發明專利說明書

97.04.22

（本申請書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫）

※申請案號：92115568
※申請日期：92 年 06 月 09 日　　※IPC 分類：H04L 9/32

一、發明名稱：

(中) 付有電子憑證註銷清單發行通知功能之認證基礎系統
(英) Authentication and authorization infrastructure system with CRL issuance notification function

二、申請人：(共 1 人)

1.姓　名：（中）日立製作所股份有限公司
　　（英）
　代表人：（中）1.庄山悅彥
　　（英）
　地　址：（中）日本國東京都千代田區神田駿河台四丁目六番地
　　（英）
　國籍：（中英）日本　　JAPAN

三、發明人：(共 5 人)

1.姓　名：（中）鍛忠司
　　（英）
　國　籍：（中）日本
　　（英）JAPAN

2.姓　名：（中）藤城孝宏
　　（英）
　國　籍：（中）日本
　　（英）JAPAN

3.姓　名：（中）熊谷洋子
　　（英）
　國　籍：（中）日本
　　（英）JAPAN

4.姓　名：（中）羽根慎吾

（英）
國　籍：（中）日本
（英）JAPAN

5.姓　名：（中）長野裕美
（英）
國　籍：（中）日本
（英）JAPAN

四、聲明事項:

◎本案申請前已向下列國家（地區）申請專利□主張國際優先權：
【格式請依：受理國家（地區）；申請日；申請案號數　順序註記】
1.日本　；2002/06/12；2002-170798 ☑有主張優先權
2.日本　；2003/05/07；2003-128549 ☑有主張優先權

（英）
國　籍：（中）日本
（英）JAPAN

5.姓　名：（中）長野裕美
（英）
國　籍：（中）日本
（英）JAPAN

四、聲明事項:

◎本案申請前已向下列國家（地區）申請專利□主張國際優先權：
【格式請依：受理國家（地區）；申請日；申請案號數　順序註記】
1.日本　；2002/06/12；2002-170798 ☑有主張優先權
2.日本　；2003/05/07；2003-128549 ☑有主張優先權

(1)

玖、發明說明

【發明所屬之技術領域】

本發明係關於，由發行公鑰憑證的失效列表之認證站、和驗證公鑰憑證的有效性之憑證驗證伺服器、和利用上述憑證驗證伺服器之客戶端所成之認證基礎系統。

【先前技術】

起初的政府認證基礎（以下，記以 GPKI），很清楚地決定電子文書的作成者，而且，因爲該電子文書保證無法更改，已利用公鑰認證基礎（Public Key Infrastructure，以下，記以 PKI）的系統得以普及之（例如，參閱非專利文件1）。已利用 PKI 的系統爲，僅保有進行對電子文書、電子簽章的人（以下，記以簽名者），實施了根據所謂的密鍵（Private Key）的電子簽章。於接收已實施了電子簽章的電子文書的場合，驗證上述電子簽章，確認電子文書的作成者與該電子文書不被改造之。

於要求高度的信賴之用途下，爲了進行電子簽章的驗證，包含了上述簽名者的公鑰憑證（以下，記以憑證），根據所謂的公鑰，並不會只有驗證該電子簽章，對驗證上述簽名者的憑證的電子簽章者來說是否爲有效的憑證，是爲有確認的必要。對於驗證上述簽名者的憑證對上述驗證者而言是否爲有效，所謂的（1）認證路徑的構築，和（2）認證路徑的驗證是有其必要之。

所謂的認證路徑，爲自上述驗證者至上述簽名者的信

賴關係鏈，表現了所謂的憑證的鏈。特別是，於認證站之間在未發行相互的憑證的場合，發行所謂的相互認證憑證之特殊的憑證。於自認證站1_1至認證站1_9之9個認證站保持於圖2所示之相互認證的關係的場合，自認證站1_2持有已發行的驗證者至認證站1_1持有已發行的憑證的簽名者的認證路徑係，第1個相互認證憑證9_{18}、第2個相互認證憑證9_{68}、第三個相互認證憑證9_{46}、第4個相互認證憑證9_{24}、直到最後的驗證者的憑證，形成所謂的順序之憑證鏈。驗證此般構築的驗證路徑的方法，於上述非專利文件1中詳細記述之。

且，於上述 GPKI 的規格書，所謂的驗證憑證的有效性的模型，是爲末端 NTT 模型（End NTT Model），於憑證驗證伺服器記載之。（例如，參閱非專利文件2）上述憑證驗證模型係，爲了驗證憑證的有效性，於客戶端提供確認了在線上代換憑證的有效性的功能，利用憑證伺服器。

上述憑證驗證模型係，對照上述末端 NTT 模型，具有以下之優點。首先，上述憑證驗證伺服器模型，因爲構築上述認證路徑之認證路徑的構築功能而實裝到客戶端是不爲必要，故可縮小客戶端的簽章認證程式。而且，客戶端係爲了信賴上述憑證驗證伺服器的判定結果，故只有變更上述憑證驗證伺服器的設定，能柔軟地對應系統構成的變化。根據上述非專利文件2，來判定憑證是否失效，利用上述認證站發行的電子憑證註銷清單（Certificate

(3)

Revocation List，以下，記以 CRL）或線上憑證狀態協定（OCSP Responder）。

因爲自每次進行驗證之上述認證站取得上述 CRL 的效率不好，於專利文件1，經由上述憑證驗證伺服器快取上述憑證或上述 CRL 或上述驗證路徑，揭示有高速化憑證的有效性判斷處理的方式。

且說，爲了驗證電子簽章、或驗證路徑等等，有必要得到簽名者的憑證。得到簽名者的憑證的方法可大致分爲兩類。

一類爲，因爲自簽名者發送附有電子簽章的電子文書，故該簽名者的憑證由別的途徑取得這樣的方法。例如，附有電子簽章的電子文書的同時，爲了驗證該電子簽章的憑證，通知顯示儲存場所的 URL 的方法等等是爲合適。於此方法，上述驗證者係，於上述憑證儲存的場所（以下，記以憑證儲存庫）等存取，有必要取得該憑證。另一類爲，簽名者，於附有電子簽章的電子文書的同時，發送添附了爲了驗證該電子簽章所利用的憑證這樣的方法。

〔專利文件1〕

日本 特開2002-72876號公報

〔非專利文件1〕

ITU, ITU-T Recommendation X.509 “Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks”, ITU, 2000年3月, p.7-53

〔非專利文件2〕

「政府認證基礎（GPKI）政府認證基礎相互運用性規格書」p.18-20, 27-29,[online]、平成13年4月25日、基本問題專門部會了承、[2003年3月14日檢索]、網址<URL:http://www.soumu.go.jp/gyoukan/kanri/010514_2.pdf>

【發明內容】

〔發明欲解決的課題〕

爲了高速化憑證的有效性處理而快取上述CRL，於上述認證站在已緊急地發行上述CRL的場合，快取的上述CRL不爲最新。於專利文件1中此一特點並未言及之。

解決上述課題的方法之一爲，爲了也於上述CRL在已緊急發行的場合有效性驗證得以正確的進行，上述憑證驗證伺服器係，於上述CRL儲存的場所（以下，記以CRL儲存庫裝置）定期地存取，上述CRL爲確認是否不用更新的方法。上述方法係，更進一步地，上述憑證驗證伺服器本身藉由網路進行確認的方式，和於上述CRL儲存庫裝置進行導入確認CRL發行確認軟體的方式這兩種。

上述CRL利用定期地確認是否不用更新的方法，爲了提高上述憑證的有效性驗證結果的精度，可以限制縮短上述確認的間隔是爲必要。但是，上述憑證驗證伺服器本身進行藉由網路確認的方式，縮短上述確認的間隔會增加

網路的負荷這樣的課題。

一方面，於導入爲了於上述 CRL 儲存庫裝置進行確認的 CRL 確認軟體的方式的場合，上述 CRL 儲存庫裝置的營運者和上述憑證驗證伺服器的營運者是爲不同，爲使允許上述 CRL 確認軟體的安裝，不用進行上述確認的場合這樣的課題。

且，在複數的上述憑證驗證伺服器存在的環境，若是全部的上述憑證驗證伺服器不利用導入到上述 CRL 儲存庫裝置的上述 CRL 發行確認軟體，因爲全部的上述憑證驗證伺服器不能進行在相同精度的憑證有效性驗證，於作動的上述憑證驗證伺服器的數目不用增減的場合，變更上述 CRL 發行確認軟體的設定是否爲必要？上述 CRL 儲存庫裝置的營運者和上述憑證驗證伺服器的營運者是爲不同之故，柔軟地變更上述憑證驗證伺服器的數目爲困難的這樣的課題。

更進一步，既使快取上述驗證路徑，根據上述認證站之舊的相互認證憑證也會被破棄，於新的相互認證憑證發行的場合，有必要構築包含新的相互認證憑證的驗證路徑。

且，在存在有複數的上述憑證驗證伺服器的環境，複數的上述憑證驗證伺服器爲，也於已驗證同樣的上述憑證的有效性的場合，爲了各個的上述憑證驗證伺服器進行上述認證路徑的構築、或上述 CRL 的取得等等，集中對特定的上述 CRL 儲存庫裝置或上述憑證儲存庫的存取，會

有網路的負荷便大的可能性。是於專利文件1中未言及之。

且，於由他處取得上述憑證的方法，上述客戶端係，爲了於上述憑證驗證伺服器委託上述憑證的有效性驗證，且，於上述憑證儲存庫不得不存取上述憑證，這樣的課題。

因此，追求解決上述各課題之新的手法。

〔欲解決課題的手段〕

本發明其特徵在於，在由：具備發行上述憑證的憑證發行手段、與發行上述 CRL 的 CRL 發行手段之認證站，和具備儲存上述認證站已發行的上述憑證的憑證儲存手段之憑證儲存庫，和具備儲存上述認證站已發行的上述 CRL 的 CRL 儲存手段之 CRL 儲存庫裝置，和具備驗證上述憑證的有效性的憑證有效性驗證手段、與快取自上述 CRL 儲存庫裝置所取得的上述 CRL 的 CRL 快取手段、與快取爲了讓上述憑證有效性驗證手段驗證上述憑證的有效性而構築的驗證路徑的驗證路徑快取手段之憑證驗證伺服器，和具備有驗證電子簽章之電子簽章驗證手段、與於上述憑證驗證伺服器委託上述憑證的有效性驗證的憑證有效性驗證委託手段之客戶端，所構成的認證基礎系統中；設有，於上述認證站，於已發行上述 CRL 的同時，於上述憑證驗證伺服器發送通知要旨爲「已發行上述 CRL」的 CRL 發行通知之 CRL 發行通知送訊手段；設有，於上述憑證

驗證伺服器，接收自上述認證站的上述 CRL 發行通知之 CRL 發行通知受訊手段。

且，本發明係其特徵爲，上述驗證伺服器的上述 CRL 快取手段爲，藉著上述 CRL 發行通知受訊手段，於已接收上述 CRL 發行通知的場合，把上述認證站已發行新的上述 CRL，自上述 CRL 儲存庫裝置取得。

更進一步，本發明係其特徵爲設有：於上述憑證驗證伺服器，發現到上述 CRL 爲新的已發行的場合，對預先登錄之，其他憑證驗證伺服器，通知要旨爲「已發行上述 CRL」之 CRL 發行通知送訊手段。

