公告本

發明專利說明書

（本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫）

※ 申請案號：94137999

※ 申請日期：94.10.28　　※IPC 分類：H04L 9/06 (2006.01)

一、發明名稱：（中文/英文）

用於檢驗憑證上數位簽名之系統及方法

SYSTEM AND METHOD FOR VERIFYING DIGITAL SIGNATURES ON CERTIFICATES

二、申 請 人：（共 1 人）

姓名或名稱：（中文/英文）

加拿大商進益研究公司

RESEARCH IN MOTION LIMITED

代表人：（中文/英文）

米赫　拉沙里迪斯

LAZARIDIS, MIHAL

住居所或營業所地址：（中文/英文）

加拿大安大略省滑鐵盧市菲利普街295號

295 PHILLIP STREET, WATERLOO, ONTARIO, N2L 3W8, CANADA

國　籍：（中文/英文）

加拿大　CANADA

三、發明人：（共 2 人）

姓　名：（中文/英文）

1. 麥可　K　布朗

   BROWN, MICHAEL K.

2. 麥可　S　布朗

   BROWN, MICHAEL S.

國　籍：（中文/英文）

1. 加拿大　CANADA

2. 加拿大　CANADA

四、聲明事項：

☐ 主張專利法第二十二條第二項☐第一款或☐第二款規定之事實，其事實發生日期為：　年　月　日。

☑ 申請前已向下列國家（地區）申請專利：

【格式請依：受理國家（地區）、申請日、申請案號　順序註記】

☑ 有主張專利法第二十七條第一項國際優先權：

1.歐洲專利機構；2004年10月29日；04105424.8

2.

☑ 無主張專利法第二十七條第一項國際優先權：

1.美國; 2004年10月29日; 10/975,988

2.

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號　順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料　【格式請依：寄存機構、日期、號碼　順序註記】

國外生物材料　【格式請依：寄存國家、機構、日期、號碼　順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

九、發明說明：

【發明所屬之技術領域】

本發明通常係關於如電子郵件訊息等訊息之處理，具體而言，本發明係關於一種在處理已編碼之訊息過程中用於驗證憑證之系統及方法。

【先前技術】

可使用數種已知協定之一來編碼電子郵件(e-mail)訊息。某些協定(例如，安全多用途網際網路郵件延伸(Secure Multiple Internet Mail Extensions；S/MIME))依賴於公開與私密加密金鑰來提供可信度及完整性，並且依賴於一公開金鑰基礎結構(Public Key Infrastructure；PKI)來傳達提供鑑認及授權的資訊。使用一私密金鑰/公開金鑰對中之私密金鑰所加密的資料僅能使用該私密金鑰/公開金鑰對中之該相對應公開金鑰予以解密，反之亦然。在編碼訊息過程中所使用之公開金鑰的確實性係使用憑證予以驗證。具體而言，如果一計算裝置的使用者想要先對一訊息進行加密，之後才傳送該訊息給一特定個體，則該使用者需要一用於該個體的憑證。該憑證典型地包括該個體的該公開金鑰，以及包括其他識別相關之資訊。

憑證係典型由憑證授權機構所發行的數位文件。為了信任一特定公開金鑰，典型必須由一也受信任之憑證授權機構來發行該公開金鑰，或由一相關聯於該受信任之憑證授權機構的實體(entity)來發行該公開金鑰。介於一受信任憑證授權機構與一發行之公開金鑰之間的關係可藉由一連串

相關憑證(也稱為一憑證鏈)予以表示。可遵循該憑證鏈來決定一憑證的有效性(validity)。

典型地，一憑證授權機構將數位簽名於其所發行的每個憑證，藉以檢定一特定公開金鑰屬於如各自憑證上所指示的據稱之擁有人。在建置憑證鏈過程中，通常必須檢驗該鏈上之該等憑證的數位簽名。檢驗一憑證上之一數位簽名係一項處理程序，其需要發行該憑證之憑證授權機構的公開金鑰。

【發明內容】

檢驗處理程序可能耗時且高成本(例如，就計算資源使用量而論)，尤其是在較小型裝置(例如，諸如行動裝置)上執行檢驗時。對於在一使用者計算裝置上處理多個憑證，相同的數位簽名可能會遭受到一次以上檢驗。本發明具體實施例一般係針對一種系統及方法，其藉由儲存簽名檢驗作業中所採用的某資訊以供再次使用，以促進更高效率檢驗憑證上的數位簽名。

在本發明一廣泛態樣中，提供一種用於在一計算裝置上檢驗一憑證上的一數位簽名之方法，該方法包括下列步驟：使用相關聯於該憑證之一發行者的一第一公開金鑰，執行一對於該數位簽名的第一簽名檢驗作業；決定在該第一簽名檢驗作業中是否成功檢驗該數位簽名；將該第一公開金鑰儲存於一記憶體儲存區中；接收一要求，以使用相關聯於該憑證之一發行者的一第二公開金鑰，執行一對於該數位簽名的第二簽名檢驗作業；比較該第二公開金鑰與

