



(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 I487359 B

(45)公告日：中華民國 104 (2015) 年 06 月 01 日

(21)申請案號：101140959

(22)申請日：中華民國 101 (2012) 年 11 月 05 日

(51)Int. Cl. : H04L9/32 (2006.01)

H04L9/28 (2006.01)

(30)優先權：2011/11/21 美國

US 61/562,050

2012/06/14 美國

US 13/523,801

(71)申請人：美國博通公司 (美國) BROADCOM CORPORATION (US)

美國

(72)發明人：齊 崢 查爾斯 QI, CHARLES (ZHENG) (US) ; 布林 馬克 BUER, MARK (US)

(74)代理人：莊志強

(56)參考文獻：

TW 200737889A

US 6148400

US 2003/0138105A1

US 2005/0166051A1

US 2006/0072762A1

WO 2011/114197A1

審查人員：蔡鴻璟

申請專利範圍項數：9 項 圖式數：7 共 31 頁

(54)名稱

用於安全金鑰產生的設備、利用終端用戶設備來進行安全金鑰產生的方法及在裝置製造者伺服器中進行安全金鑰產生的方法

SECURE KEY GENERATION

(57)摘要

本發明涉及安全金鑰產生，提供了安全金鑰產生的方法和系統。在實施方式中，在製造處理期間，裝置產生用於裝置的初級種子並在裝置中儲存該種子。裝置輸出裝置初金鑰至安全的製造者伺服器。安全的製造者伺服器產生用於裝置的公開/私有根金鑰，並向認證授權機構請求用於裝置的公開的裝置根金鑰的證書。儲存有初級種子的裝置集成至終端用戶系統。當條件發生時，裝置在集成至終端用戶系統後現場產生公開/私有根金鑰。系統也接收並安裝用於公開根金鑰的證書。

100

- 100 . . . 系統
- 110 . . . 裝置
- 115 . . . 安全模組
- 120 . . . 處理器
- 130 . . . 記憶體

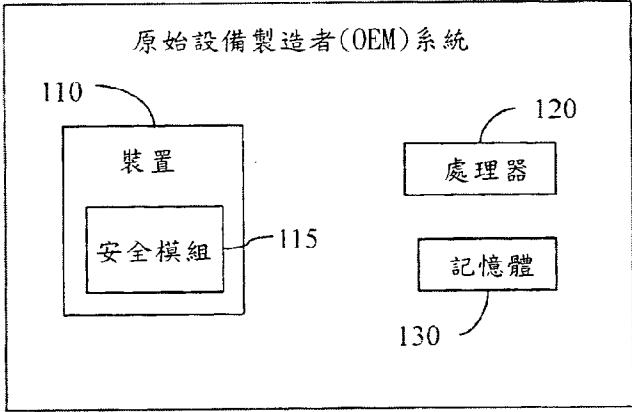


圖 1

104年2月6日修正替換本

發明專利說明書

公告本

(本說明書格式、順序，請勿任意更動，※記號部分請勿填寫)

※申請案號：101140959

H04L 9/32 (2006.01)

※申請日：101.11.5

※IPC 分類：

H04L 9/28 (2006.01)

一、發明名稱：(中文/英文)

用於安全金鑰產生的設備、利用終端用戶設備來進行安全
金鑰產生的方法及在裝置製造者伺服器中進行安全金鑰
產生的方法 / SECURE KEY GENERATION

二、中文發明摘要：

本發明涉及安全金鑰產生，提供了安全金鑰產生的方法和系統。在實施方式中，在製造處理期間，裝置產生用於裝置的初級種子並在裝置中儲存該種子。裝置輸出裝置初金鑰至安全的製造者伺服器。安全的製造者伺服器產生用於裝置的公開/私有根金鑰，並向認證授權機構請求用於裝置的公開的裝置根金鑰的證書。儲存有初級種子的裝置集成至終端用戶系統。當條件發生時，裝置在集成至終端用戶系統後現場產生公開/私有根金鑰。系統也接收並安裝用於公開根金鑰的證書。

三、英文發明摘要：

四、指定代表圖：

(一)本案指定代表圖為：圖 1。

(二)本代表圖之元件符號簡單說明：

系統 100

裝置 110

安全模組 115

處理器 120

記憶體 130

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

六、發明說明：

【發明所屬之技術領域】

本發明涉及資料通訊安全，更具體地，涉及加密金鑰管理。

【先前技術】

電腦系統越來越多地成為各種安全威脅的目標。許多電腦體系結構集成了具有安全子模組或者獨立分開的安全處理器的裝置，以為應用程式提供硬體支援。該安全子模組或者安全處理器通常成為整個系統的安全基礎。在這些系統中，期望裝置擁有裝置獨享根金鑰。通常，裝置獨享根金鑰為非對稱金鑰，其具有私有金鑰部分和公開金鑰部分。

該裝置獨享根金鑰的公開部分可由認證授權機構（CA）透過證書認證。證書透過使用受信第三方（CA）的數位簽名將裝置獨享根金鑰公開部分捆綁至實體，如個人或者公司。典型地，該數位簽名至少為利用 CA 的私有金鑰加密的裝置公開金鑰的哈希值（hash）。透過提供裝置根金鑰的證書，集成該裝置的系統能夠建立對同級或者網路分層的高等級信任。直接或者間接地，裝置根金鑰能夠用於建立系統的可靠性，以驗證系統通訊狀態，確保雙向通訊安全。

產生裝置根金鑰和頒發用於裝置根金鑰的證書給集成該裝置的系統，在邏輯上和技術上給裝置製造處理帶來了巨大的挑戰。RSA 根金鑰的產生極其耗費時間，因而不適合大量生產。此外，如果金鑰不是注入到裝置中，安全評估中的保證需要注入金鑰的設備與裝置之間的安全通訊。

因此，需要現場（in the field）安全產生裝置根金鑰和頒發裝置根金鑰證書的系統和方法。

【發明內容】

本發明提供了一種用於安全金鑰產生的設備，其包括：具有安全模組的裝置，其中，安全模組包括：非揮發性記憶體，儲存初級種子；處理器，被配置為在設備內在條件發生時從初級種子產生裝置根金鑰；並且該設備還包括記憶體，耦接到該裝置。

優選地，安全模組的處理器還被配置為透過使用第二加密裝置金鑰加密裝置根金鑰。

優選地，裝置根金鑰包括公開的裝置根金鑰和私有的裝置根金鑰。

優選地，安全模組的處理器還被配置為透過使用第二加密裝置金鑰加密私有的裝置根金鑰。

優選地，記憶體被配置為儲存已加密的裝置根金鑰。

優選地，記憶體被配置為儲存已加密的私有的裝置根金鑰。

優選地，該設備還包括：用於接收用於裝置根金鑰的證書的介面，其中，證書包括：公開的裝置根金鑰和頒發證書的認證授權機構的簽名。

優選地，記憶體還被配置為儲存用於 RSA 裝置根金鑰的證書。

優選地，條件為請求金鑰產生的命令。

優選地，條件為設備的初始啟動。

優選地，條件為安全模組的初始存取。

優選地，裝置根金鑰為 RSA 裝置根金鑰。

本發明還提供了一種利用終端用戶設備來進行安全金鑰產生的方法，終端用戶設備包括：具有安全模組和記憶體之裝置，該方法包括：接收用於公開之裝置根金鑰之證書，其中，證書包括：公開之裝置根金鑰和頒發證書之認證授權機構之數位簽名；驗證證書；在終端用戶設備內在條件發生時，使用儲存在安全模組內之記憶體中之預計算之初級種子產生私有之裝置根金鑰；以及在設備之記憶體中儲存證書和私有之裝置根金鑰。