且，本發明係其特徵爲，設有：於上述認證站，於藉由上述憑證發行手段已發行上述憑證的場合，於上述憑證驗證伺服器，發送通知要旨爲「已發行憑證」的憑證發行通知之憑證發行通知送訊手段；設有：於上述憑證驗證伺服器，接收上述憑證發行通知之憑證發行通知受訊手段；上述憑證有效性驗證手段係，於上述憑證發行通知受訊手段已接收上述憑證發行通知的場合，以包含新的已發行之上述憑證的方式，作成上述驗證路徑，上述驗證路徑快取手段係快取該驗證路徑。

更進一步，本發明係其特徵爲，設有：於上述憑證驗證伺服器，於已構築上述驗證路徑的場合，發送該驗證路徑於預先登錄之，其他的憑證驗證伺服器之驗證路徑送訊手段；上述驗證路徑快取手段係，於自其他憑證驗證伺服器已接收上述驗證路徑的場合，快取該驗證路徑。

更進一步，本發明係其特徵爲，上述客戶端係，設有：把爲了驗證上述電子簽章之必要的上述憑證的取得，委託到上述憑證驗證伺服器之憑證取得委託手段；於上述憑證驗證伺服器，把自上述客戶端已要求取得的上述憑證，由上述憑證儲存庫取得之，而且，設有：藉著上述憑證驗證手段，於判斷該憑證爲有效的場合，發送該憑證於上述客戶端之憑證取得手段。

更進一步，本發明係其特徵爲，把作成「委託上述 CRL 發行通知」爲旨的訊息的手段設到上述憑證驗證伺服器，把接收上述 CRL 發行通知委託訊息的手段設到上述認證站，更進一步，上述認證站的上述 CRL 發行通知送訊手段係，對於對該認證站能發送上述 CRL 發行通知委託訊息的憑證驗證伺服器，發送上述 CRL 發行通知。

且，本發明係其特徵爲，於已發現於上述 CRL 儲存庫裝置已儲存新的 CRL 的場合，於上述 CRL 儲存庫裝置具備有：發送「已發行上述 CRL」爲旨的 CRL 發行通知之 CRL 發行通知送訊手段、和接收「委託上述 CRL 發行通知」爲旨的 CRL 發行通知委託訊息的 CRL 發行通知委託手段。

且，本發明之 CRL 發行確認軟體係其特徵爲，監視 CRL 的發行，於新的 CRL 的發行的場合，實現發送 CRL 發行通知的手段；實現了接收 CRL 發行通知委託訊息的手段，上述 CRL 發行通知送訊手段係，發送到已接收上述 CRL 發行通知的上述 CRL 發行通知委託訊息的送訊源

。

更進一步，本發明之上述憑證驗證伺服器係其特徵爲設有，接收藉由前述 CRL 發行通知委託作成手段所作成的 CRL 發行通知委託訊息的手段。

【實施方式】

〔發明之實施形態〕

以下，說明圖面所用到本發明之實施形態。且，並不限定本發明於此實施形態。

圖1係，本發明的實施例之附有電子簽章之電子文書交換系統的系統構成圖。委託自認證站1_1至認證站1_9的9個認證站（以下，總括記述爲認證站1）、和憑證儲存庫2、和 CRL 儲存庫裝置3、和自憑證驗證伺服器4_1至憑證驗證伺服器4_n之 n 個憑證驗證伺服器（以下，總括記述爲憑證驗證伺服器4）、到上述憑證驗證伺服器4之憑證有效性的驗證，自客戶終端5_1至客戶終端5_m之 m 個客戶終端（以下，總括記述爲客戶終端5），藉由網路0連接之。

上述認證站1係，於上述客戶終端5發行憑證509，且，該憑證509的拷貝儲存到憑證儲存庫2之憑證發行功能101、和發行已失效的上述憑證509的列表的 CRL7；且，該 CRL7儲存到上述 CRL 儲存庫裝置之 CRL 發行功能102、和 CRL7通知已發行之 CRL 發行通知8、對上述憑證驗證伺服器4發送；具備有，CRL 發行通知功能103、和接收「委託上述 CRL 發行通知8的送訊」爲要旨的 CRL 發行通

知委託訊息10之 CRL 發行通知委託受訊功能105。

且，自認證站1_1至認證站1_9之上述認證站1係，發行相互認證憑證9，如圖2所示之相互認證之關係。

上述憑證儲存庫2係，保持憑證509，憑證資料庫201，和字上述認證站1接收憑證509，且，該憑證509儲存到憑證資料庫201，更進一步，已指定的上述憑證509自上述憑證資料庫201檢索回覆之，和具備有憑證資料庫管理功能202。

上述 CRL 儲存庫裝置3係，保持上述 CRL7，CRL 資料庫301和自上述認證站1接收上述 CRL7，且，該 CRL 儲存到上述 CRL 資料庫301，更進一步，已指定上述 CRL7 自 CRL 資料庫301檢索回覆之，和具備有憑證資料庫管理功能302。

上述憑證驗證伺服器4係具備有，已快取上述 CRL7之 CRL 快取401；和爲了驗證上述憑證509的有效性而使用，已快取驗證路徑的驗證路徑快取402；和接受自上述客戶終端5的要求，自上述憑證儲存庫2取得上述憑證509，且，該憑證509 的有效性根據憑證驗證功能403驗證之，更進一步，於該憑證509爲有效的場合，回覆到上述客戶終端5之憑證取得功能404；和自上述 CRL 儲存庫裝置3取得 CRL7，且，該 CRL7儲存到上述 CRL 快取401之 CRL 管理功能405；和自上述認證站1 接收上述 CRL 發行通知8，且，自上述認證站1接收 CRL 發行通知8的場合，預先登錄之，或，經由發送上述 CRL 發行通知委託訊息10，可

委託 CRL 發行通知8的轉送，於其他的憑證驗證伺服器4轉送 CRL 發行通知8之 CRL 發行通知管理功能406；和上述憑證驗證功能403已作成上述驗證路徑快取上述驗證路徑快取402，且，對預先登錄該驗證路徑之其他的憑證驗證伺服器4發送，更進一步，自其他的憑證驗證伺服器4已接收上述驗證路徑快取到驗證路徑快取402之驗證路徑管理功能407；和對認證站1委託上述 CRL 發行通知8的送訊，作成 CRL 發行通知委託訊息10之 CRL 發行通知委託作成功能410；和自其他的憑證驗證伺服器4接收上述 CRL 發行通知委託訊息10之 CRL 發行通知委託受訊功能411。

上述客戶終端5係具備有，交換其他的客戶終端5和電子文書6之電子文書交換功能501；和於上述電子文書6進行電子簽章，且，自其他的客戶終端5於已接收的電子文書6驗證以簽名之電子簽章之電子簽章功能502；和於上述憑證驗證伺服器4要求上述憑證509有效性的驗證，且，自上述憑證驗證伺服器4接收憑證509有效性驗證的結果之憑證驗證要求功能503；和於上述電子文書6沒有上述憑證509，已顯示了上述憑證509的儲存場所的 URL 於已添附的場合，爲了取得儲存該 URL 之上述憑證509，發送到上述憑證驗證伺服器4的該憑證識別資訊，且，接收自上述憑證驗證伺服器4至憑證509之憑證取得委託功能506；和利用電子簽章功能502之密鑰508；和上述認證站1已發行之憑證509。

尙且，上述客戶終端5_1的上述憑證509_1係，由上述認

證站1_1所發行，上述客戶終端5_2之上述509_2係由認證站1_2所發行。

而且，於本實施例，上述憑證驗證要求功能503和憑證取得委託功能506所利用的上述憑證驗證伺服器4係，自上述憑證驗證伺服器4_1至憑證驗證伺服器4_n之憑證驗證伺服器4之中，預先規定之，來利用特定的上述憑證驗證伺服器4。

例如，客戶終端5_2係利用憑證驗證伺服器4_1。

尙且，於圖1所示之認證站1、憑證儲存庫2、CRL儲存庫裝置3、憑證驗證伺服器4、客戶終端5之各裝置係可實現，例如，如圖9所示般，具備有CPU91、和記憶體92、和硬式磁碟等之外部記憶裝置93、和由具有CD-ROM等之可搬運性的記憶媒體99讀取資訊之讀取裝置94、和藉由網路與其他裝置爲了進行通訊之通訊裝置95、和鍵盤或滑鼠等之輸入裝置96、和螢幕或印表機等之輸出裝置97、和進行於此之各個裝置之間的資料收發之介面98，於一般的電子計算機，經由CPU91執行於記憶體92上已載入所定的程式。

換言之，憑證發行功能101、CRL發行功能102、CRL發行通知功能103、CRL發行通知委託受訊功能105、憑證資料庫管理功能202、CRL資料庫管理功能302、憑證驗證功能403、憑證取得功能404、CRL管理功能405、CRL發行通知管理功能406、驗證路徑管理功能407、CRL發行通知委託作成功能410、CRL發行通知委託受訊功能411、電

子文書交換功能501、電子簽章功能502、憑證驗證要求功能503、憑證取得委託功能504係，根據 CPU91執行所定的程式可實現這樣的處理。又，憑證資料庫201、CRL 資料庫301、CRL 快取401、驗證路徑快取402係，經由 CPU91利用記憶體92或外部記憶裝置93可實現之。

於此般的電子計算機上，爲了實現上述各裝置之所定的程式係，無論藉由讀取裝置94電子計算機自利用可能的記憶媒體99導入也好，或是，輸入裝置96藉由所謂的網路或傳送搬運網路之傳送波，由電子計算機藉由利用可能的通訊媒體之其他的伺服器導入也是可以的。

於導入之際，一旦，無論已儲存到外部記憶裝置93後，自此記憶體92上載入到 CPU91執行也好，或是，不儲存到外部記憶裝置93，直接從記憶體92上載入到 CPU91上執行也是可以的。

其次，於圖1之電子簽章利用系統之動作，上述憑證驗證伺服器4對上述認證站1委託上述 CRL 發行通知8的送訊的場合的動作，使用圖面說明之。

圖7係，於圖1之電子簽章利用系統，上述憑證驗證伺服器4對上述認證站1委託 CRL 發行通知8的送訊的場合，顯示上述憑證驗證伺服器4和認證站1之動作。

於上述憑證驗證伺服器4，上述 CRL 發行通知委託作成功能410，作成上述 CRL 發行通知委託訊息10（步驟7101），發訊到認證站1（步驟7102）。

於圖8（a）所例示，由上述 CRL 發行通知委託訊息

10係，要旨爲「委託 CRL 發行通知8之送訊」的訊息、和與上述 CRL 發行通知8之送訊端成爲網路0上的位址之主機名稱所構成之。

於認證站1，上述 CRL 發行通知委託受訊功能105接收上述 CRL 發行通知委託訊息10（步驟7201），和已發送該 CRL 發行通知委託訊息10，上述憑證驗證伺服器4之主機名稱追加到 CRL 發行通知送訊端列表104（步驟7202）。

於委託自上述憑證驗證伺服器4_1至上述憑證驗證伺服器4_2之上述 CRL 發行通知8之轉送的場合，首先，憑證驗證伺服器4_1之上述 CRL 發行通知委託作成功能410作成 CRL 發行通知委託訊息10，發送到憑證驗證伺服器4_2。

上述憑證驗證伺服器4_2之 CRL 發行通知委託受訊功能411係，接收該 CRL 發行通知委託訊息10，送訊源之上述憑證驗證伺服器4之主機名稱追加到 CRL 發行通知轉送端列表408。

