



(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 201403376 A

(43)公開日：中華民國 103 (2014) 年 01 月 16 日

(21)申請案號：102122426

(22)申請日：中華民國 102 (2013) 年 06 月 24 日

(51)Int. Cl. : **G06F21/73 (2013.01)**

G06F21/60 (2013.01)

(30)優先權：2012/06/22 美國

61/663,266

2013/06/21 美國

13/923,756

(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)；伊凡奇肯 狄米崔

IVANCHYKHIN, DMYTRO (UA)

(74)代理人：陳長文

申請實體審查：無 申請專利範圍項數：39 項 圖式數：10 共 52 頁

(54)名稱

用於保全來源認證之系統、方法及設備

SYSTEMS, METHODS AND APPARATUSES FOR SECURING ROOT CERTIFICATES

(57)摘要

本文中所闡述之系統、方法及設備提供管理來源認證之一計算環境。根據本發明之一設備可包括儲存複數個來源認證之一非揮發性儲存器及一監督器。該監督器可經組態以接收識別待撤銷之儲存於該非揮發性儲存器中之該複數個來源認證中之一者之一訊息、驗證該訊息係由對應於儲存於該非揮發性儲存器中之兩個來源認證之至少兩個私密金鑰所簽署，及撤銷該訊息中所識別之該來源認證。

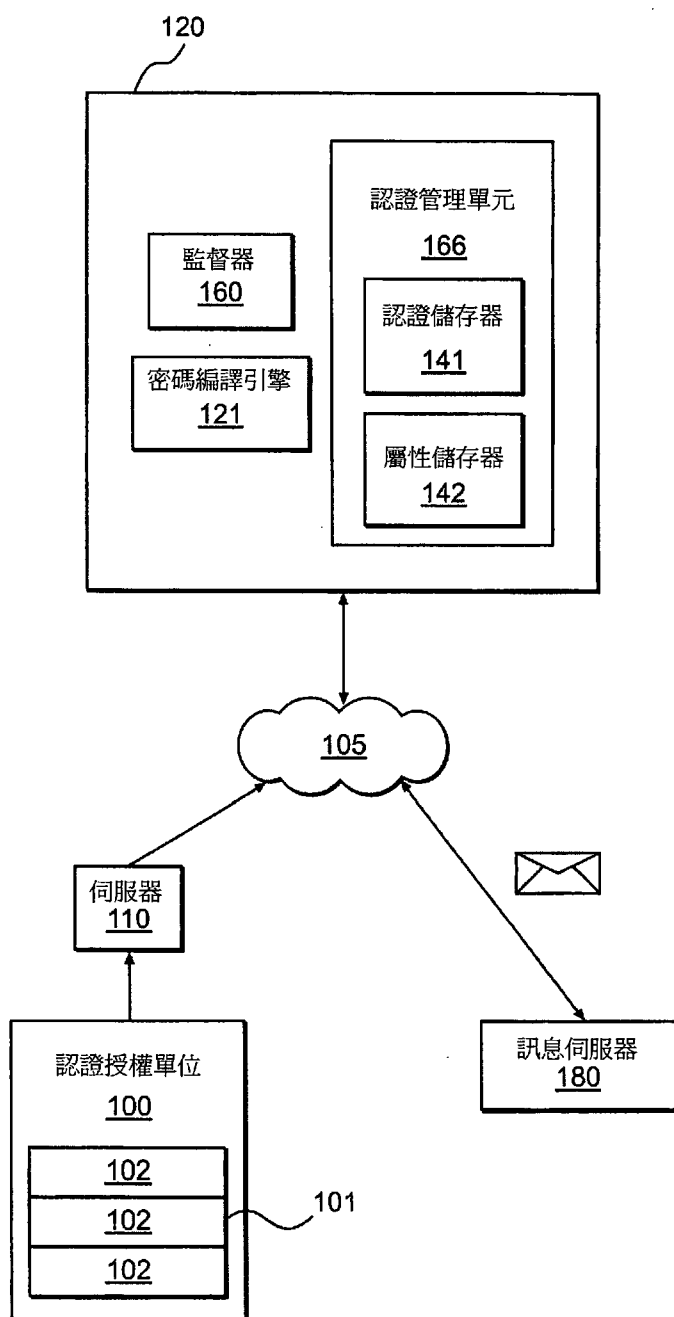


圖 1

100：認證授權單位
(CA)

101：集合

102：來源私密金鑰/
私密來源金鑰

105：通信通道

110：中間伺服器

120：電子裝置/裝置

121：密碼編譯引擎

141：來源認證儲存
器/認證儲存器

142：認證屬性儲存
器/屬性儲存器

160：監督器

166：專用認證管理單
元/認證管理單元

180：遠端電子裝置或
伺服器



(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 201403376 A

(43)公開日：中華民國 103 (2014) 年 01 月 16 日

(21)申請案號：102122426

(22)申請日：中華民國 102 (2013) 年 06 月 24 日

(51)Int. Cl. : **G06F21/73 (2013.01)**

G06F21/60 (2013.01)

(30)優先權：2012/06/22 美國

61/663,266

2013/06/21 美國

13/923,756

(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)；伊凡奇肯 狄米崔

IVANCHYKHIN, DMYTRO (UA)

(74)代理人：陳長文

申請實體審查：無 申請專利範圍項數：39 項 圖式數：10 共 52 頁

(54)名稱

用於保全來源認證之系統、方法及設備

SYSTEMS, METHODS AND APPARATUSES FOR SECURING ROOT CERTIFICATES

(57)摘要

本文中所闡述之系統、方法及設備提供管理來源認證之一計算環境。根據本發明之一設備可包括儲存複數個來源認證之一非揮發性儲存器及一監督器。該監督器可經組態以接收識別待撤銷之儲存於該非揮發性儲存器中之該複數個來源認證之一者之一訊息、驗證該訊息係由對應於儲存於該非揮發性儲存器中之兩個來源認證之至少兩個私密金鑰所簽署，及撤銷該訊息中所識別之該來源認證。

發明摘要

※ 申請案號：102122426

※ 申請日：102.6.24

※IPC 分類：G06F21/73 (2013.01)
G06F21/60 (2013.01)

【發明名稱】

用於保全來源認證之系統、方法及設備

SYSTEMS, METHODS AND APPARATUSES FOR SECURING
ROOT CERTIFICATES

○ 【中文】

本文中所闡述之系統、方法及設備提供管理來源認證之一計算環境。根據本發明之一設備可包括儲存複數個來源認證之一非揮發性儲存器及一監督器。該監督器可經組態以接收識別待撤銷之儲存於該非揮發性儲存器中之該複數個來源認證中之一者之一訊息、驗證該訊息係由對應於儲存於該非揮發性儲存器中之兩個來源認證之至少兩個私密金鑰所簽署，及撤銷該訊息中所識別之該來源認證。

【英文】

○

The systems, methods and apparatuses described herein provide a computing environment that manages root certificates. An apparatus according to the present disclosure may comprise a non-volatile storage storing a plurality of root certificates and a supervisor. The supervisor may be configured to receive a message identifying one of the plurality of root certificates stored in the non-volatile storage to be revoked, verify the message being signed by at least two private keys corresponding to two root certificates stored in the non-volatile storage and revoke the root certificate identified in the message.

【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 認證授權單位(CA)
- 101 集合
- 102 來源私密金鑰/私密來源金鑰
- 105 通信通道
- 110 中間伺服器
- 120 電子裝置/裝置
- 121 密碼編譯引擎
- 141 來源認證儲存器/認證儲存器
- 142 認證屬性儲存器/屬性儲存器
- 160 監督器
- 166 專用認證管理單元/認證管理單元
- 180 遠端電子裝置或伺服器

【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】

用於保全來源認證之系統、方法及設備

SYSTEMS, METHODS AND APPARATUSES FOR SECURING
ROOT CERTIFICATES

相關申請案

本申請案主張2012年6月22日提出申請之美國臨時申請案第61/663,266號及2013年6月21日提出申請之美國非臨時申請案第13/923,756號(此兩者標題為「Systems, Methods and Apparatuses for Securing Root Certificates」)之優先權，兩個申請案之內容以其全文引用之方式併入本文中。

【技術領域】

本文中所闡述之系統、方法及設備係關於資料安全。更特定而言，其係關於安全地替換諸如電腦、膝上型電腦、智慧電話、遊戲控制台、電視機、平板電腦等電子裝置內之來源認證。

【先前技術】

數位認證及公開金鑰基礎建設(PKI)係用於電鑑別個體之眾所周知的機制。在PKI中，每一實體具有一唯一、不對稱金鑰對，包括一公開金鑰及一私密金鑰。一認證授權單位(CA)發佈一數位認證，列舉實體之身份憑證(例如，名稱及組織)及實體之公開金鑰，將實體之身份連結至其公開金鑰。然後，實體可用其私密金鑰加密其所有(或一雜湊)傳出訊息且可連同經加密訊息一起散佈其數位認證。訊息接收者可使用發送者之公開金鑰來解密經加密訊息，從而允許接收者確認：(i)發送者可以使用對應私密金鑰，且因此(ii)發送者係數位認證

中所識別之個體。

然而，亦已知數位認證可係鍛造的。因此，通常，當一CA發佈一新數位認證時，CA將使用其自己的私密金鑰中之一者來以數位方式簽署該認證。然後，CA將公佈其自己的數位認證，識別本身及對應公開金鑰。此將允許一訊息接收者確認發送者之數位認證係由CA發佈的。數位認證已變得較難以鍛造(由於其需要使用CA之私密金鑰)且變得較值得信任。

然而，聲稱的CA不值得信任係可能的。(舉例而言，一惡意使用者可已出於簽署數位認證之目的而創建其自己的「CA」。) 因此，可期望CA之數位認證係由又一CA簽署。此鏈可一直往回持續至體系頂部處之一「來源認證」，該來源認證較佳地已由一眾所周知且受信任的CA發佈。常見的保持來源認證的CA係 VeriSign、Entrust、Comodo及GlobalSign。

在資訊安全領域中，依賴於來源私密金鑰及來源認證之系統係極常見的。歸根結底，鏈之值得信任度取決於此來源認證之值得信任度。與此等系統相關之兩個眾所周知的問題係(1)來源私密金鑰之安全儲存及(2)需要其以進行鑑別之系統內之來源認證群體。

通常，藉由除一數位認證以外之某些機制(諸如，藉由安全實體分配)而使得來源認證值得信任。舉例而言，在製造硬體或安裝軟體時，將某些大部分眾所周知的來源認證嵌入於硬體或軟體中(舉例而言，通常將來源web認證嵌入於網際網路瀏覽器中)。

用於分配來源認證之此方法依賴於系統外部及先前所儲存之來源認證本身之安全性，此方法具有其缺點。特定而言，若此一來源認證(或對應於來源認證之私密金鑰)受危及，則不存在於裝置中更新該來源認證之方式；而是，必須藉由系統外部之某一機制來執行更新。舉例而言，可能需要一系統管理者自一據推測安全源下載一新瀏覽

器。此外，一旦受危及，此來源認證即不可用以驗證含有待使用之一新來源認證之一訊息之完整性及真實性。因此，裝置基本上變為不能夠驗證該裝置自其接收一訊息之任何發送者之身份。取決於上下文，此可使得裝置本身無用。

需要的係用於在一來源認證當前實際上變為受危及之後安全地使得新來源認證可用於電子裝置之系統、方法及裝置。

【圖式簡單說明】

圖1係根據本發明之一例示性系統之一方塊圖。

圖2展示一例示性認證替換訊息及一例示性認證管理單元之內容。

圖3A至圖3C展示可藉以在一電子裝置內替換一作用中認證之例示性程序。

圖4展示可藉以在一電子裝置內替換多個認證之一例示性程序。

圖5展示兩個例示性認證替換訊息及一例示性認證管理單元之內容。

圖6展示可藉以在一電子裝置內替換多個認證之一例示性程序。

圖7展示一例示性自撤銷註釋、一休眠中認證撤銷訊息及一例示性認證管理單元之內容。

圖8展示可藉以在一電子裝置內撤銷一休眠中認證之一例示性程序。

圖9展示一例示性新認證訊息及一例示性認證管理單元之內容。

圖10展示可藉以將一認證添加至一電子裝置之一例示性程序。

【實施方式】

本文中結合以下說明及附圖來闡述根據本發明之系統、裝置及方法之某些說明性態樣。然而，此等態樣僅指示可採用本發明之原理之各種方式中之幾種且本發明意欲包含所有此等態樣及其等效物。當

結合各圖考量時，可自以下詳細說明明瞭本發明之其他優點及新穎特徵。

在以下詳細說明中，陳述眾多特定細節以提供對本發明之一透徹理解。在其他例項中，為不會不必要地模糊本發明，未詳細展示眾所周知之結構、介面及程序。然而，熟習此項技術者將明瞭，本文中所揭示之彼等特定細節未必用於實踐本發明且不表示對本發明之範疇之一限制，除非如申請專利範圍中所陳述。意欲本說明書之任何部分皆不被視為實行對本發明之完全範疇之任何部分之一否定。儘管闡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完全範疇。

本文中所揭示之發明提供用於安全地替換諸如電腦、膝上型電腦、智慧電話、遊戲控制台、電視機、平板電腦等電子裝置內之來源認證之系統、方法及設備。圖1展示根據本發明之一例示性電子裝置120。

如圖1中所展示，電子裝置120可經由耦合至裝置120之一通信通道105而與一或多個遠端電子裝置或伺服器180通信。舉例而言，一智慧電話可係能夠經由網際網路郵件伺服器傳輸及接收電子郵件。此通信通道可係用於(例如，使用一USB連接或一快閃驅動器)傳送資料(在線(例如，網際網路)或離線)之任何適合機構。