該記憶體儲存區中所儲存的該第一公開金鑰，以決定該第一公開金鑰與該第二公開金鑰是否匹配；以及如果在該第一簽名檢驗作業中成功檢驗該數位簽名，並且如果在該比較步驟決定一匹配，則回應該要求而指示成功檢驗該數位簽名，藉以不需要執行該第二簽名檢驗作業。

【實施方式】

本發明某些具體實施例利用一行動台。一行動台是一種含進階資料通信能力的雙向通信裝置，其具有與其他電腦系統通信的能力，並且在本文中也普遍稱為一行動裝置。一行動裝置也可包括語音通信能力。依據一行動裝置所提供的功能，而可被稱為一資料傳訊裝置、一雙向傳呼機、一含資料傳訊能力之行動電話、一無線網際網路設備或一資料通信裝置(含或不含電話能力)。一行動裝置透過一含多個收發器站的網路來與其他裝置通信。

為了輔助閱讀者理解一行動裝置之結構及其與其他裝置通信之方式，請參閱圖1至3。

請先參考圖1，在一實例實施方式中之一行動裝置的方塊圖係一般地繪示為100。行動裝置100包括若干組件，控制組件係微處理器102。微處理器102控制該行動裝置100的整體運作。透過通信子系統104來執行通信功能，包括資料及語音通信。通信子系統104接收來自一無線網路200的訊息以及傳送訊息至該無線網路200。在此實例實施方式之行動裝置100中，通信子系統104係依照行動通信全球定位系統(Global System for Mobile Communications；

GSM)及通用封包無線電服務(General Packet Radio Services；GPRS)標準予以組態。該GSM/GPRS無線網路全球通行，並且預期彼等標準最終將被增強可資料GSM環境(Enhanced Data GSM Environment；EDGE)及通用行動式電信服務(Universal Mobile Telecommunications Service；UMTS)所取代。新標準仍然在定義中，但是相信彼等新標準將具有對本文描述之網路運作模式的相似點，並且熟悉此項技術者也明白，本發明預定使用未來開發的任何其他適合的標準。連接通信子系統104與無線網路200的無線鏈路代表一或多個不同之射頻(RF)頻道，依照針對GSM/GPRS通信所指定之已定義協定運作。配合較新的網路協定，彼等頻道能夠支援電路交換式語音通信且支援封包交換式資料通信。

雖然在此實例實施方式之行動裝置100中，相關聯於行動裝置100的無線網路係一GSM/GPRS無線網路，但是在變化版實施方式中，其他無線網路也可能與行動裝置100相關聯。例如，可採用的不同類型無線網路包括資料中心無線網路、語音中心無線網路以及可透過相同實體基地台來支援語音及資料通信的雙模式網路。結合的雙模式網路包括(但不限於)分碼多向近接(Code Division Multiple Access；CDMA)或CDMA2000網路、GSM/GPRS網路(如上文所述)及未來第三代(3G)網路(像是EDGE及UMTS)。某些較舊之資料中心網路實例包括Mobitex™無線電網路及DataTAC™無線電網路。較舊之語音中心網路實例包括個

人通信系統(Personal Communication Systems；PCS)網路(像是GSM)及分時多向近接(Time Division Multiple Access；TDMA)系統。

微處理器102也與附加的子系統互動，諸如隨機存取記憶體(Random Access Memory；RAM)106、快閃記憶體108、顯示器110、輔助輸入/輸出(I/O)子系統112、序列埠114、鍵盤116、揚聲器118、麥克風120、短矩離通信122及其它裝置124。

行動裝置100的某些子系統執行通信相關功能，而其他子系統可提供「常駐」(resident)或裝置上功能。舉例而言，對於通信相關功能(諸如輸入一擬透過網路200傳輸之文字訊息)及裝置常駐之功能(諸如計算機或工作清單)，皆可使用顯示器110及鍵盤116。微處理器102所使用的作業系統軟體典型被儲存在一永續性儲存區(persistent store)，諸如快閃記憶體108，或可能是一唯讀記憶體(ROM)或類似的儲存元件(圖中未繪示)。熟悉此項技術者應明白，作業系統、特定裝置之應用程式或其部分可被暫時載入至一揮發性儲存區中，諸如RAM 106。

行動裝置100可在已完成必要的網路註冊或啟動程序之後，透過網路200傳送及接收通信訊號。網路存取係相關聯於一行動裝置100的一用戶或使用者。為了識別一用戶，行動裝置100需要將一用戶識別模組(Subscriber Identity Module)或「SIM」卡126插入在一SIM介面128中，才能使用一網路進行通信。SIM介面126是一種類型之

