等。

3.2 自由聯盟

自由聯盟是作爲由BT、AOL、Oracle、Intel、NTT、CA、Fidelity Investment、NTT以及Sun Microsystems之類的公司領導的產業論壇發起

的。該聯盟已經發佈了從事ID聯合（ID-FF）和標識web服務（ID-WSF）的Liberty Alliance Frameworks（自由聯合框架）系列規範。

自由標識聯合（ID-FF）規範1.0是這樣一個規範，它允許基於網際網路的服務和電子商務應用的消費者及使用者從任一設備驗證並登錄一次網路或域，然後存取來自多個網站的服務，由此迴避了使用者重新驗證和控制隱私問題的需要。自由聯盟還發佈了兩個版本的標識聯合規範，並將其聯合規範提供給了OASIS（http://www.oasis.org），由此形成了安全斷言標記語言（SAML）2.0的基礎。此外，自由聯盟還發佈了自由聯盟Web服務框架（ID-WSF），該框架解決的是基於標識的web服務。這個規範是用於在安全和尊重隱私的聯合社交網路中部署並管理多種基於標識的web服務的開放框架，例如，這些Web服務可以是地理定位、聯絡簿、日曆、行動消息傳遞等等。

這裏公開的實施方式公開的是可以用於在UE上下文中爲自由聯盟標準的安全和其他方面提供支持的創新。例如，一個實施方式公開了一種行動設備，該行動設備具有作爲可拆除模組或作爲集成模組的安全環境，例如UICC、智慧卡或集成可信環境（TrE），其中所述安全環境可以單獨或共同託管所公開的一些功能，例如UE上的可信票據伺服器或TTverifier（TT核驗器）的功能。與只支援已有自由聯盟客戶協定的常規UE當前可用的功能相比，所公開的這些功能可以單獨或共同添加至更多的安全性和信任證據。

3.3 OASIS和SAML

結構化資訊標準促進組織（OASIS）是一個用於開發、融合並採用電子商務及web服務標準的全球性開放協會。在IdM上下文中，OASIS開發了安全斷言標記語言（SAML），其當前版本是2.0。

SAML是基於XML的標準，用於在安全域之間、也就是在標識供應方（標識斷言的產生者）與服務供應方（斷言的使用者）之間交換驗證和授權資料

。SAML嘗試解決Web瀏覽器的單點登錄（Web SSO）問題，以便將基於網內的傳統SSO解決方案擴展到Web的開放環境中。SAML嘗試使用基於XML（和XHTML）的開放的標準化協議來克服不可互操作的專用技術的增殖效應。SAML與諸如OpenID之類的其他IdM技術的不同之處在於其依靠使用者代理來提供請求和斷言。

第2圖顯示的是用於在標識供應方與服務供應方之間交換驗證和資料的SAML協定。

這裏公開的實施方式公開的是可以用於在UE情景中爲SAML的安全性和其他方面提供支援的創新。例如，其中一個實施方式公開了一種行動設備，該設備具有作爲可拆除模組或作爲集成模組的安全環境，例如UICC、智慧卡或集成可信環境（TrE），其中所述安全環境可以單獨或共同託管所公開的一些功能，例如UE上的可信票據伺服器或TTverifier的功能。與只支援已有SAML客戶協定的常規UE當前可用的功能相比，所公開的這些功能可以單獨或共同添加更多的安全性和信任證據。

3.4 Kantara Initiative

Kantara Initiative是自由聯盟的後繼組織，並且由自由聯盟的一些初始支持者領導，例如BT、NTT、T-Mobile、AOL和Fidelity Investment。Kantara並不是一個定義標準的組織（SDO），這是因爲Kantara發佈的都是建議，並且其重點放在兩個主要的技術主題上：標識保證和互操作性。Kantara首先規定的是擴展了自由聯盟做出的IAP v1.0規範工作的標識保證框架（IAP）v2.0。IAP規範初始詳述了很多標識保證等級，這有助於以公共的標準化規則以及與每一個標識保證等級相關聯的安全風險評定爲基礎來將啓用可信標識的企業、社交網路以及Web 2.0應用聯繫在一起。同樣，該框架啓用了針對標識要求和評估的靈活而具有間隔（granular）的信任保證。所規定的保證等級以NIST Special Publication（特定公開

）800-63第1.0.1版概述的四個保證等級爲基礎，並且其置信等級範圍是從低到很高。

這裏公開的實施方式公開的是可以用於在UE上下文中爲IAP的安全性和其他方面提供支援的創新。例如，其中一個實施方式公開了一種行動設備，該設備具有作爲可拆除模組或集成模組的安全環境，例如UICC、智慧卡或集成可信環境（TrE），其中所述安全環境可以單獨或共同託管所公開的一些功能，例如UE上的可信票據伺服器或TTverifier的功能。與只支援已有Kantara IAP客戶協定的常規UE當前可用的功能相比，所公開的這些功能可以單獨或共同添加至更多的安全性和信任證據。

3.5 OpenID

OpenID是用於驗證使用者的開放標準，該標準可被用於存取控制，以便在不同服務信任驗證組織的情況下允許使用者使用相同的數位標識登錄這些服務。OpenID取代了常規的使用者登錄處理，由此允許使用者登錄一次並存取多個軟體系統的資源。術語OpenID也可以指該標準中使用的ID。

OpenID是由OpenID基金會開發和維護的，該基金會是一個美國的非營利組織。該OpenID基金會（OIDF）是由致力於啓用、促進和保護OpenID技術的個人和公司組成的。

作爲OpenID協議所用ID的術語，OpenID是唯一URL的形式，並且由使用者的OpenID供應方（即託管其OpenID URL的實體）進行驗證。OpenID協定不依靠中心機構來驗證使用者標識，也不依賴特定的驗證方法本身。由於OpenID協定和需要標識的網站都不能強制執行特定類型的驗證，因此可以使用多種驗證處理，例如使用智慧卡、生物測定學或常規密碼。

這裏公開的實施方式公開的是可以用於在UE情景中爲OpenID的安全性和其他方面提供支援的創新。例如，其中一個實施方式公開了一種行動設備，該設備具有作爲可拆除模組或作爲集成模組的安全環境，例如UICC、智慧

卡或集成可信環境（TrE）。這裏使用的OpenID是作爲示例協定的，其中諸如可信票據伺服器（TTS）、TTverifier和TCTicket（TC票據）之類的新公開的功能可以由UE中的所述安全環境託管，並且可以單獨或者共同使得UE更加安全可靠，此外，在UE依照OpenID協定執行使用者標識客戶功能的時候，通過使用所公開的這些方法，還會使得這種增強的安全性和可信賴性是能在外部核驗的。

3.6 3GPP SA3及其關於OpenID的工作

3GPP SA3是一個3GPP安全標準化工作組，在3GPP SA3中，在2G、3G和下一代的行動電話、終端和系統的廣泛的安全性方面採用了一種綜合處理方法。當前，在IdM空間中，存在一個關於OpenID與通用自舉（Bootstrapping）架構的集成的技術報告（TR 33.924）。此外還有另一個關於自由聯盟與GBA互通的技術報告（TR 33.980）。

這裏公開的實施方式公開的是可以用於在UE上下文中爲OpenID的安全性和其他方面和/或OpenID與GBA或其他驗證機制的集成提供支援的創新。例如，其中一個實施方式公開了一種行動設備，該行動設備具有作爲可拆除模組或作爲集成模組的安全環境，例如UICC、智慧卡或集成可信環境（TrE），其中所述安全環境可以單獨或共同託管所公開的一些功能，例如UE上的可信票據伺服器或TTverifier的功能。與只支援3GPP規定的已有協定而在3G網路上實現OpenID或自由聯盟互通的常規UE當前可用的功能相比，所公開的這些功能可以單獨或共同添加至更多的安全性和信任證據。

4 技術概述

本節提供的是能夠提供標識管理（IdM）解決方案的實施方式的技術概述。例如，這些實施方式可被用於將OpenID供應方（OP）伺服器功能置於行動本地平臺中，尤其是智慧卡中。

在第4.1節，我們提供的是關於OpenID的介紹。

第4.2節論述的是提供智慧卡上的OpenID以及架構、實施選項、變體、和3GPP GBA的集成（通用自舉架構）的實施方式。

第4.3節論述的是設想了OpenID供應方（OP）實施平臺選項的實施方式。此外，第4.3節還論述了實施相容JavaCard™的智慧卡的實施方式，以及在智慧卡Web伺服器（SCWS）上實施OP的實施方式。

第4.4節論述的是處理本地使用者驗證的實施方式。本地使用者驗證是一個涉及OpenID和其他SSO技術的主題。此外，第4.4節還論述了使用生物測定學的實施方式。

第4.5節論述的是提供了可以在OpenID上下文中發展的“信任”和“信任關係”方法的實施方式。例如，在這裏描述的是若干個公開了MNO的作用的實施方式，此外還詳細探討了所述MNO與OpenID協定中的其他實體/行動者可能具有的信任關係。在一個示例實施方式中，MNO與主標識供應方（IdP）是完全相同的，並且智慧卡上的OP是MNO的代理（充當IDP）。在第二示例實施方式中，MNO並不擁有或管理智慧卡上的OP，並且該MNO不是IdP，但第三方IdP擁有並管理智慧卡上的OP。

第4.6節論述的是允許在智慧卡之外的平臺上實施OP的實施方式。例如，某些實施方式公開的是JavaCard™和嵌入式安全元件上的實施可行性。此外，某些實施方式描述的是可以如何集成平臺信任概念（與可信計算中一樣）與行動OP的概念，以便爲行動OP提供更高的信任和安全等級。

4.1 關於OpenID的介紹

OpenID允許使用者使用單個OP登錄到不同的可依賴方站點。OP是使用者標識的中心儲存位置，並且充當了使用者的單個驗證點。由於使用者是針對其OP被驗證的，因此，該OP可以向可依賴方（RP）發佈斷言，所述可依賴方則轉而允許使用者存取服務。爲了方便起見，OP還被允許儲存那些可以與使用者設定檔相比的個人資訊。然後，在登錄處理之後，該資訊可以在

OP與RP之間交換，以便爲RP提供關於使用者的更詳細資訊。

第3圖顯示的是允許使用者使用單個OP登錄到不同的可依賴方站點的OpenID協定流程。如第3圖所示，使用者嘗試執行OpenID登錄，而這將會導致RP啓動發現OpenID URI的處理。在RP與OP之間可以創造一個建立了共用秘密的可選安全關聯。當發現處理結束時，RP會將使用者重定向到嘗試進行使用者驗證的OP。OP爲使用者提供一個登錄網頁，在該頁面中，一旦輸入了恰當的證書，則驗證所述使用者。一旦驗證成功，則將使用者重定向到RP，並且在那裏向使用者顯示針對web服務的登錄。

4.2 智慧卡上的OpenID

在OpenID協議中，OP可以是使用者證書及其他使用者個人資訊的儲存庫。從而，由於通過竊取用於向OP進行驗證的使用者證書可以允許攻擊者以使用者的名義來存取所有啓用OpenID的站點，因此，在OpenID協議中，OP變成了大多數攻擊的目標。在更溫和的攻擊方案中，舉例來說，攻擊者會在使用者向其OP進行了驗證之後使用登錄使用者的瀏覽器，例如代表使用者來執行隱蔽的操作，在此類攻擊方案中，攻擊者並未得到使用者證書，因此不能使用這些證書來登錄任意站點。但是，OpenID協議設計允許攻擊者登錄到使用者在先前的瀏覽器會話中登錄的所有RP站點。攻擊者不必存取使用者的機器，例如通過惡意軟體或MITM，這種攻擊可以由任何站點（該站點不必是RP站點）通過將XSRF攻擊使用網站中的隱蔽框架來執行。如果攻擊者能夠注入惡意軟體或是充當MITM，那麼整個登錄處理都有可能會被捕獲，然後在需要時在單獨的瀏覽器會話中重放。此外，如果使用者決定（在OP上）允許後續登錄而無需再次向OP提供其證書（舉例來說，如果OP在使用者瀏覽器中儲存了永久性cookie）並且站點使用了OpenID協定的“請求立即驗證”選項，那麼使用者有可能未經通知即被攻擊者獲得登錄。因此，對於OpenID實施方式來說，OP安全性是一個主要的問題。

OpenID本身允許使用者在其擁有的部落格之類的網站上安裝自己的OP。但是，使用者不太可能擁有主機。因此，使用者相信其主機供應方運作正確且以恰當方式保護其私有資料。雖然具有使用者專用設計的客製化OP可以阻礙網路釣魚攻擊，但是，由於攻擊不再以簡單自動的方式進行，因此，所有那些使用了OP實施方式以及使用者瀏覽器與OP的介面的弱點的攻擊（MITM，惡意軟體等等）仍舊是可能存在的。

在一個示例實施方式中，諸如OP之類的SSO供應方的功能可被帶給使用者控制和/或擁有的UE。例如，通過執行該處理，可以提供集中環境來管理使用者標識，同時提供OpenID協定供應的無縫和簡易驗證的好處。如果使用者能在其控制的安全設備上具有自己的OP，那麼某些攻擊將更難以常規方式進行。這種爲使用者儲存和執行OP的設備可以是使用者在其行動設備中攜帶的可信計算環境，例如智慧卡。大多數智慧卡（例如UICC、Java卡等）都能執行增強的功能，並且能與使用者互動。

通過在屬於使用者的智慧卡上運行OP，可以允許使用者對其私有資料保持更多的控制。對於一些方案來說，例如當RP針對其服務收取費用時，如果將基於智慧卡的OP的可信性資訊從MNO傳送到RP，那麼將會是很有用的。這其中可以包括允許RP經由MNO來向使用者收費的反向頻道。使用者可以使用本地頻道來向OP進行驗證，例如經由PIN碼。OP可以由MNO遠端安裝，用於OP的必要證書可以經由GBA協議帶給智慧卡。

第4圖顯示的是爲SSO協定提供可信計算環境上的集成OP的協定流程的示例實施方式。例如，通過使用該協定流程，可以爲OpenID提供處於智慧卡上的集成OP。

如第4圖所示，在201，使用者可以使用web瀏覽器之類的使用者介面代理來存取RP，並且可以選擇使用OpenID進行登錄。在202，RP可以將使用者介面代理重定向到可能包含在例如智慧卡、UICC、Java卡等可信計算環境

內部的本地OP。在203，使用者可以在本地通過PIN碼、生物測定標識等等來向可信計算環境上的OP進行驗證。在204，可信計算環境內部的OP可以產生驗證響應。在205，OP可以將使用者介面代理重定向到RP，並且可以包括使用者已驗證的斷言。在206，使用者介面代理可被重定向到RP，且當RP核驗了來自OP的斷言之後，使用者可以登錄。

RP有可能必須使用諸如公共網際網路通信來與MNO提供的web服務實體建立連接（如果OP是由MNO提供的）。例如，該處理有可能在RP無法直接與可信計算環境上的OP通信的時候進行。MNO可以具有與可信計算環境形成介面的遠端管理介面以及額外通信頻道，例如SMS，這樣允許MNO與設備和/或可信計算環境進行通信。該MNO可以充當RP與可信計算環境上的OP的協商橋樑。

第5圖顯示的是用於爲OpenID提供處於智慧卡上的集成OP的協定流程的示例實施方式。

如第5圖所示，在207，使用者可以存取RP，並且選擇使用OpenID進行登錄。在208，該服務可以將使用者（使用者瀏覽器）重定向到其本地OP。例如，使用者可以在本地使用PIN碼並借助智慧卡介面和/或生物測定標識來向OP進行驗證。在210，OP可以產生驗證響應。在211，OP可以將瀏覽器重定向到RP，並且可以包括使用者已被驗證的斷言。在212，瀏覽器可以被重定向到RP，且當RP核驗了來自OP的斷言之後，使用者可以登錄。

RP有可能必須使用諸如公共網際網路通信來與MNO提供的web服務實體建立連接（如果OP是由MNO提供的）。例如，該處理有可能在RP無法直接與智慧卡上的OP進行通信的時候進行。MNO可以具有形成介面到智慧卡的遠端管理介面以及額外通信頻道，例如SMS，這樣允許MNO與設備和/或智慧卡進行通信。該MNO可以充當RP與智慧卡上的OP的協商橋樑。

4.2.1 架構和偏好

4.2.1.1 RP OP通信需求

在一個示例實施方式中，爲使RP從在智慧卡之類的可信計算環境上運行的OP獲得斷言，RP必須與OP進行通信。該RP可以將使用者識別字傳送到OP，然後，OP可以在驗證之後向RP告知驗證結果。

OpenID協定在協定過程中使用了兩種不同類型的通信。間接通信是借助HTTP重定向或HTML格式提交執行的。從該通信經過使用者瀏覽器的意義上講，該通信是間接的。間接通信被用於驗證請求（從RP經由瀏覽器到達OP）和驗證響應（從OP經由瀏覽器到達RP）。直接通信是在RP與OP之間直接執行的，其被用於與OP直接建立關聯並核驗斷言。

由於在RP與OP之間建立關聯（由此建立共用秘密）的處理並不是強制性的，因此有兩個用於OpenID驗證的協定流程。

這裏描述的實施方式可以用任何一個用於OpenID驗證的協定流程來實施。

4.2.1.1.1 基於關聯的通信的背景

第6圖顯示的是用於以關聯爲基礎的通信的OpenID協定流程。

如第6圖所示，在OpenID協議中，OP與RP之間的關聯不依賴於OP與RP之間預先共用的秘密。它是在使用者向RP提供其OpenID識別字並且希望使用OpenID登錄RP之後由RP執行的初始步驟。在215，RP（經由HTTPS）連接到OP，並且通過執行迪菲-赫爾曼（Diffie-Hellmann）密鑰交換來與OP建立（短期的逐個驗證會話）共用秘密k。然後，在230，RP稍後使用該共用秘密來核驗最初源自OP但卻是由RP經由間接通信（瀏覽器重定向）而從使用者瀏覽器那裏接收的斷言消息的簽名。

在220，如果在RP與OP之間建立了關聯（並且由此建立了共用秘密k），則在驗證請求和回應中（經由間接通信）傳遞該關聯控制。在225，來自OP的驗證回應包含了關聯控制以及使用共用秘密k的斷言的簽名。然後，RP可以使用k來自動地核驗該簽名。通過使用關聯控制，可以允許OP和RP追蹤多個

同時進行的會話。

4.2.1.1.2 無狀態簽名核驗的背景

第7圖顯示的是用於無狀態簽名核驗的OpenID協定流程。

如第7圖所示，如果在RP與OP之間沒有建立關聯，那麼在240，RP必須在去往OP的直接消息中核驗在235接收的驗證響應中的簽名。在245，如果該斷言有效並且確實是由OP發佈的，那麼OP必須向RP發佈包含了被設置成“是”的“is_valid”欄位的聲明（statement）。

雖然驗證請求和回應是借助HTTP重定向並通過使用者瀏覽器傳遞的，並且由此在任何方案中都不需要在RP與OP之間具有任何直達通信頻道，但是必定有一種方法供RP核驗接收到的斷言上的簽名。如果初始協議必須保持符合標準，那麼RP至少必須能在接收到用於簽名核驗的斷言之後與OP聯繫一次。然後將不再需要建立關聯。

4.2.1.2 用於驗證的本地設備上的OP的發現的實施方式

當使用OpenID協定時，RP未必需要在執行間接通信的時候發現OP。

在一個示例實施方式中，用於存取RP的瀏覽器將會得到指向智慧卡上的本地OP的重定向。由於使用的是瀏覽器與RP之間的頻道，因此，該RP甚至可以不需要知道OP的位址。但是，該重定向有可能需要將瀏覽器指向一個位址。該位址可以作爲設備本地IP位址（類似於指示本地主機的127.0.0.1）來給出，並且瀏覽器將會辨認出這個位址，然後參與本地驗證。

在另一個實施方式中，可以使用由瀏覽器出於重定向到本地OP以及繼續進行使用者驗證的目的而轉換的專門識別字。例如，此類識別字可以採用sc://openid/identifier的形式，而這將會告知瀏覽器參與到與智慧卡上的OP進行的關於識別字的驗證會話中。該驗證請求可以採用正確的通信格式來變換，以便用於智慧卡之類的可信計算環境。然後，依照UICC能力，在使用者與UICC之間可以經由恰當的介面來進行驗證。例如，驗證可以

使用PIN碼、生物測定核驗等等來進行。該驗證可以表明使用者已經以其他方式贊同驗證。例如，如果攻擊者或非授權使用者在不瞭解使用者的情況下使用智慧卡來進行驗證，那麼通過執行該處理，可以防止在這種情況下可能發生的攻擊。

通過將驗證與使用者交互耦合，使用者可以知道正在進行的事務處理。依照智慧卡的能力，比較好的有可能是顯示實際事務處理細節，也就是哪一個站點充當RP、RP上的返回URL、以及將要使用哪一個標識。如果智慧卡上的OP支援多個OpenID標識，那麼OP甚至可以向使用者呈現與該RP結合使用的可選標識。在進行了針對OP的本地驗證之後（例如使用PIN碼），瀏覽器被重定向到RP，由此包含了來自OP的肯定斷言。

在一個示例實施方式中，該斷言可以由RP核驗，由此需要在RP與OP之間進行直達通信，其中該直達通信經由關聯或經由先前章節中描述的直接簽名核驗進行。用於斷言核驗的方法是特定於實施方式的，在下面的第4.2.2.1節中對其進行了進一步描述。

4.2.1.3 用於MNO斷言的標識的實施方式

在一個示例實施方式中，諸如智慧卡之類的可信計算環境上的本地OP被用於本地使用者驗證。該MNO可以是在接收到來自智慧卡上的本地OP的觸發消息之後向RP提供必要斷言的實體，由此聲明使用者已被成功驗證。在第4.2.2.1.2節的分離OP方案中更進一步地描述了該實施方式。

4.2.2 實施選項和實施方式變體

本節論述的是可以與這裏公開的更一般概念結合的實施方式的實施選項和變體。

4.2.2.1 用於斷言核驗的RP-OP通信的實施方式

4.2.2.1.1 用於集成BONDI的實施方式

在一個示例實施方式中，RP與OP之間的直達通信頻道至少可以用於核驗斷

言簽名。例如，該直達頻道可以通過在OP與RP之間經由使用者瀏覽器而以隧道方式傳送業務量來提供。該概念有可能需要瀏覽器在當前會話內部執行額外重定向。

在另一個實施方式中，瀏覽器可以充當RP的單個接觸點，以便實施可以用於在RP與OP之間建立通信頻道的第二處理。由於在RP與OP之間指定的通信協議是HTTP或HTTPS，因此，該瀏覽器能夠傳送所有業務量。

爲了便於瀏覽器與智慧卡之類的可信計算環境進行通信，可以使用OMTP BONDI API。BONDI API可以允許瀏覽器使用JavaScript來與智慧卡進行通信，進而與OP進行通信。通過使用BONDI，甚至可以減少重定向。所述RP在其發送給瀏覽器的網頁中包含了恰當的JavaScript呼叫。JavaScript呼叫引起（invoke）BONDI API，並且可以允許存取該智慧卡。然後，呼叫結果可以用相同的JavaScript包裝到發送給RP的回應消息中（例如在HTTPPOST消息中）。依照RP使用BONDI呼叫的時間，RP可以在所述RP使用驗證請求重定向頁面中的智慧卡呼叫的時候建立關聯，或者它也可以使用在RP接收到OP斷言之後顯示的頁面，由此允許RP能夠在沒有關聯的情況下執行直接核驗。

第8圖顯示的是將BONDI與基於關聯的OpenID進行集成的示例實施方式。如第8圖所示，在245，在OP與RP之間通過使用BONDI建立關聯。BONDI可以允許瀏覽器與智慧卡之類的可信計算環境和/或可以處於該可信計算環境內部的OP進行通信。在250，在OP上接收來自RP的驗證請求。在255，將驗證回應反向通信到RP。

第9圖顯示的是將BONDI與無狀態（沒有關聯的）的簽名核驗進行集成的示例實施方式。如第9圖所示，在260，OP和RP經由BONDI和瀏覽器來進行通信。在265，RP向OP傳送驗證請求。在270，OP向RP傳送驗證回應。

4.2.2.1.2 分離OP的實施方式

在一個示例實施方式中，RP可以通過使用分離OP來核驗接收到的斷言。在分離OP中，在MNO與本地OP之間可以分離OP的功能。雖然本地OP可以負責實施使用者驗證，但是MNO可以通過與RP進行通信來核驗源自智慧卡OP的簽名。該處理既可以結合在RP與MNO之間建立的關聯進行，也可以經由無狀態的簽名核驗進行。

第10圖顯示的是啓用分離OP的示例實施方式。如第10圖所示，在275，在RP與MNO之間可以建立關聯。RP可以與MNO建立共用秘密，然後，OP可以在斷言消息的簽名處理中使用該共用秘密。如果RP與不同使用者具有多個同時的連接，那麼該斷言消息有可能要包含關聯控制，以使RP識別正確的共用秘密。該共用秘密可以允許RP核驗斷言簽名，而不必與OP進行通信。該關聯可以在執行從RP首次重定向UE瀏覽器之前進行。

在280，OP可以向RP傳送驗證請求。在285，RP可以向OP傳送驗證回應。在290，OP可以與MNO建立關聯控制和簽名密鑰。該關聯控制和簽名密鑰可以使用GBA來建立。

如果在RP與MNO之間沒有建立關聯，那麼RP仍舊有可能需要能夠通過與MNO上的實體取得聯繫來核驗接收到的簽名。該實體有可能需要發佈關於簽名有效性的聲明。在一個示例實施方式中，一個選項是檢查OP是否確實屬於MNO發佈的OP。這種檢查有可能需要OP在發送給RP的驗證斷言消息中包含唯一識別字，然後，RP會將該消息轉發給MNO。OP地址（IMEI/IMSI）甚至也可作爲該識別字。如果OP是作爲有效OP註冊到MNO的，那麼MNO會向RP返回將“is_valid”欄位設置成“是”的消息，以使RP接受該斷言消息（斷言核驗）。分離OP方案可以允許MNO以一種將所有驗證負擔卸載到智慧卡上的本地OP的方式來保持其對OpenID處理的控制，同時MNO仍舊可以通過使用設置成“否”的“is_valid”來回覆，從而選擇撤銷標識。簽名核驗可以作爲協定中的最後一個步驟而在使用者登錄到RP之前執行。

第11圖顯示的是啓用分離OP的無狀態（無關聯）實施方式的示例。在295，在MNO與RP之間可以進行斷言核驗。在300，RP可以向OP傳送驗證請求。在305，OP可以向RP傳送驗證回應。在310，在OP與MNO之間可以建立關聯控制和簽名密鑰。該關聯控制和簽名密鑰可以使用GBA來建立。

在另一個示例實施方式中，爲使MNO與智慧卡上的OP進行通信，還研究了是否可以使用將加密SMS用作承載的標準OTA管理過程。包含在SMS中的命令可以由SIM卡解密，並且可以依照3GPP TS 11.11定義的方式運行。

在另一個示例實施方式中，承載獨立協定（BIP）可以與卡應用工具箱傳輸協定（CAT_TP）結合使用。BIP允許開放從手機到OTA伺服器以及（U）SIM卡的資料頻道，由此產生端到端的資料頻道。一個SMS的大小是140位元組，與之相比，用於BIP的資料封包包含了1472個位元組。BIP可以使用UE的GPRS連接來實施更快的連接。BIP是在3GPP TS 31.111中標準化的，而CAT TP則是在ETSI TS 102 124中標準化的。

4.2.2.2 將3GPP GBA用於智慧卡上的OP的實施方式

在一個示例實施方式中，GBA可被用於引入在本申請中描述的基於UICC/H(e)NB的OP。例如，GBA協定可以由許多MNO使用和建立。

4.2.2.2.1 關於GBA的介紹

3GPP GBA協定規範（3GPP TS 33.220）是一種能在歸屬位置暫存器（HLR）或家庭使用者伺服器（HSS）上使用使用者的有效標識來實施使用者驗證的技術。GBA架構是通過讓網路元件質詢UE中的SIM卡、以及核驗所述回答與HLR/HSS預測的回答的相似性來進行的。GBA代表的是一種共用密鑰驗證方法。

自舉伺服器功能（BSF）是MNO網路實體，其充當的是兩個端點之間的仲介，並且能使這兩個端點建立共用秘密（其壽命可能是有限的）。

以下圖示是作爲參考而被包括進來的，並且給出的是GBA架構及其元件的概

括。

第12圖顯示的是在GBA架構中使用的BSF功能。

第13圖顯示的是GBA架構概括。

第14圖顯示的是來自3GPP TS 33.220的GBA參考模組。

第15圖顯示的是來自3GPP TS 33.220的被存取網路的GBA參考模組。

4.2.2.2.2 集成GBA與SSO的現有技術

通過使用GBA，可以運用3GPP驗證和密鑰協定處理而在SSO上下文中產生專用於應用的證書。該運用的一個示例是在描述了GBA與自由聯盟SSO協議之間的互通方案的3GPP TR 33.980中給出的。描述了GBA與OpenID協議之間的互通方案的3GPP TR 33.924中給出了另一個示例。3GPP TR使用了GBA密鑰而在作爲標識供應方的相同位置的NAF/OP與UE/使用者的UICC之間執行使用者驗證。在本節的剩餘部分，舉例來說，我們將重點放在了GBA與OpenID之間的互通上。

UE在Ub介面上使用MNO HSS的BSF來創造這些應用層證書。然後，這些證書經由Zn介面與OP/NAF共用。之後，UE客戶可以使用這些證書來與服務供應方直接通信。

第16圖顯示的是用於my MacDonald等人撰寫的“A Web Services Shopping Mall for Mobile Users”（用於行動使用者的Web購物中心）中所示的Liberty/GBA的架構方案。如第16圖所示，GBA可以與自由聯盟協議集成，以便提供實施自由IdP的購物中心。通過該自由IdP，購物中心（shopping mall）可以爲使用者提供可供其在購物服務時使用的標識。該IdP使用了GBA協定作爲驗證機制。

第16圖顯示了以下步驟：

315 一旦進行了註冊，則（UE）的使用者代理在Ub上執行帶有（BSF）的GBA U。

320 爲UICC內部的使用者代理小應用程式提供Ub參數。

325 使用者代理的UICC元件計算Ks，並且爲UE提供服務層證書（Ks(int/ext) NAF）。所述Ks始終保持在UICC中。

330 使用者代理與（NAF/IdP）進行聯繫，以便獲取“Shopping Mall”標識。

335 將適合使用者代理的服務證書經由Zn傳遞給（NAF/IdP）。

340 將用於“shopping mall”的驗證權杖從（NAF/IdP）提供給使用者代理）。

345. （UE）使用服務證書來與（SP）進行通信，並且請求服務。

350. （SP）確認（UE）服務證書的有效性。

4.2.2.2.3 使用GBA和OpenID的實施方式

在一個示例實施方式中，通過使用GBA，可以在UICC與NAF之間建立共用秘密。NAF可以與其他服務（例如IdP）處於相同位置，並且不必處於MNO網路之外。NAF可以向BSF（處於MNO網路內部）請求連接。例如，UE內部的UICC與NAF之間的連接可以借助HTTP或HTTPS上的SOAP。在下文進一步論述的其他實施方式中，對於可以用於OP與MNO之間的通信的基於UICC的OP來說，該OP可以使用GBA協定。

4.2.2.2.3.1 作爲OP的（直接）可信供應方的MNO

在一個示例實施方式中，從MNO可用於在RP與OP之間建立信任的意義上講，MNO可以直接包含在RP－OP通信中。

以下實施方式可以與先前在第4.5.2.2.1節中描述的實施方式相結合。

用於RP與MNO之間的直接連接的實施方式

第17圖顯示的是將GBA用於MMO支援的標識聲明的示例實施方式。

如第17圖所示，在370，RP可以連接到MNO的網路實體，以便建立關聯。該MNO實體可以充當基於UICC的OP的斷言支援；該實體可被稱爲OPsup。

OPsup可以具有集成的NAF功能，並且可以作爲MNO網路內部（但是可到達）或外部（但是可以由MNO操作或認證）的實體。在365，OPsup和UICC上的OP可以執行必要的自舉處理，以便使用GAA/GBA建立共用秘密。在355，使用者瀏覽器可被從RP重定向到本地OP。在360，在瀏覽器與OP之間可以進行通信。

使用者可以向本地（UICC）OP進行驗證。在進行了360處的本地驗證之後（例如使用PIN），在365，OP可以向OPsup發送包含會話識別字的消息（或是RP在初始重定向中傳遞的額外臨時用法（nonce）），其中該會話識別字是用從Ks_NAF得到的RP特定的密鑰Ks_NAF_RP簽名的，作爲選擇，用於簽名的也可以是會話特定的密鑰。在370，如果已經在OPsup與RP之間建立了安全連接，那麼由於所建立的頻道已經提供了來源的真實性，並且爲消息提供了完整性保護，因此，OPsup可以將消息轉發到RP。但是，OPsup可以用公共鑰匙來對消息進行簽名，以便在與通信頻道無關的情況下提供完整性保護和真實性。RP可以配備一個從Ks_NAF得到的RP專用密鑰Ks_NAF_RP來核實OP簽名，作爲選擇，該密鑰可以是會話專用密鑰。然後，Ks_NAF_RP可以經由OPsup被傳遞到RP。在另一個實施方式中，KS_NAF可以直接用於創造和核驗簽名。

經由OP的間接通信的實施方式

在一個示例實施方式中，通過使用間接通信，可以將臨時用法從RP傳送到OP，然後，OP會將其轉發到MNO。MNO對該臨時用法進行簽名，其中該臨時用法可以包含在本地驗證成功之後被從OP反向傳送到RP的斷言中。由於MNO對該臨時用法進行了簽名，因此可以向RP提供表明OP在MNO發佈的UICC上運行的保證。

用於組合方法的實施方式

在一個示例實施方式中，可以使用在RP與MNO之間經由直接通信（例如

HTTPS連接）建立的共用秘密。然後，在驗證結束時，RP可能期望OP將該秘密包含在斷言消息中。

在另一個示例實施方式中，可以使用GBA。由於GBA協議不允許在NAF與UICC之間建立任意共用秘密（例如RP的秘密），因此，在這裏可以使用間接手段（例如同處一地的OPsup實體）。RP向OPsup發送會話識別字，OPsup可以使用GBA來與UICC建立共用秘密。然後，OPsup使用與UICC（由此結合UICC上的OP）建立的秘密相同的秘密來對會話識別字進行簽名，並且可以將帶有簽名的會話識別字送回RP。RP可以保持這個帶有簽名的會話識別字作爲參考。該RP將會話識別字包含在重定向消息中，由此可以允許OP使用GBA秘密來對其進行簽名。然後，OP可以將帶有簽名的會話識別字包含在發送給RP的斷言消息中。之後，RP可以比較來自OP和來自OPsup的帶有簽名的消息。如果兩者匹配，則RP證明OP屬於OPsup的MNO的使用者。該實施方式可以代表閉環處理，其中簽名匹配加固了消息保護處理並且建立了OpenID驗證。

4.2.2.2.3.2 當在MNO與智慧卡上的OP（分離OP）之間分離OP功能時使用GBA的實施方式

第18圖顯示的是允許實施分離OP的示例實施方式。如第18圖所示，在375，在RP與MNO之間可以建立關聯。RP可以與MNO建立共用秘密，然後，IP可以在斷言消息的簽名處理中使用該共用秘密。如果RP與不同使用者具有多個同時連接，那麼該斷言消息還有可能需要包含關聯控制，以使RP識別正確的共用秘密。該共用秘密可以允許RP核驗聲明簽名，而不必與OP進行通信。這種關聯可以在首次從RP重定向UE瀏覽器之前進行。

在380，OP可以向RP傳送驗證請求。在385，RP向OP傳送驗證回應。在390，OP可以與MNO建立關聯控制和簽名密鑰。該關聯控制和簽名密鑰可以用GBA建立。

在一個示例實施方式中，OP的功能可以劃分在MNO與本地OP之間。如果所使用的是RP與MNO之間的關聯，那麼RP可以與MNO建立共用秘密，然後，OP可以在斷言消息的簽名過程中使用這個共用秘密。如果RP與不同使用者具有多個同時的連接，那麼該斷言消息還有可能需要包含關聯控制，以使RP識別正確的共用秘密。該共用秘密可以允許RP核驗聲明簽名，而不必與OP進行通信。如果假設執行了GBA，那麼可以將MNO與RP之間的共用密鑰傳遞到受Ks_NAF保護的OP。由此，OP可以使用借助關聯建立的共用密鑰來對斷言消息進行簽名。

RP可以與MNO建立關聯，然後，MNO執行產生MNO與OP之間的共用秘密的GBA過程。MNO可以在RP可到達的伺服器上實施NAF功能。NAF可以與UICC上的OP建立共用秘密，而RP則從NAF接收共用秘密。關聯控制（爲NAF和RP所知）還可以被從MNO接觸點（NAF）發送到OP。然後，OP可以使用包含關聯控制的GBA共用秘密來對發送給RP的斷言進行簽名。由於RP已經借助關聯鏈路而從NAF那裏接收到了相同的共用密鑰，因此，RP可以核驗OP簽名。通過使用關聯控制，可以允許OP和RP處理多個（同時的）會話。

4.2.2.2.3.3 在分離終端中的行動OpenID中使用GBA的範例

在一個示例實施方式中，可以在瀏覽器和OP/UICC組合駐留在分離設備的分離終端配置中使用GBA。可以假設所使用的是分離終端類型的配置，但是OP是使用者本地的實體，並且其中如前所述，使用者在本地與OP執行驗證。

第19圖顯示的是啓用分離終端/本地OpenId的示例實施方式。如第19圖所示，舉例來說，確保兩個設備之間的頻道的安全的處理可以使用藍牙安全鏈路完成，或者可以借助TS 33.259中描述的用以建立共用密鑰Ks_本地_設備（Ks_local_device）的過程等等來完成。密鑰可以在UICC內部計算，並且可以經由安全隧道傳遞到瀏覽器。共用秘密的建立可以由GBA來支援

。該共用密鑰可以從GBA生成的密鑰Ks_(ext/int)_NAF中得到。

在一個示例實施方式中，當使用33.259時，這時可以使用具有基於證書的相互驗證的HTTPS來建立用於連接NAF和遠端設備的安全隧道。例如，瀏覽器可以是基於PC的，並且隧道是在網際網路/TCP連接環境中工作的。隧道的安全性可以借助信任機制來加固。依照行動電話規範（MPWG）中的需求，在這裏可以假設包含瀏覽器的遠端設備是相容TCG的。通過設備中的TPM證據，可以將HTTPS隧道確立綁定到瀏覽器設備的信任狀態。因此，嵌入本協議的完整性檢查會將Ks_本地_設備綁定到平臺。