亦如圖1中所展示，電子裝置120可經由通信通道105連接至一或多個認證授權單位(CA) 100。如下文將更詳細地闡述，CA 100可經組態以經由通信通道105將關於其來源認證之資訊傳輸至電子裝置120。應理解，可在CA 100與一電子裝置120之間存在一或多個中間伺服器110。

為實施本文中所闡述之功能性，電子裝置120可執行需要在執行某些活動時(藉由使用一所儲存來源認證)鑑別一數位認證之某些應用

或功能。在前述實例中，智慧電話可鑑別且視需要解密包含一數位認證、經由通信通道105接收之任何電子郵件。應理解，電子郵件僅係對來源認證之一個例示性使用；存在對來源認證之諸多其他使用，此兩者係關於直接服務於一使用者之需要之活動(諸如鑑別電子郵件或網頁)以及服務於電子裝置120內部之目的之活動(諸如，舉例而言安全時間保持)。

如圖1中所展示，電子裝置120可含有一或多個專用認證管理單元166。認證管理單元166可包括來源認證儲存器141及相關聯之認證屬性儲存器142。(下文更詳細地論述此等認證屬性。) 在某些實施例中，認證儲存器141可實施為唯讀、非揮發性記憶體，而屬性儲存器142可實施為讀取/寫入、非揮發性記憶體。在其中電子裝置120經組態以與多個CA通信之實施例中，可較佳地組態認證管理單元166以使得保存且單獨管理CA 100中之每一者之來源認證。

根據本發明之一電子裝置120可進一步包括一監督器160。該監督器可用以執行電子裝置120之某些操作規則以便給終端使用者提供某些安全保障。其可經組態以(1)識別預儲存於認證管理單元166內之來源認證中之哪一來源認證係當前在使用的；(2)使用當前操作來源認證來證實(例如)如可附加至一所接收訊息之一或多個數位認證；且(3)更新一或多個來源認證屬性。本文中更詳細地闡述此等功能中之每一者。在某些實施例中，如下文更詳細地闡述，認證儲存器141可實施為一讀取-寫入、非揮發性記憶體，且監督器160可另外經組態以更新一或多個來源認證。

監督器160可實施於電子裝置120內之硬體及/或軟體中，只要在任何何實施方案中藉由選定實施方案維持監督器160之完整性即可。舉例而言，可出於此目的而使用防竄改及/或竄改偵測技術。此外，若電子裝置120實施用以載入並執行第三方程式碼之選項，則應採取

措施以確保任何此第三方程式碼不能夠影響或接聽監督器160之狀態。

(另一選擇係，或除防竄改以外)，監督器160及/或電子裝置120亦可併入有一或多個竄改偵測技術。舉例而言，已知用於保護密碼編譯處理器之數個防竄改方法且在此項技術中已闡述該等方法。在此等實施例中之某些實施例中，若電子裝置120偵測到晶片之完整性已受危及及/或若其偵測到裝置之外殼之穿透，則電子裝置120可經組態以執行一或多個可能回應。此等回應可自抹除敏感資料至實體破壞電子裝置120之全部或部分而變化。

在某些實施例中，電子裝置120可進一步包括可尤其在支援數位認證驗證中由監督器160使用之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。密碼編譯引擎121可自監督器160接收資料以用於加密或解密，且可將所得加密文字(或純文字，視情況)往回提供至監督器160。舉例而言，此密碼編譯能力可用於數位簽章之驗證中。在其他實施例中，監督器160可經組態以執行密碼編譯引擎121之某些或全部功能性，且可不需要一單獨密碼編譯引擎121。

如圖1中所展示，電子裝置120可經由通信鏈路105連接至一或多個CA 100。根據本發明，每一認證授權單位100可具有至少兩個來源私密金鑰102之一集合101。對於每一來源私密金鑰102，CA可具有一對應來源數位認證(含有適當對應公開金鑰)。

每一來源私密金鑰亦可具有命名為(舉例而言)「作用中」、「休眠中」或「經撤銷」之一相關聯之狀態屬性。在此一實施例中，具有一「作用中」狀態之一來源私密金鑰102可由CA 100用來簽署資料，諸如數位認證。具有「休眠中」狀態之來源私密金鑰102可被認為當前不可用於供CA 100使用，但有資格供將來使用。休眠中金鑰可由CA

100安全地儲存以防止其丟失或洩露給未經授權之第三方。另外，出於安全原因，一旦一來源私密金鑰102已經選擇為作用中，即可較佳地確保其不可能被錯誤識別為休眠中。最終，具有一「經撤銷」狀態之來源私密金鑰102可完全不可用於供CA 100使用。舉例而言，經撤銷狀態可用以識別已受危及之任何金鑰。

在根據本發明之一項實施例，每一CA 100可具有至少五(5)個來源私密金鑰102之一集合101。應理解，雖然具有較少來源私密金鑰102在本發明之範疇內，但其可減少系統對某些種類之攻擊之抵抗力。

當製造一電子裝置120時，可針對每一CA 100將至少兩個來源數位認證(對應於來源私密金鑰102之集合101之全部或一子集)儲存於認證儲存器141內。另外，可將與每一來源認證相關聯之一或多個屬性儲存於屬性儲存器142內。舉例而言，對應於當前由CA 100使用之來源私密金鑰102之來源認證可指定為作用中，且所有其他來源認證可識別為休眠中。在製造之後，電子裝置120之監督器160可經組態以僅使用作用中認證來進行傳入訊息簽章驗證。

應理解，一旦已將來源認證儲存於認證儲存器141中(例如，在裝置120製造期間)，此等認證即可能在裝置之壽命(可係數年)期間保持於認證儲存器141中。舉例而言，諸多電子裝置120 (諸如電視機或電腦)僅每幾年替換一次，且某些電子裝置可使用達十年或甚至更長。在此漫長時間段期間，一電子裝置120之一惡意使用可能夠存取儲存於裝置120內之來源認證公開金鑰中之一或多者，且試圖使用該來源認證來得到對應私密金鑰，此可導致對整個系統之完全危及。因此，在某些實施例中可較佳地針對整個認證系統選擇加密方法以使得：在一對應時間段期間，統計上將不可能使一惡意使用者(舉例而言，使用一暴力攻擊)找到對應於儲存於裝置中之任何來源認證之公開金鑰之私密

金鑰。舉例而言，當前相信，瑞未斯特-希米爾-愛得曼(Rivest-Shamir-Adleman) (RSA)加密方法之一特定金鑰長度(舉例而言，2048位元或更大)可滿足此性質。

儘管存在加密方法及金鑰長度，但時常一CA 100可判定可需要使一私密金鑰無效。舉例而言，可在金鑰已受危及之情況下或由於一金鑰到期原則而發生此情況。在此等情形中，CA 100可需要用另一現有私密來源金鑰替換一私密來源金鑰或撤銷一私密金鑰。在其中CA 100已替換或撤銷一私密金鑰之情形中，可進一步期望將一或多個新私密金鑰添加至系統。以下說明中提供用於每一此操作之系統、方法及設備。

圖2至圖6圖解說明可藉以由另一私密來源金鑰及其對應來源公開金鑰及/或認證替換一私密來源金鑰及對應來源公開金鑰及/或來源認證之例示性程序及對應資料結構。

在一第一實施例中，CA 100可撤銷一當前作用中私密金鑰且可用(在其金鑰集合101內之)一休眠中私密金鑰替換該當前作用中私密金鑰，該休眠中私密金鑰可變為新作用中金鑰。此新作用中私密金鑰可用以簽署數位認證且執行其他基於來源金鑰之活動，且對應來源認證可用以驗證此等數位簽章。在此一情形中，CA 100可將一認證替換訊息發送至一或多個電子裝置120，該認證替換訊息可含有關於待替換之來源認證之資訊且可進一步含有關於待啟動之一替換來源認證之資訊。

圖2展示一例示性認證替換訊息200及一例示性認證管理單元166之內容。圖3A至圖3C展示可在由一CA 100替換對應私密來源金鑰101後藉以在一電子裝置120中替換一當前作用中認證之例示性程序。出於闡釋之目的，關於圖3A至圖3C所闡述之程序將參考圖2上所展示之認證替換訊息200及認證管理單元166之值。然而，應理解，此等值僅

係例示性的且所闡述之方法意欲對任何適當值起作用。

圖2展示具有儲存於認證儲存器141內之三個來源認證之一認證管理單元166：來源認證A、B及C。屬性儲存器142具有列舉為作用中之來源認證A之狀態以及列舉為休眠中之來源認證B及C之狀態。

在步驟310 (圖3A)處，監督器160可自CA 100或經由一或多個中間伺服器(例如，伺服器110)接收一訊息200 (圖2)，且可基於訊息類型201而判定該訊息係一認證替換訊息200且因此應被處置。此訊息類型201可係適於指示此係一替換訊息200之任何資料。舉例而言，如圖2上所展示，訊息類型201可係串「認證替換」。在其他實施例中，訊息類型201可係將訊息200唯一地識別為一替換訊息之一整數。

如圖2上所展示，除其訊息類型201欄位以外，替換訊息200亦可進一步包括闡述待撤銷之認證及替換認證之資訊。經撤銷認證識別符210可用以識別認證儲存器141中之已由CA 100使其對應來源私密金鑰無效之來源認證。在圖2上所展示之實例中，經撤銷認證識別符210將來源認證A識別為待撤銷之來源認證。替換認證識別符215可用以識別認證儲存器141中之已由CA 100啟動其對應來源金鑰之來源認證。在圖2上，替換認證識別符215將來源認證B識別為應啟動之來源認證。

可使用下文將更詳細地闡述其中之每一者之步驟320至340 (圖3A)來驗證替換訊息200之真實性。舉例而言，在某些實施例中，在將替換訊息200發送至電子裝置120之前，CA 100可使用兩個或兩個以上(「N」個)不同私密「簽署」金鑰(其係私密來源金鑰102之集合101之一子集)以數位方式簽署替換訊息200。如下文將更詳細地論述，此數位簽章使用可防止當前作用中來源認證之未經授權無效及/或替換。取決於實施例，簽署金鑰之實際數目N可變化(例如，一項實施例可具有由五個金鑰簽署之訊息200，而在另一實施例中可僅由兩個金鑰簽

署訊息200)，但在任何給定實施例內，此數目N應保持恆定(且可不超過來源私密金鑰102之集合101之總體大小)。

舉例而言，在一項例示性實施例中，每一裝置120可能能夠儲存最多五個金鑰，但N可僅係2。在另一例示性實施例中，每一裝置120可能能夠儲存七個金鑰，且N可僅係2。在又一例示性實施例中，每一裝置120可能能夠儲存七個金鑰，且N可係等於3。

在某些實施例中，N個簽署金鑰僅選自休眠中之來源私密金鑰102之集合101內之金鑰子集；換言之，無效之(作用中)私密金鑰可不用以簽署替換訊息200。在其他實施例中，此等N個簽署金鑰中之一者可係正無效之(作用中)來源私密金鑰102。

另外，可需要N個簽署金鑰包含替換來源私密金鑰；換言之，可需要N簽署金鑰包含對應於應由電子裝置120之監督器160使用作為新作用中認證之(已經儲存於認證儲存器141內之)數位認證之私密金鑰。(應理解，在其中N個簽署金鑰包含正撤銷之私密金鑰之實施例中，替換來源私密金鑰不應係正撤銷之私密金鑰，以使得新的作用中認證不同於舊的經撤銷認證。)

在圖2上所展示之例示性實施例中，替換訊息200 (亦即，經撤銷認證識別符210及替換認證識別符215)之主體可由兩個簽署金鑰簽署，以使得替換訊息200包含兩個數位簽章，「簽章1」230及「簽章2」231。如圖2上所展示，簽章1 230係使用與認證B相關聯之來源私密金鑰而創建且簽章2 231係使用於認證C相關聯之來源私密金鑰而創建。在某些實施例中，可期望使一個簽章涵蓋另一簽章，例如，簽章2 231可涵蓋經撤銷認證識別符210、替換認證識別符215及簽章1 230中之全部作為經簽署欄位；在其他實施例中，簽章1 230及簽章2 231可係獨立的。然而，應認識到，替換訊息200之額外分量亦可視情況類似地簽署。

在某些實施例中，替換訊息200可進一步包括識別可用以證實N個簽章之認證之一或多個欄位。舉例而言，替換訊息200可包含識別與來源私密金鑰之集合101相關聯且先前儲存於認證儲存器141中之認證之一子集之欄位。此等認證識別符用以給監督器160提供其應出於證實N個簽章之目的而嘗試哪些認證之某一意見，如下文進一步詳細地闡述。如圖2上所展示，舉例而言，認證識別符欄位220及221將認證B及C分別識別為應出於驗證簽章1 230及簽章2 231之目的而嘗試之認證。此可改良系統之效率，此乃因除監督器160嘗試使用認證儲存器141中之每一認證來證實每一簽章(例如，簽章1 230)以外，僅需要使用替換訊息200中(使用認證識別符，例如，220)所識別之特定認證。

在步驟320 (圖3A)處，監督器160可驗證所接收替換訊息200具有所有N個簽章。舉例而言，如圖2上所展示，按照預期，替換訊息具有兩個簽章。

在步驟323 (圖3A)處，監督器160可驗證可使用先前(例如，在製造時)儲存於認證儲存器141內之對應數位認證來驗證彼等N個簽章。舉例而言，如圖2上所展示，可使用所儲存之來源認證B及C來驗證兩個簽章230、231。因此，應理解，由於使用來自來源私密金鑰102之集合101之N個私密金鑰來簽署每一替換訊息200以使儲存於電子裝置120內之任何來源認證無效，因此一攻擊者必須具有至少N個私密金鑰。在其中替換訊息200包含認證識別符欄位(例如，如圖2上所展示之220及221)之實施例中，監督器160可使用彼等識別符來減少嘗試證實兩個簽章230、231之認證之數目。