優選地，條件為請求金鑰產生之命令。

優選地，條件為設備之初始啟動。

優選地，條件為安全模組之初始存取。

優選地，該方法還包括：提供證書至第二設備以驗證裝置。

本發明還提供了一種在裝置製造者伺服器中進行安全金鑰產生的方法，方法包括：接收用於裝置之初級種子，其中，初級種子用製造者金鑰進行加密；在裝置製造者伺服器解密用於裝置之初級種子；在裝置製造者伺服器之安全模組中，透過使用接收到的用於裝置之初級種子，產生公開和私有 RSA 根金鑰；向認證授權機構請求用於已產生之公開之裝置根金鑰之證書；從認證授權機構接收用於已產生之公開之裝置根金鑰之證書；提供證書至集成裝置之系統；並且從裝置製造者伺服器中刪除私有根金鑰。

優選地，該方法還包括：將公開之裝置根金鑰與裝置根金鑰名稱相關聯。

優選地，裝置根金鑰名稱透過使用用於裝置之序列號和用於裝置之初級種子產生。

優選地，序列號對於多個裝置內的裝置是唯一的。

優選地，該方法還包括：在製造者資料庫中儲存裝置根金鑰名稱和公開的裝置根金鑰。

【實施方式】

下面的描述中，顯示了大量的具體細節，以透徹理解本發明。然而，本領域技術人員應當理解，包括結構、系統以及方法的本發明可在沒有這些特定細節的情況下實施本發明。此處的描述和呈現為本領域技術人員所用的通用手段，以高效傳達給他們工作的實質內容給其他本領域的技術人員。在其他情況下，公知的方法、步驟、元件和電路未進行詳細描述，以避免不必要地混淆本發明的方面。

本說明書中提到的“一個實施方式”、“實施方式”、“範例性實施方式”等，表示所描述的實施方式可包括特定的特徵、結構或特性，但每個實施方式不必須要包括該特定的特徵、結構或特性。此外，這些短語不一定需要指相同的實施方式。進一步地，當關於某個實施方式描述特定的特徵、結構或特性時，這表示，本領域技術人員應當瞭解，無論是否明確描述，都可結合其他實施方式來影響這樣的特徵、結構或特性。

用於安全金鑰產生的系統

終端用戶系統，如手機、電腦或者其他電子裝置，集成了來自眾多製造者的裝置。例如，手機在多個元件中可包括基帶處理器、收發器、GPS 接收器和/或藍牙裝置。透過用於終端用戶系統的元件的各種裝置製造者，向系統製造者（通常指原始裝置製造者）提供系統所必要的裝置。

圖 1 是包括本發明實施方式的系統 100 的高級方塊圖。系統 100 可以為任何形式的電子裝置，包括但不限於，臺式電腦、無線電腦、伺服器、路由器、無線手持裝置或任何其他形式的電子裝置。系統 100 可由原始設備製造者（OEM）製造。在高層次上，系統 100 包括裝置 110、處理器 120 和記憶體 130。

實施方式中，裝置 110 可以由不同於原始設備製造者的製造者製造。實施方式中，裝置 110 包括安全模組 115。安全模組 115 為安全應用提供硬體支援。在可選的實施方式中，裝置 110 可以為獨立安全處理器，例如通用安全網路集線器（USH）。裝置 110 具有根加密金鑰（本文中指“裝置根金鑰”）。用於裝置的根金鑰為主金鑰，其能夠用於多種目的，包括但不限於產生其他金鑰。

用於例如裝置 110 的裝置的根金鑰可以對於各個裝置在統計學上唯一，而且必須繫結到該裝置。為保證繫結，裝置根金鑰或者在裝置上產生，或者在外部產生並安全注入到裝置中。在該裝置被部署後，該裝置根金鑰儲存在裝置 110 的非揮發性記憶體中或者儲存在加密繫結到該裝置的外部非揮發性記憶體（例如記憶體 130）中。

裝置根金鑰通常為長效金鑰，其可能不能被撤銷。因為該裝置根金鑰用於建立與其他各方的信任，該裝置根金鑰必須具有充分強的加密性和良好保護性。基於公開金鑰加密的非對稱金鑰是更為優選的，因為私有金鑰不在同類（同級，peer）間共用。

裝置根金鑰可以由認證授權機構（CA）予以認證。在認證處理過程中，該 CA 產生用於裝置根金鑰的證書。該

證書將裝置根金鑰的公開金鑰部分與標識（如裝置製造者）繫結。在其要素中，該證書包括：裝置根金鑰（如裝置公開根金鑰）、裝置製造者的標識、CA 的標識和用於 CA 的數位簽名。該用於 CA 的數位簽名透過對證書中的資訊進行哈希處理，並利用 CA 的私有金鑰加密哈希處理後的資訊而獲得。透過提供用於裝置根金鑰的證書，可以發展與網路環境中其他成員的額外信任。

創建裝置根金鑰和相應的根金鑰證書存在巨大挑戰。例如，製造過程中創建裝置根金鑰增加了製造處理的成本。在大批量裝置製造處理中，裝置的成本由材料成本（例如晶片、光罩和封裝成本）以及處理成本決定。處理成本的主要貢獻者為在每個裝置所耗費的處理時間。

理想地，該裝置根金鑰應該在製造處理中透過裝置基於片上隨機熵源以及具有測試函數的其他加密函數產生。該處理確保裝置根金鑰的私有部分僅該裝置知曉且永遠不離開該裝置。然而，當該裝置根金鑰為 RSA 金鑰時，由該裝置產生 RSA 金鑰存在挑戰。

目前，RSA 是安全應用程式支援的主要演算法。因而，裝置根金鑰的主要部分是 RSA 金鑰。RSA 安全性源自於分解大量數位的難度。為產生 RSA 公開/私有金鑰對，應該首先選擇兩個隨機大質數(prime number) p 和 q 。 p 和 q 的選擇基於使用片上的熵源產生的種子的米勒-拉賓 (Miller-Rabin) 演算法。對於 2048 位的 RSA 金鑰，該兩個質數都為 1024 位。質數選擇演算法極其耗費時間。該處理持續的時間顯著差異可達大約 15 秒至超過 1 分鐘。如果在製造處理過程中要由裝置產生 RSA 根金鑰，則裝置的

耗費將由於質數選擇處理導致的處理時間增加而顯著增加。此外，計算的非確定性使得對於大批量生產難以設定測試程式。

此外，例如裝置 110 的裝置限制了片上記憶體。由於私有金鑰操作使用中國餘數定理，RSA 私有金鑰由五元組 $\{p, q, dp, dq, qinv\}$ 表示，以用於使用中國余部定理的私有金鑰操作。對於 2048 位元 RSA 裝置金鑰，每個參數都為 1024 位。如果 RSA 金鑰在片上產生，則私有金鑰必須安全儲存，並繫結到裝置上。在第一種方法中，裝置 110 在片上具有足夠的非揮發性記憶體，以允許 RSA 私有金鑰在產生後編程至裝置的非揮發性記憶體中。在第二種方法中，RSA 私有金鑰由裝置獨有的對稱金鑰（如 256 位 AES 金鑰）加密並被輸出。在這種方法中，裝置獨有的對稱金鑰必須編程至裝置內的可編程非揮發性記憶體。

對於使用先進 CMOS 數位處理製造的裝置，例如嵌入式快閃記憶體的片上可重新編程非揮發性記憶體的技術尚不可用。使用一次編程（OTP）非揮發性記憶體以儲存如此大的金鑰將顯著增加晶片尺寸。此外，OTP 儲存使得不可能撤銷並重建用於特定應用的根金鑰。因此，第一種方法不可用於使用這些先進 CMOS 數位處理製造的裝置。

然而，第二種方法遭遇邏輯上的挑戰。例如，當第二種方法用於裝置製造處理中時，加密私有金鑰和其相應的公開金鑰必須收集和盤存到資料庫中。加密的私有金鑰隨後必須由系統 100 的原始設備製造者（OEM）注入回裝置中。

可選地，一旦外部附接快閃記憶體可用，加密金鑰可

現場注入到裝置中。如下文進一步詳細描述，現場注入根金鑰存在安全挑戰。

圖 2 是根據本發明實施方式的範例性安全模組 210 的方塊圖。安全模組 210 包括一個或多個安全處理單元 202、亂數產生器 226、公開金鑰加速器 234 以及非揮發性記憶體 222。亂數產生器 226 被配置為產生亂數。例如，本文所描述的實施方式中，亂數產生器 226 被配置為產生亂數，作為用於產生 RSA 公開/私有金鑰的種子。公開金鑰加速器 (PKA) 234 被配置為處理所支援的公開金鑰操作專有的處理。例如，公開金鑰加速器應被配置為產生 RSA 公開/私有根金鑰。

