(19)中華民國智慧財產局
(12)發明說明書公開本 (11)公開編號：TW 201412075 A
(43)公開日： 中華民國 103 (2014) 年 03 月 16 日

(21)申請案號：102123348 (22)申請日： 中華民國 102 (2013) 年 06 月 28 日
(51)Int. Cl.： *H04L9/14 (2006.01)* *H04L9/08 (2006.01)*
G06F21/62 (2013.01)
(30)優先權：2012/06/28 美國 61/665,695
2013/06/27 美國 13/928,925
(71)申請人：歐樂岡科技公司 (列支敦斯登) OLOGN TECHNOLOGIES AG (LI)
列支敦斯登
(72)發明人：伊納貞克 瑟吉 IGNATCHENKO, SERGEY (CA)
(74)代理人：陳長文
申請實體審查：無 申請專利範圍項數：35 項 圖式數：9 共 44 頁

(54)名稱

安全金鑰儲存系統、方法及裝置

SECURE KEY STORAGE SYSTEMS, METHODS AND APPARATUSES

(57)摘要

本文所描述之系統、方法及裝置提供管理私密金鑰儲存器之一計算環境。根據本發明之一裝置可包括一第一非揮發性儲存器，其用於儲存簽署數位憑證之一私密根金鑰；一輸入器件，其用於自一操作者接收手動輸入；一通信介面，其由用於自該裝置傳輸資訊之一單向傳輸器組成；及一處理器。該處理器可經組態以自該第一非揮發性儲存器擷取該私密根金鑰，透過該輸入器件接收一新數位憑證之資訊，根據該接收資訊產生新數位憑證，使用該私密根金鑰簽署該新數位憑證且使用該傳輸器自該裝置傳輸該新數位憑證。

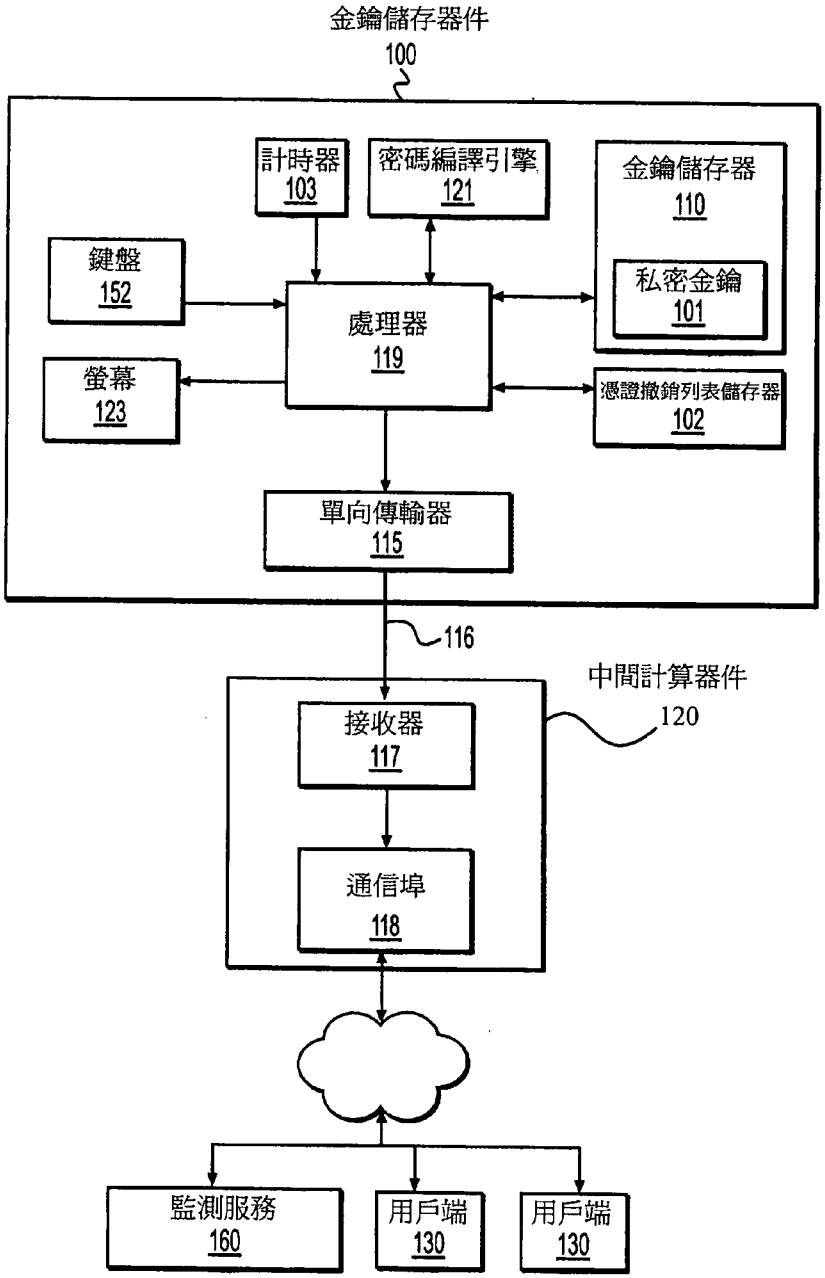

圖 1

100：金鑰儲存器件

101：密碼編譯金鑰/私密根金鑰

102：憑證撤銷列表儲存器

103：計時器

110：金鑰儲存器/記憶體

115：單向傳輸器

116：單向通信鏈接/光纖電纜

117：接收器

118：通信埠

119：處理器

120：中間計算器件/金鑰儲存器件/中間器件

121：密碼編譯引擎

123：螢幕

130：用戶端/用戶端計算器件

152：鍵盤

160：監測服務

(19)中華民國智慧財產局
(12)發明說明書公開本 (11)公開編號：TW 201412075 A
(43)公開日： 中華民國 103 (2014) 年 03 月 16 日

(21)申請案號：102123348 (22)申請日： 中華民國 102 (2013) 年 06 月 28 日
(51)Int. Cl.： *H04L9/14 (2006.01)* *H04L9/08 (2006.01)*
G06F21/62 (2013.01)
(30)優先權：2012/06/28 美國 61/665,695
2013/06/27 美國 13/928,925
(71)申請人：歐樂岡科技公司 (列支敦斯登) OLOGN TECHNOLOGIES AG (LI)
列支敦斯登
(72)發明人：伊納貞克 瑟吉 IGNATCHENKO, SERGEY (CA)
(74)代理人：陳長文
申請實體審查：無 申請專利範圍項數：35 項 圖式數：9 共 44 頁

(54)名稱

安全金鑰儲存系統、方法及裝置

SECURE KEY STORAGE SYSTEMS, METHODS AND APPARATUSES

(57)摘要

本文所描述之系統、方法及裝置提供管理私密金鑰儲存器之一計算環境。根據本發明之一裝置可包括一第一非揮發性儲存器，其用於儲存簽署數位憑證之一私密根金鑰；一輸入器件，其用於自一操作者接收手動輸入；一通信介面，其由用於自該裝置傳輸資訊之一單向傳輸器組成；及一處理器。該處理器可經組態以自該第一非揮發性儲存器擷取該私密根金鑰，透過該輸入器件接收一新數位憑證之資訊，根據該接收資訊產生新數位憑證，使用該私密根金鑰簽署該新數位憑證且使用該傳輸器自該裝置傳輸該新數位憑證。

201412075

發明摘要

※ 申請案號：102123348

※ 申請日：102.6.28　　※IPC 分類：H04L 9/14 (2006.01)
H04L 9/08 (2006.01)
G06F 21/62 (2013.01)

【發明名稱】

安全金鑰儲存系統、方法及裝置

SECURE KEY STORAGE SYSTEMS, METHODS AND APPARATUSES

【中文】

本文所描述之系統、方法及裝置提供管理私密金鑰儲存器之一計算環境。根據本發明之一裝置可包括一第一非揮發性儲存器，其用於儲存簽署數位憑證之一私密根金鑰；一輸入器件，其用於自一操作者接收手動輸入；一通信介面，其由用於自該裝置傳輸資訊之一單向傳輸器組成；及一處理器。該處理器可經組態以自該第一非揮發性儲存器擷取該私密根金鑰，透過該輸入器件接收一新數位憑證之資訊，根據該接收資訊產生新數位憑證，使用該私密根金鑰簽署該新數位憑證且使用該傳輸器自該裝置傳輸該新數位憑證。

【英文】

The systems, methods and apparatuses described herein provide a computing environment that manages private key storage. An apparatus according to the present disclosure may comprise a first non-volatile storage for storing a private root key for signing digital certificates, an input device for receiving manual input from an operator, a communication interface consisting of a one-way transmitter for transmitting information from the apparatus, and a processor. The processor may be configured to retrieve the private root key from the first non-volatile storage, receive information for a new digital certificate through the input device, generate the new digital certificate according to the received information, sign the new digital certificate using the private root key and transmit the new digital certificate from the apparatus using the transmitter.

【代表圖】

【本案指定代表圖】：第（ 1 ）圖。

【本代表圖之符號簡單說明】：

100	金鑰儲存器件
101	密碼編譯金鑰/私密根金鑰
102	憑證撤銷列表儲存器
103	計時器
110	金鑰儲存器/記憶體
115	單向傳輸器
116	單向通信鏈接/光纖電纜
117	接收器
118	通信埠
119	處理器
120	中間計算器件/金鑰儲存器件/中間器件
121	密碼編譯引擎
123	螢幕
130	用戶端/用戶端計算器件
152	鍵盤
160	監測服務

【本案若有化學式時，請揭示最能顯示發明特徵的化學式】：

無

發明專利說明書

（本說明書格式、順序，請勿任意更動）

【發明名稱】

安全金鑰儲存系統、方法及裝置

SECURE KEY STORAGE SYSTEMS, METHODS AND APPARATUSES

相關申請案

本申請案主張2012年6月28日申請之美國臨時申請案第61/665,695號及2013年6月27日申請之美國非臨時申請案第13/928,925號，兩者標題爲「Secure Key Storage Systems, Methods and Apparatuses」之優先權，該兩個申請案之內容之全文以引用方式併入本文中。

【技術領域】

本文所描述之系統、方法及裝置係關於密碼編譯金鑰之安全電子儲存器。

【先前技術】

公用金鑰基礎結構(PKI)爲用於電子認證個體之一已知機構。在PKI中，各實體(或個體)具有一唯一非對稱密碼編譯金鑰對，其包括一公用金鑰及一私密金鑰。一憑證授權單位(CA)發出一數位憑證-一電子文件-列出實體之身份之身份碼(例如，名稱及組織)及實體之公用金鑰，將該實體之身份繫結至其公用金鑰。該實體可使用其金鑰以使資訊加密且解密。例如，該實體可用其私密金鑰使其傳出訊息之全部或一部分加密，且可連同該加密訊息分佈其數位憑證。訊息接受者可使用發送者之公用金鑰使該加密訊息解密，容許該接受者證實(i)該發送者控制對應私密金鑰，且因此推斷(假定僅憑證中所識別之實體具

