



(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 201220804 A1

(43)公開日：中華民國 101 (2012) 年 05 月 16 日

(21)申請案號：099138438

(22)申請日：中華民國 99 (2010) 年 11 月 09 日

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

(71)申請人：中華電信股份有限公司 (中華民國) CHUNGHWA TELECOM CO., LTD. (TW)

桃園縣楊梅市民族路 5 段 551 巷 12 號

(72)發明人：簡長成 (TW)；林景榮 (TW)；蔡文慧 (TW)；謝東明 (TW)；張耿豪 (TW)

(74)代理人：李保祿

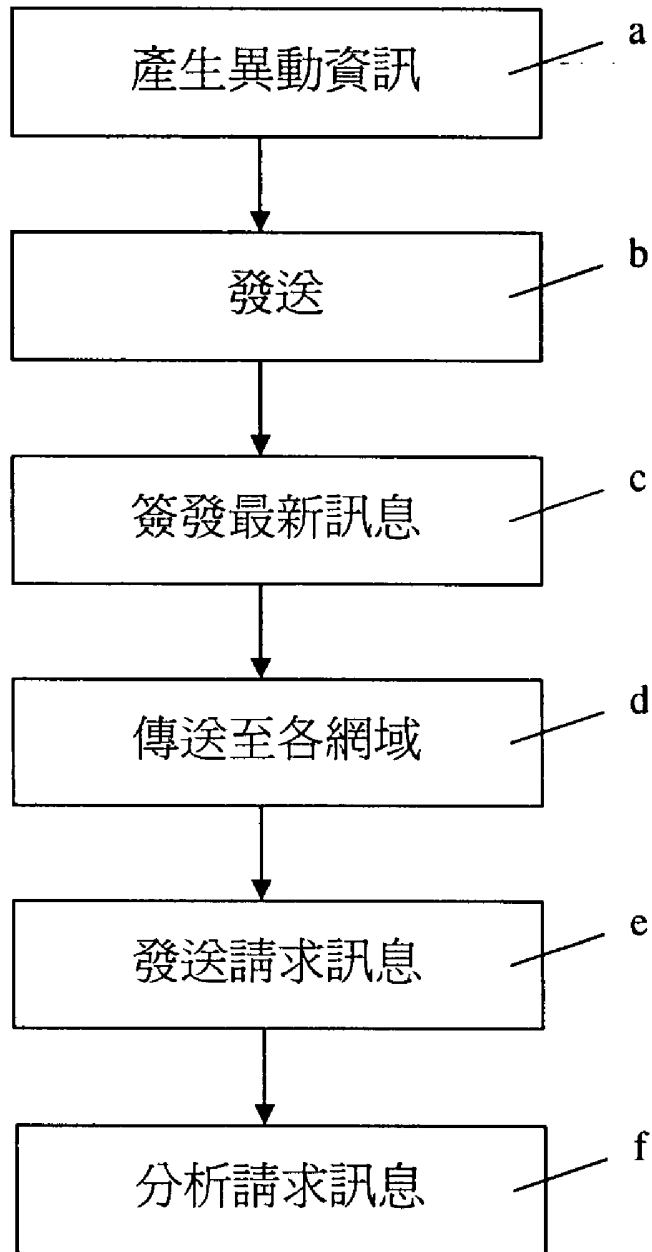
申請實體審查：有 申請專利範圍項數：8 項 圖式數：3 共 24 頁

(54)名稱

具有高信任度的分散式快速驗證憑證狀態之方法

(57)摘要

一種具有高信任度的分散式快速驗證憑證狀態之方法，係包含下列步驟：a、產生異動資訊；b、發送；c、簽發最新訊息；d、傳送至各個網域；e、用戶端發送請求訊息；以及 f、用戶端接收回應訊息；藉此，運用線上憑證狀態協定(Online Certificate Status Protocol，以下簡稱 OCSP)為基礎，提供高信任度的訊息驗證保護，再以分散式系統架構來提供更快速的憑證狀態查詢與驗證之服務，以完成具有高信任度的快速憑證狀態查詢之作業。



a：產生異動資訊

b：發送

c：簽發最新訊息

d：傳送至各網域

e：發送請求訊息

f：分析請求訊息

六、發明說明：

【發明所屬之技術領域】

本發明係有關於一種具有高信任度的分散式快速驗證憑證狀態之方法，特別是指如何快速地取得高信任度的電子憑證狀態之資訊，尤適於應用在電子交易系統、高機密性的資訊系統或類似系統者。

【先前技術】

早期電子憑證狀態驗證技術，有採用電子憑證路徑驗證方法，若待查詢的憑證路徑可以成功地建立，就可以確認於該憑證狀態的有效性，已見於先前的中華民國發明專利第 I252662 號「公鑰憑證驗證之高速化方法及裝置」一案中，但是，憑證路徑成功建立，不代表該憑證狀態就是有效的，憑證狀態為廢止之憑證，該憑證的憑證路徑一樣可以被成功地建立。