在另一個示例實施方式中，作爲所述過程的一部分，存放使用者瀏覽器的遠端設備可以請求UICC主機設備向其發送NAF_ID列表。MiTM可以很容易地產生這種請求並接收被請求的ID。對於保護隧道的處理來說，其證書和相互驗證方面結合所假設的恰當信任特徵將會確保在分離終端配置內部不會發生MiTM攻擊，或者如果發生了這種攻擊，該攻擊也是能被檢測到的。一旦完成了這種設置，則可以將Ks_本地_服務密鑰經由隧道安全地發送到遠端設備；隨後，遠端設備（瀏覽器）可以發送密鑰生成請求消息（完整性受保護），以便在UICC主機設備上發起關於Ks_本地_服務的計算。

在這裏描述了用於分離終端類型配置的標識斷言協定。在這裏可以假設已經實施了GBA，並且實施了在遠端平臺（瀏覽器-PC）與包含UICC/OP（UE）的設備之間建立共用密鑰Ks_本地_服務的過程。如第19圖所示，在405（連接UE和NAF/OPsup）和400（連接UE和PC）處標識的頻道可以是安全的。在另一個示例實施方式中，MNO可以用於爲這裏的基於UICC的OP應用的標識斷言提供支援。

在另一個示例實施方式中：

·使用者使用OpenID登錄格式來將其OP識別字（URL）提供給RP（在395）

·使用者被RP重定向到其OP——該重定向消息包括臨時用法或會話識別字

·RP與MNO建立安全關聯（例如HTTPS連接——在410）

·RP還向OPsup發送會話識別字——該消息受前述安全關聯保護（在410）

·使用者使用通過瀏覽器輸入的PIN（或密碼）進行驗證

·在一個消息中將該資訊從PC經由400傳遞到UICC/OP，其中該消息還包括從RP獲取的會話識別字——如上所述，該消息是用Ks_local_device保護的

·OPsup使用GBA密鑰Ks_(ext/int)_NAF來對會話識別字進行簽名，並且將其送回RP，RP則保持該簽名作爲參考（410）

·現在，OP同樣使用GBA密鑰Ks_(ext/int)_NAF來對從瀏覽器發送給它的會話識別字進行簽名，並且將該簽名包含在隨後發送給RP的斷言消息中（395）

·RP比較這兩個簽名，其中一個簽名來自Opsup（410），另一個簽名來自OP（395）；如果兩者匹配，則RP斷定該OP屬於OPsup的MNO的使用者。

4.3 用於智慧卡web伺服器上的OP的有效協定的實施方式

本部分旨在顯現SCWS上的OP提供的優點，尤其是提供了有效改善並在本申請中被進一步描述的實施方式的優點。例如，所提出的實施方式可以是實施OpenID協定的實施方式，這些實施方式的其中一個優點是驗證業務量處於本地，並且除了現有HTTP消息流需要的空中介面網路或網路服務之外，該業務量不會對其他的空中介面網路或網路服務造成負擔。發現和關聯業務量並沒有經由空中介面網路，並且是在營運商OP與RP之間的固定線路的公共網際網路上進行的。

4.3.1 標準的OpenID

第20圖顯示的是標準的OpenID協定。對該協議來說，本地業務量是不存在的，並且從空中網路卸載的業務量僅僅是發現處理以及在RP與OP之間建立關聯的處理。由於OP是web服務，因此，使用者/瀏覽器/設備與OP之間的

所有通信全都會經由空中介面來進行。例如，信號420、435、440、445、450、455、460和465是在通過作爲資料業務量（例如HTTP，基於IP的通信）並經由在MNO/空中網路上執行的空中通信過程出現的。這代表了MNO網路上的負擔。此外，信號425和430是在固定線路的網際網路上出現的業務量，並且可以使用現有基礎架構。

4.3.2 OpenID/GBA

第21圖顯示的是來自3GPP TR 33.924 v9.1.0的OpenID/GBA的業務流程。對於該協議定義來說，無論RP與MNO之間具有怎樣的關聯步驟，所有通信都是在空中網路上進行的。但是，由於需要用於驗證的472和474，而這又會在空中資料網路以及GBA驗證需要的後端服務、即BSF和NAF子系統上增加負擔，因此，與基於web的OP相比，OpenID/GBA中的業務量甚至還會增大。因此，在這裏我們將會看到空中網路業務量增大，以及網路實體的負擔增大。

4.3.3 用於改善協定的實施方式

第22圖顯示的是用於減小空中傳送業務量的協定流程的示例實施方式。例如，該有效協議可以用於SCWS上的OpenID。在該實施方式中，假設在與SCWS相關聯的OP與MNO之間存在長期共用密鑰。

如第22圖所示，空中傳送業務量可以卸載到本地設備，從而減小空中介面網路業務量。舉例來說，通過執行該處理，可以允許驗證業務量處於本地，以使驗證業務量將空中介面網路或網路服務的負擔最小化。此外，發現和/或關聯業務量未必經由空中介面網路發生，並且可以在固定線路的公共網際網路上發生。

在480，使用者可以與瀏覽器之類的使用者介面形成介面，並且可以存取RP，以及使用OpenID來請求登錄。在485，RP和OP（MNO）可以基於OpenID標識來執行發現OP伺服器的發現。在490，RP可以向OP傳送關聯請求。OP

可以產生隨機的唯一關聯控制A，並且可以計算密鑰S。OP可以向RP傳送關聯回應。該關聯回應可以包括關聯控制A和密鑰S。所述RP則可以儲存密鑰S和關聯控制A。

在495，RP可以向瀏覽器傳送重定向。該重定向可以將瀏覽器重定向到OP，並且可以將關聯控制A包含在請求參數中。OP可以被關聯到SCWS。瀏覽器可以接收所述重定向，並且可以通過執行經過修改的本地DNS查找來映射到SCWS。在500，瀏覽器可以向OP傳送本地驗證請求。在505，驗證可以在本地進行。例如在510，OP可以基於長期共用密鑰K和關聯控制A來核驗證書。此外，OP還可以計算密鑰S，並且可以使用密鑰S來計算簽名。該簽名可以用於對斷言消息進行簽名，和/或對諸如return_to（返回_到）URL、標識和/或模式之類的參數進行簽名。

在515，OP可以向瀏覽器傳送能將瀏覽器重定向到RP的重定向。該重定向可以包括關聯控制A和帶有簽名的參數。在520，瀏覽器可以向RP傳送一個請求，該請求可以包括來自OP且帶有簽名的斷言消息。RP可以使用密鑰S來核驗斷言消息上的簽名。然後，在525，RP可以允許瀏覽器顯示登錄頁面，並且可以向瀏覽器提供服務存取。

4.4 用於在智慧卡web伺服器上實施OP的實施方式

存在可供使用者設備（UE）與SIM卡通信的可用並被標準化的方法，例如，3GPP TS 11.14規範定義了可供SIM應用使用的SIM應用工具箱（SAT）介面，但是並未定義如何可以在來自不同SIM廠家的不同SIM卡類型上以統一的方式使用命令。在一個示例實施方式中，通過使用SIM應用工具箱，SIM卡可以獲得對UE的臨時控制權（先期採取行動）。與UE向SIM卡發送請求並且SIM卡做出回應的情形相比，UE可以從SIM那裏取得SAT命令。SIM卡向UE發佈SAT命令；無論命令是否執行成功，UE都會做出相應的反應，並且向SIM回送回應。

4.4.1 智慧卡web伺服器上的OP

智慧卡web伺服器（SCWS）是在USIM卡上運行的web伺服器，其行爲與傳統的web伺服器相似。它可以被視爲是SIM工具箱的進步，並且在用於顯示電話簿的當前應用方案中，它可以被視爲使用本地UE瀏覽器且經由HTML介面的額外MNO服務等等。SCWS使用了標準的HTTP協定來將其內容遞送到瀏覽器，但是與傳統的web伺服器不同，SCWS可以使用兩個不同的承載：BIP（在T=0智慧卡協定之上）或USB介面上的完整TCP/IP堆棧（在卡上實施）。UE負責路由那些來自SCWS USIM和去往SCWS USIM的業務量，由此充當了將(U)SIM連接到MNO和網際網路的閘道。如果使用的是BIP，那麼ME中的路由器會將來自UE瀏覽器的某些HTTP請求重定向到本地SCWS。所定義的TCP埠上的HTTP請求將被發送到（U）SIM上的SCWS，並且響應中的HTML頁面是由SCWS產生的。不使用專用於BIP的TCP埠的HTTP請求被引導到網際網路上的伺服器。如果在(U)SIM上將USB協議與完整的TCP/IP堆棧組合使用，那麼UE與將內部網連接到網際網路的其他計算機具有相同的IP閘道功能。ME閘道還取決於使用的IP協定版本，即IPv4或IPv6。與BIP相比，完整的TCP/IP堆棧還提供了將請求從(U)SIM路由到網際網路的可能性。

第23圖顯示的是用於SCWS上的OP的內部路由的示例實施方式。如第23圖所示，SCWS可以用作OP的基礎，並且UE的路由能力可被修改，以便在指定的外部埠上作出反應，以及將通信轉發到SCWS上的OP。例如，通過執行該處理，可以在不具有經過瀏覽器的隧道的情況下創造直接通信。這些業務量有可能仍舊經過相同的設備，但是有可能以不同方式被重定向。

UE中的路由功能（RF）可以啓用多條通信路徑。當使用者首次使用瀏覽器存取RP站點時，RF可以將所述請求經由可用的出站TCP/IP介面（例如3G網路連接性）重定向到RP。現在，由於在該連接上建立了公共會話，因此，RP知道瀏覽器的IP位址。RP可以使用與使用者/瀏覽器會話中相同的位址

來與OP取得聯繫。RP可以在設備上使用另一個（預定義的）埠，該埠不同於在與瀏覽器進行的HTTP會話中的埠。RF將這個埠看做是應被路由到SCWS上的OP的埠。RF可以直接將消息重定向到OP，該OP可以允許RP與OP建立關聯。RP還有可能向瀏覽器發佈重定向，以便執行OpenID驗證。該瀏覽器可以被重定向到SCWS上的OP。RF可以將來自瀏覽器的呼叫看做是可被路由到本地SCWS的呼叫。OP可以執行本地使用者驗證（該處理即可以經由安全的UI進行，也可以由SCWS作爲控制所述設備的UICC能力的一部分來提供，而這通常需要使用者提供PIN碼）。

在驗證之後，OP可以用肯定斷言來將瀏覽器重定向到RP。由於RP和OP有可能已經建立關聯，因此，RP能夠自主核驗該斷言。如果不能創造關聯，那麼還可以實施OpenID的直接核驗方案。在這種情況下，RP在接收到肯定斷言之後即可在預定埠聯繫UE，RF會將請求路由到OP，而OP可以應答核驗請求。

在一個示例實施方式中，在本地設備上可以限制針對OP的存取。例如，只有本地瀏覽器才可被允許獲取關於標識的斷言。這樣做可以防止攻擊者從外部設備檢索標識斷言。RF還可以將入站業務量到OP的路由與先前的瀏覽器請求相耦合。例如，對於與瀏覽器通信的單個RP來說，路由有可能在有限的時間中是活動的。

MNO還可以使用RF而分別在SCWS和OP上執行管理任務。

4.4.1.1.1 一般需求

以下是OpenID規範闡述的一般需求：

（R-1）在OpenID中，RP可以決定在無狀態或是以關聯爲基礎的通信模式中工作。由於不能在RP上進行假設，因此，這兩個選項全都需要得到OP實施方式的支援。

（R-2）在無狀態模式中，在OP與RP之間沒有建立共用秘密，在RP經由瀏

覽器接收到來自OP的斷言消息之後，RP會直接與OP取得聯繫。然後，RP會與OP建立直接的HTTP(S)連接，以便請求OP核驗該斷言消息上的簽名。OpenID規範允許兩種不同類型的（對稱）簽名方案：HMAC-SHA1-160位元密鑰長度以及HMAC-SHA256-256位元密鑰長度。如果RP使用了關聯，那麼，在關聯建立處理中，在OP與RP之間可以交換該對稱密鑰。秘密交換是以如下方式保護的：使用Diffie-Hellman密鑰交換保護，隨後用DH-密鑰-值來加密共用秘密，或者如果沒有使用Diffie-Hellman，則必須通過傳輸層安全措施來保護連接免受竊聽者竊聽。OP在斷言消息上發佈的所有簽名都是使用了所提及的演算法中的一種演算法的對稱簽名。諸如全球平臺之類的智慧卡術語使用了術語密碼或是更常見的“資料驗證模式（DAP）”來描述這種密碼簽名方案。

（R-3）在基於關聯的OpenID中，RP與OP建立用關聯控制識別的共用秘密。RP將這個關聯控制包含在初始重定向消息中，該消息將瀏覽器重定向到OP。然後，OP可以使用關聯控制來發現RP的共用秘密，並且然後使用該秘密來對斷言消息進行簽名。一旦接收到這個消息，RP可以自動核驗接收到的簽名。

（R-4）在（R-1）、（R-2）、（R-3）中描述的通信選項全都需要從RP到可以經由公共網際網路到達的實體E1的至少一個直接連接，其中對正常OpenID來說，E1是OP伺服器。

（R-5）來自（R-4）的實體E1必須能在基於關聯的模式在OP伺服器與RP之間建立共用秘密。在無狀態模式中，該秘密必須爲OP所知，以便對消息進行簽名，此外，該秘密還必須爲這個可到達實體E1所知，然後，RP會通過與之聯繫來核驗OP簽名。

（R-6）OpenID中的簽名一般以HMAC-SHA1爲基礎，OP和核驗方必須能使用恰當演算法來對資料進行簽名並核驗簽名。

（R-7）MNO必須提供網路實體E2，所述網路實體E2依照OpenID標準來提供借助於HTML或XRDS發現的OP發現處理。實體E2必須在作爲OpenID識別字一部分的DNS位址上運行，例如，如果該識別字是http://openid.mno.com/id，那麼MNO必須在http://openid.mno.com上運行web服務E2，也就是說，MNO必須具有所述域和伺服器，以便作爲發現服務來運行。發現服務借助於公共網際網路進行，並且可以是羽量級的。實體E2可以與來自（R-4）的實體E1共處於提供這兩種功能的公共物理實體中。此外，E2可以與E1分離，在這種情況下，發現處理爲使用OpenID的漫遊設備選項提供了進入點。

（R-8）來自（R-7）的E2的（DNS）地址不應改變，以便爲使用者提供一致的識別字。

（R-9）OP必須能夠由使用者瀏覽器至少經由HTTP到達。

（R-10）與（R-9）中相同的連接可以使用HTTPS而不是HTTP。

可選的（R-11）：OP必須能夠產生並顯示用作驗證頁的HTML頁面。由於未規定實際驗證，因此該處理是可選的。如果未使用驗證頁面，那麼OP至少應向使用者告知其OpenID識別字已被使用，以免隱瞞標識的使用情況。但是，不顯示驗證頁面可能有益於爲使用者提供更爲一致的SSO體驗，例如，使用者每天只對SCWS上的OP進行一次驗證，然後，所有的後續驗證處理都會自動進行。

可選的（R-12）：如果使用了驗證頁面，並且該驗證頁面接收來自使用者的資料，例如使用者名稱和密碼，那麼OP必須能接受該資料，對該資料進行處理和核驗，以及執行相應的操作。

可選的（R-13）：如果使用了驗證頁面，那麼該驗證頁面可以使用RP接收的資訊而以易於理解的方式向使用者使用者顯示額外資訊，例如通過顯示RP名稱以及將在文本中使用、作爲圖形圖像使用或者同時以這兩種方式的

組合形式使用的識別字。

可選的（R-14）：如果使用了驗證頁面，則驗證頁面可以包括被用作指示符的（可視）秘密，該指示符向使用者表明該使用者正在與合法的OP進行通信。

4.4.1.1.2 在OpenID中使用SCWS的實施方式的實施方式

上一節論述的是OpenID標準設置的一般需求。在本節中，我們將要描述的是用於在如上所述OpenID需求以內實施使用SCWS的本地OP的實施方式。

在一個示例實施方式中，SCWS可以不是從公共網際網路直接可到達的，也就是說，RP不能直接與SCWS上的OP取得聯繫。如果給出了需求（R-1）、（R-2）、（R-3），那麼可以使用間接指向。例如，MNO可以提供能夠經由公共網際網路到達的web服務，並且該服務能夠與關聯於SCWS的OP共用秘密（參見本文中關於分離OP的章節）。此外，該web服務還能與RP共用該秘密，由此可以在RP與關聯於SCWS的OP之間共用秘密。在另一個實施方式中，RF可以將請求路由到SCWS上的OP。

從MNO到SCWS的通信可以借助HTTP(S)並經由遠端管理介面進行，例如經由SCWS遠端更新和相關聯的小應用程式來進行，該通信也可以來自手機瀏覽器並借助本地HTTP(S)來進行。本地連接介面可以被用於OpenID通信。另外，本地連接還可以充當用於與SCWS和OP通信的通用HTTP(S)介面。

ETSI SCP定義了借助TCP/IP的智慧卡存取（9），並且該存取可以不僅限於本地存取。例如，從外部實體對SCWS進行的受限存取可能不是技術問題；相反地，依照用於SCWS的當前標準規範，它有可能是設備內部的路由功能限制。對SCWS進行的直接HTTP存取可以在SCWS的未來版本中實現。此類存取可以不是管理存取。例如，對OpenID操作而言，RP可以存取由SCWS提供服務的網頁（實施OP伺服器邏輯的動態小應用程式）。

4.4.1.2 用於爲將OP-相關聯的-SCWS實施處理額外和衍生需求的實施方式

當在UICC上實施OP並且OP與SCWS相關聯時，以下實施方式有可能產生額外需求：

（RSCWS-1）在一個示例實施方式中，MNO必須實施支持OP伺服器功能（OPSF），該OPSF能夠與關聯於SCWS的本地OP（以及可選地與RP）產生、共用和分佈用於OpenID協議的秘密。

所述支援OP功能有可能需要在RP與UE上的本地OP實體之間爲在OpenID上的簽名中使用的共用秘密充當協商可信方。該支援功能可以提供HTTP(S)介面，以使RP發起關聯處理（如果使用了關聯）或者在RP請求時確認來自本地OP的簽名。因此，它是可以經由公共網際網路到達的，並且該功能還必須能與本地OP進行通信，以便交換秘密。這種針對本地OP的通信可能必須至少在使用者希望存取的每一個RP上執行一次。在一個示例實施方式中，本地OP由MNO管理和維護。MNO可以通過與本地OP/SCWS進行通信來更新共用秘密，而OMA SCWS標準可滿足需要。在另一個示例實施方式中，非MNO的遠端OpenID標識服務對智慧卡上的本地OP進行管理並與之通信，此外，也可以使用全球平臺標準。

通常，在OP與RP之間可以爲每一個RP建立新的（對稱）秘密。由於很難限制使用者存取的RP使用OpenID登錄，因此很難爲使用者希望在未來存取的所有RP預先提供這些共用秘密。如果每一次爲UICC中的每一個RP產生秘密（例如從種子值中將其導出），那麼可以將該秘密與RP共用，這一點參見在稍後章節中的協定流程，在那裏我們將對該選項進行討論。

（RSCWS-2）在另一個示例實施方式中，來自（RSCWS-1）且由MNO操作的網路實體可以使用不同的頻道和通信方法而在與SCWS關聯的OP中建立秘密，並將其分佈給RP。從MNO到RP的通信被OpenID協議限制成是基於HTTP的通信。從MNO到與SCWS相關聯的OP的通信可以使用安全的SMS-PP，或者舉例來說，該通信可以由GBA引導，和/或可以使用安全的通信協定，例如

HTTP(S) SCWS遠端管理介面。

（RSCWS-3）在另一個示例實施方式中，與SCWS相關聯的本地OP必須可以存取在來自（RSCWS-1）的MNO實體與智慧卡之間共用的秘密。這些秘密並不是網路專用密鑰，而是僅用於OpenID協定；如有需要，它們可被呼叫，並借助OTA措施來重新建立。這些秘密是供OP用於對從RP發送的HTTP參數進行簽名的對稱密鑰。

如果OP擁有本地OP，那麼MNO可能不必分佈這些秘密，這是因爲OP可以與其本地OP建立密鑰（得到GP和/或GMA的確認）。MNO有可能需要用於遠端管理SCWS的秘密，但是他有可能借助該途徑來建立用於本地OP的密鑰。

（RSCWS-4）在另一個示例實施方式中，對來自（RSCWS-3）的秘密的保護應該使其不能從手機上的其他應用中被讀取，並且作用於這些秘密的所有演算法都是在智慧卡提供的安全環境中運行的，由此不會將秘密暴露在智慧卡環境中的應用空間之外。

如果本地OP是全球平臺應用，那麼可以由本地OP的安全域來儲存密鑰，其中所述本地OP的安全域爲本地OP執行密碼運算。

（RSCWS-5)在另一個示例實施方式中，與SCWS相關聯的本地OP可以儲存供OP在以後使用的秘密和關聯控制，從而如果再次存取該RP，則可以減少從MNO到OP的額外OTA業務量。

（RSCWS-6）在另一個示例實施方式中，與SCWS相關聯的本地OP可以在顯示給使用者的驗證頁面中使用只能由合法的本地OP顯示的額外安全特徵，例如安全地儲存在智慧卡中的秘密圖像。

（RSCWS-7）在另一個示例實施方式中，與SCWS相關聯的OP必須實施處理HTTP請求和顯示HTML頁面的應用邏輯之外的應用邏輯，尤其是用於對來自RP的參數進行簽名的應用邏輯。

（RSCWS-8）在另一個示例實施方式中，如果使用了由與SCWS相關聯的OP

產生秘密的實施選項，那麼來自（RSCWS-7）的應用邏輯必須產生對稱秘密，並且將其安全傳遞到MNO網路中的實體。

（RSCWS-9）在另一個示例實施方式中，來自（RSCWS-7）和（RSCWS-8）的應用邏輯可以在由SCWS動態呼叫的Java小應用程式或小服務程式中實施，以便執行必要的操作，隨後將控制權返回給SCWS。所述小應用程式/小服務程式應在UICC中的安全環境裏運行。

（RSCWS-10）在另一個示例實施方式中，SCWS可以提供用於驗證的動態網頁，該網頁基於使用者設定檔來顯示從MNO檢索的資訊，例如廣告橫幅，其中該使用者設定檔可以通過追蹤在RP上使用的使用者OpenID標識來產生。MNO可以在SCWS上提供用於市場行銷/廣告目的的RP‘網路空間’。這樣做會爲SCWS上的OP帶來另外的價值。

（RSCWS-11）在另一個示例實施方式中，如果SCWS證明在具體方案中過於受限，那麼另一個選項可以是基於模仿SCWS功能的JavaCard應用來實施應用邏輯：該應用接受輸入的HTTP請求，爲使用者提供驗證介面（例如PIN），對簽名進行計算，生成HTTP回應，以及向瀏覽器做出回應。在該方案中可以探究BONDI框架是否有助於瀏覽器與取代SCWS的智慧卡應用之間的間接通信部分。

4.4.1.3 命名規則

用於實體的下列命名規則是適用的：

·與SCWS相關聯的OP：本地OpenID標識供應方，其發佈帶有簽名的斷言消息，並且將這些消息通過使用者瀏覽器發送到RP。存放SCWS的智慧卡乃至OP被假設成與MNO具有關係，由此與MNO關聯的所有實體都具有關係。

·RP：依賴方，它可以是任何使用OpenID來爲使用者提供登錄的網站。RP完全獨立於所有其他實體，因此，在RP上不能施加額外需求，並且不能改動用於RP的OpenID協定流程。OP必須支援RP選擇使用的任一通信模式（無

狀態或基於關聯）。如果MNO決定使用者不應該使用某些RP，那麼由於使用者還可以使用別的標識，因此，MNO不能通過拒絕對於這些RP的OpenID存取來拒絕對於這些站點的存取。MNO只能使用額外裝置來限制對於RP的存取，其中所述額外裝置通常阻止的是對消耗帶寬的站點進行的存取。

·OP-Agg：OP-Agg實施的是來自（R-7）的實體E2，其爲RP提供了發現服務。

·OPSF：OP服務功能（OPSF）實施的是能與關聯於SCWS的OP並且可選地與來自（RSCWS-1）的RP一起產生、共用和分佈秘密的支援OP功能。從RP的角度來看，OPSF和關聯於SCWS的OP的行爲就好像它們是單個實體。OPSF能夠核驗與SCWS相關聯的OP發佈的簽名，並且可以由RP經由公共網際網路直接到達。通過修改設備上的本地DNS解析快取，可以將設備上的瀏覽器重定向到與SCWS相關聯的OP，以使OPSF的位址映射到與SCWS相關聯的本地OP。

·瀏覽器：在協定流程圖中顯示，以便明確往來於與SCWS相關聯的OP的路由和消息傳遞功能。否則，它只是顯示和接收使用者驗證的前端。

4.4.1.4 用於在SCWS/UICC上實施OP的實施方式

在嘗試保持相容標準的OpenID驗證協定的同時，本節使用了從如上所述的通用概念中得出的實施方式。以下論述了無狀態和基於關聯的模式協定的兩個實施方式；其中第二實施方式使用了密碼假設，這其中包括在OP卡功能與網路側的伺服器功能之間共用密鑰，以便加強驗證過程。

4.4.1.4.1 協定流程描述

以下章節描述了用於實施與SCWS相關聯的OP的協定流程的示例實施方式。在一個示例實施方式中，如上在（R-1）中顯示的，這兩個方案（無狀態和基於關聯）都可被覆蓋。在下文中提供了關於實施方式的呼叫流程的協定流程圖和描述。通用的OpenID協定則是對照第3圖顯示的。

在第24-27圖中顯示了多個選項，並在相應的描述中解釋了這些選項。

4.4.1.4.2 用於使用無狀態模式的RP的協定流程

第24圖顯示的是能使RP使用無狀態模式來執行OpenID驗證的協定流程的示例實施方式。例如，RP可以使用無狀態模式來執行OpenID使用者驗證。如第24圖所示。

530：使用者可以存取RP網站並輸入其OpenID識別字。例如http://op.org/identity。

535：瀏覽器可以向RP網址發送包含了OpenID識別字的HTTP消息。

540：RP可以使用基於HTTP/HTML的OpenID‘簡單’發現處理，並且經由公共網際網路來聯繫OP-Agg，以便檢索針對OpenID識別字的標識頁面。例如，HTTP獲取（GET）http://op.org/identity。

545：OP-agg可以接收該請求，並且使用包含了OPSF的網際網路位址的HTML頁面來做出回應，例如包含以下位址：

<link rel = “openid.server” href =http://op.org/server.cgi>

OPSF可以像標準的OpenID標識供應方web服務一樣對RP進行操作，也就是說，在RP請求時，OPSF能夠核驗斷言消息上的簽名（由本地OP發佈）。

OPSF可以經由公共網際網路到達，並且可以被假設成具有能夠經由http://op.org到達的DNS名稱，如op.org。由於外界不可能知道智慧卡的IP位址，因此使用了這種間接OP-agg和OPSF來進行通信。

OPSF的位址可以不同於OP-agg的位址。

a．選項1：該項並非必需，而是給出一個選項。如果在這裏未使用該選項，則可以在協定的後續階段中使用570處的選項2。

i．OP-agg通過向OPSF發送RP識別字和OpenID使用者識別字來向OPSF告知來自RP的請求。

ii．OPSF可以嘗試在本地資料庫中查找關於該RP的秘密和OpenID標識。

iii．如果沒有發現秘密，則OPSF可以產生新的秘密和關聯控制，並且將

這二者發送到與SCWS相關聯的OP，所述SCWS則轉而對其進行儲存。

iv．如果發現秘密，則OPSF會在以後使用該秘密來執行簽名核驗。可以假設，如果OPSF在本地資料庫中發現了秘密，那麼與SCWS相關聯的OP已經在先前與該RP執行的協議過程中接收到該秘密和關聯控制，由此能夠儲存並重新使用該秘密。

OPSF用以核驗簽名的秘密與關聯於SCWS的OP用以產生簽名的秘密可以是相同的。簽名的新鮮度可以由下一個步驟中插入的RP臨時用法來確保，並且該RP臨時用法需要是簽名的一部分。OpenID規範對簽名秘密本身的新鮮度保持默認。OP負責確保秘密的密碼強度，保持其秘密性，以及在需要時確保其新鮮度。OPSF和關聯於SCWS的OP可以持續有限壽命或是用於對該目的簽名秘密的使用計數。關於秘密共用的選項的更多內容是在第4.4.1.4.3.1節中描述的。

550：RP可以接收OPSF的位址，並且創造臨時用法和會話識別字，例如臨時用法=123123，會話=使用者。RP可以編譯return_to（返回_到）參數，該參數向OP告知應該在使用者驗證之後將瀏覽器重定向到哪一個URL。RP可以發佈HTTP重定向，由此將瀏覽器重定向到OP伺服器位址，其中所述HTTP重定向可以包含下列參數：

openid .mode = checked_setup ,

openid .identity = http://op .org/identity ,

openid .return_to = http://rp .org/return

.cgi?session=User&nonce=123123

555：瀏覽器可以接收重定向，並且開放與RP在重定向消息中規定的URL相連的連接。

560：結合可以將OPSF的URL映射到SCWS本地IP位址的經過修改的本地DNS查找表，例如通過使用具有項http://op .org == 127 .0 .0 .1的主機

檔，可以將瀏覽器重定向到與SCWS相關聯的本地OP，並且發佈包含了來自550的參數的HTTP請求。

經過修改的本地DNS查找表可以在設備上使用，並且它會使設備認爲URL http://op .org處於SCWS的本地IP地址。因此，瀏覽器可以開放與SCWS/本地OP的連接，而不是連接到OPSF（可以經由在URL http://op .org的公共網際網路而到達該OPSF）。

565：通過執行以下處理，可以確保將驗證業務量保持在本地，這些步驟不是OpenID協定規範所需要或規定的：

a. OP可以與SCWS相關聯，並顯示本地驗證頁面

b. 使用者可以輸入其驗證證書，例如使用者名稱和密碼

c. OP可以與SCWS相關聯，以核驗這些證書

570：如果使用的是處於545的選項1，那麼與SCWS相關聯的OP有可能具有在關聯於SCWS的OP與OPSF之間共用的秘密和關聯控制，其中所述秘密和關聯控制是從OPSF那裏新接收的，或者是從秘密和關聯控制的本地記憶體中檢索得到的。

a．選項2，如果在545沒有使用選項1：

i．與SCWS相關聯的OP可以產生新的秘密和關聯控制

ii．與SCWS相關聯的OP可以將這個秘密和關聯控制經由SCWS發送到OPSF

iii．OPSF可以接收該秘密，並且安全地儲存該秘密，以便用於以後的存取

舉例來說，這裏的目標可以是在OPSF與本地OP之間共用秘密，因此，如果本地OP生成秘密，則可以在生成該秘密之後將其傳遞到OPSF。

啓用工具箱的本地OP可以使用CAT來主動與手機通信，從而繞過SCWS。該消息可以依照標準的OTA（例如用於經由SMS-PP承載來發送OPSF的OTA）而被格式化。但是，這種處理有可能需要OPSF經由MNO的OTA系統來與所述卡

進行通信。作爲替換，BIP閘道可以擷取工具箱消息的有效負載，並且手機可以使用TCP/IP將其發送到OPSF。但這仍舊要求消息經由MNO的OTA伺服器。如果所述卡不具有IP位址並且不支援TCP/IP，那麼可以使用BIP。

575：與SCWS相關聯的OP計算下列參數的簽名：return_to、標識以及模式。

580：與SCWS相關聯的OP向瀏覽器發送HTTP重定向消息，其中包含了在步驟550中從RP接收到的參數，此外還包括下列各項：

openid.signed參數中的一系列帶有簽名的參數，

openid.assoc_handle參數中的關聯控制，以及

openid.sig參數中的簽名（base64編碼）。

該消息用於將瀏覽器重定向到RP上的return_to URL。

585：瀏覽器將使用者重定向到RP上的return_to URL。

590：RP接收帶有簽名的斷言消息，並且通過經由公共網際網路且基於HTTP（S）的直接通信來參與到與OPSF一起進行的核驗過程中。

595：RP發佈一個HTTPPOST消息，該消息包含了在580中從與SCWS相關聯的OP接收到的參數。

600：OPSF使用共用密鑰來核驗接收到的資料上的簽名。

605：如果簽名核驗成功，則OPSF返回is_valid:真（true）。

610：對RP來說，使用者現在被標識爲http://op.org/identity。

615：瀏覽器顯示RP的HTML頁面。

620：將使用者作爲http://op.org/identity登錄到RP上。

4.4.1.4.3 用於無狀態模式的額外實施方式

4.4.1.4.3.1 共用秘密

OpenID的無狀態模式的特徵在於RP從OP那裏接收帶有簽名的聲明的過程，但是由於RP不知道用於簽名的秘密，因此其本身是不能核驗該簽名的。在

無狀態模式中，RP再次與OP進行聯繫，以便核驗簽名。由於從RP的角度來看，發佈簽名的OP（與SCWS相關聯）和檢查簽名的OP（OPSF）被視爲相同的實體，因此它們必須能夠共用秘密。適用於此的選項有若干個。

4.4.1.4.3.1.1 選項1：由OPSF來管理秘密

本節概述的是一些使用了在上文中參考第24圖描述的454處的選項1的實施方式。一旦執行發現過程，則OP-agg可以向OPSF發出通知。然後，OPSF可以創造秘密和關聯控制，並且將這二者發送到與SCWS相關聯的OP。如果OPSF是MNO的一部分，那麼可以使用SCWS遠端管理處理。如果OPSF不是MNO的一部分，那麼在假設手機提供支援的情況下，全球平臺方法允許OPSF向所述卡上的本地OP發送密鑰。在選項1中，在OPSF上可以實施中心秘密/關聯控制資料庫及管理，其在資料庫中儲存了OpenID識別字、RP到關聯控制以及秘密的映射。一旦OPSF接到通知，則OPSF可以執行標識和RP查找，如果沒有發現秘密，則OPSF可以生成新的秘密和關聯控制，並且將其發送到SCWS上的OP。本示例實施方式假設SCWS上的OP能夠儲存RP的秘密以及關聯控制，並且SCWS上的OP用於簽名的秘密與OPSF用於簽名核驗的秘密是相同的。然後，該過程會在每一個RP上執行一次。

4.4.1.4.3.1.2 選項2：由SCWS上的OP生成新秘密

本節概述的是一些使用了在上文中參考第24圖描述的選項2的實施方式。一旦接收到來自RP的參數，則與SCWS相關聯的OP可以產生新的關聯控制和秘密。與SCWS相關聯的OP可以使用該秘密來對參數進行簽名，然後將這個秘密和關聯控制發送到OPSF。如果SCWS上的OP也能夠儲存該秘密，那麼OPSF可以決定儲存這個秘密和關聯控制，以便在以後使用。然後，該過程可以針對每個RP只執行一次。該處理假設已經存在永久性秘密，所述秘密可以允許本地OP對新秘密進行加密，以使其只能被OPSF解密。這種加密處理允許本地OP在不需要傳輸層安全性的情況下向OPSF發送新的秘密。

4.4.1.4.3.1.3 選項3：從公共種子中導出的秘密

在一個示例實施方式中，如果關聯於SCWS的OP和OPSF共用了公共種子，該公共種子可以被預先確立並獨立於結合不同RP所使用的一個或多個秘密，那麼可以使用另一個變體。假設SCWS上的OP和OPSF共用公共種子值S。通過將加密功能應用於在唯一識別當前的OpenID過程的通信過程中接收的S和資訊P，這二者可以擁有相同的秘密。例如，該共用秘密可以通過將散列函數應用於S與P的串聯來計算，例如通過將共用秘密作爲k=SHA1(SIP)來計算。通過檢查關聯於SCWS的OP和OPSF接收到的信息P，可以考慮不同的候選者，例如RP IP位址和OpenID識別字、從RP接收的整個參數集、參數子集以及上述各項的任何組合等等。

與預先生成並可以在需要時使用秘密和關聯控制的密鑰推導功能中一樣，這樣導出的秘密也可以依照公共模式來預先生成。

4.4.1.4.3.1.4 更進一步的選項

更進一步的選項也是適用的，這些選項可以產生類似的狀態，例如OP和OPSF共用相同秘密的狀態。

4.4.1.4.3.2 驗證選項

由於在OpenID規範中並沒有規定實際使用者驗證，因此，不同的選項都是適用的。

4.4.1.4.3.2.1 用於集成來自可信OpenID的概念的實施方式

在一個示例實施方式中，舉例來說，通過使用TPM，設備可以產生關於軟體的測量。然後，這些測量可以在驗證會話過程中被傳送到與SCWS相關聯的OP。本地OP可以具有用於與測量進行比較的參考值，並且只有在所報告的測量與這些已知的良好參考值相對應的情況下，該驗證才會成功。

4.4.1.4.3.2.2 使用驗證證書來解鎖OpenID秘密

在一個示例實施方式中，使用者和OPSF可以共用公共秘密，例如PIN碼。

PIN碼可以用於在使用者每次輸入證書的時候計算秘密，這與在4.4.1.4.3.1.3中描述的實施方式相似。該PIN可以通過帶外登記處理來共用。

4.4.1.4.3.2.3 將使用者驗證綁定到設備和網路驗證

如果智慧卡（和SCWS）支援生物測定使用者驗證，那麼可以將OpenID驗證與使用者提供的生物測定識別字綁定。由於OP位於本地（在智慧卡上），因此，它可以直接存取生物測定參考資料，並且不會向MNO或別的網際網路實體洩露生物測定資料。

在一個示例實施方式中，通信設備可以連接到網路。該設備可以保持證書，所述證書可以安全地保存在設備或是UICC之類的智慧卡上，並且所述證書被用於啓用設備對網路的驗證。爲了向那些只能被所述使用者存取的設備和網路服務提供安全的存取，所述設備上可以包括生物測定掃描器，以便提供完全的三要素驗證機制，其中所述機制組合了生物測定、使用者知道的某些事物（例如pin或密碼）、以及使用者具有的某些事物（例如安全權杖生成器fob）。