有對該對應私密金鑰之存取)(ii)該發送者爲數位憑證中所識別之實體。

由於基於PKI之認證其前提係假定能使用一私密金鑰之任何人必定爲對應數位憑證中所識別之實體，所以私密金鑰之安全性爲PKI之一關鍵要素。具有對一私密金鑰之存取之一未授權個體或實體可使用該私密金鑰以在電子通信及交易中模仿合法擁有者。

在一PKI環境內，一憑證授權單位(CA)可使用其根私密金鑰以簽署所有新發出之數位憑證且執行其他安全性相關功能(諸如，(例如)簽署憑證撤銷列表(CRL)及/或OCSP回應)。保護CA之根私密金鑰對維持CA之正當性及根本上維持PKI之一般概念非常重要。若一CA之跟私密金鑰被洩露，則未使用根憑證而簽署之任意者-例如，由根憑證而簽署之任意附屬憑證，或由一附屬憑證簽署之任意分葉憑證-可受信任，因此使CA基本上爲無用。同時，CA需要使用安全儲存之根金鑰快速且有效率地實行此等簽署操作。

各種系統及方法係用於保護私密金鑰免於未授權使用，其範圍自軟體等級加密至基於硬體之密碼編譯。例如，一些作業系統將私密金鑰儲存於已使用一隨機對稱金鑰(亦稱爲一主金鑰)加密之檔案中，該隨機對稱金鑰繼而被加密且儲存於該作業系統內之任意處。在其他系統中，私密金鑰可儲存於防篡改及/或篡改證據硬體中。

然而，此等系統及方法可仍易受攻擊。例如，基於軟體之安全性機構可易於受主機作業系統中之漏洞影響。一般認爲較安全之諸多基於硬體之密碼編譯器件仍受控於軟體(諸如一作業系統)或經由軟體控制，其可使該等硬體器件曝露於透過軟體中之漏洞之攻擊。若一攻擊者可指導硬體器件以簽署攻擊者所要之任意者，則在諸多案例中，其在功能上類似於擁有私密金鑰本身。

一般而言，個體可接受之安全性等級通常不足以儲存CA根金

鑰，此係由於一洩露之衝擊之差異。當一個體之金鑰被洩露時，其僅影響此個體及或許與他通信之數十人。然而，當一CA之根金鑰被洩露時，可能影響數億人。另一方面，可用於CA之資源(硬體及軟體兩者)一般比可用於普通個體之資源更有意義。

需要可提供高度安全私密金鑰儲存器之系統、方法及裝置，同時確保需要使用私密金鑰之操作可以一適時方式執行。

【圖式簡單說明】

圖1係根據本發明之一例示性器件及/或系統之一方塊圖。

圖2展示一金鑰儲存器件可藉由其而用於產生一新的附屬憑證之一例示性方法。

圖3展示一CRL可藉由其而分佈之一例示性方法。

圖4A係根據本發明之一交替器件及/或系統之一方塊圖。

圖4B描繪可用於支援圖4A所展示之系統之一操作者記錄之一例示性結構。

圖5展示一附屬憑證可藉由其而使用圖4A中所描繪之系統而發出之一例示性方法。

圖6描繪可用於支援相對於圖5所描述之方法之一「新憑證請求」之一例示性結構。

圖7展示一已發出數位憑證可藉由其而添加至一CRL使得該已發出憑證被視爲撤銷前進之一例示性方法。

圖8描繪可用於支援相對於圖7所描述之方法之一「更新CRL請求」之一例示性結構。

【實施方式】

在本文，結合下列描述及附圖描述根據本發明之系統、裝置及方法之某些繪示性態樣。然而，此等態樣僅指示可使用本發明之原理之少數各種方式，且本發明意欲包含全部此等態樣及其等效物。本發

明之其他優點及新穎特徵在結合圖考量時自下列詳細描述可變得顯而易見。

在下列詳細描述中，許多特殊細節被闡釋以提供本發明之一透徹理解。在其他例子中，未詳細展示已知結構、介面及程序以不致不必要地使本發明不清楚。然而，一般技術者將瞭解，本文所揭示之該等特殊細節無需用於實踐本發明且不表示對本發明之範疇之一限制，除了如申請專利範圍中所敘述之外。意欲本說明書之任意部分不被解譯爲否定本發明之全範疇之任意部分。儘管已描述本發明之某些實施例，但此等實施例同樣不意欲限制本發明之全範疇。

本發明提供經組態以安全儲存密碼編譯金鑰之系統、方法及裝置，而同時確保需要使用此等經儲存金鑰之操作可以一適時方式執行。例如，本文所揭示之系統、方法及裝置可對憑證授權單位(CA)根私密金鑰之儲存有用，其可能出於簽署附屬憑證之目的或出於重新簽署CRL或OCSP回應之目的而需要頻繁存取。

圖1展示根據本發明之一例示性系統。如圖1所展示，該系統首先可包括經組態以儲存及操縱秘密密碼編譯金鑰之一或多個密碼編譯金鑰儲存器件100。該金鑰儲存器件100可由能執行本文所討論之功能性之任意適當計算器件組成，諸如(但不限於)一個人電腦、一工作站、一伺服器、一特別設計之計算器件或類似者。

一金鑰儲存器件100首先可包括經組態以儲存一或多個密碼編譯金鑰101(諸如一私密金鑰(亦即，一非對稱金鑰對之私密部分))之一金鑰儲存器110。該金鑰儲存器110可爲任意合適形式之揮發性儲存器(諸如RAM)或非揮發性儲存器(諸如，一硬碟驅動、快閃記憶體、固態磁碟、CD-ROM等等)。

金鑰儲存器件100亦可包括一憑證撤銷列表(CRL)儲存器102。此CRL儲存器102可用於儲存可被一用戶端器件130用來效驗根據本發明

產生及簽署之一或多個附屬憑證之一或多個CRL。如同金鑰儲存器110，CRL儲存器102可爲任意合適形式之揮發性儲存器(諸如RAM)或非揮發性儲存器(諸如，一硬碟驅動、快閃記憶體、固態磁碟、CD-ROM等等)。

如圖1之例示性方塊圖中所展示，金鑰儲存器件100可進一步包括至少一處理器119，其尤其可經組態以：(1)擷取先前儲存於金鑰儲存器110內之一私密金鑰101；(2)使用一經擷取之私密金鑰101以簽署一附屬憑證；及/或(3)使用一經擷取之私密金鑰101以簽署一CRL。一般技術者將理解，此處理器119可爲一微控制器、電腦處理器、可程式化電路、特殊應用積體電路(ASIC)或任意其他適當器件之任意者。此外，在某些實施例中，一或多個處理器119可包含內部記憶體(諸如一快取記憶體(未展示))，其可用於暫時儲存可能被頻繁存取之某些資料(諸如所產生之CRL，如下文更詳細討論)。在其他實施例中，此一快取記憶體(未展示)可與一或多個處理器119分離，但連接至一或多個處理器119。

金鑰儲存器件100可額外包括一計時器103，其可經組態以追蹤一當前時間，且可經進一步組態以產生一或多個時戳。在某些實施例中，此計時器103可爲(例如)可使用一「原子時鐘」及/或GPS信號接收器實施之一高精度時鐘。

金鑰儲存器件100可進一步包括一或多個輸入/輸出器件(諸如，一鍵盤152、一滑鼠(未展示)、一螢幕123、任意其他合適I/O器件或其之任意組合)，其可提供資料至一使用者及/或自一使用者接收資料。例如，且如下文更詳細描述，一鍵盤152可用於輸入一附屬憑證之某些欄位，該附屬憑證係使用儲存於記憶體110內之一私密根金鑰101而簽署。輸入資料及請求發出附屬憑證可受限於經授權系統操作者，且對金鑰儲存器件120之存取可同時在實體上(例如，位於一存取受限空

間中)及/或操作上(例如，需要輸入登錄及密碼資訊)受控。

在某些實施例中，金鑰儲存器件100可進一步包括一或多個密碼編譯引擎121。此等密碼編譯引擎121可經組態以實施一或多個密碼編譯演算法(諸如AES或RSA)，且可實施於硬體、軟體或其之任意適當組合。密碼編譯引擎121可自一或多個輸入/輸出器件(諸如一鍵盤152)接收資料，以使用一私密根金鑰101加密或解密。在某些實施例中，取代密碼編譯引擎121或除密碼編譯引擎121以外，處理器119可經組態以執行此等密碼編譯行爲。

在一實施例中，金鑰儲存器件100可進一步包括一單向傳輸器115，其經組態使得金鑰儲存器件100可經由一單向通信鏈接116而傳輸資訊，但無法在該通信鏈接116上接收任意資訊。此傳輸器115可採取任意形式之硬體(及可能隨附軟體)，適於建立且維持一或多個單向通信鏈接116，其限制條件爲單向傳輸器115無法接收資料。例如，此單向傳輸器115可包括連接至一光纖電纜116之一LED，但缺少在該光纖電纜116上接收資料之一光電二極體。在另一實施例中，該單向傳輸器115可爲用於無線資料傳輸之一傳輸天線。然而，一般技術者將理解，此等參考僅爲例示性，且本發明不限於任意特殊形式之單向通信技術。

在一實施例中，除了需要存在接近於該器件100之一人來完成輸入之硬體及/或軟體(例如，一鍵盤152及/或一滑鼠(未展示))之外，金鑰儲存器件100缺少允許或接收來自一外部源之輸入之任意硬體及/或軟體。

如圖1所展示，一單向通信鏈接116可將金鑰儲存器件100連接至一中間計算器件120。如將在下文更詳細描述，該中間計算器件120可用於將接收自金鑰儲存器件100之資訊(諸如，經簽署之附屬憑證)傳輸至一或多個其他用戶端計算器件130(例如，需要透過使用一附屬憑

證效驗分葉憑證之伺服器或終端使用者電腦)以用於PKI。使用一單向連接可增強系統之安全性，使得其他電子器件無法藉由使用金鑰儲存器件100與中間計算器件120之間之連接而遠端修改或存取金鑰儲存器件100(包含其金鑰儲存器110)。

另外，可期望確保金鑰儲存器件100爲結構上安全。例如，金鑰儲存器件100可經建構使得其爲防篡改或至少篡改證據。在某些實施例中，此可能意謂，(例如)金鑰儲存器101將在未授權存取或另外篡改金鑰儲存器件100之後自動破壞。

如上文所注意，圖1所展示之例示性系統亦可包括一中間計算器件120。該中間計算器件120可爲任意形式之計算器件(諸如一個人電腦、伺服器、膝上型電腦、桌上型電腦、平板電腦或其他專門器件)，其經組態以：(i)經由單向通信鏈接116自金鑰儲存器件100自單向傳輸器115接收資訊，及(ii)將接收自金鑰儲存器件100之資訊傳輸至一或多個其他計算器件130以用於PKI。