在公開金鑰基礎建設(Public Key Infrastructure，以下簡稱 PKI)系統應用領域裡，一般憑證狀態驗證流程，是到各個憑證管理中心定期下載憑證廢止清冊(Certificate Revocation List，以下簡稱 CRL)，已見於先前的中華民國發明專利第 I300303 號「付有電子憑證註銷清單發行通知功能之認證基礎系統」一案中，依據 CRL 裡面所記載的憑證序號與憑證廢止原因，與待查詢的憑證序號進行比對，若該憑證序號存在於 CRL 裡面，代表該憑證已被廢止。由於 CRL 檔案為預先簽發，無法保證在這一段時效內，是否有某個憑證的狀態被更新過，且若該憑證狀態為已過期，也不存在於 CRL 檔案裡面，但是該憑證狀態確實是無效的。

現行電子交易系統或者高機密性的資訊系統，都有在使用線上憑證狀態協定(Online Certificate Status Protocol，以下簡稱 OCSP)系統來確認憑

證狀態的正確性，因為 OCSP 系統是提供即時地憑證狀態資訊，且具有憑證管理中心 OCSP 伺服器的簽章保證，但是，現行 OCSP 系統負載能力只符合小型到中型 PKI 系統的應用範疇，若再加上用戶端可攜式設備受限於頻寬的困境，要如何地讓用戶端在有線與無線網路頻寬限制之下，快速且低成本環境之下，使用 OCSP 服務，來驗證電子憑證狀態的有效性，這才是本發明所考量的重點。

由此可見，上述習用技術仍有諸多缺失，實非「憑證狀態查詢」技術的良善之設計者，而亟待加以改良。

【發明內容】

本發明之主要目的，在提供一種提高憑證狀態可信度與資訊安全性之具有高信任度的分散式快速驗證憑證狀態之方法，以有效改善舊有的憑證狀態查詢與驗證方法不足者。

本發明之次要目的，在提供一種可快速取得電子憑證狀態之具有高信任度的分散式快速驗證憑證狀態之方法，使符合線上交易應用系統的理想者。

為達成上述目的，本發明之具有高信任度的分散式快速驗證憑證狀態之方法，係包含下列步驟：

- a、產生異動資訊：由憑證管理中心 (Certification Authority)，簡稱 CA 主機產生憑證狀態異動資訊；
- b、發送：憑證管理中心 CA 主機發送該憑證狀態異動資訊至憑證狀態異動資料庫；
- c、簽發最新訊息：當 OCSP 服務主系統監控憑證狀態異動資料庫，發現

存在有異動資料之後，由 OCSP 服務主系統利用所查詢到的憑證狀態異動資料，與安全簽章保密器之簽章功能，簽發出與這些憑證狀態異動資料相對應的最新 L-OCSPResponses 訊息；

- d、傳送各網域：OCSP 服務主系統透過網際網路上所應用的安全加密通道，分別發送到各個網域負責儲存的 L-OCSP(LightWeight-OCSP System)系統上的資料庫中；
- e、發送請求訊息：OCSP 用戶端透過所指引的 L-OCSP 系統的 OCSP 網址所在，發送 OCSP 請求訊息到該 L-OCSP 系統，進行憑證狀態查詢作業；以及
- f、分析請求訊息：L-OCSP 系統分析所接收到的 OCSP 請求訊息，到本機上的資料庫取得相對應的 OCSP 回應訊息，然後回應傳送給 OCSP 用戶端，以完成具有高信任度的快速憑證狀態查詢之作業。

本發明以 OCSP 協定為基礎，設計出分散式輕量型 OCSP 子系統的架構，以提升應用系統查詢憑證狀態的速度，進而促進後續電子交易的處理效率，且保有原本憑證管理中心 OCSP 系統的簽章證明，證明每一個輕量型 OCSP 子系統回應訊息中，該憑證狀態資訊的可靠性，讓應用系統端不需要花費太多額外的界接與建置成本，又將各個輕量 OCSP 子系統設立在應用系統的區域網路之內，降低網路傳輸影響的不確定因素，讓憑證狀態查詢資訊的回應更加的快速與可信。

如上所述之具有高信任度的分散式快速驗證憑證狀態之方法，該 OCSP 用戶端為符合 OCSP 協定的應用程式或者系統，OCSP 用戶端應用程式將可設置於電腦主機上面或者可攜式的智慧型主機上。

如上所述之具有高信任度的分散式快速驗證憑證狀態之方法，該資訊傳遞的過程係為加入網際網路上應用於資料安全傳輸通道（Secure Sockets Layer，SSL）與傳輸層安全協定（Transport Layer Security，TLS）的安全傳輸通道服務，來提供通信安全及資料的完整性。

如上所述之具有高信任度的分散式快速驗證憑證狀態之方法，該 OCS P 用戶端所發送的憑證查詢請求訊息，與輕型 L-OCSP 子系統所回應的 L-OCSP Response 訊息係為皆符合 OCSP 協定的規範。

如上所述之具有高信任度的分散式快速驗證憑證狀態之方法，該 L-OCSP Response 訊息中的「thisUpdate(產製時間)」與「nextUpdate(下次更新時間)」兩個時間屬性值，係為根據實際執行環境之需要，進行彈性地調整與設定。

如上所述之具有高信任度的分散式快速驗證憑證狀態之方法，該輕型 L-OCSP 子系統係加入授權管理機制，只允許接受與處理特定已被授權的 OCSP 用戶端所發送的憑證狀態查詢請求。