於上述憑證驗證伺服器4對上述認證站1委託 CRL 發行通知8之送訊停止的場合，如圖8(b)所示般，CRL 發行通知委託訊息10發送到認證站1。

圖8（b）之 CRL 發行通知委託訊息10係，由要旨爲「委託上述 CRL 發行通知8的送訊停止」的訊息、和上述 CRL 發行通知8的送訊端的主機名稱所構成。

上述認證站1係，已接收圖8（b）之 CRL 發行通知委託訊息10，記載上述憑證驗證伺服器4之主機名稱由 CRL

發行通知轉送端列表408刪除之。

上述憑證驗證伺服器4於其他的憑證驗證伺服器4委託上述 CRL 發行通知8，於委託轉送停止的場合，於委託端的憑證驗證伺服器4，發送上述 CRL 發行通知委託訊息10。

其次，於圖1之電子簽章系統，上述 CRL7發行的場合，上述認證站1、和上述 CRL 儲存庫裝置3、和上述憑證驗證伺服器4之動作，用以圖面說明之。

圖3係，關於圖1之電子簽章利用系統，顯示於上述CRL7已發行之場合之上述認證站1、和 CRL 儲存庫裝置3、和憑證驗證伺服器4之動作圖。

首先，關於上述認證站1之動作說明之。

上述認證站1係，上述 CRL 發行功能102作成上述CRL7（步驟3101），和該 CRL 發行功能102爲該 CRL7發送到上述 CRL 儲存庫裝置3（步驟3102）。

其次，上述 CRL 發行通知功能103爲，作成 CRL 發行通知8，已預定的、或根據發送到上述 CRL 發行通知委託訊息10已能委託該 CRL 發行通知8之送訊，發送到憑證驗證伺服器4（步驟3103）。

尙且，於本實施例，認證站1係，記載到 CRL 發行通知送訊端列表104之主機名稱，於上述憑證驗證伺服器4發送上述 CRL 發行通知8。

圖6（a）係，上述認證站1管理 CRL 發行通知送訊端列表104之一例，記載上述憑證驗證伺服器4_1之主機名稱

和上述憑證驗證伺服器4_n之主機名稱。

因此，上述認證站1之上述 CRL 發行通知功能103係，於上述憑證驗證伺服器4_1和上述憑證驗證伺服器4_n上發送 CRL 發行通知8。

其次，關於上述 CRL 儲存庫裝置3的動作說明之。

上述 CRL 儲存庫裝置3之上述 CRL 資料庫管理功能302係，上述認證站1、或、等待接受自上述憑證驗證伺服器4之存取，自上述認證站1接收上述 CRL7（步驟3301），和該 CRL7儲存在 CRL 資料庫301（步驟3302），再者，上述認證站1、或、等待接受自上述憑證驗證伺服器4之存取。

一方面，自上述憑證驗證伺服器4，接受如發送上述CRL7般地委託（步驟3033），自上述 CRL 資料庫301檢索該 CRL7（步驟3304），於上述憑證驗證伺服器4發送該CRL7（步驟3305），再者，上述認證站1、或、等待接受自上述憑證驗證伺服器4之存取。

其次，關於上述憑證驗證伺服器4的動作說明之。

於此，根據自上述認證站1接受上述 CRL 發行通知8之上述憑證驗證伺服器4_1之動作，說明上述憑證驗證伺服器4的動作。

首先，於上述憑證驗證伺服器4_1係，上述 CRL 發行通知管理功能406爲，上述認證站1、或、自其他之憑證驗證伺服器4接收 CRL 發行通知8（步驟3401），和首先，調查是否既已接收該 CRL 發行通知8（步驟3402），於既

已接收CRL發行通知8的場合，結束這樣的處理。

一方面，於最初接收上述CRL發行通知8的場合，上述CRL管理功能405爲，存取到上述CRL儲存庫裝置3（步驟3403），取得上述CRL7（步驟3404），快取上述CRL快取401（步驟3405）。

其次，上述CRL發行通知管理功能406係，已預先登錄，或，根據發送上述CRL發行通知委託訊息10已委託該CRL發行通知8的轉送，於其他的憑證驗證伺服器4轉送上述CRL發行通知8（步驟3406）。

上述憑證驗證伺服器4係，利用所謂的CRL發行通知轉送端列表408的列表，轉送上述CRL發行通知8，管理上述憑證驗證伺服器4。

圖6（b）係，上述憑證驗證伺服器4_1管理上述CRL發行通知轉送端列表408之一例，記載上述憑證驗證伺服器4_2之主機名稱、和上述憑證驗證伺服器4_3之主機名稱、和上述憑證驗證伺服器4_n之主機名稱。

因此，上述CRL發行通知管理功能406係，轉送上述CRL發行通知8到憑證驗證伺服器4_2、和憑證驗證伺服器4_3、和憑證驗證伺服器4_n。

尙且，於本實施例，自上述憑證驗證伺服器4_1至憑證驗證伺服器4_n之各個主機名稱係，自上述憑證驗證伺服器4_1至憑證驗證伺服器4_n之憑證驗證伺服器4各自保持之，上述CRL發行通知轉送端列表408之任一個必須記載之。

根據如此，任一之上述憑證驗證伺服器4爲自上述認

證站1接受取得上述 CRL 發行通知8，自上述憑證驗證伺服器4_1至憑證驗證伺服器4_n之全部的憑證驗證伺服器4爲可以接受取得上述 CRL 發行通知8。

而且，追加新的憑證驗證伺服器4的場合，上述憑證驗證伺服器4_1至上述憑證驗證伺服器4_n之憑證驗證伺服器4爲各自保持之，追加上述 CRL 發行通知轉送端列表408之任一個該憑證驗證伺服器4的主機名稱，成爲不必要變更上述 CRL 發行通知送訊端列表104。

以上，上述 CRL7已發行的場合之圖1之電子簽章利用系統之動作。

其次，於附有電子簽章之電子文書交換系統，自上述客戶終端5_1，於上述客戶終端5_2，於發送上述電子文書6的場合，用以圖面說明之。

尙且，於本實施例，爲了於上述電子文書6驗證已施予之電子簽章之上述憑證509係，於上述電子文書6添附的場合、和於上述電子文書6未添附的場合之這兩種場合，首先，爲了於上述電子文書6驗證已施予之電子簽章之上述憑證509，於上述電子文書6添附的場合說明之。

圖4係，於附有電子簽章之電子文書交換系統，爲了於上述電子文書6驗證已施予之電子簽章之上述憑證509，於上述電子文書6添附的場合，自上述客戶終端5_1，顯示於上述客戶終端5_2，發送上述電子文書6之際，上述客戶終端5_1、和上述客戶終端5_2、和上述憑證驗證伺服器4_1、和上述憑證驗證伺服器4_2之動作圖。

首先，關於上述客戶終端5_1之動作說明之。

上述客戶終端5_1係，上述電子文書交換功能501，於上述客戶終端5_2發送，作成上述電子文書6（步驟4051）；上述電子簽章功能502，使用上述密鑰508_1，於該電子文書6施予電子簽章（步驟4052）。

其次，上述電子文書交換功能501係，已施予電子簽章，上述電子文書6，與憑證509_1一同地，於上述客戶終端5發送之（步驟4503）。

其次，關於上述客戶終端5_2之動作說明之。

上述客戶終端5_2係，爲了驗證接收上述電子文書6（步驟4511），與上述電子文書6一同地能已發送上述憑證509_1之有效性，上述憑證驗證要求功能503，於上述憑證驗證伺服器4_1，委託該憑證509_1之有效性驗證（步驟4512），自上述憑證驗證伺服器4_1接收有效性驗證的結果（步驟4513）。

於此，上述有效性驗證的結果，上述憑證509_1係，對於上述客戶終端5_2來說不爲有效，於這樣的場合，結束處理。

一方面，上述有效性驗證的結果，上述憑證509_1係，對於上述客戶終端5_2來說是爲有效，於這樣的場合，上述憑證驗證要求功能503係，自上述憑證509_1取出公鑰，驗證於上述電子文書6所施予的電子簽章（步驟4515）。於此，上述電子簽章於已判定爲不正確的場合結束處理。

一方面，於上述電子簽章判定爲正確的場合，保存上

述電子文書6（步驟4516）。

其次，關於上述憑證驗證伺服器4之動作說明之。

首先，上述憑證驗證伺服器4_1係，自上述客戶終端5_2委託上述憑證509_1之有效性驗證（步驟4401），和上述憑證驗證功能403，自上述客戶終端5_2至上述客戶終端5_1之驗證路徑，確認是否保存於上述驗證路徑快取402（步驟4402）。

於此，於上述驗證路徑快取402，於該驗證路徑存在的場合，進行到步驟4404。一方面，於上述驗證路徑快取402，該驗證路徑已不存在之場合，構築該驗證路徑（步驟4403），進行到步驟4404。

於步驟4404，上述憑證驗證功能403係，自上述 CRL 快取401取出 CRL7，判定上述驗證路徑是否有效。其次，發送判定結果至上述客戶終端5_2（步驟4405）。

於此，上述驗證路徑，於在步驟4403並未已重新構築的場合，結束處理。一方面，於在步驟4403已重新構築的場合，於驗證路徑送訊端列表409之主機名稱記載之，於上述憑證驗證伺服器4發送該驗證路徑（步驟4407），結束處理。

上述驗證路徑送訊端列表409係，發送已重新構築之上述驗證路徑，已記載上述憑證驗證伺服器4支主機名稱的列表；於本實施例，上述 CRL 發行通知轉送端列表408利用上述驗證路徑送訊端列表409。

因此，於步驟4407，上述驗證路徑係，發送到上述憑

證驗證伺服器4_2、和上述憑證驗證伺服器4_3和上述憑證驗證伺服器4_n。

尚且，於本實施例，是否於上述 CRL 發行通知轉送端列表408和上述驗證路徑送訊端列表409使用同樣的列表，本發明於此並未限定，以利用各個不同的列表爲較佳。

一方面，上述憑證驗證伺服器4_2、或上述憑證驗證伺服器4_3、或上述憑證驗證伺服器4_n係，自上述憑證驗證伺服器4_1接收上述驗證路徑（步驟4411），和上述驗證路徑管理功能407係確認該驗證路徑是否於驗證路徑快取402快取之（步驟4412）。

於此，於上述驗證路徑快取402，上述驗證路徑若被快取之，則不做任何動作，結束處理。一方面，於驗證路徑快取402，上述驗證路徑若不被快取之，該驗證路徑於驗證路徑快取402快取之（步驟4413），於驗證路徑送訊端列表409記載主機名稱，於上述憑證驗證伺服器4發送該驗證路徑（步驟4414），結束處理。

尚且，在本實施例，上述憑證驗證伺服器4之上述驗證路徑管理功能407係，是否反覆收發、快取驗證路徑這樣的作法，本發明並未限定之，反覆收發能專心地識別上述驗證路徑這樣的驗證路徑資訊、反覆快取之，在必要的時候構成自該驗證路徑資訊對應之驗證路徑是爲較佳。

以上爲，於爲了驗證於上述電子文書6已施予電子簽章之上述憑證509於上述電子文書6所添附的場合的，自上述客戶終端5_1於上述客戶終端5_2發送電子文書6之際的，

圖1的附有電子簽章之電子文書交換系統的動作。

其次，關於爲了驗證於上述電子文書6已施予電子簽章之上述憑證509，於上述電子文書6爲添附的場合的，自上述客戶終端5_1於上述客戶終端5_2發送上述電子文書6之際的，圖1之附有電子簽章之電子文書交換系統的動作，用以圖面說明之。