在步驟326 (圖3A)處，監督器160可驗證位於認證儲存器141中之對應數位認證在對應屬性儲存器142內未標記為經撤銷。在前述實例中，如圖2上所展示，來源認證B或C中任一者在屬性儲存器141內皆

未標記為經撤銷。

在某些實施例中，可較佳地進一步確保可僅由特定而言識別為休眠中之(位於儲存器141內之)數位認證來驗證N個簽章230、231。在前述實例中，兩個來源認證B及C在屬性儲存器141內展示為休眠中。

在步驟330 (圖3A)處，監督器160可確認替換認證識別符215參考已儲存於認證儲存器141內之一認證，且在步驟335處可進一步驗證(如儲存於屬性儲存器142內之)任何此認證之狀態屬性係休眠中的。在圖2上所展示之實例中，替換認證識別符215參考來源認證B，來源認證B展示為存在於認證儲存器141中且其展示為在屬性儲存器142內具有一休眠中狀態。

在步驟340 (圖3A)處，監督器160可驗證由替換認證識別符215所識別之替換認證(亦即，新的作用中來源認證)對應於訊息200之N個簽章中之一者(例如，圖2上之230或231)。在圖2上所展示之實例中，由替換認證識別符215所識別之替換認證係來源認證B。其對應於簽章1，圖2上展示為230。

若在步驟320至340中之任一者處執行之驗證中之一者失敗，則監督器160可不執行任何額外替換操作而是在某些實施例中可在步驟350處試圖(直接地或經由一或多個額外伺服器間接地)將一原則違規通知CA 100。此一通知可包含(舉例而言)由電子裝置120接收之替換訊息200及任何其他適當資訊，諸如方法失敗之特定原因。否則，若在步驟320至340處執行之所有驗證皆成功通過，則監督器160可繼續進行至處理認證替換。

圖3B及圖3C展示用於使與經撤銷來源私密金鑰相關聯之認證無效且用新的作用中認證替換該認證之不同方法。在關於圖3B所展示之實施例中，在步驟360處，監督器160可判定應撤銷當前作用中認證。舉例而言，此可藉由比較經撤銷認證識別符210與當前作用中認

證之認證識別符來判定。舉例而言，在圖2上，經撤銷認證識別符210將來源認證A列舉為待撤銷之認證。屬性儲存器142將來源認證A之狀態展示為作用中。

若兩個識別符匹配，則方法可繼續進行至步驟365 (圖3B)且監督器160可將當前認證之狀態更新為經撤銷(例如，在屬性儲存器142內)。因此，在圖2上所展示之實例中，來源認證A之狀態應在屬性儲存器142內更新為經撤銷。若兩個識別符不匹配(亦即，正由CA 100撤銷之認證與電子裝置120內之作用中認證不相同)，則在步驟367處監督器160可將當前作用中認證之狀態更新為休眠中。

在步驟370 (圖3B)處，監督器160可將由替換認證識別符215參考之認證之狀態更新為作用中(例如，在屬性儲存器142內)，且在步驟375處，監督器160可開始使用新的作用中來源認證來進行任何認證驗證。在圖2上所展示之實例中，由替換認證識別符215識別來源認證B；因此，其在屬性儲存器142內之狀態應更新為作用中。

在另一實施例中，可使與經撤銷來源私密金鑰相關聯之認證無效且將其替換，如圖3C上所展示。關於圖3C所闡述之步驟中之諸多步驟類似於關於圖3B所闡述之步驟。

在圖3C中所闡述之方法中，在圖3A之步驟340之後，在步驟380處，監督器160可判定是否應撤銷當前作用中認證。舉例而言，此可藉由比較經撤銷認證識別符210與當前作用中認證之認證識別符來判定。舉例而言，在圖2上，經撤銷認證識別符210將來源認證A列舉為待撤銷之認證。屬性儲存器142將來源認證A之狀態展示為作用中。

若兩個識別符匹配，則方法可繼續進行至步驟382且監督器160可將當前認證之狀態更新為經撤銷(例如，在屬性儲存器142內)。因此，在圖2上所展示之實例中，來源認證A之狀態應在屬性儲存器142內更新為經撤銷。

在步驟384 (圖3C)處，監督器160可將由替換認證識別符215參考之認證之狀態更新為作用中(例如，在屬性儲存器142內)，且在步驟386處，監督器160可開始針對任何認證驗證使用新的作用中來源認證。在圖2上所展示之實例中，由替換認證識別符215識別來源認證B；因此，其在屬性儲存器142內之狀態應更新為作用中。

然而，若在步驟380處，經撤銷認證識別符210與當前作用中認證之認證識別符不匹配(亦即，正由CA 100撤銷之認證與電子裝置120內之作用中認證不相同)，則監督器160可不執行任何替換操作，而是在某些實施例中可在步驟390處試圖(直接地或經由一或多個額外伺服器間接地)將替換訊息200與電子裝置120內之目前認證狀態不一致通知CA 100。此通知可包含目前替換訊息200以及緊鄰先前替換訊息200，最後一作用中認證曾基於緊鄰先前替換訊息200而接收其狀態(在可存在此一緊鄰先前替換訊息之條件下)。

關於圖3A至圖3C所闡述之例示性方法展示可如何根據本發明替換一單個私密來源金鑰102。因此，若僅一個私密來源金鑰102已受危及(假定CA 100具體知曉哪一私密來源金鑰102已受危及)，則CA 100可執行關於圖3A至圖3C所闡述之替換程序。然而，如下文將闡述，此方法可經修改以替換多個來源認證。

圖4展示針對兩個來源認證之一例示性私密來源金鑰替換程序，其中待替換之金鑰中之一者係作用中認證。然而，應理解，可針對任何數目個認證使用本文中所闡述之方法。如關於圖3A至圖3C所闡述之方法中，關於圖4所闡述之方法假定CA 100具體知曉哪兩個私密來源金鑰必須替換。圖5 (類似於圖2)展示一例示性認證管理單元166之內容及兩個認證替換訊息之值。出於闡釋之目的，關於圖4所闡述之程序將參考圖5上所展示之認證替換訊息及認證管理單元166之值。然而，應理解，此等值僅係例示性的且所闡述之方法意欲對任何適當值

起作用。

如圖5上所展示，一例示性認證管理單元166具有儲存於認證儲存器141內之五個來源認證：來源認證A、B、C、D及E。屬性儲存器142具有列舉為作用中之來源認證A之狀態以及列舉為休眠中之來源認證B、C、D及E之狀態。CA 100知曉對應於來源認證A及B之來源私密金鑰為受危及。

在步驟405處，CA 100可創建使目前作用中認證(亦即，對應於待替換之兩個私密來源金鑰中之一者之認證)無效且用對應於第二受危及來源金鑰之認證替換該目前作用中認證之一第一替換訊息500。此第一替換訊息500可由第二受危及金鑰及一第三未受危及金鑰簽署。因此，在圖5上所展示之實例中，來源認證A係認證管理單元166內之目前作用中認證且應由來源認證B替換。第一替換訊息500已由對應於認證B (受危及)及認證C (未受危及)之來源私密金鑰簽署。

在步驟410處，CA 100可創建使目前作用中認證(如下文所闡述，其將係第一替換訊息500中所識別之替換認證)無效且用對應於一未受危及金鑰之一認證替換該目前作用中認證之一第二替換訊息510。此第二替換訊息510可由兩個未受危及金鑰簽署。因此，在圖5上所展示之實例中，來源認證B被認為係目前作用中認證且應由來源認證C替換。第二替換訊息510已由對應於認證C及D (兩者皆未受危及)之私密來源金鑰簽署。

注意，在其中可使用當前作用中私密金鑰創建一替換訊息之簽章中之一者之實施例中，則可使用受危及金鑰中之兩者來替換第一認證且可使用受危及金鑰中之一者及一第二未受危及金鑰來替換第二認證。

如圖5上所展示，每一替換訊息500、510可擁有與關於圖2所闡述之替換訊息200相同之欄位中之某些欄位，外加三個額外欄位：一

需要先前訊息之旗標540、560、一需要下一訊息之旗標541、561及下一訊息之一雜湊551、571。此等欄位可用以執行用以在一單個程序中替換數個認證之替換訊息之完整性。

在一項例示性實施例中，第一替換訊息500可設定需要下一訊息之旗標541以需要一第二後續訊息，*例如*，第二替換訊息510。(應理解，此旗標541之值可係適合之任何值，包含布林(boolean)值，諸如「是」/「否」、1/0等)。因此，第一替換訊息500亦可在欄位551中包含第二替換訊息510之一雜湊。此雜湊可係整個第二替換訊息510之一雜湊(具有或不具有其簽章)。當此係鏈中之第一替換訊息時，需要先前訊息之旗標540可經設定以指示不需要先前訊息。

類似地，第二替換訊息510可經創建以使得需要先前訊息之旗標560經設定以需要一先前訊息，*例如*，第一替換訊息500。需要下一訊息之旗標561可經設定以指示不需要後續訊息，且欄位571之對應值可設定至任何值。

應理解，在此一例示性實施例中，可必需以一特定次序計算任何必要雜湊及簽章。舉例而言，可必需首先針對訊息鏈中之最後一訊息、然後針對訊息鏈中之倒數第二訊息等等計算之雜湊及簽章。

應進一步理解，以上關於圖5所展示之說明僅係例示性的，且舉例而言，可藉由使用先前訊息之一雜湊替代下一訊息之一雜湊來達成相同效應。在此等實施例中，可較佳地計算雜湊及簽章，以訊息序列中之第一訊息開始且以最後一訊息結束。

在步驟415 (圖4)處，CA 100可將第一替換訊息500發送至電子裝置120，且在步驟420處，CA 100可將第二替換訊息510發送至電子裝置120。基於每一訊息500、510之訊息類型，監督器160將能夠判定存在認證替換訊息且因此繼續進行。

在步驟425處，監督器160可判定已滿足由兩個替換訊息(*例如*，

540、541、560及561)中之每一者中之旗標設定之條件。舉例而言，談及第一替換訊息500具有經設定以需要一後續訊息之需要下一訊息之旗標541，監督器160可確認(i)其確實接收一第二替換訊息510且(ii)第二替換訊息510之雜湊具有與在第一替換訊息500之資料欄位551中接收之值相同之值。

類似地，談及第二替換訊息510具有經設定一需要一先前訊息之需要先前訊息之旗標540，監督器160可確認其接收一第一替換訊息500。

若在步驟425處已滿足由旗標設定之所有條件，則在步驟430處監督器160可處理第一替換訊息500 (例如，如上文關於圖3A至圖3C所闡述)，且在步驟435處監督器160可處理第二替換訊息510。在圖5上所展示之實例中，在完成步驟435後，旋即替換認證A及B兩者，且認證C係目前作用中認證。

在使用此結構之實施例中，訊息序列有效地形成一「訊息鏈」(不與一傳統「認證鏈」混淆)。在某些實施例中，可能期望不可部分完成地處理此等訊息，其中將訊息連結在一起以確保其不可單獨處理。而是，可將任何一整個訊息鏈一起處理，或若出於某一原因，該鏈中之一個訊息係無效的，則不處理該等訊息中之任一者。在此意義上，每一訊息鏈可被認為係不可部分完成的或不可分割的來處理，且電子裝置120不可處於一中間狀態。(i)應改變來源公開金鑰之狀態以便使該鏈中之所有訊息生效，或(ii)來源公開金鑰之狀態應根本不改變。

在其他實施例中，可能期望使用一第二類型之不可部分完成訊息處理，使得若訊息鏈中之訊息中之一者係無效的(亦即，未滿足上文所闡述之有效性條件)，則跳過訊息鏈中之無效訊息。有效之彼等訊息係用以形成一第二(暫時)訊息鏈，該第二(暫時)訊息鏈包括原始

鏈中的且呈相同次序的有效訊息，但不具有無效訊息。然後，不可部分完成地處理此第二暫時訊息鏈，如上文所闡述。在某些情形中(諸如，舉例而言若不同現有裝置120具有不同值(此可由於(舉例而言)對具有多個裝置120之一系統之某些攻擊而發生)，此邏輯可係有用的。此第二類型之不可部分完成之處理可用以應用於相同鏈，以使(處於不同無效狀態之)裝置120達到一單個有效狀態。

此一例示性情形可係如下：一攻擊者可能能夠控制兩個休眠中金鑰D1及D2，且可使用此等休眠中金鑰將兩個訊息集合發佈至：(a) 某些裝置120，攻擊者可發佈用休眠中金鑰D1替換作用中金鑰A之訊息；及(b)其他裝置120，攻擊者可發佈用休眠中金鑰D2替換作用中金鑰A之訊息。因此，某些裝置120將使金鑰D1為作用中，且其他裝置將使D2為作用中。為補救此情形，若金鑰C1及C2仍未受波及，則可由CA將以下訊息鏈發佈至所有裝置：(a)「用C1替換D1」(用C1及C2簽署)；及(b)「用C1替換D2」(用C1及C2簽署)。若如上文所闡述而使用此第二類型之不可部分完成之處理來進行處理，則在其中D1係作用中金鑰的裝置中，將跳過訊息鏈之部分(b)；在其中D2係作用中金鑰的裝置中，將跳過訊息鏈之部分(a)。因此，將使所有裝置達到相同有效狀態(其中C1係作用中金鑰)而不管一特定裝置使D1或D2為一作用中金鑰。

關於圖4所闡述之方法假定，兩個受危及私密來源金鑰中之一者對應於電子裝置120內之當時作用中認證。圖6展示當兩個受危及私密金鑰102對應於電子裝置120內之休眠中認證時可藉以替換認證之一例示性方法。如圖4中，圖6展示兩個來源認證之一例示性私密來源金鑰替換程序；然而，應理解，可針對任何數目個認證使用其中所闡述之方法。