如上所述之具有高信任度的分散式快速驗證憑證狀態之方法，該輕型 L-OCSP 子系統與 OCSP 用戶端係為加入系統校時機制，確認系統互動之間時間的正確性。

如上所述之具有高信任度的分散式快速驗證憑證狀態之方法，該 OCS P 用戶端係為發送 OCSP 請求訊息給予 OCSP 服務主系統，進行高信任度的憑證狀態查詢。

本發明所提供之具有高信任度的分散式快速驗證憑證狀態之方法，與其他習用技術相互比較時，更具有下列之優點：

- 1、利用線上憑證狀態協定(OCSP)與分散式輕量型 OCSP 子系統結合，以提升電子憑證應用系統查詢憑證狀態的效率，也可以加速電子線上交易的安全認證速度，並且提供原本憑證管理中心 OCSP 系統的簽章證明，證明每一個輕量型 OCSP 子系統回應訊息中，該憑證狀態資訊的即時性與可信度。
- 2、與既有的憑證廢止清冊(CRL)相比較，沒有 CRL 所出現的憑證狀態資訊空窗期的情形，同時不需要進行整份 CRL 的分析與查詢，避免遇到 CRL 資料內容過多，導致查詢效率低落的狀況，有效地解決 CRL 所遇到的困境，並提供更快速與準確的憑證狀態查詢的方法。
- 3、PKI 系統已漸達上千萬張以上的憑證簽發，為了提升現行的 OCSP 系統的服務效率，並且降低有線與無線網路頻寬的限制，故本法採用此分散式的輕量型 OCSP 子系統的系統運作架構，來提高電子憑證狀態查詢的可信任性與效率性。
- 4、利用 OCSP 驗證方法為基礎，而電子憑證應用系統端使用既有的 OCSP 應用服務用戶端程式介面，即可以在不需要花費界接與使用成本的情形之下，就可以直接使用本發明，進行高可信任度的憑證狀態查詢，且在本發明執行過程當中，採用預先簽發 OCSP Responses 之方式，電子憑證應用系統端將會享受到更快速的回應效果。
- 5、本發明系統之間的傳輸模式，皆可以結合網際網路上軟硬體模式的資訊安全傳輸方法，可以確實保護本發明內容中系統之間的資訊安全傳輸，以做到高信任度的服務目標。

- 6、本發明具有高信任度的分散式快速驗證憑證狀態之方法，有效地減低網路頻寬的影響因素，係可安全的運用於各式有線與無線網路應用的電子設備（例如：個人上網的電腦，智慧型手機或 PDA 等）上。

【實施方式】

(1)系統主架構

請參圖一，為本發明「具有高信任度的分散式快速驗證憑證狀態之方法」之流程圖，主要包含下列步驟：

- a、產生異動資訊：由憑證管理中心 (Certification Authority, 以下簡稱 CA) 主機產生憑證狀態異動資訊；
- b、發送：憑證管理中心 CA 主機發送該憑證狀態異動資訊至憑證狀態異動資料庫；
- c、簽發最新訊息：當 OCSP 服務主系統監控憑證狀態異動資料庫，發現存在有異動資料之後，由 OCSP 服務主系統利用所查詢到的憑證狀態異動資料，與安全簽章保密器之簽章功能，簽發出與這些憑證狀態異動資料相對應的最新 L-OCSP Responses 訊息；
- d、傳送至各網域：OCSP 服務主系統透過網際網路上所應用的安全加密通道，分別發送到各個網域負責儲存的 L-OCSP(LightWeight-OCSP System)系統上的資料庫中；
- e、發送請求訊息：OCSP 用戶端透過所指引的 L-OCSP 系統的 OCSP 網址所在，發送 OCSP 請求訊息到該 L-OCSP 系統，進行憑證狀態查詢作業；以及
- f、分析請求訊息：L-OCSP 系統分析所接收到的 OCSP 請求訊息，到本

機上的資料庫取得相對應的 OCSPP 回應訊息，然後回應傳送給予 OCSPP 用戶端，以完成具有高信任度的快速憑證狀態查詢之作業。

請參圖二，為本發明之系統架構，主要具有一電子憑證管理中心 1 藉由網際網路 3 與複數個憑證應用區域網路 L11、L12、L13 串連，其中電子憑證管理中心 1 的 CA 主機 11 負責產生憑證狀態異動資訊 12，該憑證狀態異動資訊 12 包含有憑證序號、憑證狀態、發生時間、憑證用戶所屬分類群組、或者自訂欄位內容，CA 主機 11 將憑證狀態異動後的相關資訊，透過安全又穩定的傳輸通道，例如內部防火牆所保護的網路，或者 SSL 安全傳輸通道(網路資料安全傳輸協定，Secure Sockets Layer，以下簡稱 SSL)，即時地儲存到憑證狀態異動資料庫 13 裡面。