圖5係已顯示，於圖1之附有電子簽章之電子文書交換系統，爲了驗證於上述電子文書6已施予的電子簽章之上述憑證509爲，於上述電子文書6並未添附的場合，自上述客戶終端5_1於上述客戶終端5_2發送上述電子文書6之際的，上述客戶終端5_1、和上述客戶終端5_2和上述憑證驗證伺服器4、和上述憑證儲存庫2之動作圖。

首先，關於上述客戶終端5_1之動作說明之。

上述客戶終端5_1係，上述電子文書交換功能501，於上述客戶終端5_2發送，作成上述電子文書6（步驟5501），和上述電子簽章功能502，使用上述密鑰5081，於該電子文書6施予電子簽名（步驟5502）。

其次，上述電子文書交換功能501係，已施予電子簽名，上述電子文書6，與顯示上述憑證509_1之儲存場所之URL一同地，於上述客戶終端5_2發送（步驟5503）。

尙且，於本實施例，與上述電子文書6一同地，是否發送已顯示上述憑證509的儲存場所的 URL，於本發明並未限定之，發送於上述憑證509所記載之資訊的一部份是爲較佳。

其次，關於上述客戶終端5_2之動作說明之。

上述客戶終端52係，接收上述電子文書6（步驟5511），和上述憑證取得委託功能504，與上述電子文書6一同地已發送上述 URL 所對應的上述憑證509_1，於上述憑證驗證伺服器4_1取得委託（步驟5512），自上述憑證驗證伺服器4_1接收委託結果（步驟5513）。

於此，於上述委託結果上述憑證509_1已未包含的場合，換言之，上述 URL 所顯示上述憑證509_1於上述客戶終端5_2不爲有效，和於上述憑證驗證伺服器4_1已判斷的場合，處理結束。一方面，於上述委託結果已包含上述憑證509_1的場合，上述憑證驗證要求功能503係，自上述憑證509_1取出公鑰，驗證於上述電子文書6施予電子簽章（步驟5515）。於此，於上述電子簽章判斷不爲正確的場合，結束處理。一方面，於上述電子簽章判斷爲正確的場合，保存上述電子文書6（步驟5516），結束處理。

其次，關於上述憑證驗證伺服器4之動作說明之。

上述憑證驗證伺服器4_1之上述憑證取得功能404係，自上述客戶終端5_2，接受取得上述憑證509_1的委託（步驟5401），使用自上述客戶終端5_2已發送的上述 URL，於上述憑證儲存庫2存取之（步驟5402），取得上述憑證509_1（步驟5403）。

其次，根據上述憑證驗證功能403，上述憑證509_1，於上述客戶終端5_2，判定是否爲有效的憑證（步驟5404）。

於此，於上述憑證驗證功能403的動作係，與自圖4之步驟4402至步驟4409的動作相同，省略說明之。

根據上述判定，上述憑證509_1，對上述客戶終端5_2而言，判斷是爲有效的憑證的場合，作成包含該憑證509_1之委託結果，發送到上述客戶終端5_2（步驟5407）。一方面，上述憑證509_1，對於上述客戶終端5_2而言，判斷不爲有效的憑證的場合，作成顯示要旨爲「不爲有效」的委託結果（步驟5406），發送到上述客戶終端5_2（步驟5407）。

其次，關於上述憑證儲存庫2之動作說明之。

上述憑證儲存庫2之上述憑證資料庫管理功能202係，自上述憑證驗證伺服器4_1，接受發送上述憑證509_1的委託（步驟5201），和自憑證資料庫201檢索該憑證509_1（步驟5202）於上述憑證驗證伺服器4發送該憑證509_1（步驟5203）。

以上，爲了驗證於上述電子文書6已施予的電子簽章之上述憑證509於電子文書6爲添附的場合的，自上述客戶終端5_1於上述客戶終端5_2發送上述電子文書6之際的圖1的附有電子簽章之電子文書交換系統的動作。

於此，於本實施例的附有電子簽章的電子文書交換系統，上述認證站1發行上述 CRL7之際，上述 CRL 發行通知8，記載上述 CRL 發行通知送訊端列表104，於上述憑證驗證伺服器4發送之，已發行的上述 CRL7於憑證驗證伺服器4通知，且，已接收上述 CRL 發行通知8的上述憑證驗證伺服器4係，自上述 CRL 儲存庫裝置3取得上述 CRL7

，快取之。

爲此，也於上述認證站1緊急地發行上述 CRL7的場合，爲了上述憑證驗證伺服器4快取的 CRL 爲最新，能保證上述憑證509的有效性檢驗結果的精度。

而且，於本實施例的附有電子簽章的電子文書交換系統，接收上述 CRL 發行通知8之上述憑證驗證伺服器4係，於上述 CRL 發行通知轉送端列表408記載主機名稱，於其他的憑證驗證伺服器4，轉送該 CRL 發行通知8。

爲此，也於追加新的憑證驗證伺服器4的場合，於上述憑證驗證伺服器4的上述 CRL 發行通知轉送端列表408，只要記載新的憑證驗證伺服器4的主機名稱，成爲可接收上述 CRL 發行通知8，上述認證站1側的設定沒有必要變更。

而且，於本實施例的附有電子簽章的電子文書交換系統，上述憑證驗證伺服器4，於自其他的憑證驗證伺服器4接收上述驗證路徑的場合，快取該驗證路徑，而且，於上述憑證驗證伺服器4已構築新的驗證路徑的場合，於上述驗證路徑送訊端列表409記載主機名稱，於其他的憑證驗證伺服器4，發送該新的驗證路徑。

爲此，在憑證驗證伺服器4之間爲了能共有驗證路徑，至上述憑證儲存庫2或上述 CRL 儲存庫裝置3的存取集中之，可防止網路的負荷增大。

更進一步，於本實施例的附有電子簽章的電子文書交換系統，上述客戶終端5，於接收已顯示上述憑證509的儲

存場所的 URL 的場合，於上述憑證儲存庫2不存取之，於上述憑證驗證伺服器4上委託憑證509的取得，且，上述憑證驗證伺服器4係，自上述憑證儲存庫2已取得上述憑證509，爲了對於上述客戶終端5而言爲有效憑證的場合，上述憑證509回覆上述客戶終端5。

爲此，於上述客戶終端5係，實裝於上述憑證儲存庫2存取的功能是沒有必要的。

尙且，於本實施例，於上述 CRL 發行通知8，是否爲了記載「CRL 已發行的主旨」的通知，於本發明並未限定之。

例如，於上述 CRL 發行通知8，包含了新發行的上述CRL7本身，或者，和以前已發行的 CRL7，和新發行的CRL7之，包含了差分資訊是爲較佳。更進一步，包含了新的已失效的憑證509的識別資訊之一覽爲較佳。

於上述 CRL 發行通知8，新發行的上述 CRL7本身，或以前發行的…和新發行的 CRL7之差分資訊，經由包含了新的失效憑證509的識別資訊的一覽，已接收該 CRL 發行通知8的上述憑證驗證伺服器4係，可更省力的取得於上述 CRL 儲存庫裝置3存取新的已發行的 CRL7的處理。

而且，於本實施例，上述 CRL 發行通知8的送訊，或上述 CRL 發行通知委託訊息10的收訊係，上述認證站1進行之，本發明於此部爲限定之。例如，上述 CRL 發行通知8的送訊，或上述 CRL 發行通知委託訊息10的收訊由上述 CRL 儲存庫裝置3進行爲較佳。

或者，於 CRL 儲存庫裝置3，監視上述 CRL7的發行，於新的 CRL7已發行確認的場合，導入實現發送上述 CRL 發行通知8的功能之 CRL 發行確認軟體，更進一步，該 CRL 發行確認軟體係，實現上述 CRL 發行通知委託受訊功能，上述 CRL 發行通知委託受訊功能係，於已接收上述 CRL 發行通知委託訊息的送訊源，發送上述 CRL 發行通知是爲較佳。

利用了上述 CRL 發行確認軟體，成爲未持有上述 CRL 發行通知送訊功能之上述認證站1或上述 CRL 儲存庫裝置3也可利用之。更進一步，上述 CRL 發行通知委託受訊功能爲管理上述 CRL 發行通知的送訊端，上述 CRL 儲存庫裝置的營運者和上述憑證驗證伺服器的營運者也爲不同的上述憑證驗證伺服器的數目可以柔軟地變更。

經由本實施例，上述 CRL 發行通知係上述認證站發行上述 CRL 之時，爲了自該認證站能僅對上述憑證驗證伺服器進行，每隔一定的時間上述 CRL 發行的確認是爲不必要，網路0所承擔的負荷可變小。

且，上述 CRL 發行通知8係爲了根據上述認證站1而進行，也於上述 CRL 儲存庫裝置3，和上述憑證驗證伺服器4的營運者不同之場合，可進行高精度的憑證有效性的驗證。

更進一步 K 上述憑證驗證伺服器4係，爲了能經由發送上述 CRL 發行通知委託訊息10委託上述 CRL 發行通知8的送訊，上述 CRL 儲存庫裝置3的營運者與上述憑證驗證

伺服器4的營運者也爲不同之憑證驗證伺服器4的數目可柔軟地變更。

更進一步，上述憑證驗證伺服器爲發現新的 CRL 已發行的場合，該憑證驗證伺服器與其他的憑證驗證伺服器通知發行新的上述 CRL。

於發送上述憑證驗證伺服器未變更的場合，爲了變更該憑證驗證伺服器的設定，上述 CRL 儲存庫裝置的營運者和上述憑證驗證伺服器的營運者爲不同的上述憑證驗證伺服器的數目可柔軟地變更。

更進一步，上述憑證驗證伺服器爲，於構築信的驗證路徑的場合，該驗證路徑轉送也爲其他的憑證驗證伺服器，爲了共有驗證路徑，特定的上述 CRL 儲存庫裝置或上述憑證儲存庫之存取集中，可抑制網路的負荷。

而且，也於利用別的途徑入手上述憑證的場合，上述客戶端係，不爲取得於上述憑證儲存庫存取上述憑證，於上述憑證驗證伺服器，取得上述憑證，且，爲了委託驗證該憑證的有效性，於客戶端，實裝取得於上述憑證儲存庫存取上述憑證不爲必要之。

〔發明的效果〕

因此，經由本發明，可確實地進行上述憑證的有效性驗證爲高精度低負荷。

【圖式簡單說明】

【圖1】顯示適用本發明之實施形態，附有電子簽章之電子文書交換系統的系統構成圖。

【圖2】顯示於圖1之附有電子簽章之電子文書交換系統，認證站1之間的相互認證的關係圖。

【圖3】顯示於圖1之附有電子簽章之電子文書交換系統，CRL7已發行的場合的動作圖。

【圖4】顯示於圖1之附有電子簽章之電子文書交換系統，於憑證509與電子文書同時的發送的場合，客戶終端5收發電子文書6之際的動作圖。

【圖5】顯示於圖1之附有電子簽章之電子文書交換系統，於憑證509與電子文書同時的發送的場合，客戶終端5收發電子文書6之際的動作圖。

【圖6】顯示 CRL 發行通知送訊端列表104和 CRL 發行通知轉送端列表408之一例圖。

【圖7】顯示於圖1之附有電子簽章之電子文書交換系統，憑證驗證伺服器4對認證站1委託 CRL 發行通知8的送訊的場合的動作圖。

【圖8】顯示 CRL 發行通知委託訊息10之一例圖。

【圖9】顯示於圖1所示之認證站1、憑證儲存庫2、CRL 儲存庫裝置3、憑證驗證伺服器4、客戶終端5之各個硬體構成例圖。

[圖號說明]