通過與先前描述的用於設備驗證的實施方式相結合，還可以在驗證過程中引入使用者驗證。在使用者使用這些驗證機制的組合而向設備驗證了該使用者本身之後，設備可以檢查使用者驗證是否正確，也就是說，設備首先對使用者進行驗證，然後，如果結果證明無誤，則將那些已被檢查的使用者驗證資訊（例如採用原始形式、散列形式或其他壓縮形式而在使用者驗證過程中使用的使用者證書）組合到其自身內部保持的設備證書中，之後則將組合的綁定證書資訊發送到網路。

一旦接收到組合的證書，則網路可以評定該設備是否正被合法使用者使用，以及設備本身是否合法。

如果設備本身不能檢查使用者的真實性，那麼它可以先將組合的證書資訊

發送到網路，而不允許使用者執行任何其他處理，並且只在網路評定組合證書並且傳達了關於使用者通過驗證的資訊之後才允許使用者存取它的其他功能。然後，設備可以允許使用者存取它的其他功能。

該方法可以提供最嚴格的安全性，但是基於所實施的安全策略，驗證中使用的要素數量有可能減少。

驗證機制

可以引入這些實施方式的驗證方案包括：

1．使用者向設備提供所有的三種形式的驗證資訊，這樣針對設備對使用者進行驗證。一旦驗證成功，則提供對設備功能以及保持在設備上的資料的存取。然後，設備採用正常方式來向網路驗證，以便爲使用者提供設備上可用的基於網路的服務。

2.使用者向設備提供所有三種形式的驗證資訊，這樣會使用某些或所有資訊來向設備驗證該使用者，一旦驗證成功，則將某些或所有驗證資訊連同保持在設備上的證書資訊一起傳送到網路，以便用於與網路進行額外驗證。一旦設備與網路間的驗證成功，則允許使用者存取設備功能、保持在設備上的資料以及基於網路的服務。

3.上述（2）的一個變體是向網路發送生物測定資訊或是安全導出的唯一資訊元素，例如生物測定資訊的模糊散列，以便進行網路級使用者驗證，而不需要將使用者生物測定資訊用於針對設備的本地驗證。

4.（2）或（3）的另一個變體是允許使用者受限地存取設備功能和資料，直至網路驗證了該使用者（以及設備），並且設備獲得了網路回送的關於該評定的指示。在該模式中，使用者將被允許存取或使用某些預先指定的“安全有保證的”功能、以及那些只有在完成了使用者和設備證書的網路驗證以及向設備回送了恰當授權之後才允許存取的功能。

將使用者驗證功能分散在設備與網路之間或者分佈於一個實體的上述機制

的變體也是可行的。此外，通過將使用者驗證與設備驗證綁定，可以提供關於使用者和/或設備的強驗證。

雖然可以引入多種生物測定類型，但是示例實施方式可以使用指紋掃描器或視網膜掃描器之類的生物測定掃描。通過引入生物測定掃描作爲使用者介面的自然延伸，可以採用一種在使用者執行功能或者存取處於設備本地或其他經由通信網路的特定服務時，基於觸發事件來提供動態透明的使用者驗證的方式將生物測定掃描引入到安全功能中。例如，指紋掃描器可被引入一個軟鍵，以使手指敲擊時觸發軟鍵操作，例如“發送”，從而在驗證使用者的同時進行呼叫。作爲替換，通過結合使用者在顯示器表面、設備主體或觸摸按鍵上對設備進行的物理接觸，可以採用一種不引人注目的驗證處理來向設備連續地驗證使用者。

4.4.1.4.4 使用了基於關聯的模式的RP的協定流程

第25圖顯示的是允許RP使用基於關聯的模式來執行OpenID使用者驗證的協定流程的示例實施方式。該關聯可以在使用者首次與RP進行聯繫並將其OpenID識別字與該RP結合使用之後進行。如果建立了關聯，則可以重新使用該關聯，這樣做會進一步減少通信工作。但是，OP可能不會要求RP的工作模式，並且有可能由RP來決定兩種通信模式之一。

該關聯在RP與OP之間建立永久性秘密，並且RP可以使用該秘密來對斷言消息進行簽名，此外，RP還可以使用該秘密來核驗OP簽名。OP可以決定共用秘密的有效期。RP和OP使用關聯控制作爲所述秘密的識別字。該RP將關聯控制包含在去往OP的第一請求消息中，然後，OP可以根據關聯控制來使用相應的秘密。如果OP確定該關聯已經到期，那麼OP會在回應消息中通知RP。原則上，這樣做可以允許OP拒絕任何關聯請求。只要RP也能支援無狀態模式，則可以使用該處理來迫使RP退回到無狀態通信模式。例如，如果OP不能支援RP請求的簽名模式（HMAC-SHA1或HMAC-SHA256），那麼OP可以

拒絕關聯請求。

與使用者每次登錄RP時都在RP與OP之間建立新秘密的無狀態通信模式相反，每一個標識和RP都會建立一次關聯。如果在OP與RP之間已經建立關聯，那麼RP和OP可以重新使用該關聯。

一旦知道了OPSF的位址，也就是在發現階段之後，RP可以建立關聯，並且在繼續執行協議之前，也就是在將關聯控制包含在重定向消息中之前，所述RP必須完成所述關聯。

如第25圖所示：

625：使用者可以存取RP站點，以便使用OpenID來進行登錄；他可以輸入其OpenID識別字，例如http://op.org/identit

630：瀏覽器可以向RP網址發送包含了OpenID識別字的HTTP消息。

635：RP可以使用基於HTTP/HTML的OpenID‘簡單’發現處理，並且經由公共網際網路來與OP-agg取得聯繫，以便在標識頁面上檢索OpenID識別字，例如HTTP獲取http://op.org/identity

640：OP-agg可以接收請求，並且它可以通過使用包含OPSF位址的HTML頁面做出回應，舉例來說，包含以下位址：

<link rel="openid.server" href=http://op.org/server.cgi>

OPSF的位址可以不同於OP-agg的位址

645：RP可以使用帶有下列參數且針對OPSF的HTTP POST（傳遞）呼叫：

openid.mode（openid.模式）=associate（關聯），

openid.assoc_type（openid.關聯_類型）=HMAC-SHA1，

openid.session_type（openid.會話_類型）=blank（空），

openid.dh_*= ‘Diffie-HellmanParameters（迪菲赫爾曼參數）’

650：OPSF可以產生用於RP的共用秘密和關聯控制

655：OPSF可以使用將關聯控制和秘密（如果使用了Diffie-Hellman，則

該秘密是經過加密的）包含在密鑰=數值格式化文件中的HTTPPOST來對RP做出回應。每一個RP和OpenID標識都可以建立一次這種關聯。由於Diffie-Hellman可能受到MITM攻擊的襲擊，因此，OpenID最佳安全實踐建議使用HTTPS驗證

660：RP可以創造會話臨時用法和會話識別字，例如

nonce=123123,

session（會話）=User（使用者）

665：RP可以儲存從OPSF接收的秘密和關聯控制

670：RP可以將關聯控制包含在重定向消息中

675：RP可以向瀏覽器發送一個包含下列參數的HTTP REDIRECT消息：

openid.mode=checked_setup（核驗_建立），

openid.identity=http://op.org/identity，

openid.return_to=http://rp.org/return.cgi?session=User&nonce=123123

openid.assoc_handle（openid.關聯_控制）= ‘association_handle

，

680：瀏覽器可以接收重定向消息，並且開放與RP在重定向消息中規定的URL的連接

685：借助於將OPSF的URL映射到SCWS本地IP位址的經過修改的DNS查找表，例如，通過使用具有項http://op.org==127.0.0.1的主機檔，可以將瀏覽器重定向到與SCWS相關聯的本地OP，並且發佈包含了來自675的參數的HTTP請求

在設備上可以使用經過修改的本地DNS查找表，以使所述設備認爲URL http://op.org處於SCWS的本地IP地址。因此，瀏覽器可以開放與SCWS/本地OP相連的連接，而不是連接到OPSF（所述OPSF可以經由公共網際網路而在URL http://op.org處到達）

690：下列各項並非由OpenID協定規範規定：

a. 與SCWS相關聯的OP可以顯示本地驗證頁面

b.使用者可以輸入其驗證證書，例如使用者名稱和密碼

c.與SCWS相關聯的OP可以核驗證書

695：與SCWS相關聯的OP有可能需要使用已經在OPSF與RP之間共用的秘密來對返回消息進行簽名，並且可以應用以下若干個選項：

a. 選項1：

i.該秘密有可能已經存在，例如由OPSF預先共用和預先配備

b.選項2：

i.OPSF可以向與SCWS相關聯的OP發送關聯控制和和秘密，例如經由安全的SMS來發送，或者通過由GBA來引導，和/或使用安全的通信協定，例如SCWS HTTPS遠端管理介面

ii.與SCWS相關聯的OP可以儲存秘密和關聯控制

c.選項3：

i.與SCWS相關聯的OP可以通過使用從RP接收的關聯控制來從OPSF那裏請求秘密。用於該消息的協定可以借助SMS運行，此外，其他選項也是可行的，其可行性有待進一步研究

ii.OPSF可以基於關聯控制來執行秘密查找

iii.OPSF可以將秘密和關聯控制發送到與SCWS相關聯的OP，例如經由安全的SMS-PP發送、或者由GBA引導、和/或使用安全的通信協定，例如SCWS HTTPS遠端管理介面

700：與SCWS相關聯的OP可以使用秘密來計算return_to URL、標識以及模式參數上的簽名

705：與SCWS相關聯的OP可以將簽名作爲額外參數包含在HTTP重定向中

710：與SCWS相關聯的OP可以向瀏覽器發送HTTP重定向消息，該HTTP重定

向消息包含下列參數：

openid.mode=id_res,

openid.return_to=http://rp.org/return.cgi?session=User&nonce=123123

openid.identity=http://op.org/identity,

openid.signed=mode,identity,return_to,

openid.assoc_handle= 'association handle' ,

openid.sig= 'base64 encoded signature（基本64位元編碼的簽名）

'

715：瀏覽器可以在不需要進一步使用者參與的情況下將使用者重定向到RP上的return_to URL

720：RP可以接收帶有簽名的斷言消息

725：RP可以使用預先建立的共用秘密來核驗簽名

730：對於RP來說，使用者可被標識爲http://op.org/identity

735：瀏覽器可以顯示RP的HTML頁

740：使用者可被作爲http://op.org/identity登錄到RP

基於關聯的模式的額外實施方式

額外實施方式可以基於那些將額外實施方式用於第4.4.1.4.3節的無狀態協定的實施方式。

4.4.2 用於SCWS上的OP改進的實施方式

4.4.2.1 關於改進的一般方法

在第4.4.1節的示例實施方式中，可以關聯於SCWS的本地OP以及OPSF有可能需要爲每一個RP至少建立一次用於斷言簽名及其核驗的共用秘密。但是，還可以應用其他方法，其中該協議是進一步通過使用額外密碼手段改進的，該手段允許在OPSF與本地OP之間只建立一個（長期）共用秘密，然後使用密碼函數來導出用於該簽名的秘密。此外，OPSF與本地OP之間的秘密

交換處理的集成可以在協定消息內部執行。

4.4.2.2 關於改進的背景技術資訊

以下章節提供的是可能的實施和實施方式的更多技術背景。

SCWS可以使用基於IP的方法或傳統UICC方法來與手機進行安全通信，並且間接地與外界各方進行安全通信；UICC應用的擁有方可以將這些應用下載到UICC，並且對其進行遠端管理。

就UICC上的資源的使用情況而言，可以注意到的是，能夠支持全球平臺、SCWS以及後續IP堆棧的UICC很有可能支援大容量記憶體和USB。這種UICC可以具有足夠強大的處理器，並且O/S將會承擔資源管理。

在第24圖中的575（無狀態模式）以及第25圖中的695（關聯模式），與SCWS相關聯的OP可以儲存和使用秘密。例如，通過執行該處理，可以將簽名密鑰保持在其永不丟棄的受保護的記憶體中，並且該密鑰只供卡本身的密碼演算法使用。該密鑰可以是某個能與另一（可信）方（類似於MNO）安全共用並被保證不會離開智慧卡的密鑰。對於所下載的小應用程式中的應用特定簽名密鑰而言，我們需要考慮四個問題：（1）密鑰如何進入UICC以及進入小應用程式，（2）如何保持密鑰安全性，（3）誰可以使用密鑰，以及（4）可以如何更新密鑰。

在一個示例實施方式中（對於問題（1）的回答），專用於UICC上的OP的密鑰可以作爲小應用程式的可執行載入檔的一部分載入，並且可以駐留在小應用程式的指定密鑰檔中。該應用下載可以不使用SCWS管理更新處理。但是，SCWS可以呼叫智慧卡應用（意味著任何應用，而不只是SCWS網頁）。這意味著本地OP可能是在全球平臺框架中運行的小應用程式。對這種複雜的小應用程式來說（它不僅僅是SCWS HTML頁面），較爲有利的是使用全球平臺小應用程式載入過程。

在另一個示例實施方式中（對於問題（2）的回答），屬於任何已載入應用

的秘密均由UICC的O/S保護。我們可以依靠O/S來實施該處理。UICC載入的程式運行時所在的記憶體受O/S保護。

在另一個示例實施方式中（對於問題（3）的回答），舉例來說，本地OP可以使用（專用）簽名密鑰來對一些資料進行簽名（或解密/加密）。任何能夠經由SCWS來與UICC上的本地OP進行通信的外部實體都可以爲小應用程式提供資料，以便執行簽名或解密，但是針對SCWS的這種通信有可能必須作爲重定向經由終端瀏覽器進行。對於共用密鑰來說，可以由OP之類的密鑰所有者來將這類密鑰分佈給MNO之類的TTP，以使它們可以在與UICC的互動中使用這些密鑰。

如果在與SCWS相關聯的OP中使用了密鑰檔來儲存密鑰，那麼可以使用標準化的小應用程式更新處理來更新密鑰文件。如果使用了SCWS管理更新處理，那麼該處理可以由SCWS更新處理的所有者完成（假設是MNO）。此外，使用卡上密鑰生成作爲替換方案也是可行的。

SCWS提供了BIP/CAT通信以及經由USB的TCP/IP/HTPP。在後一種情況中，在設備與SCWS之間可以使用TLS（基於PSK或PKI）。

在另一個示例實施方式中，OP伺服器應用可以作爲JavaCard小應用程式而被載入到UICC上，隨後則以2006年3月發佈的第2.2版的全球平臺卡規範中規定的方式來對其進行管理。所述小應用程式可以位於卡發佈者（CI）的安全域（SD）或是應用供應方的（AP）SD中，即便這兩個域實際由同一方(即MNO/CI)擁有也是如此。作爲替換，OP應用可以是韌體或本地應用。

OMA可以爲SCWS的內容和設置提供安全處理，其中所述內容和設置是由遠端伺服器應用使用針對SCWS且經過相互驗證的HTTPS來更新的。例如，該處理是爲了供作爲卡發佈方的MNO使用而被執行的，因此是圍繞用於傳輸的傳統OTA設計的。該特徵並不用於下載那些與SCWS相關聯的應用，而是用於更新此類應用（僅僅供MNO使用）。

SCWS可以使用傳統的工具箱和OTA技術（其SMS-PP被默認是無處不在的）。因此，如果UICC沒有自己的IP位址，那麼SCWS描述的是將CAT/BIP用於UICC/ME連接，以便從客戶瀏覽SCWS上的網頁，以及從管理實體傳送和管理SCWS上的網頁。同樣，SCWS還可以支援用於來自遠端管理員的消息的串聯SMS-PP。但是，如果UICC具有自己的位址，那麼SCWS還可以支持處於UICC高速（即USB）介面之上的直接TCP/IP連接，以便從客戶瀏覽網頁，以及通過直接TCP/IP連接上的直接TLS連接來從管理實體傳送和管理SCWS上的網頁。

4.4.2.3 關於SCWS上的改進OP的介紹

以下實施方式描述的是SCWS上的OP的概念的改進變體。SCWS上的OP可以是對OpenID/GBA的改進。例如，這些實施方式可以提供以下優點：

SCWS上的OP可以使驗證處理處於設備本地，並且由此顯著降低通信成本，從而改進OpenID/GBA。

關於SCWS上的OP的進一步改進可以在OP與網路端實體之間通過在標準的OpenID消息欄位內部傳遞驗證秘密來進行。這樣做可以進一步減小通信開銷，並且可以緩解SCWS上的OP與網路實體（OPSF）之間的關係，這樣則能夠在網路之間遷移OpenID。

此外，以下實施方式可以允許SCWS上的OP爲網路營運商產生以下主要優點，例如：

·在行動網路上沒有驗證業務量

·驗證業務量在公共網際網路上

·所有應用資料業務量都在行動網路上

4.4.2.4 本地OP所做的改進

在示例實施方式中，本地驗證可以是對與SCWS相關聯的OP執行的，由此顯著地減少業務量。例如，通過執行該處理，可以將驗證業務量本地化，從

而減小網路本身的負擔。在一個示例實施方式中，在網路OPSF實體與關聯於SCWS的OP之間可以爲使用者存取的每個RP建立共用秘密。在這裏描述了若干種用於建立這種秘密的機制。例如，在一個示例實施方式中，如果RP使用關聯，那麼它們可以儲存用於簽名核驗的秘密，並且可以在使用者下一次對其進行存取的時候重新使用該秘密。在另一個示例實施方式中，如果RP使用無狀態模式，那麼RP不能保存該秘密。OP可以創造秘密，並且可以與OPSF安全地共用該秘密。與SCWS相關聯的OP可以儲存該秘密，並且可以在使用者下一次存取相同RP的時候重新使用該秘密，OPSF也可以儲存相同的秘密，由此OPSF可以在無狀態模式中將其直接用於簽名核驗。

在另一個示例實施方式中，在某種程度上，在OSPF與關聯於SCWS的OP之間共用過一次的秘密是可以被重新使用的。例如，如果在智慧卡上可以爲OP保存總共5個秘密，那麼可以在使用者每次存取RP時重新使用這些秘密。舉例來說，與在3GPP TR 33.924中規定的OpenID/GBA相比，通過執行該處理，可以極大地減小網路業務量。例如，日常業務量可以縮減一半，如果考慮的是數天，那麼由於可以重新使用秘密，因此縮減量甚至會變得更大。

所提到的秘密可以不同於在OpenID/GBA中使用的秘密，在OPSF與關聯於SCWS的OP之間共用的秘密是用於對斷言消息進行簽名的OpenID秘密。與標準的OpenID協議過程中一樣，這些秘密是可以與RP共用的，並且是可以作爲壽命較長的秘密來建立的，例如，所述秘密比單個登錄會話持續的時間更長，由此基本上是允許這種重新使用的。

4.4.2.5 更進一步的改進

在一個用於實施SCWS上的OP的協定流程的示例實施方式中，MNO運行的OPSF網路實體可以參與到與關聯於設備上的SCWS的OP進行的額外通信中。由於這兩個實體都必須配備相同的對稱密鑰，以使每一個RP對斷言消息進

行簽名或者分別對其進行核驗，因此，該通信是必需的。

通過進一步改進這些實施方式，可以極大地減少設備與網路之間的額外通信，以及將建立秘密所必需的資訊直接封裝到OpenID消息的協定欄位中。這些消息是作爲HTTP消息經由公共網際網路發送的，它們有可能對MNO的空中網路基礎架構造成額外負擔。例如，通過執行該處理，可以確保驗證業務量處於本地，也就是介於瀏覽器與設備中的UICC/SCWS之間，由此可以防止不使用網路。由於將通信從（空中）網路卸載到了設備內部的內部通信上，因此，這種處理能夠減少一般的業務量。

通過確保在MNO與UICC/設備之間不必執行用於驗證的額外信令業務量，可以給出對這些實施方式所做的另一個改進。例如，對於每一個驗證來說可能沒有GBA過程（run），或者在網路與設備之間不會經由空中介面來發送SMS/MMS或控制消息。所有必要的資訊都可以在HTTP消息內部直接傳送，其中所述HTTP消息可以部分借助空中網路並通過網際網路（設備到RP）、而且部分通過固定線路的公共網際網路（RP到MNO）被傳送。但是該業務量可以1）由希望使用OpenID登錄的使用者觸發，2）經由現有資料平面而向使用者收費，3）比基於web的OpenID少，並且比在OpenID/GBA中少。

4.4.2.4 關於協議改進的技術細節

4.4.2.4.1 命名規則

在這裏將會重複如上所述的相同命名規則以供參考：

·與SCWS相關聯的OP：本地OpenID標識供應方，其發佈帶有簽名的斷言消息，並且將這些消息通過使用者瀏覽器發送到RP。假設存放SCWS的智慧卡乃至OP與MNO具有關係，並且由此與所有關聯於MNO的實體具有關係。

·RP：依賴方，它可以是任何使用OpenID來爲使用者提供登錄的網站。RP完全獨立於所有其他實體，因此，在RP上不能施加額外需求，並且不能改動RP的OpenID協定流程。OP必須支援RP選擇使用的任意通信模式（無狀態

或基於關聯）。如果MNO決定使用者不應該使用某些RP，那麼由於使用者還可以使用別的標識，因此，MNO不能通過拒絕對於這些RP的OpenID存取來拒絕對於這些站點的存取。MNO只能使用額外裝置來限制對於RP的存取，其中所述額外裝置通常阻止的是對消耗帶寬的站點進行的存取。

·OP-Agg：OP-Agg實施的是依照OpenID協議來爲RP提供發現服務的網路實體。

·OPSF：OP服務功能（OPSF）實施的是能與關聯於SCWS的OP並且可選地與來自（RSCWS-1）的RP產生、共用和分佈秘密的支援OP功能。從RP的角度來看，OPSF和關聯於SCWS的OP的行爲就好像它們是單個實體。OPSF能夠核驗與SCWS相關聯的OP發佈的簽名，並且可以由RP經由公共網際網路直接到達。通過修改設備上的本地DNS解析快取，可以將設備上的瀏覽器重定向到與SCWS相關聯的OP，以使OPSF的位址映射到與SCWS相關聯的本地OP。

關於該實體OPSF的需求及其必要功能是如上在先前文件“OP on SCWS specification draft（SCWS上OP的規範草案）”中精確描述的。

·瀏覽器：在協定流程圖中顯示，以便明確往來於與SCWS相關聯的OP的路由和消息傳遞功能。否則，它只是顯示和接收使用者驗證的前端。

4.4.2.4.2 關於實施方式的可能假設

關聯於SCWS的OP和OPSF功能可以建立長期秘密K，該長期秘密K由智慧卡的安全特性保護，並且只能被與SCWS相關聯的OP存取。例如，該秘密既可以借助單個GBA過程建立，也可以用另一個允許從AKA密鑰中推導出密鑰的密鑰推導功能建立，還可以用其他任何在MNO與關聯於SCWS的OP之間產生共用秘密的方法來建立，其中所述共用秘密可以由UICC的安全特徵來保護。此外，建立秘密的處理可以使用本領域中已知的任何方法來進行。

智慧卡也可以提供密碼功能（演算法和計算），以便計算從K中得到的新秘密。該功能的具體屬性可以從安全需求描述中得到。相同或相似的功能也

可以爲OPSF所知，這樣可以允許OPSF從K中推導出密鑰。

這兩個實體都能爲密碼操作產生足夠長的隨機值。

4.4.2.4.3 協定流程描述

以下章節描述的是用於實施與SCWS相關聯的OP的協定流程的示例實施方式。

4.4.2.4.3.1 使用無狀態模式的RP的協定流程的示例實施方式

如果RP使用無狀態模式來執行OpenID使用者驗證，則可以應用第26圖描述的實施方式。

4.4.2.4.3.1.1 關於無狀態模式的描述

第26圖顯示的是改進的無狀態模式的協定流程的示例實施方式。

745：使用者可以存取RP網址，並且爲了使用OpenID登錄，他輸入了他的OpenID識別字，例如http://op.org/identity

750：瀏覽器可以向RP網址發送包含OpenID識別字的HTTP消息。

755：RP可以使用基於HTTP/HTML的OpenID‘簡單’發現處理，並且經由公共網際網路來與OP-agg取得聯繫，以便在標識頁面上檢索OpenID識別字，例如HTTP獲取http://op.org/identity。

760：OP-agg可以接收請求，並且可以使用包含OPSF網際網路位址的HTML頁面來做出回應。例如，OP-agg可以通過包含以下位址來做出回應：

<link rel="openid.server" href=http://op.org/server.cgi>

OPSF可以像標準的OpenID標識供應方web服務那樣對RP進行操作。例如，OPSF能夠按照RP的請求來核驗斷言消息上的簽名（由本地OP發佈）。根據需求，OPSF必須可以經由公共網際網路到達，由此假設該OPSF具有DNS名稱，例如可以經由http://op.org到達的op.org。由於外界不知道智慧卡的IP位址，因此，OP-agg和OPSF的這種間接性可被用於通信。

OPSF的位址可以不同於OP-agg的位址。

765：RP可以接收OPSF的位址，並且創造臨時用法和會話識別字，例如nonce = 123123，session = User。RP可以編譯return_to參數，所述參數會向OP告知應該在使用者驗證之後將瀏覽器重定向到哪一個URL。RP可以通過發佈包含下列參數的HTTP重定向來將瀏覽器重定向到OP伺服器位址：

openid.mode=checkid_setup,

openid.identity=http://op.org/identity,

openid.return_to=http://rp.org/return.cgi?session=User&nonce=123123

770：瀏覽器可以接收所述重定向，並且可以開放RP在重定向消息中規定的至URL的連接

775：借助於經過修改而將OPSF的URL映射到SCWS本地IP位址的DNS查找表，例如通過使用具有項http://op.org==127.0.0.1的主機檔，瀏覽器可被重定向到與SCWS相關聯的本地OP，並且發佈包含了765處的參數的HTTP請求。

在設備上可以使用經過修改的本地DNS查找表，以使所述設備認爲URL http://op.org在SCWS的本地IP地址處。瀏覽器可以開放與SCWS/本地OP的連接，而不是連接到OPSF（所述OPSF可以經由公共網際網路而在URL http://op.org可到達）。

780：通過執行下列處理，可以確保驗證業務量保持在本地，這些步驟並不是OpenID協定規範必需或規定的：

a. 與SCWS相關聯的OP可以顯示本地驗證頁面

b.使用者可以輸入其驗證證書，例如使用者名稱和密碼

c.與SCWS相關聯的OP可以核驗證書

785：與SCWS相關聯的OP可以創造唯一的隨機關聯控制A。通過使用函數f，可以使用S=f(A,K)來計算斷言消息的簽名秘密，其中所述f應該是單向

的，由此對於A的認識不會展現任何對於K的認識。在一個示例實施方式中，即便顯現了S和A，也就是給出了S和A，f也不會顯現任何關於K的認識，在計算方面，爲函數g計算K=g(S,K)是不可行的。

由於可以將A作爲重定向消息中的參數的一部分顯現給RP，因此可以假設RP不會在OpenID協定過程的無狀態模式中獲得對於S的認識。關聯控制A可以包含在重定向消息中。此外還可以假設，用S簽名了的帶有簽名的消息m不會向簽名核驗器顯現任何關於K的資訊（由於使用了對稱密鑰簽名，因此簽名核驗器始終需要擁有S來核驗簽名，由此我們不要求該簽名不展現S）。在這裏可以規定關聯控制是長度爲255個字元或更少的字串，並且可以只包括處於封閉區間33-126中的ASCII字元（可列印的非空白字元）。

OPSF用於核驗簽名的秘密與關聯於SCWS的OP用於產生簽名的秘密可以是相同的。簽名的新鮮度可以由下一個步驟中插入的RP臨時用法來確保，並且該RP臨時用法必須是簽名的一部分。OpenID規範對簽名秘密本身的新鮮度保持默認。OP負責確保秘密的密碼強度，保持其秘密性，以及在需要時確保其新鮮度。OPSF和關聯於SCWS的OP可以持續有限壽命或是用於對該目的簽名秘密的使用計數。

啓用工具箱的本地OP可以使用CAT來主動與手機通信，同時繞過SCWS。該消息可以依照標準的OTA（例如用於經由SMS-PP承載來發送到OPSF的OTA）而被格式化。但是，這種處理有可能需要OPSF經由MNO的OTA系統來與所述卡進行通信。在另一個示例實施方式中，BIP閘道可以擷取工具箱消息有效負載，並且手機可以使用TCP/IP將其發送到OPSF。這就有可能要求消息經由MNO的OTA伺服器而被傳送。SCWS聲稱只有在所述卡不具有IP位址並且不支援TCP/IP的情況下才可以使用BIP。因此，期望的是通過使用TCP/IP經由SCWS進行發送。

d.可以應用進一步的選項，這些選項有可能在關聯於SCWS的OP與OPSF之間

產生共用秘密。這種方法的可行性有待下一步研究。

790：與SCWS相關聯的OP可以計算下列參數上的簽名：return_to、標識以及模式。

795：與SCWS相關聯的OP可以向瀏覽器發送HTTP重定向消息，該消息包括在765處從RP接收到的參數。此外還可以包括下列各項：

·openid.signed參數中的一系列帶有簽名的參數

·openid.assoc_handle參數中的關聯控制A

·openid.sig參數中的簽名（經過base64編碼）。

該消息可以用於將瀏覽器重定向到RP處的return_to URL。

800：瀏覽器可以將使用者重定向到RP處的return_to URL。

805：RP可以接收帶有簽名的斷言消息，並且在經由公共網際網路且基於HTTP（S）的直接通信中加入到與OPSF的核驗過程中。

810：RP可以發佈HTTPPOST消息，該HTTPPOST消息包含了在795處從與SCWS相關聯的OP接收的參數。HTTPPOST消息可以包括由與SCWS相關聯的OP產生的關聯控制A。

815：OPSF可以從參數列表中擷取A，並且可以與關聯於SCWS的OP使用具有相同輸入的相同函數f，也就是說，OPSF計算f(A,K)=S，並且使用S作爲共用秘密來核驗從與SCWS相關聯的OP接收的資料上的簽名。

820：如果簽名核驗成功，則OPSF可以返回is_valid:真。

825：對RP來說，現在可以將使用者標識爲http://op.org/identity。

830：瀏覽器可以顯示RP的HTML頁面。

835：使用者可以作爲http://op.org/identity而在RP上登錄

4.4.2.4.3.2 使用了基於關聯的模式的RP的協定流程

第27圖顯示的是用於改進的基於關聯的模式的協定流程的示例實施方式。例如，該處理可以在RP使用基於關聯的模式執行OpenID使用者驗證的時候

執行。該關聯可以在使用者首次與RP進行聯繫並將其OpenID識別字與該RP結合使用之後發生。如果建立了關聯，那麼可以重新使用該關聯，以便進一步減少通信工作。但是，OP可能不能夠要求RP的工作模式，並且有可能是由RP來決定兩種通信模式之一。

該關聯可以在RP與OP之間建立永久性秘密，並且RP可以使用該秘密來對斷言消息進行簽名，此外，RP還可以使用該秘密來核驗OP簽名。OP可以決定共用秘密的有效期。RP和OP可以使用關聯控制作爲該秘密的識別字。該RP將關聯控制包含在去往OP的第一請求消息中，然後，OP可以根據關聯控制來使用相應秘密。如果OP確定該關聯已經到期，那麼OP可以在回應消息中通知RP。這樣做可以允許OP拒絕任何關聯請求。只要RP能夠支援無狀態模式，則可以使用該處理來迫使RP退回到無狀態通信模式。例如，如果OP不支援RP請求的簽名模式（HMAC-SHA1或HMAC-SHA256），那麼OP可以拒絕關聯請求。

與使用者每次登錄RP時都可以在RP與OP之間建立新秘密的無狀態通信模式相反，每一個標識和RP都會建立一次關聯。例如，並不是第27圖所示的所有項都可以在使用者登錄的時候執行。如果在OP與RP之間已建立了關聯，那麼該關聯可以被RP和OP重新使用。

一旦知道了OPSF位址，也就是在發現階段之後，RP可以建立關聯，並且在繼續執行協議之前，也就是在將關聯控制包含到重定向消息中之前，該RP可以完成所述關聯。

如第27圖所示：

840：使用者可以存取RP網址，並且爲了使用OpenID進行登錄，他可以輸入他的OpenID識別字，例如http://op.org/identity。

845：瀏覽器可以向RP網址發送包含OpenID識別字的HTTP消息。

850：RP可以使用基於HTTP/HTML的OpenID‘簡單’發現處理，並且可以

經由公共網際網路來與OP-agg取得聯繫，以便在標識頁面上檢索OpenID識別字，例如HTTP獲取http://op.org/identity。

855：OP-agg可以接收該請求，並且使用包含OPSF位址的HTML頁面來做出回應，例如，OP-agg可以通過包含下列各項來做出回應：

<linkrel="openid.server" href=http://op.org/server.cgi>

OPSF的位址可以不同於OP-agg的位址。

860：RP可以針對OPSF使用帶有下列參數的HTTP POST呼叫：

openid.mode=associate,

openid.assoc_type=HMAC-SHA1,

openid.session_type=blank,

openid.dh_*= 'Diffie-HellmanParameters'

865：OPSF可以爲RP產生唯一的隨機關聯控制A。另外，OPSF可以使用函數f，並且計算S=f(A,K)。然後，S可被用作RP與OPSF之間的關聯（中期）共用秘密。該RP稍後可以使用S核驗來自與SCWS相關聯的OP的斷言消息上的簽名。在一個示例實施方式中，由於可以在870處與RP共用A和S，因此，即便A和S是已知的，也可以假設f是保持單向的函數，由此不能在給出S和A的情況下計算出K。函數f本身可以不需要保密。

870：OPSF可以使用HTTPPOST來對RP做出回應，該HTTPPOST將關聯控制A和秘密S（如果使用了Diffie-Hellman，則該秘密是經過加密的）包含在密鑰=數值格式化文件中。每一個RP和OpenID標識都可以建立一次這種關聯。

880：RP可以創造會話臨時用法和會話識別字，例如

nonce = 123123,

session = User

885：RP可以儲存從OPSF接收到的秘密S以及關聯控制A。

890：RP可以將關聯控制A包含在重定向消息中。

895：RP可以向瀏覽器發送HTTP重定向消息。該HTTP重定向消息可以包括下列參數：

openid.mode=checkid_setup,

openid.identity=http://op.org/identity,

openid.return_to=http://rp.org/return.cgi?session=User&nonce=12312

openid.assoc_handle=A

900：瀏覽器可以接收重定向消息，並且可以開放與RP在重定向消息中規定的URL的連接

借助於經過修改而將OPSF的URL映射到SCWS的本地IP位址的DNS查找表，例如通過使用具有項http://op.org==127.0.0.1的主機檔，瀏覽器可被重定向到與SCWS相關聯的本地OP，並且可以發佈包含了來自885的參數的HTTP請求。

在設備上可以使用經過修改的本地DNS查找表，而這會讓所述設備認爲URL http://op.org位於SCWS的本地IP地址。

905：瀏覽器可以開放與SCWS/本地OP的連接，而不是連接到OPSF（所述OPSF可以經由公共網際網路而在URL http://op.org處可到達）。

910：通過執行下列處理，可以確保驗證業務量保持在本地，這些步驟並不是OpenID協定規範必需或規定的：

a.與SCWS相關聯的OP顯示本地驗證頁面

b.使用者輸入其驗證證書，例如使用者名稱和密碼

c.與SCWS相關聯的OP核驗證書

915：與SCWS相關聯的OP有可能需要使用能在OPSF與RP之間共用的秘密S來對返回消息進行簽名。參數A可以是從接收到的HTTP請求中擷取的，並且在這裏可以應用函數f，以使S=f(A,K)。

920：與SCWS相關聯的OP可以使用秘密S來計算return_to URL、標識以及模式參數上的簽名。我們有可能需要函數f在給出了用S簽名的帶有簽名的消息m的情況下，不向m上的簽名的核驗器展現任何關於K的資訊。

925：與SCWS相關聯的OP可以將簽名作爲額外參數包含在HTTP重定向中。

930：與SCWS相關聯的OP可以向瀏覽器發送HTTP重定向消息，該消息可以包括以下參數：

openid.mode=id_res,

openid.return_to=http://rp.org/return.cgi?session=User&nonce=123123

openid.identity=http://op.org/identity,

openid.signed=mode,identity,return_to,

openid.assoc_handle=A,

openid.sig= 'base64 encoded signature calculated using S'

935：瀏覽器可以在不需要進一步的使用者參與的情況下將使用者重定向到RP處的return_to URL。

940：RP可以接收帶有簽名的斷言消息。

945：RP可以使用所確定的共用秘密S來核驗簽名。

950：對RP來說，現在可以將使用者標識爲http://op.org/identity。

955：瀏覽器可以顯示RP的HTML頁面。

960：使用者可以作爲http://op.org/identity在RP上登錄。

基於關聯的模式的額外實施方式

以下公開的是與在第4.4.1.4.3節中描述的無狀態協定的實施相關的額外實施方式。

4.4.2.5 改進的SWCS上的OP與現有OpenID/GBA之間的比較

在OpenID/GBA中，使用者使用GBA協議進行驗證，也就是爲在任何RP處的每一次OpenID登錄嘗試都會觸發使用了經由空中介面的OP/NAF的GBA過程

，從而由於業務量的增長而對網路實體（OP/NAF）和網路本身造成負擔。假設在給出了數量爲10,000名使用者的客戶基礎的情況下，每一個使用者每天登錄到10個不同的RP。依照OpenID/GBA，這會導致每天總共執行100,000個GBA驗證過程；如果每一個GBA過程（質詢+響應）只消耗1-5kB，那麼每天總共會有1-4.8GB的額外驗證業務量。

4.4.2.6 安全性論述

下節提供的是可以在用於無狀態和基於關聯的模式的SCWS上的OP協定的示例實施方式中使用的密碼工具的背景。在這裏論述了諸如可以使用的散列演算法之類的特性。

4.4.2.6.1 概括

函數f可以用於在本地OP與OPSF之間建立共用秘密S。OPSF和本地OP可以具有公共共用長期秘密K，該秘密可以作爲f的一個輸入使用，並且所述K永不會被洩露給協議中的另一方。但是，在基於關聯的模式中，由於RP可能會核驗斷言消息上的簽名，因此有可能將秘密S洩露給RP。由於共用秘密有可能具有安全性含義，因此有必要論述所述RP在瞭解S的情況下具有的選項。該處理同樣適用於標準的OpenID協議。假設RP是惡意的，那麼對於S的認識不能允許該RP在另一個RP上登錄使用者，這是因爲另一個RP將會與OP建立另一個共用秘密S'，由此會將使用S產生的簽名認定爲無效。因此，將秘密展現給RP未必是安全問題。但是，將S顯現給瀏覽器（或使用者）有可能會成爲安全問題。在這種情況下，攻擊者可以使用受害人的OpenID識別字來啓動OpenID協定。如果攻擊者可以檢索到在RP與OP之間共用的共用秘密S，那麼攻擊者可以在沒有對OP執行實際驗證的情況下使用S來對斷言消息進行簽名。因此，攻擊者可以使用受害人的識別字進行登錄，而不用在受害人的OP上進行驗證。從這種情況中可以看出，RP與OP之間的共用秘密S是不能顯現給瀏覽器的，但是將S暴露給RP則是可以的。