由 OCSPP 服務主系統 14 內所使用的常駐系統模組，監控憑證狀態異動資料庫 13 中的資料異動，並藉由 OCSPP 服務主系統 14 上所設置的憑證資料查詢模組，進行憑證資料查詢比對，若查詢到該資料庫資料有所異動，OCSPP 服務主系統 14 將依據該資料庫中的憑證狀態異動資料，使用安全簽章保密器 15 上的電子簽章模組，立即針對這些憑證狀態異動資料，加入電子簽章的保護，以成為已簽章的 L-OCSPP Responses 訊息 16，此 L-OCSPP Responses 訊息 16 必須是符合 OCSPP 協定中所規範的 OCSPP 回應訊息的格式，接著 OCSPP 服務主系統 14 將產製出的 L-OCSPP Responses 訊息 16 儲存在該主機的記錄資料庫裡面。

當 OCSPP 服務主系統 14 處理完成憑證狀態異動資料庫 13 裡面的憑證狀態異動資訊 12 之後，藉由 OCSPP 服務主系統 14 上所設置的憑證資料查詢模組，將這些已處理資料做些註記於憑證狀態異動資料庫 13 中，避免後

續的重複處理，並且新增記錄資料到 OCSP 服務主系統 14 上的記錄資料庫裡面，以做為日後管理查詢與反饋機制所使用。

OCSP 服務主系統 14 將所簽發的 L-OCSP Responses16 封包，依據這些訊息封包的各自所屬 L-OCSP 系統 17(輕量型 OCSP 子系統)之分類，並透過網際網路 3 上所應用的安全加密通道，如 SSL 安全傳輸通道與傳輸層安全協定 (Transport Layer Security, TLS)，或者高安全度的資料庫之間同步機制，分別發送到各個憑證應用區域網域 L11、L12、L13，所負責儲存的 L-OCSP 系統 17 主機上的資料庫裡面，讓 L-OCSP 系統 17 可以將所儲存的 L-OCSP Responses 訊息 16，作為 OCSP 服務的回應訊息，提供標準化的 OCSP 服務，給予 OCSP 用戶端 18 來查詢可信任的憑證狀態。

OCSP 用戶端 18 依據憑證裡面所指引的 L-OCSP 系統 17 的 OCSP 網址所在，或者依據特定指示的 L-OCSP 系統 17 的 OCSP 網址所在，藉由 OCSP 用戶端應用模組，發送 OCSP 請求訊息 M11 到該 L-OCSP 系統 17，進行高可信度的憑證狀態查詢作業。

L-OCSP 系統 17 分析所接收到的 OCSP 請求訊息 M11，利用本機上的資料庫裡面，取得相對應的 OCSP 回應訊息 M12，然後將 OCSP 回應訊息 M12 傳送給予 OCSP 用戶端 18。

OCSP 用戶端 18 收到 L-OCSP 系統所回傳的 OCSP 回應訊息 M12，藉由 OCSP 用戶端應用模組，進行內容分析，並且以 OCSP 服務主系統 14 的電子憑證，進行驗證該 OCSP 回應訊息是否確實為 OCSP 服務主系統 14 所簽發，若驗證無誤，再取得待查詢的憑證狀態，並且驗證 OCSP 回應訊息 M12 內容的訊息時間之設定，是否仍為有效可信賴的時間區間

內；若 OCSP 回應訊息 M12 內容中的 OCSP 服務主系統 14 電子簽章驗證無誤，且 OCSP 回應訊息 M12 內容的時間設定符合可信賴的時間規定之內，即可確認 OCSP 回應訊息 M12 所記載的憑證狀態資訊是可靠信任的。

(2)反饋機制

請參圖三，本發明的反饋機制是處理極少數查詢不到憑證序號的方法，若 OCSP 用戶端 18 所查詢的憑證序號，不存在於 L-OCSP 系統 17 資料庫中，L-OCSP 系統 17 將會依據 OCSP 規範標準產製出 OCSP 回應訊息，該訊息內容中的 OCSP Response Status 屬性值設定為未授權狀態 (unauthorized)，並將由 L-OCSP 系統 17 產製出的 OCSP 回應訊息，回應傳送給 OCSP 用戶端 18，以通知 OCSP 用戶端 18「目前」不提供該待查詢的憑證序號之查詢服務，接著 OCSP 用戶端 18 可以藉由此資訊的表示，瞭解到該憑證序號不是有效的憑證，或者 OCSP 用戶端 18 也可以等待一段時間之後，再來執行 OCSP 查詢服務，因為本反饋機制已經重新準備完成最新的 OCSP 回應訊息給予 OCSP 用戶端 18。

L-OCSP 系統 17 將會由系統上的搜集記錄模組，記錄這些 OCSP 用戶端 18 查詢不到憑證狀態的憑證序號清單，累積一定程度的數量之後，產製出待查詢的憑證序號清單 19，透過安全加密通道，傳送給 OCSP 服務主系統 14。

OCSP 服務主系統 14 依據所接受到的憑證序號清單 19，再由本系統上的憑證資料查詢模組，與憑證狀態異動資料庫系統 13 進行連線，並且進行資料比對查詢，若該憑證序號存在於該資料庫當中，找出正確的憑證狀態資訊，並使用安全簽章保密器 15 之電子簽章模組，立即地簽發出與這些待

查詢的憑證序號相對應新的已簽章 L-OCSP Responses 訊息 20，所產出的 OCSP 回應訊息皆是符合 OCSP 協定規範之格式。若該憑證序號資料不存在於憑證狀態異動資料庫系統 13 裡面，將該憑證狀態設定為「未知狀態 (UnKnown)」，並使用安全簽章保密器 15 之簽章功能，立即地簽發出與這些待查詢的憑證序號相對應新的已簽章 L-OCSP Responses 訊息 20。