如圖1中所展示，一例示性中間計算器件120首先可包括一接收器117，其經組態以經由單向通信鏈接116自金鑰儲存器件之單向傳輸器115接收資料。例如，若該單向傳輸器115爲連接至一光纖電纜116之一LED，則中間計算器件之接收器117可包括一光電二極體以及相關聯之硬體及軟體以接收且解碼資訊。

中間計算器件120可進一步包括合適於將資訊發送至一或多個其他計算器件130及/或接收資訊之一或多個通信埠118。該一或多個通信埠118可由適於建立及維持雙向通信之硬體及/或軟體之任意組合組成，其包含(但不限於)有線協定(諸如，串列、平行、共軸、USB、乙太網路、LAN、WAN、網際網路)及無線協定(諸如，藍芽、近場通信、紅外線、IEEE 802.11及蜂巢式連接器(諸如3G、4G及4G LTE))。然而，應理解，此等參考僅爲例示性，且本發明不限於任意特殊形式

之通信技術。例如，此通信埠118可用於將新產生之附屬憑證發送至其意欲之持有人以用於PKI或在PKI內分佈CRL。

最後，儘管未展示於圖1，但一般技術者將理解，中間器件120可包含一或多個額外組件部分，諸如，額外處理器、記憶體、其他資料儲存單元、資料傳輸線、通信埠及/或其他專門電路。

亦可期望將金鑰儲存器件100及中間計算器件120兩者放置於一安全設備內，使得僅某些預授權個體具有對金鑰儲存器件100及中間計算器件120所定位之空間或區域之存取。此可進一步增強系統及儲存於器件100內之私密根金鑰101之安全性。

然而，應理解，儘管可採取措施以確保中間計算器件120之安全性，然相較於金鑰儲存器件100之安全性，該中間計算器件120之安全性可較不緊要，使得即使該中間計算器件120被洩漏，一惡意實體可藉由攻擊該中間計算器件120達成之極限爲拒絕服務。

在某些實施例中，金鑰儲存器件100可經組態使得一操作者必須與該金鑰儲存器件100直接互動(即，透過經由(例如)鍵盤152提供之操作者輸入)以使用一經儲存之私密根金鑰101。換言之，若一操作者希望產生一新的附屬憑證或簽署一CRL，則該操作者必須使用一I/O器件手動輸入命令(及任意支援資料)，該I/O器件需要操作者實體上接近於金鑰儲存器件100。

圖2展示一金鑰儲存器件100可藉由其而用於產生一新的附屬憑證之一例示性方法。

在步驟200處，金鑰儲存器件100可自一操作者接收一命令以產生一新的附屬憑證。在具有一鍵盤152之實施例中，操作者可使用此鍵盤152手動輸入命令。

在步驟205處，金鑰儲存器件100可提示一操作者輸入附屬憑證所必需之一或多個欄位。例如，若附屬憑證爲一X.509憑證，則可提

示操作者輸入至少下列各者：(i)憑證所發出之實體(或個人)之名稱；(ii)憑證所發出之實體(或個人)之公用金鑰，以及該金鑰意欲與其一起使用之公用金鑰演算法之名稱；及/或(iii)憑證之有效週期，即，附屬憑證在其內爲有效之日期及時間。該憑證亦可需要一序列號，其可由一操作者輸入，由金鑰儲存器件100自動產生，或兩種方法在一單一器件100中皆爲可能的。

在步驟215處，金鑰儲存器件100可提示操作者選擇一經儲存之根私密金鑰101以用來簽署新產生之附屬憑證。若該金鑰儲存器件100經組態使得其僅儲存一個私密金鑰101，則此步驟可不必要。在器件100儲存多個私密根金鑰101之實施例中，操作者可藉由(例如)提供或選擇根私密金鑰101應使用於數位簽署憑證之實體之一識別符(例如，對應於所期望根私密金鑰101之一名稱或一公用金鑰)而選擇所期望金鑰101。

在步驟220處，金鑰儲存器件100可自操作者接收此私密金鑰101資訊，且可在金鑰儲存器110內擷取對應私密金鑰101。

在步驟225處，金鑰儲存器件100可使用在步驟205及220處所接收之資訊而產生附屬憑證。應理解，產生附屬憑證可包含金鑰儲存器件100產生及/或供應某些額外資訊(諸如，展示產生憑證之時間之一時戳)。

在步驟230處，金鑰儲存器件100可使用在步驟220處所擷取之金鑰而數位簽署所產生之附屬憑證，且可包含此數位簽名作爲新產生之附屬憑證之部分。例如，若新產生之憑證爲一X.509憑證，則X.509標準指定該簽名應如何產生且放置於憑證內。

在步驟235處，金鑰儲存器件100可使用其單向傳輸器115以經由單向通信鏈接116將新產生之附屬憑證(包含其相關聯之數位簽名)發送至中間計算器件120。

作爲一額外安全性措施，視情況在步驟240處，金鑰儲存器件100可經由單向通信鏈接116而將包含關於其近期行爲之資訊之一訊息發送至中間計算器件120。例如，該訊息可包括關於行爲類型(例如，發出一新憑證)及行爲時間之資訊。在任選步驟245處，中間計算器件120可將該訊息轉遞至能分析及/或監測金鑰儲存器件100之行爲之一監測服務160。例如，若此一監測服務接收指示一問題或不適當行爲(例如，該行爲發生在通常不應發生行爲之一時間)之一訊息時，則此一監測服務可對一適當的個人及/或器件(未展示)發出一警報或一警告。替代地，中間計算器件120可分析該訊息中之資訊且引發適當警告或警報。

在某些實施例中，可期望使不需要實質操作者輸入之一或多個私密金鑰101操作自動化。例如，在一寬範圍之PKI系統中，期望提供一數位簽署訊息之接受者可藉由其自適當CA獲得訊息發送者之數位憑證(其可用於認證訊息)仍有效之證實之一機構。此證實通常爲一CRL (或一OCSP回應)之形式。各CRL一般包含一時戳，且藉由適當CA數位簽署。對於提供充分安全性之此方案(特定言之，防止重播攻擊)，新的CRL一般定期(例如，每天一次或每小時一次)重新發出。除非一憑證撤銷發生於一CRL重新發出之間，否則新重新發出之CRL一般與先前CRL完全相同(除時戳及簽名之外)，且可如下文所描述而自動重新發出且無需操作者輸入。

圖3展示一金鑰儲存器件100可藉由其重新發出且分佈儲存於CRL儲存器102內之一或多個CRL之一例示性方法。重新分佈一CRL之命令可基於通過一預定時間量由金鑰儲存器件100自動產生。例如，在某些實施例中，金鑰儲存器件100可經組態以每天一次、每小時一次或每一些其他時間間隔一次自動重新發出且重新簽署一CRL。在其他實施例中，重新分佈一CRL之命令可由一操作者手動起始。

在又其他實施例中，重新分佈一CRL之命令可在一操作者更新CRL儲存器102中之一CRL時自動產生。爲增強安全性，根據本發明之實施例可經組態以需要操作者手動更新CRL，即，在操作者未經由(例如)鍵盤152將資料輸入至金鑰儲存器件100之情況下，CRL可不被更新。在此等實施例中，應理解，操作者可能需要特別識別用以更新及重新分佈之CRL儲存器102內之一特定CRL，及應使用於數位簽署經更新之CRL之特定私密根金鑰101。

在步驟300處，金鑰儲存器件100可自CRL儲存器102擷取適當CRL。接著，在步驟305處，金鑰儲存器件100可將一時戳添加至CRL。此時戳可由(例如)計時器103產生。在步驟310處，金鑰儲存器件100可使用適當私密金鑰101而數位簽署經添加時戳之CRL。

在步驟315處，金鑰儲存器件100可將一或多個錯誤偵測及/或錯誤校正碼附加至具有經簽署之CRL之訊息。由於連接116爲一單向連接-及因此，傳統校正方法(涉及來自將接收CRL之中間計算器件120之回饋)(例如，TCP再傳輸)係不可能的-錯誤偵測及/或校正碼可用於促進CRL之可靠遞送。

在一實施例中，可將一訊息核對和(例如，一循環冗餘檢查(諸如CRC-32))添加至訊息以使能偵測傳輸中之錯誤。在另一實施例中，可發送不具有額外核對和之訊息，及中間器件120可代以依靠於CRL之簽名驗證(步驟335處所執行，如下文所描述)。

取代錯誤偵測機構或除錯誤偵測機構以外，一些實施例可提供一或多個錯誤校正碼(諸如，(例如)漢明(Hamming)碼或里德索羅門(Reed-Solomon)碼)之使用，其可用於校正可在資料傳輸程序期間發生之偶然錯誤。

在步驟320處，可經由單向傳輸器115在單向連接116上將訊息(即，CRL，包含其數位簽名以及錯誤偵測及校正碼(若存在))發送至

中間計算器件120，及在步驟325處，中間計算器件120可經由接收器117接收經簽署之訊息。

在步驟330處，取決於錯誤之實際存在及由金鑰儲存器件100發送之錯誤偵測/校正碼之本質，可執行各種錯誤偵測及校正，及在步驟335處，所接收之CRL可使用對應於用於簽署CRL之根私密金鑰101之公用金鑰而效驗。在步驟340處，若成功通過步驟330及335處執行之校正及效驗，則可將CRL重新分佈至一或多個用戶端130以用於進一步使用。在另一實施例中，可將CRL公佈於網際網路上。在一些實施例中，中間計算器件120可快取所接收之CRL，且回覆一或多個用戶端130請求而提供該所接收之CRL。

在一些實施例中，對於各經簽署之CRL，可期望重複步驟320至340多次。例如，一CRL可能僅需要每天重新簽署一次，但相同經簽署之CRL可在當天之中在單向連接116上每分鐘重新傳輸一次。以此方式，若經由單向連接116之任意給定傳輸被中斷或另外受到不利影響，則其在步驟330至335中之效驗之一者將失敗(且隨後將丟棄)，但可在其後不久之一隨後傳輸期間獲取適當訊息。

由於單向通信鏈接116之單向性質，應理解，(若可能)非常難以將一遠端攻擊(除針對中間計算器件120之一DoS攻擊之外)安裝於儲存於金鑰儲存器件100內之一私密金鑰101上，即使中間計算器件120在攻擊者之完全控制下。

相對於圖3之前述討論係關於CRL之重新發出及分佈。在一些實施例中，取代重新發出CRL(或除重新發出CRL之外)，可期望重新發出OCSP回應。在此等實施例中，上文相對於圖3所描述之用於CRL之例示性方法可用於重新發出OCSP回應(不具有一臨時擴展)。相應地，取代金鑰儲存器件100定期重新簽署及重新發送CRL，該金鑰儲存器件100可在單向鏈接116上(以及CRL或取代CRL)以相同於對於

