

發明專利說明書

(本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫)

※申請案號：94136526

(2006.01)

(2006.01)

※申請日期：94.10.18

※IPC 分類：H04L 9/28, H04L 29/06

一、發明名稱：(中文/英文)

用戶認證系統和方法

User Authentication System

二、申請人：(共1人)

姓名或名稱：(中文/英文)(簽章) ID：

美國博通公司/Broadcom Corporation

☐ 指定 為應受送達人

代表人：(中文/英文)(簽章) 狄·韓德森/Dee Henderson

住居所或營業所地址：(中文/英文)

美國加州爾灣市奧爾頓公園路 16215 號, 92618-7013

16215 Alton Parkway, Irvine, California USA, 92618-7013

國籍：(中文/英文) 美國/U.S.A.

電話/傳真/手機：

E-MAIL：

三、發明人：(共3人)

姓名：(中文/英文) ID：

1. 馬克·布林/Mark Buer

2. 埃德華·H·弗蘭克/Edward H. Frank

3. 納拜瑞簡·塞亞爵/Nambirajan Seshadri

國籍：(中文/英文)

1.2.3: 美國/U.S.A.

四、聲明事項：

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

☒ 申請前已向下列國家（地區）申請專利：

【格式請依：受理國家（地區）、申請日、申請案號 順序註記】

☒ 有主張專利法第二十七條第一項國際優先權：

1. 美國 2004 年 10 月 20 日 60/620,645
2. 美國 2005 年 08 月 05 日 11/197,815

☐ 無主張專利法第二十七條第一項國際優先權：

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號 順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料 【格式請依：寄存機構、日期、號碼 順序註記】

國外生物材料 【格式請依：寄存國家、機構、日期、號碼 順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

九、發明說明：

【發明所屬之技術領域】

本發明涉及資料通訊系統，更具體地，本發明涉及一種驗證一個或複數個用戶以使用通訊系統內一個或複數個設備的系統和方法。

【先前技術】

人們可以使用計算設備例如個人電腦和無線手持設備來存取多種服務。例如，用戶可對存儲或運行在計算設備上的資料或應用程式進行存取。此外，用戶還可以連接到資料網路，以存取遠端伺服器上的資料或應用程式。

某些情況下，一項服務只對授權用戶開放。例如，這種服務可以是對，例如金融資訊或個人資訊這樣的敏感資料的存取。此外，對一些服務的存取是需要付費的。

已有多種技術用於通過計算設備來實現對服務的安全存取。例如，用戶可能需要向提供服務的計算設備（“服務提供者”）出示某種形式的信用證明。在這裏，該信用證明可以用於指示一個特定用戶（或任何掌握該信用證明的人）是否可以對指定的服務進行存取。在某些應用中，信用證明可以採用用戶名和密碼的形式，這些用戶名和密碼由系統管理員提供給用戶和服務提供者。當用戶存取一項服務時，需要向服務提供者出示其用戶名和密碼。然後服務提供者將對這份信用證明進行檢驗，以確認該用戶是所請求服務的授權用戶。

在一個典型的資料網路中，對資料網路的存取只向那些正確的載入在該網路上的設備開放。作為這種載入的一部分，需要使用加密技

術來確保只有授權了的設備才可以連接到網路上。通常來說，加密技術可以包括一個或複數個加密、解密、認證、簽名和校驗過程。

例如，網路管理員可以在每台授權連接到網路上的設備上裝載一個或複數個加密密鑰（以下用“密鑰”表示）。該網路管理員還在連接到例如廣域網（“WAN”）上的網路接入設備（例如，路由器）上裝載相應的密鑰。當一台設備試圖存取網路時，網路接入設備將檢驗該設備是否裝載了正確的密鑰。一旦檢驗通過，網路接入設備將允許請求設備對網路進行存取。

在現實中，向用戶使用某種服務進行授權，以及將設備載入到網路上的過程可能會相對的繁瑣和耗時。如上所述，這些操作相對來說都是通過手動方式進行的。然而分散式計算服務存取正變得越來越普遍和可以支援存取。例如，無線計算網路和手持設備的增長使得用戶可以使用多種設備存取一個城市中的多種不同網路。因此，需要一種更高效的技術，使得用戶可以存取加密服務。

此外，傳統的用於輸入信用證明或向設備裝載密鑰的方法，在某些情況下將存在安全隱患。例如，當用戶使用計算設備存取加密服務的時候，首先需要將信用證明輸入到計算設備中。通常情況下，這步操作是通過使用例如鍵盤等輸入設備來完成的。隨後，該計算設備將這些信用證明發送給服務提供者，由該服務提供者來確認該用戶是否有權存取其所請求的服務。

這時，如果該計算設備被黑客控制，或者感染了電腦病毒，那麼非授權個人將有可能存取到這些信用證明。例如，一台個人電腦可以

使用可信計算模組 (trusted computing module, TPM) 來控制對特定加密服務的存取 (例如, 對加密資料檔案或加密網路的存取)。這裏, 在允許用戶存取這些服務之前, TPM 會要求其輸入密碼或其他信用證明。如果用戶使用鍵盤來輸入這些資訊, 那麼這些密碼可能在個人電腦內通過一條不安全路徑從鍵盤路由到 TPM。例如, 該鍵盤可能連接在一個 USB 埠上, 並且使用驅動程式來從 USB 匯流排向 TPM 傳輸資料, 該 TPM 可能, 例如連接到個人電腦的南橋上。然而, 黑客或病毒可以存取由驅動程式發送的或存儲在其上的資料。這樣一來, 非授權個人就可以獲取該密碼, 進而存取上述加密服務了。

類似的, 使用在無線設備中的密鑰資訊也將受到威脅。例如, 為加強兩個藍牙設備之間通訊的安全性, 可能需要在每台設備上裝載補充密鑰。在某些應用中, 密鑰通過藍牙網路從一台藍牙設備傳送給另一台藍牙設備。但是, 非授權個人可以對包含密鑰的廣播藍牙訊號進行破譯。這樣一來, 非授權個人就可以獲取該密碼, 進而存取加密服務。

當上述加密服務控制並提供對類似金融資料或個人資訊的敏感資料的存取時, 將可能導致更加嚴重的後果。因此, 需要一種更安全的技術, 來為加密服務提供更加安全的存取。

【發明內容】

本發明涉及一種驗證一個或複數個用於以使用通訊系統內一個或複數個設備的系統和方法。為方便起見, 根據本發明構建的系統或實現的方法, 其實施例在下文中簡稱為“實施例”。

一方面，本發明涉及對存取由接入設備（例如計算設備）提供的或通過接入設備接入的服務的用戶進行驗證。例如，所述用戶可存取存儲在接入設備或遠端計算設備上的資料。所述用戶還可存取運行在所述接入設備或遠端伺服器上的應用程式。此外，所述用戶還可通過所述接入設備獲得對資料網路的存取。

某些實施例中，需要在所述接入設備和服務提供者之間建立安全通訊機制。例如，最初，用戶可通過一種安全方式向所述接入設備提供信用證明。某些實施例中，包括將信用證明輸入到所述接入設備的安全邊界內。所述接入設備中的加密處理部件隨後對所述安全邊界內的所述信用證明進行加密和/或簽名。在此，所述簽名/加密的真實性將通過一個已發佈的數位證書向第三方（例如，服務提供者）進行驗證。所述接入設備隨後將簽名/加密後的信用證明提供給服務提供者。

所述服務提供者將驗證該信用證明由一特定接入設備產生。例如，所述服務提供者的加密處理器將使用所述接入設備的公共密鑰詢問所述接入設備，使其證明它確實具備對應的私有密鑰。此外，因為所述服務提供者已經進存取了所述公共密鑰的證書，所以必須確保所述接入設備具備密鑰保護機制，以及所述接入設備的私有密鑰不會泄漏到安全邊界的外部。這樣一來就更加確保了提供給所述服務提供者的所述信用證明是來自一個特定和/或受信接入設備。

某些實施例中，對來自用戶的信用證明的認證可用來自動為用戶建立網路連接。例如，用戶可向希望通過其來連接網路的接入設備提供他的或她的信用證明。這些信用證明隨後將提供給接入伺服器，所

述接入伺服器能建立與所述接入設備之間的安全通訊。如上所述信用證明將進行驗證，確保所以接入伺服器與所述接入設備建立安全通訊所必須的密鑰以安全地發送給該接入設備。例如，可使用所述信用證明來檢驗所述接入設備是其所聲稱的那台設備，並且所述密鑰資訊可以安全的發送、使用和存儲在所述接入設備中。

用戶可通過向接入設備出示他的或她的信用證明來啟動將額外的接入設備連接到網路的過程。在這種情況下，當從每個接入設備接收到適當的認證資訊（例如，簽過名的信用證明），並對所述接入設備的身份證明進行檢驗之後，接入伺服器將向每個這些接入設備提供與所述用戶相關聯的密鑰。因此，用戶可以很輕鬆的將接入設備連接到網路上。此外，這些操作將以一種非常安全的方式完成。

任何用戶都可以使用同一個或其他的接入設備來構建他們自己的接入設備網路。這裏，每個用戶將得到獨一無二的密鑰，分配給該用戶的接入設備。這樣一來，每個用戶的網路將通過加密的方式區別於其他用戶的網路。

某些實施例中，輸入設備可通過加密處理部件結合在安全邊界內，使用戶將信用證明安全的輸入到接入設備中。例如，這些部件相互連接，以保證部件之間傳送的資料不會通過不安全的媒體路由，例如可能被非授權個人、設備或處理截獲的資料記憶體、軟體棧或無線傳輸。在某些應用中，這可以通過將所述部件安裝到同一個積體電路（即晶片）上來完成。

通過這種方式，來自輸入設備的資料可安全的提供給所述接入設

備的安全邊界，然後在該安全邊界內對資料進行加密。這樣一來，該資料將永遠不會以明文（例如，未加密的）形式出現在安全邊界（例如，由晶片的物理邊界提供的邊界）外部的不安全路徑中。

某些實施例中，可以使用認證來進行檢驗用戶是否正處於接入設備的旁邊。例如，只有在分配給用戶的無線權杖處於提供安全服務接入的接入設備旁邊時，才會向授權用戶提供服務接入。通過這種方式，可以進行如下合理假設：所述授權用戶實際上正在使用特定的接入設備請求服務。

某些實施例中，用戶的信用證明存儲在一個 RFID 權杖上，並且在接入設備的安全邊界內包含一個 REID 讀取器。通過這種方式，可以將信用證明直接傳送給安全邊界，而不必通過軟體消息或應用程式在所述接入設備中傳送。這樣一來，所述信用證明就不會被所述接入系統上的威脅軟體執行的黑客或電腦病毒破譯。

某些實施例中，輸入設備可包括例如指紋識別器之類的生物感測器。在這種情況下，信用證明可包含生物資訊（例如，掃描的指紋）。

某些實施例中，根據本發明構建的系統包括有線和/或無線網路，其中，接入設備包括安全邊界內的 RFID 讀取器和加密處理。用戶通過將其 RFID 權杖放置在接入設備的旁邊，就可以使用該設備中的任何一個來存取網路。這使得信用證明可安全的傳送給用於接入網路的接入伺服器。隨後，所述接入伺服器將與該用戶相關聯的密鑰提供給每台接收該用戶提供的信用證明的接入設備。通過這種方式，該用戶可被自動認證以使用這些接入設備中的任何一個存取網路。

根據本發明的一個方面，提出一種通訊方法，包括：

向複數個接入設備認證至少一個用戶；

建立包括有所述接入設備的至少一個網路。

優選地，所述認證包括向所述接入設備提供至少一個信用證明。

優選地，所述方法進一步包括對所述至少一個信用證明進行密碼簽名。

優選地，所述方法進一步包括使用數位證書以對所述至少一個簽名後的信用證明進行認證。

優選地，所述方法進一步包括使用數位證書來驗證與至少一個所述接入設備相關的安全性。

優選地，所述方法進一步包括使用數位證書來驗證所述至少一個用戶與至少一個所述接入設備是否接近。

優選地，所述方法進一步包括驗證所述至少一個信用證明與一個授權用戶有關。

優選地，所述方法進一步包括回應所述至少一個信用證明與一個授權用戶有關的驗證結果，向所述接入設備提供至少一個密鑰。

優選地，所述驗證包括將所述至少一個信用證明與至少一個登記的信用證明進行比較。

優選地，所述建立至少一個網路包括向所述接入設備提供至少一個密鑰。

優選地，所述建立至少一個網路包括使用所述至少一個密鑰將所述接入設備連接到所述網路上。

優選地，所述方法進一步包括依據向所述接入設備的至少一部分認證所述至少一個用戶中的一個用戶的認證結果，自動將所述至少一部分接入設備組合到一起。

根據本發明的一個方面，提出一種通訊方法，包括：

向複數個接入設備認證複數個用戶；

建立包括有所述接入設備的複數個網路。

優選地，所述網路分別加密。

● 優選地，所述方法進一步包括為所述用戶登記信用證明。

優選地，所述認證包括向所述接入設備提供至少一個所述信用證明。

優選地，所述方法進一步包括對所述至少一個信用證明進行密碼簽名。

優選地，所述方法進一步包括使用數位證書對所述至少一個簽名的信用證明進行認證。

● 優選地，所述建立網路包括向所述接入設備提供複數個密鑰。

優選地，每個所述密鑰與一個所述用戶相關聯。

優選地，所述建立網路包括使用所述密鑰將所述接入設備連接到網路上。

優選地，每個所述網路與一個所述用戶相關聯。

優選地，所述方法進一步包括依據向所述接入設備的至少一部分認證所述至少一個用戶中的一個用戶的認證結果，自動將所述至少一部分接入設備組合到一起。

根據本發明的一個方面，提出一種向設備認證用戶的方法，包括：

定義與一個接入設備相關聯的安全邊界；

直接向所述安全邊界內提供至少一個信用證明，以向所述接入設備認證一個用戶。

優選地，所述安全邊界包括一個密鑰管理邊界。

優選地，所述提供包括將包括所述至少一個信用證明的至少一個RFID 訊號接收入所述安全邊界內。

● 優選地，所述至少一個信用證明包括生物資訊。

優選地，所述提供包包括將包括有生物訊號的至少一個訊號接收入所述安全邊界內。

優選地，所述提供包括將包括有指紋訊號的至少一個訊號接收入所述安全邊界內。

優選地，所述提供包括通過一個感測器在所述安全邊界內的生成至少一個訊號。

● 優選地，所述提供包括通過一個指紋讀取器在所述安全邊界內生成至少一個訊號。

優選地，所述安全邊界由一塊積體電路定義。

優選地，所述安全邊界通過對資料進行加密實現。

根據本發明的一個方面，提出一種用於存取服務的方法，包括：

接收與用戶相關聯的信用證明；

對所述信用證明進行認證；

將所述認證後的信用證明提供給服務提供者；

回應所述認證後的信用證明，接收來自服務提供者的至少一個密鑰；

使用所述至少一個密鑰對服務進行存取。

優選地，所述方法進一步包括建立一個安全邊界，用於接收所述信用證明。

優選地，所述方法進一步包括建立一個安全邊界，用於認證所述信用證明。

● 優選地，所述認證包括對所述信用證明進行密碼簽名。

優選地，所述認證包括對所述信用證明進行加密。

根據本發明的一個方面，提出一種通訊系統，包括：

複數個接入設備，用於接收認證資訊，每個接入設備包括至少一個用於對認證資訊進行簽名的加密處理器；

一個接入伺服器，用於接收所述簽名的認證資訊，所述接入伺服器包括至少一個加密處理器以爲所述接入設備生成至少一個密鑰，所述接入伺服器依據所述簽名的認證資訊向所述接入設備提供所述至少一個密鑰。