在步驟605處，CA 100可創建使目前作用中認證(其不對應於待替

換之兩個私密來源金鑰中之一者)無效且用對應於第一受危及來源金鑰之認證替換該目前作用中認證之一第一替換訊息。此第一替換訊息可由第一及第二受危及金鑰簽署。

在步驟610處，CA 100可創建使目前作用中認證(其係對應於第一受危及金鑰且在第一替換訊息中識別之替換認證)無效且用對應於第二受危及金鑰之一認證替換該目前作用中認證之一第二替換訊息。此第二替換訊息可由第二受危及金鑰及一個未受危及金鑰簽署。

在步驟615處，CA 100可創建使目前作用中認證(其係對應於第二受危及金鑰且在第二替換訊息中識別之替換認證)無效且用對應於一未受危及金鑰之一認證替換該目前作用中認證之一第三替換訊息。此第三替換訊息可由兩個未受危及金鑰簽署。

如圖4中，此等三個替換訊息應形成一序列；因此，每一替換訊息應使其需要先前訊息及需要下一訊息之旗標(及下一訊息雜湊，在適用之情形下)相應地設定。

在步驟620處，CA 100可將第一替換訊息發送至電子裝置120，在步驟625處，CA 100可將第二替換訊息發送至電子裝置120，且在步驟630處，CA 100可將第三替換訊息發送至電子裝置。

在步驟635處，在判定此等訊息中之每一者係替換訊息後，監督器160旋即判定是否已滿足由三個替換訊息中之每一者中之旗標設定之條件。舉例而言，談及第一替換訊息具有經設定以需要一後續訊息之需要下一訊息之旗標，監督器160可確認(i)其確實接收一第二替換訊息且(ii)第二替換訊息之雜湊具有與在第一替換訊息之雜湊資料欄位中接收之值相同之值。可針對第二及第三替換訊息執行此相同程序。

若在步驟635處已滿足由旗標設定之所有條件，則在步驟640處監督器160可處理第一替換訊息(例如，如上文關於圖3A至圖3C所闡

述)，在步驟645處監督器160可處理第二替換訊息，且在步驟650處監督器160可處理第三替換訊息。在步驟650結束時，將已替換三個金鑰(作用中金鑰及兩個受危及之休眠中金鑰)，且將已啟動一未受危及金鑰。

關於圖2至圖6所闡述之方法及資料結構展示可如何替換一或多個認證。然而，在其中替換兩個休眠中認證之關於圖6所展示之例示性方法中，在使兩個休眠中金鑰無效之過程中，亦撤銷當時作用中金鑰。因此，在某些實施例中，可較佳地執行僅撤銷(而非替換)一單個私密來源金鑰之一或多個程序。

應理解，可期望將本文中所闡述之撤銷程序之使用限制至僅休眠中來源金鑰；亦即，可不期望關於一作用中來源金鑰使用一撤銷程序。若關於一作用中來源金鑰使用一撤銷程序(而非隨後替換經撤銷金鑰)，則使用此等認證之系統將不具有作用中金鑰來用於認證驗證。

在一項實施例中，該系統可經組態以基於一或多個「自撤銷註釋」來處理一休眠中認證撤銷，該一或多個「自撤銷註釋」可係適於識別應撤銷之一私密來源金鑰102之任何類型之自鑑別訊息。可在執行任何撤銷操作之前由一CA 100準備一自撤銷註釋。舉例而言，在某些實施例中，可在緊鄰產生一來源私密金鑰之後準備一自撤銷註釋。儘管由CA 100提前準備自撤銷註釋700，但可期望將此等註釋700與金鑰101本身單獨地儲存以便減少一金鑰102及對應自撤銷註釋700兩者之一同時丟失之可能性。在某些實施例中，每一自撤銷註釋可與儲存其對應私密來源金鑰一樣安全地儲存。

圖7展示一例示性自撤銷註釋700、一對應休眠中認證撤銷訊息710及一例示性認證管理單元166之內容。圖8展示在由一CA 100撤銷對應私密來源金鑰101後可旋即藉以在一電子裝置120中替換一休眠中

認證之一例示性程序。出於闡釋之目的，關於圖8所闡述之程序將參考圖7上所展示之自撤銷註釋700、休眠中認證撤銷訊息710及認證管理單元166之值。然而，應理解，此等值僅係例示性的且所闡述之方法意欲對任何適當值起作用。

如圖7上所展示，一自撤銷註釋700可具有三個欄位：(1)一註釋類型702，其可係用以指示此係一自撤銷註釋700（諸如串「自撤銷」，如圖7上所展示）之任何適合資料；(2)一經撤銷認證識別符704，其可識別對應於待撤銷之休眠中來源私密金鑰102之認證；及(3)一自撤銷註釋數位簽章706，其可係使用對應於經撤銷認證識別符704之私密來源金鑰102創建之囊括註釋類型702及經撤銷認證識別符704兩者之一數位簽章。舉例而言，在圖7上所展示之例示性實施例中，待撤銷認證B，且自撤銷註釋700包含使用對應於認證B之來源私密金鑰創建之一數位簽章。

圖7亦展示可藉以結合一自撤銷註釋700使用之一例示性休眠中金鑰撤銷訊息710。如圖7上所展示，此休眠中金鑰撤銷訊息可包括：(1)訊息類型701，其可係用以指示此係一撤銷訊息710之任何適合資料；(2)一自撤銷註釋700，其識別對應於待撤銷之休眠中金鑰之認證；及(3)兩個數位簽章，「簽章1」 730及「簽章2」 731，其簽署休眠中金鑰撤銷訊息710。儘管上述實例闡述兩個數位簽章之使用，但應理解，本發明並不限於兩個簽章，且在某些實施例中，簽章之數目可係不同的，諸如一個或三個或三個以上。

在一項實施例中，可期望使用兩個休眠中金鑰來簽署休眠中金鑰撤銷訊息710。在另一實施例中，該等簽署金鑰中之一者可係一當前作用中金鑰。舉例而言，在圖7上所展示之例示性實施例中，待撤銷認證B，且休眠中金鑰撤銷訊息710已由當前作用中金鑰(亦即，對應於認證A之來源私密金鑰102)及一休眠中金鑰(亦即，對應於認證C

之來源私密金鑰102)簽署。

在某些實施例中，替代使用自撤銷註釋700來識別待撤銷之認證，休眠中金鑰撤銷訊息710可包括一經撤銷休眠中認證識別符(未展示)。在此等實施例中，休眠中金鑰撤銷訊息710應由對應於正撤銷之認證之自撤銷註釋700達成。

應理解，出於目前所闡述之例示性實施例之目的，不存在「替換認證識別符」(如關於圖2所闡述)，此乃因不需要替換當前作用中認證；僅正撤銷一休眠中(亦即，未使用)認證。

圖8展示在由一CA 100撤銷對應私密來源金鑰101後可旋即藉以在一電子裝置120中撤銷之一當前休眠中認證之一例示性程序。此外，應理解，出於目前所闡述之例示性方法之目的，不需要替換當前作用中認證，此乃因僅正撤銷一休眠中認證。

在步驟810處，監督器160可接收一休眠中認證撤銷訊息710及一相關聯之自撤銷註釋700(圖7)。此訊息可由CA 100直接或經由一或多個中間伺服器(例如，伺服器110)發送至監督器160且可基於訊息類型701而識別為一休眠中認證撤銷訊息710。

可使用下文將更詳細地闡述其中之每一者之步驟820至835來驗證休眠中認證撤銷訊息710及相關聯之自撤銷註釋700之真實性。

在步驟820處，監督器160可驗證在休眠中認證撤銷訊息內接收之數位簽章(例如，簽章1 730及簽章2 731)。此可包含若干子步驟，包含驗證休眠中認證撤銷訊息710包含正確數目個簽章且先前未撤銷簽署金鑰，如(舉例而言)關於圖3上所展示之步驟320至326所闡述。

在需要待由休眠中金鑰簽署之休眠中認證撤銷訊息中之所有數位簽章之實施例中，在步驟825處，監督器160可驗證休眠中認證撤銷訊息中之所有數位簽章實際上由休眠中金鑰簽署。

在步驟830處，監督器160可驗證其已接收一合法的自撤銷註釋

700。此可包含驗證註釋類型702將所接收資料闡述為一自撤銷註釋700，且可進一步包含驗證數位簽章706（在自撤銷註釋700內）與對應於由經撤銷休眠中認證識別符704識別之私密來源金鑰之所儲存認證匹配，亦即，自撤銷註釋700實際上由待撤銷之金鑰以數位方式簽署。

在步驟835處，監督器160可確認對應於所識別金鑰之認證係休眠中的。

若在步驟820至835中之任一者處執行之驗證中之一者失敗，則監督器160可不執行任何額外撤銷操作而是可在步驟850處試圖（直接地或經由一或多個額外伺服器間接地）將一原則違規通知CA 100。此一通知可包含（舉例而言）由電子裝置120接收之休眠中認證撤銷訊息710及自撤銷註釋700以及任何其他適當資訊，諸如方法失敗之特定原因。否則，若在步驟820至835處執行之所有驗證皆成功通過，則在步驟840處監督器160可將所識別認證之狀態改變為經撤銷。

應理解，即使一私密來源金鑰102被盜竊（例如，以使得金鑰102為一攻擊者所擁有，但不為CA所擁有）或被破壞，只要其自撤銷註釋700保持為各別CA 100所擁有，亦可使用此自撤銷註釋700來撤銷對應數位認證。另外，即使一攻擊者具有兩個金鑰，攻擊者亦不可在不具有針對任何其他金鑰之一自撤銷註釋之情況下撤銷彼其他金鑰。

關於圖7及圖8之上述說明闡述可藉以使用一自撤銷註釋700直接撤銷一單個休眠中金鑰之一程序。然而，在某些情景中可期望使用自撤銷註釋700來撤銷多個休眠中金鑰。在某些實施例中，可僅針對待撤銷之每一休眠中金鑰重複關於圖8所展示之方法。在其他實施例中，可較佳地使用關於圖6所闡述之方法之一變型，其中每一休眠中金鑰撤銷訊息710可進一步包括需要下一訊息之欄位、需要先前訊息之欄位及下一訊息雜湊欄位，例如，如關於圖5所闡述。

由於金鑰之撤銷將減少其餘有效金鑰之數目，因此在某些實施例中，可期望提供可藉以將一新來源私密金鑰添加至系統中且可將一對應認證上載至電子裝置120中之一機制。應理解，在此等實施例中，認證儲存器141可需要係可寫入的(亦即，並非唯讀)。

圖9展示一例示性新認證訊息900及一例示性認證管理單元166之內容。圖10展示在由一CA 100創建一新私密來源金鑰101後可旋即藉以將一新認證添加至一電子裝置120之一例示性程序。出於闡釋之目的，關於圖10所闡述之程序將參考在圖9上所展示之新認證訊息900及認證管理單元166之值。然而，應理解，此等值僅係例示性的且所闡述之方法意欲對任何適當值起作用。

如圖9上所展示，一新認證訊息900可具有四個或四個以上欄位：(1)訊息類型901，其可係用以指示此係一撤銷訊息900之任何適合資料；(2)一新認證識別符902，其可識別對應於新來源私密金鑰102之新認證；(3)新認證(或來源公開金鑰) 904；及(4)一或多個數位簽章，其中一或多個現有私密來源金鑰102可用於以數位方式簽署新認證識別符902及新認證904。舉例而言，為增強系統之中體安全性，在一項例示性實施例中，可較佳地用其餘未經撤銷金鑰(無論作用中還是休眠中)以數位方式簽署新認證識別符902及新認證904。在圖9上所展示之例示性實施例中，已撤銷認證A，且將新認證識別為認證D之新認證訊息900已由對應於認證B及C (分別展示為簽章1 930及簽章2 931)之兩個其餘來源私密金鑰簽署。

由於認證管理單元166之容量可係有限的，因此在某些實施例中，認證管理單元166中之至少一個金鑰應具有一「經撤銷」狀態，以使得當接收一新認證訊息900時，將替代一先前經撤銷金鑰而儲存新認證904。為確保此性質，在某些此等實施例中，可緊鄰一認證替換或撤銷訊息之後發送新認證訊息900。

圖10展示在由一CA 100產生一新私密來源金鑰101之後可藉以將一新認證添加至一電子裝置120之一例示性程序。

在步驟1010處，監督器160可接收一新認證訊息900 (圖9)。此訊息可由CA 100直接或經由一或多個中間伺服器(例如，伺服器110)發送至監督器160且可藉由訊息類型901識別為一新認證訊息900。

可使用下文將更詳細地闡述其中之每一者之步驟1020至1040來驗證新認證訊息900之真實性。

在步驟1020處，監督器160可驗證在新認證訊息內接收之數位簽章，例如，簽章1 930及簽章2 931。此可包含若干子步驟，包含驗證新認證訊息900包含正確數目個簽章(例如，全部(並非僅一子集)未經撤銷金鑰)且先前未撤銷簽署金鑰，如(舉例而言)關於圖3上所展示之步驟320至326所闡述。舉例而言，在圖9上所展示之實施例中，監督器160可確認(i)新認證訊息900使用對應於認證B及認證C兩者之來源私密金鑰102以數位方式簽署且(ii)其並非使用對應於認證A (其先前已經撤銷，如欄位142中所展示)之來源私密金鑰102而簽署。

在步驟1030處，監督器160可驗證新接收之數位認證904先前未儲存於認證管理單元166內。

在步驟1040處，監督器160可確認可將一新認證添加至認證管理單元166。舉例而言，在某些實施例中，認證管理單元166可確認其具有可由一新認證替換之至少一個「經撤銷」認證。