CRL所描述之方式定期重新簽署及重新發送OCSP回應。例如，該金鑰儲存器件100可對於藉由儲存於該金鑰儲存器件100內之一私密根金鑰101發出之各有效憑證而重新簽署及重新發送一OCSP回應。

應理解，儘管相對於圖3所展示之方法已集中於CRL及OCSP回應，然此等訊息格式僅爲例示性，且其他類似訊息亦可以一類似方式以如相對於圖3所描述之相同或類似時間間隔重新簽署。

應進一步注意，在一些實施例中，一根私密金鑰持有人(諸如一CA)可選擇不簽署CRL及/或OCSP回應自身，而將CRL及/或OCSP回應之簽署委派給具備一附屬金鑰(具有一適當憑證，例如由根私密金鑰持有人簽署之一憑證)之一「委派簽名者」。

在具有一委派簽名者之實施例中，如相對於圖1所描述而組態之一金鑰儲存器件可：(i)儲存根私密金鑰；(ii)發出一或多個憑證(包含用於委派簽名者之憑證)；(iii)更新、發出及重新發出一或多個CRL(若任意此憑證被洩漏，則CRL可經更新以包含一委派簽名者之一憑證)；及/或(iv)發出及重新發出一或多個OCSP回應(包含一委派簽名者之OCSP回應)。

在具有一委派簽名者之一些實施例中，一第一金鑰儲存器件100可儲存根私密金鑰且發出一或多個憑證(包含用於委派簽名者之憑證)，而再次如相對於圖1所描述而組態之一第二金鑰儲存器件100可儲存委派簽名者金鑰作爲一根私密金鑰且負責發出/重新發出CRL及/或OCSP回應。

圖4A描繪根據本發明之一交替實施例。在一些情形中，可能需要CA足夠頻繁地發出新憑證，而需要一操作者手動輸入新憑證資訊可能不切實際。圖4A中所描繪之例示性系統經組態以容許與一金鑰儲存器件400之極有限雙向通信，如本文更詳細描述。此可容許將資料(諸如新憑證資訊)自一中間計算器件420傳輸至金鑰儲存器件400

中，但由於對進入該金鑰儲存器件400中之通信之明顯限制，系統之整體安全性可被保留。

將理解，除了如本文另外特別注意之外，金鑰儲存器件400、中間計算器件420及任意用戶端器件130之各者之組件可在結構上及功能上類似於已相對於圖1描述之類似編號之對應物。

如圖4A中所展示，一金鑰儲存器件400可包括：一金鑰儲存器110，其經組態以儲存一或多個密碼編譯金鑰101；一或多個CRL儲存器102，其用於儲存一或多個CRL；至少一處理器119，其經組態以擷取及操縱一或多個經儲存之私密根金鑰101；一計時器103；一或多個輸入/輸出器件，諸如，一鍵盤152、一滑鼠(未展示)、一螢幕123或其之任意組合；及/或一或多個密碼編譯引擎121。

不同於圖1中所描繪之實施例，如圖4A中所展示之一金鑰儲存器件400可包括一雙向收發器415，而非一單向傳輸器115。類似地，中間計算器件420可包括一雙向收發器417，而非一單向接收器117，使得該金鑰儲存器件400與該中間計算器件420可藉由一雙向連接416而連接。

然而，在此一實施例中，該雙向連接416可為一非可路由點對點連接(諸如一RS-232或10BASE-T連接)，而非一規則網路連接(諸如傳統TCP/IP網路)。若該雙向連接416為一10BASE-T(或類似)連接，則應理解，在一些實施例中，確保此為一嚴謹OSI等級1連接(即，不具有對應OSI等級2層)可為較佳。儘管使用一等級2連接係可能的，但應理解，在某些實施例中，使用等級2連接可因一增加之攻擊表面而不利影響安全性。然而，一般技術者將理解，此等參考僅為例示性，且本發明不限於任意特殊形式之通信技術。在此實施例中，該系統可支援因外部約束而取決於用於提供任意必需資料之網路存取之憑證操作。

在某些實施例中，該系統僅可容許由金鑰儲存器件400在雙向連

接416上接受一極有限組之操作，而需要手動完成或自動發出其他操作。例如，在一例示性實施例中，金鑰儲存器件400可經組態以經由雙向連接416接收一指令以產生一新憑證，但可經進一步組態以需要一指令來更新在鍵盤152上手動輸入之一CRL，且需要一指令來重新發出在金鑰儲存器件100內自動發出(例如，基於計時器103)之一CRL。

此外，一金鑰儲存器件400可包括列出遠端操作者435之一資料庫413，該等遠端操作者435經授權以在雙向連接416上發出該金鑰儲存器件400執行某些操作之請求。圖4B展示此資料庫413內之一例示性遠端操作者記錄450，其展示一經授權遠端操作者之一或多個屬性。如圖4B所展示，各記錄450可包括(例如)一操作者ID 452、一操作者公用金鑰454(其可用於操作者簽名驗證)，及容許一特定操作者執行之一列表之操作456(例如，簽署新憑證)。出於安全性原因，在某些實施例中，可手動輸入及維持此一列表。

一或多個遠端操作者435可(透過一中間計算器件420)使用一遠端計算器件而連接至一金鑰儲存器件400。遠端操作者435可使用此一遠端計算器件以將命令提供至金鑰儲存器件400及以另外方式操作金鑰儲存器件400。一遠端操作者435可(例如)接收且處理來自一客戶440之一或多個憑證簽署請求(CSR)，如將相對於圖5及圖6更詳細描述。

應認知，取決於如熟習此項技術者所理解之背景，如本文所使用之遠端操作者435可意指操作遠端計算器件之一個人，遠端計算器件本身或兩者。

圖5繪示可藉由其使用圖4所描繪之系統而發出一附屬憑證之一例示性方法。圖6描繪可用於支援相對於圖5所描述之方法之一「新憑證請求」600之一例示性結構。

在步驟500處，一遠端操作者435可自一憑證申請者(例如客戶

440)接收一新憑證簽署請求(CSR)。一CSR可包含識別該申請者之資訊(諸如一X.509憑證之情況下之一區別名稱及/或其他欄位)，及由該申請者選擇之公用金鑰(例如，一申請者可產生一公用/私密金鑰對且發送該公用金鑰作爲CSR之一部分)。該CSR可進一步伴隨其他身份碼或身份證明。

在步驟505處，遠端操作者435可檢視CSR，驗證申請者之身份碼，且判定是否應簽署申請者之憑證。

在步驟510處，遠端操作者435可準備一新憑證請求600。此一請求600可包括：(i)憑證簽署請求610(如接收自申請者)；(ii)一根私密金鑰識別符620，其指示應使用哪一個經儲存之根私密金鑰101來簽署新產生之附屬憑證；(iii)操作者ID 630，其識別遠端操作者435；及(iv)操作者之數位簽名640，其可用於展示請求600係由操作者ID 630識別之遠端操作者435準備。該請求600可視情況包括其他相關資訊(未展示)。

在步驟515處，遠端操作者435可將新憑證請求600發送至中間計算器件420。取於遠端通信器件435與中間計算器件420之間之通信鏈接之本質，該中間計算器件420可執行適當接收請求之一或多個驗證。在步驟520處，可將新憑證請求600自中間計算器件420(使用其雙向收發器417)傳輸至金鑰儲存器件400。

在接受新憑證請求600之後，金鑰儲存器件400可相對於該新憑證請求600而執行一或多個驗證以證實其之真實性。例如，在步驟525處，金鑰儲存器件400可驗證：(i)操作者之資料庫413包括用於具有操作者ID 630之一遠端操作者435之一記錄450；(ii)經識別之遠端操作者435具有用以簽署新憑證之適當授權(如欄位456中所發現)；及/或(iii)遠端操作者之數位簽名640可藉由遠端操作者之金鑰454驗證。若此等驗證之一或多者失敗，則可拒絕產生一新憑證之請求。在一些實

施例中，可將反映作出且拒絕一請求之事實之一訊息發送至中間計算器件420，使得該中間計算器件420可將此訊息轉遞至能記入、分析及/或監測金鑰儲存器件400之行爲之一監測服務160。

另外，若所有驗證成功通過，則在步驟530處，金鑰儲存器件400可自金鑰儲存器110擷取由識別符620識別之根私密金鑰101。

在步驟535處，金鑰儲存器件400可使用憑證簽署請求610中所發現之資訊而產生新的附屬憑證，及在步驟540處，金鑰儲存器件400可使用在步驟530處擷取之金鑰而數位簽署該所產生之附屬憑證，且可將此數位簽名添加至該新產生之附屬憑證。

在步驟545處，金鑰儲存器件400可使用其雙向收發器415以經由雙向通信鏈接416將新產生之附屬憑證(及其相關聯之數位簽名)發送至中間計算器件420。

作爲一額外安全性措施，視情況在步驟550處，金鑰儲存器件400可經由雙向通信鏈接416將具有關於其近期行爲之資訊之一訊息發送至中間計算器件420。例如，該訊息可包括關於行爲類型之資訊(例如，處理一新憑證請求)、遠端操作者之操作者ID，及/或由金鑰儲存器件400接收新憑證請求之時間。在任選步驟555處，中間計算器件420可將此訊息轉遞至能記入、分析及/或監測金鑰儲存器件100之行爲之一監測服務160。例如，若一監測服務接收指示一問題或不適當行爲 (例如，該行爲發生在通常不應發生行爲之一時間)之一訊息，則此一監測服務可對一適當的個人或器件(未展示)發出一警報或一警告。替代地，中間計算器件420可記入、分析及/或監測該訊息中之資訊且發出適當警告或警報。

在一些實施例中，爲增強安全性，可藉由一個以上之遠端操作者簽署一新憑證請求。在此一實施例中，新憑證請求600可包含一個以上遠端操作者ID 630，及對應數量之遠端操作者簽名640。例如，

兩個遠端操作者可獨立驗證一憑證申請者之身份碼且簽署請求。在此等實施例中，在步驟525處，金鑰儲存器件400可驗證列於憑證請求600中之所有遠端操作者ID 630之數位簽名640。

在另一實施例中，相對於圖4所展示之系統可支援一或多個額外操作。圖7展示可藉由其將一先前發出之數位憑證添加至一CRL使得該經發出之憑證被視爲撤銷前進之一例示性方法。圖8描繪可用於支援相對於圖7所描述之方法之一「更新CRL請求」800之一例示性結構。

在步驟700處，一遠端操作者435可準備一「更新CRL請求」800以傳輸至金鑰儲存器件400。

更新CRL請求800首先可包括一CRL識別符810，其可爲(例如)CRL之名稱或對應於在過去已被用於簽署CRL之根私密金鑰101之一公用金鑰。更新CRL請求800可進一步包括一憑證識別符820，諸如應被撤銷之憑證之一序列號。該更新CRL請求800可進一步包括一根私密金鑰識別符830，其指示應使用哪一個經儲存之根私密金鑰101來重新簽署經更新之CRL。