優選地，所述認證資訊包括至少一個信用證明。

優選地，所述接入伺服器的至少一個加密處理器接收一個數位證書以對所述認證資訊進行認證。

優選地，所述接入伺服器驗證所述認證資訊是否與一個授權用戶相關聯。

優選地，所述接入伺服器回應所述認證資訊是否與一個授權用戶

相關聯的驗證結果，向所述接入設備提供至少一個密鑰。

優選地，所述驗證包括將所述認證資訊與至少一個登記的信用證明進行比較。

優選地，每個接入設備包括一個安全邊界。

優選地，所述接入伺服器包括一個安全邊界。

優選地，所述接入伺服器的至少一個加密處理器為所述接入設備生成複數個密鑰，並且所述接入伺服器依據與複數個用戶相關聯的簽

● 名認證資訊，提供所述密鑰來選擇一個所述接入設備。

根據本發明的一個方面，提出一種接入設備，包括：

安全邊界內的至少一個加密處理器；

至少一個輸入設備，用於直接向所述安全邊界內提供認證訊號。

優選地，所述至少一個輸入設備包括一個 RFID 讀取器。

優選地，所述至少一個輸入設備包括一個感測器。

優選地，所述至少一個輸入設備包括一個生物感測器。

● 優選地，所述至少一個輸入設備包括一個指紋讀取器。

優選地，所述至少一個輸入設備包括一個鍵盤。

優選地，所述至少一個輸入設備和所述至少一個加密處理器內置於一個共同的積體電路內。

優選地，所述至少一個輸入設備包括一個感測器。

優選地，所述至少一個輸入設備包括一個指紋讀取器。

優選地，所述至少一個輸入設備包括一個 RFID 讀取器。

【實施方式】

以下將結合具體實施例對本發明進行詳細描述。很明顯，本發明可以多種形式實現，其中的一些可能與下文中公開的實施例截然不同。因此，本申請中公開的具體結構和功能特徵僅僅是爲了對本發明進行描述而列舉的例子，不是對本發明範圍的限制。

一方面，本發明涉及一種提供用戶級認證的系統和方法。例如，這裏描述了向設備認證用戶的各種技術。此外，這裏還描述了向設備認證用戶以使其能接入資料網路的各種技術。

在傳統的資料網路中，使用設備級認證來確保只有授權設備才允許連接到網路。本申請中，使用加密技術來對一台設備進行認證，以證實這台試圖連接到網路的設備就是其所聲稱的那台設備，並且是該網路的授權用戶。例如，設備一般通過像路由器這樣的網路橋接器連接到網路。這樣的話，向路由器和授權設備提供一致的加密密鑰，使得這些設備可以執行加密操作，用來提供所期望的認證。在這種網路中，必須提供一種安全機制以向所有可能連接到網路的設備安全的分配密鑰。傳統的做法是，由用戶或管理員手動地將密鑰載入到這些設備上（例如，通過鍵盤或軟體程式）。

這種設備級認證有許多的缺點。例如，它不能驗證到底是哪個用戶正在使用該設備。此外，當複數個用戶使用同一台設備的時候，沒有一種有效的機制以確定應該使用哪個驗證資訊（例如，密碼證書）來對系統進行認證。

圖 1 所示爲根據本發明的一個實施例的系統 100，該系統中，一個和複數個用戶（圖中未標出）可以通過接入伺服器 106 使用一台或

多台接入設備 102 和 104 來存取服務 130（例如，連接到資料網路）。例如，若要存取某服務，用戶需首先向接入設備 102 出示認證資訊（例如信用證明 108，例如密碼）。為方便起見，術語“信用證明”可用于代表用戶為進行認證所出示的任何資訊。

接入設備 102 可包括一個安全模組，用於提供加密處理，並可結合使用其他的安全機制。例如，安全模組可包括一個或複數個加密處理器 128，用於執行加密操作，包括加密、解密、認證、驗證和簽名。

● 使用該安全模組，接入設備 102 可對從用戶接收到的信用證明進行認證，並安全地將它們傳送給接入伺服器 106 中的密鑰管理器 110。

密鑰管理器 110 提供了一種安全的環境，用於生成、分配和維護在系統中使用的密鑰。該密鑰管理器包括一個或複數個加密處理器 124，用於安全的執行加密操作，包括加密、解密、認證等。該密鑰管理器還包括一個安全資料記憶體 122，用於通過一種防止密鑰被非授權個人或方法存取的方式來存儲密鑰 126。

● 為提供安全處理和密鑰存儲，提供了一個與該密鑰管理器相關聯的安全邊界，並由該密鑰管理器實施。該安全邊界可使用硬體和/或加密技術來建立。

用於提供安全邊界的硬體技術可包括，例如將所涉及的部件安裝在單個積體電路中。此外，通過使用例如環氧封裝等防拆封和/或防篡改技術可以從物理結構上對一個或複數個積體電路提供保護。

用於建立安全邊界的加密技術可包括，例如在任何敏感資料離開密鑰管理器之前對其進行加密。出於此目的，該密鑰管理器可使用一

個或複數個加密處理器 124，並將相關的加密/解密密鑰 126 存儲在一個內部的安全資料記憶體 122 中。

為維護系統 100 的安全性，由密鑰管理器分發給系統中其他部件的任何密鑰都需要得到足夠的保護。例如，制定相關規定以保證密鑰只發送給相關的授權設備。此外，制定相關規定以對處於分發階段和接收設備中的密鑰進行保護。

某些實施例中，接入設備 102 包括一個或複數個加密處理器 128 和從接入設備 102 發往接入伺服器 106 的用於認證資訊的密鑰(例如，密鑰 114)，用來加強發往接入設備 102 的密鑰的安全傳輸，並為接入設備 102 使用的密鑰提供保護。

例如，通過使用數位證書和其他的加密處理，接入設備 102 可向接入伺服器 106 提供強大的認證，以保證發往接入伺服器 106 的信用證明是來自使用特定接入設備的用戶。此外，這些處理還可用於驗證接入設備 102 是否為密鑰資訊提供了高級保護。

一旦認證資訊被提交給接入伺服器 106，密鑰管理器 110 會將密鑰安全的分發給接入設備 102，使得用戶可以存取所期望的服務。例如，密鑰管理器會將密鑰發給接入設備，使得該接入設備可以連接到資料網路。

圖 1 中所示的實施例提供了一種有效的機制，使得用戶可使用多種接入設備來獲得對網路的存取。用戶首先需向每台設備認證其自己。隨後，通過向每台設備分發必要的密鑰，接入伺服器自動的建立起相應網路。正如這裏所描述的那樣，這個過程可在具有高級安全性

的環境中完成。此外，因為所述接入伺服器向每台設備分配了適當的密鑰，所以密鑰資訊不必提供給用戶。而且，用戶也不必向其在網路中使用的每台接入設備出示數位證書。

系統 100 的操作將在下面結合圖 2 中的流程圖進行詳細的解釋。如模組 202 所示，可生成一個或複數個密鑰以使接入設備安全地與接入伺服器通訊。某些實施例中，這一過程通過使用非對稱密鑰來實現。

例如，可向每台接入設備提供唯一的非對稱身份密鑰 114。該非對稱密鑰的私有密鑰部分將存儲在所述接入設備的安全邊界（如虛線部分 112 所示）內。例如，加密處理器 128 可在該安全邊界內生成密鑰，並且該密鑰的私有部分將永遠不允許以明文（例如，未加密）的方式出現在安全邊界 112 的外部。下面將對安全邊界的其他細節進行描述。

該密鑰的公共部分將與數位證書一起發佈。例如，接入設備的製造商可在公共的可存取伺服器上發佈該公共密鑰和數位證書。數位證書的作用是驗證如下內容：公共密鑰是真實的，私有密鑰並未泄漏在安全邊界的外部，持有私有密鑰的接入設備提供了一種安全的機制以接收、使用和維護密鑰。因此，該數位證書可用來為由持有相應私有密鑰的接入設備所提供的任何資訊的真實性提供功能強大的驗證。

某些實施例中，接入設備和接入伺服器可使用非對稱密鑰來協商一個或複數個其他的密鑰，用來進行加密處理。例如，可使用這些其他的密鑰對在這些部件之間傳送的資訊進行加密、解密和簽名等。通過這種方式，可在接入設備和接入伺服器之間建立一條安全通道（如

虛線部分 116 所示)。這就是說，每個部件將可以得到一個或複數個密鑰，使得他們可以對來自其他部件的加密資訊進行解密。通過這種方式，敏感資料（例如，密鑰）可以在不安全的鏈路 118 上進行安全的傳送。

現在來看模組 204，為使接入伺服器能夠識別分配給指定用戶的信用證明，所述身份證明需要在接入伺服器中登記（例如，輸入）。這可以通過使用，例如信用證明登記機制 120 來完成。某些實施例中，信用證明登記機制可包括一個鍵盤和伺服器的監控台。某些實施例中，信用證明登記機制 120 可以位於與密鑰管理器 110 相關聯並由其進行加強的安全邊界內。例如，信用證明登記機制 120 可包括一個物理上與密鑰管理器連接的鍵盤，一個 RFID 讀取器，一個生物感測器等。這些部件的其他細節將在下面進行描述。

信用證明登記機制 120 向密鑰管理器 110 提供所述信用證明信息，隨後密鑰管理器 110 將生成一個或複數個與該信用證明相關聯的密鑰。這些密鑰包括，例如 SSL 或 IPSEC 密鑰/安全關聯，使用戶可以登錄到加密網路上。隨後，該密鑰管理器將維護一個資料庫，該資料庫將每個授權用戶的信用證明（例如，信用證明 A）與為該用戶生成的密鑰和證書（例如，密鑰 A）關聯起來。

所述信用證明和與其相關的密鑰可存儲在安全資料記憶體 122 中。某些實施例中，資料記憶體 122 可以在密鑰管理器 110 的物理安全邊界內得到保護。例如，資料庫 122 可位於一個安全封裝內和/或跟密鑰管理器位於同一積體電路上。某些實施例中，資料記憶體 122 還

可以位於密鑰管理器的外部。但是，在這種情況下，密鑰管理器需要在將密鑰存儲在資料記憶體之前對其進行加密。

現在來看模組 206，當用戶想通過接入設備 102 對服務進行存取的時候，該用戶需向該接入設備出示其信用證明。某些實施例中，信用證明 108 可通過例如接入設備提供的鍵盤和顯示器來提供給該接入設備。

某些實施例中，信用證明可通過一條直接通往所述接入設備安全邊界的路徑提供給所述接入設備。例如，在接入設備 104 中，信用證明 132 可直接輸入（如虛線部分 134 所示）到位於安全邊界 136 內的設備中。這可以通過使用一個在物理上結合到安全邊界 136 內一個部件上的鍵盤、一個 RFID 讀取器、一個生物感測器等來完成。這些部件的其他細節將在下面進行描述。

現在來看模組 208，接入設備 102 通過上述安全通道 116 向接入伺服器 106 傳送信用證明 108。例如，加密處理器 128 可使用從與接入伺服器 106 的上述協商結果中獲得的密鑰，對所述信用證明進行加密。一般來說，加密處理器 128 使用這樣的密鑰或私有密鑰 114 對所述信用證明進行簽名。

在模組 210，接入伺服器 106 中的加密處理器 124 對加密的/簽名的信用證明進行處理。通過這一加密處理，接入伺服器獲得了對所述信用證明確實是來自一個正在使用特定接入設備 102 的用戶這一事實的充分認證。此外，還可以通過數位證書確保用戶輸入信用證明時使用的輸入設備（例如，鍵盤、感測器和 RFID 部件等）是與該接入設

備組合在一起的。

隨後，接入伺服器 106 檢查信用證明資料庫以驗證所述信用證明是與一個授權用戶相關聯的。例如，接入伺服器會確定該信用證明是否與存儲在資料記憶體 122 中的信用證明（例如，信用證明 A）相匹配。

如果結果相匹配，那麼接入伺服器 106 會生成或從資料庫中獲取對應於所述信用證明的密鑰（例如，密鑰 A）。隨後，所述接入伺服器將該密鑰傳送給接入設備 102（模組 212）。一般，爲了對傳輸過程中的密鑰提供保護，加密處理器 124 將對其進行加密。這裏，加密處理器可使用協商的密鑰或與私有密鑰 114 相對應的公共密鑰對密鑰 A 進行加密。

一旦接入設備 102 接收到加密的密鑰 A，加密處理器 128 隨即對該密鑰進行解密，並將解密後的密鑰 A 140 存儲在安全邊界 112 內。這裏，加密處理器 128 可使用一個協商的密鑰或私有密鑰 114 來對密鑰 A 進行解密。隨後，接入設備 102 使用密鑰 A 140 來建立到網路（模組 214）的連接。

如果有必要的話，該用戶還可在隨後使用另一個接入設備（例如，接入設備 104）來存取網路。這時，該用戶會再一次向接入設備 104 出示其信用證明（例如跟上面一樣的信用證明）。隨後，加密處理器 142 對所述信用證明進行加密/簽名，並將它們通過不安全鏈路 148 上的安全通道 146 傳送給接入伺服器。非對稱身份密鑰 144 會再一次被用於建立所述安全通道 146，形成數位證書的基礎，以及對信用證明

進行簽名等。隨後，接入伺服器 106 會驗證該信用證明。這裏，因爲接入伺服器收到了相同的信用證明，它就會假設是同一用戶在向接入設備 104 進行認證。因此，接入伺服器會通過所述安全通道 146 將相同的密鑰（例如，密鑰 A）發送給接入設備 104，從而將這些接入設備組合到一起。加密處理器 142 對加密密鑰 A 進行解密，並將解密後的密鑰 A 150 存儲在安全邊界內。隨後，接入設備 104 使用密鑰 A 來連接網路或存取另一服務。

此外，可以將不只一組的信用證明出示給指定的接入設備以存取網路。例如，分別分配了不同信用證明的複數個用戶可共用一台接入設備。此外，在存取例如個人服務或雇主服務等不同的服務時，同一用戶可能會使用不同的信用證明。因此，可在接入伺服器資料庫中存儲另一組信用證明，並與一個唯一的密鑰（例如，密鑰 B）相關聯。當向接入設備 104 出示這些其他的信用證明時，密鑰 B 將通過上述安全技術提供給接入設備 104。因此，接入設備可使用密鑰 B 150 來建立一條單獨的連接網路的加密安全連接。

本發明的這些方面將結合圖 3 和 4 進行更詳細的描述。圖 3 是可支援多種通訊和資料處理設備的網路系統的一個實施例的方框示意圖。

在圖 3 中，接入設備通過網路橋接器（例如，一台路由器）304 連接到例如 Internet 的廣域網（“WAN”）302。這裏，該網路橋接器用作上述的接入伺服器。可選擇地，網路橋接器 304 還可以連接到一台接入伺服器（未標出），這樣一來，當在接入伺服器和接入設備之間

傳送時，信用證明和密鑰將通過該網路橋接器。在這兩種情況下，系統所有授權用戶的信用證明可在該接入伺服器中登記。

網路橋接器 304 可為有線或無線設備提供連接。例如，網路印表機 312 可通過如實線部分 306 表示的有線連接連接到該網路橋接器上。基於因特網協定的語音（“VoIP”）電話 314 也可以通過如實線部分 308 表示的有線連接連接到該網路橋接器上。

其他設備可通過例如曲線 310 表示的射頻（“RF”）訊號連接到該網路橋接器上。這裏，網路橋接器 304 可支援例如藍牙、802.11 和 GSM 等無線標準。

接入設備可以是支援藍牙協定的 VoIP 電話 314，支援 802.11 和/或藍牙的筆記本電腦 316，支援 802.11 和/或藍牙的個人數位助理（“PDA”）318，支援例如 GSM 的蜂窩電話，個人娛樂設備 320，支援 GSM/802.11 以及可以通過藍牙與週邊設備例如無線手持機 324 通訊的電話 322，支援 802.11 無線連接以及可以與無線週邊設備例如支援藍牙的鍵盤 328 和滑鼠 330 通訊的個人電腦 326。

正如這裏所描述的，設備 312—330 中的每一台都可以包括一個安全模組（未標出），使上述設備可以更安全有效的接收任何連接資料網路 302 和/或其他設備所必須的任何密鑰。在後一種情況下，例如，密鑰可以在設備之間安全的發放，以使週邊設備（例如，鍵盤 328）可以與基礎設備（例如，電腦 326）安全的通訊。因此，用戶僅需要向該設備出示其信用證明，就可以將任何這些設備連接到網路或其他設備上。在週邊設備（例如，鍵盤 328）的情況下，信用證明將首先通

過基礎設備（例如，電腦 326），隨後路由到接入伺服器 304。

應用於這些設備中的認證部件和處理的其他細節將在下面進行描述。例如，向接入設備或接入伺服器提供信用證明的幾個實施例在下面結合圖 5—圖 8 進行描述。此外，安全模組的幾個實施例也在下面結合圖 9—圖 12 進行描述。

圖 4 所示為一個網路系統（例如，如圖 3 所示）中執行的操作的流程圖。例如，這樣的一個系統可以包括複數個接入設備，並支援多用戶和多級別信用證明。通常情況下，這些操作可以結合圖 1 和圖 2 來執行。為方便起見，圖 4 或下面的描述並未涵蓋處理過程中的所有操作。

如步驟 402 所示，用戶（簡稱“用戶 A”）的一個信用證明登記在所述接入伺服器中。在步驟 404，用戶 A 向一台接入設備（簡稱“接入設備 1”）出示其信用證明。接入設備 1 將該信用證明發送給接入伺服器，在接入伺服器驗證該信用證明已經登記之後，將相關聯的密鑰發送給接入設備 1（步驟 406）。隨後，接入設備 1 使用與用戶 A 關聯的密鑰來連接到網路（步驟 408）。