如果惡意使用者與RP一起工作，那RP有可能將S發送給瀏覽器，使用者則有可能會在沒有在RP上進行驗證的情況下登錄到RP。但是，由於使用者只能登錄到單個RP，並且依照假設，該RP已經受其控制（或者至少與該使用者合作），因此，這種情況未必會被認爲是攻擊。由此，即便根本沒有執行OpenID驗證協議過程，使用者也是可以登錄的。

4.4.2.6.2 示例協定的安全性特徵

在一些示例實施方式中，在重定向消息中有可能將A以及使用S簽名的消息洩露給瀏覽器，如果獲悉了A和使用S簽名的消息，那麼可能是無法計算出S的。此外，在給出了相同輸入的情況下也是無法計算出K的。

在給出了A和S（可能洩露給除OP和OPSF之外的單個第三方的最多的資訊）的情況下，如果所需要的是無法通過計算來得出K（也就是說，假設沒有函數f-1來使得f-1(A,S)=K，這可以在以輸入爲長度的時間多項式中計算），那麼沒有RP可以得出OPSF與關聯於SCWS的OP之間的長期共用秘密K。

由此，在給出了隨機輸入A和共用秘密K的情況下，有必要由f來產生新的秘密S，以使得S=f(A,K)。在給出了A（以及使用S簽名的消息）的情況下，這時是不能計算出S的。如果輸入K是正確和存在的，那麼有可能要求f可以產生正確的結果。

在多項式時間中有可能可以對f進行計算，並且所述計算較佳是在智慧卡的受保護區域中進行的。

S可以是在OpenID中使用的簽名函數的有效輸入。OpenID事先知道使用HMAC-SHA1或HMAC-SHA256作爲簽名演算法。由於OPSF和關聯於SCWS的OP有可能預先就具體的簽名演算法、密鑰長度達成一致，因此，函數f的輸出長度可以是固定的。在一個示例實施方式中，OPSF和OP可以使用兩個共用秘密K和K’，由此可以使用K來爲基於SHA1的簽名推導出S，並且使用K’來爲SHA256簽名推導出S。

4.4.2.6.3 安全性的實現

本節描述的實施方式是可以滿足前一節中指出的需求的密碼操作。在一個示例實施方式中，秘密可以直接包含在OpenID消息內部，而這可能會導致驗證需要的業務量減少。使用者驗證可以在本地執行（不涉及MNO網路），並且在OpenID協定消息內部可以安全地傳遞OPSF（MNO網路）與關聯於SCWS的OP（在設備中）之間的共用秘密，而不需要在MNO網路與設備之間進行進一步的外部額外通信。

4.4.2.6.3.1 HMAC

HMAC是在不使用任何額外機制的情況下驗證消息來源及其完整性的鍵入式散列消息驗證碼（MAC）。HMAC具有兩個功能不同的參數，即消息輸入以及僅僅爲消息發起方和一個或多個預定接收方所知的密鑰。

消息發送方使用HMAC功能來產生通過壓縮密鑰和消息輸入而形成的值（MAC）。MAC通常是與消息一起發送給消息接收方的。接收器使用與發送方使用的密鑰和HMAC函數相同的密鑰和HMAC函數來計算接收消息上的MAC，並且將計算結果與接收到的MAC進行比較。如果這兩個值匹配，則消息已經被正確接收，並且接收方確信發送方是共用密鑰的使用者團體中的成員。在給出了HMAC屬性的情況下，通過將HMAC用於函數f，可以滿足如上所述的所有相關需求。

用於HMAC的相關參數列表：

·B——散列函數輸入的塊大小，例如用於SHA1的160位元

·H——散列函數（例如SHA1）

·Ipad——內部填充符，重複B次的位元組x'36'

·K——在OP與OPSF之間共用的密鑰

·K0——預處理之後用於獲取B位元組密鑰的密鑰K

·L——散列函數的輸出塊大小，例如用於SHA1的160位元

·Opad——外部填充，重複B次的位元組x'5c'

·t——MAC位元組的數量

·text（文本）——用於從n位元的長度中計算HMAC的明文，其中0<=n<2^B-8B，在我們的範例中將會是A

·||——串聯

·XOR——異或

·K應該等於或大於L/2，也就是說，對我們的範例而言，如果使用SHA1，那麼K應該大於80位元，或者如果使用SHA256，則應該大於128位元。

·MAC(text)=HMAC(K,text)=H((K0 XOR opad)||H((K0 XOR ipad)||text))

爲了防止攻擊，有可能需要通過巢套執行兩個散列函數來計算MAC。結合大多數的散列函數，有可能在不知道密鑰K的情況下在消息中增添額外資料，並且可以獲取另一個有效MAC。如果使用其他替換方案，那麼通過使用MAC=H(message‖key)來添加密鑰，可以允許發現（非鍵入式的）散列函數中的衝突的攻擊者得到MAC中的衝突。使用MAC=H(key||message||key)會更好，但是，即便使用兩個不同的密鑰，不同的安全檔也會顯現弱點。第28圖顯示的是來自NIST-FIPS PUB 198-1的鍵入式散列消息驗證碼（HMAC）。

由於外部散列函數遮蔽了內部散列的中間結果，因此，當前協定的HMAC版本並未暴露這些弱點。對演算法的安全性而言，填充值（ipad和opad）並不重要，但是其被定義成彼此具有很大的漢明(Hamming)距離，因此，內部和外部密鑰將具有較少量共同位元，也就是說，通過使用這些填充符，可以從K0中“推導出”兩個不同的密鑰，以便在散列函數中使用。

在一個示例實施方式中，作爲隨機輸入的text=A可以由OP或OPSF分別產生。A可以包含在重定向消息中，並且通過使用K，這二者可以使用上述機制

來重新計算HMAC，所述HMAC結果可以作爲共用簽名秘密S而被用於OpenID斷言消息。

4.4.2.6.3.2 關於改進的SCWS上的OP協議的安全性證明

需要顯示的是：

1．在協議中，攻擊者能夠檢索A和S（例如作爲處於關聯模式的RP），因此有必要顯示他無法檢索K。

2．瀏覽器/使用者進行的檢索甚至少於RP，也就是只檢索A，並且必須不能從對於A的認識中計算出S。

3．瀏覽器/使用者還必須不能從A中計算出K。

當模擬一個瞭解S和A的攻擊者時，其中該攻擊者並未使用在S上給出的資訊，關於3.的證明可以從1.中推導得到。

由此必須顯示的是：

I．如果給出了S和A，那麼應該沒有函數f*，以便在S=f(A,K)的情況下使得K=f*(A,S)

II．如果只給出了A，那麼必定沒有函數g能使得在S=f(A,K）的情況下滿足S=g(A)。

在Bellare（貝賴爾）等人提供的關於HMAC（或NMAC）的描述中可以找到關於以上兩個定理的證明，其中在（11）中，它們本質上顯示的是，如果假設基本壓縮散列函數是僞隨機的，並且散列函數對衝突的抵抗力很弱，那麼HMAC是僞隨機函數。在（12）中，依照壓縮函數是PRF的唯一假設，這些假設可以通過顯示HMAC是PRF來加以緩解。

4.4.2.6.3.3 RSA

在一個示例實施方式中，通過使用必須在OPSF與關聯於SCWS的OP之間共用的私鑰來加密隨機創造的唯一關聯控制，可以使用RSA加密方案來從共用密鑰K中推導OpenID簽名秘密S。假設N=pq表示的是用於RSA方案的模數，其

中p，q是質數。更進一步，密鑰對是用e，d（私有，公共）表示的，並且是作爲長期秘密K共用的。然後，關聯控制A用私有部分e進行簽名，以便獲取簽名秘密S，也就是說，S=Ae 模 N。在爲RSA給出了安全性假設的情況下，如果公鑰d是已知的，則可以從S中計算出A，但是不能在給定了A和S的情況下計算出e。如果只給出了A，那麼無法在不瞭解e的情況下計算出S。

4.4.2.6.4 安全性實施變體

4.4.2.6.4.1 長期秘密K的改變

在第4.4.2節描述的一個示例實施方式中，雖然使用了長期秘密K，但是舉例來說，在某個時段之後，通過在OSPF與關聯於SCWS的OP之間使用密鑰交換方法，可以改變該秘密K。任何已知的密鑰交換方法都是可以使用的。K的改變可以在OPSF上執行，並且與SCWS相關聯的OP不能阻止成功的OpenID協議過程。

在一個示例實施方式中，如果OPSF和OP在無狀態模式中對新的長期秘密K’取得一致意見，那麼OP可以通過將函數f與新的密鑰結合使用來計算簽名密鑰S’，即S’=f(A,K’)。然後，S’可被用於對斷言消息進行簽名，並且OPSF可以使用新的長期共用秘密K’來重新計算S’，從而核驗斷言消息上的簽名。

在另一個示例實施方式中，如果在基於關聯的模式中建立了新的秘密長期秘密K'，那麼RP仍舊可以保持用於所述關聯的舊秘密S。如果關聯仍舊有效，並且RP沒有加入與OPSF的關聯步驟，那麼RP有可能直接使用舊的關聯控制A，並且有可能預期來自OP且用已儲存秘密S簽名的斷言消息。但是，OpenID規範允許OP將參數openid.invalidate_handle包含在斷言消息中。如果使用該參數並將其設置成舊的關聯控制A，那麼RP會被迫返回到OP，以便像在無狀態方案中那樣執行簽名核驗。這樣做可以允許與SCWS相關聯的OP包含這個對新的長期共用秘密K’而言被設置成A的參數、以及使用了

新創造的關聯控制A’的新簽名秘密S’=f(A’,K’)。這樣做有可能會使得RP上的控制碼無效，並且RP可以與OPSF進行聯繫，以便實施簽名核驗。由於所述密鑰交換，OPSF有可能已經具有K’，由此可以計算S’=f(A’,K’)，並且可以核驗斷言消息上的簽名。但是，如果RP加入與OPSF相關聯的新會話，那麼OPSF也有可能使得控制A無效，並且可以與RP使用新密鑰K’來建立新配對A’,S’。

4.4.2.6.4.2 用於K的散列鏈保證

在一個示例實施方式中，OPSF和關聯於SCWS的OP有可能希望定期改變長期秘密K。基於該秘密K，這兩個實體可以通過將（用密碼保護的）散列函數h連續應用於K來執行散列鏈保證，由此將會產生一個鏈條：K0=h(K)，K1=h(K0)=h(h(K))，……，Kn=h(Kn-1)=hn(K)。如果可以安全建立初始秘密K，那麼OP和OPSF可以獨立計算該鏈條。然後，所使用的第一共用秘密可以是Kn。如果用於構建散列鏈的散列函數具有單向屬性，那麼所述值不會允許攻擊者直接計算後續共用秘密Kn-1。攻擊者不得不反轉散列函數，以便推導出下一個秘密。這些秘密是由OPSF和本地OP以散列鏈的相反順序使用的。爲了進一步提高安全性，前進到散列鏈中的下一個值的處理、也就是OPSF和本地OP丟棄當前值並計算下一個值的處理可以遵循若干種策略，例如，該處理可以採用按月、按天、按會話等等的形式執行。

4.4.2.6.5 重複使用AKA AV和秘密，以及從AKA證書構建散列鏈

在一個示例實施方式中，OPSF可以與MNO上的網路功能處於相同位置，其中所述網路功能可以允許OPSF檢索來自HLR（歸屬位置暫存器）以及MNO的AuC（驗證中心）的AKA驗證向量（AV）。OPSF可以檢索AV，並且可以選擇其中一個AV來質詢與SCWS相關聯的OP。通過使用該AV，OPSF和關聯於SCWS的OP可以建立共用秘密CK，然後，該共用秘密CK可以用作OpenID的長期共用秘密K。在另一個示例實施方式中，不同於建立長期秘密，OP和OPSF可

以建立散列鏈的保證，其值被用作OPSF與關聯於SCWS的OP之間的共用秘密。這種處理可以是一種用於建立長期共用秘密的安全方式。

4.4.2.7 強調所述改進的好處

本節旨在顯示SCWS上的OP可以提供的好處，尤其是在該改進變體中提供的好處。

4.4.2.7.1 標準的OpenID

第29圖顯示的是標準的OpenID協定流程。通過使用已有的基於web的OpenID OP伺服器（例如myopenid.com），可以運用標準的OpenID協定過程來從行動設備存取RP。

如第29圖所示，本地業務量是不存在的，並且從空中網路卸載的唯一業務量是發現處理以及RP與OP之間的關聯建立處理。由於OP是web服務，因此，介於使用者/瀏覽器/設備與OP之間的所有通信全都經由空中介面。

空中傳送通信是在965和975處進行的，其中該通信是在MNO/空中網路上執行的，並且通常作爲代表MNO網路上的負載的資料業務量（例如基於HTTP、IP的通信）。

在970處，業務量會在固定線路的網際網路上出現，並且可以使用現有的基礎架構。

4.4.2.7.2 OpenID/GBA

第30圖顯示的是OpenID/GBA的業務流程。該圖是從源於3GPP TR 33.924 v9.1.0第13頁的第4圖-4 1.1中得到的。

如第30圖所示，不管在RP與MNO之間進行怎樣的關聯步驟，所有通信都在空中網路上進行。例如，980和985處的信號是通過空中傳送通信傳送的，該通信作爲資料業務量而在MNO/空中網路上進行，並且代表MNO網路上的負載。與基於web的OP相比，由於需要用於驗證的額外步驟，因此，OpenID/GBA中的業務量甚至更大，而這會給空中資料網路以及GBA驗證所

需要的後端服務、即BSF和NAF子系統造成負擔。因此，空中網路業務量將會增長，並且網路實體上的負載將會增大。

4.4.2.7.3 簡化的基於關聯的通信

第31圖顯示的是基於關聯的通信模式的協定流程的另一個示例實施方式。如第30圖所示，空中傳送業務量可以卸載到本地設備上，從而減少空中介面網路業務量。例如，通過執行該處理，可以允許驗證業務量處於本地，以使驗證業務量將空中介面網路或網路服務上的負擔最小化。此外，發現和/或關聯業務量可以不經由空中介面網路發生，並且可以在固定線路的公共網際網路上進行。

在990處，使用者可以與瀏覽器之類的使用者介面形成介面，並且可以存取RP，還可以使用OpenID來請求登錄。在995處，RP和OP（MNO）可以基於OpenID標識來執行發現OP伺服器的處理。在1000處，RP可以向OP傳送關聯請求。OP可以產生隨機的唯一關聯控制A，並且可以計算密鑰S。所述OP可以向RP傳送關聯回應。該關聯回應可以包括關聯控制A和密鑰S。RP可以儲存密鑰S和關聯控制A。

在1005處，RP可以向瀏覽器傳送重定向。所述重定向可以將瀏覽器重定向到OP，並且可以將關聯控制A包含在請求參數中。OP可以與SCWS相關聯。瀏覽器可以接收重定向，並且可以通過執行經過修改的本地DNS查找來映射到SCWS。在1010處，瀏覽器可以向OP傳送本地驗證請求。在1015處，驗證可以在本地進行。例如在1020處，OP可以基於長期共用秘密鑰K和關聯控制A來核驗證書。此外，OP還可以計算密鑰S，並且可以使用密鑰S來計算簽名。該簽名可以用於對斷言消息進行簽名，和/或對返回URL、標識和/或模式之類的參數進行簽名。

在1025處，OP可以向瀏覽器傳送指示瀏覽器存取RP的重定向。該重定向可以包括關聯控制A和帶有簽名的參數。在1030處，瀏覽器可以向RP傳送請

求，該請求可以包括來自OP且帶有簽名的斷言消息。RP可以使用密鑰S來核驗斷言消息上的簽名。然後，在1035處，RP可以允許瀏覽器顯示登錄頁面，並且可以向瀏覽器提供針對服務的存取。

在一個示例實施方式中，假設在關聯於SCWS的OP與MNO之間存在長期共用密鑰。

如第31圖所示，1010、1015、1020和1025代表的是不會在MNO/空中網路上產生負載的本地通信。此外，由於這些通信可以在設備內部進行，因此，這些通信可以在其他（固定線路或非MNO）網路沒有業務量的情況下進行。

990、1005、1030和1035代表的是空中傳送通信，該通信可以作爲資料業務量（例如基於HTTP、IP的通信）在MNO/空中網路上進行，並且可以代表MNO網路上的負載。

995和1000代表的是可以在固定線路網際網路之類的固定線路上發生並且可以使用現有基礎架構的業務量。該通信不會增大MNO/空中介面網路上的負載。

第32圖顯示的是基於關聯的通信模式所具有的協定流程的另一個示例實施方式。如第32圖所示，空中傳送業務量可以卸載到本地設備，從而減少空中介面網路業務量。例如，通過執行該處理，可以允許驗證業務量處於本地，以使驗證業務量將空中介面網路或網路服務的負擔最小化。此外，發現和/或關聯業務量可以經由空中介面網路進行，並且可以在固定線路的公共網際網路上進行。

在1040處，使用者可以與瀏覽器之類的使用者介面形成介面，並且可以存取RP，還可以使用OpenID來請求登錄。在1045處，瀏覽器可以向RP傳送HTTP消息，該HTTP消息可以包括OpenID標識URL。在1050處，RP和OP（MNO）可以基於OpenID標識來執行發現OP伺服器。例如，RP可以向OP傳送

HTTP（S）獲取標識頁面消息，OP則可以使用OpenID IDP伺服器位址來做出回應。

在1055處，RP可以向OP傳送關聯請求。例如，RP可以向OP傳送HTTP（S）POST。OP可以產生隨機的唯一關聯控制A，並且可以計算秘密S。OP可以向RP傳送關聯回應。例如，OP可以向RP傳送HTTP（S）POST。所述關聯回應可以包括關聯控制A和秘密S。RP可以儲存秘密S和關聯控制A。該RP可以創造臨時用法和會話識別字。

在1060處，RP可以向瀏覽器傳送重定向。例如，RP可以向瀏覽器傳送HTTP重定向。所述重定向可以將瀏覽器重定向到OP，並且可以將關聯控制A包含在請求參數中。OP可以與SCWS相關聯。瀏覽器可以接收重定向，並且可以通過執行經過修改的本地DNS查找來映射到SCWS。在1065處，瀏覽器可以向OP傳送本地驗證請求。例如，瀏覽器可以向OP傳送包含了所述重定向中包含的參數的HTTP獲取http://op.org/server。

在1070處，驗證可以在本地進行。瀏覽器可以爲使用者呈現請求使用者驗證證書的驗證頁面。使用者可以輸入包含使用者名稱和密碼的驗證證書。

在1075處，OP可以基於長期共用秘密密鑰K和關聯控制A來核驗證書。此外，OP還可以計算秘密S，並且可以使用秘密S來計算簽名。該簽名可以用於對斷言消息進行簽名，和/或對諸如返回URL、標識和/或模式之類的參數進行簽名。

在1080處，OP可以向瀏覽器傳送指示瀏覽器存取RP的重定向。例如，OP可以向RP傳送HTTP重定向。所述HTTP重定向可以包括關聯控制A和帶有簽名的參數。在1085處，瀏覽器可以向RP傳送請求，該請求可以包括來自OP且帶有簽名的斷言消息以及OP提供的參數。例如，瀏覽器可以向RP傳送HTTP獲取http://rp.org/return。RP可以使用秘密S來核驗斷言消息上的簽名。然後，在1090處，RP可以允許瀏覽器顯示登錄頁面，並且可以向瀏覽器

提供針對服務的存取。例如，RP可以指示瀏覽器顯示HTML頁面。在1095處，瀏覽器向使用者告知其在RP上登錄。

在一個示例實施方式中，假設在關聯於SCWS的OP與MNO之間存在長期共用密鑰。

如第32圖所示，1040、1065、1070、1080和1095代表的是不會在MNO/空中網路上產生負載的本地通信。此外，由於這些通信可以在設備內部進行，因此，這些通信可以在其他（固定線路或非MNO）網路上沒有業務量的情況下進行。

1045、1005、1085和1090代表的是空中傳送通信，該通信可以作爲資料業務量（例如基於HTTP、IP的通信）而在MNO/空中網路上進行，並且可以代表MNO網路上的負載。

1050和1055代表的是可以在固定線路網際網路之類的固定線路上發生並且可以使用現有基礎架構的業務量。該通信不會增大MNO/空中介面網路上的負載。

第33圖顯示的是基於關聯的通信模式所具有的協定流程的另一個示例實施方式。如第33圖所示，空中傳送業務量可以卸載到本地設備，從而減少空中介面網路業務量。例如，通過執行該處理，可以允許驗證業務量處於本地，以使驗證業務量將空中介面網路或網路服務的負擔最小化。此外，發現和/或關聯業務量可以經由空中介面網路進行，並且可以在固定線路的公共網際網路上進行。

在1100處，使用者可以與瀏覽器之類的使用者介面形成介面，並且可以存取RP，還可以使用OpenID來請求登錄。在1105處，瀏覽器可以向RP傳送可以包含OpenID標識URL的HTTP消息。在1110，RP和OP（MNO）可以基於OpenID標識來執行發現OP伺服器。例如，RP可以向OP傳送HTTP（S）獲取標識頁面消息，OP可以使用OpenID IDP伺服器位址來做出回應。

在1115處，RP可以向OP傳送關聯請求。例如，RP可以向OP傳送HTTP（S）POST。OP可以產生隨機的唯一關聯控制A，並且可以計算秘密S。OP可以向RP傳送關聯回應。例如，OP可以向RP傳送HTTP（S）POST。該關聯回應可以包括關聯控制A和秘密S。RP可以儲存秘密S和關聯控制A。該RP可以創造臨時用法和會話識別字。

在1120處，RP可以向瀏覽器傳送重定向。例如，RP可以向瀏覽器傳送HTTP重定向。所述重定向可以將瀏覽器重定向到OP，並且可以將關聯控制A包含在請求參數中。OP可以與SCWS相關聯。瀏覽器可以接收重定向，並且可以通過執行經過修改的本地DNS查找來映射到SCWS。在1125處，瀏覽器可以向OP傳送本地驗證請求。例如，瀏覽器可以向OP傳送可以包含所述重定向中包含的參數的HTTP獲取http://op.org/server。

在1130處，驗證可以在本地進行。瀏覽器可以爲使用者呈現請求使用者驗證證書的驗證頁面。使用者可以輸入包含使用者名稱和密碼的驗證證書。在1135處，OP可以基於長期共用秘密密鑰K和關聯控制A來核驗證書。此外，OP還可以計算秘密S，並且可以使用秘密S來計算簽名。該簽名可以用於對斷言消息進行簽名，和/或對返回URL、標識和/或模式之類的參數進行簽名。

在1140處，OP可以向瀏覽器傳送指示瀏覽器存取RP的重定向。例如，OP可以向RP傳送HTTP重定向。該HTTP重定向可以包括關聯控制A和帶有簽名的參數。在1145處，瀏覽器可以向RP傳送請求，該請求可以包括來自OP且帶有簽名的斷言消息以及OP提供的參數。例如，瀏覽器可以向RP傳送HTTP獲取http://rp.org/return。RP可以使用秘密S來核驗斷言消息上的簽名。然後，在1150處，RP可以允許瀏覽器顯示登錄頁面，並且可以向瀏覽器提供針對服務的存取。例如，RP可以指示瀏覽器顯示HTML頁面。在1155處，瀏覽器向使用者告知其在RP上登錄。

在一個示例實施方式中，假設在關聯於SCWS的OP與MNO之間存在長期共用密鑰。

如第33圖所示，1100、1125、1130、1140和1155代表的是不會在MNO/空中網路上造成負擔的本地通信。此外，由於這些通信可以在設備內部進行，因此，這些通信可以在其他（固定線路或非MNO）網路不發生業務量的情況下進行。

1105、1120、1145和1150代表的是空中傳送通信，該通信可作爲資料業務量（例如HTTP，基於IP的通信）而在MNO/空中網路上進行，並且可以代表MNO網路上的負載。

1110和1115代表的是可以在固定線路網際網路之類的固定線路上發生並且可以使用現有基礎架構的業務量。該通信不會增大MNO/空中介面網路上的負載。

第34圖顯示的是用於無狀態模式的協定流程的另一個示例實施方式。

1160：使用者可以存取RP網址，爲了使用OpenID進行登錄，他輸入了其OpenID識別字，例如http://op.org/identity。

1165：瀏覽器可以向RP網址發送包含OpenID識別字的HTTP消息。

1170：RP可以使用基於HTTP/HTML的OpenID‘簡單’發現處理，並且經由公共網際網路來與OP-agg取得聯繫，從而在標識頁面上檢索OpenID識別字，例如HTTP獲取http://op.org/identity。

1175：OP-agg可以接收請求，並且可以使用包含OPSF網際網路位址的HTML頁面來進行回應。例如，OP-agg可以通過包含下列位址來做出回應：<link rel=“openid.server” href=http://op.org/server.cgi>。OPSF可以像標準的OpenID標識供應方web服務那樣對RP進行操作。例如，OPSF能夠按照RP的請求來核驗斷言消息上的簽名（由本地OP發佈）。根據需求，OPSF必須可以經由公共網際網路到達，由此假設其具有DNS名稱，

例如可以經由http://op.org到達的op.org。由於外界不知道智慧卡的IP位址，因此，OPOP-agg和OPSF的這種間接性可以用於通信。

OPSF的位址可以不同於OP-agg的位址。

1180：RP可以接收OPSF的位址，並且創造臨時用法和會話識別字，例如nouce = 123123，session = User。RP可以編譯向OP告知應該在使用者驗證之後將瀏覽器重定向到哪一個URL的return_to參數。所述RP可以發佈HTTP重定向，以便將瀏覽器重定向到OP伺服器地址，其中所述重定向包括以下參數：

openid.mode=checkid_setup,

openid.identity=http://op.org/identity,

openid.return_to=http://rp.org/return.cgi?session=User&nonce=123123

1185：瀏覽器可以接收重定向，並且可以開放與RP在重定向消息中規定的URL相連的連接

1190：借助於經過修改而將OPSF的URL映射到SCWS本地IP位址的DNS查找表，例如，通過使用具有項http://op.org==127.0.0.1的主機檔，瀏覽器可以被重定向到與SCWS相關聯的本地OP，並且發佈包含了765處的參數的HTTP請求。

在設備上可以使用經過修改的本地DNS查找表，以使所述設備認爲URL http://op.org位於SCWS的本地IP地址。瀏覽器可以開放與SCWS/本地OP的連接，而不是連接到OPSF（所述OPSF可以經由公共網際網路而在URL http://op.org到達）。

1195：通過執行下列處理，可以確保將驗證業務量保持在本地，這些步驟並不是OpenID協定規範必需或規定的：

a.與SCWS相關聯的OP可以顯示本地驗證頁面

b.使用者可以輸入其驗證證書，例如使用者名稱和密碼

c.與SCWS相關聯的OP可以核驗證書

1200：與SCWS相關聯的OP可以創造唯一的隨機關聯控制A。通過使用函數f，可以使用S=f(A,K)來計算斷言消息的簽名秘密，其中所述f應該是單向的，以使對於A的認識不會展現任何對於K的認識。在一個示例實施方式中，即便展現了S和A，也就是給出了S和A，f也不會展現任何關於K的知識，此外，對於函數g來說，在計算方面，對K=g(S,K)進行計算的處理是不可行的。

由於可能將A作爲重定向消息中的參數的一部分展現給RP，因此可以假設RP不會在OpenID協定過程的無狀態模式中獲得對於S的認識。關聯控制A可以包含在重定向消息中。此外還可以假設，使用S簽名的帶有簽名的消息m不會向簽名核驗器展現任何關於K的資訊（由於使用的是對稱密鑰簽名，因此，簽名核驗器始終需要擁有S來核驗簽名，由此我們不要求該簽名不展現S）。

在一個示例實施方式中，關聯控制可以被規定成是長度爲255個字元或更少的字串，並且可以只包括處於閉區間33-126中的ASCII字元（可列印的非空白字元）。

OPSF用於核驗簽名的秘密與關聯於SCWS的OP用於產生簽名的秘密可以是相同的。簽名的新鮮度可以由下一個步驟中插入的RP臨時用法來確保，並且該RP臨時用法必須是簽名的一部分。OpenID規範對簽名秘密本身的新鮮度保持默契。OP負責確保秘密的密碼強度，保持其秘密性，以及在需要時確保其新鮮度。OPSF和關聯於SCWS的OP可以持續有限壽命或是用於該目的簽名秘密的使用計數。

啓用工具箱的本地OP可以繞過SCWS而使用CAT來主動與手機通信。該消息可以依照標準的OTA（例如用於經由SMS-PP承載來發送OPSF的OTA）而被格式化。但是，這種處理有可能需要OPSF經由MNO的OTA系統來與所述卡進行

通信。在另一個實施方式中，BIP閘道可以擷取工具箱消息的有效負載，並且手機可以使用TCP/IP將其發送到OPSF。這可能要求消息經由MNO的OTA伺服器來傳送。另外，SCWS聲稱只在所述卡不具有IP位址並且不支援TCP/IP的情況下使用BIP。因此，所預期的有可能是使用TCP/IP並借助SCWS來進行發送。

d.其他選項也是可以應用的，這些選項有可能在關聯於SCWS的OP與OPSF之間產生共用秘密。此類方法的可行性有待下一步研究。

1205：與SCWS相關聯的OP可以計算下列參數上的簽名：return_to、標識以及模式。

1210：與SCWS相關聯的OP可以向瀏覽器發送HTTP重定向消息，其中該消息包含了在1180處從RP接收的參數。此外還可以包括下列各項：

·openid.signed參數中的一系列帶有簽名的參數

·openid.assoc_handle參數中的關聯控制A

·openid.sig參數中的簽名（base64編碼）。

在1212處，該消息可以用於將瀏覽器重定向到處於RP的return_to URL。

1215：瀏覽器可以將使用者重定向到RP上的return_to URL。

1220：RP可以接收帶有簽名的斷言消息，並且在經由公共網際網路且基於HTTP（S）的直接通信中加入與OPSF的核驗過程。

1225：RP可以發佈HTTP POST消息，該消息包含了在795處從與SCWS相關聯的OP接收的參數。HTTP POST消息可以包括由與SCWS相關聯的OP產生的關聯控制A。

1230：OPSF可以從參數列表中擷取A，並且可以與關聯於SCWS的OP使用具有相同輸入的相同函數f，即OPSF計算f(A,K)=S，並且使用S作爲共用秘密來核驗從與SCWS相關聯的OP接收的資料上的簽名。

1235：如果簽名核驗成功，那麼OPSF可以返回is_valid:真。

1240：對RP來說，現在可以將使用者標識爲http://op.org/identity。

1245：瀏覽器可以顯示RP的HTML頁面。

1250：使用者可以在RP上作爲http://op.org/identity登錄。

如第34圖所示，1160、1190、1212、1215和1250代表的是不會在MNO/空中網路上產生負載的本地通信。此外，由於這些通信可以在設備內部進行，因此，這些通信可以在其他（固定線路或非MNO）網路未產生業務量的情況下進行。

1165、1180、1220和1245代表的是空中傳送通信，該通信可以作爲資料業務量（例如基於HTTP、IP的通信）而在MNO/空中網路上進行，並且可以代表MNO網路上的負載。

1170、1175、1225和1235代表的是可能在諸如固定線路的網際網路之類的固定線路上出現並且可以使用現有基礎架構的業務量。該通信不會增大MNO/空中介面網路上的負載。

4.5 方案和應用

本節論述的是先前章節中描述的方法和協定的額外實施方式。例如，本節通過顯性列舉了一些不同的方案擴展了以上概括，由此擴展了使用範例和方案的範圍。

術語“智慧卡”（SC）可以用於描述能夠提供安全操作設施的任何類型的積體電路卡（IC）。對於可以使用SC來保持網路驗證證書（例如GSM/UMTS）的行動設備中的特定用途來說，該用途可被稱爲UICC。開放行動聯盟（OMA）定義的智慧卡web伺服器（SCWS）應用並不侷限於在UICC中使用，並且可被設想在其他任何智慧卡上使用。因此，這裏描述的實施方式很容易擴展到一般的SC，例如通過將OpenID與駐留在安全元件內部的OP實體結合使用來實施使用者驗證的實施方式。

此外，其他任何可以爲安全性至關重要的方法提供相似介面和受保護運行

的安全環境都可以是上述實施方式的實施目標。

4.5.1 利益相關者模型

4.5.1.1 MNO模型

在一個示例實施方式中，MNO可以充當全面的標識供應方。MNO可以託管作爲web服務的OP-gg以及OPSF發現和關聯點實體，並且還可以向UICC提供OP應用和使用者標識。

4.5.1.2 第三方OP和MNO

在一個示例實施方式中，假設使用者已經具有註冊到第三方OP的現有OpenID識別字，例如myopenid.com。該OP可被稱爲第三方OP（3OP）。MNO可以不再充當使用者的服務供應者，而是可以傳送資料，並且允許3OP在UICC上安裝OP應用並將其與SCWS應用相關聯。3OP有可能必須與MNO建立業務關係。MNO還可以爲OP應用許可3OP遠端管理權利。MNO可以向3OP收取服務的費用並產生收益。更進一步的細節是在下文中就相容全球平臺（GP）的卡的使用來描述的。

4.5.1.3 非MNO，非行動

在非行動方案中可以使用一個示例實施方式。例如，OpenID標識供應方可以使用諸如銀行發佈的SC之類的一般SC來安裝OP應用。舉例來說，通過執行該處理，可以使用託管了NFC票據應用和OpenID驗證OP應用的銀行卡。可以假設先前不知道將會與SC通信的設備的類型。但是，如果給出了當前的SC規範，那麼可以與SC建立借助USB的TCP/IP連接，其中舉例來說，所述連接是借助本地鏈路、SC讀取器、NFC通信介面等等建立的。SC可以配備能被外部終端到達的SCWS。

4.5.2 分離終端方案

本節描述的是這樣的實施方式，其中包含了託管SCWS和OP應用的SC的設備可以不是與希望存取RP網站的設備相同的設備。在這些實施方式中，SC可

被用作外部驗證權杖。這些分離終端實施方式可以與這裏描述的不同利益相關者模型相結合。

4.5.2.1 具有處於行動終端中的UICC的分離終端

第34圖顯示的是用於分離終端的協定流程的示例實施方式。

在一個示例實施方式中，使用者可以擁有配備了UICC的行動設備，其上安裝了SCWS和OP。使用者可以使用與該行動設備不同的設備存取RP上的期望網頁，其中該設備被稱爲瀏覽代理（BA）。當BA存取RP並提交OpenID識別字以進行登錄時，RP可以將BA重定向到OP，即OP的URL。從RP到BA的HTTP重定向消息可以包括OP應用對斷言消息上的簽名進行計算所需要的必要資訊。該消息的內容可以傳遞到行動設備以及SC上的OP。OP可以在行動設備上向使用者顯示驗證頁面，使用者會授權並驗證所述登錄。OP可以對斷言消息進行簽名。然後，帶有簽名的斷言消息可以被送回RP，這個處理通常由RA完成。然後，RP可以核驗該簽名，並且使用者/BA將會登錄在RP上。

在另一個包含了BA與行動設備之間通信的示例實施方式中，舉例來說，在兩個實體之間可以借助藍芽或WLAN來建立本地鏈路，並且可以將設備註冊成是託管OP的設備。然後，瀏覽器可以經由本地鏈路來向行動設備發送重定向，行動設備則可以將這個重定向轉發給OP/SCWS。然後，OP可以向使用者要求其證書。使用者可以在其行動設備上使用任何一種爲了使用者驗證而實施的方法（例如密碼、PIN、生物測定）來向OP進行驗證。OP可以對斷言消息進行簽名，並且將其經由本地鏈路轉發給BA。然後，BA可以使用這個消息來向RP進行驗證。在該方案中，BA充當了RP與行動設備之間的MITM。由於使用者有可能知道其發起了該OpenID會話，因此，他可以在他的行動設備上檢測到非授權請求。

如第35圖所示，在1255處，BA可以存取RP，並且可以請求使用OpenID進行登錄。在1260，RP可以接收登錄請求，並且可以基於OpenID標識來與OP（

MNO）發起發現OP伺服器的處理。在1265，RP可以向OP（MNO）傳送關聯請求，OP（MNO）則可以傳送關聯回應。該關聯回應可以包括關聯控制A和密鑰S。在1270，RP可以將瀏覽器重定向到與SCWS相關聯的OP。所述RP請求可以將A包含在請求消息中。BA與使用者可以建立本地鏈路。

在1275處，BA可以向與SCWS相關聯的OP傳送本地驗證請求。在1280處，在關聯於SCWS的OP與使用者/行動設備之間可以建立本地驗證處理。

在1285處，與SCWS相關聯的OP可以將BA重定向到RP。該定向可以包括關聯控制，並且可以包括帶有簽名的參數。在1290處，BA可以向RP傳送請求。該請求可以包括來自與SCWS相關聯的OP且帶有簽名的斷言消息。在1295處，RP可以允許BA顯示登錄頁面。

4.5.2.2 外部讀卡器/NFC中的帶有智慧卡的分離終端

在關於非行動SC部署的示例實施方式中，SC可以由基於web的OP或另一個第三方（例如銀行）發佈。在這裏可以應用與行動分離終端範例中描述的步驟相似的步驟。然後，本地鏈路可以借助外部智慧卡讀取器或是借助附著於電腦的NFC（近場通信）終端來建立。該介面可以支援HTTP消息，並且該HTTP消息可被發送給在SC上實施的OP/SCWS。

4.6 OpenID中的信任關係

4.6.1 現有OpenID中的信任關係

第35圖顯示的是OpenID中的信任關係。

4.4.6.1.1 OpenID協定步驟1

如第36圖所示，在1300處，使用者存取允許其在登錄之後存取服務的RP網站。如果他決定使用OpenID登錄，那麼他會被重定向到其OP。使用者必須信任恰當地執行了重定向並且不會遭遇網路釣魚攻擊的RP。此外，使用者還相信供其在登錄之後接收服務的RP，並且（出於隱私原因）相信所述RP不會展現與RP到第三方的使用者互動。