安全模組 210 (或安全處理器) 還可以包括實現安全模組 (或安全處理器) 與外部裝置通訊的元件。這些元件可以包括直接記憶體存取 (DMA) 引擎、週邊元件互聯 (PCI) 介面、通用介面、通用串列匯流排 (USB) 介面和/或一個或多個匯流排。安全模組 210 還可包括具體實施方式所需的額外或可選的元件，如加密金鑰管理器 204、安全保護邏輯以及 RAM。

圖 3 顯示了包括本發明實施方式的範例性操作環境 390。環境 390 包括裝置製造者、原始設備製造者 (OEM)、認證授權機構以及用戶。裝置製造者具有裝置製造者設施 340、可選的金鑰伺服器 350 以及加密金鑰管理資料庫 355。在實施方式中，金鑰伺服器 250 和資料庫 355 不在裝置製造者設施中。製造者設施 340 製造裝置 310。如上所述，各裝置 310 具有相關聯的裝置根金鑰。製造者設施 340 還包括一個或多個電腦 345，其被配置為與製造者

金鑰伺服器 350 通訊。製造者金鑰伺服器 350 負責用於管理金鑰和用於製造者裝置 310 的證書。製造者金鑰伺服器 350 為安全伺服器。在實施方式中，製造者金鑰伺服器 350 包括硬體安全模組 (HSM)。

範例性環境 390 還可包括認證授權機構 360。認證授權機構 360 被配置為認證製造者裝置公開金鑰並產生用於裝置公開金鑰的證書。在實施方式中，認證授權機構 360 由第三方操作。在可選的實施方式中，認證授權機構 360 可以由製造者提供或主持。環境 390 還包括原始設備製造者 (OEM) 設施 370 和終端用戶設施 380。OEM 設施 370 將包括至少一個裝置組裝至終端用戶系統 300 中。圖 3 中所示元件可與網路 380 耦接在一起。網路 380 可以為一個或多個公開資料通訊網路 (例如網際網路)、一個或多個私有資料通訊網路、或公開資料通訊網路和私有資料通訊網路的組合。

用於安全金鑰產生的方法

圖 4 顯示了根據本發明實施方式的裝置根金鑰按需現場產生方法的流程圖 400。圖 4 是參考圖 3 的範例性操作環境而描述的。然而，圖 4 不局限於該實施方式。

在步驟 S410 中，裝置 310 透過使用例如 DSA 或橢圓曲線 DSA (ECDSA) 的演算法產生裝置公開/私有金鑰對。為便於討論，此處 DSA 金鑰指用於公開金鑰部分的 Kdi-pub 和用於私有金鑰部分的 Kdi-priv。私有的 DSA 裝置金鑰儲存於裝置內的記憶體中。

在步驟 S420 中，公開的 DSA 裝置金鑰 Kdi-pub，輸出至製造者設施 340 中的電腦 345 中。電腦 345 從製造者

設施 340 製造的多個裝置 310 接收公開的 DSA 裝置金鑰。

在步驟 S430 中，電腦 345 將公開的 DSA 裝置金鑰通訊至製造者金鑰伺服器 350。通訊至製造者金鑰伺服器 350 的各個 DSA 公開裝置金鑰 Kid-pub，都與用於該裝置的識別字相關聯。製造者金鑰伺服器 350 儲存用於裝置 310 的 Kdi-pub。例如，Kdi-pub 可以儲存於製造者金鑰管理資料庫 355 中。

在步驟 S440，將裝置 310 提供給 OEM 以集成至電腦系統 300 中。然後，OEM 可提供組裝好的電腦系統給終端用戶（例如終端用戶 380）。

在步驟 S450 中，裝置 RSA 根金鑰按需現場產生。裝置 RSA 根金鑰可在系統首次啟動、初始存取安全模組/安全處理器或接收到對於 RSA 根金鑰產生的請求時產生。裝置根金鑰可在 OEM 設施或（可選地）終端用戶裝置中產生。為了便於討論，公開/私有裝置 RSA 根金鑰指 EK-pub（用於公開金鑰部分）和 EK-priv（用於私有金鑰部分）。

在步驟 S460 中，裝置 310 透過使用儲存在裝置 310 的記憶體中的私有的 DSA 金鑰 Kdi-priv，為公開的 RSA 裝置根金鑰 EK-pub 簽名。

在步驟 S470 中，已簽名的公開的 RSA 裝置根金鑰被通訊至製造者金鑰伺服器 350。已簽名的公開的裝置 RSA 根金鑰也可以與識別裝置 310 的資訊通訊。

在步驟 S475 中，製造者金鑰伺服器 350 使用儲存的公開的 DSA 金鑰 Kdi-pub 驗證接收到的簽名。如果簽名透過驗證，則操作前進至步驟 S480。

在步驟 S480 中，裝置製造者在證書簽名請求中將 RSA

裝置根金鑰 (EK-pub) 提供至 CA 360。

在步驟 S485 中，認證授權機構 360 產生包括公開的 RSA 裝置根金鑰的裝置證書，並將證書提供給製造者金鑰伺服器 350。如上所述，證書由認證授權機構 360 數位簽名。

步驟 S490 中，裝置證書提供給 OEM 或者終端用戶。然後，OEM 或終端用戶能使用證書以向第三方證明該裝置。

如圖 4 的方法需要由裝置製造者建立證書頒發機制，以允許終端用戶或 OEM 申請證書。對於大批量生產的裝置，建立和維護該機制比較昂貴。此外，終端用戶需要技術上足夠瞭解以請求和安裝證書。許多終端用戶缺乏這種技術。因此，圖 4 方法可能需要額外的支援。

圖 5 和圖 6 中所述實施方式涉及 RSA 裝置金鑰的外部產生和已產生的金鑰向裝置的注入。金鑰注入設備與裝置之間的安全是關鍵。在金鑰注入實施方式中，在金鑰注入設備和接收金鑰的裝置之間可建立安全通訊。此外，在實施方式中，可以提供金鑰注入裝置和裝置相互驗證。例如，金鑰注入裝置可驗證裝置為真正裝置，以保證 RSA 金鑰注入到預期裝置中。裝置也可能夠驗證金鑰注入設備，以使得其能夠確保從受信源接收 RSA 裝置金鑰。最後，金鑰注入設備應透過操作者的適當存取控制（物理的或者邏輯的），在安全環境中得到足夠保護。

圖 5 顯示了根據本發明實施方式的提供 OEM 將裝置根金鑰注入至裝置的方法的流程圖 500。圖 5 是參考圖 3 的範例性操作環境而描述的。然而，圖 5 不局限於該實施

方式。在圖 5 所示的實施方式中，用於裝置的 RSA 根金鑰由 OEM 主持的安全伺服器外部產生。

在步驟 S510 中，裝置 310 透過使用例如迪斐-海爾曼 (Diffie Hellman, DH) 演算法、橢圓曲線 DH (ECDH)、DSA、橢圓曲線 DSA (ECDSA) 或其他類似的演算法產生金鑰材料 (如公開/私有金鑰對)。裝置金鑰材料可儲存在裝置 310 的記憶體內。

在步驟 S520 中，例如，在裝置 310 和伺服器之間使用迪斐-海爾曼金鑰交換建立共用秘密。

在步驟 S530 中，將裝置 310 提供給 OEM，以集成到電腦系統 300 中。

在步驟 S540 中，RSA 裝置根金鑰 (EK-pub、EK-priv) 由 OEM 的安全伺服器為裝置產生。

在步驟 S550 中，安全伺服器透過使用共用秘密產生的對稱金鑰加密所產生的私有的 RSA 裝置根金鑰 (EK-priv)。

在步驟 S560 中，已加密的私有的 RSA 裝置根金鑰注入到裝置 310 中。如上所述，在步驟 S560 之前，OEM 的金鑰注入設備可以在提供 RSA 裝置金鑰之前驗證裝置為真正裝置。此外，裝置可包括驗證金鑰注入設備的功能。