如步驟 410—步驟 414 中所示，當用戶向系統中的複數個接入設備出示其信用證明後，網路將會自動建立。如步驟 410 所示，用戶 A 可向另一台接入設備（簡稱“接入設備 2”）出示其信用證明。接入設備 2 將該信用證明發送給接入伺服器，在接入伺服器驗證該信用證明已經登記之後，將相關聯的密鑰發送給接入設備 2（步驟 412）。隨後，接入設備 2 使用該與用戶 A 關聯的密鑰來連接到網路（步驟 414）。

如步驟 416—步驟 422 所示為幾個用戶可以使用同一台指定設備來存取網路。這裏，每個用戶分配有不同的信用證明。如步驟 416 所示，另一個用戶（簡稱“用戶 B”）的信用證明將登記到接入伺服器中。在步驟 418，用戶 B 也向接入設備 1 出示其信用證明。接入設備 1 將該信用證明發送給接入伺服器，在接入伺服器驗證該信用證明已經登記之後，將相關聯的密鑰發送給接入設備 1（步驟 420）。隨後，接入設備 1 使用該與用戶 B 關聯的密鑰來建立一條完全獨立的到網路的加密安全連接（步驟 422）。

實際中，上述關聯到用戶 B 的一組完全獨立的信用證明可以是分配給指定用戶（例如，用戶 A）的第二組信用證明。例如，一個用戶可以使用分配給他的一組信用證明來存取一個網路（例如，一個家庭網路），而使用分配給他的另一組信用證明來存取另一個網路。在圖 3 中，設備 314 和 316 可用於連接用戶辦公室中的一個企業 LAN。在這種情況下，可通過 WAN 302 和其他的路由機制 332 向辦公室網路 334 提供第二組信用證明。一旦交換了合適的密鑰，就可以在接入設備和辦公室網路 334 之間建立起一條企業虛擬專用網（“VPN”）或其他形式的連接。再次重申，這一網路與該用戶的或系統中其他用戶的所有其他網路連接完全獨立並進行了加密保護。

步驟 424—步驟 428 所示為其他用戶向系統中的複數個接入設備出示其信用證明時該網路可繼續自動建立。如步驟 424 所示，用戶 B 可向另一個接入設備（簡稱“接入設備 3”）出示其信用證明。接入設備 3 將該信用證明發送給接入伺服器，在接入伺服器驗證該信用證

明已經登記之後，將相關聯的密鑰發送給接入設備 3（步驟 426）。隨後，接入設備 3 使用這個與用戶 B 關聯的密鑰來連接到網路（步驟 428）。

與傳統系統相比，上述的系統體現出了許多優勢。傳統網路只能提供通過對前端和所有可能連接到網路的設備進行手工配置來實現的設備級認證。例如，路由器需要由物理連接至該路由器的 LAN 埠的管理員對其進行配置。這裏，該管理員需要為路由器輸入密鑰，並且確認每台可能連接到該路由器的設備。此外，為使這些設備能夠連接到該路由器，管理員還需為網路中的每台設備手工配置必需的密鑰。

相比之下，根據本申請構建的網路，可在用戶向相應設備認證其身份後，通過將這些設備組合（例如，接入設備）到一起而自動的建立。這是通過，例如在系統級進行安全認證來實現。例如，還可以驗證用戶的鄰近程度以及安全模組對密鑰提供的保護（例如，使用適當的硬體）。

可以使用多種安全技術來向設備提供用戶認證。例如，可以通過一直接連接將信用證明提供給密鑰管理邊界，還可以通過 RFID 訊號或物理上位於設備安全邊界內的感測器將信用證明傳送給設備的安全邊界。

這裏，可以使用基於公共/私有密鑰對的數位證書來建立網路。該處理可通過使用在每個部件中都能得到保護的私有密鑰來初始化，該處理還提供了一種安全環境，在該環境中，各部件可以動態的改變密鑰。

此外，每個用戶不必存取用於驗證其身份的密鑰，這是因為該用戶不必在每台設備上預先配置正確的密鑰。作為替代，用戶只需出示信用證明等類似資訊就可以通過指定設備對網路進行存取。

此外，還可以對系統進行配置，使其可以提供複數個網路。每個網路可包含指定的一組部件，定義給不同的用戶和/或同一指定用戶的不同許可級別。通過使用加密技術對網路存取進行認證，對通過每個網路的資料流程加密，這些網路彼此之間可以安全的分開。

● 現在來看圖 5—圖 8，向設備提供信用證明的機制的幾個實施例將在接下來進行討論。總之，以下將介紹向一個接入設備提供信用證明。雖然如此，這些方法也可用于向接入伺服器或系統中的某些其他部件提供信用證明。

圖 5 所示為系統 500 的一個實施例，其中，當分配給用戶的無線權杖臨近計算設備時，所選擇的服務將通過計算設備提供給用戶。接入設備 502，例如一台電腦，包括一些部件，用於確定分配給用戶的無線權杖（例如，一個 RFID 權杖）是否處於臨接近入設備 502 的位置。例如，可以使用一個無線接近讀取器（例如，一個 RFID 讀取器 506）接收來自無線接近權杖 516 的訊號 530。訊號 530 可包括有確認無線接近權杖 516 的唯一身份的資訊。例如，這些資訊可包括一個或複數個信用證明 528（例如，密碼），用於通過接入伺服器 504 來存取加密服務。

在確定權杖 516 跟讀取器 506 之間接近程度時，可使用許多種方法，這依賴于實際應用的情況。某些實施例中，只有當權杖處於讀取

器的指定距離範圍內時，該權杖才會生成訊號。而這可以通過，例如使用被動權杖來完成，該被動權杖解讀讀取器發出的訊號，並回應接收的訊號向該讀取器發出訊號。表示接近程式的權杖 516 和識別器 506 之間的不同距離可根據應用的要求以及某些情況下根據作業系統的特徵來定義。

接入設備 502 可通過在通訊鏈路 526 上發送請求，向接入伺服器 504 請求存取服務。根據特定的應用，通訊鏈路 526 可包括，例如，
● 電線、光纜或無線連接。因此，接入設備 502 可支援與接入伺服器 504 之間的有線或無線通訊。

一般來說，對服務的存取開始於用戶同接入設備 502 之間的交互。例如，用戶可使用鍵盤或點擊設備（例如，電腦滑鼠）來存取服務。在此期間，用戶將被要求輸入密碼和/或向生物感測器提供生物（例如，指紋）資訊，以認證其身份。在這種情況下，只有當用戶提供了足夠的信用證明包括，用戶所掌握的資訊（例如，密碼），用戶所具備
● 的證件（例如，權杖），和該用戶的身份（例如，物理或生物特徵）之後才能存取相應的服務。

接入設備 502 使用了安全機制，來確保維護在接入設備中的用戶所提供的信用證明，在發往接入伺服器 504 的過程中是安全的。例如，接入設備可提供一個安全邊界，其內的任何接收自權杖的資訊都將以一種安全的方式使用和維護。此外，接入設備 502 還可包含一個安全模組 508，用於提供加密處理，以對信用證明進行加密。某些實施例中，資訊只能在識別器 506 和安全模組 508 之間，通過一條位於公共

積體電路 512 上的連接來傳送。因此，可對接入設備進行配置，使得信用證明永遠不會在該積體電路外部以明文方式出現。

此外，接入設備 502 還可與接入伺服器 504 進行加密通訊。例如，可在安全模組 508 和接入伺服器 504 之間建立密碼加密通訊通道 518。在這種情況下，安全模組 508 向接入伺服器 504 發送信用證明之前，會首先對其進行處理（例如，加密/簽名）。因此，安全模組將提供強大的認證，即該信用證明是來自接近特定接入設備 502 的特定權杖 516。

在接入伺服器 504 從接入設備 502 收到認證後的信用證明之後，接入伺服器就可以提供所請求的服務。“服務”可包括，例如存取資料和/或資料處理服務。因此，一項服務可使得接入設備在資料記憶體中讀取或寫入資料，存取加密的資料，使用加密密鑰，對加密資訊例如安全關聯和密鑰進行存取，存取網頁，存取資料網路或存取處理程式。

正如這裏所用到的一樣，術語“資料”可包括任何可由計算設備存取的資訊，包括，例如資料檔案、密碼和包含密鑰在內的加密安全關聯。

正如這裏所用到的一樣，術語“存取”可包括，例如獲取、使用或調用等。因此，可通過向接入設備提供一份該資料的副本來存取資料，也可以通過允許接入設備操作或使用該資料來存取資料。後者的一個例子是，一旦用戶被授權存取某項服務，可信平臺模組可使用密鑰來為用戶執行相應的操作。對於資料網路來說，存取可包括，例如

通過網路發送和/或接收資料。對於處理應用來說，存取可包括，例如對該應用程式進行調用，與其進行交互，對其進行使用或將其載入到接入設備中。

接入伺服器可包括用於提供服務硬體和/或軟體。例如，接入伺服器可包括處理系統，用於處理服務請求，驗證該請求者是否是所請求服務的授權用戶或提供所請求的服務。

實際中，就與所請求服務（例如，接入設備 502）的位置關係而言，接入伺服器可位於本地或遠端。例如，一個本地的可信平臺模組可控制對計算系統中密碼的存取。而一個遠端無線網路橋接器可控制計算系統對連接到該網路橋接器上的資料網路的存取。

接入設備可包括硬體和/軟體，用於對服務進行存取。例如，接入設備可包括電腦系統，例如但不限於個人電腦、伺服器、蜂窩電話和個人數位助理等。

為方便起見，在圖 5 中只描述了一個權杖、接入設備和接入伺服器。但是，應當明白，該系統可包括任意數量的這類部件。例如，用戶可使用一個權杖通過一個或多接入設備來存取一項或多項服務。因此，一台接入設備可存取來自多台接入伺服器的服務。同樣的，多台接入設備可存取由一台指定接入伺服器提供的服務。

對存取服務的授權依賴於所使用的特定權杖和接入設備。例如，用戶可分配到一個權杖，用於通過某一接入設備來存取某一服務。此外，用戶還可分配到另一權杖，用於通過同一或另一接入設備來存取其他的服務。同樣的，單個權杖上可包含多組資訊（例如，信用證明），

使得同一用戶可存取不同的服務，或讓複數個用戶共用同一權杖。

無線接近讀取器和權杖可使用多種無線接近技術中的一種或幾種來實現。例如，無線接近讀取器和權杖可支援，例如但不限於，RFID、ISO14443 和 ISO15693 中的一個或複數個。

依賴于不同應用的需要，權杖可通過多種物理形式實現。例如，權杖可採用易於攜帶的形式，類似於塑膠信用卡、智慧卡或閘卡等。同樣的，權杖也可采可附著在其他物質上的標籤或標貼的形式。

● 權杖可以是包括但不限於智慧卡、信用卡、加密狗、標記卡、生物設備例如指紋識別器、移動設備例如蜂窩電話和 PDA 等。某些實施例中，權杖包括使用在通用智慧卡中的電路。例如，權杖可存儲將發送給認證系統的加密密碼。

現在來看圖 6，這裏將描述對基於接近技術的認證系統的有關操作和配置方面的其他細節。如步驟 602 所示，在接入設備 502 中提供了一個安全邊界，用於對獲取服務存取的過程進行保護，包括對認證● 過程和認證過程中用到的資訊進行保護。該安全邊界可通過使用硬體和/或加密技術來實現。

用於提供安全邊界的硬體技術可包括，例如，將相關部件安裝在單個積體電路上。如圖 5 所示，RFID 讀取器 506、安全模組 508 和其他處理部件 510 可共同安裝到同一塊積體電路 512 上。因此，除非通過物理存取積體電路 512，並使用入侵技術分析積體電路 512 內部的操作和資料，否則積體電路 512 上執行的任何處理過程或在其上使用或存儲的任何資訊都不會被泄露。對於許多應用來說，這種形式的

硬體安全邊界可提供一種可以接受的高級安全保護。

安全邊界還可以使用其他方法來提供。例如，可以通過使用已知技術（例如，環氧封裝）的物理結構對一個或複數個積體電路（例如，積體電路 512）提供保護。同樣的，處理系統 502 和/或其內部部件也可以採用防篡改和/或防拆封技術。

用於提供安全邊界的加密技術包括對通過系統中通過非安全路徑發往或發自積體電路的任何重要資訊進行加密。例如，安全關聯和密鑰只可能在積體電路 512 內部才以明文方式出現。當密鑰需要發往積體電路 512 外部（例如，存儲在資料記憶體 514 上）時，會首先進行加密。

類似的，在積體電路 512 和接入伺服器 504 之間傳送的任何重要資訊都被加密。例如，從 RFID 權杖 516 接收到的資訊（例如，信用證明 528）在通過鏈路 526 發送前會被加密。

圖 5 中加密安全邊界由虛線部分 518 表示。虛線部分 518 部分的展示了加密資訊在安全模組 508、處理部件 510 和資料記憶體 514 之間進行傳送。因此，該資訊可以被安全的傳送，儘管資訊所通過的某些器件可能並不是安全的（例如，資料匯流排 520）。

加密資訊同樣也可以通過通訊鏈路 526 在積體電路 512 與接入伺服器 504 的密鑰管理器 524 中的加密處理器 522 之間傳遞。在這種情況下，當需要發送和接收加密資訊並以明文形式提供該資訊以進行內部處理時，加密處理器將執行密鑰交換、加密、解密和/或認證等操作。

通常來說，系統內部提供的保護形式依賴于指定應用的要求。例

如，FIPS—140—2 規範定義了可以在系統內部實現的複數個安全級別。

積體電路 512 提供的安全邊界和加密邊界 518 可用于提供一種安全機制，以對存取服務的用戶進行認證。例如，從 RFID 權杖 516 接收到的信用證明 528 可通過射頻訊號 530 直接提供給積體電路 512。因此，無需將信用證明 528 通過軟體機制或可由軟體存取的硬體輸入到處理系統 502 中。這樣一來，在這一處理階段中該資訊將不會受到黑客或軟體病毒的威脅。

一旦資訊到達積體電路 512，就將受到積體電路 512 的物理邊界和加密邊界 518 的保護。例如，規定必須確保上述資訊不會以明文的形式出現在積體電路 512 的外部。因此，即使處理系統 502 中的欺詐軟體獲得了對晶片 512 外部的資訊的存取，但在沒有正確的密鑰資訊的情況下，該軟體也不能對上述資訊進行解密。而且密鑰資訊也在積體電路 512 和加密邊界 518 中受到保護。也就是說，密鑰資訊不會以明文形式出現在安全邊界的外部。這樣一來，信用證明就可以安全的路由到接入伺服器 504 中。

此外，通過這種安全機制，在特定 RFID 權杖 516 接近接入設備 502 時，該接入設備 502 可以向接入伺服器 504 提供可靠的認證。首先，如前所述，信用證明將以一種安全的方式接收。其次，將在安全邊界內作出有關權杖 516 是否足夠接近的有效判斷。然後安全模組 508 將使用在它與密鑰管理器 524 中的加密處理器 522 之間建立的安全協定對這一資訊進行密碼簽名。通過這個簽名，接入伺服器可確定指定

的資訊是來自特定的處理系統（例如，接入設備 502），並且資訊沒有受到入侵。因此，權杖 516 接近處理系統 502 這一方法，可用作對服務提供者所提供的加密服務進行存取的一種可靠授權方法。

以下將結合圖 6 介紹用於存取服務的操作的一個實例。如步驟 604 所示，當 RFID 權杖 516 位於接入設備 502 的合適範圍內時，RFID 讀取器 506 將從 RFID 權杖 516 接收到一個 RFID 訊號 530。如上所述，RFID 訊號 530 將被安全邊界內的接入設備 502 接收到。

● 如步驟 606 所示，可以對系統 500 進行配置，使得 RFID 訊號中包含的任何資訊只能在安全邊界內提取出來。例如，如圖 5 所示，用於從 RFID 訊號 530 提取信用證明的 RFID 讀取器 506 安裝在包括有其他部件以保護該信用證明的積體電路 512 中。例如，積體電路 512 可包括安全模組 508，對信用證明（步驟 608）進行加密/簽名，以防止資訊以明文形式出現在積體電路 512 的外部。這裏，安全模組 508 中的加密處理器可使用私有密鑰 540 來對資訊進行加密。與此私有密鑰● 相關聯的公共密鑰可由一個可信實體連同證書一起發佈。該證書用於校驗公共密鑰的真實性。隨後，加密處理器 522 將使用公共密鑰來驗證從安全模組 508 接收到的資訊的簽名。圖 5 中，還可使用一個補充處理來通過鏈路 526 向另一個方向發送資訊。