使用者提供的OpenID\識別字進入RP域，並且充當了用於爲RP發現正確OP的手段、以及用於RP與使用者之間互動的識別字。RP僅僅獲悉該識別字，並且通過對其進行解析，RP知道了OP的位址。

根據OpenID規範，發現是可依賴方使用識別字來查找（“發現”）用於發起請求的必要資訊的處理。OpenID驗證具有三種執行發現的途徑。

如果識別字是XRI，[XRI_Resolution（解析）_2.0]（Wachob（瓦霍布），G.、Reed（裏德），D.、ChasenL（查森勒）、Tan（譚），W.以及S. Churchill（邱吉爾），“Extensible Resource Identifier (XRI) Resolution V2.0 - Committee Draft 02（擴展資源識別字（XRI）解析V2.0-委員會草案02）”），那麼它會產生包含必要資訊的XRDS文件。

應該指出的是，可依賴方可以利用CRI代理解析器，例如處於http://www.xri.net的XDI.org提供的解析器。這樣做會消除RP在本地執行XRI解析的需要。

如果它是URL，那麼首先應該嘗試Yadis（雅迪斯）協議（Miller（米勒），J.，“Yadis Specification 1.0（雅迪斯規範1.0）”）[Yadis]。如果取得成功，則結果同樣是XRDS文件。如果Yadis協議失敗並且沒有檢索到有效的XRDS文件，或者在XRDS文件中沒有發現服務元素（OpenID服務元素），則檢索所述URL，並且應該嘗試基於HTML的發現處理（基於HTML的發現）。

值得一提的是，發現步驟有可能爲攻擊者提供進入點。例如，攻擊者可以使用DNS欺騙攻擊來嘗試直接攻擊RP，以便以將RP重定向到受控於攻擊者的僞造OP而並非真實OP的方式來暗中破壞發現步驟。雖然該主機是另一個主機，但由於功能變數名稱相同，因此，RP仍舊認爲它是使用者的真實OP。與似乎處於OpenID規範的範圍以外相對，該缺點存在於OpenID協定和保護的設計中。在可信OpenID文件中業已捕獲到了這種威脅，並且其中論述

了關於某些可能的緩解方法的暗示。

4.6.1.2 OpenID協定步驟2

如第36圖所示，在1305，一旦RP發現使用者OP，則RP會與該OP建立關聯，由此允許其安全地經由共用密鑰保護資訊來進行通信，使用者識別字將會離開RP域並進入OP域。雖然OP會認定他實際託管了帶有指定識別字的使用者標識，但是OP還會獲知該使用者現在正在嘗試存取哪一個站點。如果共用秘密的建立是不安全的（該標準只定義了能被MITM攻擊的Diffie-Hellman），那麼OP無法確保與之關聯的RP與使用者在其瀏覽器中看到的RP相同。

使用者相信OP不會使用收集到的資訊（例如使用者存取過的站點和存取頻率）來構建使用者設定檔。此外，使用者相信OP不會接受來自使用者未存取過的站點的關聯請求（例如攻擊者對未知站點的隱藏登錄嘗試）。

RP相信OP的確會實際驗證使用者，以及爲RP提供可靠的使用者標識資訊。在可以借助RP來收取RP服務費用的支付方案中，RP還相信OP會提供必要的手段來進行收費。例如，如果MNO在OpenID/GBA中充當OP，那麼RP會將OP認定成是由允許借助使用者電話帳單來向其收費的MNO運行的。然後，RP相信MNO-OP會執行收費。

由於可以構建和設置任意的OP（例如那些不驗證使用者並且由此可能被垃圾郵件發送者濫用，從而爲其提供一種簡單機制來創造向論壇、部落格等等濫發通用帳號的OP），因此，RP有可能希望限制針對受限OP集合的存取。在OpenID協議中並沒有規定這種OP白/黑名單方法，但在RP上可以實施該方法來防禦惡性OP。

4.4.6.1.3 OpenID協定步驟3

如第36圖所示，在1310，使用者被重定向到OP頁面並執行驗證。證書將會離開使用者域並進入OP域。因此，使用者與OP之間的介面必須受到保護以

免竊聽。在典型方案中，通過使用HTTP之上的HTTPS，可以提供很小的保護。但是，考慮到使用者不會檢查整個證書鏈，該處理並未防禦帶有有效證書的僞造OP。

使用者相信OP不會濫用證書，也就是說，使用者不會認爲其OP是惡意的。惡意OP很容易即可代表其註冊使用者來存取所有服務。由於OP的損害會導致將使用者證書立即暴露給所有web服務，並且還會導致使用者標識受損，因此，具有較大使用者基礎的大型OP成爲了攻擊者的主要目標。

作爲驗證階段的結果，使用者瀏覽器被來自OP的斷言重定向到了RP，其中所述OP是使用者爲了使用其識別字而進行驗證的OP。

使用者標識受損尤其令人感到擔憂，這是因爲OpenID標識通常不但被用作了用於簡化針對不同web服務的存取的手段，而且還被用作了一種用於在多個站點上構建聲望的手段。因此，一旦識別字被濫用，則很難恢復受好評的標識。

4.6.1.4 OpenID協定步驟4

如第36圖所示，在1315處，通過使用來自OP的斷言，使用者被重定向到RP。RP獲取足夠資訊來相信已經執行過驗證的使用者（和OP），並且相信該使用者知道與識別字相關聯的秘密。RP不會獲得在使用者與OP之間使用的驗證方法的任何資訊或保證。

4.6.2 用於行動本地OP中的信任關係的實施方式

4.6.2.1 概括

第37圖顯示的是與本地OP的信任關係的示例實施方式。在一個示例實施方式中，如果OP成爲使用者的本地實體，那麼OP和使用者域可被認爲是用虛線1340標識的單個域。

在1330處，使用者可以執行驗證，這樣可以減小驗證過程的網路負載。使用者可以與爲其提供更多控制的本地實體共用其私有資料。如果要構建關

聯，那麼RP有可能需要直接與本地OP取得聯繫。該連接不是OpenID協議工作所必需的。RP與OP之間的通信還可以借助間接通信來執行，也就是借助於使用了使用者瀏覽器的重定向。

但是，RP在本地OP中所具有的信任度取決於可以從來自OP的斷言中推導得到的可靠信息量。通常，RP會接受每一個OP，但在需要安全性的應用中，RP可以限制針對一組OP或是具有指定屬性的OP的存取。然後，OP必須爲RP提供這些屬性的資訊。此類資訊可以通過間接通信並從本地OP經由直接頻道（例如關聯頻道）或者經由重定向消息中的附件傳送。在另一個示例實施方式中，關於OP屬性的這種斷言（例如由可信賴的MNO發佈）可以源於TTP。

在1325處，RP可以如1305中描述的那樣繼續進行處理（即4.4.6.1.1節中最後一段）。在1335處，UE可以如1315中描述的那樣繼續進行處理（即4.4.6.1.3節中最後一段）。在1320，UE可以如1300中描述的那樣繼續執行處理（即4.6.1節中第一段）。但在該方案中，如本節中第一段所述，使用者可以採用多種方式來執行本地驗證，而不用在網際網路上進行互動。

4.6.2.2 與MNO的信任關係

第38圖顯示的是與本地OP的信任關係的示例實施方式。如第38圖所示，由於MNO是在智慧卡上運行的，因此它可以與OP具有直接聯繫。RP可以與MNO具有間接聯繫，但是在相容標準的OpenID協定中，它們並不需要建立這種關係。RP可能需要與OP建立聯繫。出於若干種原因，例如借助於MNO的票據處理、標識的提升的信任等級等等，RP可能希望獲取使用者標識的額外資訊。這種信任度可以基於RP在MNO中具有的信任度。

信任度可以從MNO經由OP傳送到RP。在一個示例實施方式中，假設RP對MNO具有某個信任等級（例如通過MNO的聲譽，類似於註冊、服務以及合同協定的帶外處理）。此外，可以假設RP可以在需要時與MNO的實體進行通信，並

且該通信可以用恰當的手段保護（例如IPSEC、HTTPS）。此外還可以假設智慧卡和MNO（的伺服器）可能具有根據需要而以不同方式通信的手段。

在發現處理中可以包含MNO，由此可以通過爲RP提供OP當前位址來允許RP與OP建立直接通信頻道（關聯）。該處理有可能將使用者存取的服務暴露給MNO，由此允許其產生使用者的追蹤設定檔。如果使用了經由使用者瀏覽器的間接處理，那麼該發現處理可以不是必需的。

如果在OpenID協議中包含了MNO，那麼MNO可以具有若干種作用。

4.6.2.2.1 充當OP的（直接）信任度供應方的MNO

充當直接信任度供應方意味著MNO可以直接包含在OP與RP之間用於構建信任的處理中。這種直接包含可以即時向RP確保將OP斷言的標識註冊在了MNO上。如果MNO充當OP的直接信任度供應方，那麼在OP、RP以及適當的服務或是MNO的現有服務組合之間可以使用若干種方法。

a）用於RP與MNO之間的直接連接的示例實施方式

在一個示例中，MNO可以提供能被RP到達的中心服務。RP不能與OP直接關聯，而是經由MNO進行關聯。使用者瀏覽器可被重定向到本地OP。在驗證之後，OP可以向MNO發送聲明驗證成功的消息。該消息可以用MNO發佈給智慧卡的密鑰來簽名。MNO可以核驗該簽名，額外自己的簽名，然後將該消息轉發給RP。RP可以接收兩個消息：來自OP且表明使用者已被驗證的斷言，以及來自MNO且表明有效OP已經執行了驗證的消息。這些消息可以組合在來自MNO的單個消息中，以使所述消息包含表明驗證執行成功的斷言。

b）通過OP的間接通信的示例實施方式

在一個示例實施方式中，MNO可能不希望向RP提供這種外部服務；該通信可以間接地通過OP來傳送。信任度可以直接從來自MNO的聲明中得到，而RP與MNO之間的通信則可以經由OP執行。RP可以使用包含了臨時用法的額外欄位來將瀏覽器重定向到瀏覽器。然後，OP可以從請求中擷取該欄位，並

且可以將其轉發給MNO。MNO可以對其進行簽名，然後，帶有簽名的回應可以包含在從OP到RP的斷言回答中。由於MNO可能對從已知OP接收的臨時用法進行簽名，因此，該處理還具有向MNO隱藏了被存取的服務的額外好處。如果將使用者的真實標識洩露給了RP，那麼該臨時用法可被用作會話識別字，然後，所述會話識別字將會標識該使用者。

c）用於組合方法的示例實施方式

在一個示例實施方式中，通信類型是可以組合的：當使用者希望使用OpenID登錄RP時，RP會與MNO進行聯繫，並且在OpenID協議的關聯階段中與MNO建立共用秘密。然後，RP可以預期OP在完成驗證時將該秘密包含在斷言消息中。對MNO來說，它可以選擇使用新產生的簽名密鑰來爲RP提供帶有簽名的聲明，其中該簽名密鑰是在MNO網路智慧卡中使用GBA協定產生的。借助GBA協定，MNO可以與智慧卡建立秘密，並且這兩個實體可以簽署相同聲明。然後，OP可以將這個帶有簽名的聲明包含在發送給RP的斷言消息中。RP可以對來自MNO且帶有簽名的聲明與斷言消息中的聲明進行比較。所述來自MNO的帶有簽名的聲明（或票據）可以根據需要而產生，或者可以在設備首次與MNO進行驗證並且隨後將其保存在本地的時候產生。當設備隨後嘗試連接到RP時，先前儲存的帶有簽名的聲明可被遞送給RP。

OpenID協議可以允許RP決定是與OP建立關聯（由此建立共用秘密）還是使用無狀態協定流程。OP則可以支援所有這兩種工作模式。如果使用關聯，則可以爲每個RP和每個OP建立共用秘密。這意味著在MNO與使用者設備上的OP之間預先共用的聲明必須包含RP與MNO之間的這個最新秘密。簽名密鑰可以在設備-OP與MNO之間預先共用（例如借助GBA），然後，MNO和OP這二者會使用該簽名密鑰來對基於逐個會話的秘密/臨時用法進行簽名，其中該臨時用法可以在RP與MNO之間確定並由MNO轉發給OP。

4.6.2.2.2 充當OP的（間接）信任度供應方的MNO

在一個示例實施方式中，MNO還可以充當OP的間接信任度供應方。同樣，MNO不必牽涉到OpenID驗證期間的通信過程中。在另一個示例實施方式中，MNO可以向智慧卡發佈證書和密鑰材料，然後，所述證書和密鑰材料可被用於對從OP到RP的斷言消息中的欄位進行簽名。之後，RP可以核驗向其確保OP源于可信任的MNO的簽名和證書。所述證書核驗可以在MNO沒有進一步參與的情況下進行，例如由TTP執行。

4.6.2.2.3 充當OP的信任度和軟體供應方的MNO

在一個示例實施方式中，MNO可以遠端下載並管理智慧卡上的OP套裝軟體。對一些解決方案、例如智慧卡web伺服器（SCWS）來說，該管理可以借助HTTPS管理會話而在SCWS與MNO之間完成。MNO可以直接將用於傳遞信任度的秘密（例如證書，如經過認證的密鑰）包含在OP發佈的聲明中。然後，RP可以從已認證秘密中推導出信任度。MNO甚至還可以將一組秘密包含在OP軟體中，以便與不同的使用者識別字結合使用。RP可以從MNO發佈的OP軟體證書中推導出信任度。

在一個示例實施方式中，GBA可以允許MNO與設備上的OP建立共用秘密。由於該秘密未必爲RP所知，但是RP有可能已經與MNO建立了安全通信頻道，因此，MNO可以在關聯頻道中將這個（GBA得出的）秘密轉發給RP，以使RP可以自主核驗OP斷言聲明，其中所述聲明是用GBA導出的密鑰簽名的。

在另一個實施方式中，當在MNO與OP之間建立了GBA秘密之後，MNO可以從RP請求臨時用法和RP ID，然後使用所述臨時用法和RP ID來從其與OP之間的GBA秘密中建立僅用於該特定RP和該特定會話的進一步秘密。例如，通過執行這個處理，可以避免將GBA導出的秘密重新用於與RP的關聯，以及避免將GBA導出的秘密暴露給RP。然後，MNO可以將這個RP和會話專用秘密轉發給RP。與第一個選項中一樣，RP隨後能夠基於該會話專用密鑰來核驗斷言上的OP簽名。

4.7 全球平臺智慧卡上的實施方式

GP SC可以託管多個所謂的安全域（SD），其中所述安全域能使每一個SD代表利益相關者，並且能爲該利益相關者儲存密鑰並且安裝和個性化應用。主SD可以是屬於卡發佈者的發佈者SD。SD可以採用層級結構來組織，並且SD可以具有在其層級內部管理內容的不同許可權。發佈者SD可以具有授權的管理（AM）許可權，這意味著它具有卡的自主控制權，並且能在其層級中安裝和刪除SD。其他SD則只在駐留於卡上的獨立層級時才被給予AM。如果SD處於相同層級，那麼SD可以得到委託管理（DM）許可權，其中該DM許可權允許SD在其子層級中管理卡的內容。該SD執行的所有操作都可以由發佈者用權杖授權，其中所述權杖由DM SD呈現給發佈者SD，並由所述發佈者SD進行檢查。

駐留在不同SD中的GP SC的應用能夠使用可信路徑（TP）的概念來進行通信。TP可以是必須指定給應用的許可權，其允許這些應用借助GP的開放API來交換命令。否則，應用在GP SC上是被分離的。

第39圖顯示的是具有發佈方SD的SD層級的示例實施方式。

第40圖顯示的是具有DM的SD層級的示例實施方式。

4.7.2 實施方式的實施選項

根據可以如何在SC上實施SCWS，可以啓用不同的利益相關者模型。

4.7.2.1 作爲GP應用的SCWS的實施方式

第41圖顯示的是作爲GP應用的SCWS的示例實施方式。在一個示例實施方式中，SCWS可以在SC發佈者擁有的特定SD中作爲GP應用來實施，並且可以支援MNO模型和第三方OP模型以及非MNO模型。我們假設OP的應用邏輯可以作爲不同的應用駐留在不同的SD中，並且由此可以被與擁有SCWS應用和域的實體不同的實體擁有和管理。這兩個應用都可以使用可信路徑能力來進行通信。第三方和卡發佈者必須就用於實施該方案的業務聯繫達成一致，例

如將正確的許可權許可給SD和應用。

應用提供方（第三方OP）SD可以配備DM許可權，並且可以管理OP應用。

SCWS管理可以由卡發佈者借助SCWS管理代理SD來執行，其中所述SD通常支援OTA管理能力，例如借助HTTM的RAM。如果APSD還支援SCP80協定，那麼應用和內容可以是由第三方使用DM權杖管理的OTA。

4.7.2.2 範例2：在卡的運行時間環境（RTE）中實施的SCWS

第42圖顯示的是在卡的運行時間環境中實施的SCWS的示例實施方式。在一個示例實施方式中，由於對SCWS的存取不會通過GP框架暴露，因此，SCWS可以在卡的RTE中由SC製造商來實現，並且第三方應用無法與SCWS進行通信。因此，不能支持第三方OP的利益相關者模型。但是，支援MNO模型和非行動模型。

4.8 SCWS之外的其他平臺上的OP實施方式

4.8.1 使用Java卡作爲平臺

在Java卡上可以安裝Java運行時間環境，該環境允許跨越不同SIM卡（和廠家）的SIM卡應用的互操作性。

在一個示例實施方式中，Java卡平臺可以用於允許MNO創造並向Java卡部署小應用程式OTA。

4.4.8 使用嵌入式安全元件的實施方式

如上所述，在智慧卡中可以實施屬於使用者或是受到使用者某種程度的控制的設備中的嵌入式本地OP應用。隨著嵌入式安全解決方案在行動設備中的日益擴展，有可能存在提供了不同安全屬性的多個不同的運行環境。智慧卡上的OP設計可以擴展至其他（嵌入式）安全元件，由此可以允許安全地執行代碼以及安全地儲存證書。此外，運行環境可能需要提供連至外部環境的通信頻道，尤其是用於OP－使用者驗證互動、OP－瀏覽器通信（基於HTTP(s)）以及OP－RP關聯和斷言消息（也基於HTTP(s)）的頻道。

在一個示例實施方式中，所使用的可以是行動電話內部已可用於爲設備上的OP軟體提供可信運行環境（TEE）的已有安全環境（例如信任區域等等）。

由於智慧卡可以被視爲處於MNO的控制之下，因此，智慧卡可以代表MNO的關鍵資源。在實施嵌入式運行環境上的OP的過程中、尤其是MNO與本地OP建立共用秘密的實施方式中，MNO可能需要核驗運行環境安全屬性的裝置。該裝置可以包括但不侷限於：

·執行運行環境的完整性測量的能力

·報告完整性測量的通信

·需要對設備運行環境進行（完整性）核驗，由此將其轉入可信運行環境（TEE）中

·用於從MNO網路到嵌入式TEE中的OP的下載/供應協議/處理

·TEE的通信能力；OP必須能與RP和使用者（以及MNO）進行通信

在一些示例實施方式中（在智慧卡上或TEE內部），MNO可以獲得關於使用者行爲的額外資訊（例如使用者存取的RP、登錄頻率、使用者行爲等等）。在要求隱私的方案、例如在公司環境中，公司希望向MNO隱藏使用者行爲，並且較爲有益的則是在很大程度上都不包含MNO。

在另一個示例實施方式中，如果使用了嵌入式安全特徵來執行本地OP的實施方式，那麼MNO不能包含在OpenID處理中。這樣做可以允許使用者自主建立、管理和保持處於其設備的TEE內部的OP裝置。在該方案中，OP不能與MNO共用秘密，這是因爲可以假設MNO在OP實施方式中可能缺乏信任度。但是，在使用者與他的設備之間可以存在本地信任關係。使用者可以信任所述OP實施方式不會向第三方洩露任何私有個人資料。由於MNO不能發佈關於OP實施方式的斷言，因此，隱私性的增加可能是以來自RP的OP信任度的降低爲代價的。

4.8.3 來自可信OpenID創新的概念整合

在一個示例實施方式中，OP可以在智慧卡上實施。關於設備完整性的評定可被包含在內並且引入可供設備測量和報告完整性的需求。對於可以支援針對MNO的完整性核驗/報告的設備來說，MNO首先可以檢查設備完整性以及OP的安全/運行時間環境。然後，MNO可以爲OP軟體觸發（遠端）軟體安裝程式。此外，MNO可以爲OP應用配備設備參考值。然後，OP可以對照這些參考值來檢查在OpenID驗證過程中報告的測量，並且如果順利通過完整性檢查，則可以允許所述驗證。

雖然在上文中描述了採用特定組合的特徵和元素，但是本領域普通技術人員將會瞭解，每一個特徵既可以單獨使用，也可以與其他特徵和元素進行任何組合。此外，這裏描述的方法可以在引入到電腦可讀取媒介中並供電腦或處理器運行的電腦程式、軟體或韌體中實施。關於電腦可讀取媒介的示例包括電信號（經由有線或無線連接傳送）以及電腦可讀取媒介。關於電腦可讀取媒介的示例包括但不侷限於唯讀記憶體（ROM）、隨機存取記憶體（RAM）、暫存器、緩衝記憶體、半導體記憶裝置、內部硬碟和可拆卸磁碟之類的磁介質、磁光介質、以及CD-ROM光碟和數位多用途光碟（DVD）之類的光介質。與軟體相關聯的處理器可以用於實施在WTRU、UE、終端、基地台、RNC或任何主電腦中使用的無線頻率收發器。

【符號說明】

【0006】 100 通信系統

102、102a、102b、102c、102d 無線發射/接收單元（WTRU）

104 無線電接入網路（RAN）

106 核心網路

108 公共交換電話網絡（PSTN）

110 網際網路

112　其他網路

114a、114b　基站

116　空中介面

118　處理器

120　收發器

122　發射/接收部件

124　揚聲器/麥克風

126　數位鍵盤

128　顯示器/觸控板

130　不可移除記憶體

132　可移除記憶體

134　電源

136　全球定位系統（GPS）晶片組

138　週邊設備

140a、140b、140c　e節點-B

142　移動性管理閘道（MME）

144　服務閘道

146　分組資料網路（PDN）閘道

AM　授權的管理

assoc_handle　關聯_控制碼

BSF　自舉伺服器功能

DM　委託管理

HSS　家庭用戶伺服器

HTTP、HTTPS　通信協議

GET　獲取

GP　全球平臺

【0007】 LAP　本地斷言供應方

MNO　移動網路供應方

NAF　網路位址功能

OP　供應方

OpenID　開放ID

OPSF　伺服器功能

POST　傳遞

RAM　隨機存取記憶體

return_to　返回_到

RP　可依賴方

RTE　運行時間環境

S1、Ub、X2、Zn　介面

SCWS　智慧卡網路伺服器

SIM　使用者識別模組

SSO　單點登錄

UE　使用者裝置

UICC　通用積體電路卡

web　網路

【主張利用生物材料】

【0008】

【發明申請專利範圍】

【第1項】 一種用於通過啓用一開放管理安全協議來使一可依賴方（RP）能夠驗證一使用者的使用者環境，該使用者環境包括：

一使用者介面，該使用者介面使用一單點登錄安全協議來與所述RP進行通信，以便代表使用者來請求存取所述RP提供的一服務，並且其中所述RP與單點登錄證書的一可信供應方進行通信，以便發起對所述使用者的一驗證；以及

一處理器，該處理器在所述使用者環境內部爲所述可信供應方驗證所述使用者，所述處理器被配置成在本地執行單點登錄證書的該可信供應方的至少一些功能，以便在驗證過程中限制所述使用者環境以外的通信。

【第2項】 如申請專利範圍第1項所述的使用者環境，其中所述使用者介面接收來自所述RP的一指示，該指示表明所述RP希望對所述使用者進行驗證。

【第3項】 如申請專利範圍第1項所述的使用者環境，其中所述使用者介面接收來自所述RP的一重定向消息，該重定向消息指示所述使用者介面對所述使用者進行驗證。

【第4項】 如申請專利範圍第1項所述的使用者環境，其中所述使用者介面接收來自所述使用者的使用者證書。

【第5項】 如申請專利範圍第1項所述的使用者環境，其中所述處理器是一可信計算環境。

【第6項】 如申請專利範圍第5項所述的使用者環境，其中所述使用者介面整體或部分是由該可信計算環境保護的。

【第7項】 如申請專利範圍第5項所述的使用者環境，其中當所述使用者已被驗證時，所述可信計算環境向所述RP傳送一驗證回應。

【第8項】 如申請專利範圍第5項所述的使用者環境，其中所述可信計算環境是下列各項之一：通用積體電路卡（UICC）、使用者標識模組（SIM）、機器對機器（M2M）設備、智慧卡、java卡、全球平臺智慧卡、或安全集成晶片卡（ICC）。

【第9項】 如申請專利範圍第5項所述的使用者環境，其中所述可信計算環境是使用智慧卡網路伺服器（SCWS）來實施的。

【第10項】 如申請專利範圍第5項所述的使用者環境，其中所述可信計算環境與OpenID供應方共用秘密。

【第11項】 如申請專利範圍第5項所述的使用者環境，其中所述可信計算環境計算簽名，並且將所述簽名經由所述使用者介面提供給所述RP，以便允許所述RP核驗所述可信計算環境的證書。

【第12項】 如申請專利範圍第5項所述的使用者環境，其中所述可信計算環境計算簽名，並且將所述簽名經由所述使用者介面提供給所述OP，以便允許所述OP核驗所述可信計算環境的證書。

【第13項】 如申請專利範圍第10項所述的使用者環境，其中所述可信計算環境基於所述秘密來計算簽名，並且將所述簽名經由所述使用者介面提供給所述RP，以便允許所述RP核驗所述可信計算環境的證書。

【第14項】 如申請專利範圍第10項所述的使用者環境，其中所述可信計算環境基於所述秘密來計算簽名，並且將所述簽名經由所述使用者介面提供給所述OP，以便允許所述OP核驗所述可信計算環境的證書。

【第15項】 如申請專利範圍第5項所述的使用者環境，其中所述可信計算環境與所述OP經由所述使用者介面建立共用秘密。

【第16項】 如申請專利範圍第15項所述的使用者環境，其中所述使用者介面接收來自所述RP的包含了關聯控制的驗證請求，並且將所述關聯控制提供給所述可信計算環境。

【第17項】 如申請專利範圍第15項所述的使用者環境，其中所述使用者介面接收來自所述可信計算環境的包含了關聯控制的重定向消息，並且將所述關聯控制提供給所述RP。

【第18項】 如申請專利範圍第16項所述的使用者環境，其中所述可信計算環境基於所述共用秘密來產生簽名，並且產生包含了所述簽名和所述關聯控制的驗證響應。

【第19項】 如申請專利範圍第18項所述的使用者環境，其中所述使用者介面將所述可信計算環境產生的所述驗證響應提供給所述RP。

【第20項】 如申請專利範圍第1項所述的使用者環境，其中所述積體電路產生簽名，並且接收來自所述OP的簽名斷言消息。

【第21項】 如申請專利範圍第20項所述的使用者環境，其中所述積體電路向所述RP傳送簽名響應消息。

【第22項】 如申請專利範圍第1項所述的使用者環境，其中所述使用者介面和所述積體電路處於相同設備上。

【第23項】 如申請專利範圍第1項所述的使用者環境，其中所述使用者介面和所述積體電路處於分離的設備上。

【第24項】 如申請專利範圍第1項所述的使用者環境，其中對所述使用者的驗證是通過用密碼或PIN碼、生物測定標識、權杖或是其組合來核驗所述使用者而被執行的。

【第25項】 一種用於保護使用者環境和/或本地斷言供應方（LAP），以便在一開放管理安全協議中爲可依賴方（RP）驗證一使用者的方法，該方法包括：

經由一使用者介面接收來自所述RP且表明所述RP希望對所述使用者進行驗證的一指示，所述RP能夠與單點登錄（SSO）證書的一可信供應方進行通信；

通過所述使用者介面接收來自所述使用者的使用者證書；

使用接收到的所述使用者證書來爲所述RP驗證所述使用者，以便在本地執行SSO證書的所述可信供應方的至少一些功能，而在驗證過程中限制所述使用者環境以外的通信；以及

經由所述使用者介面來將一驗證回應傳送到所述RP。

【第26項】 如申請專利範圍第25項所述的方法，其中所述LAP處於可信計算環境內部。

【第27項】 如申請專利範圍第26項所述的方法，其中所述指示是重定向消息。

【第28項】 如申請專利範圍第27項所述的方法，其中所述重定向消息指示所述使用者介面使用所述可信計算環境來驗證所述使用者。

【第29項】 如申請專利範圍第27項所述的方法，其中驗證所述使用者是經由可信計算環境執行的。

【第30項】 如申請專利範圍第29項的方法，其中所述可信計算環境是下列各項之一：UMTS積體電路卡（UICC）、使用者標識模組（SIM）、機器對機器（M2M）設備、智慧卡、java卡、全球平臺智慧卡、或安全集成晶片卡（ICC）。

【第31項】 如申請專利範圍第26項所述的方法，其中所述驗證回應是在所述使用者已被驗證時被傳送的。

【第32項】 如申請專利範圍第26項所述的方法，其中使用可信計算環境驗證所述使用者是藉由使用智慧卡網路伺服器（SCWS）之類的安全網路伺服器而發生的。

【第33項】 如申請專利範圍第26項所述的方法，該方法還包括：與關聯於行動網路營運商（MNO）的開放管理安全供應方共用秘密。

【第34項】 如申請專利範圍第26項所述的方法，該方法還包括：與關聯於行動網路營運商（MNO）的OpenID供應方共用秘密。

【第35項】 如申請專利範圍第29項所述的方法，該方法還包括：計算簽名，並且將

所述簽名經由所述使用者介面提供給所述RP，以便允許所述RP核驗所述可信計算環境的證書。

【第36項】 如申請專利範圍第35項所述的方法，該方法還包括：經由所述使用者介面而與所述RP建立共用秘密。

【第37項】 如申請專利範圍第36項所述的方法，該方法還包括：接收來自所述RP的關聯控制。

【第38項】 如申請專利範圍第37項所述的方法，該方法還包括：基於所述共用秘密來產生簽名，以及產生包含了所述簽名和所述關聯控制的驗證響應。

【第39項】 如申請專利範圍第38項所述的方法，該方法還包括：接收來自所述RP的簽名斷言消息。

【第40項】 如申請專利範圍第39項所述的方法，該方法還包括：向所述RP傳送簽名響應消息。

【第41項】 如申請專利範圍第29項所述的方法，該方法還包括：計算簽名，並且將所述簽名經由所述使用者介面提供給所述OP，以便允許所述OP核驗所述可信計算環境的證書。

【第42項】 如申請專利範圍第41項所述的方法，該方法還包括：經由所述使用者介面而與所述OP建立共用秘密。

【第43項】 如申請專利範圍第36項所述的方法，該方法還包括：接收來自所述可信計算環境的關聯控制，並且將該關聯控制傳送給所述OP。

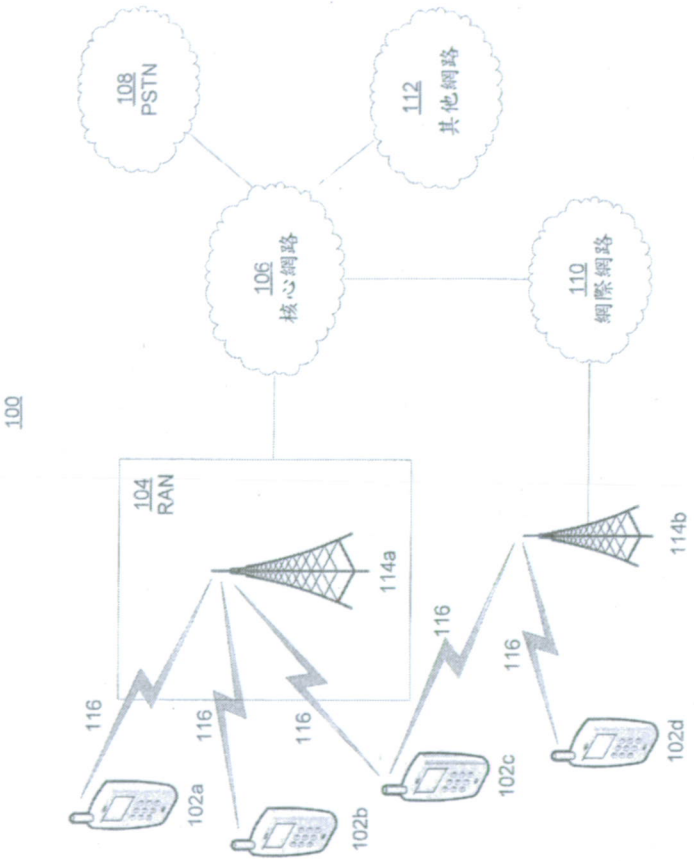
【第44項】 如申請專利範圍第43項所述的方法，該方法還包括：基於所述共用秘密來產生簽名，並且產生包含了所述簽名和所述關聯控制的驗證響應。

【第45項】 如申請專利範圍第44項所述的方法，該方法還包括：接收來自所述OP的簽名斷言消息。

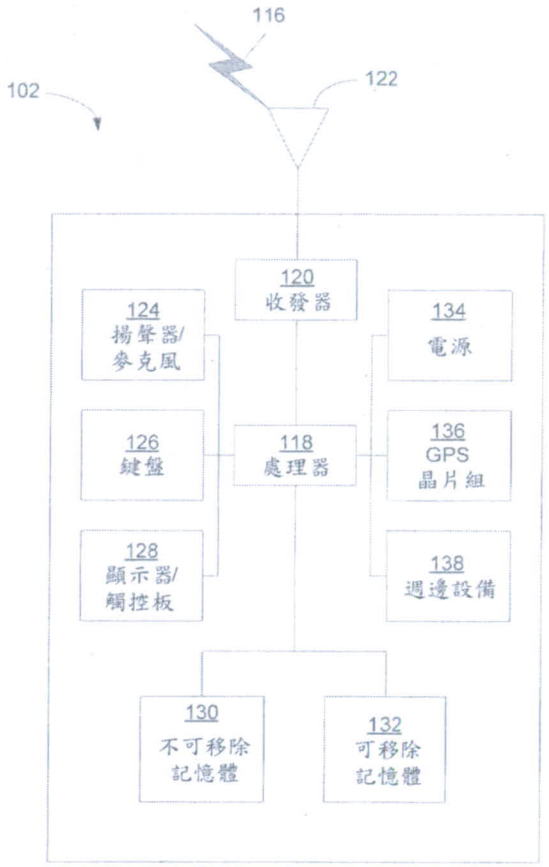
【第46項】 如申請專利範圍第45項所述的方法，該方法還包括：向所述OP傳送簽名響應消息。

【第47項】 如申請專利範圍第25項所述的方法，其中驗證所述使用者是通過用密碼或PIN碼、生物測定標識、權杖或是其組合來核驗所述使用者而被執行的。

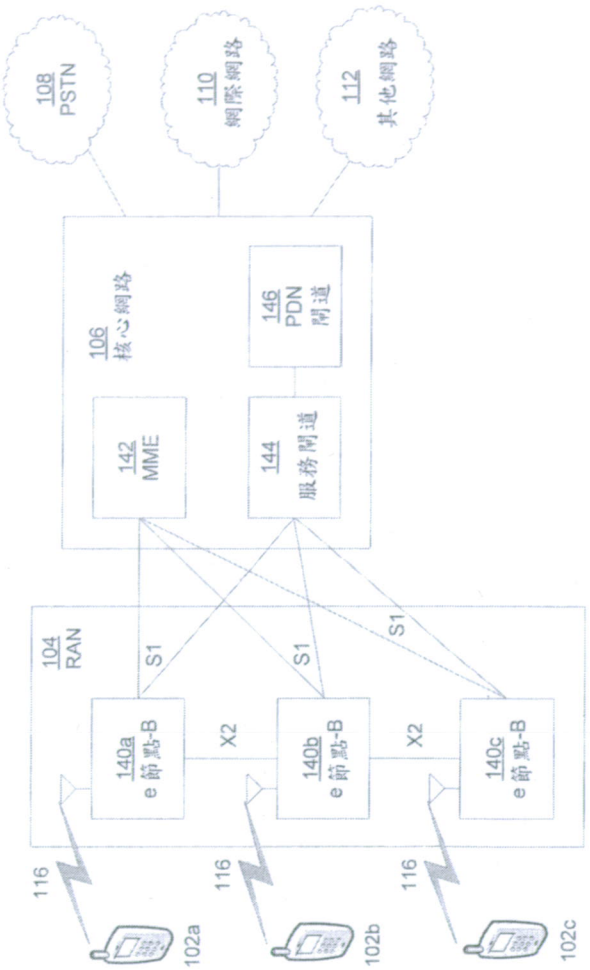
【發明圖式】


100
108
PSTN
112
其他網路
106
核心網路
110
網際網路
104
RAN
114a
114b
116
116
116
116
116
102a
102b
102c
102d

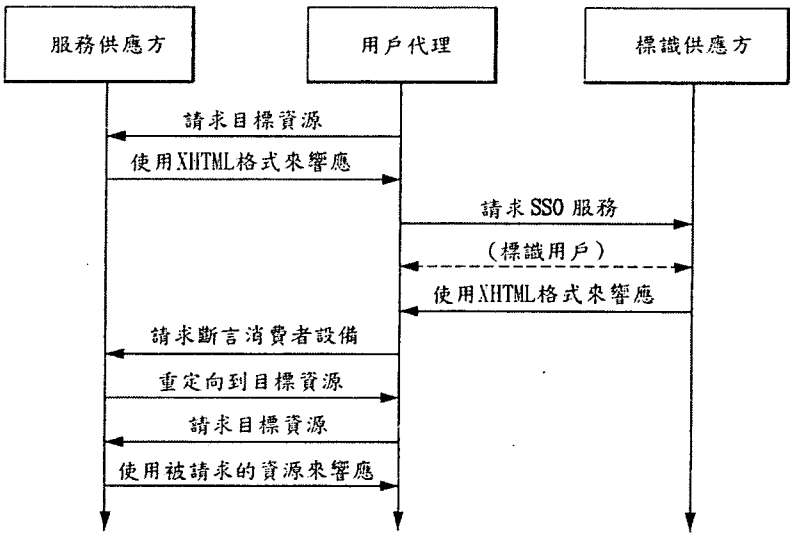
第 1A 圖


116
102
122
120
收發器
124
揚聲器/
麥克風
134
電源
126
鍵盤
118
處理器
136
GPS
晶片組
128
顯示器/
觸控板
138
週邊設備
130
不可移除
記憶體
132
可移除
記憶體