若在步驟1020至1040中之任一者處執行之驗證中之一者失敗，則監督器160可不執行任何額外更新操作而是在某些實施例中可在步驟1060處試圖(直接地或經由一或多個額外伺服器間接地)將一原則違規通知CA 100。此一通知可包含(舉例而言)新認證訊息900及任何其他適當資訊，諸如方法失敗之特定原因。否則，若在步驟1020至1040處執行之所有驗證皆成功通過，則在步驟1050處監督器160可將具有

一「休眠中」狀態之新認證添加至認證管理單元166。

時常，情形可係意外(或以其他方式)破壞一來源私密金鑰102。若經破壞金鑰係一休眠中金鑰，則CA 100可僅永不使彼金鑰作用中。然而，若其係已破壞(或盜竊)之一作用中金鑰，則裝置120可仍還原至一可管理狀態，此乃因本文中所闡述之方法不需要使用該作用中金鑰來進行其撤銷。舉例而言，使用關於圖3A至圖3C所闡述之方法，CA 100可選擇一新私密來源金鑰102來啟動且可將一訊息發送至所有電子裝置120以撤銷並替換作用中認證，其中該訊息已由(舉例而言)新金鑰及一或多個休眠中金鑰簽署。換言之，丟失且正替換之作用中金鑰並非撤銷對應認證所必需的。

應理解，雖然上述論述假定一單個作用中金鑰，但本發明亦預計使用多個作用中金鑰。在此等實施例中，可需要數個簽章來使由來源金鑰發佈之一認證有效。可如上文所闡述而處置此等實施例中之作用中金鑰。

雖然已圖解說明及闡述本發明之特定實施例及應用，但應理解本發明並不限於本文中所揭示之精確組態及組件。僅以圖解說明之方式陳述本文中所使用之術語、說明及圖且其並不意欲作為限制。可在不背離本發明之精神及範疇之情況下對本文中所揭示之本發明裝置、方法及系統之配置、操作及細節做出對於熟習此項技術者將顯而易見的各種修改、改變及變化。以非限制性實例之方式，將理解，本文中所包括之方塊圖意欲展示每一裝置及系統之組件之一選定子組，且每一所圖示之裝置及系統可包括圖式上未展示之其他組件。另外，彼等熟習此項技術者將認識到，可在不背離本文中所闡述之實施例之範疇或效能之情況下省略或重新排序本文中所闡述之某些步驟及功能性。

結合本文中所揭示之實施例所闡述之各種說明性邏輯區塊、模組、電路及演算法步驟可實施為電子硬體、電腦軟體或兩者之組合。

為說明硬體與軟體的此可互換性，上文已就其功能性總體闡述了各種說明性組件、區塊、模組、電路及步驟。此功能性實施為硬體還是軟體取決於特定應用及施加於整個系統之設計約束條件。所闡述之功能性可針對每一特定應用以不同方式來實施--諸如藉由使用微處理器、微控制器、場可程式化閘陣列(FPGA)、特殊應用積體電路(ASIC)及/或單晶片系統(SoC)之任一組合--但此等實施方案決策不應被解釋為導致對本發明之範疇之一背離。

結合本文中所揭示之實施例所闡述之一方法或演算法之步驟可直接體現於硬體中、由一處理器執行之一軟體模組中或兩者之一組合中。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、硬磁碟、一可抽換式磁碟、一CD-ROM或此項技術中已知的任何其他形式之儲存媒體中。

本文中所揭示之方法包含用於達成所闡述之方法之一或多個步驟或動作。該等方法步驟及/或動作可彼此互換而不背離本發明之範疇。換言之，除非需要一特定的步驟或動作次序來達成實施例之恰當操作，否則可在不背離本發明之範疇之情況下修改特定步驟及/或動作之次序及/或使用。

【符號說明】

- 100 認證授權單位(CA)
- 101 集合
- 102 來源私密金鑰/私密來源金鑰
- 105 通信通道
- 110 中間伺服器
- 120 電子裝置/裝置
- 121 密碼編譯引擎
- 141 來源認證儲存器/認證儲存器

142	認證屬性儲存器/屬性儲存器
160	監督器
166	專用認證管理單元/認證管理單元
180	遠端電子裝置或伺服器
200	訊息/認證替換訊息/替換訊息
201	訊息類型
210	經撤銷認證識別符
215	替換認證識別符
220	認證識別符欄位
221	認證識別符欄位
230	簽章1
231	簽章2
500	第一替換訊息/替換訊息/訊息
510	第二替換訊息/替換訊息/訊息
540	需要先前訊息之旗標
541	需要下一訊息之旗標
551	欄位/下一訊息之一雜湊
560	需要先前訊息之旗標
561	需要下一訊息之旗標
571	欄位/下一訊息之一雜湊
700	例示性自撤銷註釋
701	訊息類型
702	註釋類型
704	經撤銷休眠中認證識別符
706	數位簽章
730	簽章1

731	簽章2
900	例示性新認證訊息
901	訊息類型
902	新認證識別符
904	新認證(或來源公開金鑰)
930	簽章1
931	簽章2
A	來源認證
B	來源認證
C	來源認證
D	來源認證
E	來源認證

申請專利範圍

1. 一種設備，其包括：
 - 一非揮發性儲存器，其儲存複數個來源認證；
 - 一監督器，其經組態以：
 - 接收識別待撤銷之儲存於該非揮發性儲存器中之該複數個來源認證中之一者之一訊息；
 - 驗證該訊息係由對應於儲存於該非揮發性儲存器中之兩個來源認證之至少兩個私密金鑰所簽署；及
 - 撤銷該訊息中所識別之該來源認證。
2. 如請求項1之設備，其中該訊息係識別待撤銷之一第一來源認證及待啓動之一第二來源認證之一替換訊息。
3. 如請求項2之設備，其中用以驗證該兩個私密金鑰簽章之該兩個來源認證係該第二來源認證及尚未被撤銷之一第三來源認證。
4. 如請求項2之設備，其中用以驗證該兩個私密金鑰簽章之該兩個來源認證係該第一來源認證及該第二來源認證。
5. 如請求項2之設備，其中該複數個來源認證中之至少一個來源認證具有一作用中屬性，且該複數個來源認證中之另一來源認證具有一休眠中屬性。
6. 如請求項5之設備，其中該監督器進一步經組態以驗證用以簽署該訊息之所有私密金鑰對應於具有一休眠中屬性之儲存於該非揮發性儲存器中之來源認證。
7. 如請求項5之設備，其中該監督器進一步經組態以驗證用以簽署該訊息之一個私密金鑰對應於具有一作用中屬性之儲存於該非揮發性儲存器中之該複數個來源認證中之一來源認證，且用以簽署該訊息之所有其他私密金鑰對應於具有一休眠中屬性之儲

存於該非揮發性儲存器中之來源認證。

8. 如請求項2之設備，其中該替換訊息係各自識別待撤銷之一來源認證及待啓動之另一來源認證之一替換訊息鏈中之一個替換訊息，且該鏈中之每一替換訊息包含識別是否需要一先前訊息之一第一欄位及識別是否需要下一訊息之一第二欄位。
9. 如請求項8之設備，其中該鏈中之每一替換訊息包含用於該下一訊息之一雜湊之一第三欄位。
10. 如請求項8之設備，其中該鏈中之每一替換訊息包含用於該先前訊息之一雜湊之一第三欄位。
11. 如請求項8之設備，其中該監督器進一步經組態以不可部分完成地處理該替換訊息鏈。
12. 如請求項1之設備，其中該訊息係包含一自撤銷註釋之一休眠中認證撤銷訊息，該自撤銷註釋含有待撤銷之一來源認證之一識別符及由對應於待撤銷之該經識別來源認證之一私密金鑰簽署之一簽章。
13. 如請求項1之設備，其中該非揮發性儲存器具有用以儲存該複數個來源認證之一唯讀空間及用以儲存相關聯之屬性之一可寫入空間。
14. 如請求項2之設備，其中該非揮發性儲存器具有用以儲存該複數個來源認證之一可寫入空間。
15. 如請求項14之設備，其中該監督器進一步經組態以：

接收包含一新認證識別符、一新認證及一或多個數位簽章之一新認證訊息；

驗證簽署該新認證訊息之該一或多個數位簽章係由對應於儲存於該非揮發性儲存器中之來源認證之私密金鑰所產生；且

將該新認證添加至該非揮發性儲存器。

16. 如請求項15之設備，其中該一或多個數位簽章係由對應於未撤銷之儲存於該非揮發性儲存器中之所有來源認證之私密金鑰所產生。
17. 一種電腦實施之方法，其包括：
 - 將複數個來源認證儲存於一設備之一非揮發性儲存器中；
 - 接收識別待撤銷之儲存於該非揮發性儲存器中之該複數個來源認證中之一者之一訊息；
 - 驗證該訊息係由對應於儲存於該非揮發性儲存器中之兩個來源認證之至少兩個私密金鑰所簽署；及
 - 撤銷該訊息中所識別之該來源認證。
18. 如請求項17之電腦實施之方法，其中該訊息係識別待撤銷之一第一來源認證及待啓動之一第二來源認證之一替換訊息。
19. 如請求項18之電腦實施之方法，其中用以驗證該兩個私密金鑰簽章之該兩個來源認證係該第二來源認證及尚未撤銷之一第三來源認證。
20. 如請求項18之電腦實施之方法，其中用以驗證該兩個私密金鑰簽章之該兩個來源認證係該第一來源認證及該第二來源認證。
21. 如請求項18之電腦實施之方法，其中該複數個來源認證中之至少一個來源認證具有一作用中屬性，且該複數個來源認證中之另一來源認證具有一休眠中屬性。
22. 如請求項21之電腦實施之方法，進一步包括驗證用以簽署該訊息之所有私密金鑰對應於具有一休眠中屬性之儲存於該非揮發性儲存器中之來源認證。
23. 如請求項21之電腦實施之方法，進一步包括驗證用以簽署該訊息之一個私密金鑰對應於具有一作用中屬性之儲存於該非揮發性儲存器中之該複數個來源認證中之一來源認證，且用以簽署

該訊息之所有其他私密金鑰對應於具有一休眠中屬性之儲存於該非揮發性儲存器中之來源認證。

24. 如請求項18之電腦實施之方法，其中該替換訊息係各自識別待撤銷之一來源認證及待啓動之另一來源認證之一替換訊息鏈中之一個替換訊息，且該鏈中之每一替換訊息包含識別是否需要一先前訊息之一第一欄位、識別是否需要下一訊息之一第二欄位。
25. 如請求項24之電腦實施之方法，其中該鏈中之每一替換訊息包含用於該下一訊息之一雜湊之一第三欄位。
26. 如請求項24之電腦實施之方法，其中該鏈中之每一替換訊息包含用於該先前訊息之一雜湊之一第三欄位。
27. 如請求項24之電腦實施之方法，進一步包括不可部分完成地處理該替換訊息鏈。
28. 如請求項17之電腦實施之方法，其中該訊息係包含一自撤銷註釋之一休眠中認證撤銷訊息，該自撤銷註釋含有待撤銷之一來源認證之一識別符及由對應於待撤銷之該經識別來源認證之一私密金鑰所簽署之一簽章。
29. 如請求項17之電腦實施之方法，進一步包括：
 - 接收包含一新認證識別符、一新認證及一或多個數位簽章之一新認證訊息；
 - 驗證簽署該新認證訊息之該一或多個數位簽章係由對應於儲存於該非揮發性儲存器中之來源認證之私密金鑰所產生；及
 - 將該新認證添加至該非揮發性儲存器。
30. 如請求項29之電腦實施之方法，其中由對應於未撤銷之儲存於該非揮發性儲存器中之所有來源認證之私密金鑰產生該一或多個數位簽章。

31. 一種電腦實施之方法，其包括：

在一認證授權單位處判定需要撤銷一第一私密金鑰；

產生識別待在一用戶端裝置處撤銷之一第一來源認證之一訊息，該第一來源認證對應於該第一私密金鑰；

由對應於儲存於該用戶端裝置處之兩個來源認證之至少兩個私密金鑰簽署該訊息；及

將該所簽署訊息發送至該用戶端裝置。

32. 如請求項31之電腦實施之方法，其中該訊息係識別待啓動之一第二來源認證之一替換訊息，該第二來源認證對應於該認證授權單位處之一第二私密金鑰。

33. 如請求項32之電腦實施之方法，其中簽署該訊息之該至少兩個私密金鑰中之一者係該第二私密金鑰。

34. 如請求項31之電腦實施之方法，其中簽署該訊息之該至少兩個私密金鑰係休眠中私密金鑰。

35. 如請求項32之電腦實施之方法，其中簽署該訊息之該至少兩個私密金鑰中之一者係該第一私密金鑰。

36. 如請求項32之電腦實施之方法，其中該替換訊息係各自識別待撤銷之一來源認證及待啓動之另一來源認證之一替換訊息鏈中之一個替換訊息，且該鏈中之每一替換訊息包含識別是否需要一先前訊息之一第一欄位、識別是否需要下一訊息之一第二欄位。