當 OCSP 服務主系統 14 處理完成這份憑證序號清單 19 之後，會將這些已處理資料，由系統上的憑證資料查詢模組，做些註記於憑證狀態異動資料庫 13 中，避免後續的重複處理，並且新增記錄資料到 OCSP 服務主系統 14 上的記錄資料庫裡面，以做為日後管理查詢與反饋機制所使用。

OCSP 服務主系統 14 會立即地將所簽發新的已簽章 L-OCSP Responses 20，依據這份憑證序號清單 19 的原本所屬 L-OCSP 系統 17 之資訊，透過網路安全加密通道，如 SSL 通道，或者高安全度的資料庫之間同步機制，發送到原本傳送本憑證序號清單的 L-OCSP 系統 17 主機上的資料庫裡面，讓 L-OCSP 系統 17 可以提供充足憑證狀態查詢的 OCSP 服務，給予 OCSP 用戶 21 再次來查詢可靠的憑證狀態。

(3)主要運作訊息之編碼格式

1、電子憑證的授權驗證資訊屬性之客製化

OCSP 用戶端 18 是可以透過電子憑證內容中的授權資訊存取 (authorityInformationAccess，以下簡稱 AIA) 與憑證廢止清冊發佈點 (cRLDistributionPoints) 兩個屬性值，來判斷 L-OCSP 系統 17 的網址，所以 CA 主機 11 要有能夠依據每個憑證所屬類別或者群組，把以上兩個屬性值設定為憑證本身的所屬於的 L-OCSP 系統 17 網址。另一個彈性解決方案

為強制要求 OCSP 用戶端 18 使用它所屬的 L-OCSP 系統 17 的網址，來進行憑證狀態查詢。

2 、L-OCSP Responses 訊息格式

本發明「具有高信任度的分散式快速驗證憑證狀態之方法」之主要 L-OCSP Response16 訊息格式，是符合 OCSP 協定的規範，L-OCSP 系統 17 回應給予 OCSP 用戶端 18 的訊息，分成兩種主要情形來封裝。

a 、當待查詢的憑證序號存在於 L-OCSP 系統 17 資料庫中，L-OCSP 系統 17 會直接將與該待查詢憑證序號相對應的 L-OCSP Response16 訊息，回送給予 OCSP 用戶端 18，此 L-OCSP Response16 訊息中必須存在有「thisUpdate(產製時間)」與「nextUpdate(下次更新時間)」兩個時間屬性值，前者說明該 L-OCSP Response16 訊息預先簽發 L-OCSP Response16 訊息的時間，後者說明 L-OCSP Response16 訊息的有效使用時間，這兩者屬性值之設定，可以依據本發明方法實際運作環境來設定，盡可能地不可以太長，讓 OCSP 用戶端 18 能夠依據這兩個屬性條件來判斷與驗證 L-OCSP Response16 訊息之時效性。

b 、當待查詢的憑證序號不存在於 L-OCSP 系統 17 資料庫中，L-OCSP 系統 17 本身進行簡單式的 L-OCSP Response 訊息封裝，以 OCSP 協定規範為基礎，將 OCSP 回應訊息封包中的 OCSP ResponseStatus 屬性值，設定為「unauthorized(未授權查詢)」，用來告知 OCSP 用戶端 18 該待查詢的憑證序號 19 是為未被授權查詢的狀態，也就是代表該待查詢的憑證狀態為不可信任的；L-OCSP 系統 17 本身也會將這些無法處理的憑證序號，使用前述的反饋機制來進行處理，以此提供更完全的 OCSP 服務。

(4)資訊的安全傳輸

請再參圖一，本發明的 CA 主機 11 與憑證狀態異動資料庫 13 同在電子憑證管理中心 1 內部，可以透過資料庫管理系統的安全機制，來保護兩者之間的資料傳輸，也可以透過防火牆等網路安全控管硬體設備來保護這兩者的資料傳輸。該 OCSP 服務主系統 14 發佈 L-OCSP Responses¹⁶ 訊息到 L-OCSP 系統 17，可以透過資料安全傳輸通道(SSL)來防止惡意者的攻擊，甚至使用安全加密虛擬企業網路(SSL VPN)更加強傳輸通道的安全，或者使用網路安全控管硬體設備來保護這兩者的資料傳輸，又或者透過 OCSP 服務主系統 14 記錄資料庫與 L-OCSP 系統 17 資料庫之間的安全同步系統，讓 L-OCSP Responses¹⁶ 訊息可以即時又安全地進行傳輸。

上列詳細說明係針對本發明之一可行實施例之具體說明，惟該實施例並非用以限制本發明之專利範圍，凡未脫離本發明技藝精神所為之等效實施或變更，均應包含於本案之專利範圍之中。