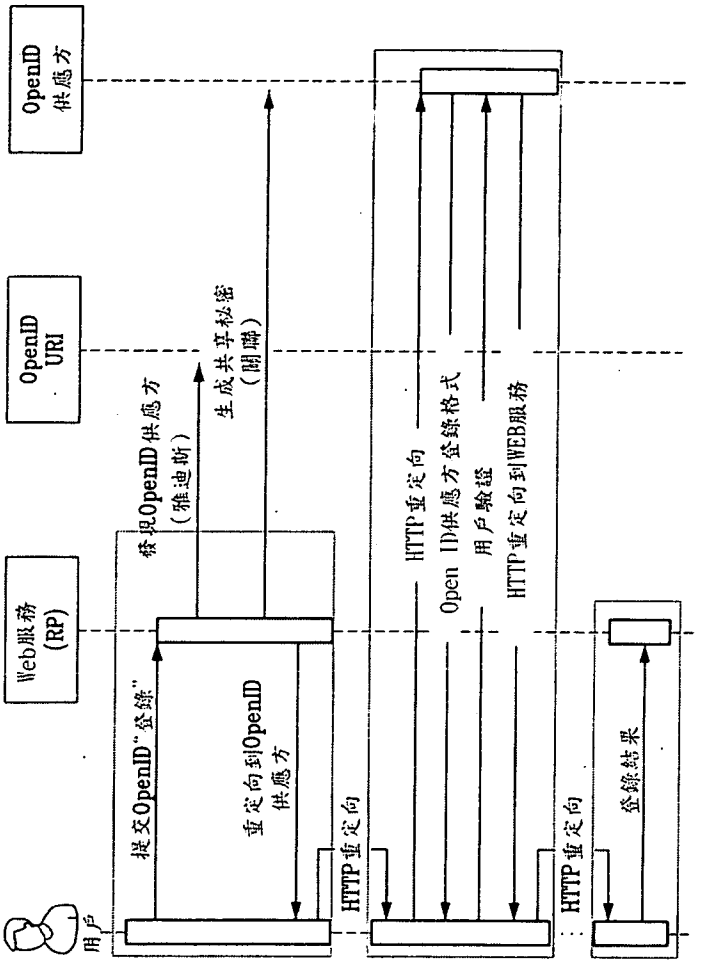
第 1B 圖


108
PSTN
110
網際網路
112
其他網路
106
核心網路
146
PDN
閘道
142
MME
144
服務閘道
104
RAN
S1
S1
S1
140a
e 節點-B
140b
e 節點-B
140c
e 節點-B
X2
X2
116
116
116
102a
102b
102c

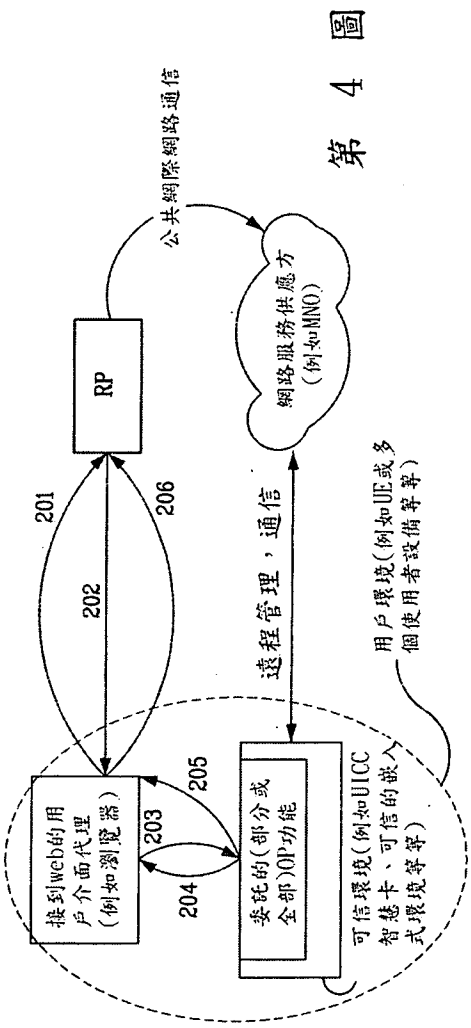
第 1C 圖


服務供應方
用戶代理
標識供應方
請求目標資源
使用XHTML格式來響應
請求SSO服務
(標識用戶)
使用XHTML格式來響應
請求斷言消費者設備
重定向到目標資源
請求目標資源
使用被請求的資源來響應

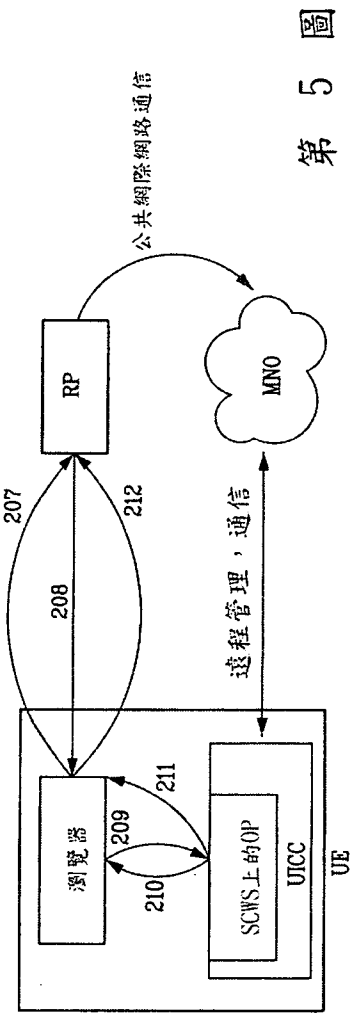
第 2 圖



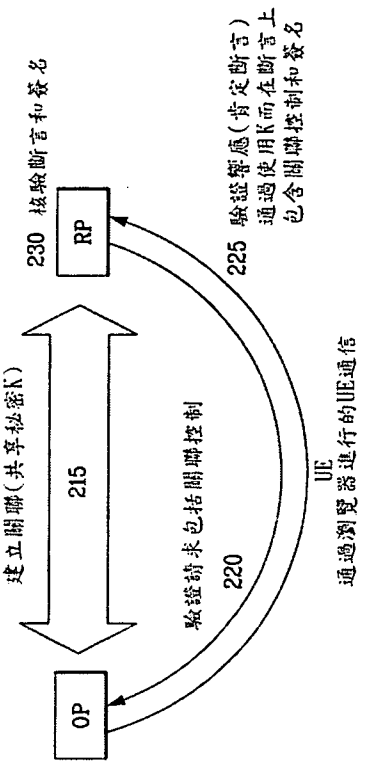
OpenID協定 第3圖


公共網際網路通信
RP
網路服務供應方
(例如MNO)
201
206
202
遠程管理，通信
用戶環境(例如UE或多個使用者設備等等)
接到web的用戶介面代理(例如瀏覽器)
205
203
204
委託的(部分或全部)OP功能
可信環境(例如UICC智慧卡、可信的嵌入式環境等等)

第 4 圖

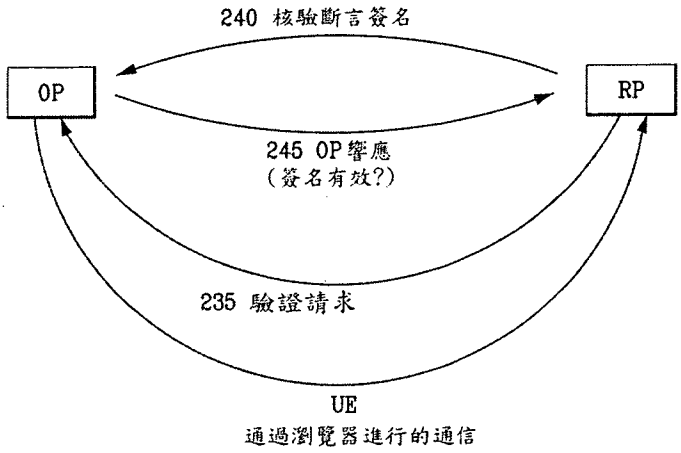

公共網際網路通信
RP
MNO
207
212
208
遠程管理，通信
瀏覽器
209
211
210
SCWS上的OP
UICC
UE

第 5 圖


230 核驗斷言和簽名
RP
225 驗證響應(肯定斷言)
通過使用K而在斷言上
包含關聯控制和簽名
建立關聯(共享秘密K)
215
驗證請求包括關聯控制
220
OP
UE
通過瀏覽器進行的UE通信

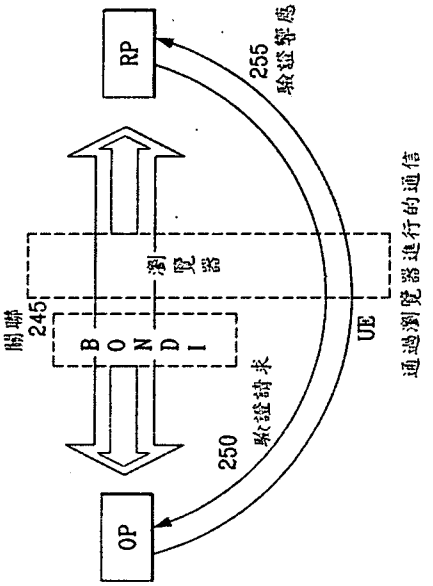
基於關聯的通信

第 6 圖



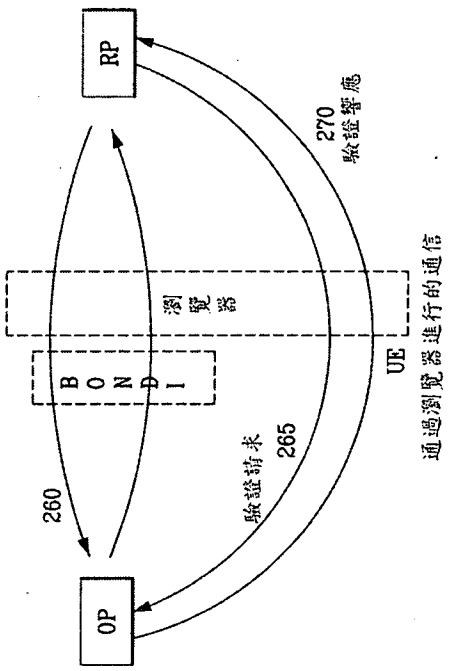
無狀態簽名核驗

第 7 圖



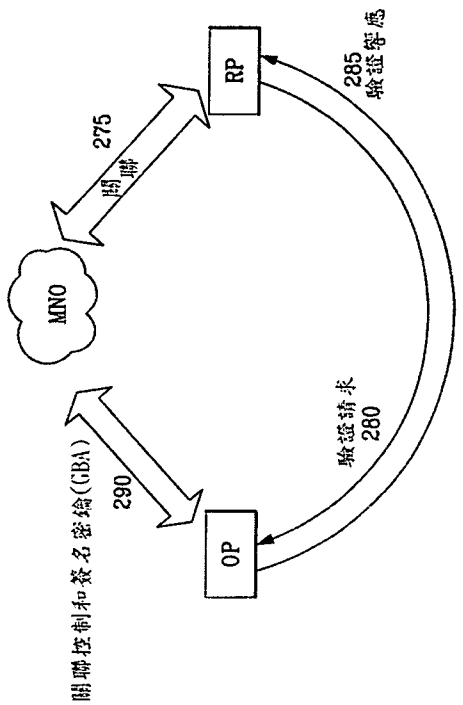
將BOND1與基於關聯的通信集成

第 8 圖

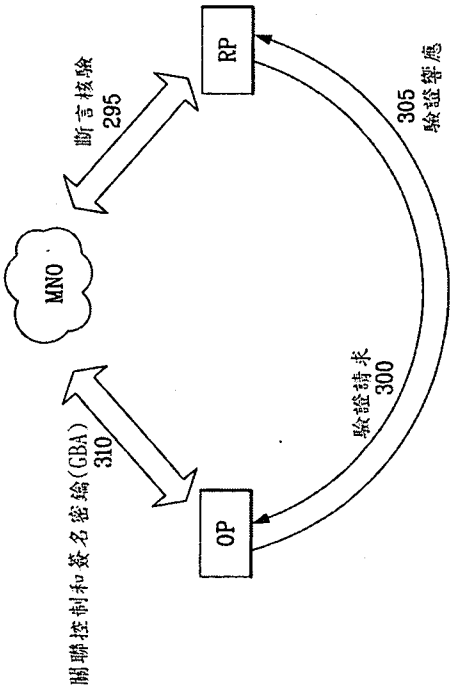


將BONDI與無狀態簽名核驗集成

第 9 圖

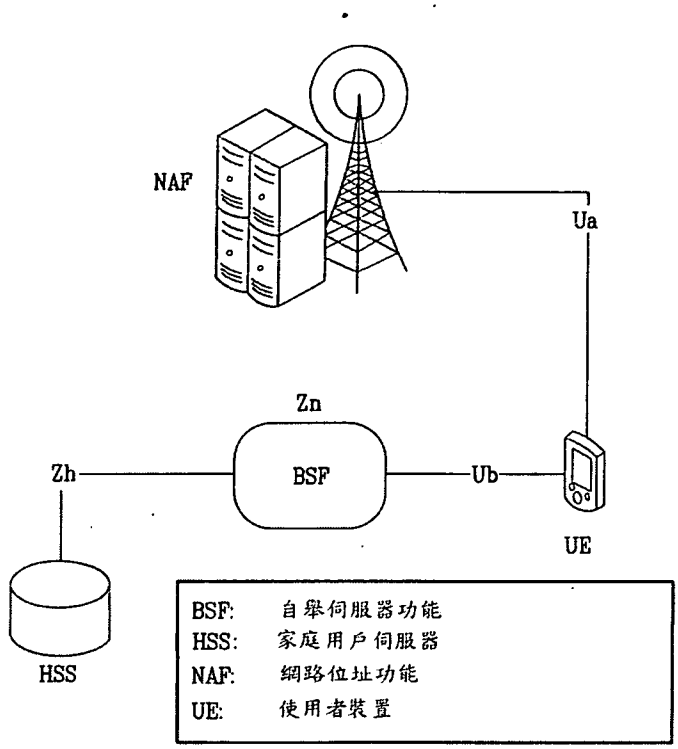

RP
285
驗證響應
275
關聯
MNO
UE
通過瀏覽器進行的通信
驗證請求
280
290
關聯控制和簽名密鑰(GBA)
OP
分離OP方案(基於關聯)

第 10 圖



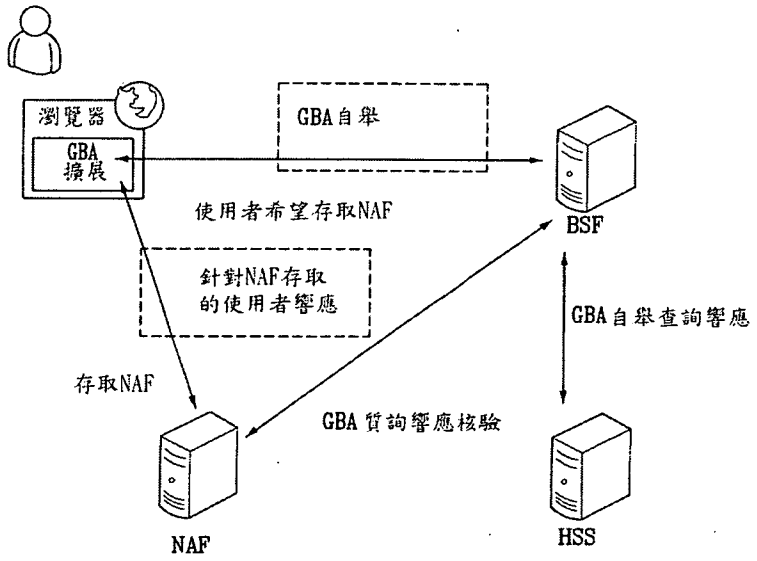
結合無狀態簽名核驗的分離OP方案

第 11 圖


NAF
Ua
Zn
Zh
BSF
Ub
UE
HSS
BSF: 自舉伺服器功能
HSS: 家庭用戶伺服器
NAF: 網路位址功能
UE: 使用者裝置

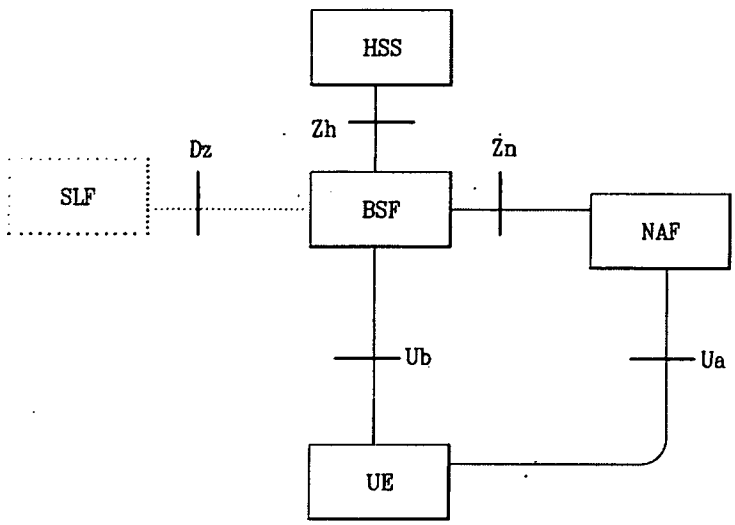
BSF 功能

第 12 圖


瀏覽器
GBA
擴展
GBA自舉
BSF
使用者希望存取NAF
針對NAF存取
的使用者響應
GBA自舉查詢響應
存取NAF
GBA 質詢響應核驗
NAF
HSS

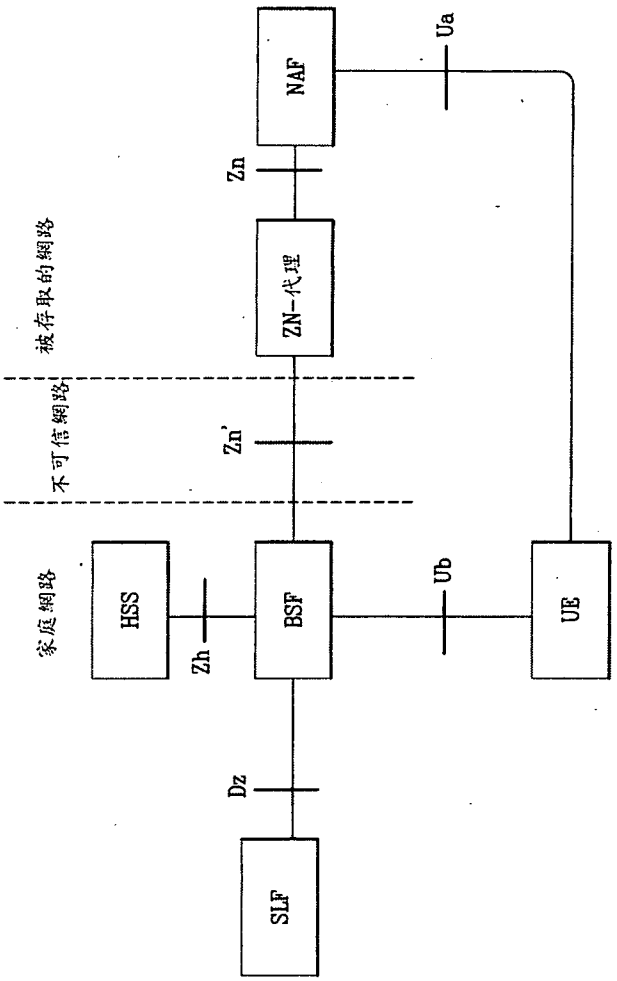
GBA 架構

第 13 圖



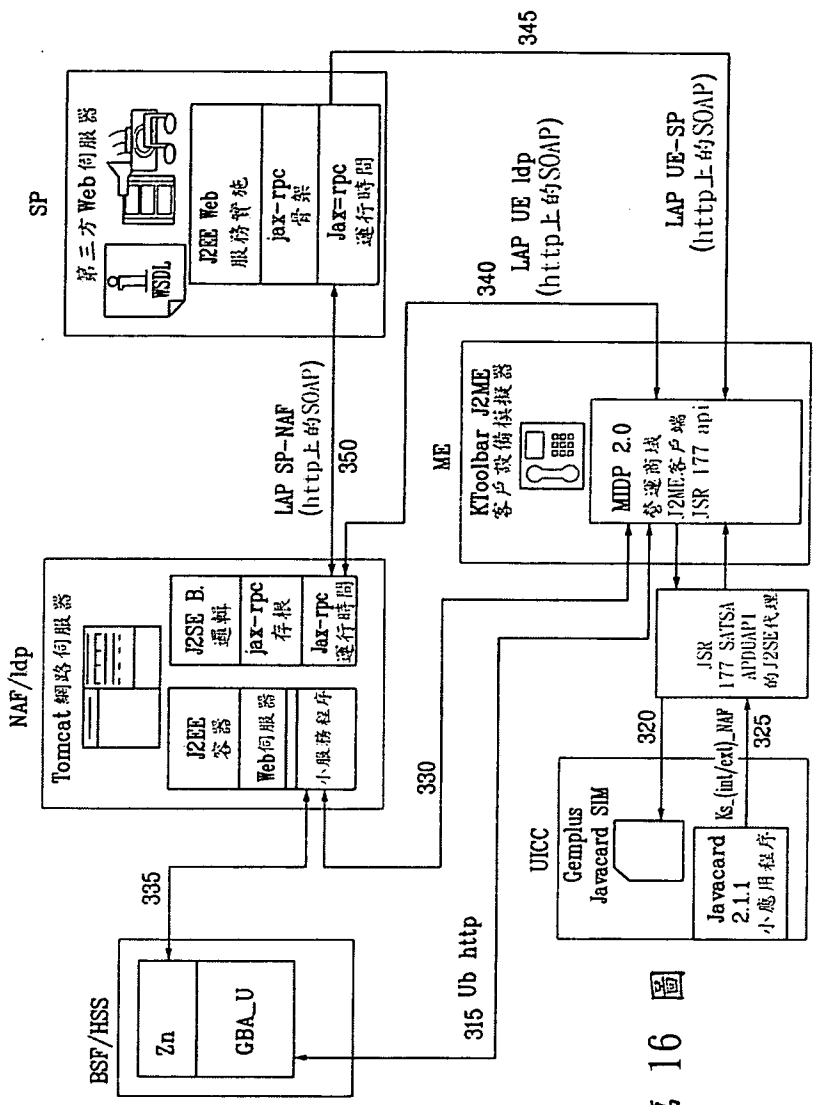
來自3GPP TS 33.220的GBA參考模型

第 14 圖

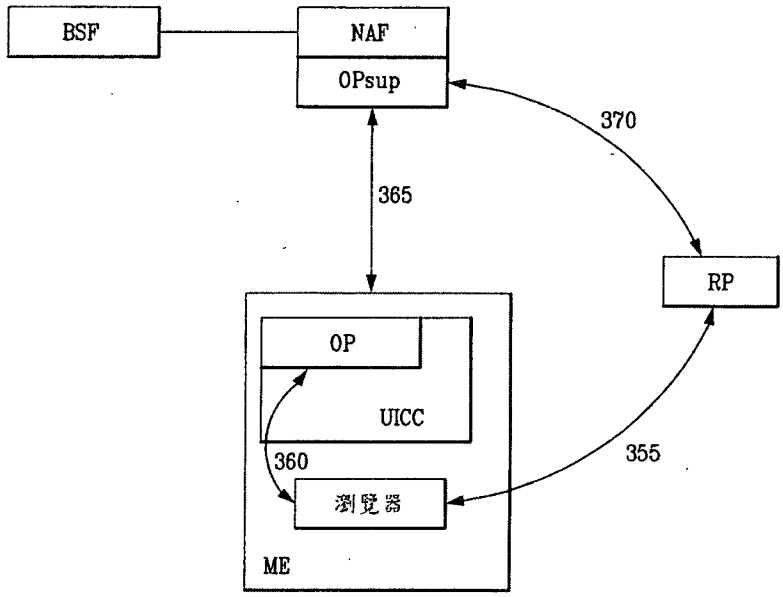


來自3GPP TS33.220的用於被存取網路的GBA參考模型

第 15 圖

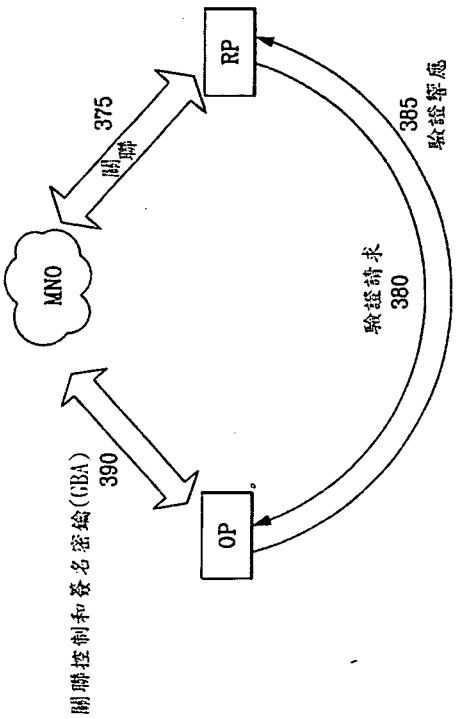

SP
第三方 Web 伺服器
WSDL
J2EE Web 服務管理
jax-rpc 骨架
Jax-rpc 運行時間
345
LAP UE ldp (http上的SOAP)
LAP UE-SP (http上的SOAP)
340
LAP SP-NAF (http上的SOAP)
350
ME
KToolbar J2ME 客戶設備模擬器
MIDP 2.0
管理商域 J2ME客戶端 JSR 177 api
NAF/ldp
Tomcat 網路伺服器
J2SE B. 通訊
jax-rpc 存根
Jax-rpc 運行時間
J2EE 容器
Web伺服器
小服務程序
330
JSR 177 SATSA APDUAPI 的J2SE代理
320
325
UICC
Gemplus Javacard SIM
Ks_(int/ext)_NAF
Javacard 2.1.1 小應用程序
335
BSF/HSS
Zn
GBA_U
315 Ub http

第 16 圖



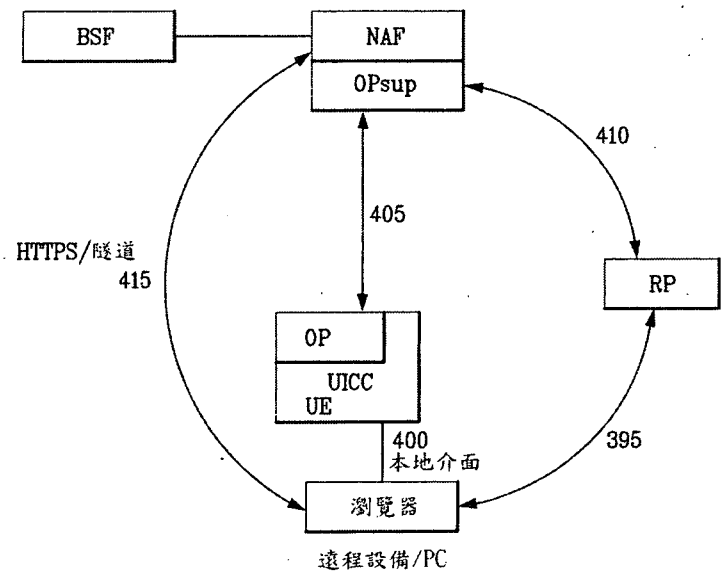
將GBA用於MNO支持的標識斷言

第 17 圖

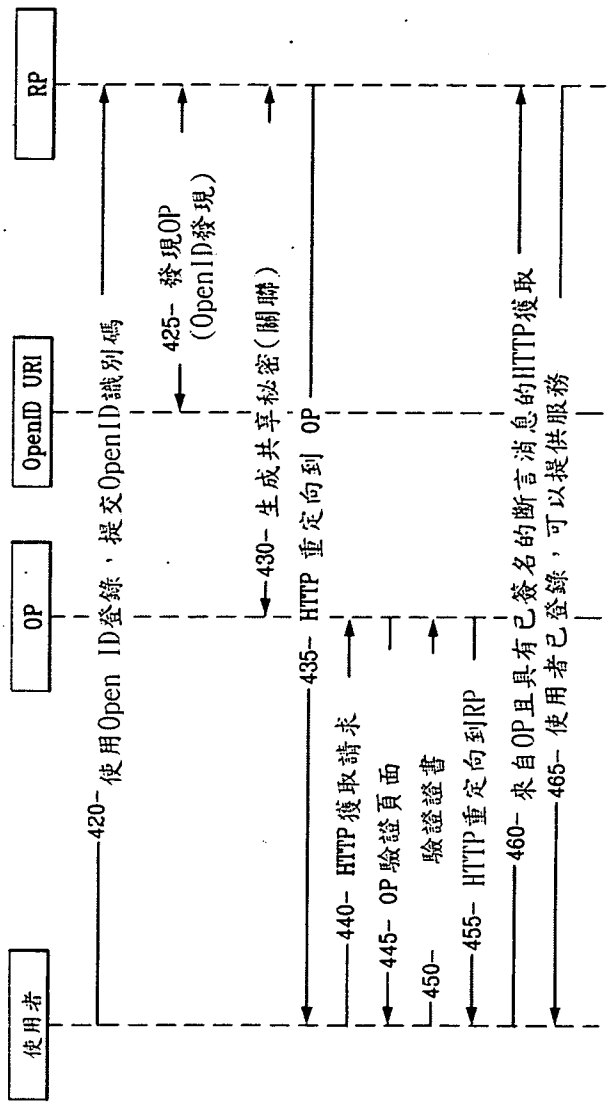

RP
375
關聯
385
驗證響應
MNO
驗證請求
380
UE
通過瀏覽器進行的通信
關聯控制和簽名密鑰(GBA)
390
OP

分離OP方案

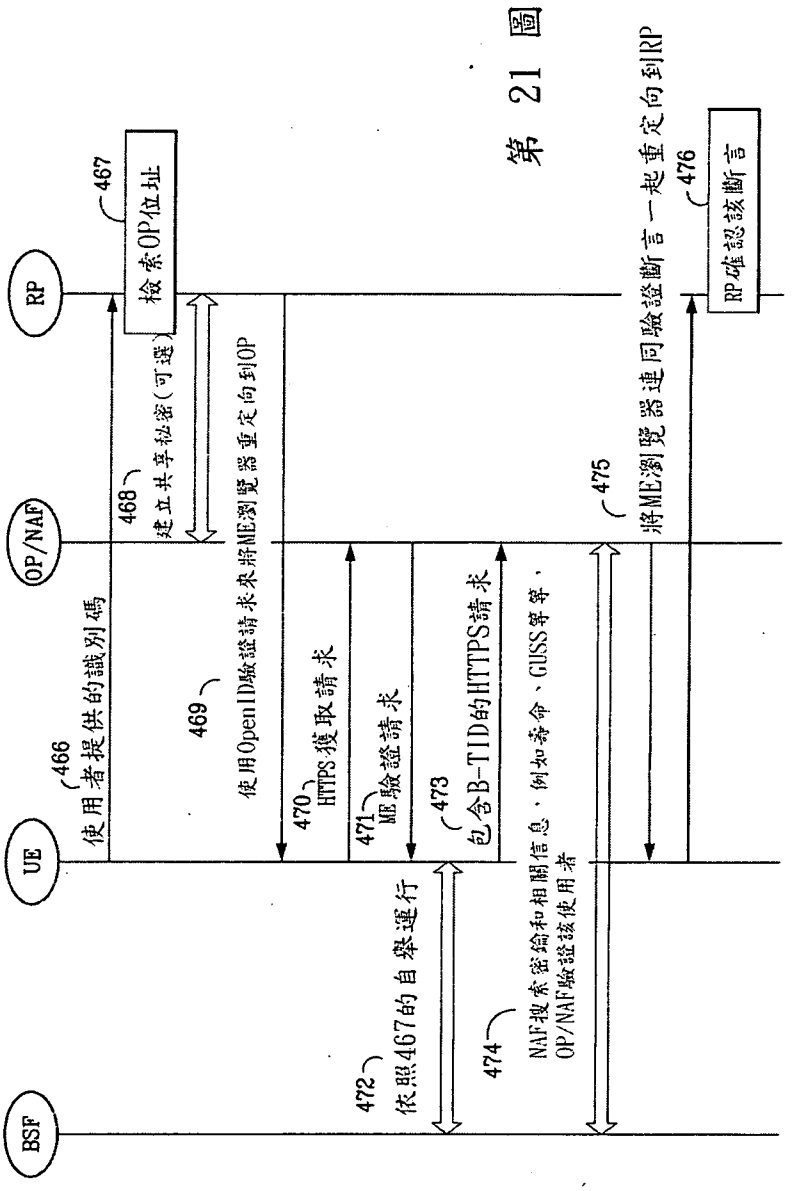
第 18 圖


BSF
NAF
OPsup
410
405
HTTPS/隧道
415
RP
OP
UICC
UE
400
本地介面
395
瀏覽器
遠程設備/PC

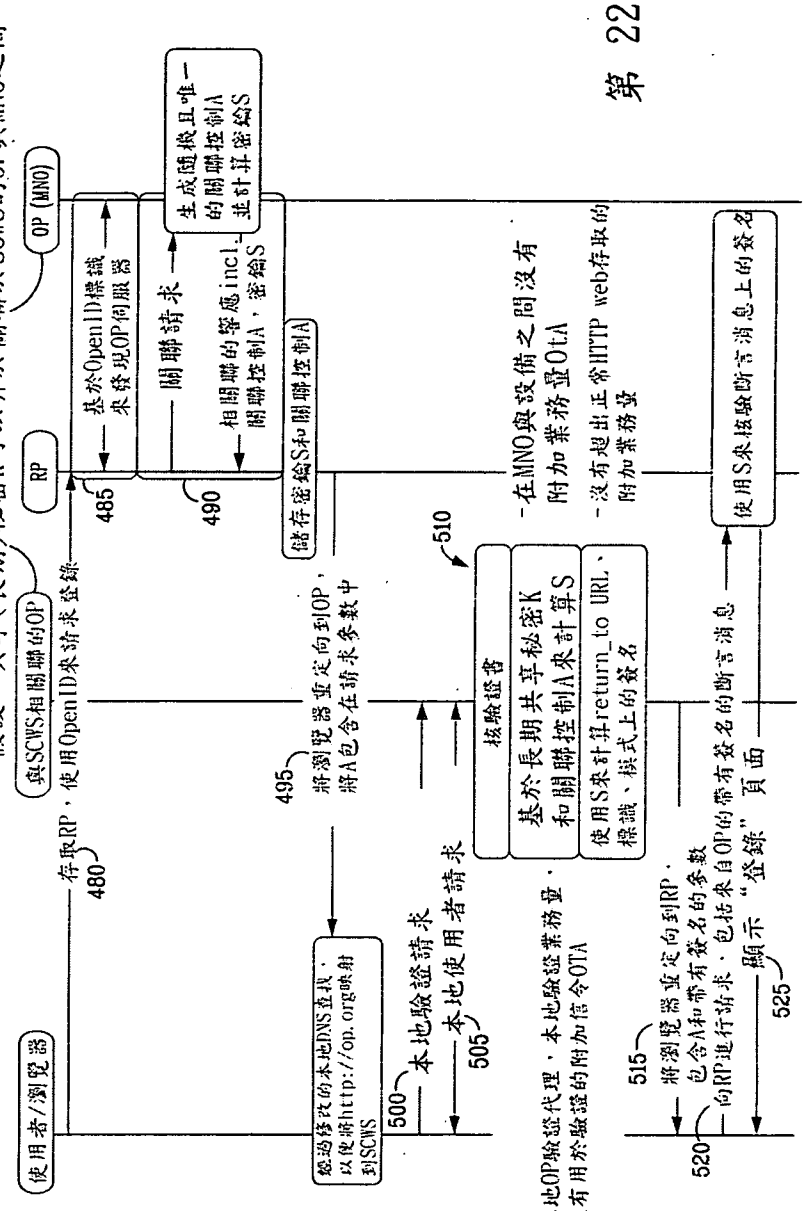
第 19 圖


使用者
OP
OpenID URI
RP
420- 使用Open ID登錄，提交OpenID識別碼
425- 發現OP
(OpenID發現)
430- 生成共享秘密(關聯)
435- HTTP 重定向到 OP
440- HTTP 獲取請求
445- OP 驗證頁面
450- 驗證證書
455- HTTP重定向到RP
460- 來自OP且具有已簽名的斷言消息的HTTP獲取
465- 使用者已登錄，可以提供服務

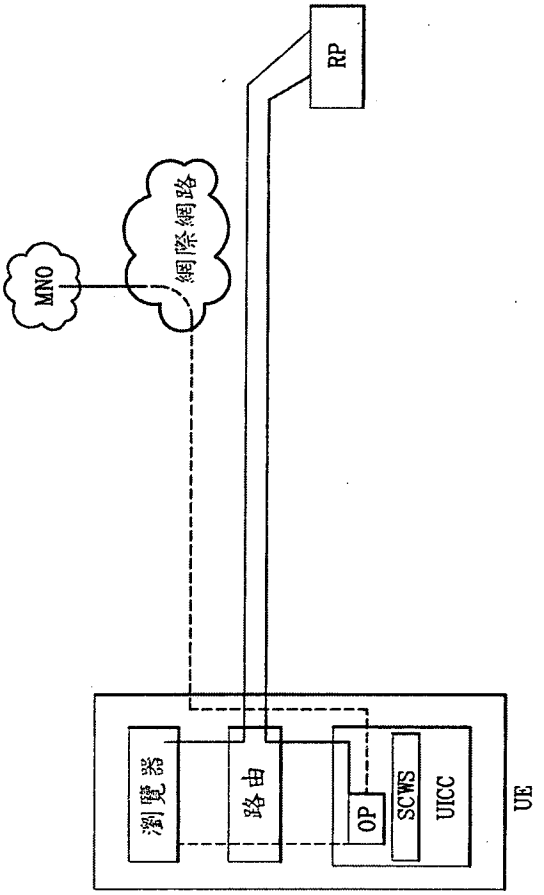
第 20 圖


RP
OP/NAF
UE
BSF
467
檢索OP位址
468
建立共享秘密(可選)
466
使用者提供的識別碼
469
使用OpenID驗證請求來將ME瀏覽器重定向到OP
470
HTTPS獲取請求
471
ME驗證請求
473
包含B-TID的HTTPS請求
472
依照467的自舉運行
474
NAF搜索密鑰和相關信息，例如壽命、GUSS等等，
OP/NAF驗證該使用者
475
將ME瀏覽器連同驗證斷言一起重定向到RP
476
RP確認該斷言