透過加密，RSA 私有金鑰得到共用秘密的保護。因此，已加密 RSA 私有金鑰可保存在裝置的安全模組外部的記憶體中。在加密的私有的 RSA 裝置金鑰注入到裝置中之後，安全伺服器從安全伺服器中刪除 RSA 金鑰。

在步驟 S570 中，RSA 裝置公開根金鑰在證書簽名請求中被通訊至認證授權機構 360。OEM 也可以將裝置製造

者的通訊標識通訊至 CA。

在步驟 S580 中，認證授權機構 360 產生裝置公開的 RSA 根金鑰證書，其包括公開的裝置 RSA 根金鑰和認證授權機構的簽名。然後，CA 將證書提供給 OEM 的安全伺服器。

在步驟 S590 中，公開的裝置 RSA 根金鑰證書被提供給 OEM，OEM 轉而將公開的裝置 RSA 根金鑰證書提供給集成該裝置的系統 300。

圖 6 顯示了根據本發明實施方式的製造者將裝置根金鑰注入的方法的流程圖 600。圖 6 是參考圖 3 的範例性操作環境而描述的。然而，圖 6 不局限於該實施方式。在圖 6 的實施方式中，RSA 金鑰由製造者主持的安全伺服器產生。

在步驟 S610 中，裝置 310 透過使用例如迪斐-海爾曼 (Diffie Hellman, DH) 演算法、橢圓曲線 DH (ECDH)、DSA、橢圓曲線 DSA (ECDSA) 或其他類似的演算法產生金鑰材料 (如公開/私有金鑰對)。裝置金鑰材料可以儲存在裝置 310 的記憶體中。

在步驟 S620 中，例如，在裝置 310 與伺服器之間使用迪斐-海爾曼金鑰交換建立共用秘密。

在步驟 S630 中，裝置 RSA 根金鑰 (EK-pub、EK-priv) 由安全伺服器在金鑰伺服器設施處產生。應注意，裝置製造者的安全伺服器可以先於裝置製造來產生 RSA 金鑰。然後，安全伺服器可以分配產生的 RSA 裝置金鑰給裝置。

在步驟 S640 中，私有的 RSA 裝置根金鑰 EK-priv 透

過從共用秘密產生的對稱金鑰而加密。

在步驟 S650 中，認證授權機構 360 在證書簽名請求中接收到公開的 RSA 裝置根金鑰 EK-pub。然後，CA 產生包括公開的 RSA 裝置根金鑰的裝置證書，並提供該證書至製造者金鑰伺服器。如上所述，該證書由認證授權機構 360 數位簽名。

在可選的實施方式中，CA 被提供有一組已產生的 RSA 金鑰。在該實施方式中，可以為該組中的每個 RSA 金鑰產生證書，並成批提供給安全伺服器。

在步驟 S660 中，加密的私有的 RSA 裝置根金鑰和公開的裝置 RSA 根金鑰證書被通訊至製造者設施的電腦 345。在將加密的私有的 RSA 裝置根金鑰通訊至電腦 345 後，製造者的安全伺服器刪除私有的 RSA 裝置根金鑰。

在步驟 S665 中，已加密的私有的裝置 RSA 根金鑰和裝置 RSA 根金鑰證書被通訊至 OEM。在實施方式中，製造者和 OEM 在將金鑰和認證資訊通訊之前，建立安全通訊。本領域技術人員應瞭解，通訊可基於已知的協議（如 SSL、TLS 或 IPSec）加密。應注意，在可選的實施方式中，已加密的裝置 RSA 根金鑰和裝置 RSA 根金鑰證書可以由裝置製造者的安全伺服器（金鑰伺服器 350）而非電腦 345 進行通訊。

在步驟 S670 中，將裝置 310 提供給 OEM，以集成到電腦系統 300 中。

在步驟 S680 中，OEM 獲得用於裝置的裝置 RSA 根金鑰證書和已加密的私有的裝置 RSA 根金鑰。然後，OEM 將私有的裝置 RSA 根金鑰注入到裝置中，並安裝證書。

如上所述，在步驟 S680 之前，OEM 的金鑰注入設備可以在提供 RSA 裝置金鑰之前，驗證裝置為真正裝置。此外，裝置可以包括驗證金鑰注入設備的功能。

圖 7 顯示了根據本發明實施方式的 RSA 裝置金鑰的基於種子的現場獲得的方法的流程圖 700。圖 7 是參考圖 3 的範例性操作環境而描述的。然而，圖 7 不局限於該實施方式。圖 7 的方法將裝置製造處理的成本影響降到最低，且不易受安全風險的攻擊。此外，圖 7 所示的方法可伸縮。

在圖 7 的實施方式中，裝置在其集成至目標系統後，現場產生其 RSA 金鑰。現場 RSA 金鑰產生的等待時間是更可容忍的，因為其通常為涉及終端用戶的交互處理。此外，因為該實施方式在系統中產生 RSA 金鑰，且目標系統中存在相關聯的記憶體（例如快閃記憶體驅動器），所述儲存的限制通常被消除。

在步驟 S710 中，由裝置 310 使用片上亂數產生器 226 產生初級種子。初級種子被編程至裝置的一次可編程非揮發性記憶體 222。對於 2048 位的 RSA 金鑰，初級種子的大小需要比 2048 為 RSA 金鑰的安全強度（即 112 位）大。為此，在實施方式中，選擇 256 位元的初級種子。因為產生初級種子不需要選擇質數，使用步驟 S710 可以以合理的速度完成。應注意，DSA 私有金鑰也可以為 256 位亂數。透過稍微修改 DSA 金鑰（kdi）產生處理，已產生的隨機種子可用作共用初級種子以獲得 RSA 根金鑰和 DSA 金鑰。

在步驟 S715 中，RSA 初級種子被編程至裝置的記憶

體中。例如，RSA 初級種子可以儲存在安全模組內的一次可編程非揮發性記憶體中。因此，以該方法，當製造裝置時，初級種子在片上產生並儲存。

在步驟 S720 中，RSA 初級種子輸出到製造者設施 340 的電腦 345 中。電腦 345 從製造者設施 340 製造的多個裝置 310 接收 RSA 初級種子。應注意，該步驟為可選步驟。如果不存在，則種子輸出至裝置製造者的安全伺服器。

在步驟 S730 中，電腦 345 透過製造者公開金鑰（KM-pub）加密 RSA 初級種子，並輸出已加密的 RSA 初級種子至製造者內的安全伺服器。製造者的公開金鑰可以為 RSA 公開金鑰、DSA 公開金鑰、DH 公開金鑰、EC DSA 公開金鑰或 EC DH 公開金鑰。本領域技術人員應當瞭解，其他形式的公開的製造者金鑰也可以用於本發明。相應的私有金鑰由製造者的安全伺服器（如硬體安全模組）保存。製造者私有金鑰通常在物理上和邏輯上得到製造者的保護，以免於未授權的存取。

在步驟 S740 中，製造者金鑰伺服器裝置中的安全伺服器透過使用製造者的私有金鑰解碼 RSA 初級種子。

在步驟 S750 中，製造者的安全伺服器使用 RSA 初級種子產生 RSA 公開/私有根金鑰對。在該步驟中，初級種子饋送至演算法中以產生 RSA 根金鑰。由於需要質數選擇，所以該步驟需要漫長的計算。該演算法確保，一旦初級種子確定並且唯一，則所獲得的 RSA 根金鑰也唯一。在產生 RSA 金鑰對後，安全伺服器從伺服器中刪除私有的 RSA 金鑰。