0　　網路

(30)

1、1_1～1_9	認證站
2	憑證儲存庫
3	CRL 儲存庫裝置
4、4_1～4_n	憑證驗證伺服器
5、5_1～5_m	客戶終端
6	電子文書
7	電子憑證註銷清單
8	CRL 發行通知
9	相互認證憑證
10	CRL 發行通知委託訊息
91	中央處理器
92	記憶體
93	外部記憶裝置
94	讀取裝置
95	通訊裝置
96	輸入裝置
97	輸出裝置
98	介面
99	記憶媒體
104	CRL 發行通知送訊端列表
408	CRL 發行通知轉送端列表
409	驗證路徑送訊端列表
508、508_1～508_m	密鑰
509、509_1～509_m	憑證

伍、中文發明摘要

發明之名稱：付有電子憑證註銷清單發行通知功能之認證基礎系統

〔課題〕

爲了高速化憑證的有效性判定處理而快取 CRL 的話，於認證站已緊急地發行 CRL 的場合，因爲快取的前述 CRL 不是最新的，故不能保證憑證的有效性驗證結果的精度。

〔解決手段〕

於前述 CRL 已發行的場合，自前述認證站進行對前述憑證驗證伺服器的 CRL 發行通知，而且，因爲已接收之該 CRL 發行通知的前述憑證驗證伺服器係快取了最新的前述 CRL，故可保證憑證有效性驗證結果的精度。

陸、英文發明摘要

發明之名稱：

(1)

拾、申請專利範圍

1.一種認證基礎系統，其特徵為：

具備有：具備發行憑證的憑證發行手段與發行 CRL 的 CRL（電子憑證註銷清單 Certificate Revocation List）發行手段之認證站，和具備儲存前述認證站已發行的前述 CRL 的 CRL 儲存手段之 CRL 儲存庫裝置，和具備驗證前述憑證的有效性的憑證有效性驗證手段、與快取自前述 CRL 儲存庫裝置取得的前述 CRL 的 CRL 快取手段之憑證驗證伺服器；

前述認證站係具備有，於已發行前述 CRL 的場合，把通知要旨為「已發行 CRL」的 CRL 發行通知，發送於前述憑證驗證伺服器的 CRL 發行通知送訊手段；

前述憑證驗證伺服器係具備有，自前述認證站接收前述 CRL 發行通知之 CRL 發行通知受訊手段。

2.如申請專利範圍第1項所記載之認證基礎系統，其中：

前述憑證驗證伺服器之前述 CRL 快取手段係，於藉著前述 CRL 發行通知受訊手段接收前述 CRL 發行通知的場合，前述認證站自前述 CRL 儲存庫裝置取得新的已發行的前述 CRL。

3.如申請專利範圍第1項所記載之認證基礎系統，其中：

前述憑證驗證伺服器係具備有，於發現到前述 CRL 新的已發行的場合，對預先登錄的其他憑證驗證伺服器，

(2)

通知要旨爲「已發行 CRL」的 CRL 發行通知送訊手段。

4.如申請專利範圍第2項所記載之認證基礎系統，其中：

前述憑證驗證伺服器係具備有，於發現到前述 CRL 新的已發行的場合，對預先登錄的其他憑證驗證伺服器，通知要旨爲「已發行 CRL」的 CRL 發行通知送訊手段。

5.如申請專利範圍第1項所記載之認證基礎系統，其中：

前述憑證驗證伺服器係具備有，作成 CRL 發行通知委託訊息之 CRL 發行通知委託手段；

前述認證站係具備有，接收前述 CRL 發行通知委託訊息之 CRL 發行通知委託受訊手段；

前述認證站的前述 CRL 發行通知送訊手段係，針對對該認證站發送前述 CRL 發行通知委託訊息的憑證驗證伺服器，發送前述 CRL 發行通知。

6.如申請專利範圍第5項所記載之認證基礎系統，其中：

前述憑證驗證伺服器係具備有：

自其他憑證驗證伺服器接收前述 CRL 發行通知委託訊息之 CRL 發行通知委託受訊手段；

和於已接收前述 CRL 發行通知的場合，對已能發送前述 CRL 發行通知委託訊息的憑證驗證伺服器，轉送前述 CRL 發行通知之 CRL 發行通知管理手段。

7.一種認證基礎系統，其特徵爲：

(3)

具備有：具備驗證憑證有效性的憑證有效性驗證手段、與快取爲了讓該憑證有效性驗證手段驗證前述憑證的有效性所構築的驗證路徑的驗證路徑快取手段之憑證驗證伺服器；和具備驗證電子簽章之電子簽章驗證手段、與於前述憑證驗證伺服器委託前述憑證的有效性驗證的憑證有效性驗證委託手段之客戶端；

前述憑證驗證伺服器係具備有，於已構築前述驗證路徑的場合，發送該驗證路徑於已預先登錄的其他憑證驗證伺服器之驗證路徑送訊手段；

前述驗證路徑快取手段係，於自其他憑證驗證伺服器接收前述驗證路徑的場合，快取該驗證路徑。

8.一種認證基礎系統，其特徵爲：

具備有：具備發行憑證的憑證發行手段之認證站；和具備儲存前述認證站已發行的前述憑證的憑證儲存手段之憑證儲存庫；和具備驗證前述憑證的有效性的憑證有效性驗證手段之憑證驗證伺服器；和具備驗證電子簽章之電子簽章驗證手段、與於前述憑證驗證伺服器委託前述憑證的有效性的憑證有效性驗證委託手段之客戶端；

前述客戶端係具備有，把爲了驗證前述電子簽章之必要的前述憑證的取得，委託到前述憑證驗證伺服器之憑證取得委託手段；

前述憑證驗證伺服器係具備有，把自前述客戶端已被要求取得的前述憑證，自前述憑證儲存庫來取得，而且，藉著前述憑證驗證手段，於該憑證判定爲有效的場合，發

送該憑證於前述客戶端之憑證取得手段。

9.一種認證站，其特徵爲：

具備有，發行憑證之憑證發行手段，和發行 CRL 之 CRL 發行手段；

具備有，於發行前述 CRL 的同時，於前述憑證驗證伺服器發送通知要旨爲「已發行 CRL」的 CRL 發行通知之 CRL 發行送訊通知手段。

10.如申請專利範圍第9項所記載之認證站，其中：

具備有接收 CRL 發行通知委託訊息之 CRL 發行通知委託受訊手段；

前述 CRL 發行通知送訊手段係，把前述 CRL 發行通知，發送到已接收的前述 CRL 發行通知委託訊息的送訊源。

11.一種憑證驗證伺服器，其特徵爲：

具備有，驗證憑證的有效性之憑證有效性驗證手段，和快取 CRL 之 CRL 快取手段；

具備有，接收通知 CRL 已發行的 CRL 發行通知之 CRL 發行通知受訊手段。

12.如申請專利範圍第11項所記載之憑證認證伺服器，其中：

前述憑證驗證伺服器的 CRL 快取手段係，藉由前述 CRL 發行通知受訊手段，於已接收前述 CRL 發行通知的場合，取得新的已發行的前述 CRL。

13.如申請專利範圍第11項所記載之憑證認證伺服器

(5)

，其中：

具備有，於發現到前述 CRL 爲新的已發行的場合，對預先登錄的其他憑證驗證伺服器，通知要旨爲「已發行 CRL」之 CRL 發行通知送訊手段。

14.如申請專利範圍第12項所記載之憑證認證伺服器，其中：

具備有，於發現到前述 CRL 爲新的已發行的場合，對預先登錄的其他憑證驗證伺服器，通知要旨爲「已發行 CRL」之 CRL 發行通知送訊手段。

15.如申請專利範圍第11項所記載之憑證驗證伺服器，其中：

具備有作成 CRL 發行通知委託訊息之 CRL 發行通知委託作成手段。

16.如申請專利範圍第15項所記載之憑證驗證伺服器，其中：

具備有，自其他的憑證驗證伺服器接收前述 CRL 發行通知委託訊息之 CRL 發行通知委託受訊手段；

和於已接收前述 CRL 發行通知的場合，對已能發送前述 CRL 發行通知委託訊息的憑證驗證伺服器，轉送前述 CRL 發行通知之 CRL 發行通知管理手段。

17.一種憑證驗證伺服器，其特徵爲：

具備有，驗證憑證的有效性之憑證有效性驗證手段，和快取爲了讓該憑證有效性驗證手段驗證前述憑證的有效性所構築的驗證路徑之驗證路徑快取手段；

(6)

具備有，於已構築前述驗證路徑的場合，於已預先登錄的其他憑證驗證伺服器，發送該驗證路徑之驗證路徑送訊手段；

前述驗證快取手段係，於已自其他的憑證伺服器驗證伺服器接收前述憑證路徑的場合，快取該驗證路徑。

18.一種客戶端裝置，其特徵爲：

具備有，驗證電子簽章之電子簽章驗證手段，和於憑證驗證伺服器委託前述憑證的有效性之憑證有效性驗證委託手段；

具備有，把爲了驗證前述電子簽章之必要的前述憑證的取得，委託到前述憑證驗證伺服器之憑證取得委託手段。

19.一種憑證驗證伺服器，其特徵爲：

具備有驗證前述憑證的有效性之憑證有效性驗證手段；

具備有把已要求取得的前述憑證，取得自前述憑證儲存庫，而且，於藉由前述憑證驗證手段判斷該憑證爲有效的場合，回覆該憑證之憑證取得手段。

20.一種 CRL 儲存庫裝置，具備有儲存認證站已發行的 CRL 之 CRL 儲存手段，其特徵爲：

前述 CRL 儲存手段具備有，儲存新的 CRL 和發送 CRL 發行通知之 CRL 發行通知送訊手段。

21.如申請專利範圍第20項所記載之 CRL 儲存庫裝置，其中：

(7)

具備有接收 CRL 發行通知委託訊息之 CRL 發行通知委託受訊手段；

前述 CRL 發行通知送訊手段係，把前述 CRL 發行通知，發送到已接收的前述 CRL 發行通知委託訊息的送訊源。

22.一種記錄 CRL 發行確認軟體之媒體，於計算機，監視 CRL 的發行，於已發行新的 CRL 的場合，實現發送 CRL 發行通知之 CRL 發行通知送訊手段，其特徵爲：

實現接收 CRL 發行通知委託訊息之 CRL 發行通知委託受訊手段；

前述 CRL 發行通知送訊手段係，把前述 CRL 發行通知，發送到已接收的前述 CRL 發行通知委託訊息的送訊源。

23.如申請專利範圍第1～6項中任一項所記載之認證基礎系統，其中：

前述 CRL 發行通知係，包含了記載在新的已發行的 CRL 本身的項目。

24.如申請專利範圍第1～6項中任一項所記載之認證基礎系統，其中：

前述 CRL 發行通知係，包含了記載自該發行通知之前已發行的 CRL 和新的已發行的 CRL 的差分資訊的項目。

25.如申請專利範圍第1～6項中任一項所記載之認證

(8)