第 21 圖

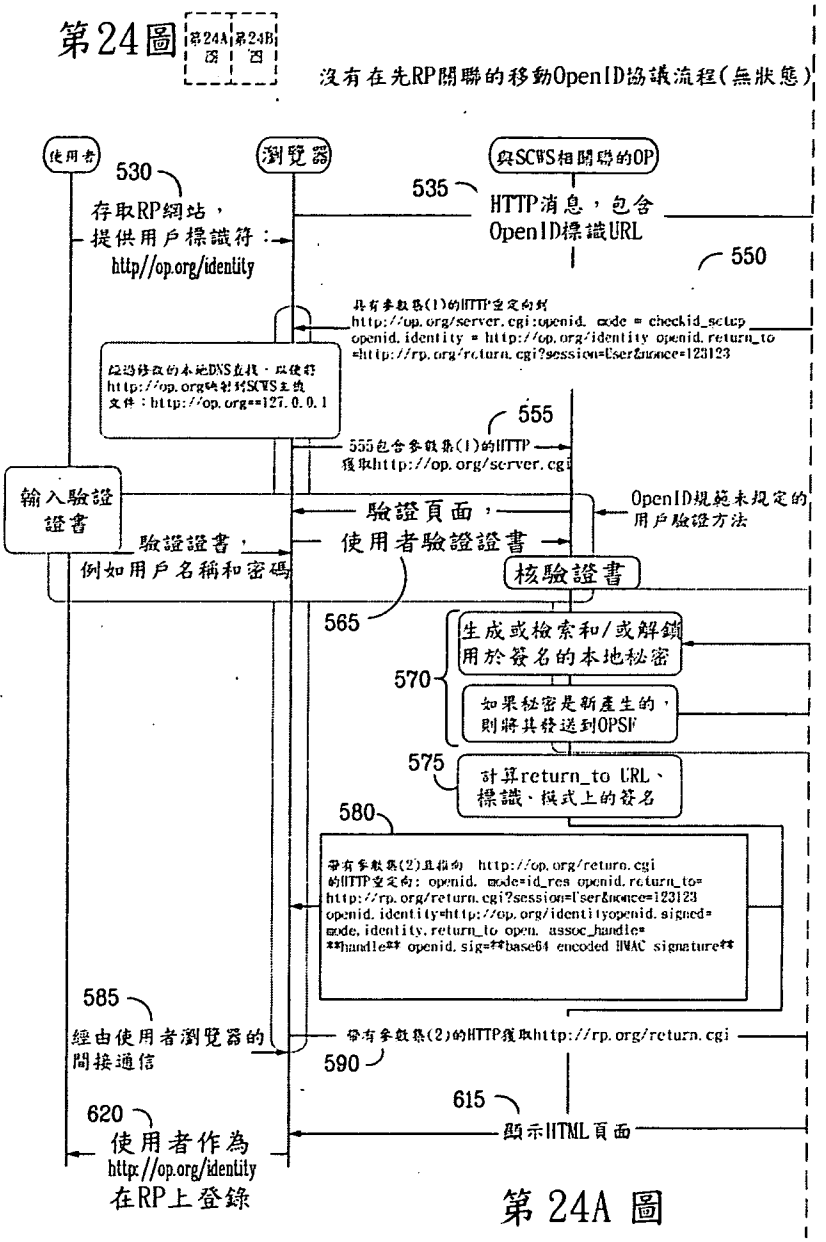

假設：共享(長期)私密K可以介於關聯於SCWS的OP與MNO之間
使用者/瀏覽器
與SCWS相關聯的OP
RP
OP (MNO)
存取RP，使用OpenID來請求登錄
480
基於OpenID標識來發現OP伺服器
485
關聯請求
490
生成隨機且唯一的關聯控制A並計算密鑰S
相關聯的答應incl. 關聯控制A，密鑰S
儲存密鑰S和關聯控制A
-在MNO與設備之間沒有附加業務豆OtA
-沒有超出正常HTTP web存取的附加業務豆
495
將瀏覽器重定向到OP，將A包含在請求參數中
經過修改的本地DNS查找，以使將http://op.org映射到SCWS
500
本地驗證請求
本地使用者請求
505
核驗證書
510
基於長期共享秘密K和關聯控制A來計算S
使用S來計算return_to URL、標識、模式上的簽名
本地OP驗證代理，本地驗證業務豆，沒有用於驗證的附加信令OTA
515
將瀏覽器重定向到RP，包含A和帶有簽名的參數
520
向RP進行請求，包括來自OP的帶有簽名的斷言消息
使用S來核驗斷言消息上的簽名
525
顯示“登錄”頁面

第 22 圖

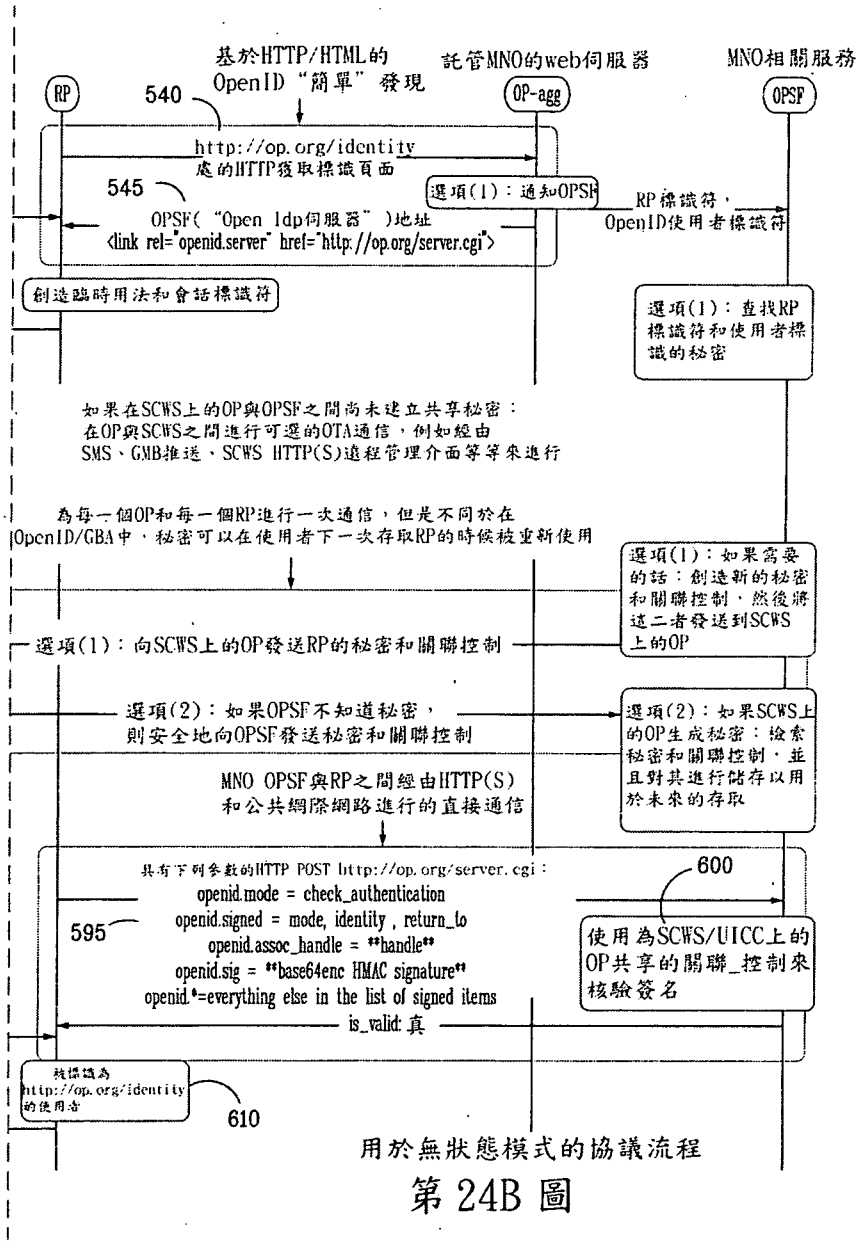


第 23 圖

第24圖 第24A圖 第24B圖

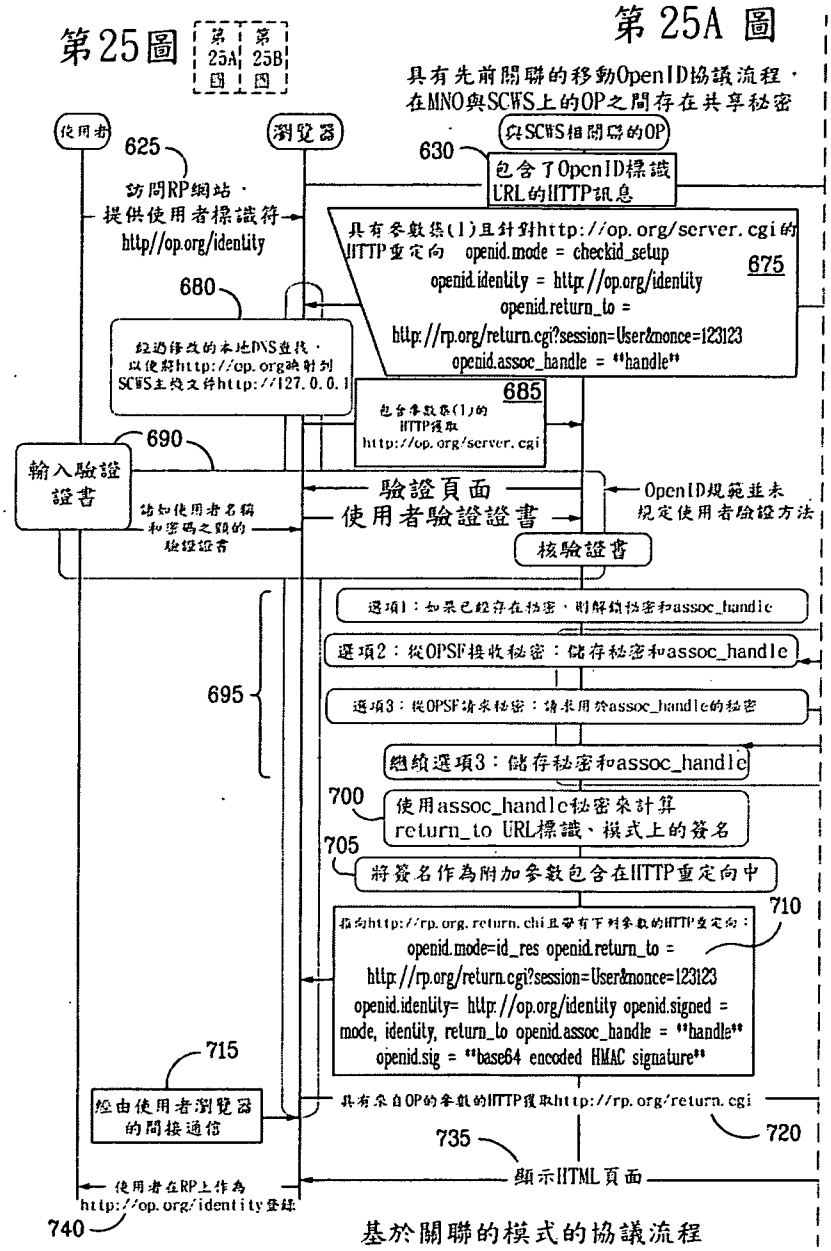


第 24A 圖

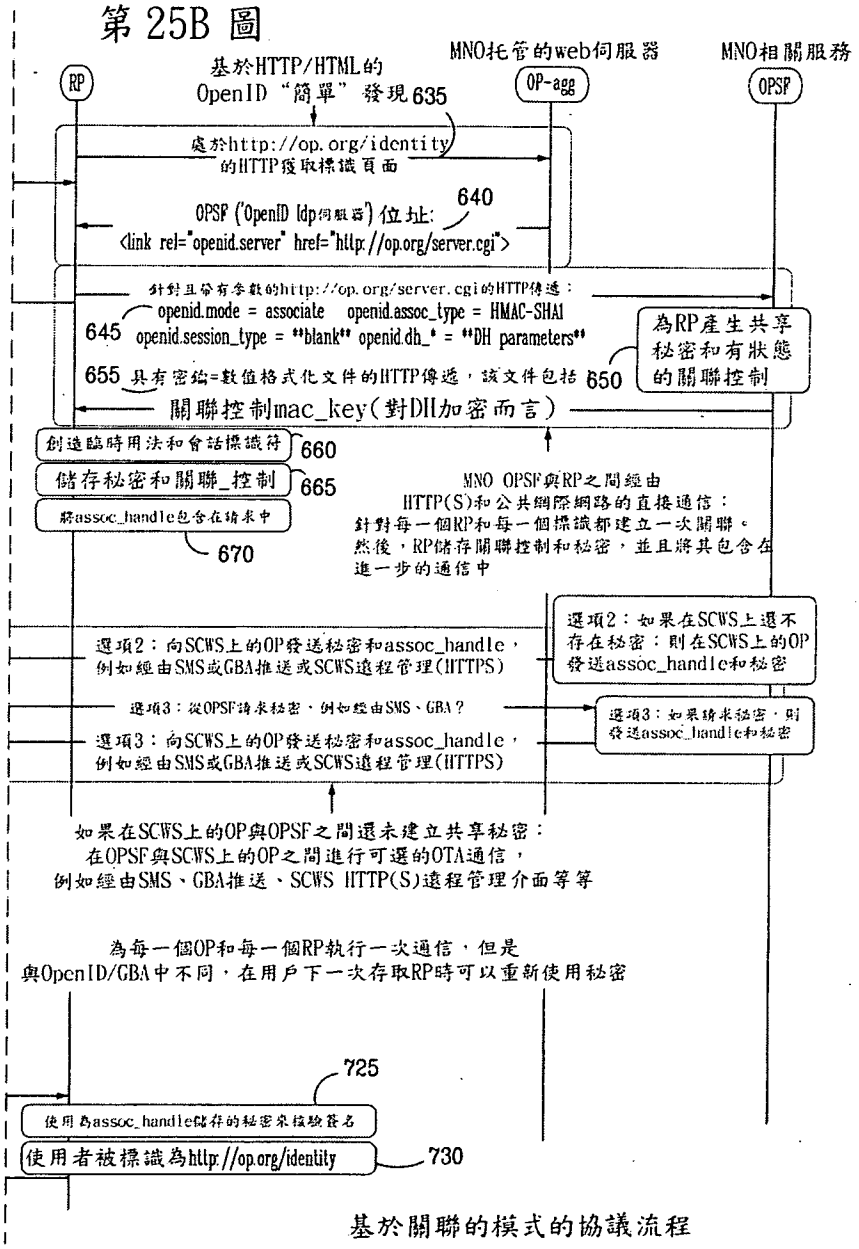

基於HTTP/HTML的
OpenID "簡單" 發現
託管MNO的web伺服器
MNO相關服務
RP
OP-agg
OPSF
540
http://op.org/identity
處的HTTP獲取標識頁面
545
選項(1)：通知OPSF
RP標識符，
OpenID使用者標識符
OPSF("Open Idp伺服器")地址
<link rel="openid.server" href="http://op.org/server.cgi">
創造臨時用法和會話標識符
選項(1)：查找RP
標識符和使用者標
識的秘密
如果在SCWS上的OP與OPSF之間尚未建立共享秘密：
在OP與SCWS之間進行可選的OTA通信，例如經由
SMS、GMB推送、SCWS HTTP(S)遠程管理介面等等來進行
為每一個OP和每一個RP進行一次通信，但是不同於在
OpenID/GBA中，秘密可以在使用者下一次存取RP的時候被重新使用
選項(1)：如果需要
的話：創造新的秘密
和關聯控制，然後將
這二者發送到SCWS
上的OP
選項(1)：向SCWS上的OP發送RP的秘密和關聯控制
選項(2)：如果OPSF不知道秘密，
則安全地向OPSF發送秘密和關聯控制
選項(2)：如果SCWS上
的OP生成秘密：檢索
秘密和關聯控制，並
且對其進行儲存以用
於未來的存取
MNO OPSF與RP之間經由HTTP(S)
和公共網際網路進行的直接通信
具有下列參數的HTTP POST http://op.org/server.cgi：
openid.mode = check_authentication
openid.signed = mode, identity , return_to
openid.assoc_handle = **handle**
openid.sig = **base64enc HMAC signature**
openid.*=everything else in the list of signed items
600
595
使用為SCWS/UICC上的
OP共享的關聯_控制來
核驗簽名
is_valid:真
610
用於無狀態模式的協議流程

第 24B 圖

第25圖 (第25A圖 第25B圖)

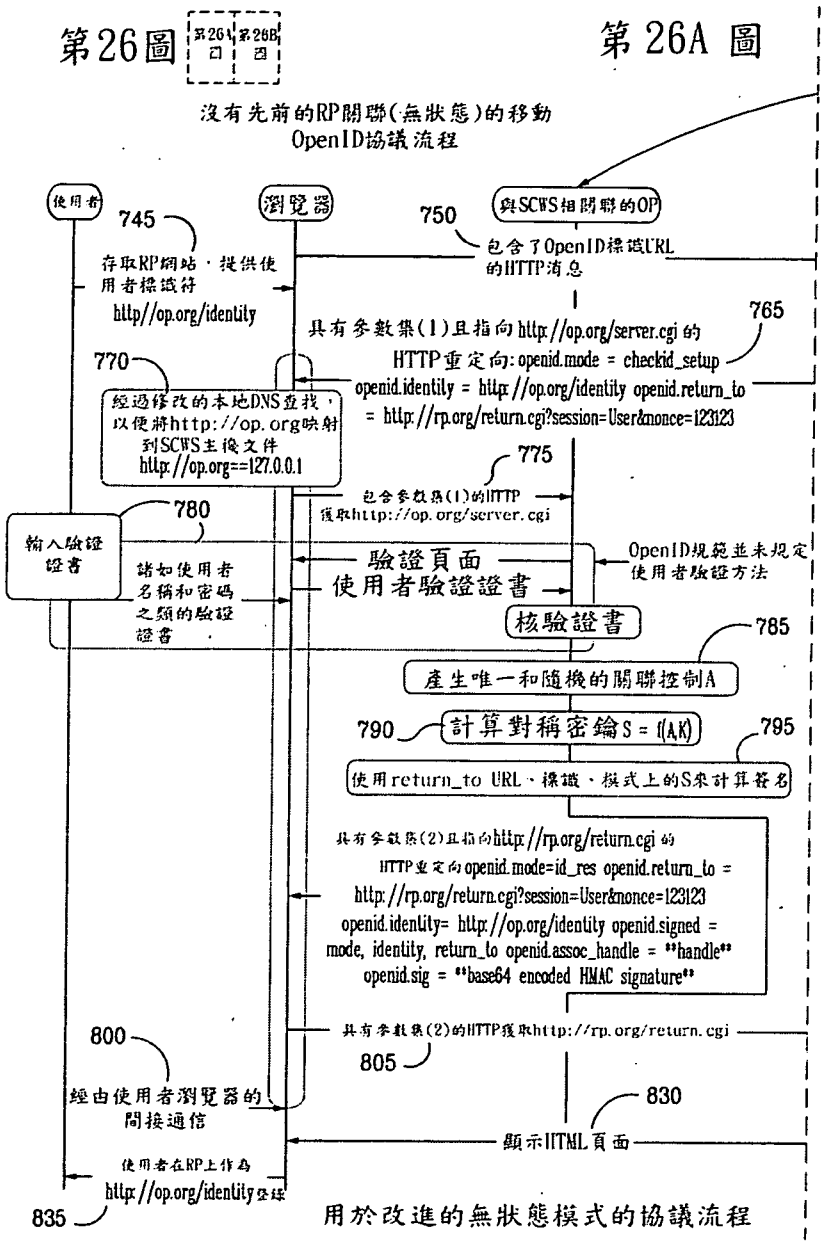


第 25B 圖

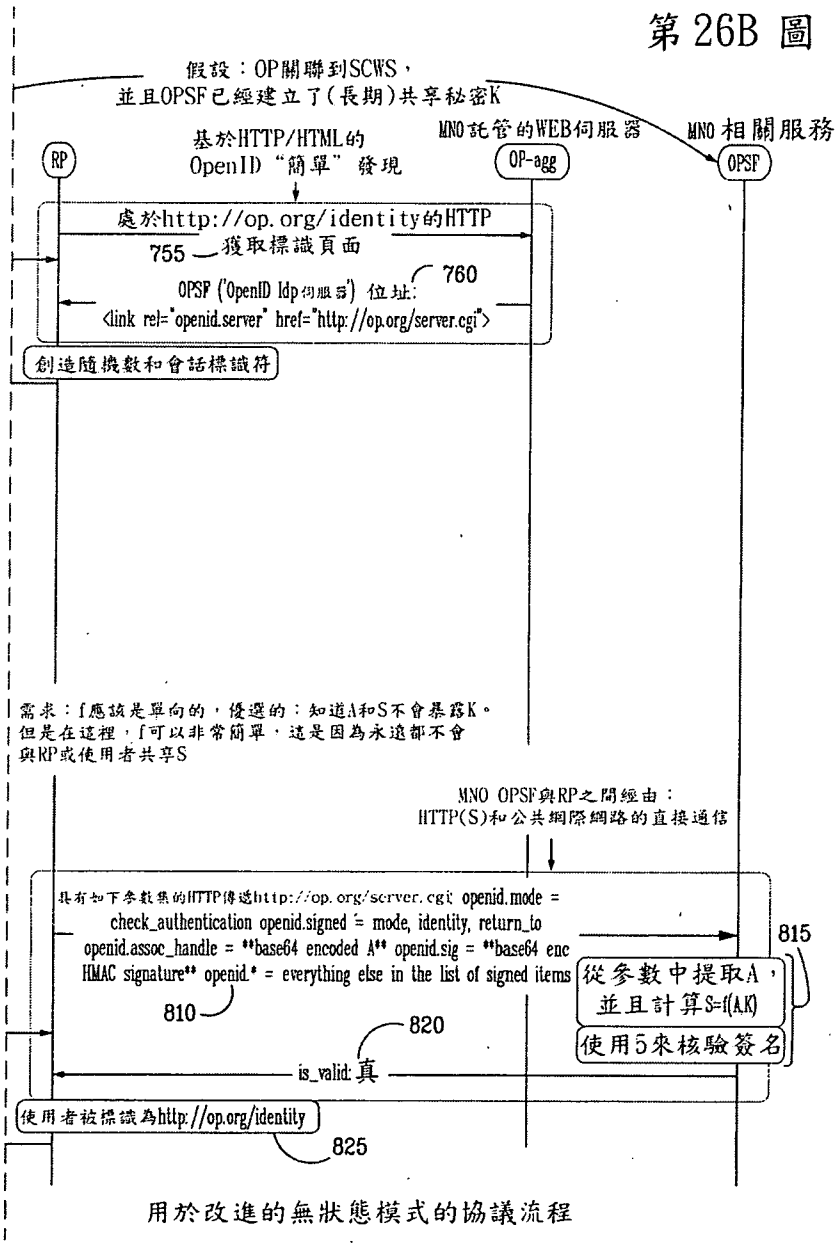


基於關聯的模式的協議流程

第26圖 第26A圖 第26B圖



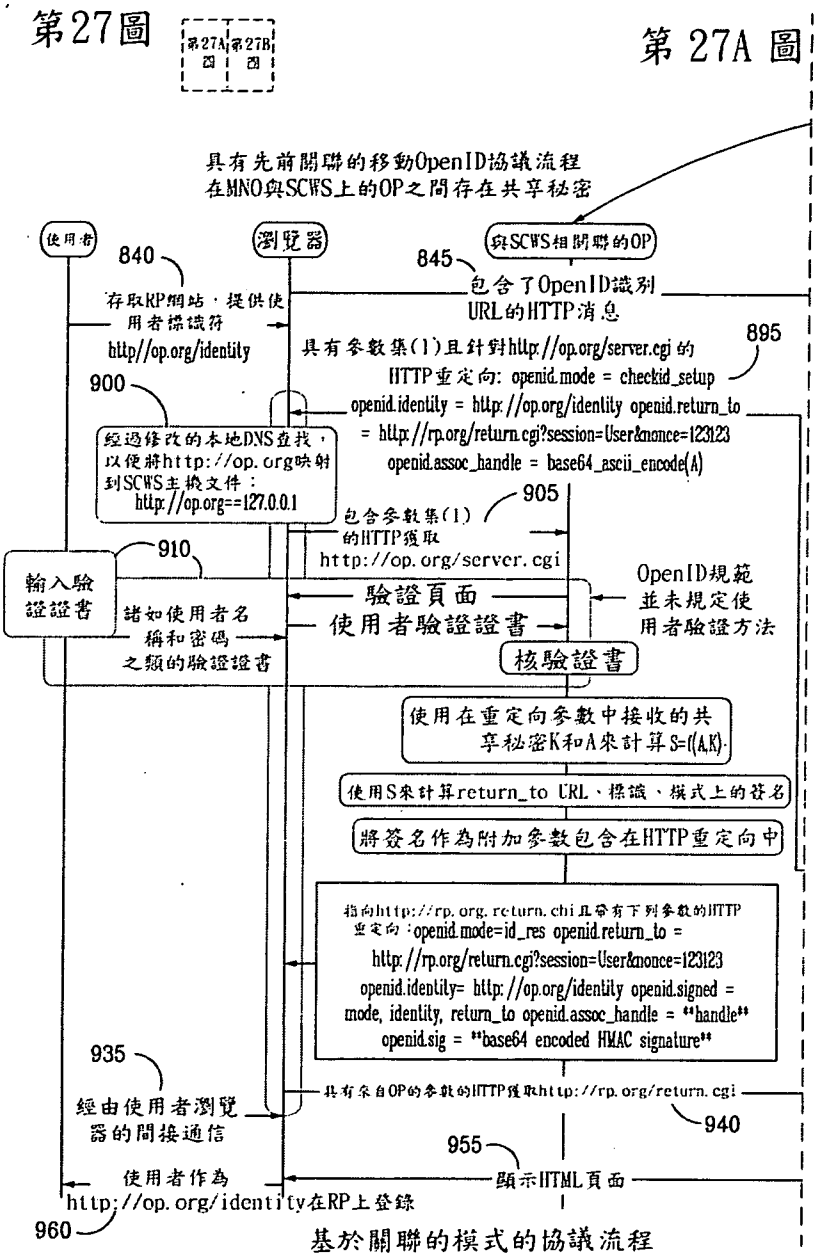
第 26B 圖



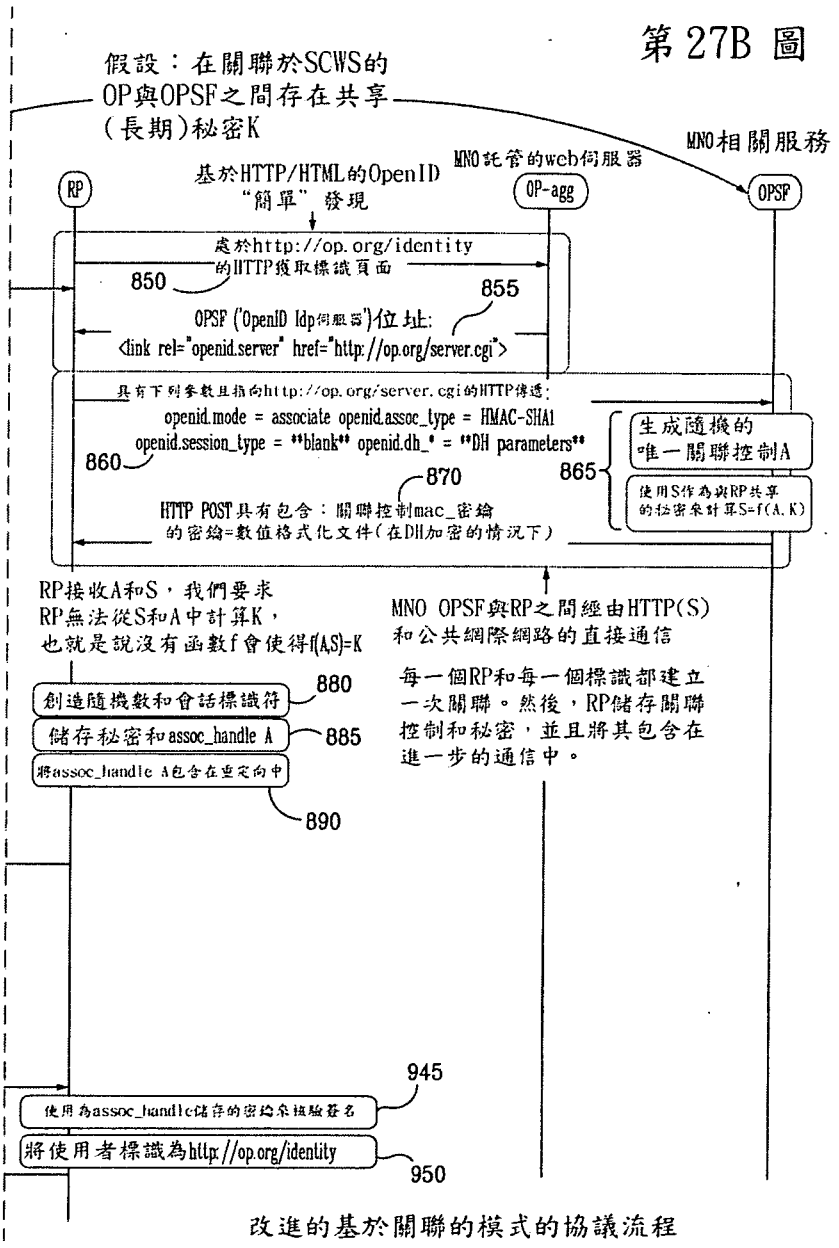
用於改進的無狀態模式的協議流程

第27圖 第27A圖 第27B圖

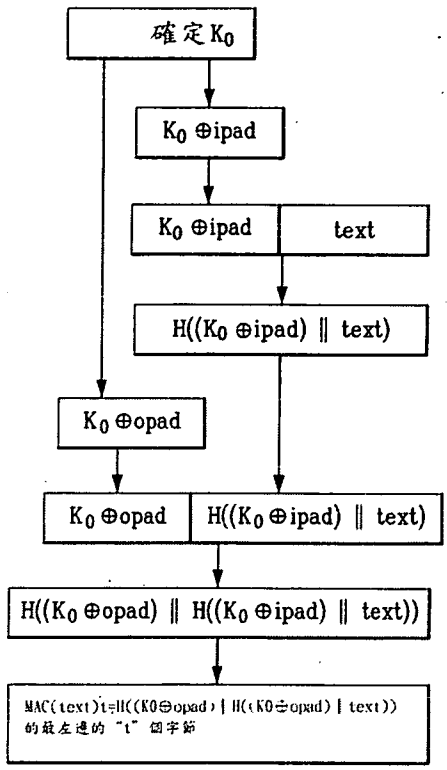
第 27A 圖



第 27B 圖

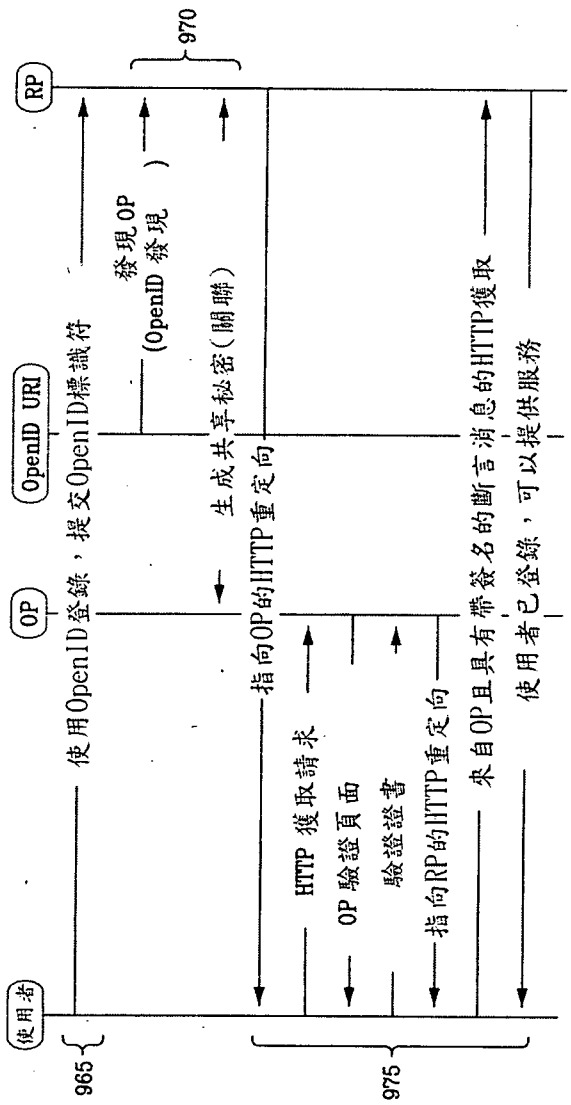


改進的基於關聯的模式的協議流程

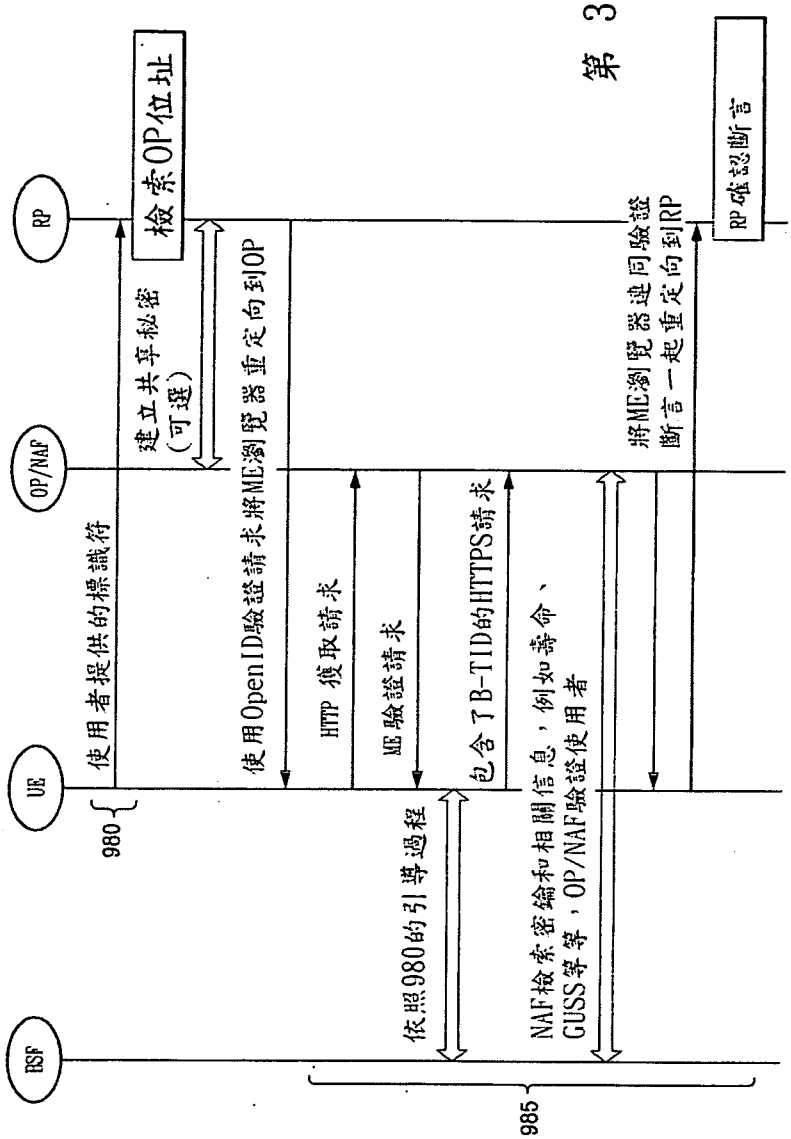

確定 K_0
$K_0 \oplus ipad$
$K_0 \oplus ipad$ | text
$H((K_0 \oplus ipad) \| text)$
$K_0 \oplus opad$
$K_0 \oplus opad$ | $H((K_0 \oplus ipad) \| text)$
$H((K_0 \oplus opad) \| H((K_0 \oplus ipad) \| text))$
MAC(text)t=H((K0⊕opad)‖H((K0⊕opad)‖text))
的最左邊的 "t" 個字節

HMAC 結構

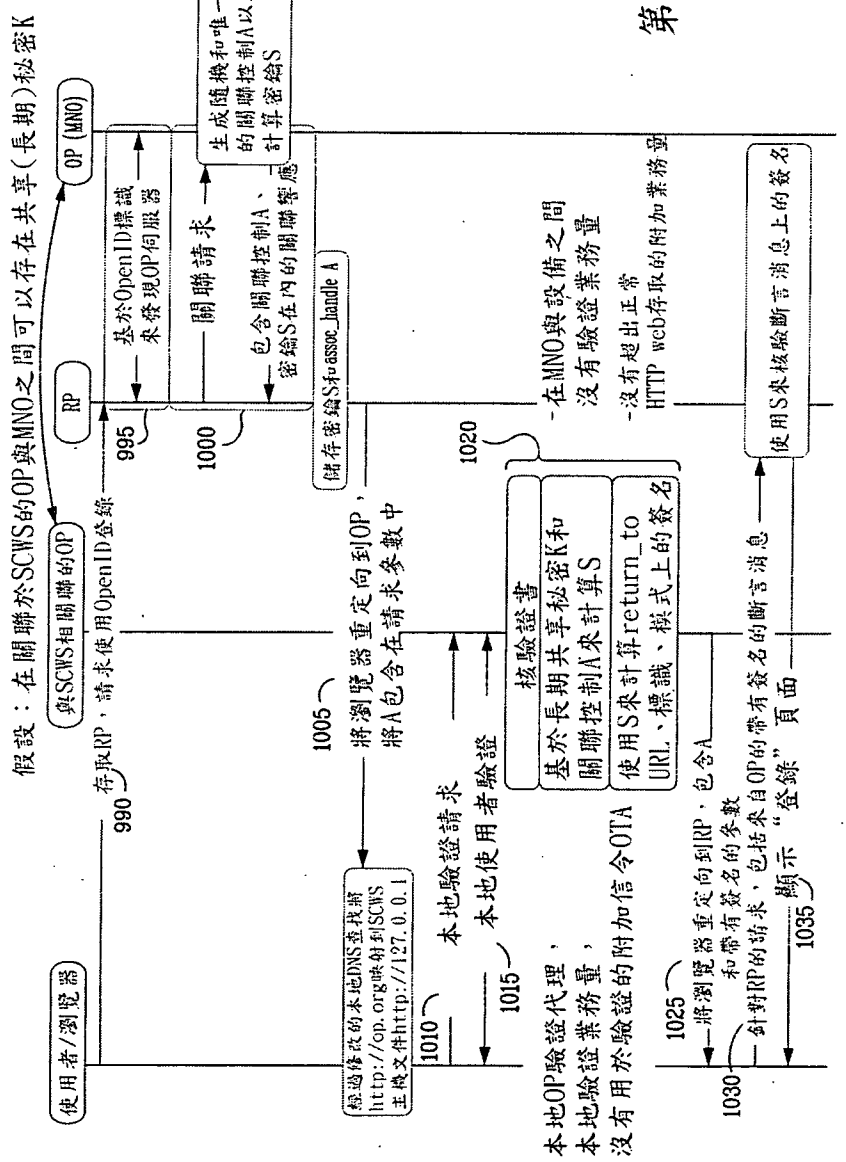
第 28 圖


使用者
OP
OpenID URI
RP
965
975
970
使用OpenID登錄，提交OpenID標識符
指向OP的HTTP重定向
HTTP 獲取請求
OP 驗證頁面
驗證證書
指向RP的HTTP重定向
來自OP且具有帶簽名的斷言消息的HTTP獲取
使用者已登錄，可以提供服務
發現OP
(OpenID 發現)
生成共享秘密(關聯)