綜上所述，本案不但在技術思想上確屬創新，並能較習用物品提升電子憑證應用系統查詢憑證狀態的效率，也可以加速電子線上交易的安全認證速度，並且提供原本憑證管理中心 OCSP 系統的簽章證明，證明每一個輕量型 OCSP 子系統回應訊息中，該憑證狀態資訊的即時性與可信度，與既有的憑證廢止清冊(CRL)相比較，沒有 CRL 所出現的憑證狀態資訊空窗期的情形，且不會需要進行整份 CRL 的分析與查詢，避免遇到 CRL 資料內容過多，導致查詢效率低落的狀況，同時有效地減低網路頻寬的影響因素，並可安全的運用於各式有線與無線網路應用的電子設備，係充分符合新穎性及進步性之法定發明要件，爰依法提出申請。

【圖式簡單說明】

圖一係為本發明實施例之步驟流程圖。

圖二係為本發明實施例之系統架構圖。

圖三係為本發明實施例反饋機制之示意圖。

【主要元件符號說明】

a 產生異動資訊

b 發送

c 簽發最新訊息

d 傳送至各網域

e 發送請求訊息

f 分析請求訊息

1 電子憑證管理中心

11 CA 主機

12 憑證狀態異動資料

13 憑證狀態異動資料庫

14 OCSP 服務主系統

15 安全簽章保密器

16 已簽章的 L-OCSP Responses

17 L-OCSP 系統

18 OCSP 用戶端

19 憑證序號清單

20 新的已簽章的 L-OCSP Responses

M11 OCSP 請求訊息

M12 OCSP 回應訊息

L11 憑證應用區域網路 1

L12 憑證應用區域網路 2

L13 憑證應用區域網路 3

發明專利說明書

(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： 9138438

※申請日： 99.11.09

※IPC 分類：

H04L 9/32 (2006.01)

一、發明名稱：(中文/英文)

具有高信任度的分散式快速驗證憑證狀態之方法

二、中文發明摘要：

一種具有高信任度的分散式快速驗證憑證狀態之方法，係包含下列步驟：a、產生異動資訊；b、發送；c、簽發最新訊息；d、傳送至各個網域；e、用戶端發送請求訊息；以及f、用戶端接收回應訊息；藉此，運用線上憑證狀態協定(Online Certificate Status Protocol，以下簡稱OCSP)為基礎，提供高信任度的訊息驗證保護，再以分散式系統架構來提供更快速的憑證狀態查詢與驗證之服務，以完成具有高信任度的快速憑證狀態查詢之作業。

三、英文發明摘要：

七、申請專利範圍：

- 1、一種具有高信任度的分散式快速驗證憑證狀態之方法，係包含下列步驟：
 - a、產生異動資訊：由憑證管理中心 CA 主機產生憑證狀態異動資訊；
 - b、發送：憑證管理中心 CA 主機以安全、穩定的傳輸通道，發送該產生憑證狀態異動資訊至憑證狀態異動資料庫；
 - c、簽發最新訊息：當 OCSP 服務主系統監控憑證狀態異動資料庫，發現存在有異動資料之後，由 OCSP 服務主系統利用所查詢到的憑證狀態異動資料，與安全簽章保密器之簽章功能，簽發出與這些憑證狀態異動資料相對應的最新 L-OCSPResponses 訊息；
 - d、傳送至各網域：OCSP 服務主系統透過網際網路上所應用的安全加密通道，分別發送到各個網域，所負責儲存的 L-OCSP 系統上的資料庫裡面；
 - e、發送請求訊息：OCSP 用戶端透過所指引的 L-OCSP 系統的 OCSP 網址所在，發送 OCSP 請求訊息，到該 L-OCSP 系統，進行憑證狀態查詢作業；以及
 - f、分析請求訊息：L-OCSP 系統分析所接收到的 OCSP 請求訊息，到本機上的資料庫取得相對應的 OCSP 回應訊息，然後回應傳送給予 OCSP 用戶端，以完成具有高信任度的快速憑證狀態查詢之作業。
- 2、如申請專利範圍第 1 項所述之具有高信任度的分散式快速驗證憑證狀態之方法，其中若 OCSP 用戶端為符合 OCSP 協定的應用程式或者系

統，OCSP 用戶端應用程式將可設置於電腦主機上面或者可攜式的智慧型主機上。

- 3、如申請專利範圍第 1 項所述之具有高信任度的分散式快速驗證憑證狀態之方法，其中資訊傳遞的過程係為加入網際網路上應用於資料安全傳輸通道 (Secure Sockets Layer, SSL) 與傳輸層安全協定 (Transport Layer Security, TLS) 的安全傳輸通道服務，來提供通信安全及資料的完整性。
- 4、如申請專利範圍第 1 項所述之具有高信任度的分散式快速驗證憑證狀態之方法，其中 OCSP 用戶端所發送的憑證查詢請求訊息，與輕型 L-OCSP 子系統所回應的 L-OCSPResponse 訊息係為皆符合 OCSP 協定的規範。
- 5、如申請專利範圍第 1 項所述之具有高信任度的分散式快速驗證憑證狀態之方法，其中 L-OCSPResponse 訊息中的「thisUpdate(產製時間)」與「nextUpdate(下次更新時間)」兩個時間屬性值，係為根據實際執行環境之需要，進行彈性地調整與設定。
- 6、如申請專利範圍第 1 項所述之具有高信任度的分散式快速驗證憑證狀態之方法，其中輕型 L-OCSP 子系統係加入授權管理機制，只允許接受與處理特定已被授權的 OCSP 用戶端所發送的憑證狀態查詢請求。
- 7、如申請專利範圍第 1 項所述之具有高信任度的分散式快速驗證憑證狀態之方法，其中該輕型 L-OCSP 子系統與 OCSP 用戶端係為加入系統校時機制，確認系統互動之間時間的正確性。
- 8、如申請專利範圍第 1 項所述之具有高信任度的分散式快速驗證憑證狀態之方法，其中該輕型 L-OCSP 子系統係加入授權管理機制，只允許接受與處理特定已被授權的 OCSP 用戶端所發送的憑證狀態查詢請求。