基礎系統，其中：

前述 CRL 發行通知係，包含了記載新的已失效的憑證識別資訊一覽的項目。

26.如申請專利範圍第9項或第10項所記載之認證站，其中：

前述 CRL 發行通知係，包含了記載在新的已發行的CRL本身的項目。

27.如申請專利範圍第9項或第10項所記載之認證站，其中：

前述 CRL 發行通知係，包含了記載自該發行通知之前已發行的 CRL 和新的已發行的 CRL 的差分資訊的項目。

28.如申請專利範圍第9項或第10項所記載之認證站，其中：

前述 CRL 發行通知係，包含了記載新的已失效的憑證識別資訊一覽的項目。

29.如申請專利範圍第11～16項中任一項所記載之憑證驗證伺服器，其中：

前述 CRL 發行通知係，包含了記載在新的已發行的CRL本身的項目。

30.如申請專利範圍第11～16項中任一項所記載之憑證驗證伺服器，其中：

前述 CRL 發行通知係，包含了記載自該發行通知之前已發行的 CRL 和新的已發行的 CRL 的差分資訊的項目

。

31.如申請專利範圍第11～16項中任一項所記載之憑證驗證伺服器，其中：

前述 CRL 發行通知係，包含了記載新的已失效的憑證識別資訊一覽的項目。

32.如申請專利範圍第20項或第21項所記載之 CRL 儲存庫裝置，其中：

前述 CRL 發行通知係，包含了記載在新的已發行的 CRL 本身的項目。

33.如申請專利範圍第20項或第21項所記載之 CRL 儲存庫裝置，其中：

前述 CRL 發行通知係，包含了記載自該發行通知之前已發行的 CRL 和新的已發行的 CRL 的差分資訊的項目。

34.如申請專利範圍第20項或第21項所記載之 CRL 儲存庫裝置，其中：

前述 CRL 發行通知係，包含了記載新的已失效的憑證識別資訊一覽的項目。

圖1

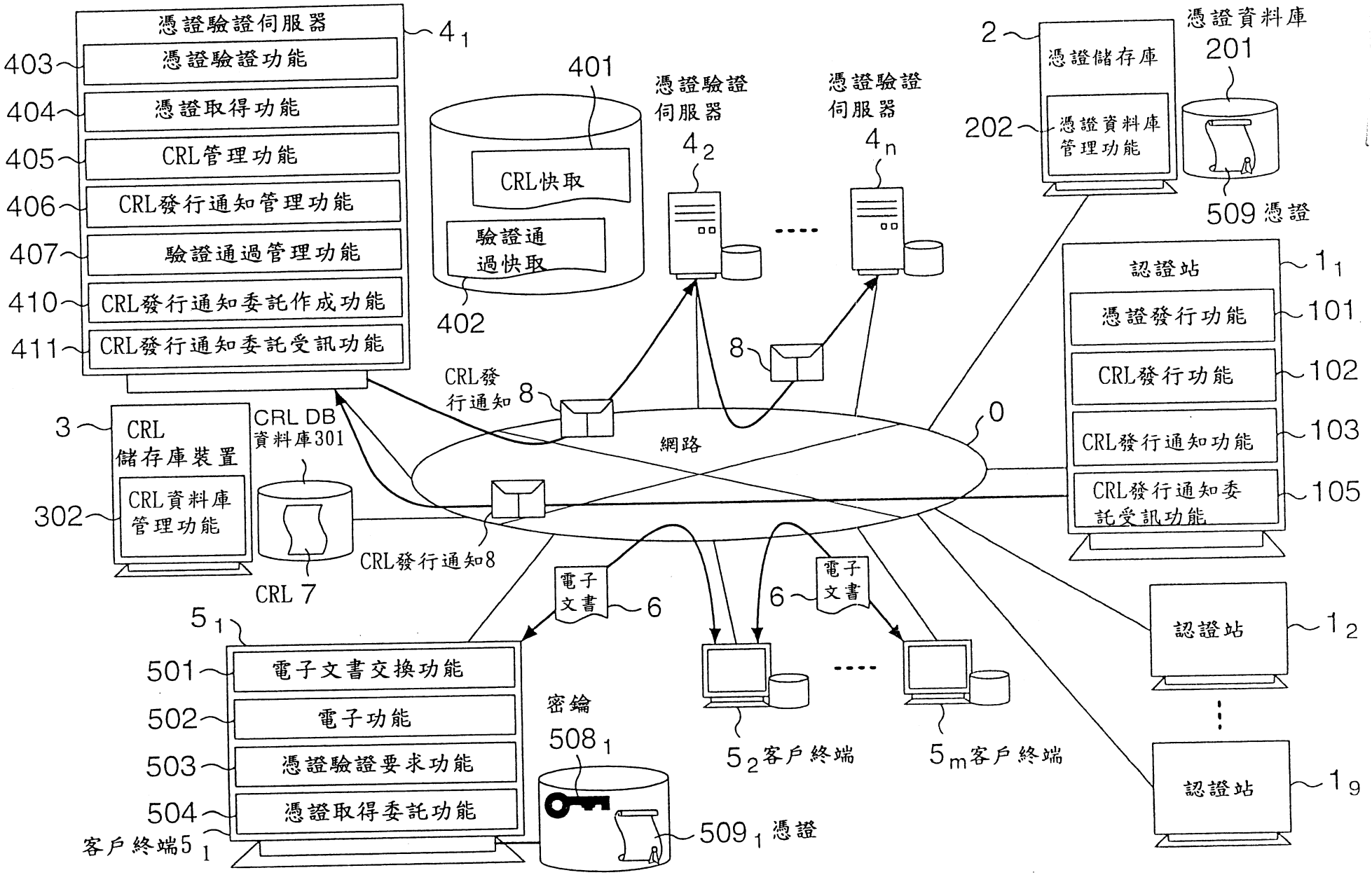

憑證驗證伺服器
4 1
403
憑證驗證功能
404
憑證取得功能
405
CRL管理功能
406
CRL發行通知管理功能
407
驗證通過管理功能
410
CRL發行通知委託作成功能
411
CRL發行通知委託受訊功能
401
CRL快取
驗證通過快取
402
憑證驗證伺服器
4 2
憑證驗證伺服器
4 n
2
憑證儲存庫
202
憑證資料庫管理功能
憑證資料庫
201
509 憑證
認證站
1 1
101
憑證發行功能
102
CRL發行功能
103
CRL發行通知功能
105
CRL發行通知委託受訊功能
8
CRL發行通知 8
網路
0
3
CRL儲存庫裝置
302
CRL資料庫管理功能
CRL DB資料庫301
CRL 7
CRL發行通知8
電子文書
6
6
電子文書
5 1
501
電子文書交換功能
502
電子功能
503
憑證驗證要求功能
504
憑證取得委託功能
客戶終端5 1
密鑰
508 1
509 1 憑證
5 2客戶終端
5 m客戶終端
認證站
1 2
認證站
1 9

圖2

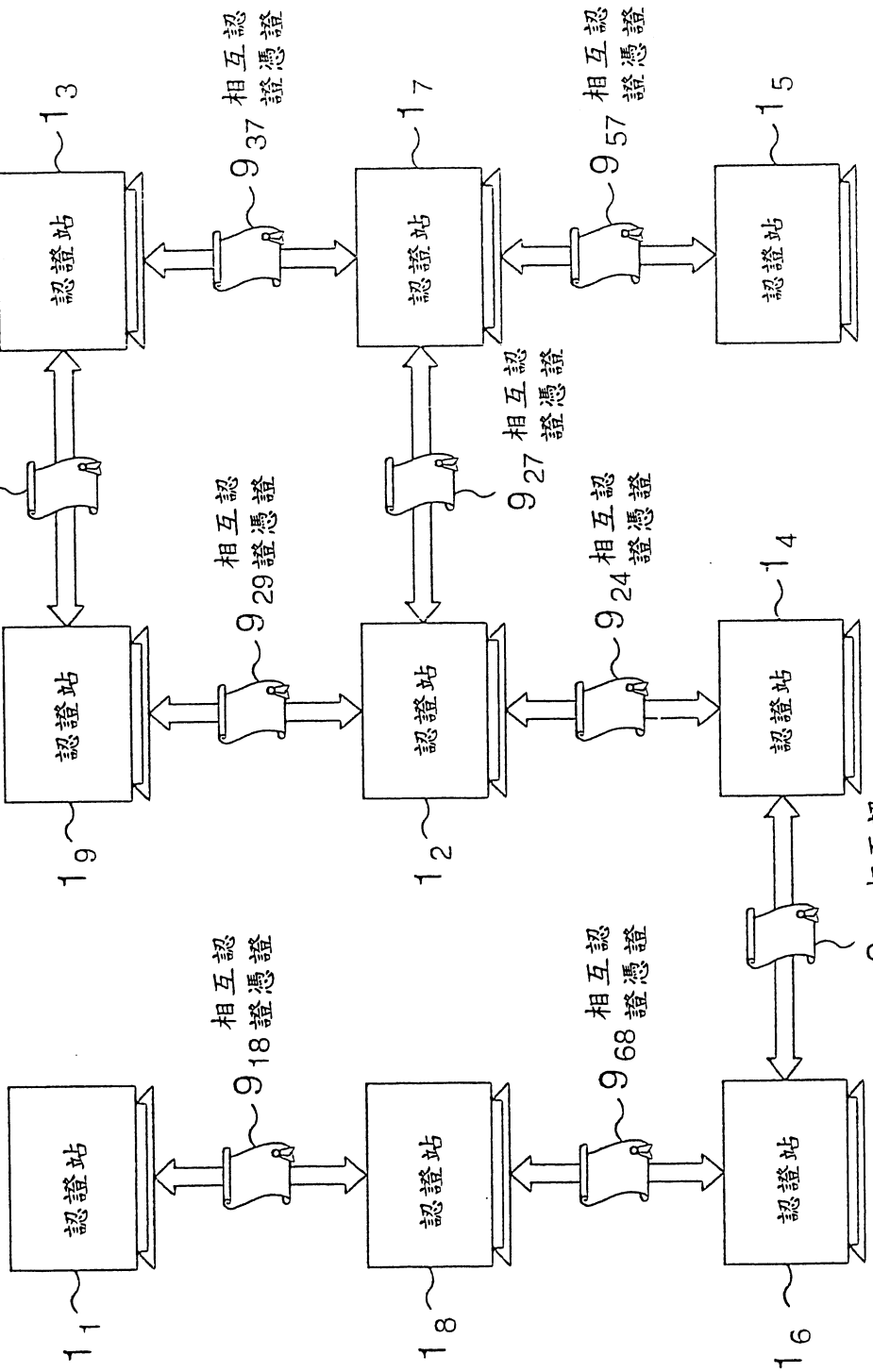

認證站
相互認證憑證
1_1
1_2
1_3
1_4
1_5
1_6
1_7
1_8
1_9
9_{18}
9_{24}
9_{27}
9_{29}
9_{37}
9_{39}
9_{46}
9_{57}
9_{68}