在實施方式中，在 RSA 初級種子產生和輸出後，裝置

根金鑰的序列號和名稱也可以由製造者產生。序列號和/或名稱可以由電腦 345 和/或製造者的安全伺服器產生。序列號可對於裝置是唯一的，並被編程至裝置的記憶體中。RSA 裝置根金鑰名稱可以透過加密地哈希處理多個連接欄位（如裝置版本號、序列號和初級種子）而產生。本領域技術人員應當瞭解，其他的用於產生金鑰名稱的技術也可以用於本發明的實施方式。序列號、根金鑰名稱和產生的 RSA 根金鑰儲存在製造者的資料庫中。

在步驟 S760 中，認證授權機構（CA）260 從製造者的安全伺服器接收來自包括公開的 RSA 裝置根金鑰 EK-pub 的製造者的證書簽名請求。然後，CA 產生包括公開的 RSA 裝置根金鑰的 RSA 公開裝置根金鑰證書，並將 RSA 公開裝置根金鑰證書提供給製造者。證書簽名請求也可包括序列號以及根金鑰名稱。如果這些都提供給 CA 360，則 CA 360 將此資訊包括到其頒發的證書中。如上所述，證書由認證授權機構 360 數位簽名。

在步驟 S770 中，製造者的安全伺服器提供公開的 RSA 根金鑰證書至電腦 345。

在步驟 S780 中，電腦 345 將公開的 RSA 根金鑰證書分配給包括該裝置的終端用戶系統 300。應注意，步驟 780 為可選的。在實施方式中，製造者的安全伺服器（或製造者的其他平臺）可以執行將公開的 RSA 金鑰證書分配給包括該裝置的終端用戶系統 300 的步驟。還應注意，在實施方式中，裝置製造者可以提供此資訊給 OEM，OEM 轉而將該資訊提供給終端用戶系統。

在步驟 S785 中，公開的裝置 RSA 根金鑰證書裝載至

終端用戶系統中，並被驗證。如果驗證成功，則操作處理前進至步驟 S790。如果驗證不成功，則終端用戶系統 300 通知 OEM 或裝置製造者，並請求新的證書。

在步驟 S790 中，終端用戶系統 300 中的裝置 310 在條件發生時產生 RSA 公開/私有根金鑰對。例如，一旦接收到產生 RSA 根金鑰的請求或命令時，裝置 RSA 根金鑰對可以立刻產生。可選地，裝置 RSA 根金鑰可以在系統初始啟動時或當安全模組或者安全處理器首次被存取時產生。

在該步驟中，所儲存的初級種子饋送至演算法中以產生 RSA 根金鑰。由於需要質數選擇，所以該步驟需要漫長的計算。因此，其在裝置部署後現場執行。該演算法確保，一旦初級種子確定並且唯一，所獲得的 RSA 根金鑰也唯一。此外，因為該步驟現場執行，所以 RSA 根金鑰（全部根金鑰或私有的 RSA 根金鑰）可以由裝置包裹加密，且在明顯沒有任何軟體干預的情況下，儲存在所附的快閃記憶體裝置中。

應理解，上述本發明的實施方式可以以硬體、固件、軟體或者它們的任意組合來實現。本發明的實施方式也可實施為儲存在機器可讀介質上的指令，其可被一個或多個處理器讀取和執行。機器可讀介質可以包括以機器（例如計算裝置）可讀的形式儲存和傳送資訊的任何機器。例如，機器可讀介質可包括唯讀記憶體（ROM）；隨機存取記憶體（RAM）；磁片儲存介質；光學儲存介質；快閃記憶體裝置；電學、光學、聲學或其他形式的傳播信號。

以上，已在顯示了特定功能的實現和它們的關係的功

能構建方塊的幫助下描述了本發明。為了描述方便起見，這些功能構建方塊的邊界已在本文中任意定義。只要能夠適當執行特定功能和它們的關係，也可以定義其他的邊界。

【圖式簡單說明】

圖 1 是包括本發明實施方式的系統的高級方塊圖。

圖 2 是根據本發明實施方式的範例性安全模組的方塊圖。

圖 3 顯示了包括本發明實施方式的範例性操作環境。

圖 4 顯示了根據本發明實施方式按需現場產生裝置根金鑰的方法的流程圖。

圖 5 顯示了根據本發明實施方式透過 OEM 將裝置根金鑰注入裝置的方法的流程圖。

圖 6 顯示了根據本發明實施方式製造者注入裝置根金鑰的方法的流程圖。

圖 7 顯示了根據本發明實施方式 RSA 裝置金鑰的基於種子的現場獲得的方法的流程圖。

【主要元件符號說明】

系統 100

裝置 110

安全模組 115

處理器 120、320

記憶體 130、330

安全處理單元 202

安全模組 210

非揮發性記憶體 222

亂數產生器 226

金鑰加速器 234

電腦系統 300

裝置 310

電腦 345

製造者金鑰伺服器 350

加密金鑰管理資料庫 355

認證授權機構 360

OEM 設施 370

終端用戶 380

環境 390

各個步驟流程 S410～S490、S510～S590、S610～S680
、S710～S790

七、申請專利範圍：

1. 一種用於安全金鑰產生的設備，其包括：

具有安全模組的裝置，其中，所述安全模組包括：

亂數產生器，被配置為產生初級種子；

非揮發性記憶體，被配置為儲存所述初級種子；以及

處理器，被配置為在所述設備內在條件發生時從所述初級種子產生裝置根金鑰，其中所述裝置根金鑰包括公開的裝置根金鑰和私有的裝置根金鑰；以及

記憶體，耦接到所述裝置；

其中，所述裝置被配置為輸出所述初級種子至製造者伺服器中，並且使得所述製造者伺服器向認證授權機構請求用於所述公開的裝置根金鑰的證書；

其中，所述裝置還被配置為從所述製造者伺服器中接收所述認證授權機構所提供的用於所述公開的裝置根金鑰的所述證書。

2. 如申請專利範圍第 1 項所述的設備，其中，所述安全模組的處理器還被配置為透過使用第二加密裝置金鑰加密所述裝置根金鑰。

3. 如申請專利範圍第 1 項所述的設備，其中，所述安全模組的處理器還被配置為透過使用第二加密裝置金鑰加密所述私有的裝置根金鑰。

4. 如申請專利範圍第 1 項所述的設備，其中，所述條件為：請求金鑰產生的命令，或者所述設備的初始啟動，或者所述安全模組的初始存取。

5. 如申請專利範圍第 1 項所述的設備，其中，所述裝置根金鑰為 RSA 裝置根金鑰。

6. 一種利用終端用戶設備來進行安全金鑰產生的方法，所述終端用戶設備包括：具有安全模組的裝置和記憶體，所述方法包括：

在具有所述安全模組的所述裝置中產生初級種子；

從所述裝置中輸出所述初級種子至製造者伺服器，並且使得所述製造者伺服器向認證授權機構請求用於公開的裝置根金鑰的證書；

從所述製造者伺服器接收所述認證授權機構所提供的用於所述公開的裝置根金鑰的所述證書，其中，所述證書包括：所述公開的裝置根金鑰和頒發所述證書的所述認證授權機構的數位簽名；