另外，此更新CRL請求800可包括(i)一操作者ID 840，其可用於識別遠端操作者，及(ii)遠端操作者之數位簽名850，其可用於展示請求800係由操作者ID 840識別之遠端操作者準備。該請求800可視情況包括其他相關資訊。

在步驟710處，遠端操作者435可將該更新CRL請求800發送至中間計算器件420。取決於遠端操作者435與中間計算器件420之間之通信鏈接之本質，該中間計算器件420可執行適當接收請求之一或多個驗證。

在步驟715處，可將更新CRL請求800自中間計算器件420(使用其雙向收發器417)傳輸至金鑰儲存器件400，及在步驟720處，可藉由金

鑰儲存器件400(使用其雙向收發器415)接收更新CRL請求。

在接受更新CRL請求800之後，金鑰儲存器件400可相對於該更新CRL請求800而執行一或多個驗證以證實其真實性。例如，在步驟725處，金鑰儲存器件400可驗證：(i)遠端操作者之資料庫413包含用於具有操作者ID 840之一遠端操作者之一記錄450；(ii)經識別之遠端操作者435具有適當授權以更新CRL(如在欄位456中所發現)；及(iii)遠端操作者之數位簽名850可由遠端操作者之金鑰454驗證。若此等驗證之一或多個失敗，則可拒絕更新CRL之請求。在一些實施例中，可將反映作出且拒絕一請求之事實之一訊息發送至中間計算器件420，使得該中間計算器件420可將此訊息轉遞至能記入、分析及/或監測金鑰儲存器件400之行爲之一監測服務160。

若在此步驟725處成功效驗遠端操作者身份碼，則在步驟730處，金鑰儲存器件400可自金鑰儲存器110擷取由識別符830識別之根私密金鑰101，且在步驟735處，金鑰儲存器件100可自CRL儲存器102擷取適當CRL。

在步驟740處，金鑰儲存器件100可將憑證識別符820添加至CRL，及在步驟745處，可使用(例如)計時器103將一時戳附加至CRL。在步驟750處，金鑰儲存器件100可使用適當私密金鑰101數位簽署經添加時戳之CRL。在步驟755處，可經由雙向收發器415在雙向連接416上而將經簽署之訊息(即，CRL及數位簽名)發送至中間計算器件420。現可將經更新之CRL適當地分佈至用戶端130。另外，例如，可自動重新發出此經更新之CRL，如相對於圖3所描述。此外，金鑰儲存器件400可藉由執行類似於如相對於圖5討論之步驟550及555之步驟而報告關於其近期行爲之資訊。

應注意，在一些實施例中，爲增強安全性，可由一個以上遠端操作者簽署一更新CRL請求。在此等實施例中，更新CRL請求800可

包含一個以上遠端操作者ID 840及對應數量之數位簽名850。在此等實施例中，在步驟725處，金鑰儲存器件100可驗證列於該更新CRL請求800中之所有遠端操作者ID 840之數位簽名850。

儘管已繪示及描述本發明之特殊實施例及申請案，但應理解，本發明不限於本文所揭示之精確組態及組件。本文所使用之術語、描述及圖僅以繪示方式闡釋且不意謂限制性。在不脫離本發明之精神及範疇之情況下，可在本文所揭示之本發明之裝置、方法及系統之配置、操作及細節中作出熟習此項技術者將瞭解之各種修改、改變及變更。藉由非限制實例，應理解，本文所包含之方塊圖意欲展示各裝置及系統之組件之一選擇子組，及各成像裝置及系統可包含圖式上未展示之其他組件。另外，一般技術者將認知，在不減損本文所描述之實施例之範疇或效能之情況下，可省略或重新排序本文所描述之某些步驟及功能。

組合本文所揭示之實施例而描述之各種繪示性邏輯區塊、模組、電路及演算法步驟可被實施爲電子硬體、電腦軟體或兩者之組合。爲繪示硬體與軟體之此互換性，上文一般已根據其功能性而描述各種繪示性組件、區塊、模組、電路及步驟。此等功能性是否被實施爲硬體或軟體取決於施加於整體系統上之特定應用及設計約束。對於各特定應用，可以各種方式實施所描述之功能性-諸如藉由使用微處理器、微控制器、場可程式化閘極陣列(FPGA)、特殊應用積體電路(ASIC)及/或單晶片系統(SoC)之任意組合-但此等實施方案決策不應解譯爲引起本發明之範疇之一偏離。

組合本文所揭示之實施例而描述之一方法或演算法之步驟可在硬體中、由一處理器實行之一軟體模組中或二者之一組合中直接體現。一軟體模組可駐存於RAM記憶體、快閃記憶體、ROM記憶體、EPROM記憶體、EEPROM記憶體、暫存器、硬碟、一可移除磁碟、

一CD-ROM或技術中已知之任意其他形式之儲存媒體中。

本文所揭示之方法包括用於達成所描述之方法之一或多個步驟或行動。在不脫離本發明之範疇之情況下，該等方法步驟及/或行動可彼此互換。換言之，除非實施例之適當操作需要一特殊順序之步驟或行動，否則可在不脫離本發明之範疇之情況下修改特殊步驟及/或行動之順序及/或使用。

【符號說明】

100 金鑰儲存器件

101 密碼編譯金鑰/私密根金鑰

102 憑證撤銷列表儲存器

103 計時器

110 金鑰儲存器/記憶體

115 單向傳輸器

116 單向通信鏈接/光纖電纜/連接

117 接收器

118 通信埠

119 處理器

120 中間計算器件/金鑰儲存器件/中間器件

121 密碼編譯引擎

123 螢幕

130 用戶端/用戶端計算器件

152 鍵盤

160 監測服務

400 金鑰儲存器件

413 資料庫

415 雙向收發器

416 雙向連接

417 雙向收發器

420 中間計算器件

435 遠端操作者/遠端通信器件

440 客戶

450 遠端操作者記錄

452 操作者ID

454 操作者公用金鑰

600 新憑證請求

610 憑證簽署請求

620 根私密金鑰識別符

630 操作者ID

640 數位簽名

800 更新CRL請求

810 CRL識別符

820 憑證識別符

830 根私密金鑰識別符

840 操作者ID

850 數位簽名

申請專利範圍

1. 一種裝置，其包括：

一第一非揮發性儲存器，其用於儲存簽署數位憑證之一私密根金鑰；

一輸入器件，其用於自一操作者接收手動輸入；

一通信介面，其由用於自該裝置傳輸資訊之一單向傳輸器組成；及

一處理器，其經組態以：

自該第一非揮發性儲存器擷取該私密根金鑰；

透過該輸入器件接收一新數位憑證之資訊；

根據該接收資訊產生該新數位憑證；

使用該私密根金鑰簽署該新數位憑證；及

使用該傳輸器自該裝置傳輸該新數位憑證。

2. 如請求項1之裝置，其進一步包括：

一計時器，及

一第二非揮發性儲存器，其用於儲存一憑證撤銷列表(CRL)；及

其中該處理器經進一步組態以：

擷取該CRL；

將由該計時器產生之一時戳添加至該經擷取之CRL；

使用該私密根金鑰簽署該經擷取之CRL；及

透過該傳輸器自該裝置傳輸該經簽署之CRL。

3. 如請求項2之裝置，其中該處理器經進一步組態以將一或多個錯誤偵測碼、錯誤校正碼或兩者附加至該經簽署之CRL。

4. 如請求項2之裝置，其中該處理器經進一步組態以將一時戳添加

至該經擷取之CRL，簽署該經擷取之CRL且定期傳輸該經簽署之CRL。

5. 如請求項2之裝置，其中該處理器經進一步組態以定期傳輸該經簽署之CRL。

6. 如請求項1之裝置，其中該處理器經進一步組態以定期傳輸該新數位憑證。

7. 如請求項1之裝置，其中該處理器經進一步組態以根據透過該輸入器件接收之該手動輸入而自複數個私密根金鑰選擇該私密根金鑰。

8. 如請求項1之裝置，其中該處理器經進一步組態以經由該傳輸器將包含關於該裝置之近期行爲之資訊之一訊息傳輸至用於分析及監測該裝置之行爲之一監測服務。

9. 一種系統，其包括：

一第一器件，其包括：

一第一非揮發性儲存器，其用於儲存簽署數位憑證之一私密根金鑰；

一輸入器件，其自一操作者接收手動輸入；

一通信介面，其由用於將資訊自該第一器件傳輸至一第二器件之一單相傳輸器組成；及

一處理器，其經組態以產生待傳輸至該第二器件之新數位憑證；及

該第二器件，其包括：

一接收器，其耦合至該第一器件之該傳輸器；及

一通信埠，其用於建立與一外部網路之一雙向通信通道。

10. 如請求項9之系統，其中，欲產生待傳輸至該第二器件之新數位憑證，該第一器件之該處理器經組態以；

自該第一非揮發性儲存器擷取該私密根金鑰；

透過該輸入器件接收一新數位憑證之資訊；

根據該接收資訊產生該新數位憑證；

簽署該新數位憑證；及

使用該傳輸器將該新數位憑證自該第一器件傳輸至該第二器件。

11. 如請求項9之系統，其中該第一器件進一步包括：

一計時器，及

一第二非揮發性儲存器，其用於儲存一憑證撤銷列表(CRL)；及

其中該處理器經進一步組態以：

擷取該CRL；

將由該計時器產生之一時戳添加至該經擷取之CRL；

使用該私密根金鑰簽署該經擷取之CRL；及

透過該傳輸器自該裝置傳輸該經簽署之CRL。

12. 如請求項11之系統，其中該處理器經進一步組態以將一或多個錯誤偵測碼、錯誤校正碼或兩者附加至該經簽署之CRL。

13. 如請求項12之系統，其中該第二器件經組態以執行附加至該經簽署之CRL之錯誤偵測及校正，且將該經簽署之CRL分佈至用戶端器件。

14. 如請求項11之系統，其中該處理器經進一步組態以將一時戳添加至該經擷取之CRL，簽署該經擷取之CRL且定期傳輸該經簽署之CRL。

15. 如請求項9之系統，其中該處理器經進一步組態以根據透過該輸入器件接收之該手動輸入而自複數個私密根金鑰選擇該私密根金鑰。

16. 如請求項9之系統，其中該處理器經進一步組態以經由該傳輸器及該第二器件將包含關於該第一器件之近期行爲之資訊之一訊息傳輸至用於分析及監測該第一器件之行爲之一監測服務。