因此，當安全模組 508 中的加密處理器對信用證明簽名後，簽名後的信用證明將通過鏈路 526（步驟 610）發往密鑰管理器 524。通過這種方式，實際上，該資訊通過一條安全通道發送（如實線部分 518 相應部分所示），即使實際的資料路徑並不安全。

密鑰管理器 524 將接收到的資訊發往加密處理器 522 進行必要的解密和/或認證處理。隨後，密鑰管理器 524 驗證該接收的資訊，指示該用戶已經得到授權可以存取該網路（步驟 612）。某些實施例中，接入伺服器 504 可包括無線接近設備（例如，RFID 讀取器）和相關的處理，使得在用戶向接入伺服器出示其權杖之後，其信用證明可以很容易並直接地載入到接入伺服器中。在其他實施例中，還可以使用非專用 RFID 讀取器來獲取該資訊。隨後所獲取的資訊可使用其他方法（例如，通過通訊媒體下載）載入到接入伺服器中。

因為密鑰管理器 524 已經通過與信用證明相關聯的密碼簽名得知權杖 516 鄰近接入設備 502，所以一旦該信用證明通過驗證，密鑰管理器 524 將確信可以提供對所請求服務的存取了。如上所述，提供對網路的存取包括向接入設備 502 發送安全關聯或密鑰。這些密鑰可通過安全通道（加密邊界 518）發送給接入設備 502。因此，加密處理器 522 會在將這些密鑰發送到鏈路 526 上之前，對其進行加密（步驟 614）。

可對接入設備 502 進行配置，使得這些密鑰等資訊可以在其安全邊界內進行解密和維護（步驟 616）。例如，這些密鑰（例如，密鑰 540）可存儲在積體電路 512 中。可選擇地，在將這些密鑰存儲到資料記憶體 514 之前，安全模組中的加密處理器可使用密鑰（例如，密鑰 540）對接收到的密鑰進行加密。

如步驟 618 所示，接入設備隨後使用接收到的密鑰來獲得對網路的存取。需要再次強調的是，某些實施例中，這些密鑰只有在處於接入設備 502 的安全邊界內的時候，才允許以明文形式使用。

接近認證設備的其他細節在 2004 年 9 月 30 日申請的申請號為 10/955806 的美國專利申請中有公開，本申請在此全文引用該美國專利申請公開的內容。

圖 7 所示為提供安全機制以輸入信用證明的接入設備的另一實施例。接入設備 700 包括一個輸入設備 704，位於接入設備 700 的安全邊界內。例如，輸入設備 704 可以和安全模組 706 位於同一積體電路 702 上。這樣一來，用戶可以直接將其信用證明輸入到安全邊界內。

此外，安全模組 706 還可以使用一個或複數個密鑰（例如，密鑰 708）對安全邊界內的信用證明進行加密，這樣一來，該信用證明就不會以明文的形式出現在安全邊界的外部。因此，安全模組使用加密技術對安全邊界進行了有效的擴展。例如，通過在存儲之前對資料進行加密，安全邊界可有效的擴展至外部的資料記憶體 714（如虛線部分 716 所示）。此外，該安全邊界還可通過通訊媒體有效的擴展（如虛線部分 720 所示）到另一加密處理系統（未標出）。

在圖 7 所示的實施例中，接入設備結合有無線介面 710 和天線 712（或另一形式的無線收發器），以通過無線訊號 718 來和其他的無線設備（例如，無線網路橋接器和接入伺服器，未標出）進行通訊。某些實施例中，該接入設備的資料通訊介面 710 可與例如安全模組 706 位於同一積體電路上。該無線介面可支援 802.11、藍牙和/或其他無線通訊標準。

某些實施例中，輸入設備 704 可以是一個感測器，例如生物感測器。該感測器可包括一個指紋讀取器。可選擇的，該感測器還可包括

視網膜/虹膜掃描器，用於語音識別的語音輸入設備（例如，麥克風），用於面部特徵識別的照相感測器（例如，CCD 設備）或 DNA 檢測設備。此外，積體電路上還提供有合適的處理以對該資訊進行提取和分析。

某些實施例中，接入設備將輸入資訊傳送給接入伺服器以獲得對服務的存取。該資訊也可登記在密鑰管理器中。因此，如上所述，密鑰管理器可將接收自接入設備的資訊與保存已授權信用證明（例如，指紋資料）的密鑰管理器資料庫中的資料進行對比。當找到匹配項時，密鑰管理器就會向發出請求的接入設備提供相關的密鑰。

某些實施例中，接入伺服器可包括輸入設備和相關的處理，以使上述資訊可以更容易、更直接地載入到接入伺服器中。在其他實施例中，可使用非專用輸入設備（例如，感測器）來獲取上述資訊。隨後，通過其他方法（例如，通過通訊媒體下載）將所獲取的資訊載入到接入伺服器中。

圖 8 所示為系統 800 的一個實施例，為用戶輸入信用證明提供一種安全機制。處理系統 802 包括一個安全處理系統，例如可信平臺模組（“TPM”）804。

一般來說，該可信平臺模組可為處理系統生成和維護密鑰。例如，TPM 可具備一系列加密能力，使得某些電腦進程可以在 TPM 環境（例如，硬體）中安全的執行。在這點上，該 TPM 可包括一個或複數個用於執行加密操作的加密處理器，其執行的加密操作包括加密、解密、認證和密鑰管理。有關 TPM 的規範由可信計算聯盟(Trusted Computing

Group) 定義。

一般，為存取由 TPM 管理的服務，用戶必須首先在 TPM 中登記其信用證明。這包括，例如，向 TPM 提供密碼。在這點上，TPM 可包括一個輸入設備（未標出），該輸入設備中用到了前面已經討論以及下面將要討論的一些安全輸入機制和技術（例如，直接連接、RFID、生物探測器和鍵盤等）。

隨後，當用戶想要存取由 TPM 所管理的服務時，該用戶必須首先向 TPM 認證其身份。這包括，例如，向 TPM 提供原始密碼。在這點上，處理系統 802 可包括一台輸入設備 806，通過鏈路 808 連接到 TPM。

某些實施例中，該鏈路可直接從輸入設備路由到 TPM，以確保資料通過該鏈路安全發送。例如，該鏈路上的資料不使用軟體常式例如作業系統呼叫來進行理由。此外，來自該鏈路的資料將不會存儲在也可以由系統中其他部件存取的資料記憶體上。例如，該資料不會通過軟體棧傳送，也不存儲在可以通過內部匯流排例如 PCI 匯流排存取的資料記憶體上。這樣一來，在輸入資訊發往 TPM 的過程中，不會受到已侵入系統的病毒和黑客等的威脅。某些實施例中，物理地將輸入設備 806 嵌入或連接到處理系統內/上，可以提供另外一級保護。

通過使用物理和加密技術，TPM 可以在其安全邊界內安全的使用和維護敏感資訊，例如信用證明。在安全邊界內完成對信用證明的驗證後（例如，將收到的信用證明跟先前登記的信用證明進行對比），TPM 804 就可以提供所請求的存取，或從另一處理實體獲取對服務的存取。

某些實施例中，用戶向 TPM 認證其身份以使用存儲在 TPM 安全

邊界內的密鑰。例如，圖 8 中的系統可用於存取存儲在本地資料記憶體（例如，文件記憶體 812）上的加密資料（例如，加密密碼）。在這種情況下，TPM 804 存儲有對加密資訊（例如，密鑰、安全關聯等）使其能對加密的資料進行解密。典型情況下，一旦用戶通過認證，TPM 在其安全邊界內使用該密鑰，然後將結果提供給用戶。例如，TPM 可將解密的資料（例如，媒體內容）或簽名的資料返回給用戶。通過這種方式，可以使用該密鑰而又不會將該密鑰以明文的形式暴露在 TPM

● 安全邊界的外部。

在 TPM 中密鑰的存儲空間不足的情況下，TPM 會將密鑰進行加密，然後將其傳送到外部的資料存儲部件（例如，文件記憶體 812）中。因此，即使文件記憶體 812 中的加密的資料檔案可以被系統中的其他部件所存取，加密資料的安全性仍然能得到保證，因為密鑰已經進行了加密。換句話說，敏感資訊只有在處於 TPM 的安全邊界內的時

● 某些實施例中，TPM 804 可控制通過網路介面 810 對一個或複數個資料網路 822 的存取。這裏，TPM 804 可向連接到網路的服務提供者提供網路認證信用證明（例如，證書），以向該服務提供者認證其身份。這些網路認證信用證明可安全地存儲在 TPM 804 的資料記憶體（未標出）中，或以加密的形式存儲在文件記憶體 812 中。

網路介面 810 可用於連接有線和/或無線網路。如此所述，可以使用加密技術來確保在 TPM 804 和其他連接到網路的設備之間所傳輸資料的安全性。因此，可使用一個網路連接來與密鑰管理器通訊，以獲

得密鑰資訊（例如，安全關聯）和對密鑰使用的授權。

輸入設備 814 是輸入設備的另一個實施例，用於向處理系統安全地提供資訊（例如，信用證明）。輸入設備 814 包括安全模組 818 和安全邊界內的密鑰 820，用來提供加密功能。例如，安全模組可用於對輸入到輸入設備的資訊（例如，信用證明）進行加密/簽名。通過這種方式，這些資訊可安全的發送（如虛線部分 816 所示）給 TPM 804。

安全模組 818 和可信平臺模組 804 可包括一些部件，並能執行一些在此介紹的操作來提供強大認證以及建立安全通道。例如，公共密鑰及相關的證書可公佈給安全模組 818，使得 TPM 可以使用本申請介紹的技術驗證輸入設備的真實性和安全性。這樣一來，就可以在這些部件之間建立安全通道 816，從而將 TPM 的安全邊界擴展至包括輸入設備 814 和該安全通道。

由於在各部件之間傳送的資訊可以通過這種方式進行保護，所以輸入設備 814 不必與處理設備安全地連接。因此，輸入設備 814 可以使用在各種應用中，即輸入設備處於處理系統 802 的遠端，並通過有線或無線介面例如網路與其相連。此外，輸入設備還可以使用在一種應用中，其中輸入設備可以通過一條不安全鏈路（例如，電腦的 USB 鏈路）連接 TPM。

某些實施例中，輸入設備 814 上的輸入機構（例如，鍵盤和感測器等）可以通過一種安全的方式與安全模組 818 連接。例如，該輸入機構可以與安全模組安裝在同一積體電路上。此外，這些部件可以實現在一個物理保護的封裝內。因此，輸入設備 814 的安全邊界可包括

該輸入機構、安全模組 818 和安全模組用來存儲加密資訊的外部記憶體（未標出）。這樣一來，輸入設備 814 可以提供一種更高級別的安全機構，以使用戶向 TPM 804 提供信用證明。

以下將結合圖 9—圖 12 對安全模組的幾個實施例所選的部件和操作進行更詳細的討論。某些實施例中，安全模組可提供多級密鑰資訊所需要的密鑰保護和管理（例如，實現密鑰的合適使用）。

此外，安全模組還可提供加密處理，例如為安裝了安全模組並使用加密服務的設備（例如，接入設備）執行加密、解密、認證、驗證和簽名等處理。例如，安全模組可安裝在需要特定形式的資料安全和認證等的終端用戶的用戶端設備上，例如蜂窩電話、筆記本電腦等。某些實施例中，安全模組可集成到這些設備的現有晶片上（例如，主處理器）。

安全模組可配置為安全邊界的一部分，並對後者進行加強。例如，該安全模組可被配置為永遠不允許明文密鑰離開安全模組或包含該安全模組的晶片。這樣一來，該安全模組就可以安全的集成到其他設備或系統上，而無需考慮位於安全模組外部的該系統是否是安全的。

通過這種方式，安全模組可以為用戶端設備提供更高的安全性和具備良好性價比優勢的遠端密鑰管理。該安全模組可提供和/或支援任何需要的加密處理。可以在設備中建立一個安全邊界來安全的維護和使用密鑰和密鑰資訊。系統可以通過該安全模組由遠端密鑰管理系統（例如，硬體安全模組和 TPM 等）進行安全管理。因此，可以使用相對較小的安全模組為終端用戶設備提供高級安全功能，並能將對該設

備其他部分的影響降到最低。

為支援這種密鑰使用和管理方法，安全模組提供了相應的機制，將一個或複數個密鑰安全的載入到該模組內，安全的存儲這些密鑰和安全的使用這些密鑰。圖 9 中所示的無狀態硬體安全模組 900 提供了這種機制。

無狀態模組 900 包括主控制器 906，用來控制該模組的全面操作。例如，該控制器可控制啟動操作、密鑰管理操作（如果適用的話）和資料及密鑰在該模組中的進出操作。該控制器可包括一個處理器和相關代碼（例如，ROM 908）和/或一個狀態機或其他硬體。該控制器和/或該無狀態模組中的任何其他部件可通過內部匯流排 930 與該無狀態模組中的其他部件進行通訊。

某些實施例中，主控制器 906 包括一個包含有 ROM 代碼的 RISC 處理器，執行用於控制該無狀態模組相關操作時所必須的多種命令。該主控制器模組還包括一個用來為內部匯流排 930 上每個從模組的位址進行解碼的位址解碼器。RISC 引擎可使用資料緩衝器 926 的受保護部分來作為臨時堆疊和臨時資料空間。

雙向外部介面 920 提供了一種機制，用來向該模組發送或從該模組接收密鑰和/或資料。例如，該外部介面包括可由控制器和連接到該無狀態模組的外部設備（例如，一台主機）寫入或讀取的寄存器。在這種情況下，可對控制器進行配置，使其永遠不向上述寄存器寫入某些資料（例如，未加密的密鑰）。

外部資料介面 920 可被一臺本地主機用來讀取全局寄存器，發佈

命令以及將資料傳送到資料緩衝記憶體 926 中，等待無狀態模組的處理。主控制器可通過全局寄存器模組 922 對外部介面進行控制。這些全局寄存器包括命令（“CMD”）、計時器和配置（“CONFIG”）寄存器。主控制器在全局寄存器模組和資料緩衝記憶體 926 之間傳輸資料。

命令介面直接向資料登錄和輸出寄存器提供流資料介面，其允許在資料的輸入和輸出過程中使用外部的 FIFO（獨立的 FIFO）。該介面使無狀態模組可以很容易的嵌入到基於分組的系統中。

某些實施例中，將要加密或解密的資料（例如，將要被處理的資料或密鑰資訊）可通過一個或複數個資料介面發往或發自無狀態模組 900。例如，資料介面 902 可用於將加密資料或密鑰（例如，由該模組進行瞭解密的資料）發送給加密加速器，反之亦然。此外，資料介面還可與生成的資料需要由無狀態模組進行加密的輸入設備（例如，感測器）連接。隨後，加密資料將通過外部介面 920 發往一個外部處理部件。

一個或複數個加密處理模組執行獲取或使用密鑰或加密處理流經該模組的資料所必須的任何加密處理。例如，可使用各個處理模組來執行非對稱密鑰演算法，例如 DSA、RSA、Diffie—Hellman（模組 914），密鑰交換協定或對稱密鑰演算法，例如 3DES、AES（模組 912），或認證演算法，例如 HMAC-SHA1（模組 910）。該加密處理模組可通過硬體中和/或使用一個執行存儲在資料記憶體（例如，ROM）上的代碼的處理器來實現。

一般，該實施例包括生成非對稱密鑰，用於與遠端設備建立安全通道，對從該模組發往遠端設備的資訊進行認證，反之亦然。這裏，該非對稱密鑰的私有部分維護在該晶片的安全邊界內。此外，該無狀態模組還包括一個將非對稱密鑰的公共部分導出的機構。例如，該公共值將載入到上述外部介面寄存器中，使其可在隨後被外部設備讀取。該公共密鑰值可以通過向無狀態模組發出一條公共密鑰讀取命令來從上述無狀態模組中讀取。作為對該命令的回應，該模組向該設備返回該公共密鑰值和任何不受保護的配置資訊（認證資料和產品配置資料等）。

某些實施例中，根身份密鑰用作非對稱密鑰的基礎。例如，無狀態模組的根密鑰可包括非對稱密鑰對（秘密或私有，公共），用於唯一的標識該無狀態模組。某些實施例中，該密鑰只用於數位簽名，以安全的標識無狀態模組。

某些實施例中，將有一個或複數個密鑰（例如，該模組的根密鑰、身份密鑰）被載入到無狀態模組中。這可以在晶片製造過程中，在晶片測試過程中，在 OEM（例如，電路板製造商）的製造過程中和在 OEM 的測試或為終端用戶安裝過程中實現。這一技術可用於載入對稱和/或非對稱密鑰。