圖3

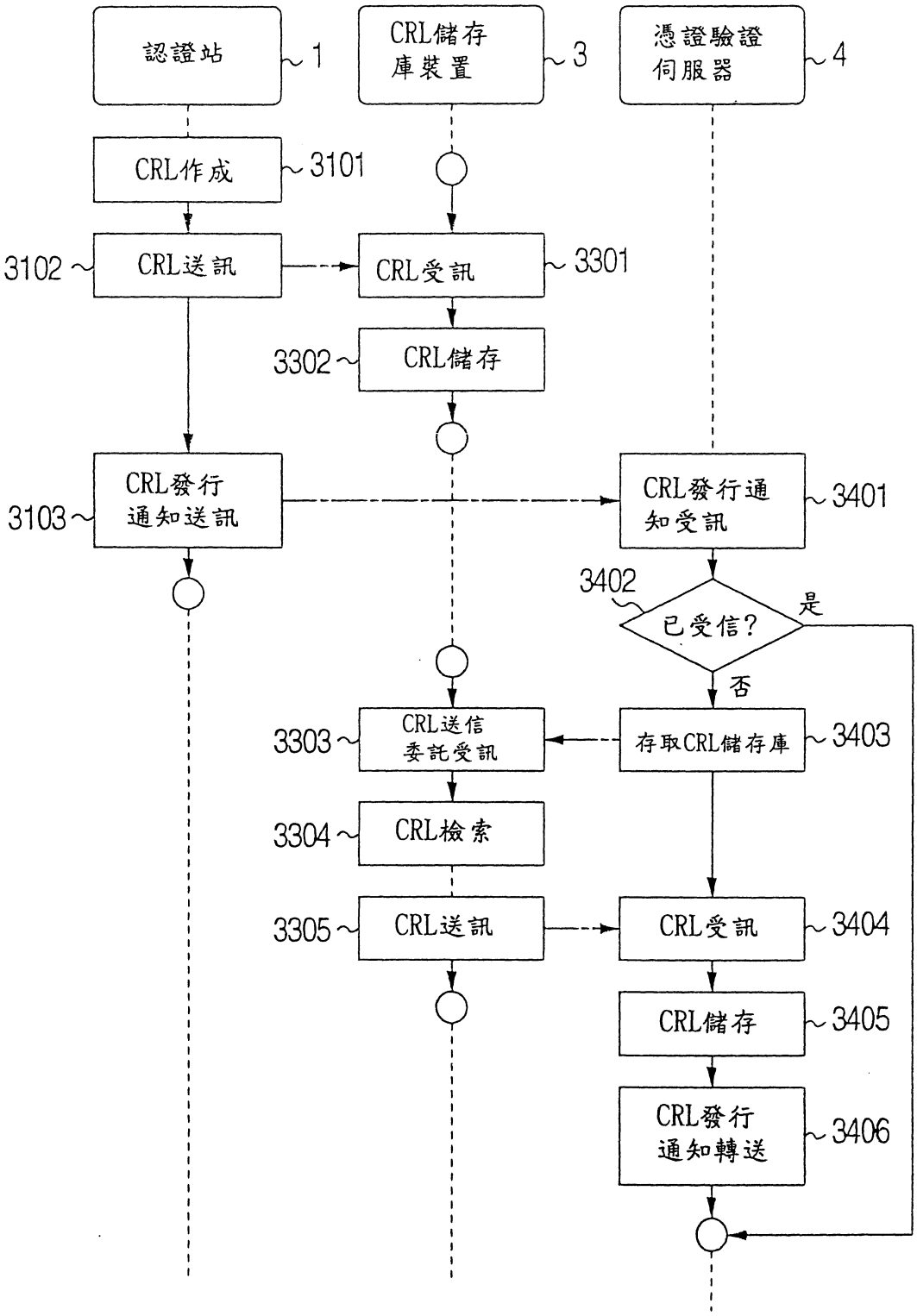

認證站
1
CRL儲存庫裝置
3
憑證驗證伺服器
4
CRL作成
3101
3102
CRL送訊
CRL受訊
3301
3302
CRL儲存
3103
CRL發行通知送訊
CRL發行通知受訊
3401
3402
已受信?
是
否
3303
CRL送信委託受訊
存取CRL儲存庫
3403
3304
CRL檢索
3305
CRL送訊
CRL受訊
3404
CRL儲存
3405
CRL發行通知轉送
3406

圖4

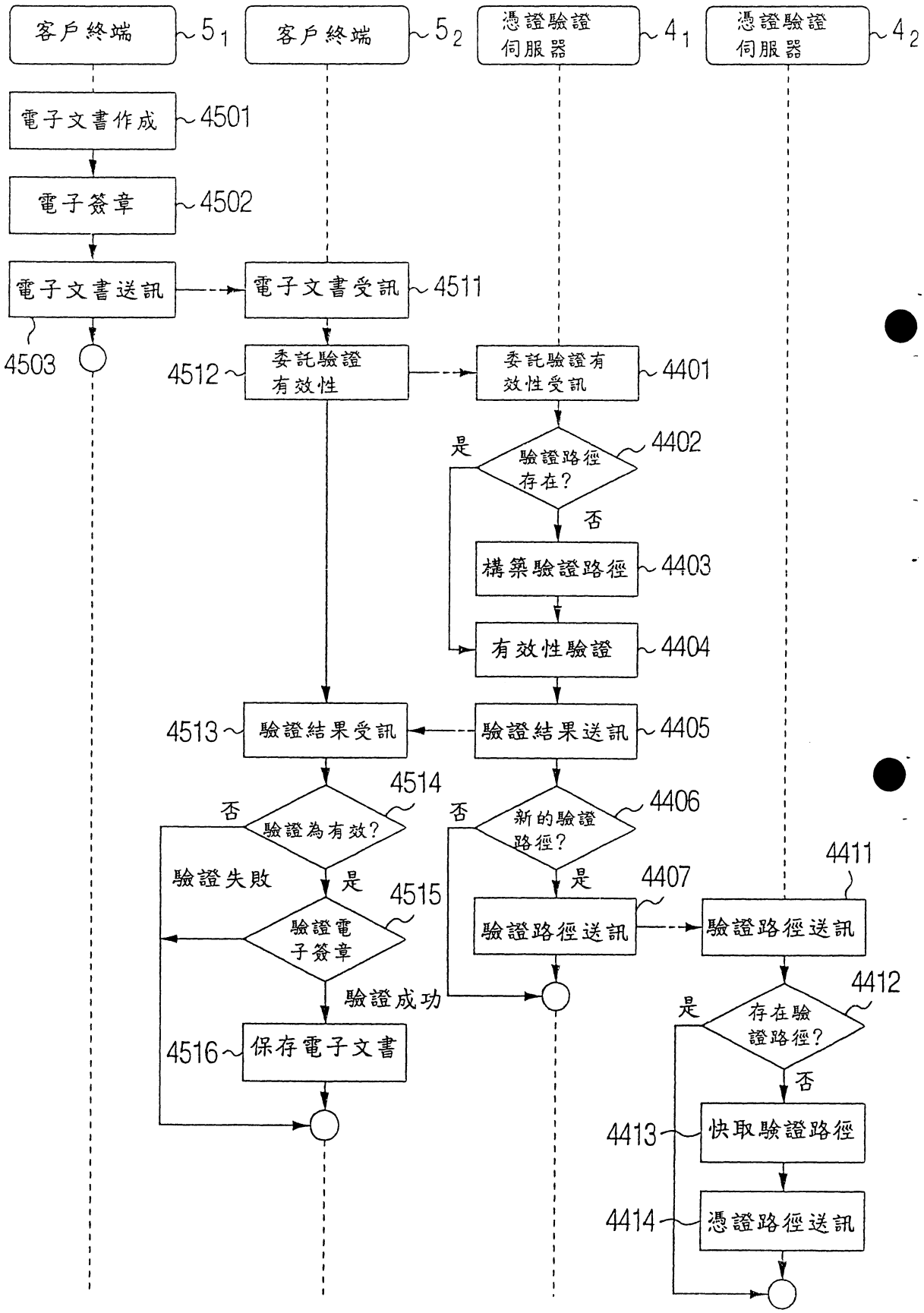

客戶終端 5₁
客戶終端 5₂
憑證驗證伺服器 4₁
憑證驗證伺服器 4₂
電子文書作成 4501
電子簽章 4502
電子文書送訊
電子文書受訊 4511
4503
4512
委託驗證有效性
委託驗證有效性受訊 4401
是
驗證路徑存在? 4402
否
構築驗證路徑 4403
有效性驗證 4404
4513
驗證結果受訊
驗證結果送訊 4405
4514
否
驗證為有效?
否
新的驗證路徑? 4406
4411
驗證失敗
是
4515
驗證電子簽章
是
4407
驗證路徑送訊
驗證路徑送訊
驗證成功
4412
是
存在驗證路徑?
4516
保存電子文書
否
4413
快取驗證路徑
4414
憑證路徑送訊

圖5

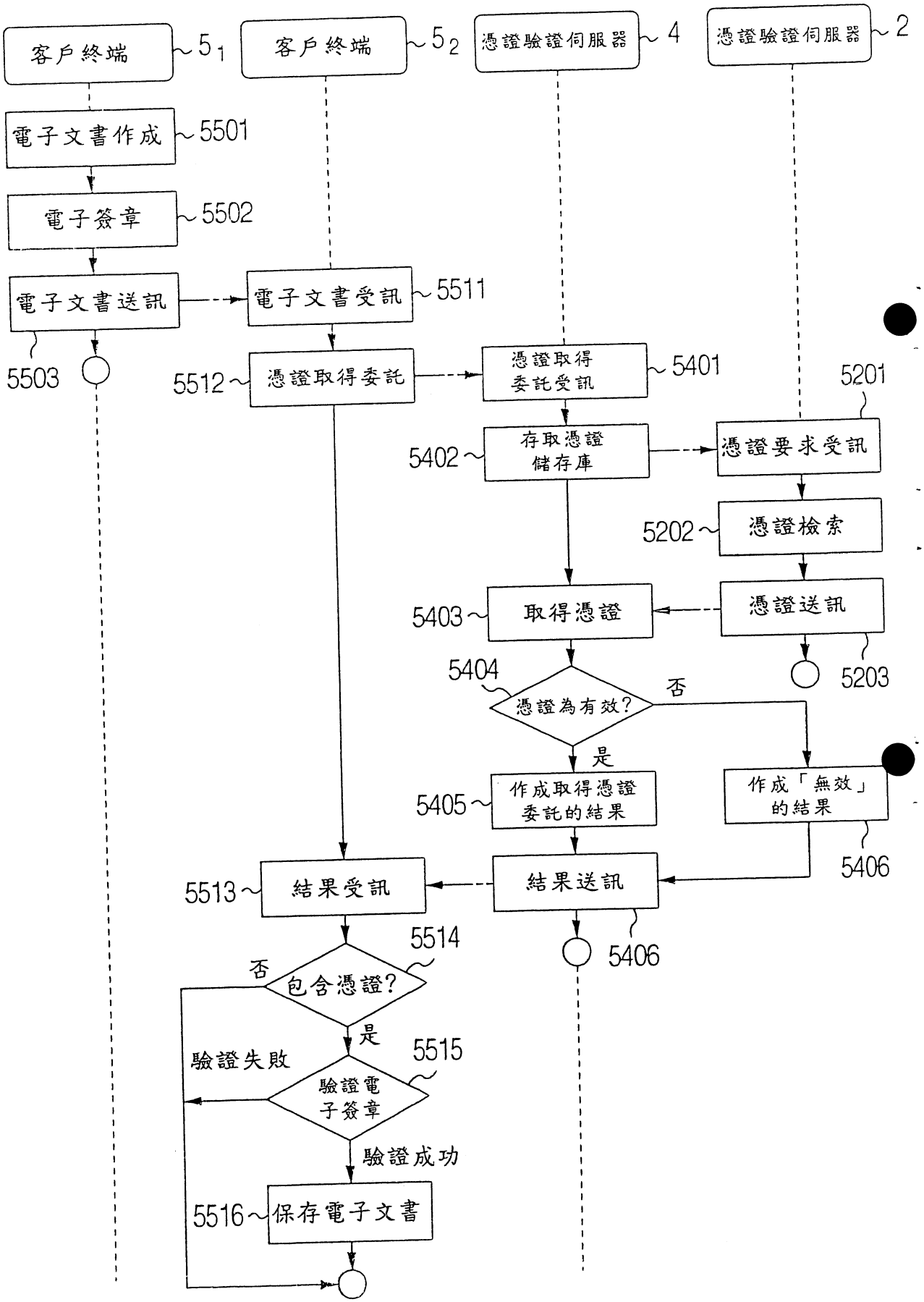

客戶終端
5 1
客戶終端
5 2
憑證驗證伺服器
4
憑證驗證伺服器
2
電子文書作成
5501
電子簽章
5502
電子文書送訊
電子文書受訊
5511
5503
5512
憑證取得委託
憑證取得委託受訊
5401
5201
存取憑證儲存庫
5402
憑證要求受訊
憑證檢索
5202
憑證送訊
取得憑證
5403
5203
5404
憑證為有效?
否
是
作成取得憑證委託的結果
5405
作成「無效」的結果
5406
結果送訊
結果受訊
5513
5406
5514
包含憑證?
否
是
驗證失敗
5515
驗證電子簽章
驗證成功
保存電子文書
5516