17. 一種系統，其包括：

一第一器件，其包括：

一第一非揮發性儲存器，其用於儲存簽署數位憑證之一私密根金鑰；

一輸入器件，其自一操作者接收手動輸入；

一第一收發器，其用於與一第二器件通信；及

一處理器，其經組態以：

接收一新憑證請求；

驗證該新憑證請求係有效的；

自該第一非揮發性儲存器擷取該私密根金鑰；

根據該新憑證請求產生該新數位憑證；

使用該私密根金鑰簽署該新數位憑證；及

使用該傳輸器將該新數位憑證自該第一器件傳輸至該第二器件；及

該第二器件，其包括：

一第二收發器，其耦合至該第一器件之該第一收發器，其中該第一收發器及該第二收發器係藉由一非可路由點對點連接而耦合在一起；及

一通信埠，其用於建立與一外部網路之一雙向通信通道。

18. 如請求項17之系統，其中該第一器件進一步包括：

一計時器，及

一第二非揮發性儲存器，其用於儲存一憑證撤銷列表(CRL)；及

其中該處理器經進一步組態以：

接收一更新CRL請求；

驗證該更新CRL請求係有效的；

擷取該CRL；

將由該計時器產生之一時戳添加至該經擷取之CRL；

使用該私密根金鑰簽署該經擷取之CRL；及

透過該傳輸器自該裝置傳輸該經簽署之CRL。

19. 如請求項17之系統，其中該新憑證請求係由一個以上遠端操作者而簽署，且該處理器經進一步組態以驗證簽署該新憑證請求之各遠端操作者具有一有效的操作者之數位簽名。

20. 如請求項17之系統，其中該更新CRL請求係由一個以上遠端操作者而簽署，且該處理器經進一步組態以驗證簽署該更新CRL請求之各遠端操作者具有一有效的操作者之數位簽名。

21. 如請求項17之系統，其中驗證該新憑證請求係有效的包括驗證簽署該新憑證請求之一遠端操作者具有一有效的操作者之數位簽名。

22. 一種電腦實施方法，其包括：

將用於簽署數位憑證之一私密根金鑰儲存於一第一器件之一第一非揮發性儲存器中；

自一操作者接收關於一新數位憑證之資訊之手動輸入；

自該第一非揮發性儲存器擷取該私密根金鑰；

根據該接收資訊產生該新數位憑證；

使用該私密根金鑰簽署該新數位憑證；及

將該新數位憑證自該第一器件傳輸至藉由一單向連接而連接至該第一器件之一第二器件。

23. 如請求項22之電腦實施方法，其進一步包括：

將一憑證撤銷列表(CRL)儲存於該第一器件處；

擷取該CRL；

將由一計時器產生之一時戳添加至該經擷取之CRL；

使用該私密根金鑰簽署該經擷取之CRL；及

將該經簽署之CRL傳輸至該第二器件。

24. 如請求項23之電腦實施方法，其進一步包括將一或多個錯誤偵測碼、錯誤校正碼或兩者附加至該經簽署之CRL。

25. 如請求項24之電腦實施方法，其進一步包括在該第二器件處執行附加至該經簽署之CRL之錯誤偵測及校正，且將該經簽署之CRL分佈至用戶端器件。

26. 如請求項23之電腦實施方法，其進一步包括將一時戳添加至該經擷取之CRL，簽署該經擷取之CRL且定期傳輸該經簽署之CRL。

27. 如請求項23之電腦實施方法，其中傳輸該經簽署之CRL包括定期傳輸該經簽署之CRL。

28. 如請求項22之電腦實施方法，其中傳輸該新數位憑證包括定期傳輸該新數位憑證。

29. 如請求項22之電腦實施方法，其進一步包括根據透過該輸入器件接收之該手動輸入而自複數個私密根金鑰選擇該私密根金鑰。

30. 如請求項22之電腦實施方法，其進一步包括將包含關於該第一器件之近期行為之資訊之一訊息傳輸至用於分析及監測該裝置之行為之一監測服務。

31. 一種電腦實施方法，其包括：

將用於簽署數位憑證之一私密根金鑰儲存於一第一器件之一第一非揮發性儲存器中；

接收一新憑證請求；

驗證該新憑證請求係有效的；

自該第一非揮發性儲存器擷取該私密根金鑰；

根據該新憑證請求產生該新數位憑證；

使用該私密根金鑰簽署該新數位憑證；及

藉由一非可路由點對點連接而將該新數位憑證自該第一器件傳輸至一第二器件。

32. 如請求項31之電腦實施方法，其進一步包括：

接收一更新CRL請求；

驗證該更新CRL請求係有效的；

擷取該CRL；

將由該計時器產生之一時戳添加至該經擷取之CRL；

使用該私密根金鑰簽署該經擷取之CRL；及

將該經簽署之CRL自該第一器件傳輸至該第二器件。

33. 如請求項31之電腦實施方法，其進一步包括驗證簽署該新憑證請求之各遠端操作者具有一有效的操作者之數位簽名。

34. 如請求項31之電腦實施方法，其進一步包括驗證簽署該更新CRL請求之各遠端操作者具有一有效的操作者之數位簽名。

35. 如請求項31之電腦實施方法，其中驗證該新憑證請求係有效的包括驗證簽署該新憑證請求之一遠端操作者具有一有效的操作者之數位簽名。

圖式

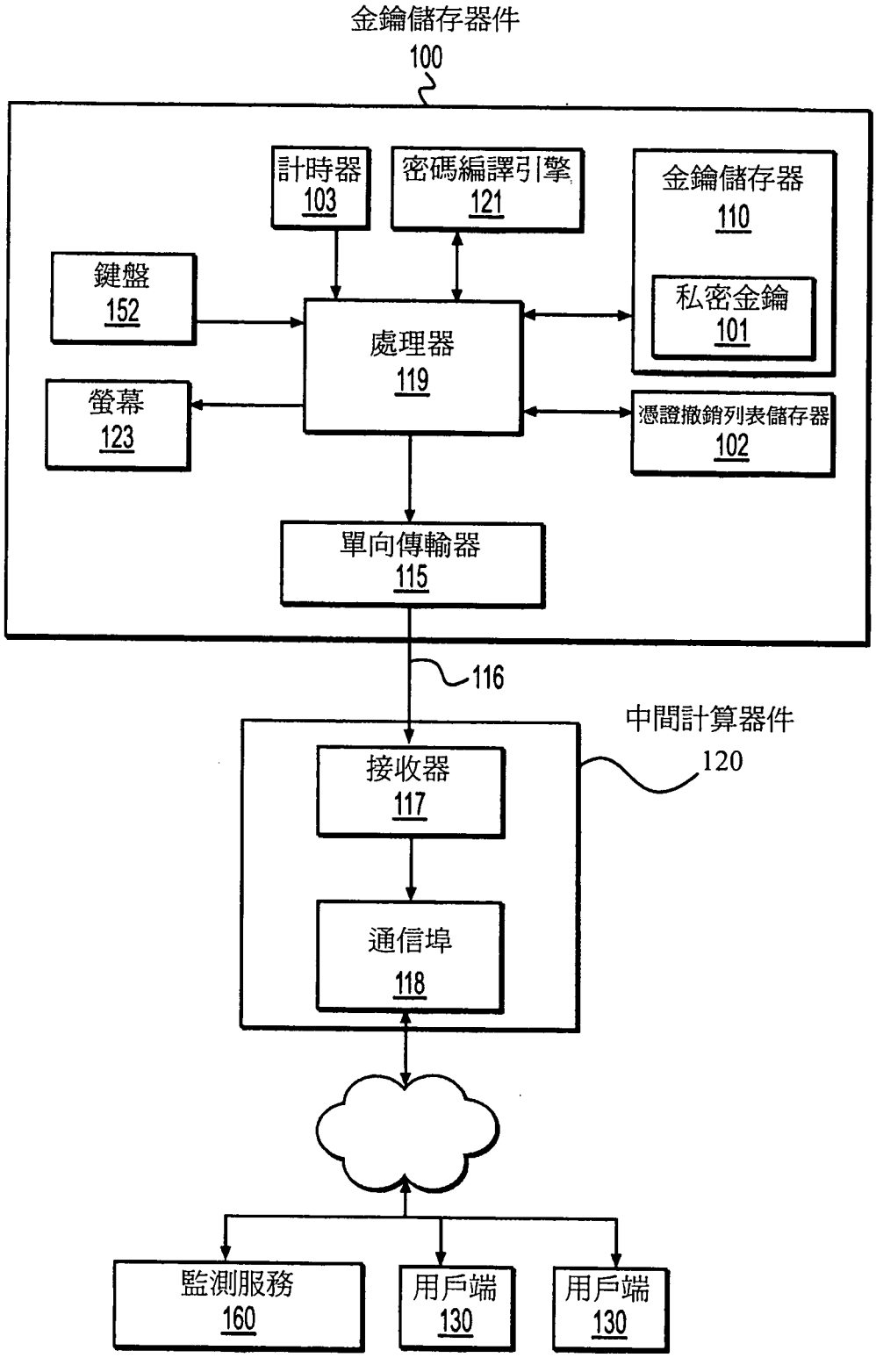
金鑰儲存器件
100
計時器
103
密碼編譯引擎
121
金鑰儲存器
110
鍵盤
152
私密金鑰
101
處理器
119
螢幕
123
憑證撤銷列表儲存器
102
單向傳輸器
115
116
中間計算器件
120
接收器
117
通信埠
118
監測服務
160
用戶端
130
用戶端
130

圖 1

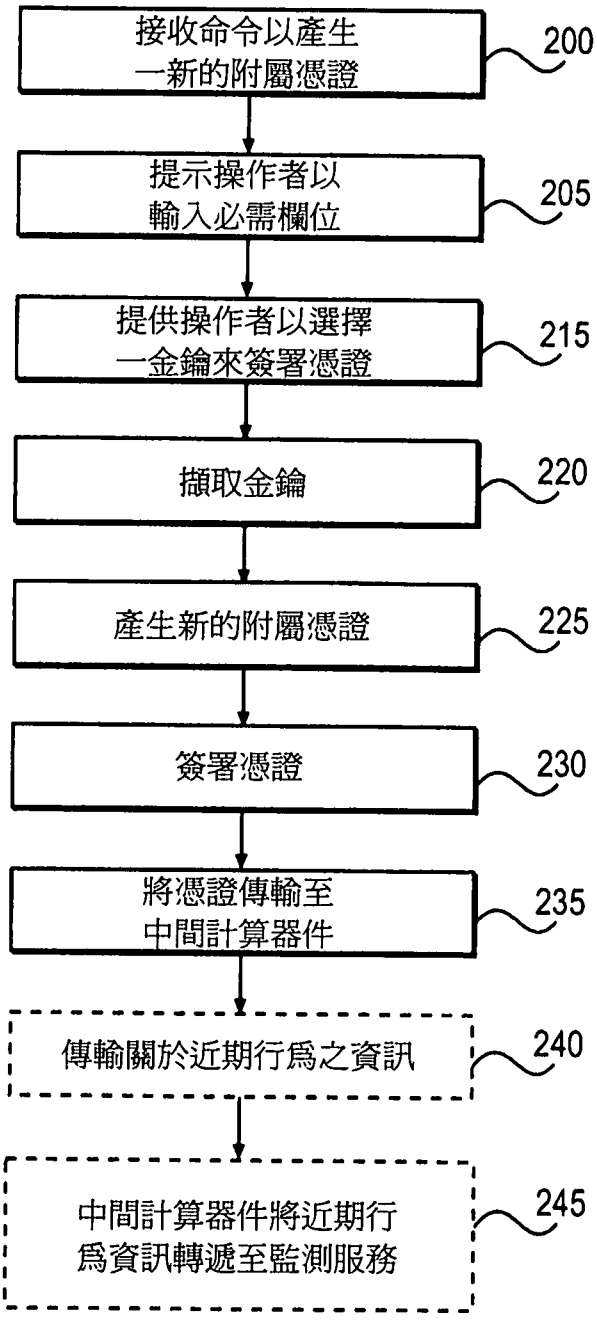
接收命令以產生一新的附屬憑證
200
提示操作者以輸入必需欄位
205
提供操作者以選擇一金鑰來簽署憑證
215
擷取金鑰
220
產生新的附屬憑證
225
簽署憑證
230
將憑證傳輸至中間計算器件
235
傳輸關於近期行爲之資訊
240
中間計算器件將近期行爲資訊轉遞至監測服務
245