某些實施例中，該無狀態模組可在其內部生成一個或複數個密鑰（例如，根密鑰，身份密鑰）。例如，該無狀態模組可包括一個亂數生成器（“RNG”）918 和其他為生成密鑰所必須的電路。這種實施例可提供增強的安全保護，使得在其中生成的密鑰永遠不會離開晶片的

安全邊界。

某些實施例中，設備身份密鑰包括一組隨機位元，用於為無狀態模組中的長時固定密鑰生成密鑰資訊。例如，RNG 918 可以使用內部亂數值生成一個亂數作為秘密初始種子。初始種子中位元的數量由系統所需要的密鑰熵的數量所決定。

某些實施例中，不會直接使用來自亂數生成器 918 的值。例如，在進行內部使用以及將該值發往外部的無狀態模組用作隨機值之前，先由主控制器使用 SHA-1 模組 910 對之進行後期處理。主控制器將在資料緩衝記憶體 926 中維護一個後期處理後的隨機位（用於密鑰生成和簽名）的高速緩衝記憶體。

亂數生成器 918 可以是一個“真正的”隨機源。例如，它可使用自由運行的振蕩器來捕捉熱雜訊作為隨機源。

無狀態模組還可包括一個私有（或機密性）非對稱密鑰對，用於通過中間不可靠的第三方（例如該第三方無權存取密鑰資訊）向無狀態模組設備傳送安全內容。某些實施例中，該機密性密鑰只用作對無狀態模組中的密鑰資訊進行解密。

上述密鑰（例如，根密鑰和身份密鑰等）可存儲在一個非易失性記憶體（“NVM”）916 中。該 NVM 包括，例如，一個一次性可編程（“OTP”）記憶體或電池供電記憶體（BBMEM），可位於晶片上，也可位於晶片外。

某些實施例中，片上 OTP 記憶體（如圖 9 所示）具備一定的優點。例如，在這種情況下，密鑰可以在設備中從物理上保護起來，不能被

輕易的改變或觀察到。此外，因為對密鑰的使用被限制在了晶片內部，該密鑰將不會以明文形式出現在晶片的外部。此外，這種 OTP 與無狀態模組的結合可使用標準 CMOS 制程來實現。這樣一來，無狀態模組可以很容易的集成到各種使用在終端用戶和其他設備中的現有晶片上。這種結合可提供一種高性價比的安全解決方案。

通過 COMS 實現的 OTP 記憶體的結構在以下文件有相應的公開：美國專利 6,525,955、6,693,819、6,700,176 和 6,704,236，以及申請日為 2002 年 12 月 20 日申請號為 09/739,952 的美國專利申請，本申請在此引用以上文件公開的全部內容。

根據外部編程訊號 VPP，主控制器 906 可通過編程介面對 OTP 進行編程。主控制器可確保（通過本地硬體加強）設備的密鑰、授權和配置資料只接受一次編程，也只能接受一次編程。

密鑰加密密鑰（“KEK”）高速緩衝記憶體 924 是一個單獨的存儲模組，其大小基於系統中所要求的 KEK 的數量而定。一般，它的大小足夠容納會話私有密鑰和一個非對稱密鑰組。

在執行任何不需要使用 KEK 密鑰的命令時，KEK 高速緩衝記憶體 924 都可以從硬體上得到保護。例如，提供給 KEK 高速緩衝記憶體的一個來自全局寄存器的訊號可顯示命令寄存器是處於鎖定還是活躍狀態，並包含一個請求 KEK 的命令。某些 KEK 高速緩衝記憶體位於 NVM 模組中，為無狀態模組實現長期密鑰。

主控制器可使用應用密鑰高速緩衝記憶體 904 來為內部加速核心（例如，公共密鑰核心 914 或 3DES 核心 912）提供加密和解密存儲

空間。當密鑰被無狀態模組命令或應用密鑰高速緩衝記憶體介面使用時，該應用密鑰高速緩衝記憶體可控制該密鑰過期。

總的來說，上述模組的性能、大小和功能可以進行適當的調整，以滿足系統的要求。例如，用於連接安全通道和密鑰管理器以傳輸和處理密鑰資訊（和/或策略）的基本加密功能可以僅僅達到最低處理性能級別。

在不用於密鑰管理時，位於無狀態模組中的加密加速器可用于進行應用資料處理。例如，用於電子商務應用的無狀態模組可用來保護 RSA 私有密鑰。這裏，安全通道所要求的公共密鑰加速度一般為最低值（小於 10 個操作/秒）。這樣一來，可將任何空閒的處理能力（例如，處理器的空閒周期）用於其他操作。

相比之下，一般的電子商務加速器所需要的公共密鑰加速度相對較高（大於 500 個操作/秒）。此種類型的應用要求使用專門設計的加密加速器以很高的速率來執行加密操作。

一個或複數個加密加速器可通過應用密鑰高速緩衝記憶體介面直接連接到無狀態模組上。一般來說，用於增加加密加速處理的應用密鑰高速緩衝記憶體介面被維護在安全邊界內。例如，該無狀態模組和加密加速器可在同一晶片上實現。通過這種方式，明文形式的密鑰將不允許離開安全邊界，包含公共密鑰加速器。然而，通過簡單的參考存儲在無狀態模組中的正確的 RSA 私有密鑰，外部應用程式還是可以像以往那樣使用公共密鑰加速器。

應用密鑰高速緩衝記憶體 904 還可以存儲外部加密加速處理器所

使用的密鑰資訊。例如，高速緩衝記憶體 904 可存儲解密後的應用密鑰（例如，在包含無狀態模組的設備上執行的應用所用到的 RSA 私有密鑰）。

無狀態模組對使用在遠端用戶端上的密鑰實施密鑰策略。該密鑰策略可由密鑰管理器為所有發送給無狀態模組的密鑰制定。該密鑰策略指出無狀態模組如何使用該密鑰。除使用策略以外，該無狀態模組還可以設置密鑰的生存周期。一般來說，密鑰的生存周期是從密鑰被載入到無狀態模組時起的一段相對時間。密鑰管理器能使用多級密鑰體系結構並實施生存周期策略來確保正確使用密鑰以及可在無狀態模組中廢止。

安全保證邏輯模組 928 對無狀態模組進行保護，防止其受到系統安全攻擊。在這點上，可以在無狀態模組和/或包含無狀態模組的晶片（和/或系統）中的其他部件上安裝幾個系統監視器。

某些實施例中，當檢測到攻擊時，保護電路將觸發無狀態模組的重啓。這一重啓將擦掉無狀態模組中的所有暫態資訊。例如，所有的密鑰高速緩衝記憶體位置將被清除。一個帶有特定資訊的中斷將提供給本地主機，基於該資訊，保護機制觸發了重啓。

低頻保護電路可確保無狀態模組的操作頻率不會低於指定的閾值，從而確保報時訊號寄存器的值在相關頻率的範圍內不會受到威脅。除了對報時訊號值進行保護，低頻保護電路還保證很難實現動態攻擊以試圖在無狀態模組的工作過程中讀取其中的值。在這種情況下，閾值越高，保護越好。

操作點保護電路可確保無狀態模組中的所有邏輯都能按照預先為所有處理、電壓和溫度條件（或穿過所有操作點的）設計的那樣運行。該保護電路可確保即使在無狀態模組中的計時路徑被攻擊的情況下，攻擊者也不能改變操作點。

在處理過程中可使用監視計時器模組來確保命令可以在預期的時間段內執行完畢。無論命令（或子命令如公共密鑰操作）是否開始執行，主控制器都會對該計時器進行設置。設定的時間取決於所期望的
● 最大命令長度。如果監視計時器的值到了 0，就向無狀態模組發出重啓命令。該監視計時器不能關閉，並且爲了避免清除無狀態模組的內容，主控制器必須定期向其中寫入資料。當無狀態模組正在從來自主機的輸入中接收命令時，該監視計時器將被暫停。

重啓監視器可提供特定的保護，來防止多種重啓攻擊。該重啓監視器使用一個基於報時訊號寄存器增量的計時器，在允許例如不止 16 次的重啓發生之前，請求至少一個報時訊號。如果在該報時期間發生
● 了超過 16 次重啓，那麼在釋放第 16 次重啓之前，該無狀態模組將請求至少兩次報時訊號。在對 NVM 進行適當的編程之前，該重啓保護處於無效狀態。例如，在生產測試過程中其處於無效狀態。

本發明提供有一種硬體保護機構，用於當無狀態模組在開啓/關閉外部介面之間轉換時進入和退出安全狀態。無狀態模組啓動後進入安全狀態時，該外部介面處於關閉狀態。這就是說，該介面由硬體鎖定。一旦重啓並自檢完畢，主控制器將順序的執行一系列命令，退出安全狀態而進入用戶狀態。某些實施例中，這些命令要求將一組預先定義

的連續指令的執行過程寫入到非連續位址中。

該硬體將對序列中每一步命令所使用的執行時間進行追蹤，並確保這些命令在精確的時鐘周期內按照所要求的順序執行，並寫入到所要求的位址中。在退出邏輯完成後，該硬體會將相關模式設定到用戶模式。在用戶模式下，該硬體將鎖定主控制器對所有內部模組的存取，除了資料緩衝區和資料登錄/輸出寄存器之外（即僅僅需要將資料傳送給設備的模組）。

● 一旦將這些命令移至資料緩衝區，主控制器就會順序的執行一系列命令以返回到安全狀態。該序列同樣通過硬體模組進行追蹤和實現，並進入到安全模式下。同時，還通過硬體確保了主控制器通過正確的入口位址進入安全模式。

可使用額外的位對主控制器 ROM 908 進行編程，來指示哪些指令是有效的代碼入口和代碼出口點。無論何時主控制器進行非序列代碼讀取，指令代碼入口/出口點都會在硬體中實現。這種機制確保了攻擊者很難繞過代碼的特定部分而進入主控制器。因此，想要在程式執行過程中通過產生隨機跳來對該模組實施成功攻擊，在實際上幾乎是不可能的。

為降低成本和封裝空間，無狀態模組不負責與通訊協定有關的處理工作。替而代之，將由相關的設備驅動程式（或集成的處理器）來處理這方面的要求。

在另一個實施例中，無狀態模組將分配到長期密鑰。在這種情況下，無狀態模組不需要與前端伺服器（例如，密鑰管理器）進行連接。

如圖 10 所示是無狀態模組的一個實施例執行的操作的流程圖。如步驟 1002 所示，當無狀態模組在生產後第一次初始化時（例如，在對晶片的最後測試中），主控制器將控制亂數生成器 918 生成一個亂數，作為種子提供給加密處理器，以生成一個公共—私有密鑰對。

主控制器將私有（身份）密鑰存儲在非易失性記憶體 916 中，並永遠不會將該密鑰導出到該模組的安全邊界外（步驟 1004）。例如，某些實施例中，該密鑰永遠不會離開該無狀態模組所在的晶片。某些實施例中，在存儲到晶片外非易失性記憶體中之前，該密鑰將被加密。

該無狀態模組還保存相應的公共密鑰，並且在收到請求後，將該公共密鑰導出（步驟 1006），因此，設備製造商（或某些其他的可信實體）可將公共密鑰連同證書一起發佈給公共伺服器。

隨後，可將無狀態模組可佈置在可通過網路或一些其他的鏈路連接到其他設備（例如，密鑰管理器）的計算設備中。如步驟 1008 所示，無狀態模組可使用其私有密鑰建立與已存取到該無狀態模組的公共密鑰的密鑰管理器之間的安全通訊通道。

如步驟 1010 所示，密鑰管理器通過該安全通訊通道將密鑰傳送給無狀態模組。例如，密鑰管理器和無狀態模組可協商獲得額外的密鑰，用於兩個部件之間的安全通訊。此外，密鑰管理器還可以通過無狀態模組將密鑰傳送給遠端的用戶端。例如，密鑰管理器可以為結合有該無狀態模組的用戶端生成一個私有會話密鑰（ K_{a-priv} ）。如上所述，在將這些密鑰發送給用戶端之前，密鑰管理器使用無狀態模組的公共密鑰（ K_{dc-pub} ）或某些協商的密鑰對該密鑰進行加密。

如步驟 1012 所示，該密鑰在無狀態模組的安全邊界內進行解密。例如，無狀態模組中的加密處理器會對這些密鑰進行解密。可選擇地，與無狀態模組位於同一晶片上的另一加密處理器也可對該密鑰進行解密。

如步驟 1014 所示，無狀態模組隨後在安全邊界內使用這些密鑰。例如，無狀態模組中的加密處理器使用該密鑰對其他密鑰（例如，會話密鑰）進行解密。此外，無狀態模組可在安全邊界內實施密鑰策略（步驟 1016）。

某些實施例中，如步驟 1018 所示，無狀態模組向安全邊界內的一個或複數個加密加速器提供密鑰。例如，這些加密加速器可以與該無狀態模組位於相同的晶片上。

圖 11 所示是無狀態安全鏈路模組 1100 的一個實施例。該實施例包括圖 9 中實施例的功能性的一個子集。具體來說，這一實施例只使用對稱密鑰來提供資料加密和解密等。這種配置的一個優勢是，其可以在其他設備中實現，對這些設備的成本和大小所產生的影響更小。

在一個典型的應用中，圖 11 中的實施例可用於從最初產生資料的輸入設備那裏取得資料，然後安全的提供給使用該資料的接收設備。這個過程包括對資料進行加密，使其不會以明文形式出現，和/或對資料進行簽名，以向接收設備證明該資料是來自特定的輸入設備。

例如，無狀態模組可集成到感測器（例如，生物感測器如指紋識別器）的晶片上。這裏，無狀態模組可用于對感測器生成的資訊進行簽名和/或加密。隨後，無狀態模組可安全地將資訊傳送給使用該資訊

的接收設備。在這種情況下，該接收設備可通過指紋比較來控制對資料或服務的存取。

某些實施例中，感測器資料總是維護在安全邊界內。首先，將無狀態模組結合在感測器晶片上，這些資訊可在離開晶片的硬體邊界之前進行加密。其次，通過交換對稱密鑰，無狀態模組建立與接收設備之間的一條安全通道。通過這種方式，這些資訊可安全的發往接收設備。最後，接收設備將使用現有方式或本申請中介紹的技術得到保護。

● 上述後一種方案的一個例子中，接收設備包括一個上述圖 9 中的無狀態模組。在這種情況下，接收設備可以使用其他密鑰將資訊安全的傳送給遠端系統。該遠端系統可以是網路接入設備，能基於用戶的信用證明如用戶指紋實現對網路的存取。

其他實施例中，只需認證資料是源於特定的輸入設備即可。例如，系統可作出規定以確保指紋資料流程的副本不會在稍後被重放。在這種情況下，沒必要對資訊進行加密，只需要確保該資訊來自特定的感測器。在這種情況下，對資料的一個簡單簽名就可以提供足夠的安全性。

● 為提供一種適用於多種輸入設備的高性價比解決方案，圖 11 中的無狀態模組的功能性相比圖 9 中實施例進行了一定的簡化。該無狀態模組包括一個主控制器 1106 和一個外部介面 1112，用於在與密鑰管理器建立安全鏈路時實現非對稱密鑰操作的執行。因此，控制器 1106 包括有生成並驗證其密鑰的有效性的電路。此外，該模組還包括保證邏輯 1120，與上述的保證邏輯相同。

但是，因為該模組只使用了單個對稱密鑰，所以圖 11 中的實施例不能提供圖 9 中所描述的許多功能。例如，該模組不需要為額外的密鑰提供管理能力（例如，密鑰策略的實施）和資料存儲（例如，應用密鑰高速緩衝記憶體）。因為只存儲一個身份密鑰和一個對稱密鑰，所以非易失性 ROM（“NVROM”）1110 可以更小。

此外，因為該模組只對來自資料流程介面的資料執行對稱加密處理，所以不需要圖 9 中所示的某些或全部的專用加密處理器（例如，公共密鑰處理和 3DES）。例如，在啟動後，該模組只執行一次非對稱密鑰操作。此外，無狀態模組無需驗證資料接收方的真實性。因此，餘下的加密處理操作可由主控制器 1106 執行。在這種情況下，加密演算法（例如，DH，DSA，3DES 和 AES）的應用代碼可存儲在 ROM 1108 中。

圖 11 所示的實施例可以通過使用 SHA-1 演算法簽名來加密輸入資料流程（DI）。為此，可提供一個單獨的處理模組 1104 來執行該操作。該處理模組簽名後的輸出提供一資料流程（DO），並通過資料介面 1102 將之發送給接收設備。在一個同樣也對資料流程進行加密的實施例中，可提供一個專用處理模組（未標出）來執行例如對稱加密演算法。