態之方法，其中該 OCSP 用戶端係為發送 OCSP 請求訊息給予 OCSP 服務主系統，進行高信任度的憑證狀態查詢。

八、圖式：

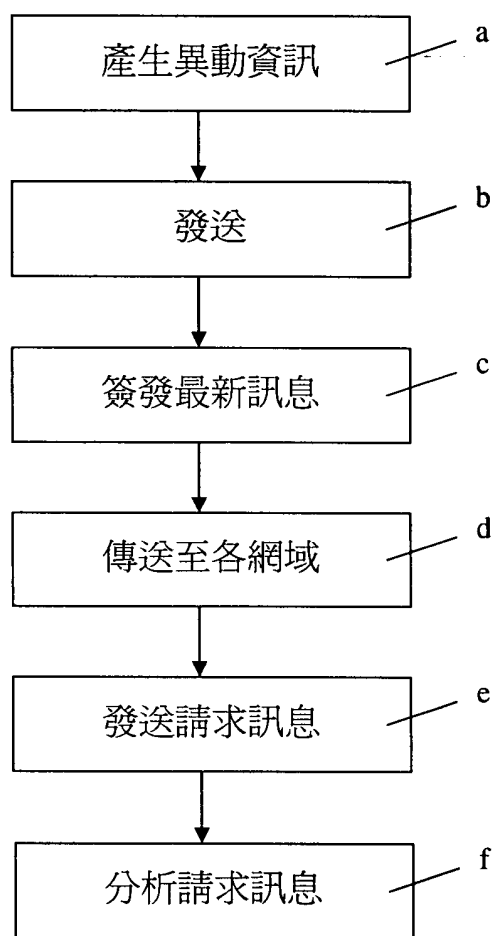


圖 一

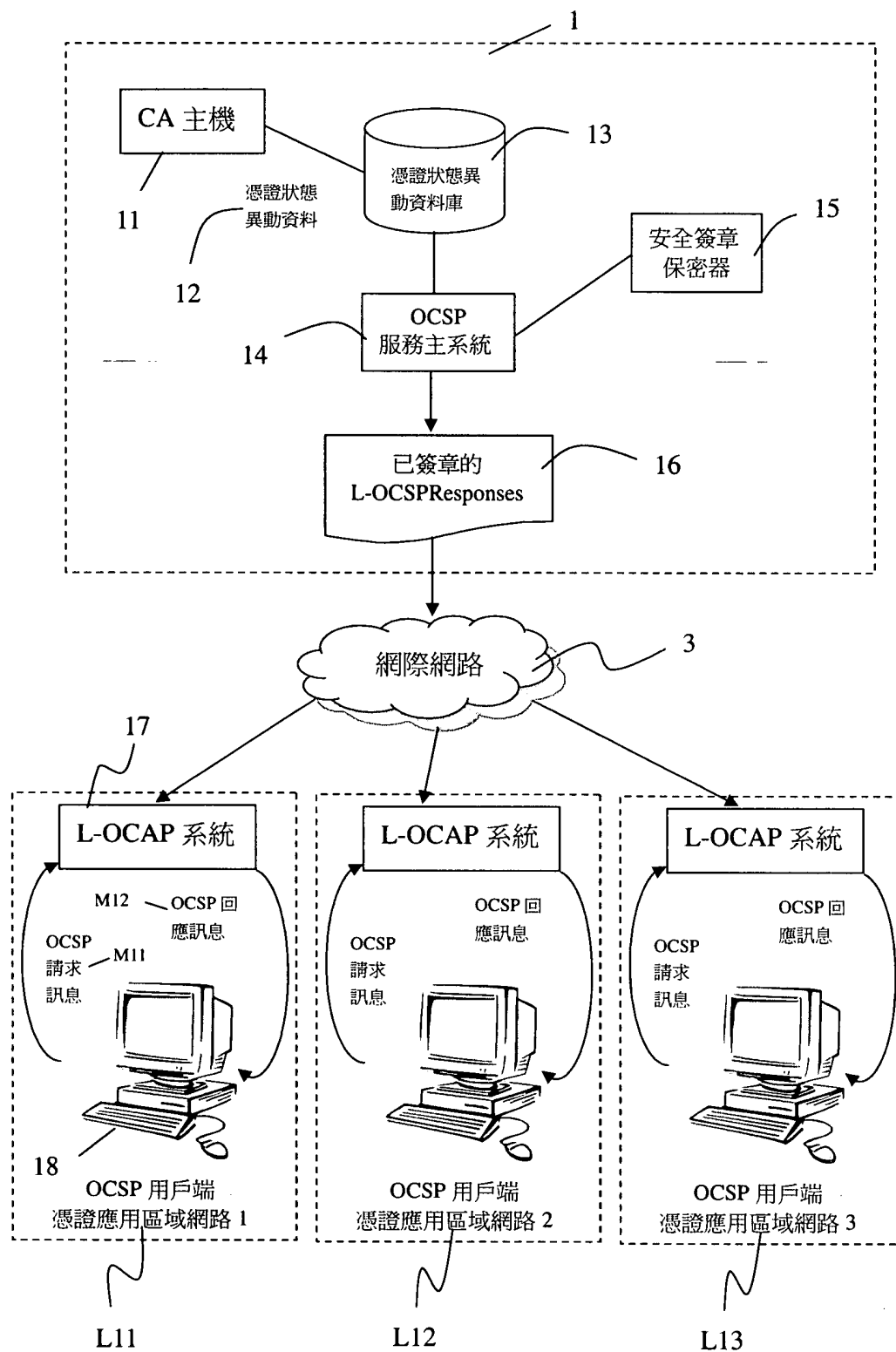


圖 二