圖 2

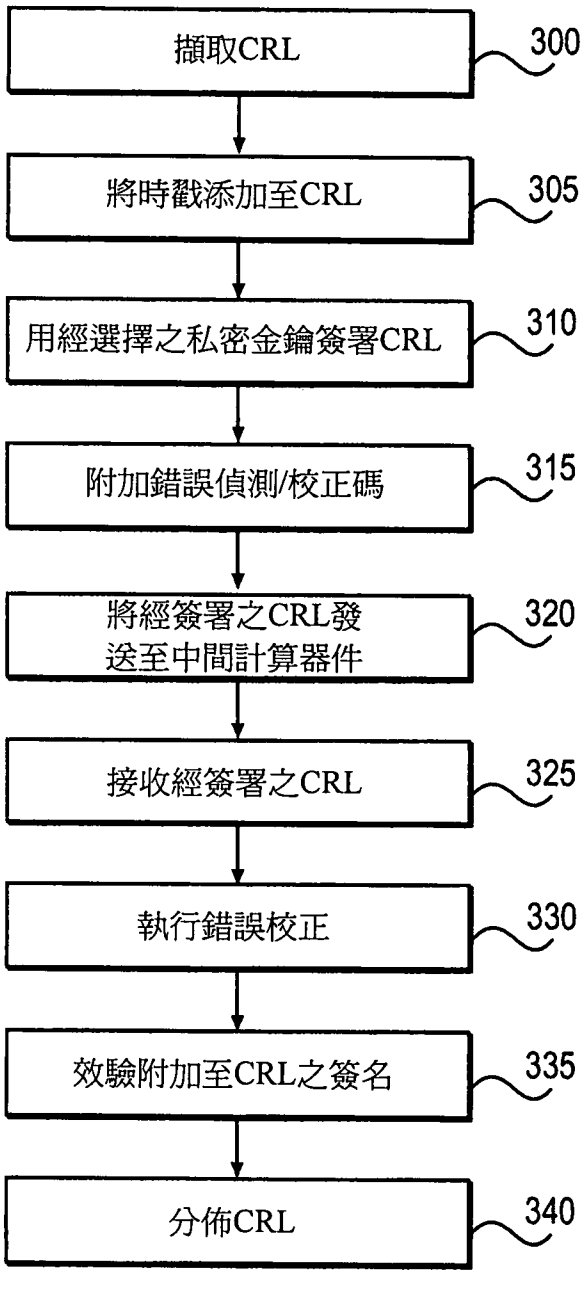
擷取CRL
300
將時戳添加至CRL
305
用經選擇之私密金鑰簽署CRL
310
附加錯誤偵測/校正碼
315
將經簽署之CRL發送至中間計算器件
320
接收經簽署之CRL
325
執行錯誤校正
330
效驗附加至CRL之簽名
335
分佈CRL
340

圖 3

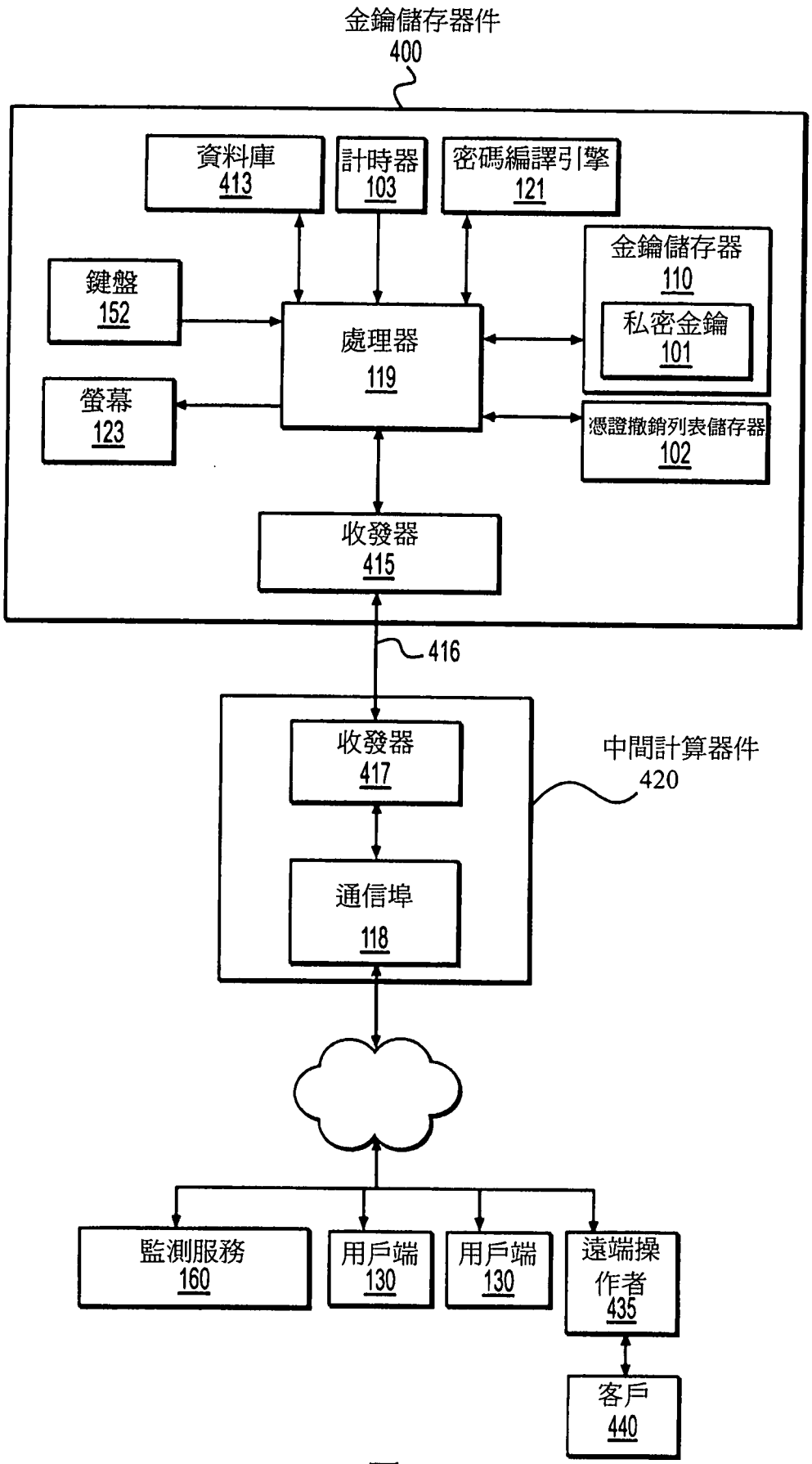
金鑰儲存器件
400
資料庫
413
計時器
103
密碼編譯引擎
121
金鑰儲存器
110
私密金鑰
101
鍵盤
152
處理器
119
螢幕
123
憑證撤銷列表儲存器
102
收發器
415
416
收發器
417
中間計算器件
420
通信埠
118
監測服務
160
用戶端
130
用戶端
130
遠端操作者
435
客戶
440