第 29 圖


RP
OP/NAF
UE
BSF
檢索OP位址
建立共享秘密
(可選)
使用者提供的標識符
使用OpenID驗證請求將ME瀏覽器重定向到OP
HTTP 獲取請求
BDA驗證請求
包含了B-TID的HTTPS請求
將ME瀏覽器連同驗證
斷言一起重定向到RP
RP確認斷言
980
依照980的引導過程
NAF檢索密鑰和相關信息，例如壽命、
GUSS等等，OP/NAF驗證使用者
985

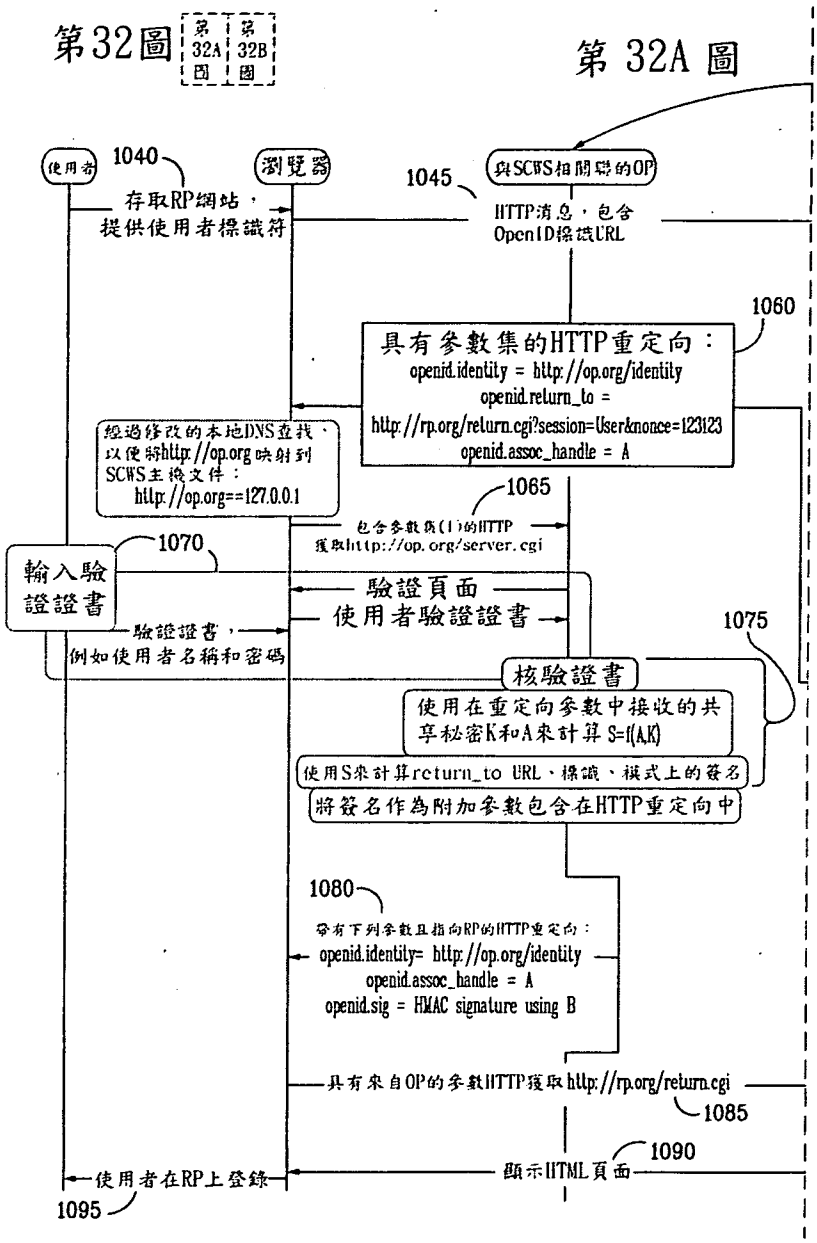
第 30 圖


假設：在關聯於SCWS的OP與MNO之間可以存在共享(長期)秘密K
使用者/瀏覽器
與SCWS相關聯的OP
RP
OP (MNO)
990
存取RP，請求使用OpenID登錄
995
基於OpenID標識來發現OP伺服器
1000
關聯請求
生成隨機和唯一的關聯控制A以及計算密鑰S
包含關聯控制A、密鑰S在內的關聯響應
儲存密鑰S和assoc_handle A
1005
將瀏覽器重定向到OP，將A包含在請求參數中
經過修改的本地DNS查找將http://op.org映射到SCWS主機文件http://127.0.0.1
1010
本地驗證請求
1015
本地使用者驗證
1020
-在MNO與設備之間沒有驗證業務量
-沒有超出正常HTTP web存取的附加業務量
核驗證書
基於長期共享秘密K和關聯控制A來計算S
使用S來計算return_to URL、標識、模式上的簽名
本地OP驗證代理，本地驗證業務量，沒有用於驗證的附加信令OTA
1025
將瀏覽器重定向到RP，包含A和帶有簽名的參數
1030
針對RP的請求，包括來自OP的帶有簽名的斷言消息
使用S來核驗斷言消息上的簽名
1035
顯示“登錄”頁面

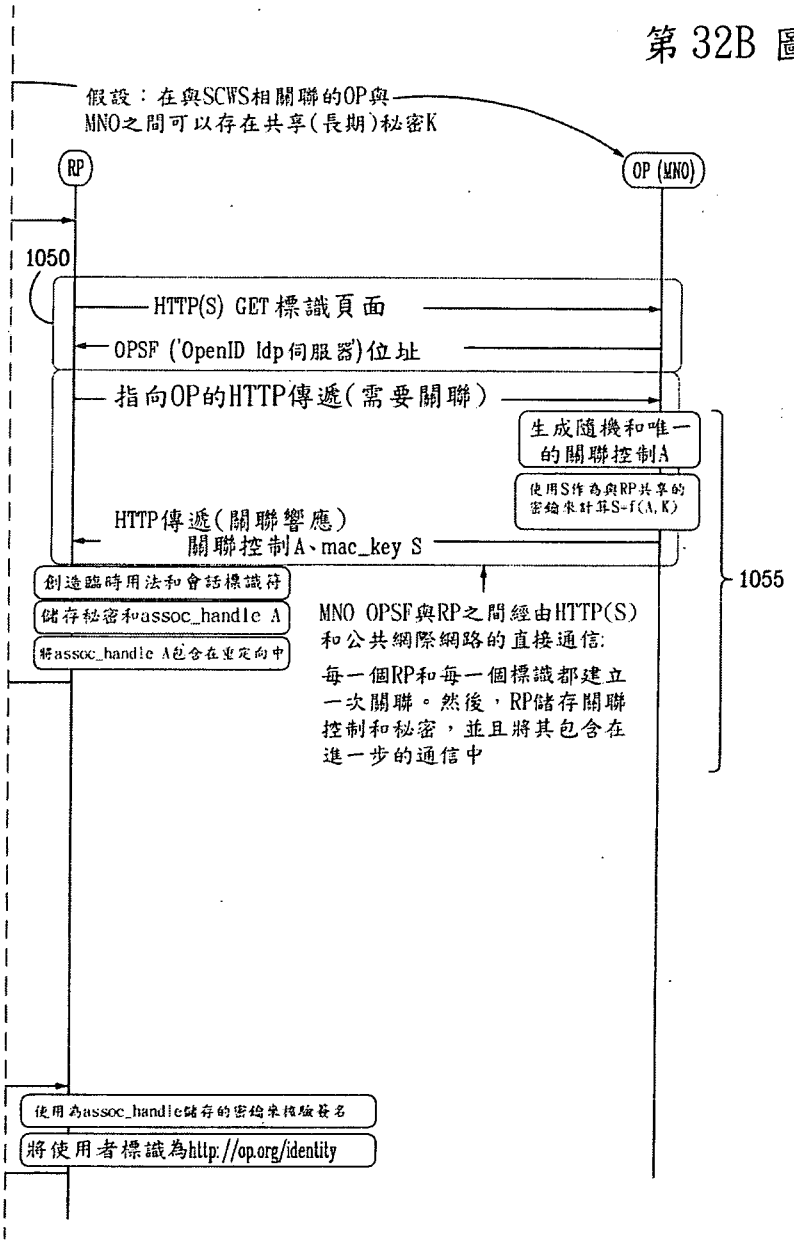
第 31 圖

第32圖 第32A圖 第32B圖

第 32A 圖

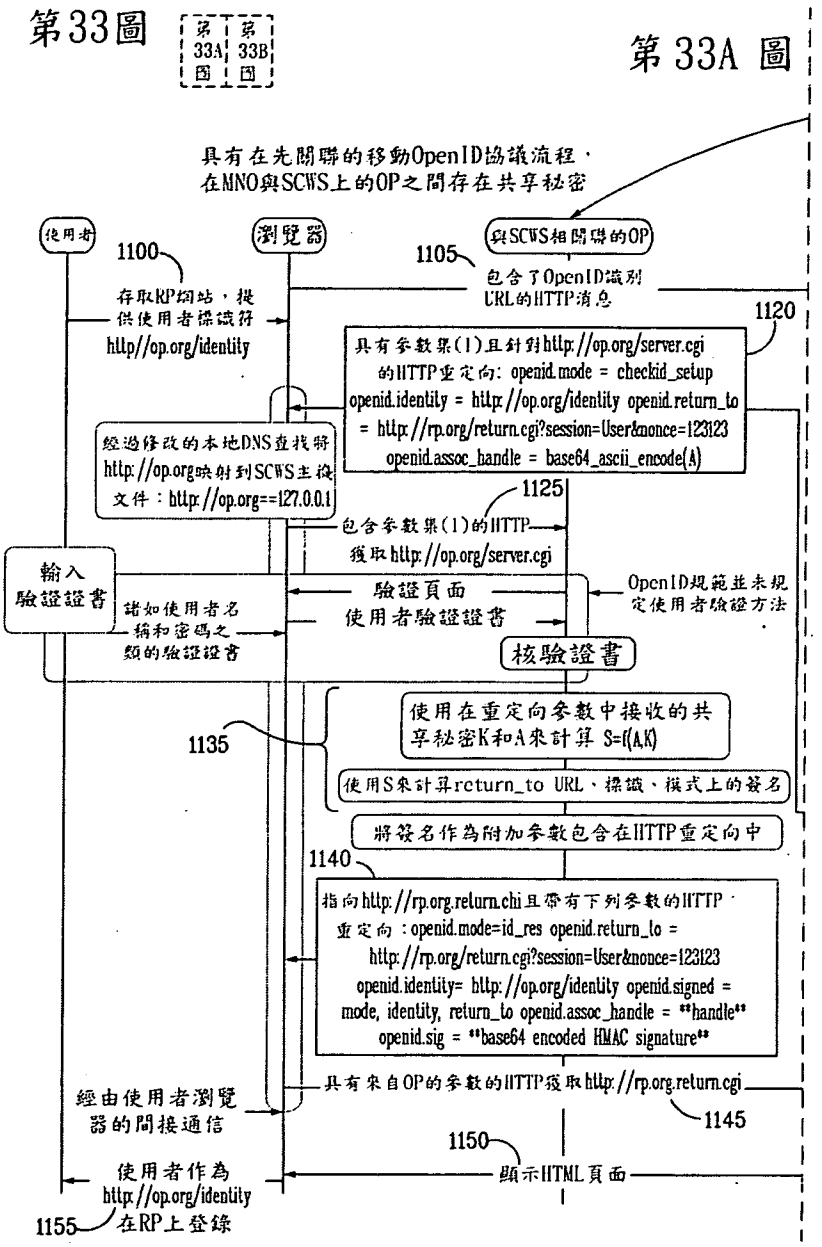


第 32B 圖

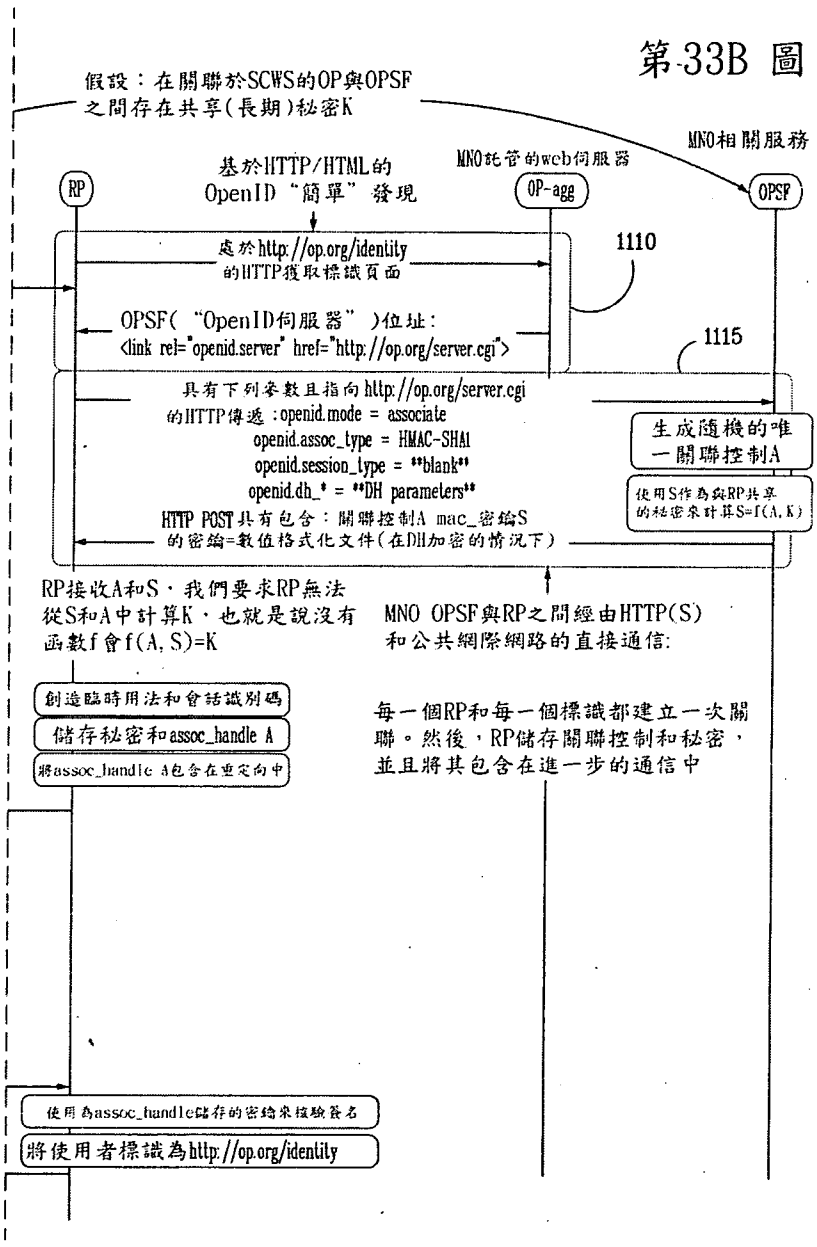

假設：在與SCWS相關聯的OP與MNO之間可以存在共享(長期)秘密K
RP
OP (MNO)
1050
HTTP(S) GET 標識頁面
OPSF ('OpenID Idp伺服器')位址
指向OP的HTTP傳遞(需要關聯)
生成隨機和唯一的關聯控制A
使用S作為與RP共享的密鑰來計算S-f(A,K)
HTTP傳遞(關聯響應)
關聯控制A、mac_key S
創造臨時用法和會話標識符
儲存秘密和assoc_handle A
將assoc_handle A包含在重定向中
MNO OPSF與RP之間經由HTTP(S)和公共網際網路的直接通信:
每一個RP和每一個標識都建立一次關聯。然後，RP儲存關聯控制和秘密，並且將其包含在進一步的通信中
1055
使用為assoc_handle儲存的密鑰來檢驗簽名
將使用者標識為http://op.org/identity

第33圖 第33A圖 第33B圖

第 33A 圖

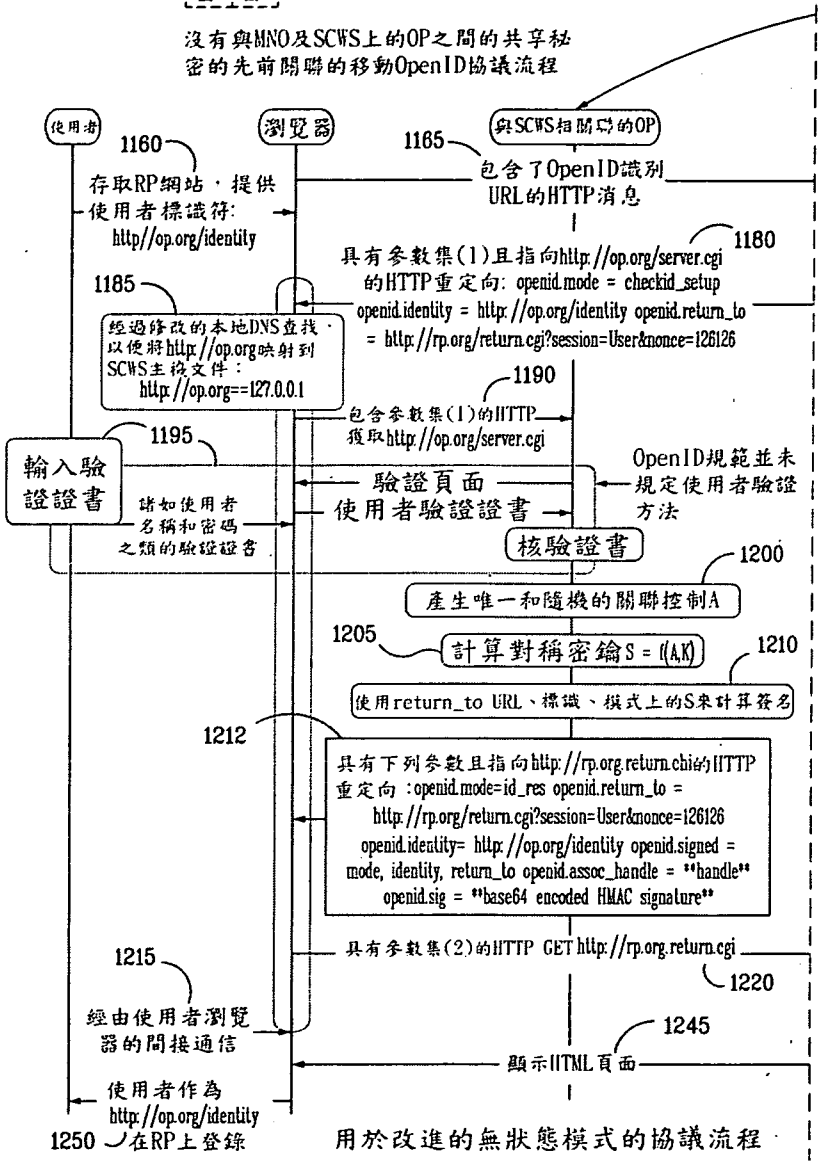


第33B 圖

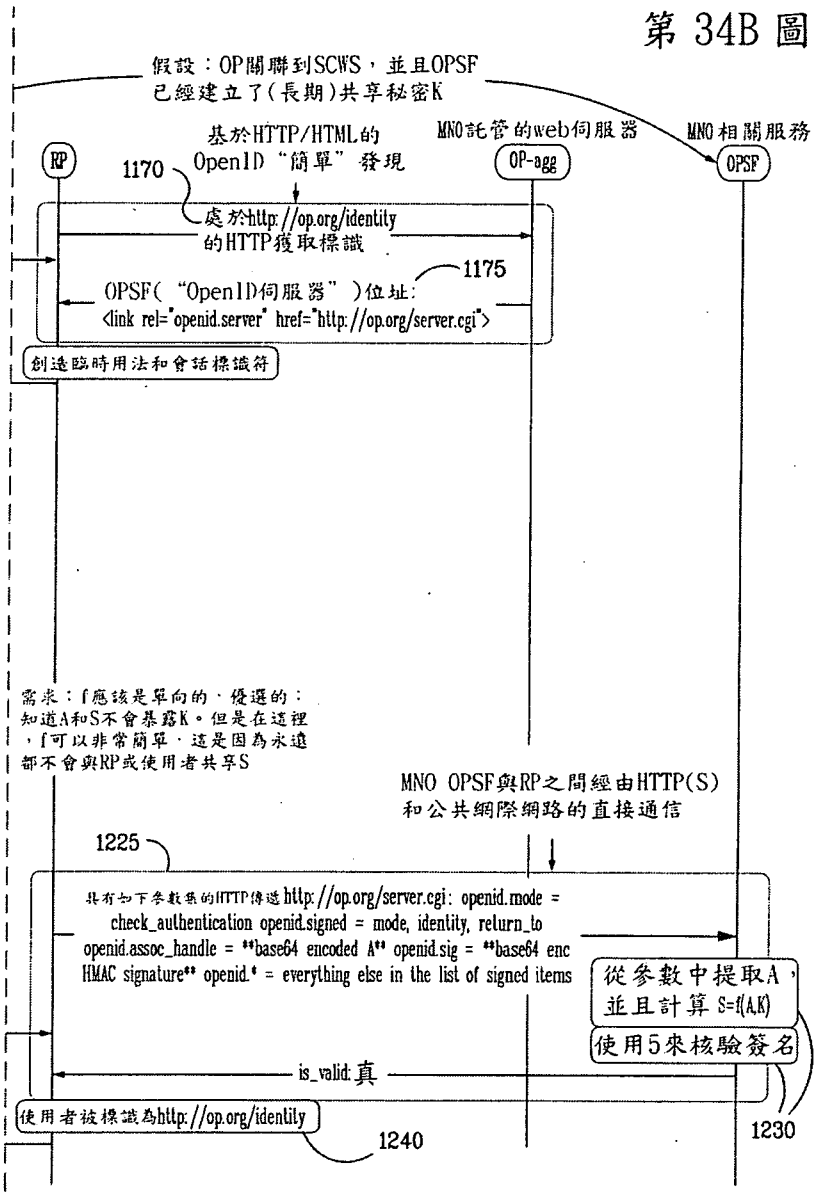

假設：在關聯於SCWS的OP與OPSF
之間存在共享(長期)秘密K
MNO相關服務
基於HTTP/HTML的
OpenID "簡單" 發現
MNO託管的web伺服器
RP
OP-agg
OPSF
處於http://op.org/identity
的HTTP獲取標識頁面
1110
OPSF("OpenID伺服器")位址:
<link rel="openid.server" href="http://op.org/server.cgi">
1115
具有下列參數且指向 http://op.org/server.cgi
的HTTP傳遞 :openid.mode = associate
openid.assoc_type = HMAC-SHA1
openid.session_type = "blank"
openid.dh_* = "DH parameters"
生成隨機的唯
一關聯控制A
使用S作為與RP共享
的秘密來計算S=f(A, K)
HTTP POST具有包含：關聯控制A mac_密鑰S
的密鑰=數值格式化文件(在DH加密的情況下)
RP接收A和S，我們要求RP無法
從S和A中計算K，也就是說沒有
函數f會f(A, S)=K
MNO OPSF與RP之間經由HTTP(S)
和公共網際網路的直接通信:
創造臨時用法和會話識別碼
儲存秘密和assoc_handle A
將assoc_handle A包含在重定向中
每一個RP和每一個標識都建立一次關
聯。然後，RP儲存關聯控制和秘密，
並且將其包含在進一步的通信中
使用為assoc_handle儲存的密鑰來檢驗簽名
將使用者標識為http://op.org/identity

第34圖 第34A圖 第34B圖

第 34A 圖

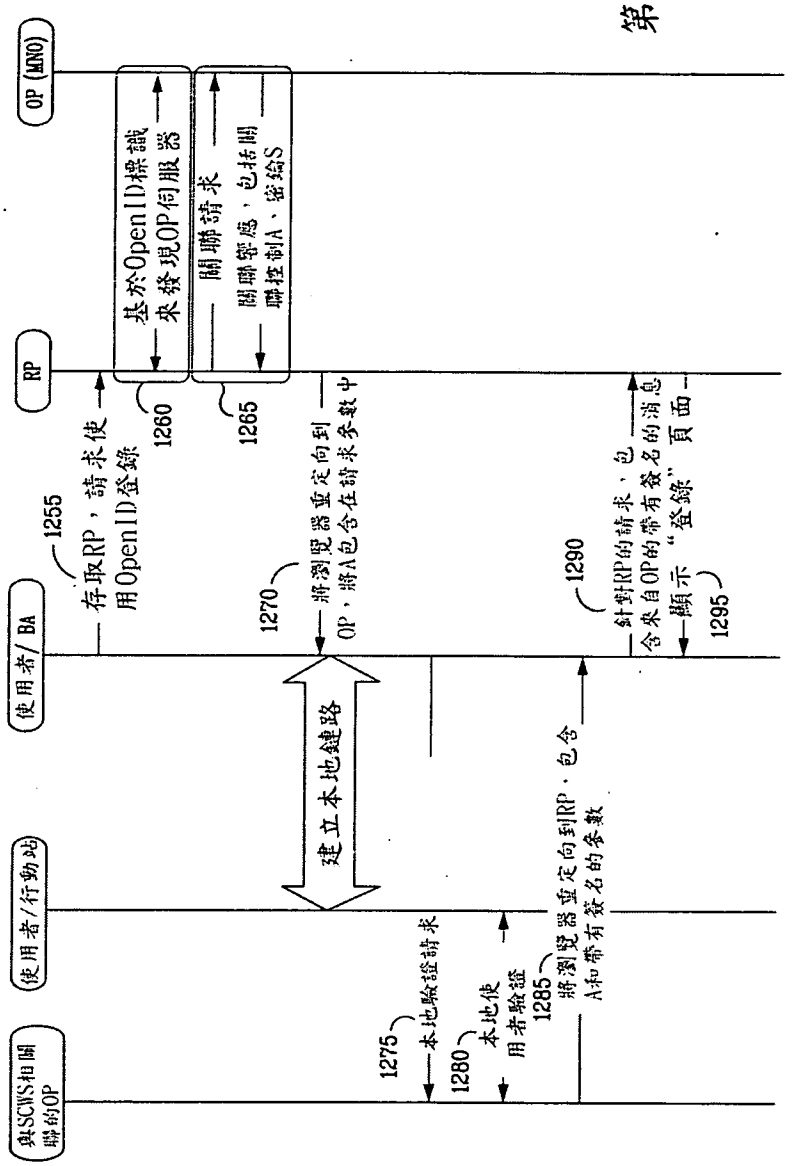


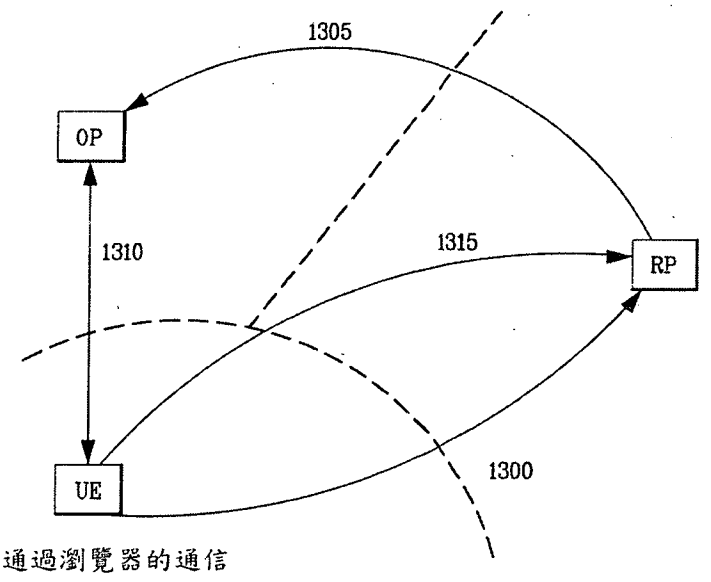
第 34B 圖



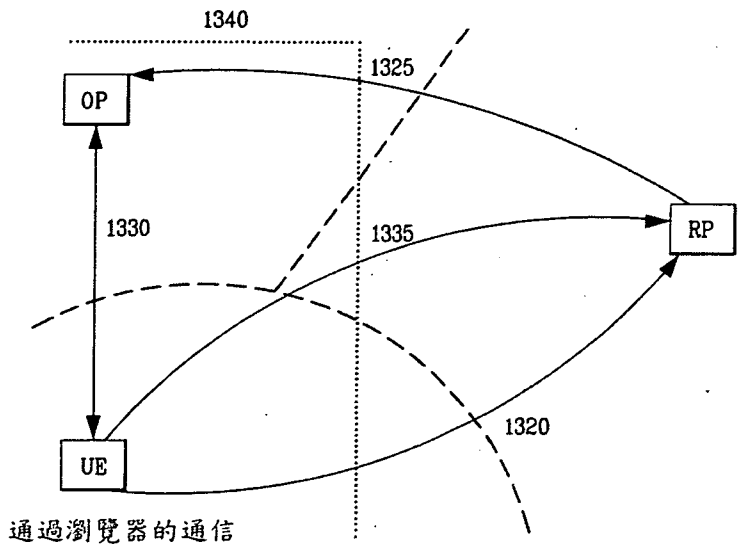
用於改進的無狀態模式的協議流程

第 35 圖

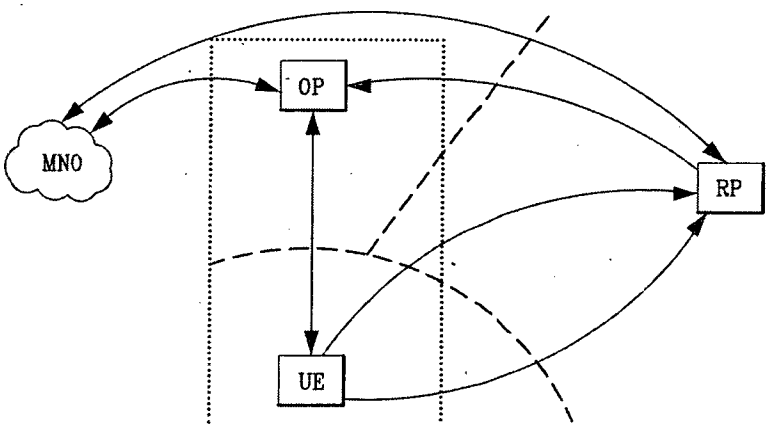

OP (MNO)
RP
使用者/ BA
使用者/行動站
與SCWS相關聯的OP
基於OpenID標識來發現OP伺服器
關聯請求
關聯管理，包括關聯控制A、密鑰S
1260
1265
1255
存取RP，請求使用OpenID登錄
1270
將瀏覽器重定向到OP，將A包含在請求參數中
1290
針對RP的請求，包含來自OP的帶有簽名的消息
顯示“登錄”頁面
1295
建立本地鏈路
1275
本地驗證請求
1280
本地使用者驗證
1285
將瀏覽器重定向到RP，包含A和帶有簽名的參數



第 36 圖

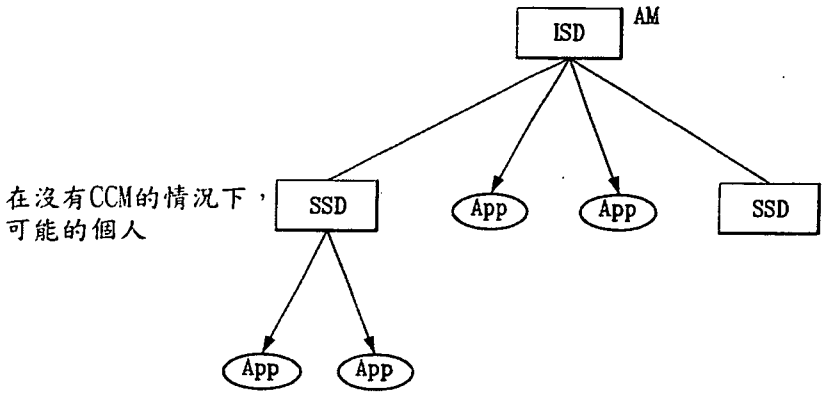


第 37 圖

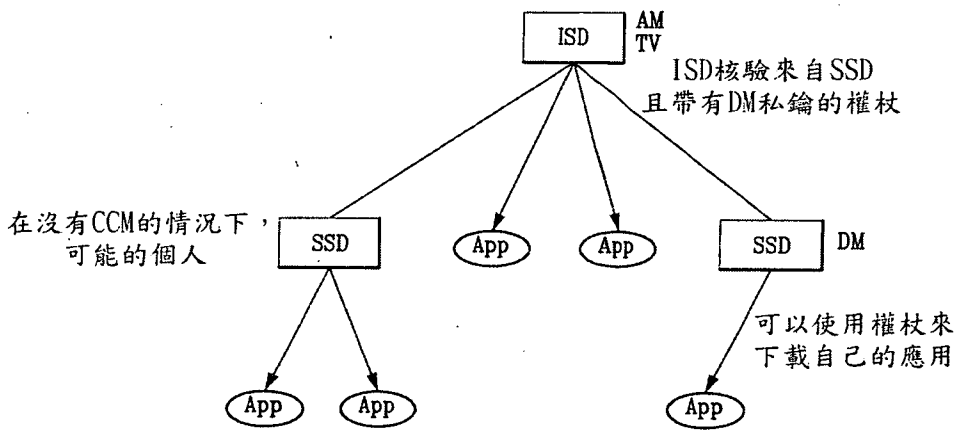


通過瀏覽器的通信

第 38 圖

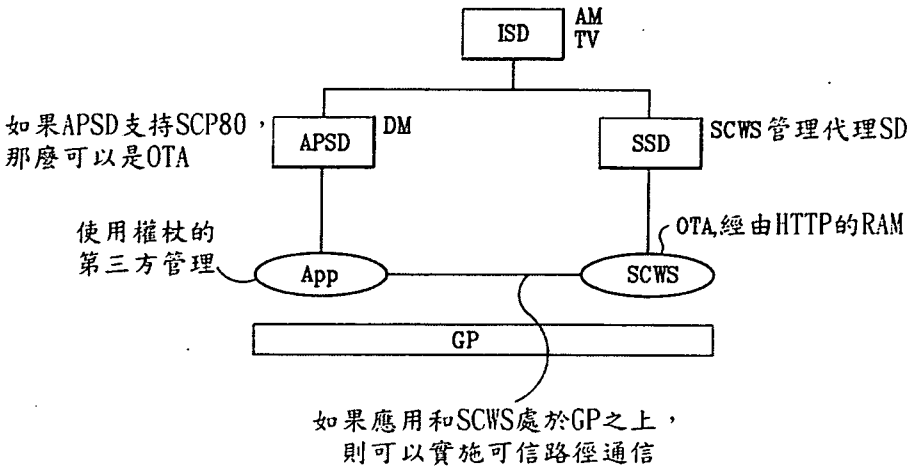


第 39 圖

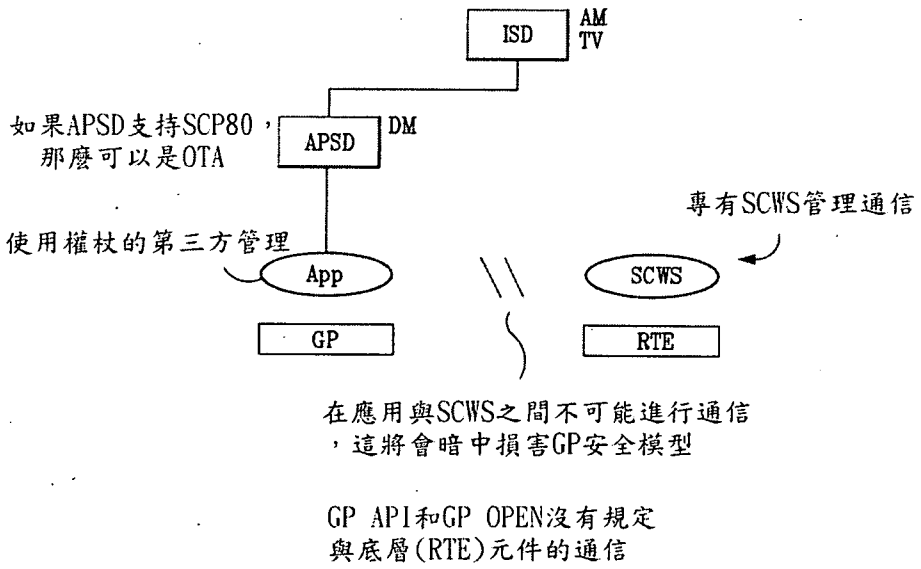


基於權杖的DM

第 40 圖


ISD
AM
TV
如果APSD支持SCP80，
那麼可以是OTA
APSD
DM
SSD
SCWS管理代理SD
使用權杖的
第三方管理
OTA,經由HTTP的RAM
App
SCWS
GP
如果應用和SCWS處於GP之上，
則可以實施可信路徑通信

第 41 圖


ISD
AM
TV
如果APSD支持SCP80，
那麼可以是OTA
APSD
DM
專有SCWS管理通信
使用權杖的第三方管理
App
SCWS
GP
RTE
在應用與SCWS之間不可能進行通信
，這將會暗中損害GP安全模型
GP API和GP OPEN沒有規定
與底層(RTE)元件的通信

第 42 圖