圖 12 所示為無狀態安全鏈路模組的一個實施例執行的操作的流程圖。如步驟 1202 至步驟 1208 所示，無狀態安全鏈路模組生成一個公共-私有密鑰對，將私有（例如，身份）密鑰存儲在安全邊界內的非易失性記憶體中，導出公共密鑰，並在其與密鑰管理器之間建立一

條安全通訊通道。

如步驟 1210 所示，密鑰管理器通過該安全通訊通道向無狀態安全鏈路模組傳送對稱密鑰。例如，密鑰管理器發送對稱密鑰，用於無狀態安全鏈路模組對從輸入設備接收到的資料進行加密和/或簽名。隨後，加密處理器對這些密鑰進行解密（步驟 1212），然後將解密後的密鑰存儲在無狀態安全鏈路模組的安全邊界內（步驟 1214）。

如步驟 1216 所示，無狀態模組從輸入設備接收將要加密的資料。

● 如上所述，該輸入設備可以是，例如，生物感測器和照相感測器等，也可以是任何其他的需要對資料進行認證或需要將資料安全的發送給另一設備（例如，遠端設備）的設備。

如步驟 1218 所示，無狀態模組在安全邊界內使用對稱密鑰對資料進行加密。隨後，如步驟 1220 所示，無狀態模組將加密後的資料發送給遠端設備。

● 有關安全模組的其他細節，在申請日為 2005 年 6 月 21 日、申請號為 10/_____、代理案號為 No.53028/SDB/B600 的美國專利申請“無狀態硬體安全模組”中已有公開，並在此被本申請全文引用。

需要明確的是，本申請中介紹的各個元件和功能特點可結合入系統中而獨立於其他元件和功能特點。例如，使用本申請的技術的系統，可以包括這些元件和功能特點的多種組合。因此，並非本申請中介紹的所有元件和功能特點都使用在每一個這種系統中。

本發明的不同實施例可以包括多種硬體和軟體處理元件。在本發明的某些實施例中，根據本發明構建的系統使用了如控制器、狀態機

和/或邏輯等硬體元件。在本發明的某些實施例中，在一個或複數個處理設備中執行的代碼如軟體或固件可以用來實現一個或複數個前述的操作。

所述的元件可以在一個或複數個積體電路上實現。例如，某些實施例中，幾個這樣的元件結合在一個積體電路中。某些實施例中，一些元件可以實現為一個積體電路。某些實施例中，複數個元件可以實現為幾個積體電路。

● 本申請中提及的元件和功能可以通過各種不同方式進行連接/聯結。使用的方式部分的取決於這些元件彼此之間是否是獨立的。某些實施例中，附圖中連接線表示的某些連接可以位於一個積體電路內、一塊電路板上和/或通過底板連接到其他電路板上。某些實施例中，附圖中連接線表示的某些連接可包含資料網路，例如本地網路和/或廣域網（例如因特網）。

● 本申請中提及的訊號可以以幾種形式出現。例如，某些實施例中，訊號是通過電纜傳輸的電訊號，通過空中或在光纖上傳輸的光脈衝，或通過空中傳輸的電磁輻射（如射頻或紅外線）。

在訊號中還可以包含一個或幾個訊號。例如，一個訊號可以由一系列的訊號組成。同樣，一個微分訊號包括有兩個補充訊號或一些其他訊號的組合。此外，一組訊號在這裏可視為一個訊號。

本申請中提及的訊號也可以以資料的形式出現。例如，某些實施例中，一個應用程式可以發送一個訊號給另一個應用程式。這一訊號可以存儲在資料記憶體中。

本申請中介紹的資料記憶體可以使用多種設備來實現。例如，資料記憶體可以包括快閃記憶體、一次性可編程（OTP）記憶體或其他類型的資料存儲設備。

本申請中提及的元件和功能可以進行直接或間接的連接/聯結。因此，某些實施例中，在連接/聯結的各元件之間可以有，也可以沒有中間設備（例如，緩衝器）。

總的來說，本發明總的涉及一種改進的認證系統和方法。雖然本申請中結合附圖詳細介紹了本發明的某些具體實施例，可以理解這些實施例僅僅是為了解釋本發明，而不是對本發明的限制。特別應當認識到的是，本發明所揭示的內容可以應用於多種系統和處理中。因此也應該認識到，可以對本發明的實施例作出各種修改而不脫離本發明的範圍。因此本發明不限於所公佈的特定實施例或配置，其包括申請專利範圍所定義的本發明的精神和範圍內的所有替換、修改和改進實施例。

【圖式簡單說明】

圖 1 是根據本發明的用戶認證系統的一個實施例的方框示意圖；

圖 2 是根據本發明執行的用戶認證操作的一個實施例的流程圖；

圖 3 是根據本發明的用戶認證系統的一個實施例的方框示意圖；

圖 4 是根據本發明執行的用戶認證操作的一個實施例的流程圖；

圖 5 是根據本發明的基於鄰近技術的認證系統的一個實施例的方框示意圖；

圖 6 是根據本發明執行的基於鄰近技術認證操作的一個實施例的流程

圖；

圖 7 是根據本發明的接入設備的一個實施例的方框示意圖；

圖 8 是根據本發明的處理系統的一個實施例的方框示意圖；

圖 9 是根據本發明的安全模組的一個實施例的方框示意圖；

圖 10 是根據本發明執行的操作的一個實施例的流程圖；

圖 11 是根據本發明的安全模組的一個實施例的簡化框圖；

圖 12 是根據本發明執行的操作的一個實施例的流程圖。

【主要元件符號說明】

系統	100	接入設備	102、104
伺服器	106	信用證明	108
密鑰管理器	110	安全邊界	112
非對稱身份密鑰	114	安全通道	116
不安全的鏈路	118	信用證明登記機制	120
安全資料記憶體	122	加密處理器	124
密鑰	126	加密處理器	128
服務	130	信用證明	132
安全邊界	136	密鑰 A	140
加密處理器	142	非對稱身份密鑰	144
安全通道	146	不安全鏈路	148
密鑰 B	150	模組	204~212
廣域網	302	網路橋接器	304
網路印表機	312	語音電話	314

筆記本電腦	316	個人數位助理	318
個人娛樂設備	320	電話	322
無線手持機	324	個人電腦	326
鍵盤	328	滑鼠	330
系統	500	接入設備	502
伺服器	504	RFID 讀取器	506
安全模組	508	公共積體電路	512
● 資料記憶體	514	權杖	516
密碼加密通訊通道	518	加密處理器	522
密鑰管理器	524	通訊鏈路	526
信用證明	528	訊號	530
接入設備	700	積體電路	702
輸入設備	704	安全模組	706
密鑰	708	無線介面	710
● 天線	712	資料記憶體	714
無線訊號	718	系統	800
處理系統	802	可信平臺模組	804
輸入設備	806	鏈路	808
網路介面	810	文件記憶體	812
輸入設備	814	安全通道	816
安全模組	818	資料網路	822
無狀態模組	900	資料介面	902

I274500

高速緩衝記憶體	904	主控制器	906
ROM	908	模組	910
3DES 核心	912	公共密鑰核心	914
非易失性記憶體	916	亂數生成器	918
雙向外部介面	920	高速緩衝記憶體	924
資料緩衝記憶體	926	安全保證邏輯模組	928
內部匯流排	930	主控制器	1106
● ROM	1108	非易失性 ROM	1110
外部介面	1112		

五、中文發明摘要：

本發明公開了一種用於用戶向系統內的部件認證其身份的技術。用戶可安全有效的將信用證明輸入這些部件中。信用證明提供給系統中的伺服器，並向其提供強大的認證以表明該信用證明來自安全部件。隨後，伺服器向用戶向其出示信用證明的每個安全部件發放密鑰，自動建立一個網路。

六、英文發明摘要：

Techniques are provided for users to authenticate themselves to components in a system. The users may securely and efficiently enter credentials into the components. These credentials may be provided to a server in the system with strong authentication that the credentials originate from secure components. The server may then automatically build a network by securely distributing keys to each secure component to which a user presented credentials.

十、申請專利範圍：

1、一種通訊方法，包括：

向複數個接入設備認證至少一個用戶；

建立包括有所述接入設備的至少一個網路。

2、如申請專利範圍第 1 項所述的通訊方法，其中，所述認證包括向所述接入設備提供至少一個信用證明。

3、如申請專利範圍第 2 項所述的通訊方法，其中，所述方法進一步包括對所述至少一個信用證明進行密碼簽名。

4、如申請專利範圍第 3 項所述的通訊方法，其中，所述方法進一步包括使用數位證書以對所述至少一個簽名後的信用證明進行認證。

5、一種通訊方法，包括：

向複數個接入設備認證複數個用戶；

建立包括有所述接入設備的複數個網路。

6、一種向設備認證用戶的方法，包括：

● 定義與一個接入設備相關聯的安全邊界；

直接向所述安全邊界內提供至少一個信用證明，以向所述接入設備認證一個用戶。

7、一種用於存取服務的方法，包括：

接收與用戶相關聯的信用證明；

對所述信用證明進行認證；

將所述認證後的信用證明提供給服務提供者；

回應所述認證後的信用證明，接收來自服務提供者的至少一個密鑰；

使用所述至少一個密鑰對服務進行存取。

8、一種通訊系統，包括：

複數個接入設備，用於接收認證資訊，每個接入設備包括至少一個用於對認證資訊進行簽名的加密處理器；
一個接入伺服器，用於接收所述簽名的認證資訊，所述接入伺服器包括至少一個加密處理器以爲所述接入設備生成至少一個密鑰，所述接入伺服器依據所述簽名的認證資訊向所述接入設備提供所述至少一個密鑰。

9、如申請專利範圍第 8 項所述的通訊系統，其中，所述認證資訊包括至少一個信用證明。

10、一種接入設備，包括：

安全邊界內的至少一個加密處理器；

至少一個輸入設備，用於直接向所述安全邊界內提供認證訊號。

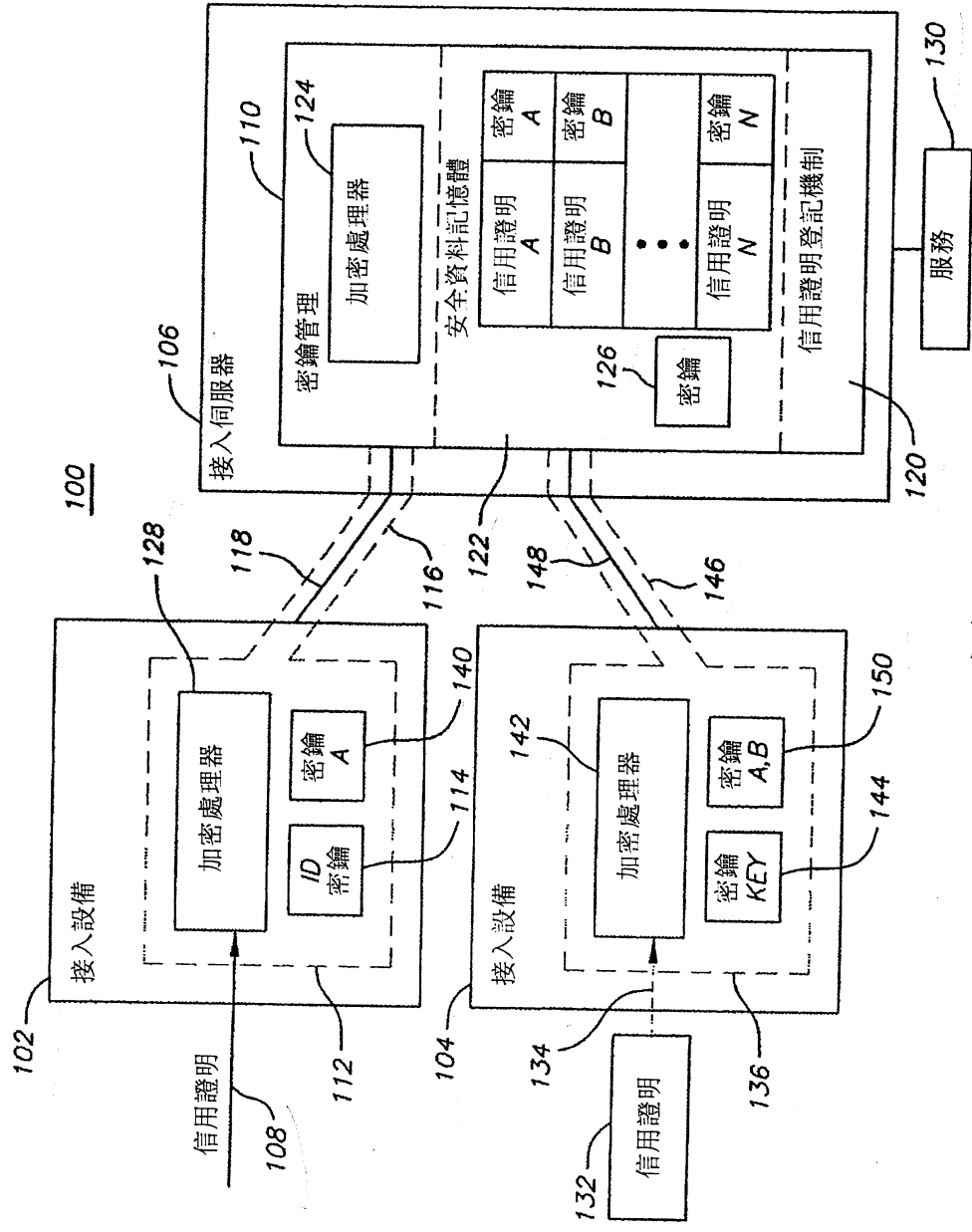


圖 1

(02)