37. 如請求項36之電腦實施之方法，其中該鏈中之每一替換訊息包含用於該下一訊息之一雜湊之一第三欄位。

38. 如請求項36之電腦實施之方法，其中該鏈中之每一替換訊息包含用於該先前訊息之一雜湊之一第三欄位。

39. 如請求項36之電腦實施之方法，其中該訊息係包含一自撤銷註

釋之一休眠中認證撤銷訊息，該自撤銷註釋含有待撤銷之一來源認證之一識別符及由對應於待撤銷之該經識別來源認證之一私密金鑰所簽署之一簽章。

圖式

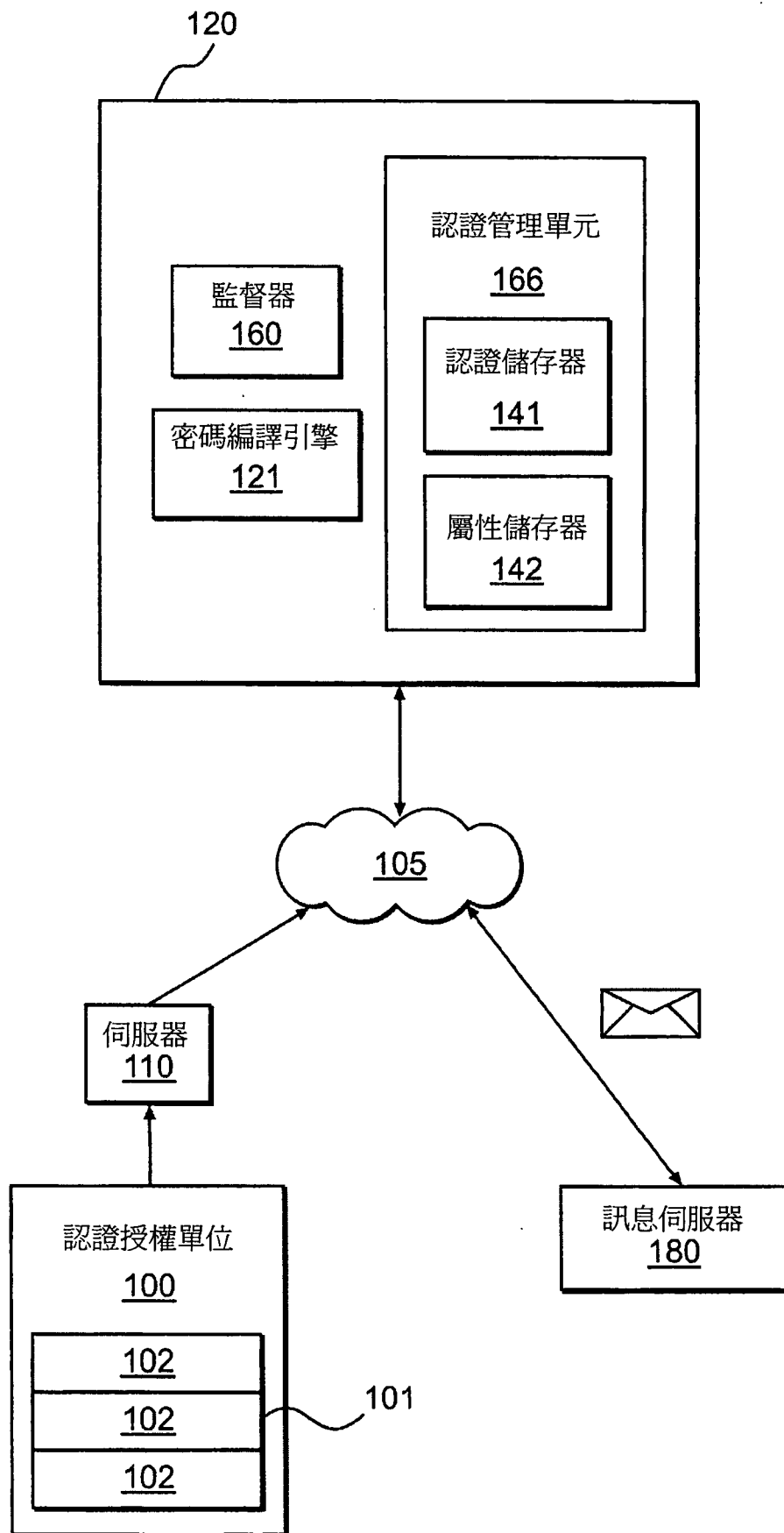


圖 1

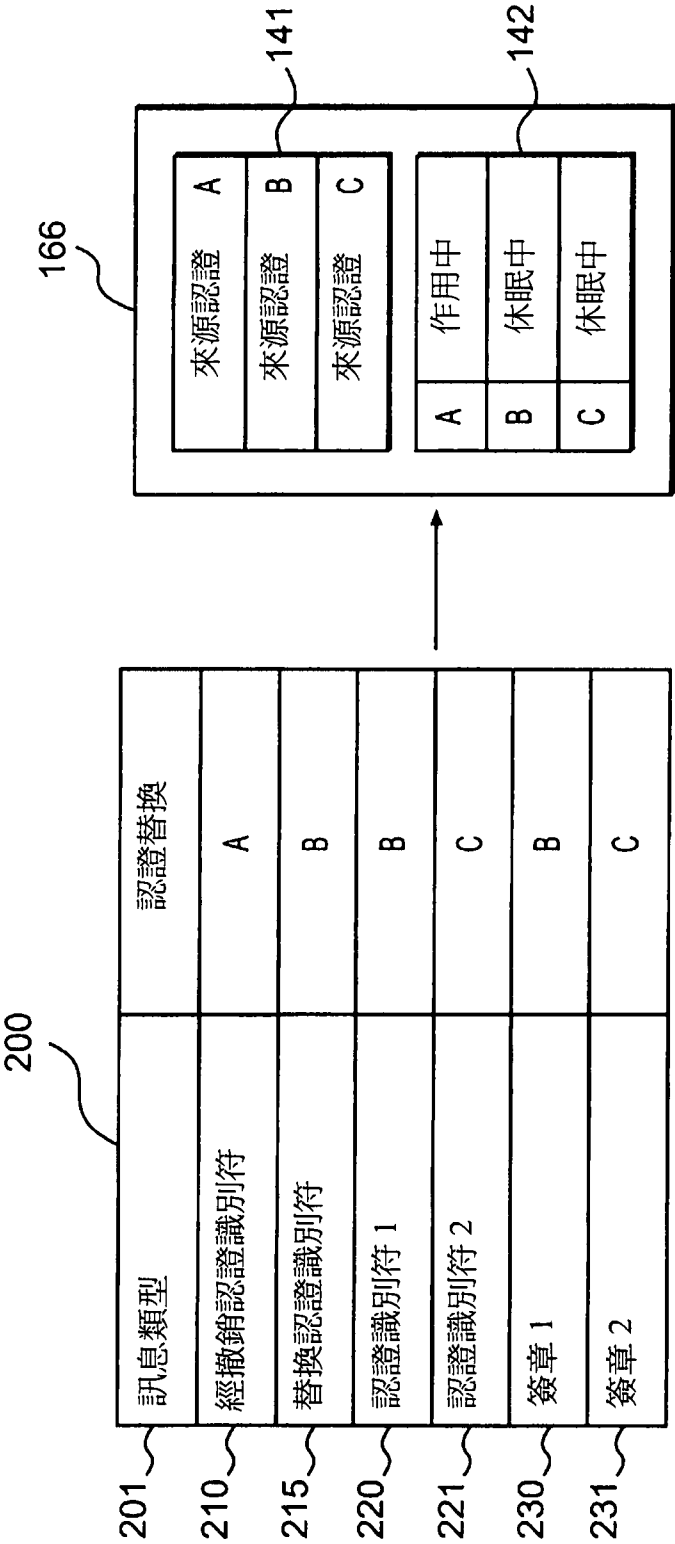


圖 2

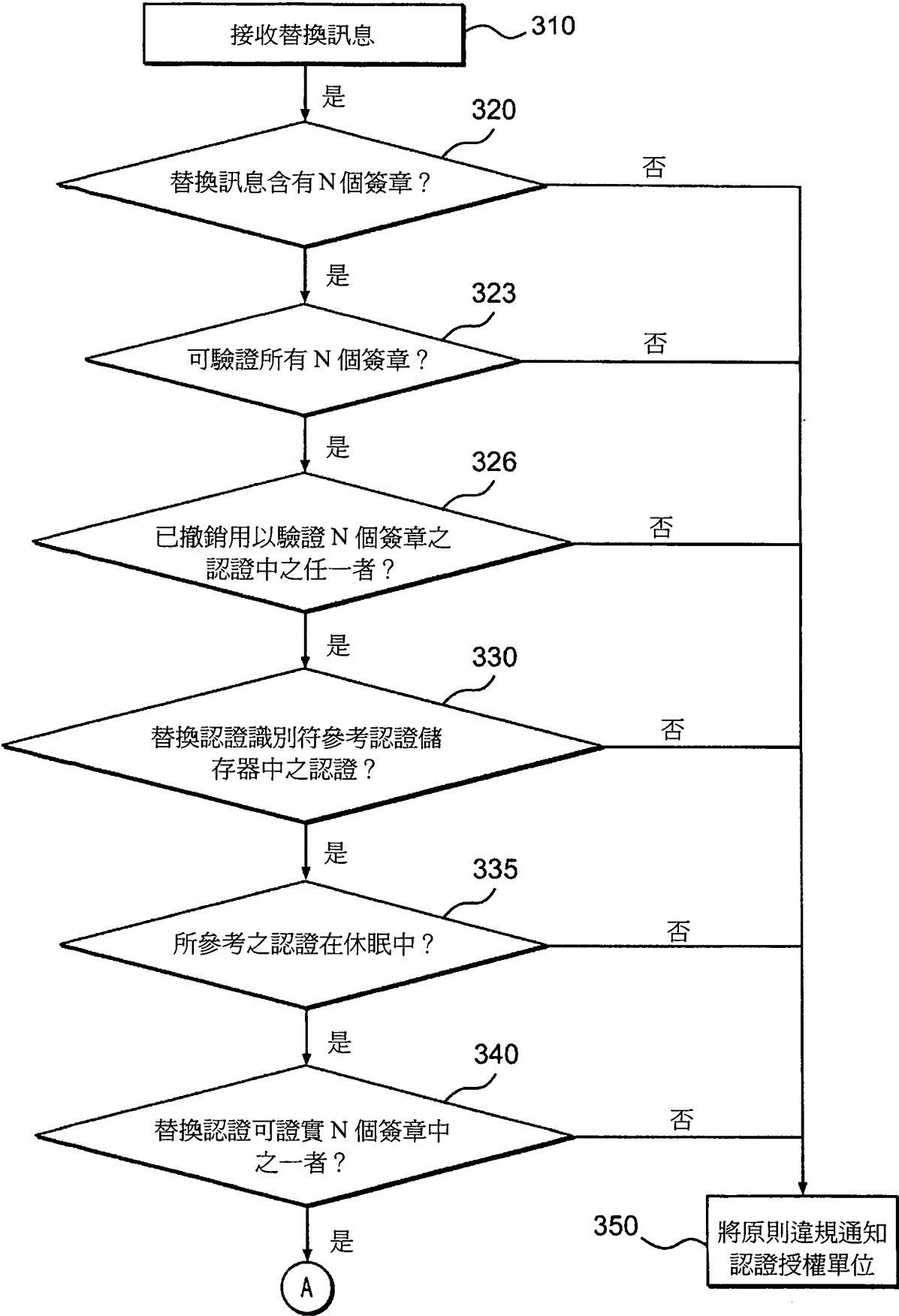


圖 3A

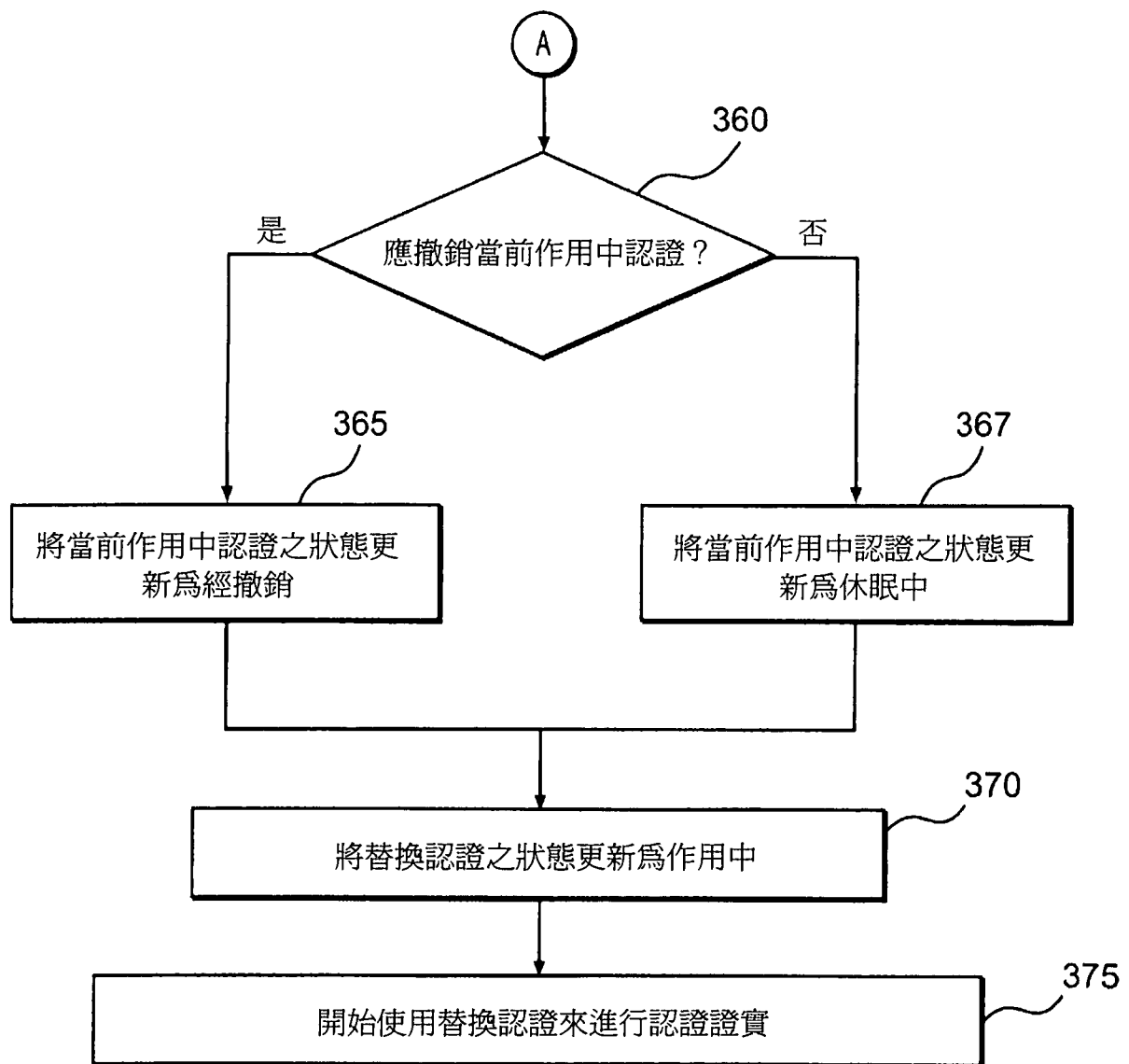


圖 3B