圖6A

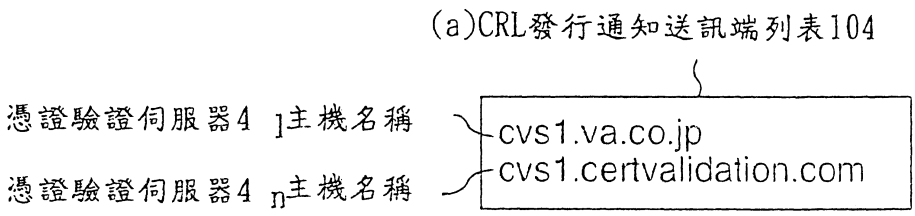

(a)CRL發行通知送訊端列表104
憑證驗證伺服器4 1主機名稱
憑證驗證伺服器4 n主機名稱
cvs1.va.co.jp
cvs1.certvalidation.com

圖6B

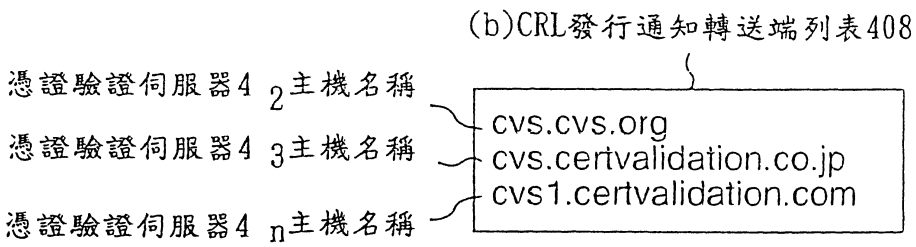

(b)CRL發行通知轉送端列表408
憑證驗證伺服器4 2主機名稱
憑證驗證伺服器4 3主機名稱
憑證驗證伺服器4 n主機名稱
cvs.cvs.org
cvs.certvalidation.co.jp
cvs1.certvalidation.com

圖7

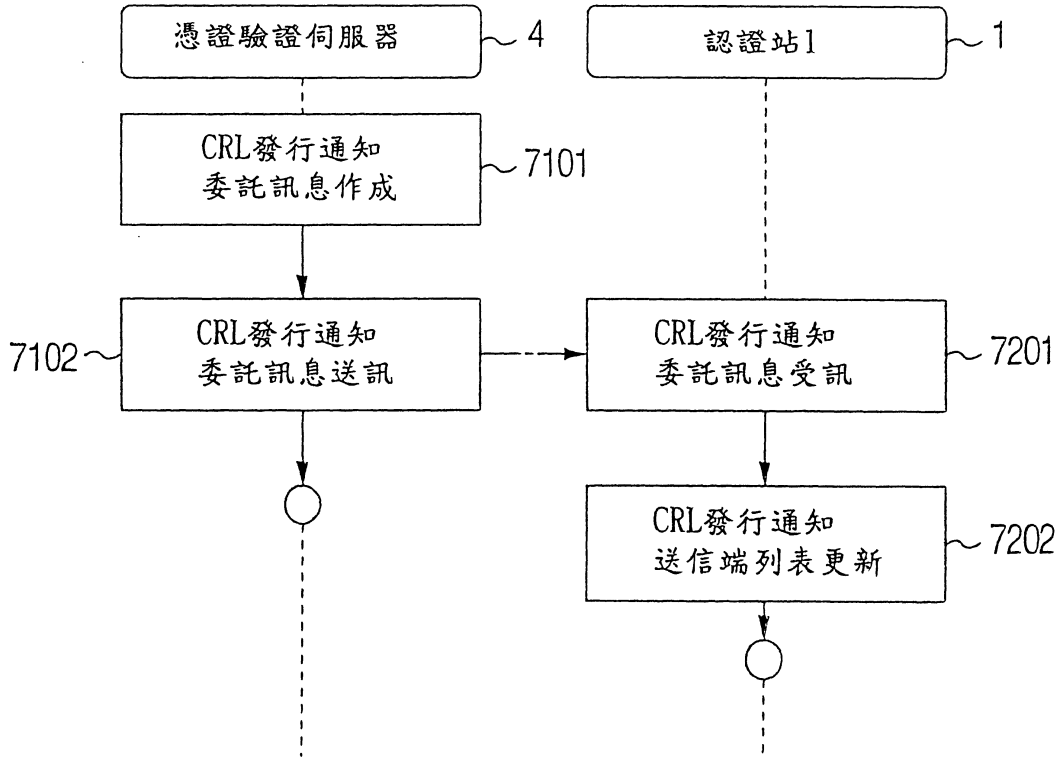

憑證驗證伺服器
4
認證站1
1
CRL發行通知
委託訊息作成
7101
7102
CRL發行通知
委託訊息送訊
CRL發行通知
委託訊息受訊
7201
CRL發行通知
送信端列表更新
7202

圖8A

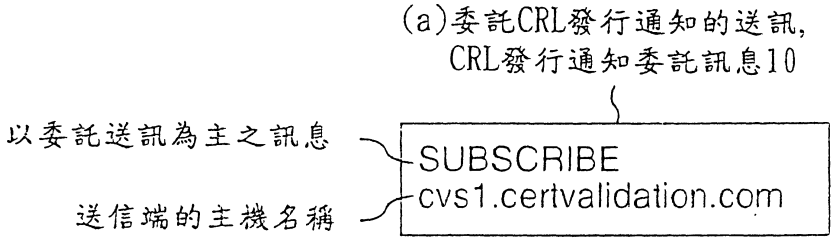

(a)委託CRL發行通知的送訊,
CRL發行通知委託訊息10
以委託送訊為主之訊息
SUBSCRIBE
送信端的主機名稱
cvs1.certvalidation.com

圖8B

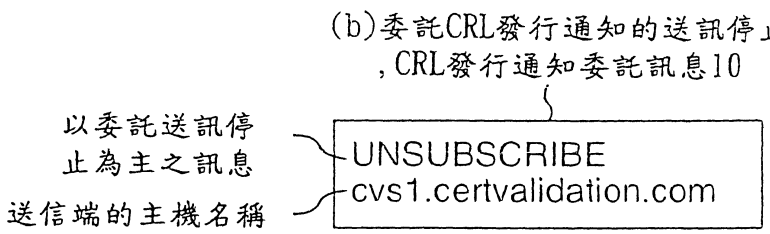
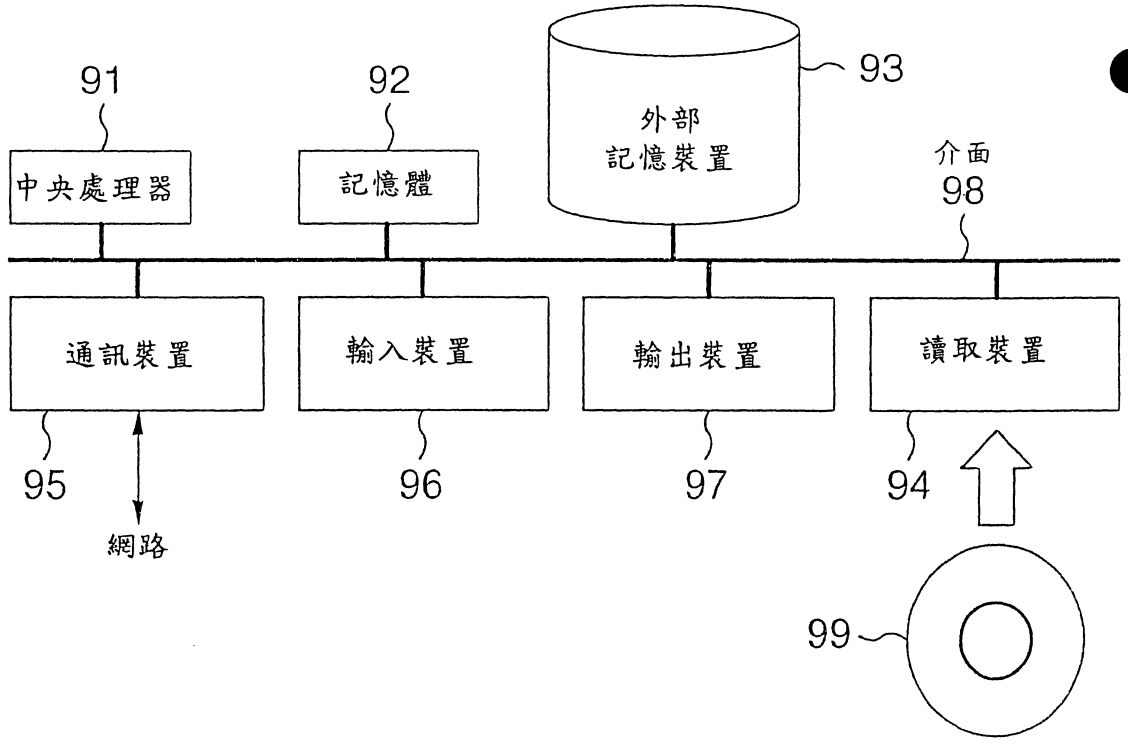

(b)委託CRL發行通知的送訊停止
,CRL發行通知委託訊息10
以委託送訊停
止為主之訊息
UNSUBSCRIBE
送信端的主機名稱
cvs1.certvalidation.com

圖9


91
92
93
中央處理器
記憶體
外部
記憶裝置
介面
98
通訊裝置
輸入裝置
輸出裝置
讀取裝置
95
96
97
94
網路
99

柒、（一）、本案指定代表圖為：第 1 圖

（二）、本代表圖之元件代表符號簡單說明：

0	網路	302	CRL 資料庫管理功能
1_1、1_2、1_9	認證站	401	CRL 快取
2	憑證儲存庫	402	驗證通過快取
3	CRL 儲存庫	403	憑證驗證功能
4_1、4_2、4_n	憑證驗證伺服器	404	憑證取得功能
5_1、5_2、5_m	客戶終端	405	CRL 管理功能
6	電子文書	406	DRL 發行通知管理功能
7	電子憑證註銷清單	407	驗證通過管理功能
8	CRL 發行通知	410	CRL 發行通知委託作成功能
101	憑證發行功能	411	CRL 發行通知委託受訊功能
102	CRL 發行功能	501	電子文書交換功能
103	CRL 發行通知功能	502	電子功能
105	CRL 發行通知委託受訊功能	503	憑證諭證要求功能
201	憑證資料庫	504	憑證取得委託功能
202	憑證資料庫管理功能	508	密鑰
301	CRL DB 資料庫	509、509_1	憑證

捌、本案若有化學式時，請揭示最能顯示發明特徵的化學式：