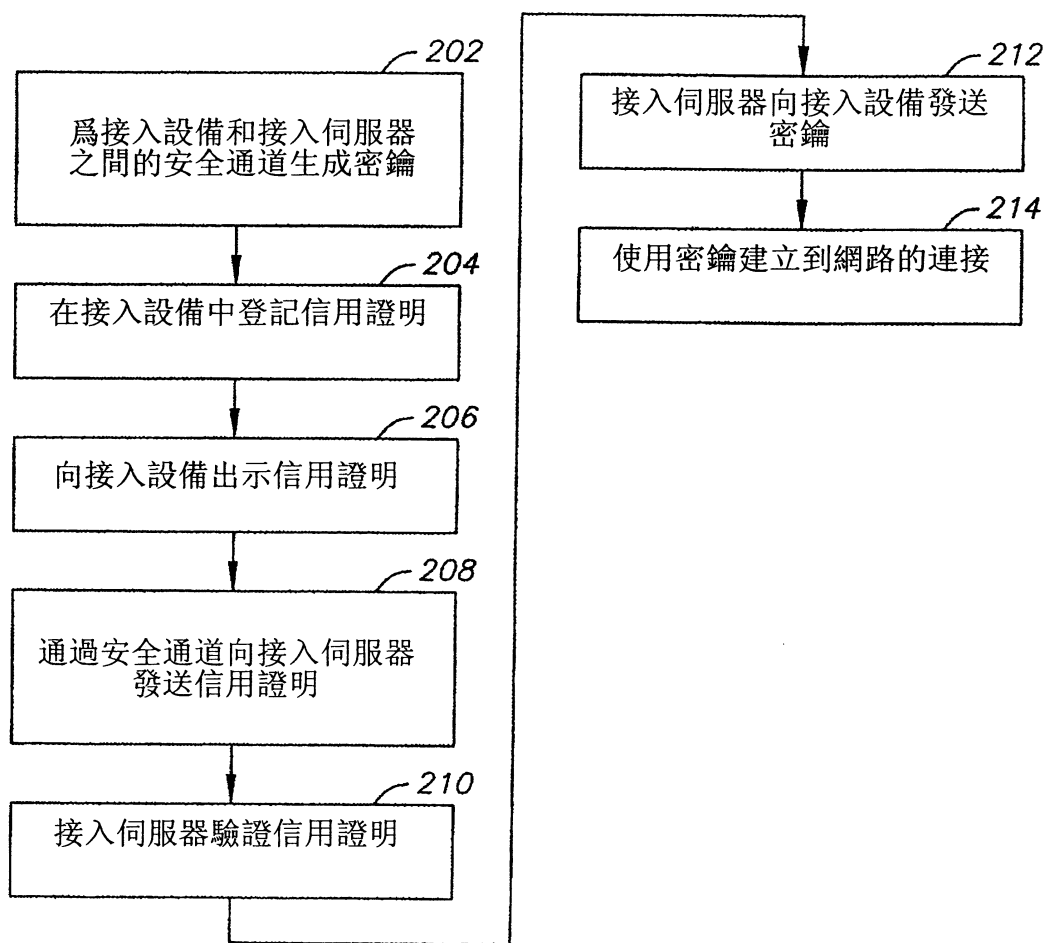


圖 2

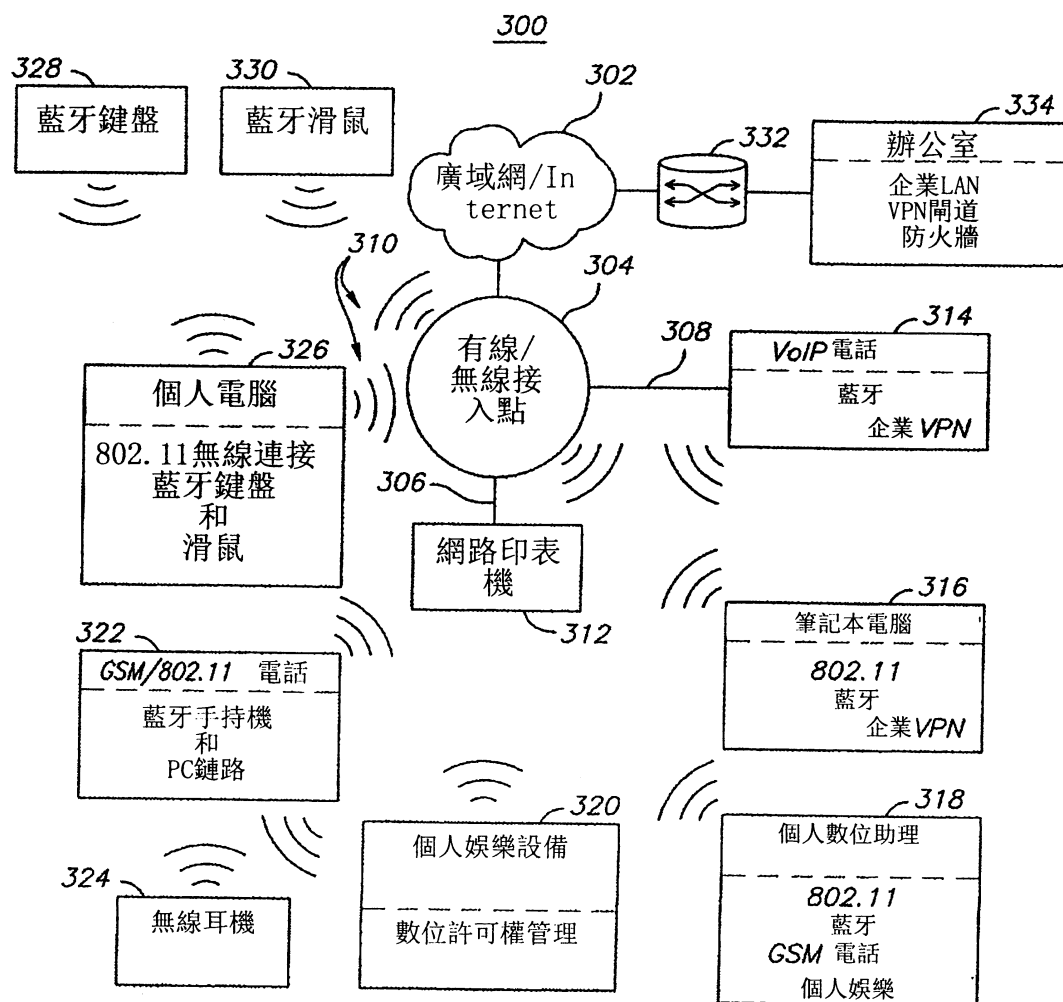


圖 3

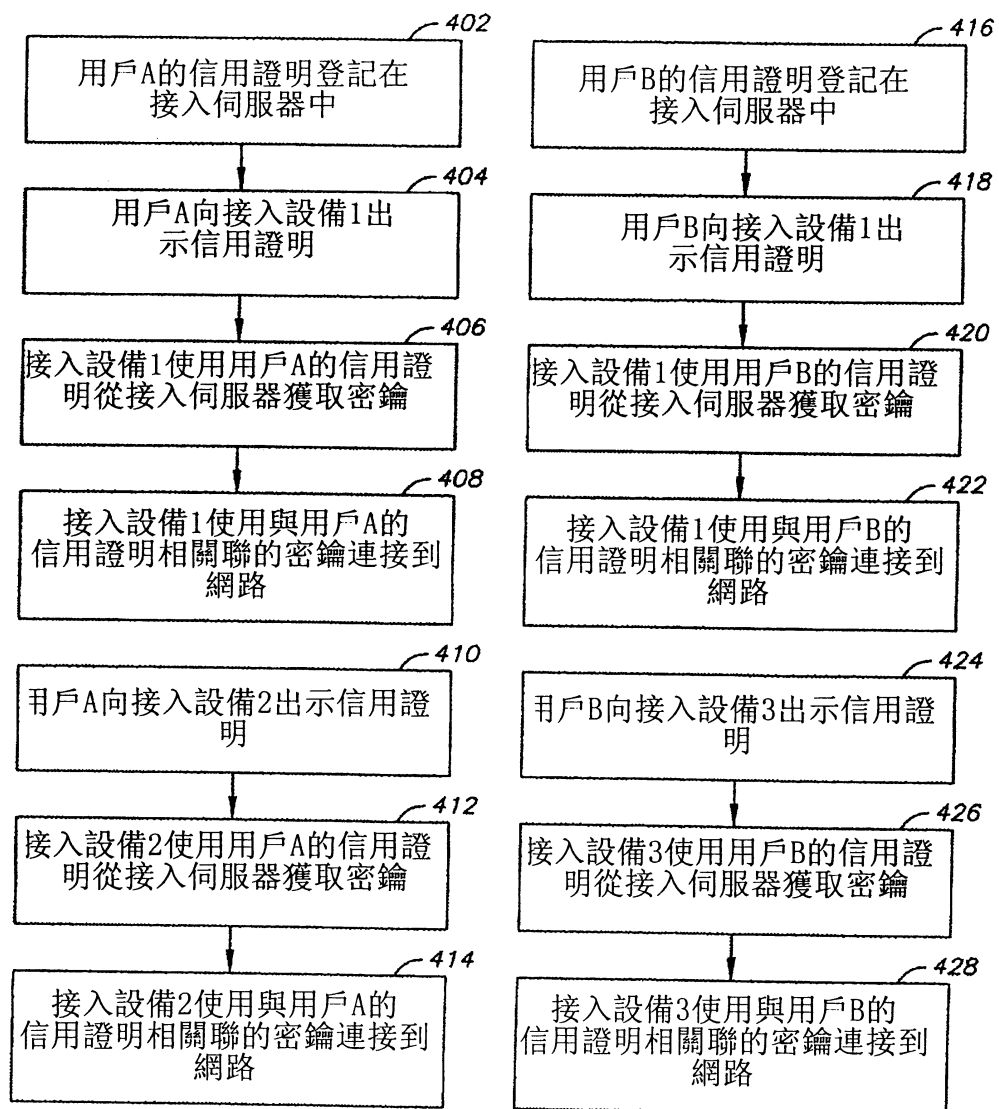


圖 4

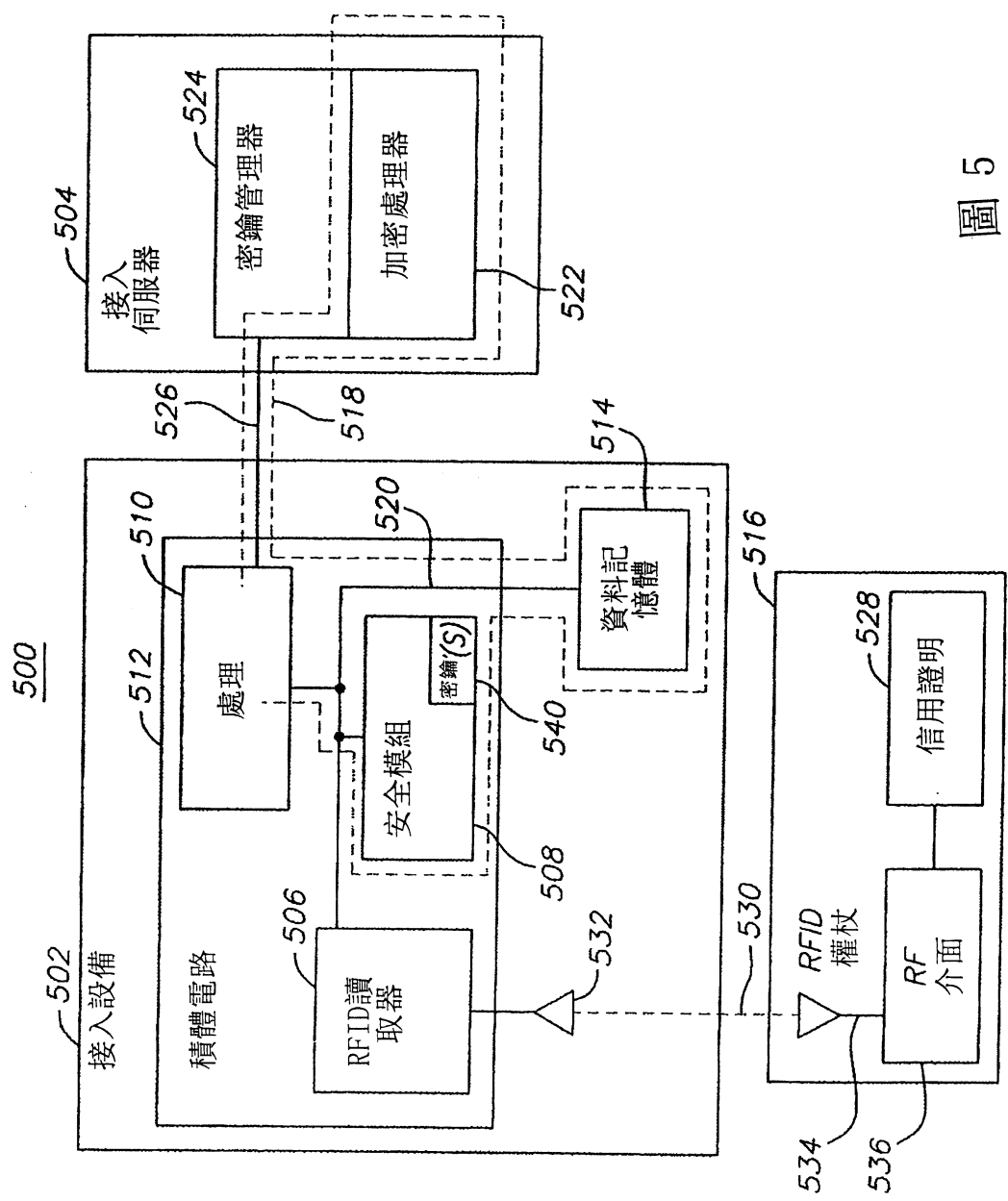


圖 5

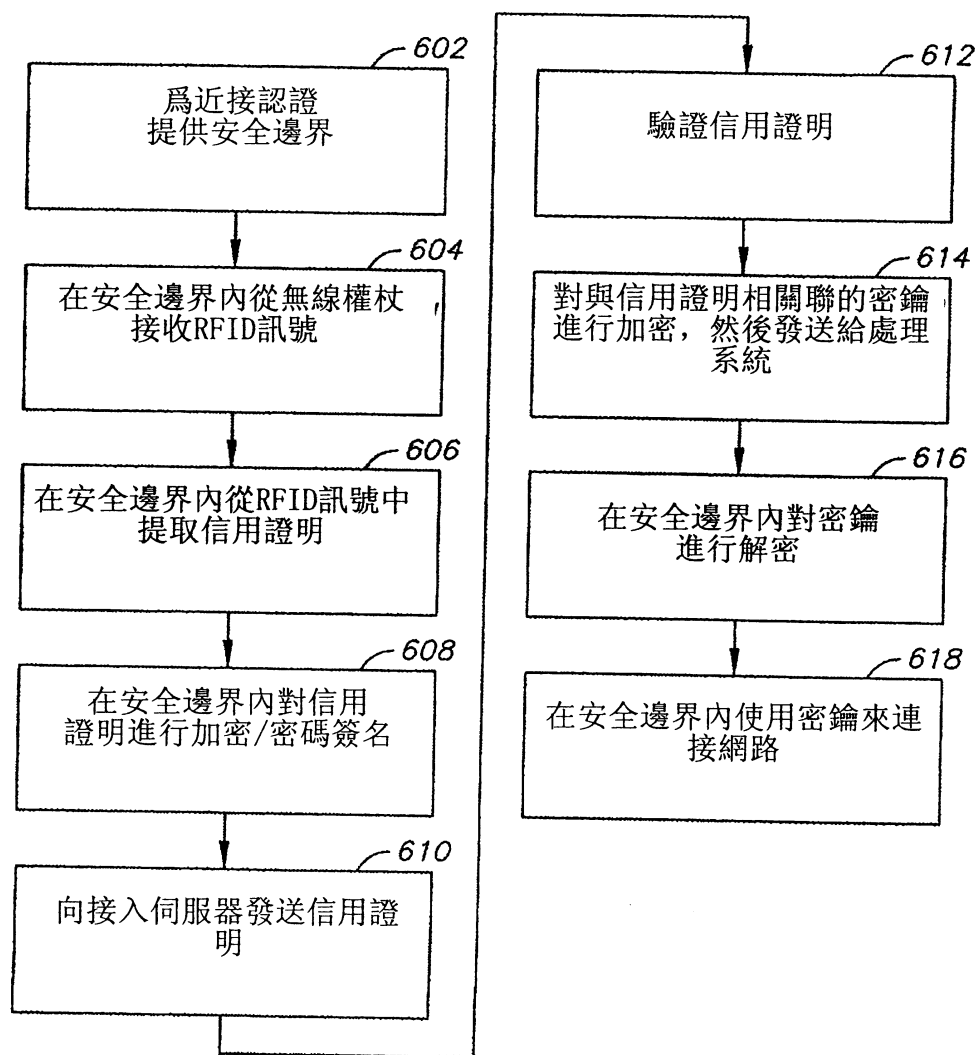


圖 6

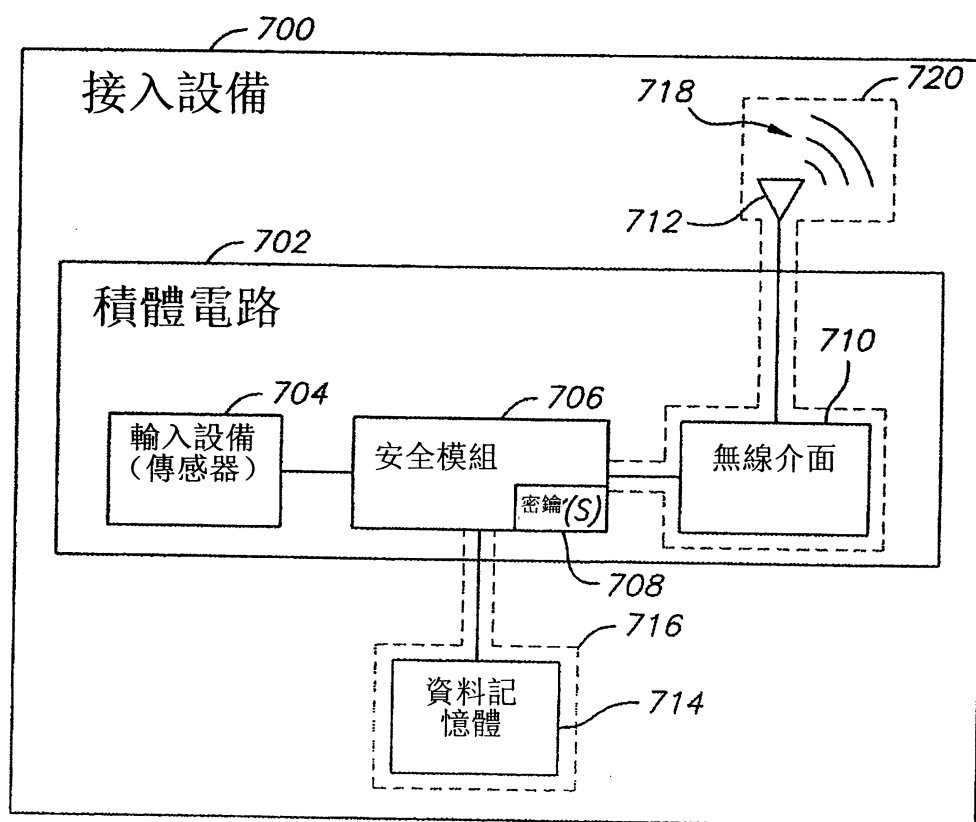


圖 7

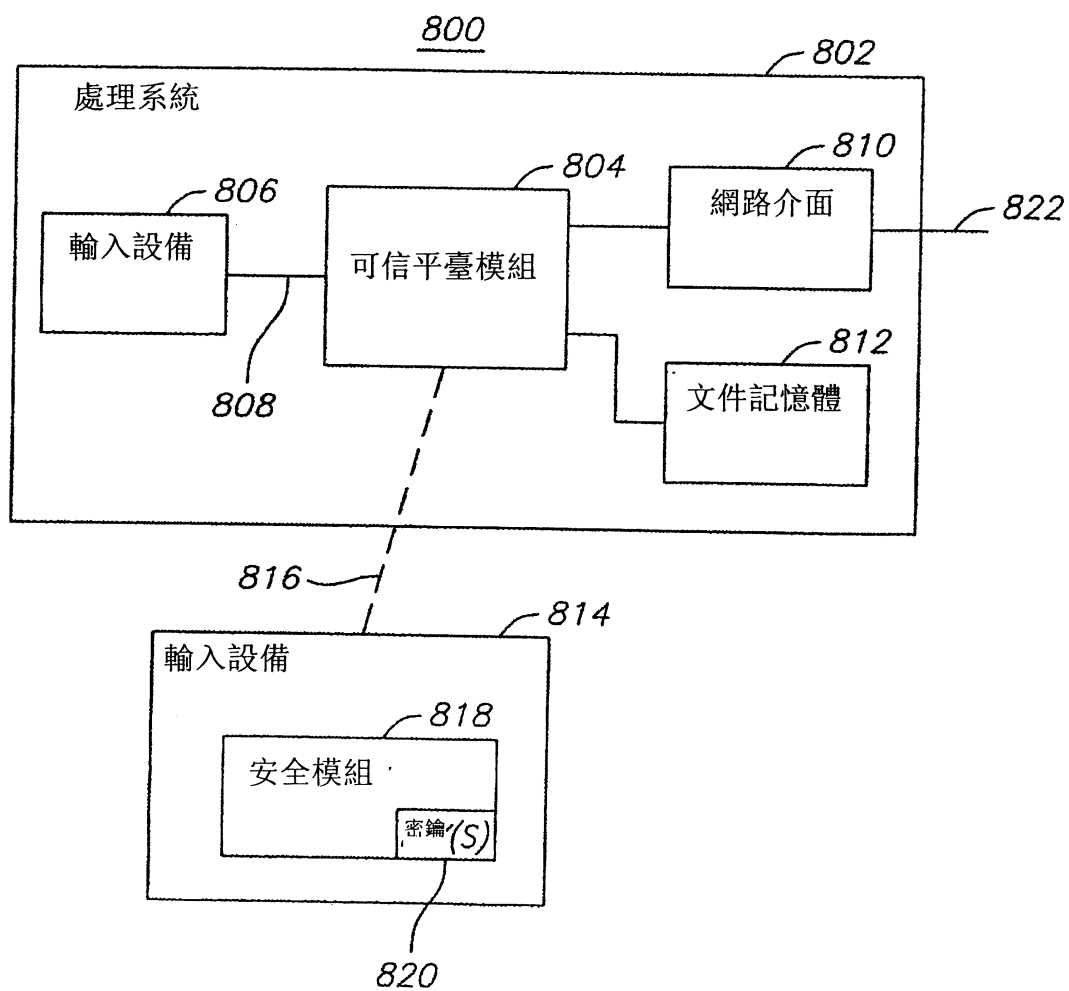


圖 8

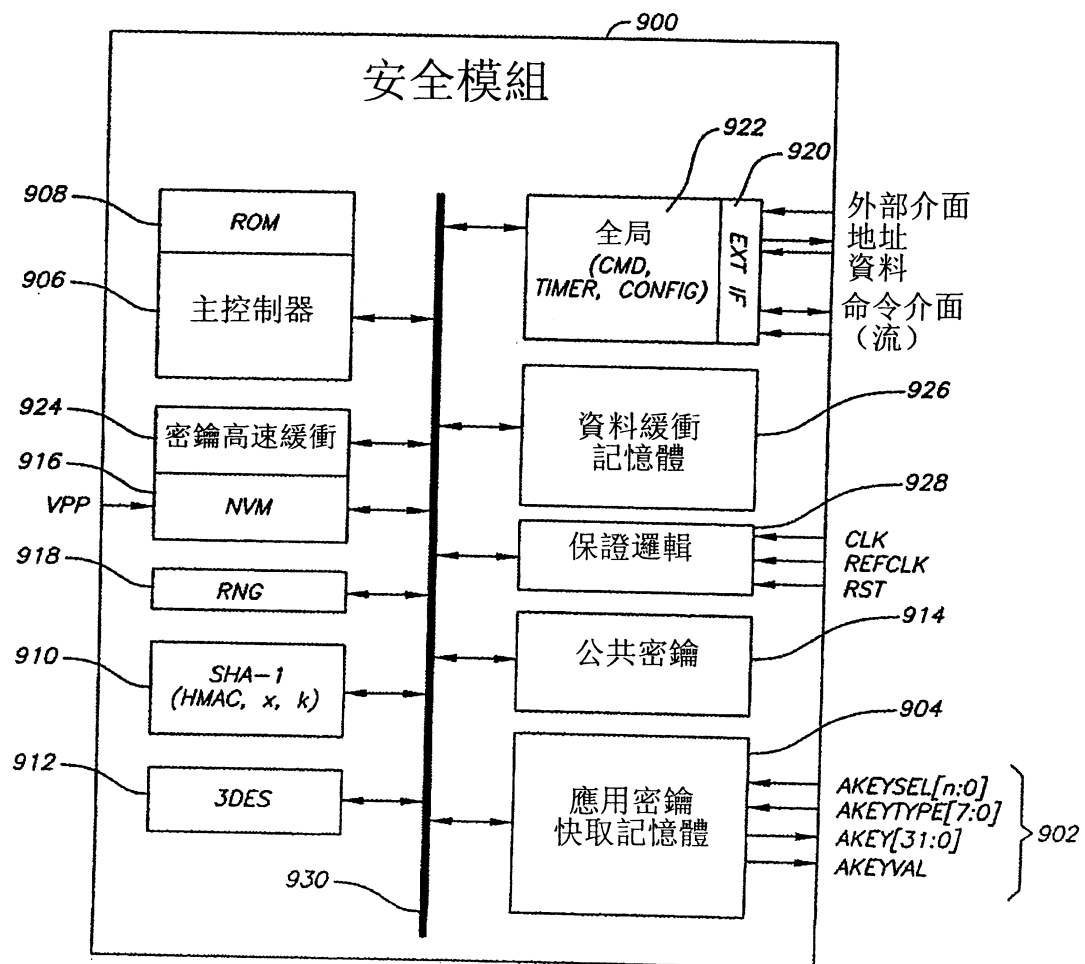


圖 9

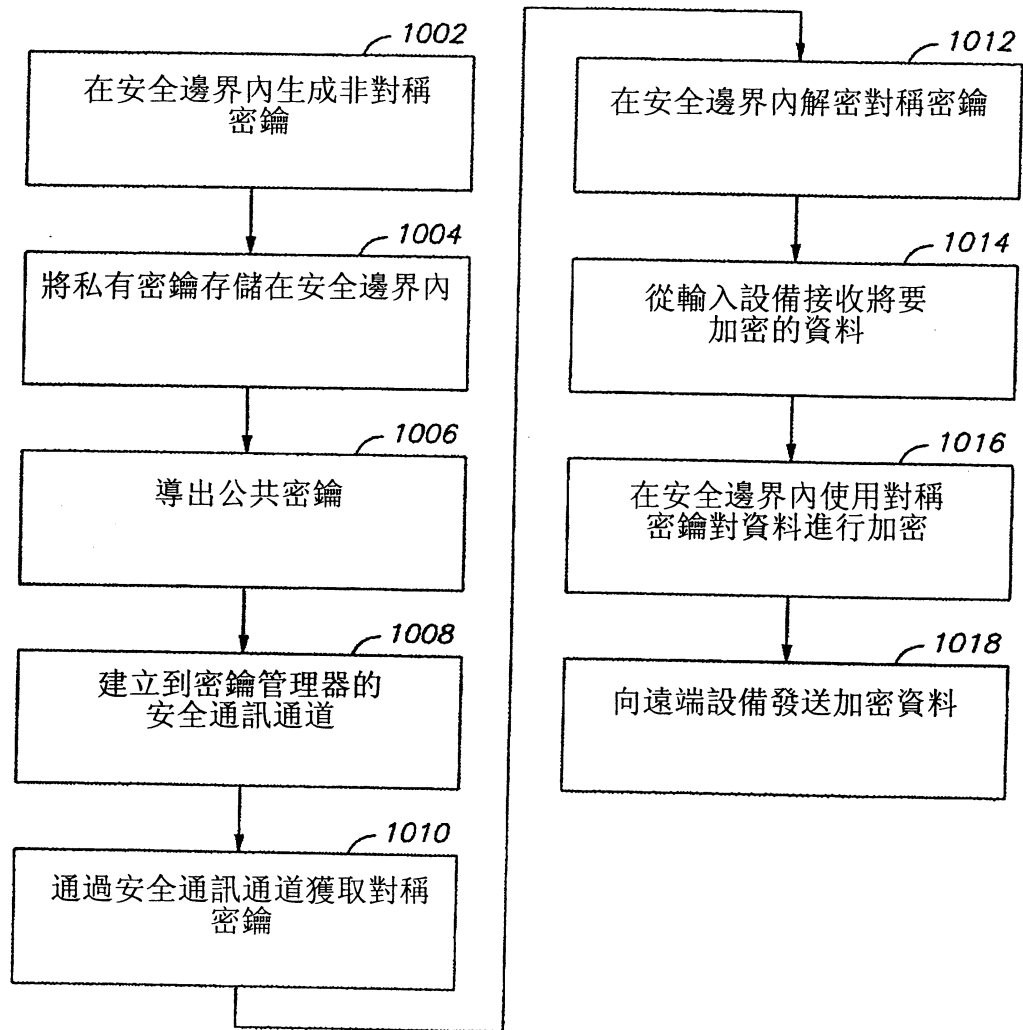


圖 10