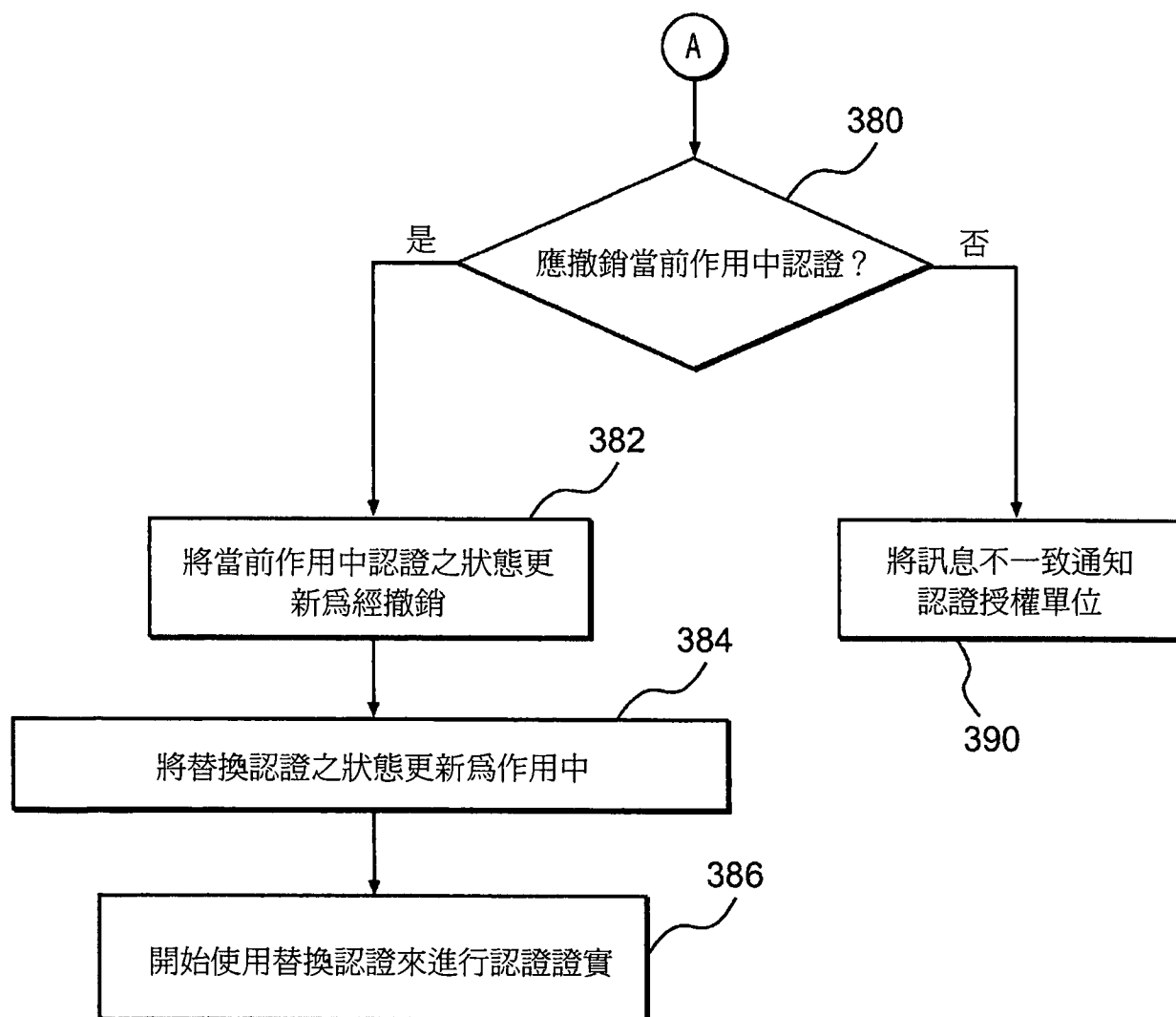


圖 3C

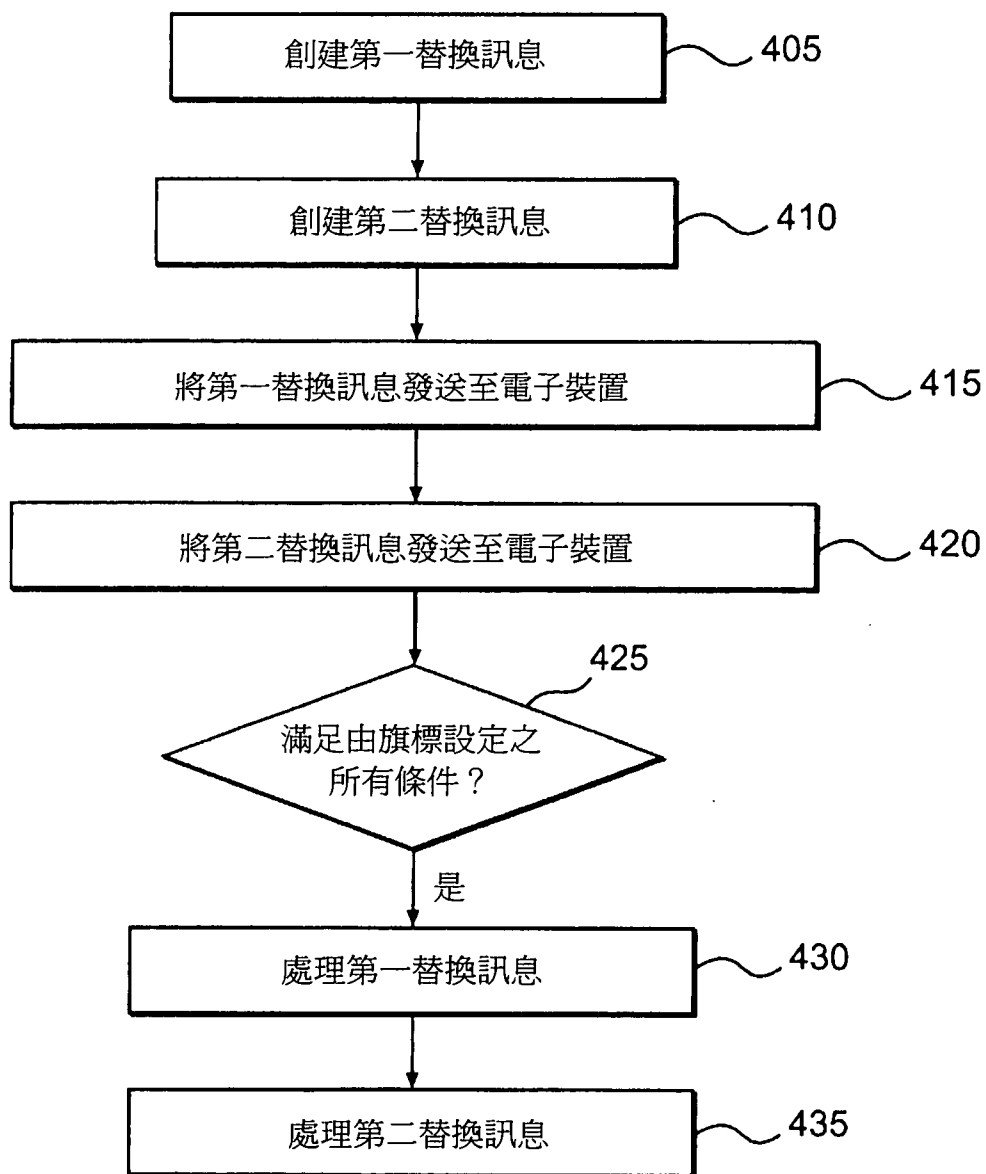


圖 4

500

501	訊息類型	認證替換
510	經撤銷認證識別符	A
515	替換認證識別符	B
530	簽章 1	B
531	簽章 2	C
540	需要先前訊息	否
541	需要下一訊息	是
551	下一訊息之雜湊	...

166

141	
來源認證	A
來源認證	B
來源認證	C
來源認證	D
來源認證	E
142	
A	作用中
B	休眠中
C	休眠中
D	休眠中
E	休眠中

510

501	訊息類型	認證替換
510	經撤銷認證識別符	B
515	替換認證識別符	C
530	簽章 1	C
531	簽章 2	D
560	需要先前訊息	是
561	需要下一訊息	否
571	下一訊息之雜湊	空值