圖 4A

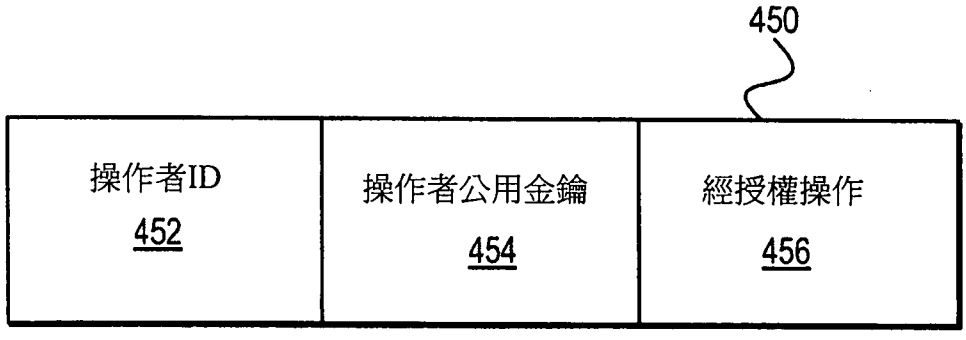

圖 4B

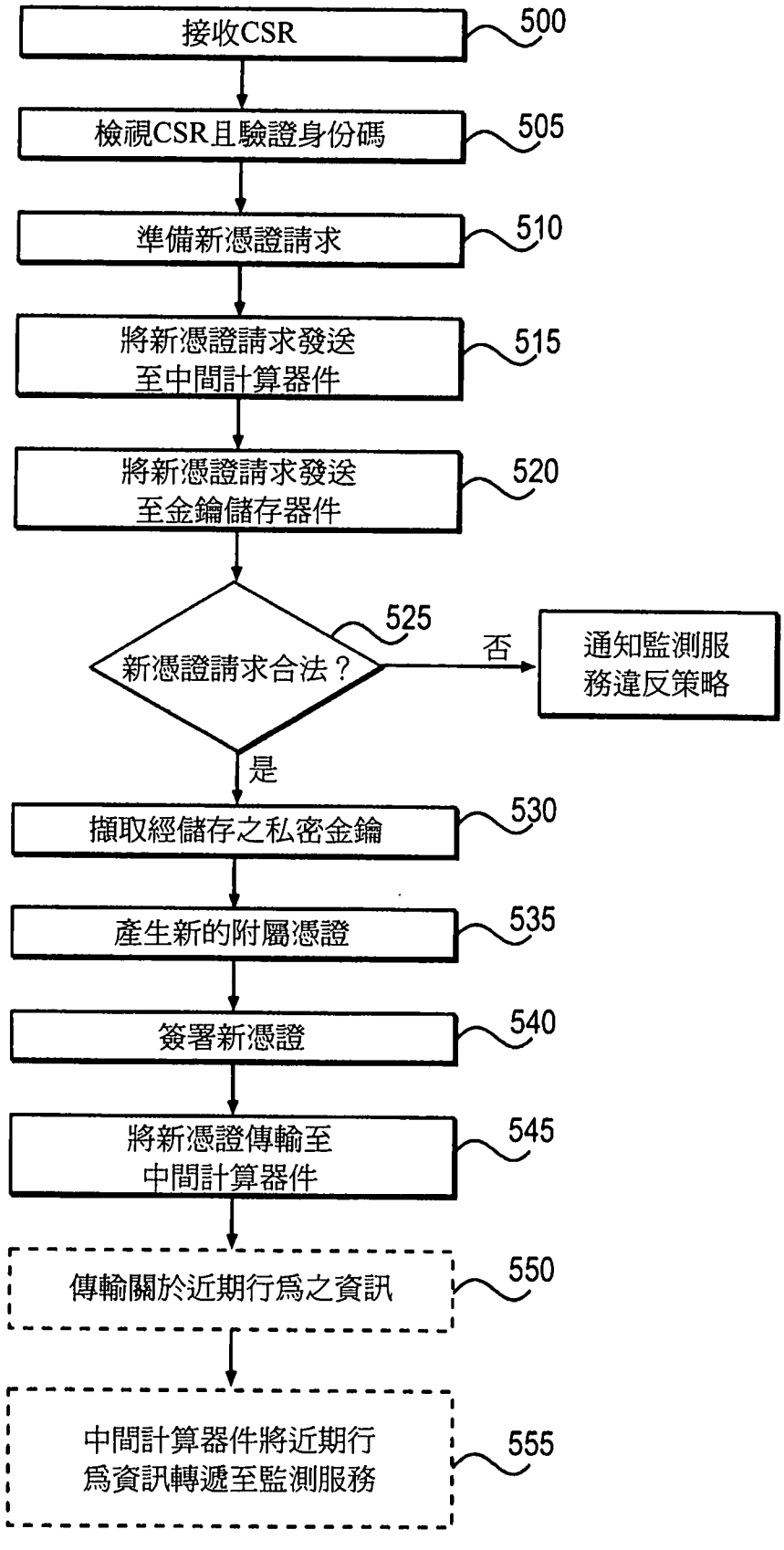
接收CSR
500
檢視CSR且驗證身份碼
505
準備新憑證請求
510
將新憑證請求發送至中間計算器件
515
將新憑證請求發送至金鑰儲存器件
520
新憑證請求合法？
525
否
通知監測服務違反策略
是
擷取經儲存之私密金鑰
530
產生新的附屬憑證
535
簽署新憑證
540
將新憑證傳輸至中間計算器件
545
傳輸關於近期行爲之資訊
550
中間計算器件將近期行爲資訊轉遞至監測服務
555

圖 5

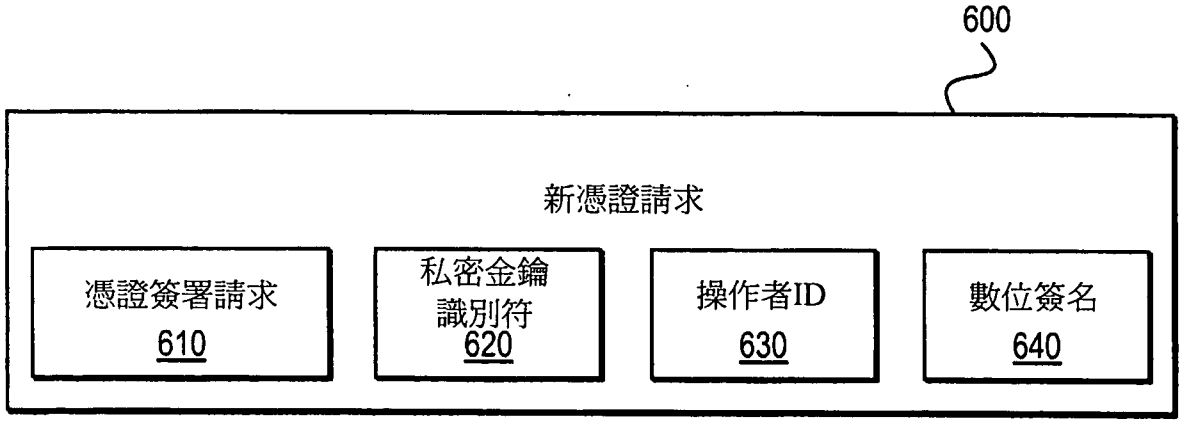

圖 6

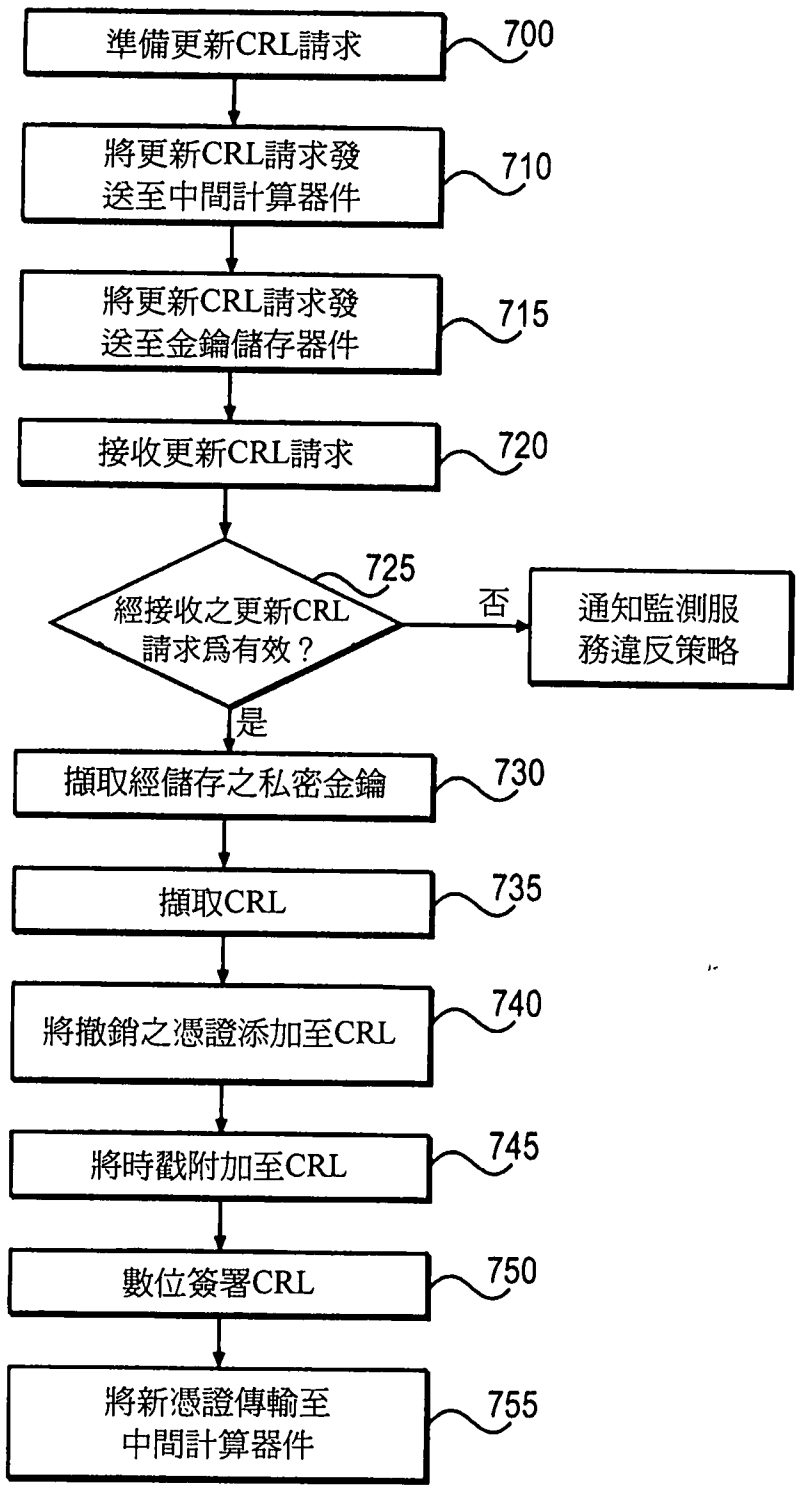
準備更新CRL請求
700
將更新CRL請求發送至中間計算器件
710
將更新CRL請求發送至金鑰儲存器件
715
接收更新CRL請求
720
725
經接收之更新CRL請求爲有效？
否
通知監測服務違反策略
是
擷取經儲存之私密金鑰
730
擷取CRL
735
將撤銷之憑證添加至CRL
740
將時戳附加至CRL
745
數位簽署CRL
750
將新憑證傳輸至中間計算器件
755

圖 7

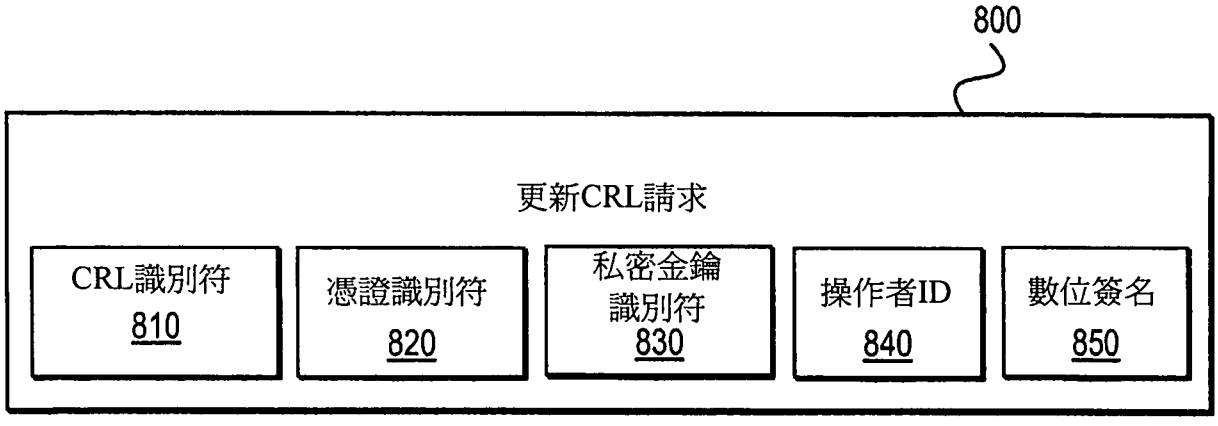
800
更新CRL請求
CRL識別符
810
憑證識別符
820
私密金鑰
識別符
830
操作者ID
840
數位簽名
850

圖 8