驗證所述證書；

在所述終端用戶設備內在條件發生時，使用儲存在所述安全模組內的記憶體中的預計算的初級種子產生私有的裝置根金鑰；以及

在所述終端用戶設備的記憶體中儲存所述證書和所述私有的裝置根金鑰。

7. 如申請專利範圍第 6 項所述的方法，其中，所述條件為：請求金鑰產生的命令，或者所述終端用戶設備的初始啟動，或者所述安全模組的初始存取。

8. 一種在裝置製造者伺服器中進行安全金鑰產生的方法，所述方法包括：

接收用於裝置的初級種子，其中，所述初級種子用製造者金鑰進行加密；

在所述裝置製造者伺服器解密所述用於裝置的初級種子；

在所述裝置製造者伺服器的安全模組中，透過使用接收到的所述用於裝置的初級種子，產生公開和私有 RSA 根金鑰；

向認證授權機構請求用於已產生的公開的裝置根金鑰的證書；

從所述認證授權機構接收所述用於已產生的公開的裝置根金鑰的證書；

提供所述證書至集成所述裝置的系統；以及

從所述裝置製造者伺服器中刪除所述私有根金鑰。

9. 如申請專利範圍第 8 項所述的方法，還包括：將所述公開的裝置根金鑰與裝置根金鑰名稱相關聯。

八、圖式：

100

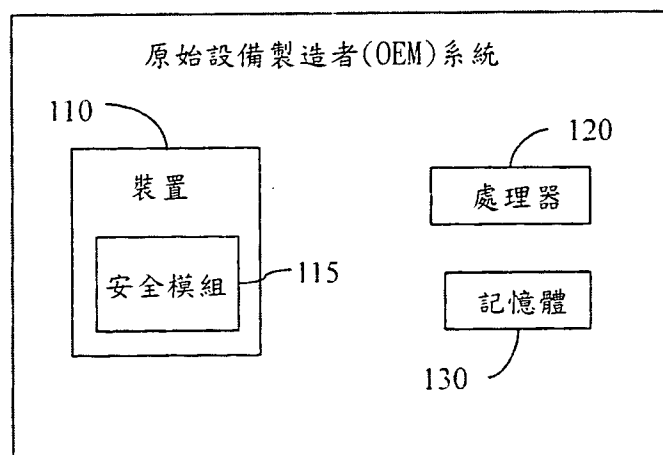


圖 1