圖 5

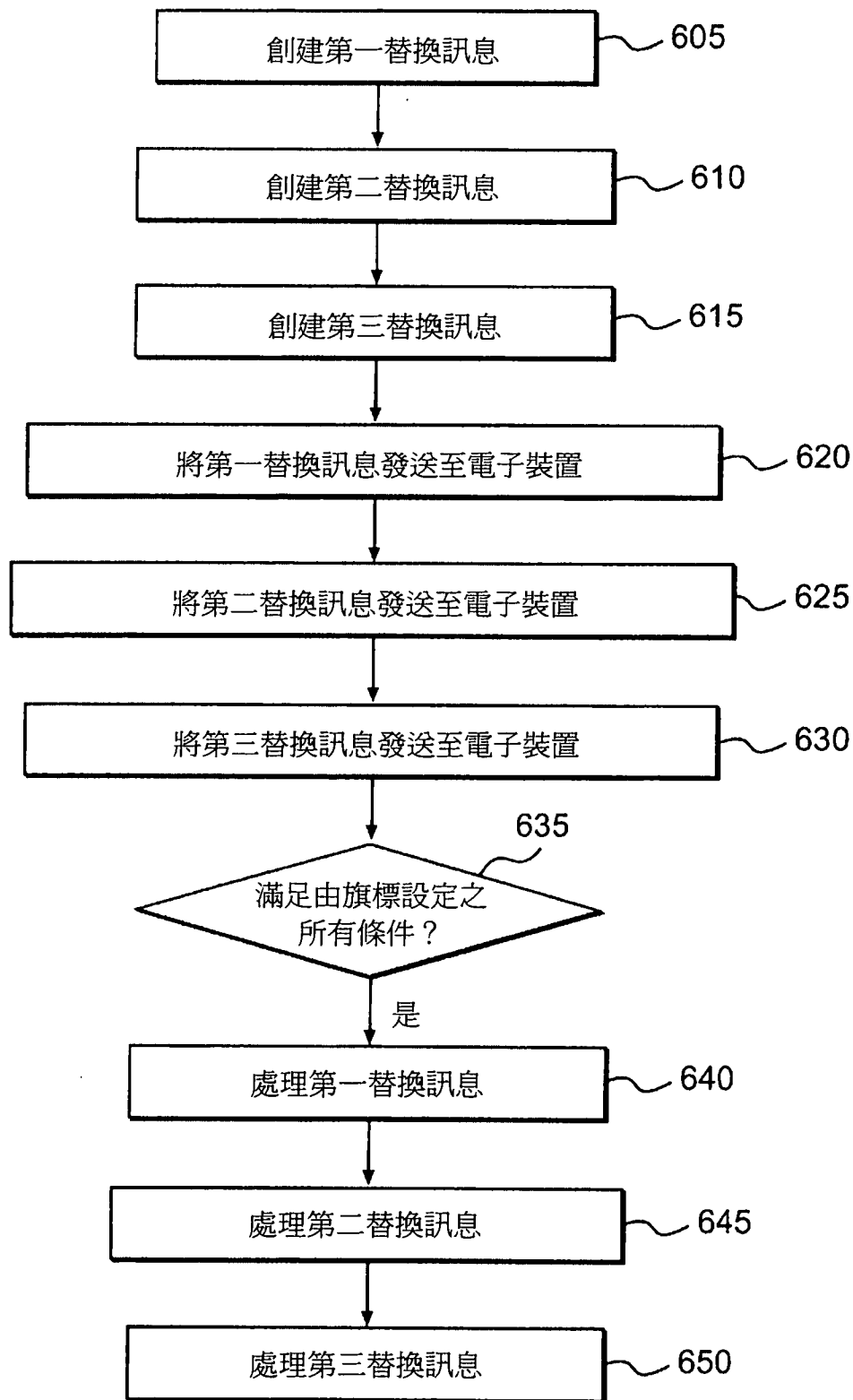


圖 6

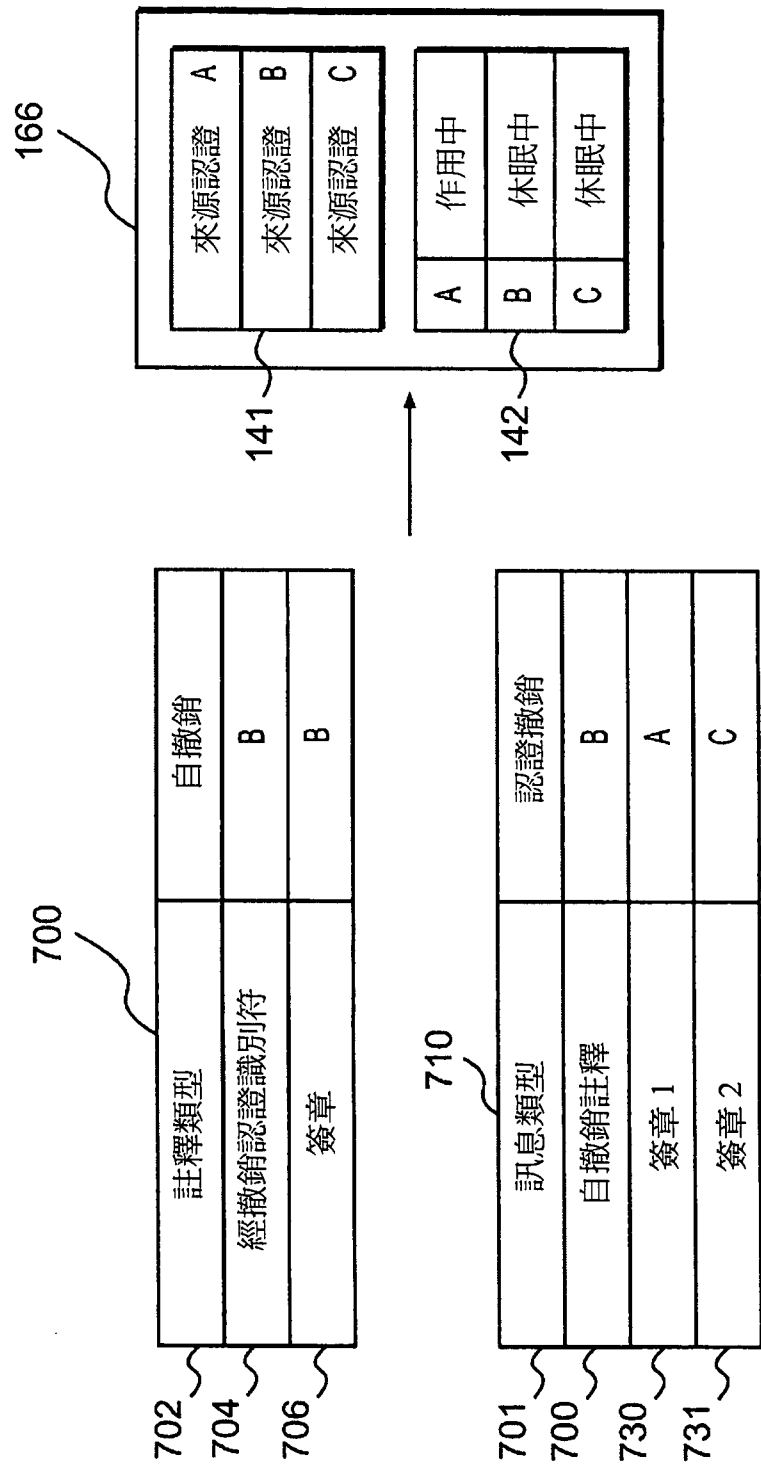


圖 7

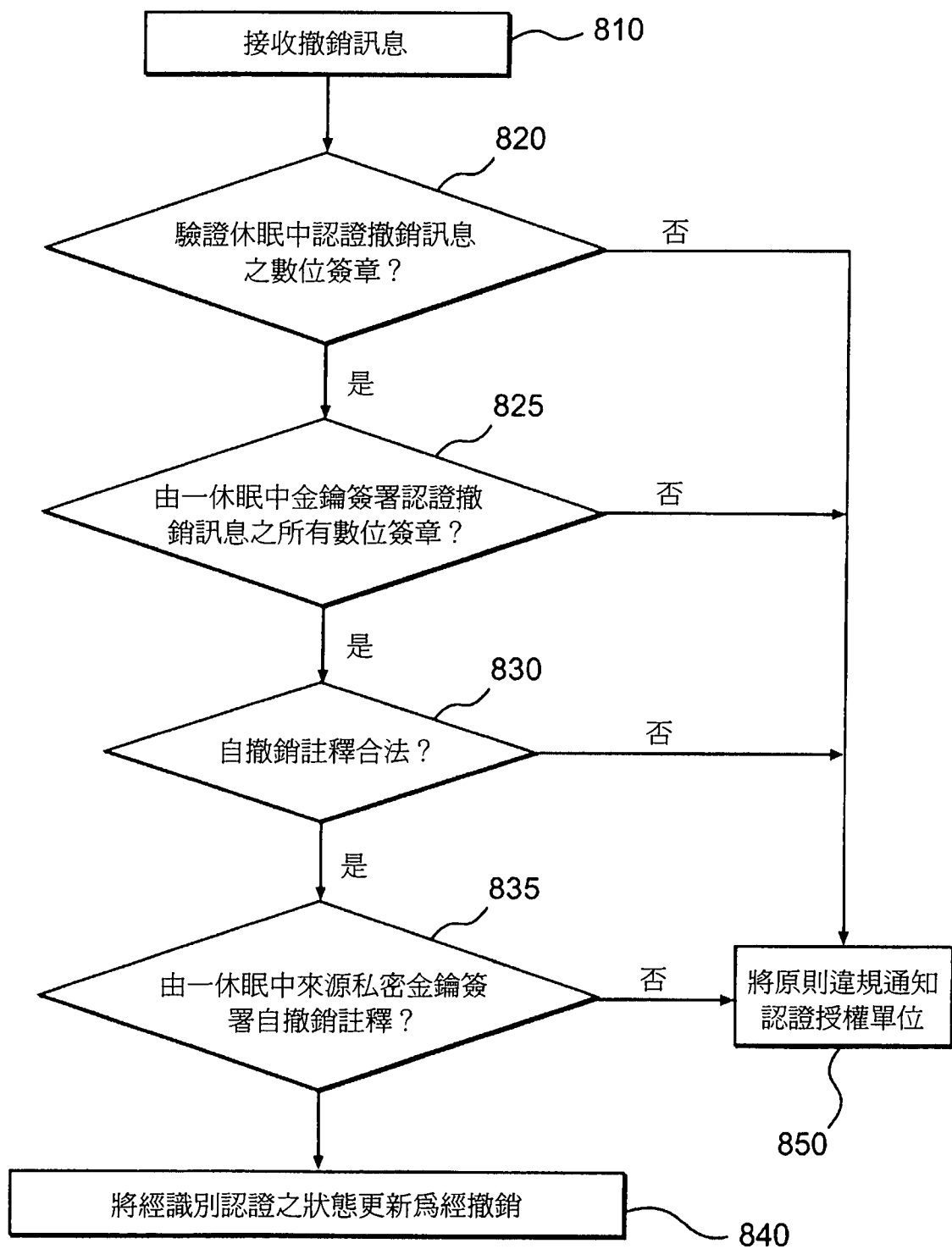


圖 8

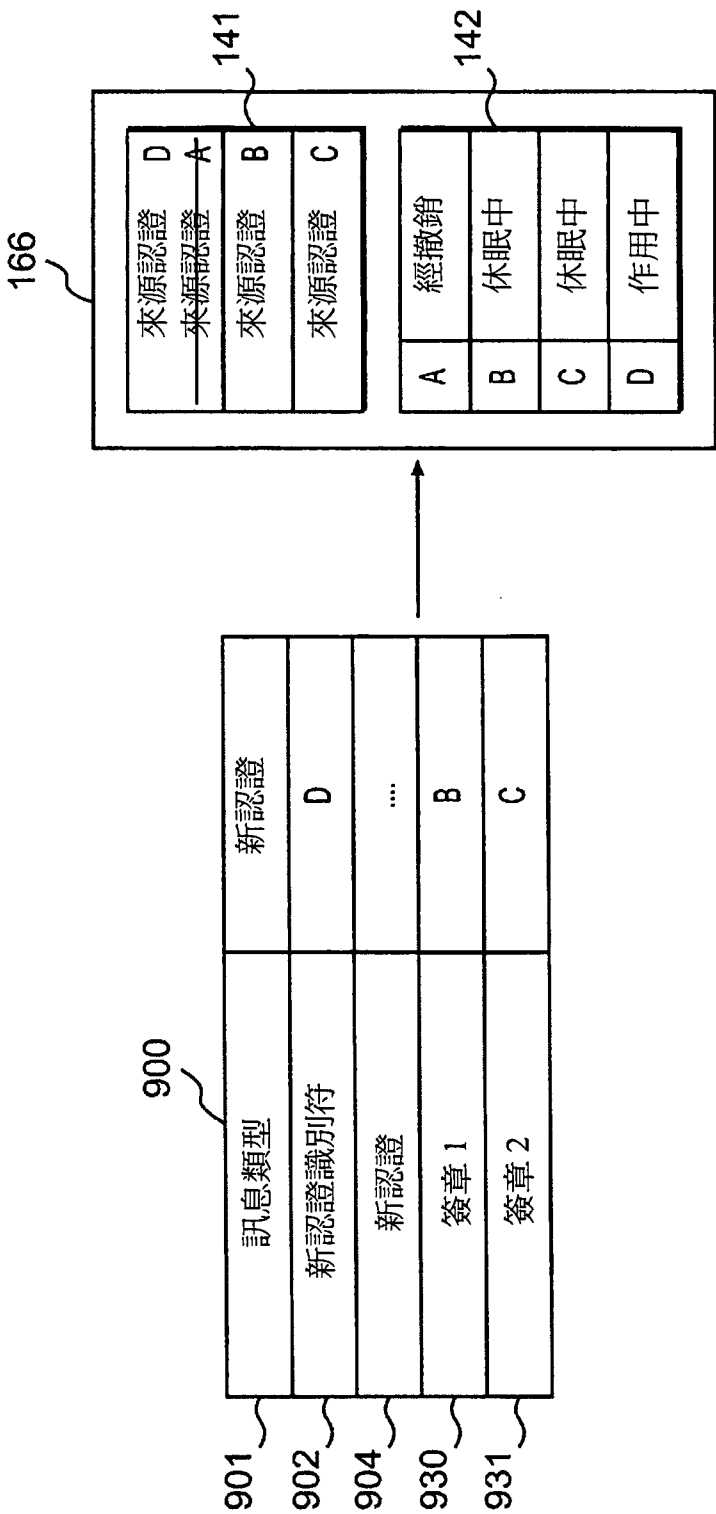


圖 9

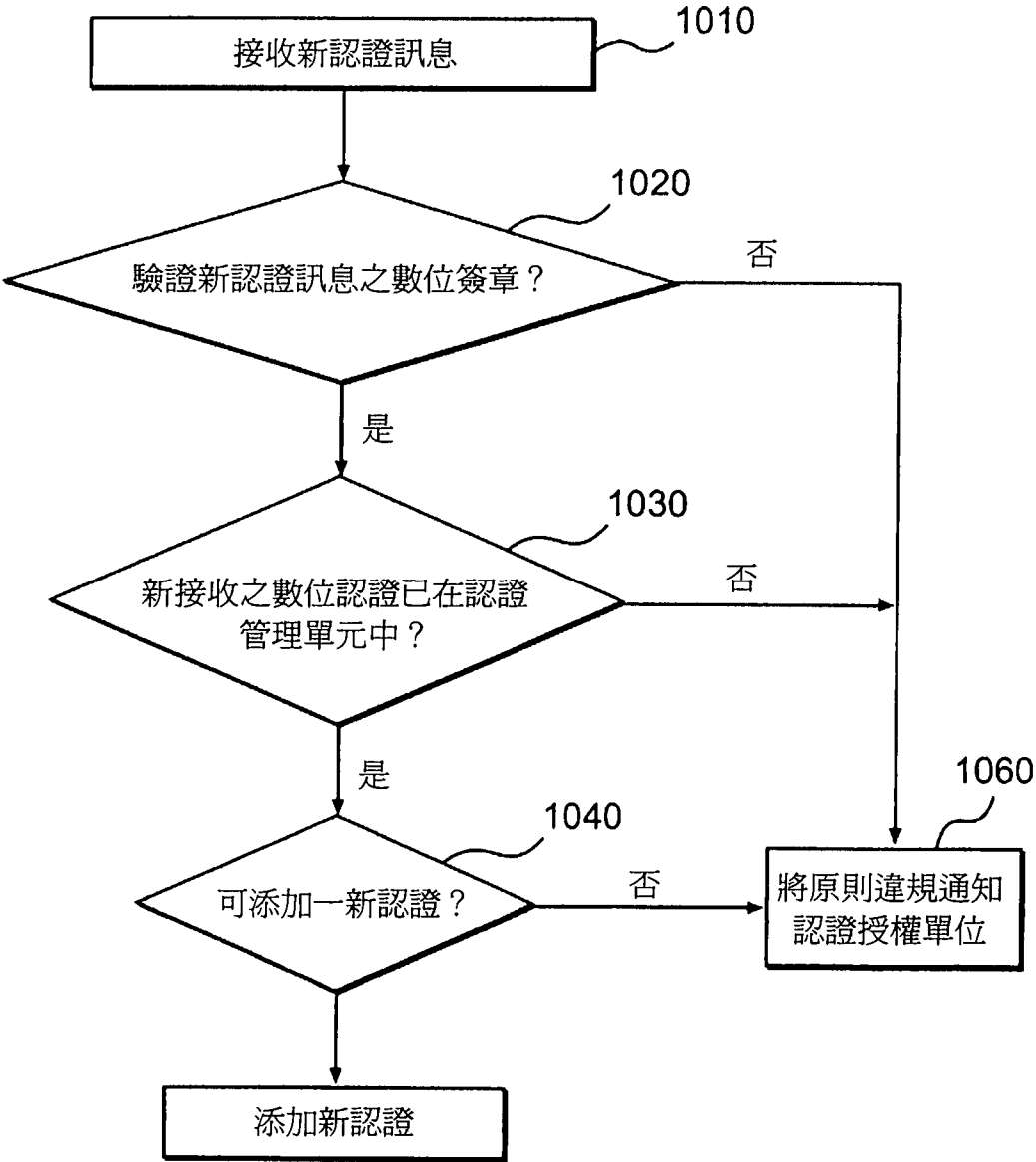


圖 10