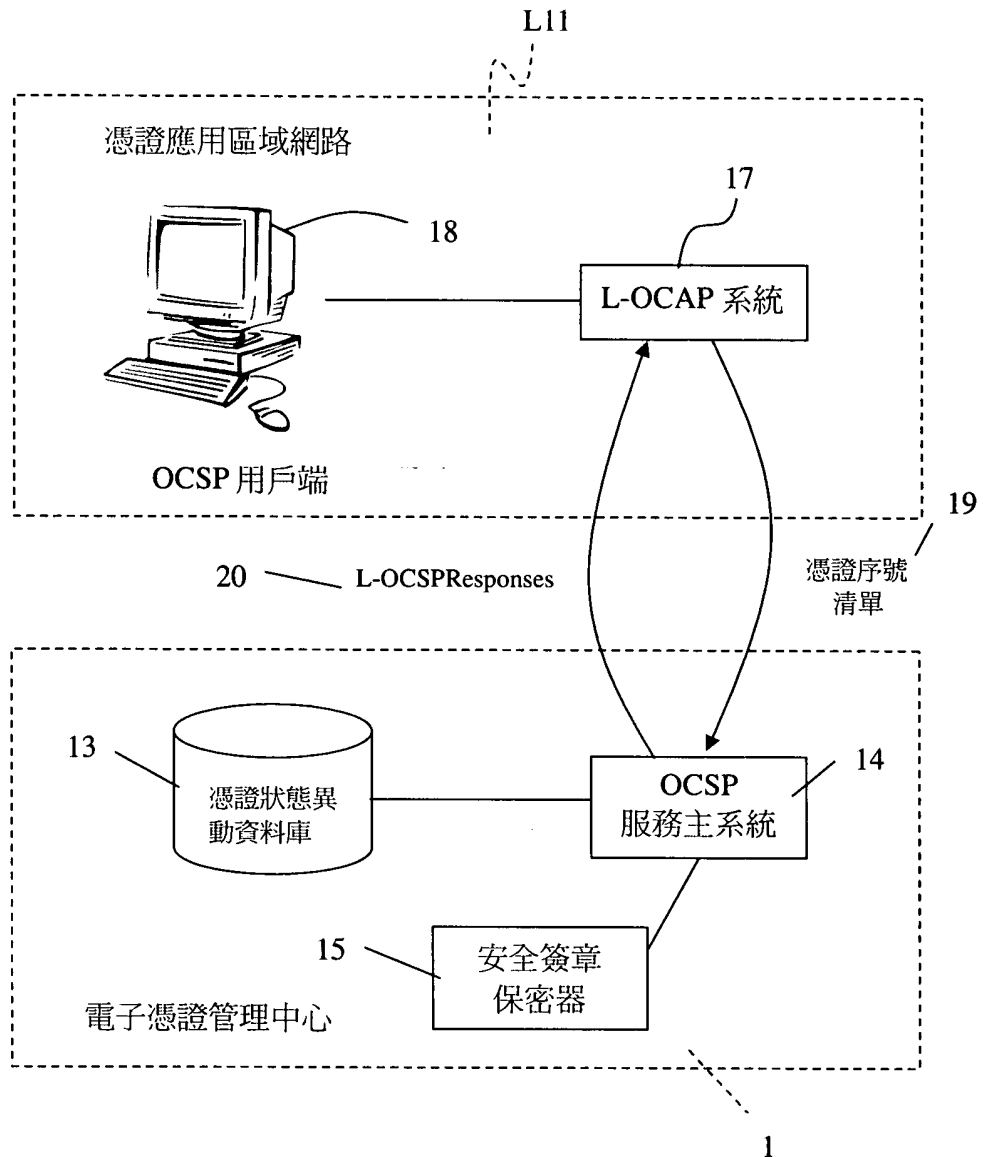


圖 三

四、指定代表圖：

(一)本案指定代表圖為：圖一

(二)本代表圖之元件符號簡單說明：

a 產生異動資訊

b 發送

c 簽發最新訊息

d 傳送至各網域

e 發送請求訊息

f 分析請求訊息

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：