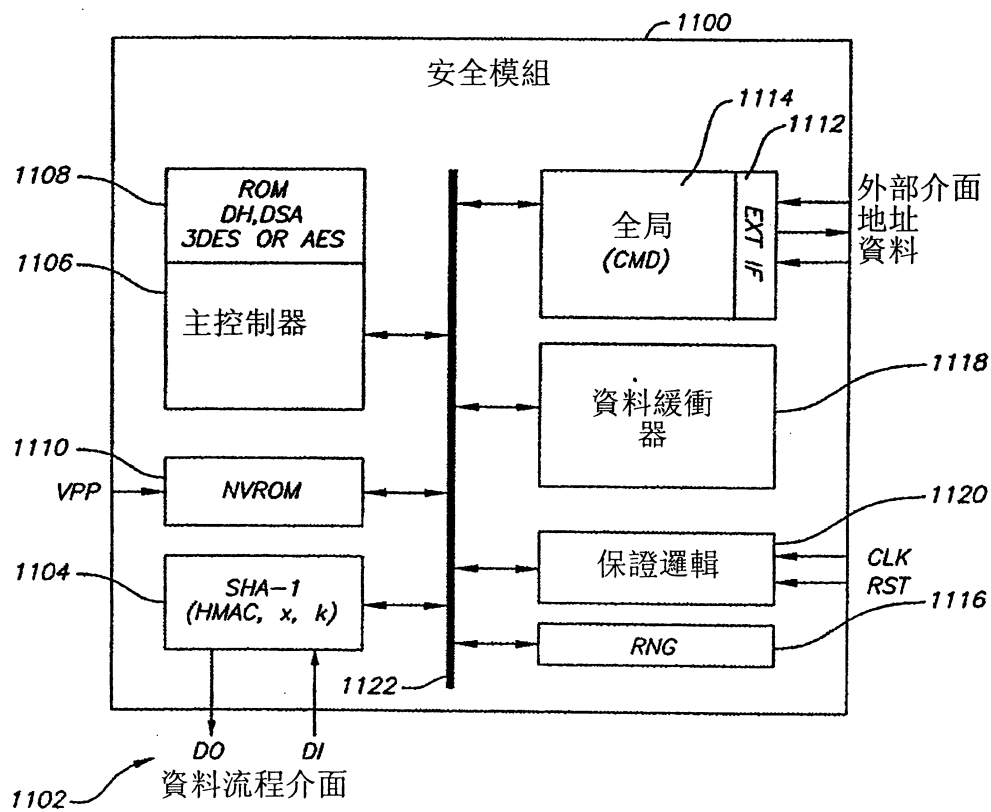


圖 11

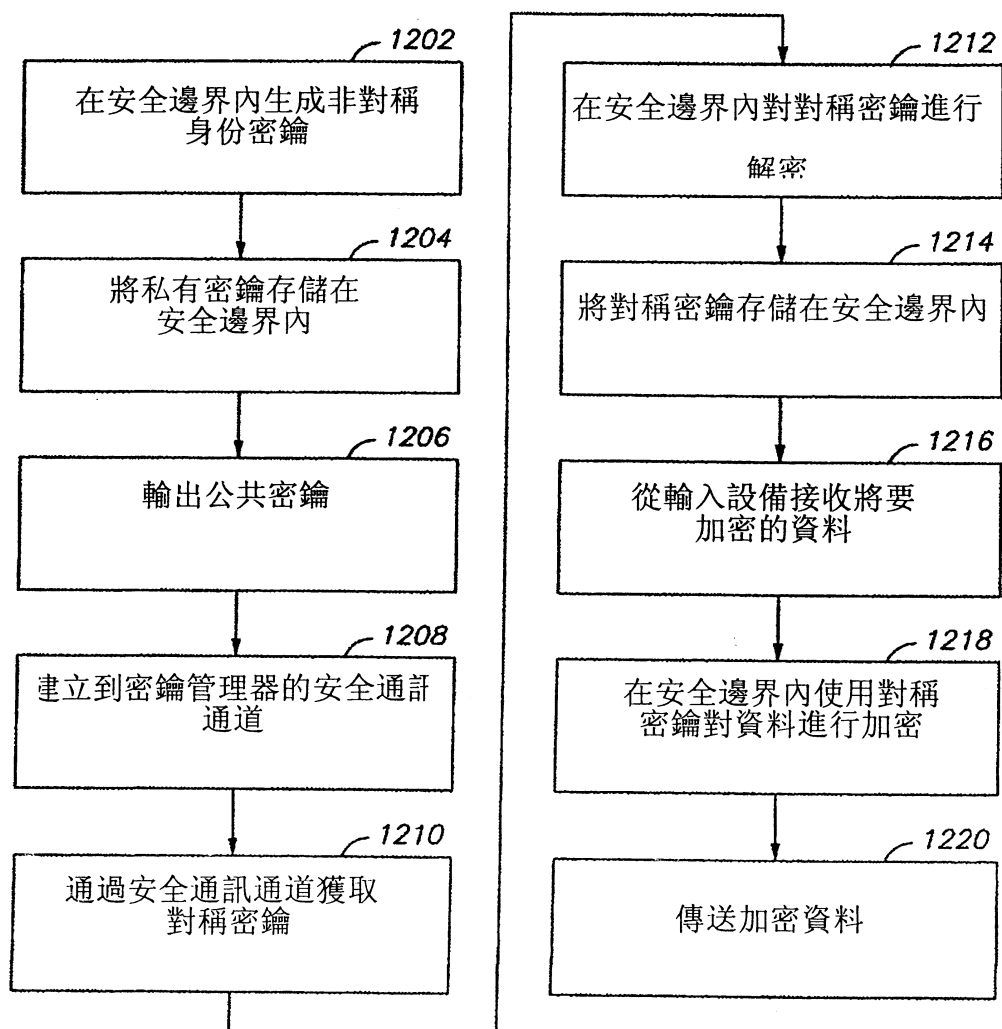


圖 12

七、指定代表圖：

(一)本案指定代表圖為：第 (1) 圖。

(二)本代表圖之元件符號簡單說明：

系統	100	接入設備	102、104
伺服器	106	信用證明	108
密鑰管理器	110	安全邊界	112
非對稱身份密鑰	114	安全通道	116
不安全的鏈路	118	信用證明登記機制	120
安全資料記憶體	122	加密處理器	124
密鑰	126	加密處理器	128
服務	130	信用證明	132
安全邊界	136	密鑰 A	140
加密處理器	142	非對稱身份密鑰	144
安全通道	146	不安全鏈路	148
密鑰 B	150		

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：