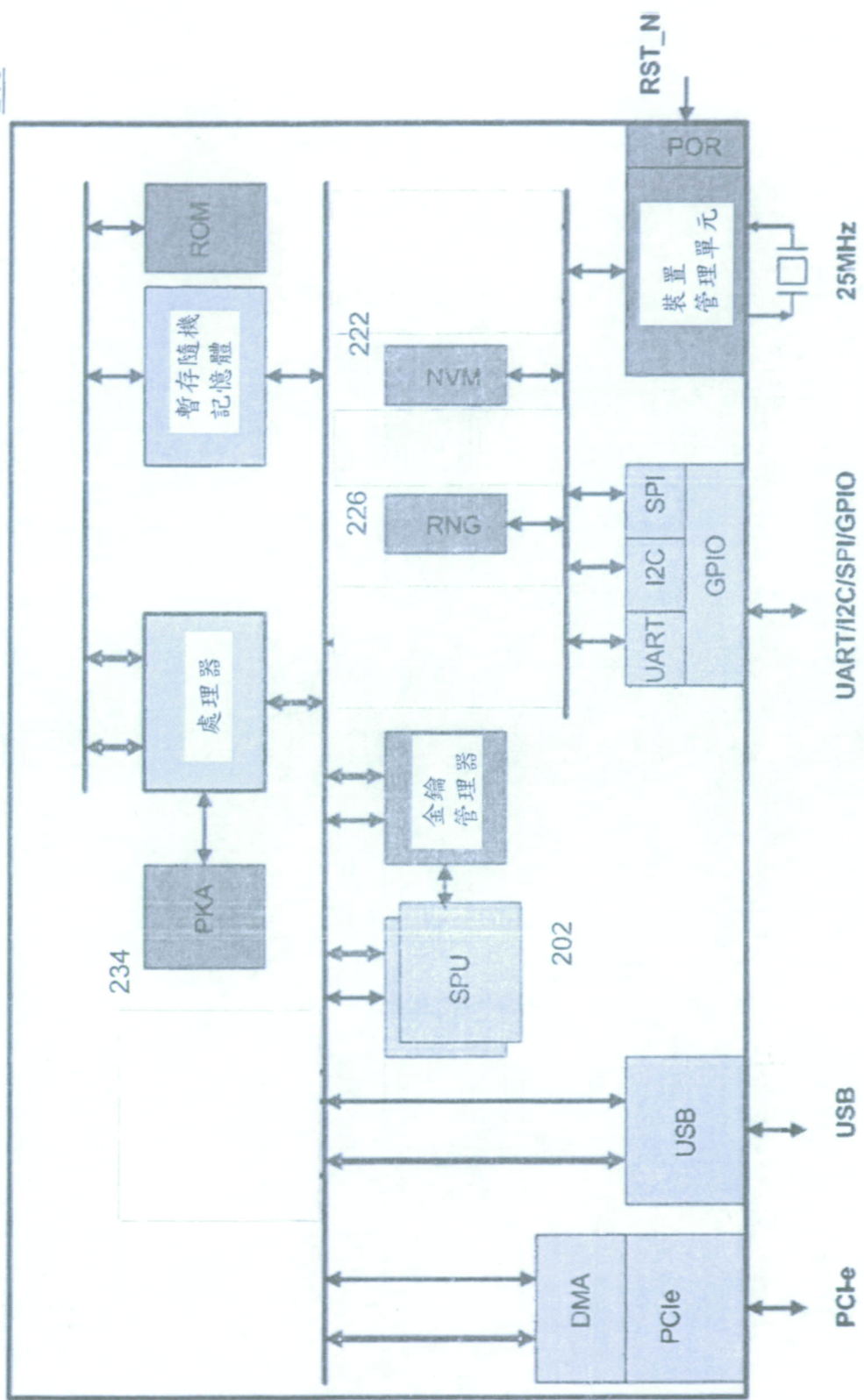


圖2

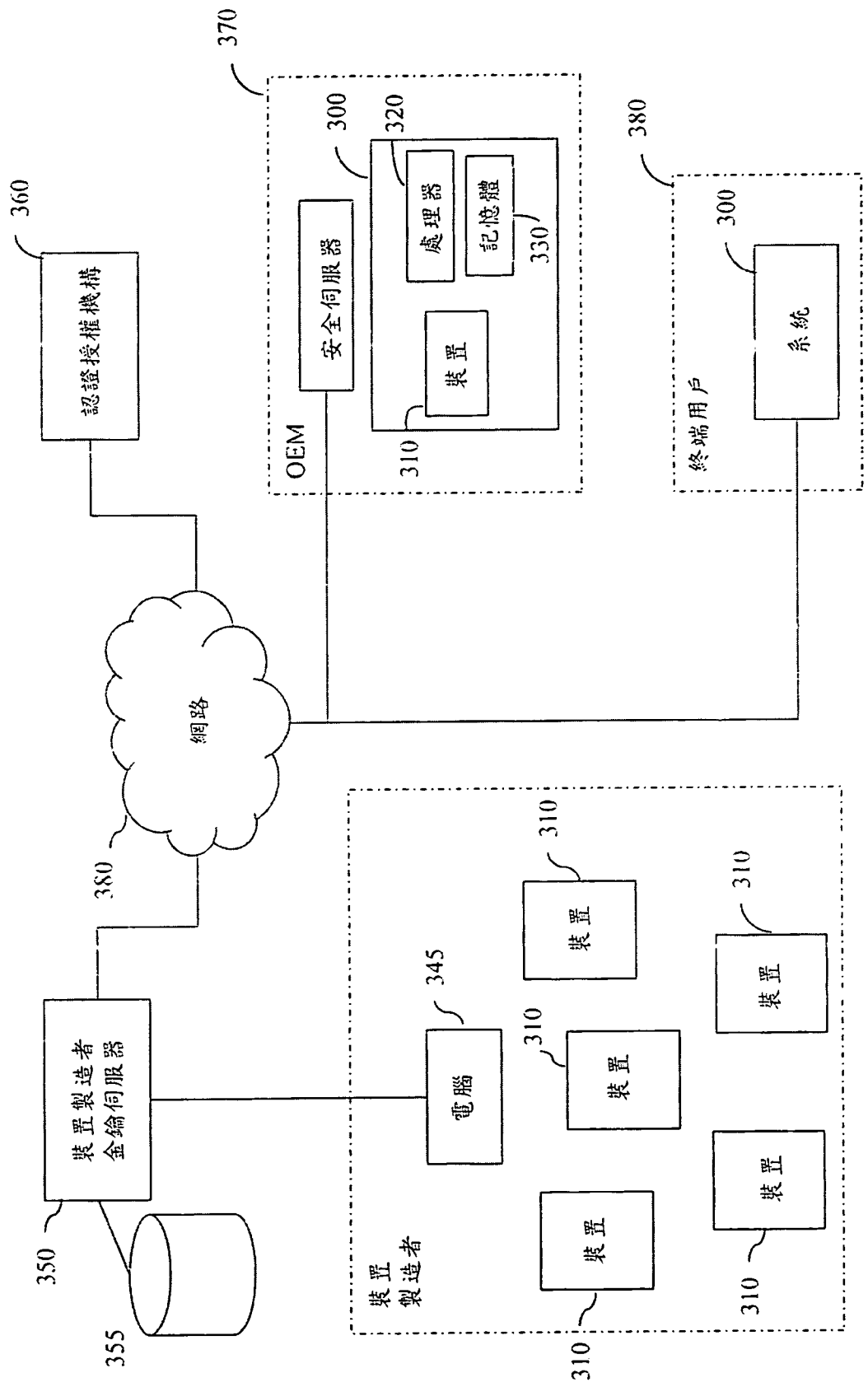


圖3

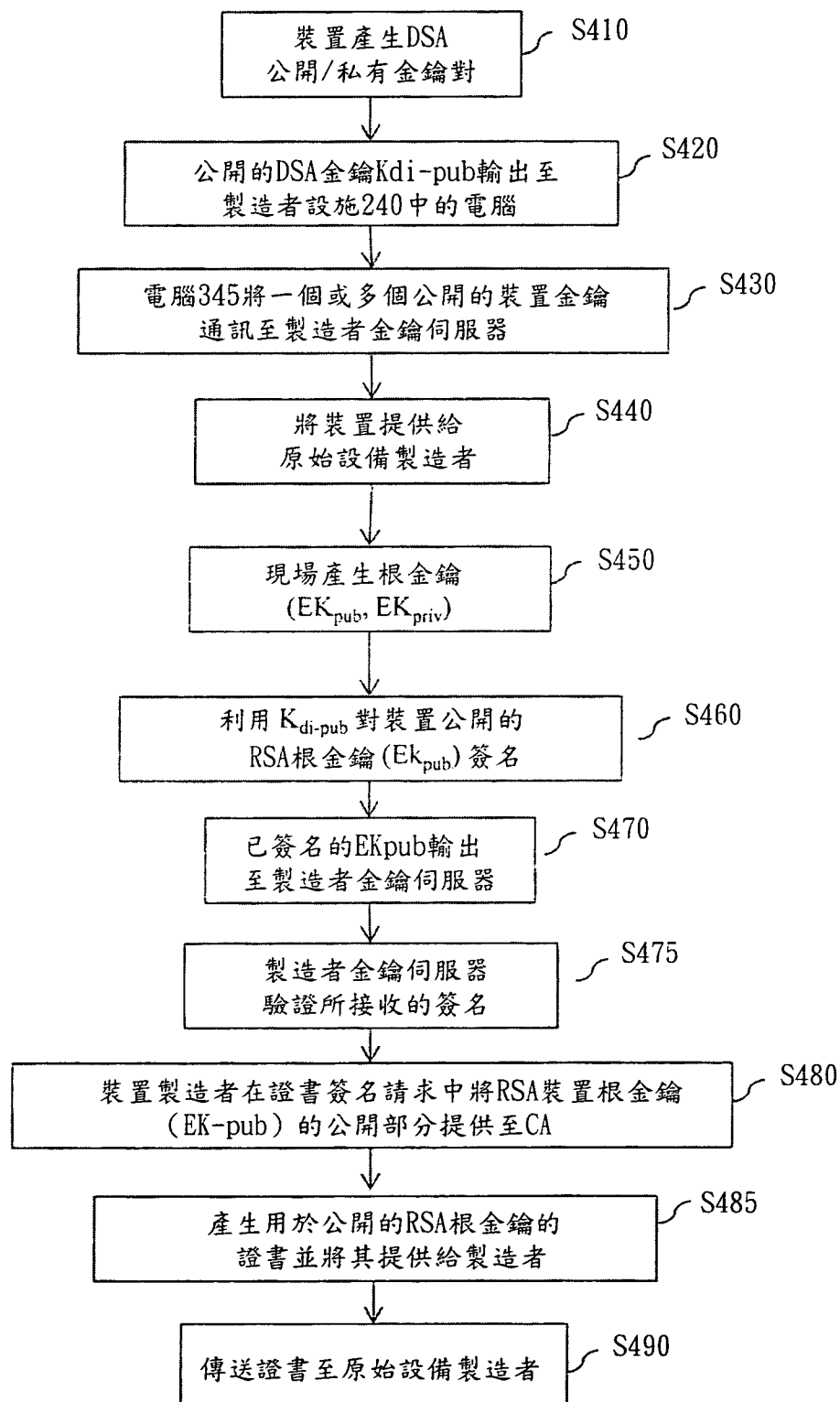


圖4

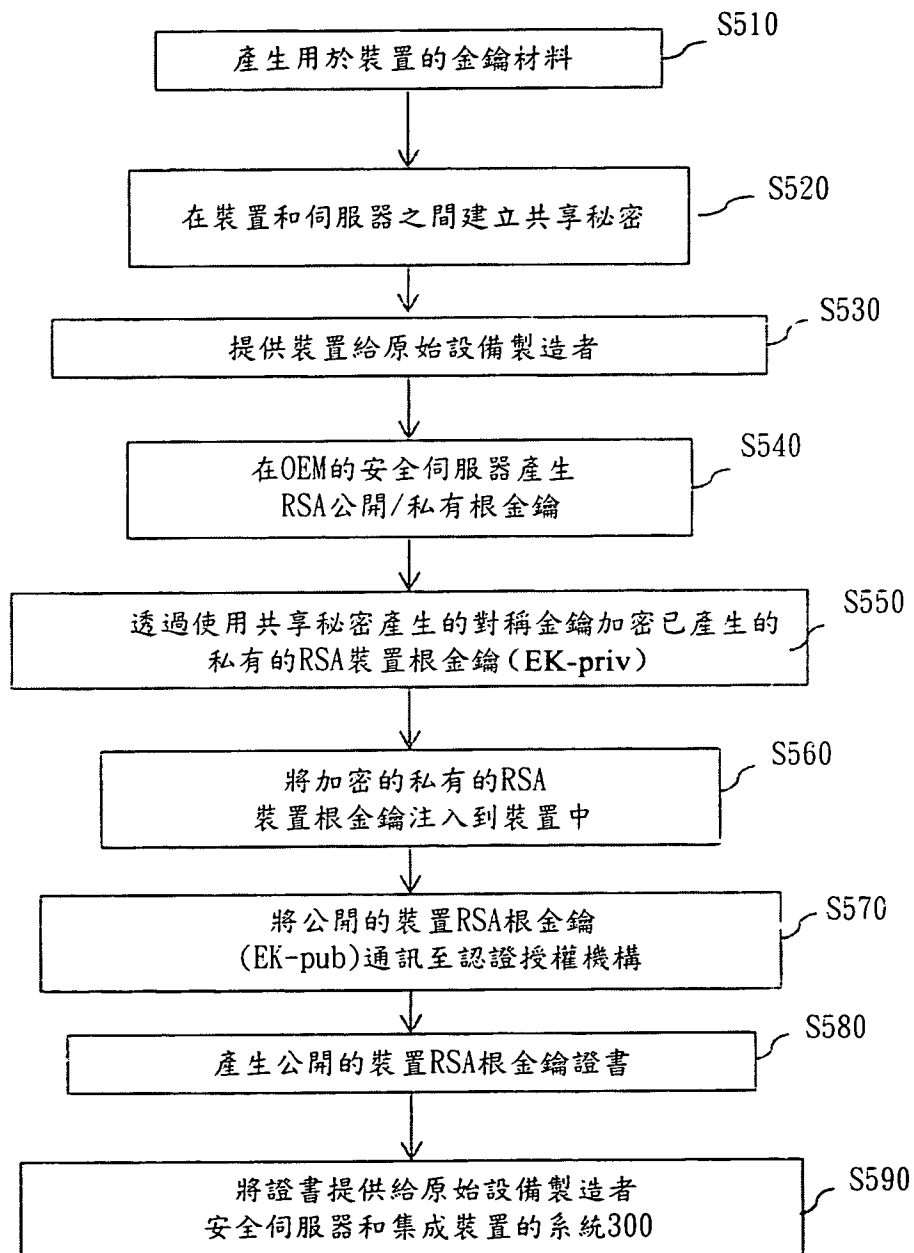


圖5

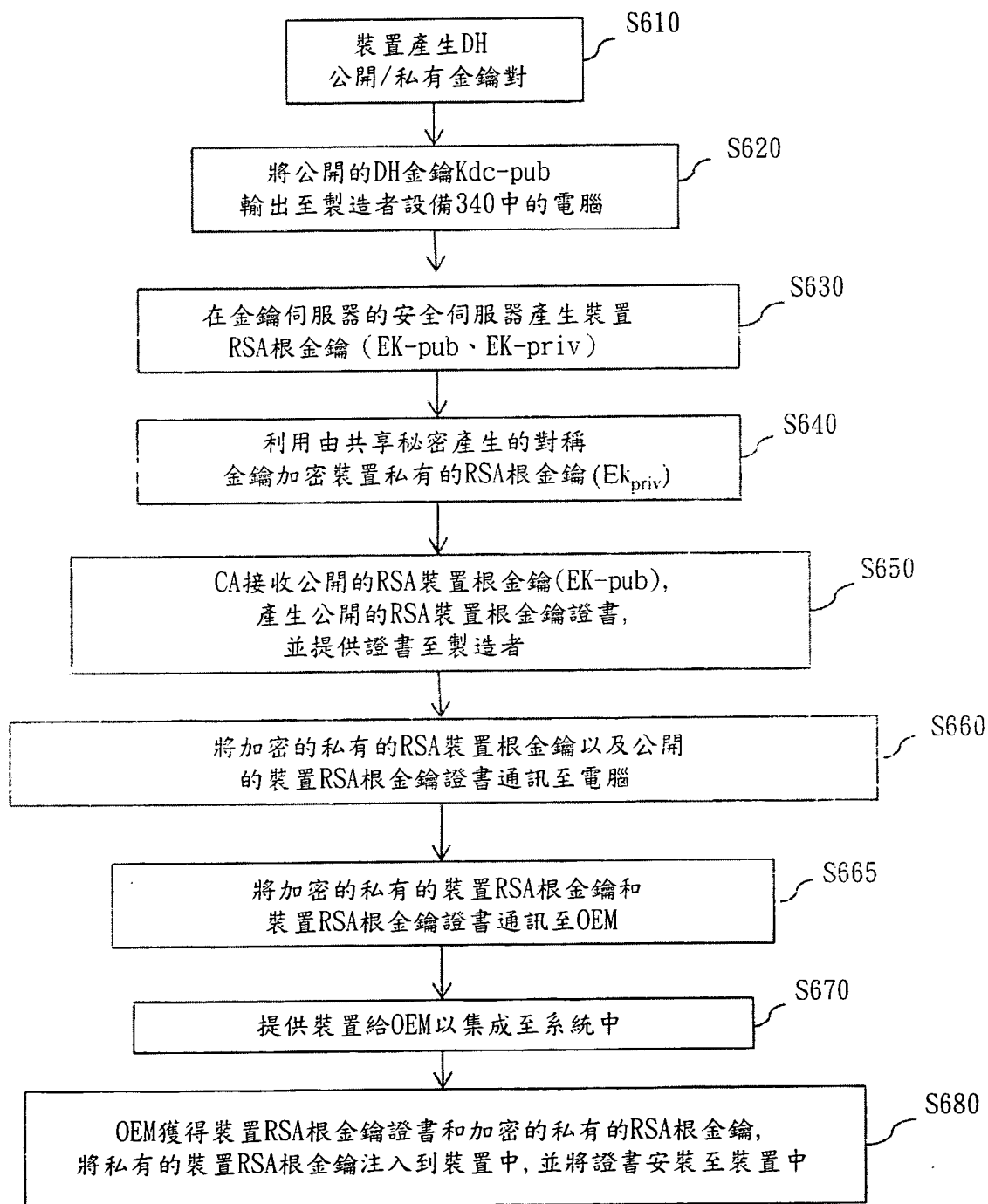


圖 6

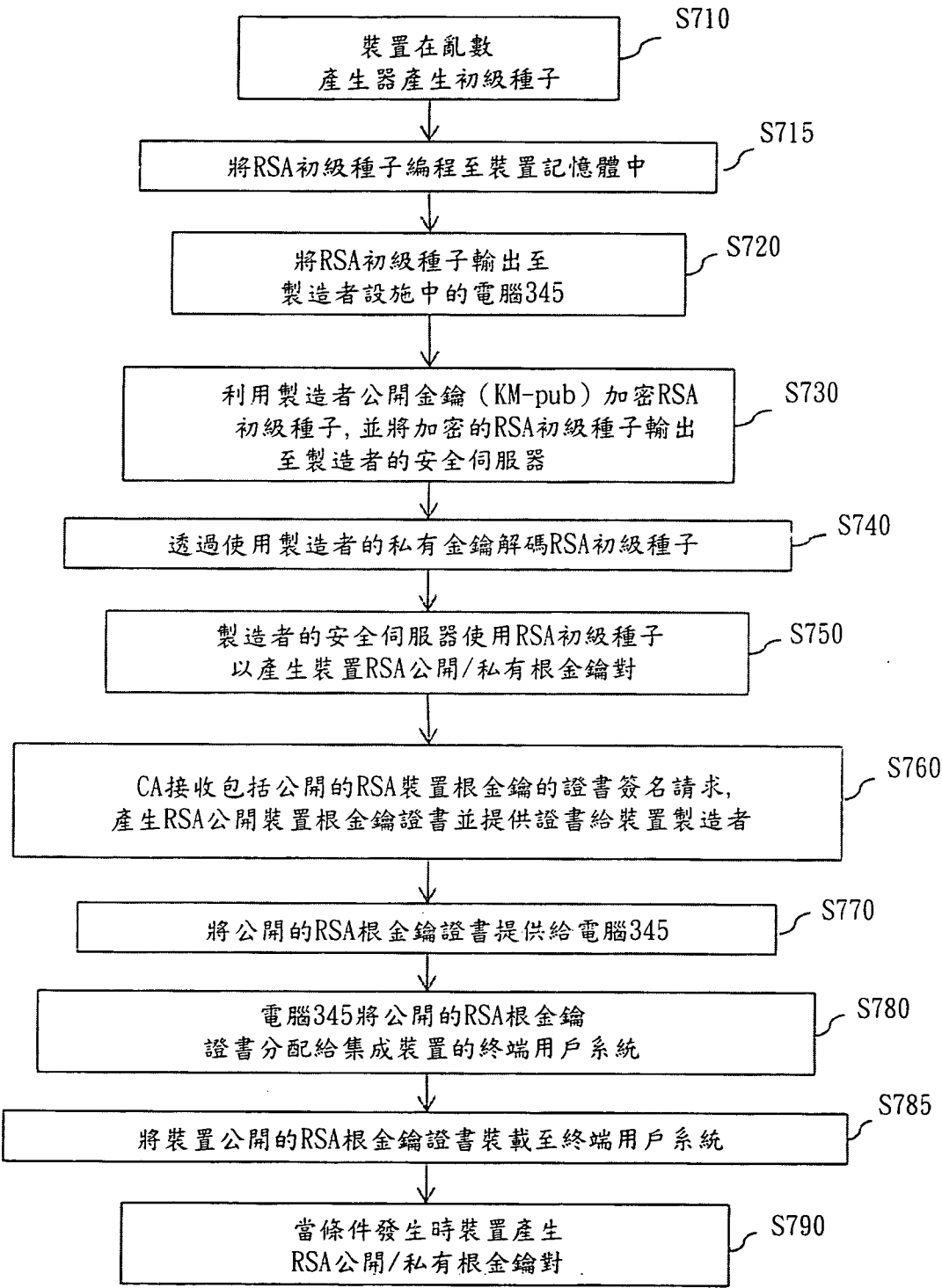


圖 7