傳統「智慧卡」，用於識別一行動裝置100的一用戶，以及用於個人化該行動裝置100等等。若沒有SIM 126，則行動裝置100操作上完全不能與網路200通信。藉由將SIM 126插入至SIM介面128中，一用戶可存取所有訂閱的服務。服務包括：web瀏覽及傳訊，諸如電子郵件、語音郵件、短訊息服務(Short Message Service；SMS)及多媒體傳迅服務(Multimedia Messaging Services；MMS)。更進階的服務包括：銷售點、現場服務及銷售人力自動化。SIM 126包括一處理器及用於儲存資訊的記憶體。一旦SIM 126被插入至SIM介面128中，其即被耦合至微處理器102。為了識別該用戶，SIM 126包含使用者參數，諸如一國際行動用戶識別號碼(International Mobile Subscriber Identity；IMSI)。使用SIM 126的一項優點在於，一用戶未必受任何單一實體行動裝置所約束。SIM 126還可儲存一行動裝置的額外用戶資訊，包括記事簿(或行事曆)資訊及最近通話資訊。

行動裝置100是一種電池供電的裝置，並且包括一電池介面132，用於容納一或多個可充電式電池130。電池介面132被耦合至一調節器(圖中未繪示)，該調節器輔助電池130提供電力V+至行動裝置100。雖然現行技術利用一電池，但是如微燃料電池等未來技術可提供電力至行動裝置100。

微處理器102除了其作業系統功能以外，還能夠在行動裝置100上執行軟體應用程式。控制基本裝置操作的一組

應用程式(包括資料及語音通信應用程式)通常係在行動裝置100的製造期間安裝在該行動裝置100上。可載入至行動裝置100上的另一應用程式是一個人資訊管理員(personal information manager；PIM)。一PIM具有用以組織及管理一用戶所感興趣之資料項目的功能，包括(但不限於)電子郵件、行事曆事件、語音郵件、約會及工作項目。一PIM應用程式具有經由無線網路200傳送及接收資料項目的能力。可用一主機電腦系統所儲存及/或所相關聯之該行動裝置用戶的相對應資料項目，來緊密地整合、同步化及更新PIM資料項目。此功能在行動裝置100上建立關於此類項目的一鏡像主機電腦。這可能對於主機電腦系統是該行動裝置用戶之辦公室電腦系統尤其有利。

也可透過網路200、輔助I/O子系統112、序列埠114、短矩離通信子系統122或任何其它適用的子系統124，將額外應用程式載入至該行動裝置100上。此項應用程式安裝方面的彈性增加行動裝置100的功能，並且可提供增強型裝置上功能、通信相關功能或這兩種功能。例如，安全通信應用程式可實現擬使用行動裝置100執行的電子商務功能及諸如金融交易等其他功能。

序列埠114讓一用戶能夠透過一外部裝置或軟體應用程式來設定偏好設定，並且藉由提供除透過一無線通信網路外將資訊或軟體下載至行動裝置100，來擴充行動裝置100的能力。例如，該替代下載路徑可用來透過一直接且因此可靠和受信任的連接來載入一加密金鑰至行動裝置100

上，藉以提供安全的裝置通信。

短矩離通信子系統122提供介於行動裝置100與不同系統或裝置之間的通信，而不需要使用網路200。例如，子系統122可包括一紅外線裝置及用於短矩離通信的相關聯之電路和組件。短矩離通信實例將包括紅外線資料協會(Infrared Data Association；IrDA)協會所開發的標準、藍芽(Bluetooth)以及IEEE所開發的802.11系列標準。

在使用中，一接收到之訊號(諸如一文字訊息、一電子郵件訊息或web網頁下載)將由通信子系統104予以處理並且輸入至微處理器102。接著，微處理器102將處理該接收到之訊號，以便輸出至顯示器110或替代地輸出至輔助I/O子系統112。一用戶也可以(例如)使用鍵盤116連同顯示器110且可能使用輔助I/O子系統112來撰寫資料項目，諸如電子郵件訊息。輔助I/O子系統112可包括如下裝置：一觸控螢幕、軌跡球、紅外線指紋偵測器或含動態按鈕能力之滾輪。鍵盤116是一文數字鍵盤及/或電話型小鍵盤。可透過通信子系統104在網路200上傳輸一撰寫之項目。

對於語音通信，行動裝置100之整體操作實質上類似，惟該接收到之訊號將被輸出至揚聲器118以及擬傳輸之訊號將由麥克風120予以產生除外。還可以在行動裝置100上實作替代的語音或音訊I/O子系統，諸如一語音訊息記錄子系統。雖然語音或音訊訊號輸出主要係透過揚聲器118來達成，但是還可以使用顯示器110來提供額外資訊，諸如，一來電方之身分、語音通話持續期間或其他語音通話

相關資訊。

現在請參考圖2，圖中繪示圖1所示之通信子系統組件104的方塊圖。通信子系統104包括一接收器150、一發射器152、一或多個內嵌式或內部天線元件154和156、本機振盪器(LO) 158以及一處理器模組(諸如一數位訊號處理器(DSP) 160)。

通信子系統104的特殊設計係取決於行動裝置100所預定在其中操作的網路200，因此應明白，圖2所示之設計僅作為一實例。天線154透過網路200所接收到的訊號被輸入至接收器150，該接收器150可執行常見的接收器功能，諸如訊號放大、降頻轉換、濾波、頻道選擇及類比轉數位(A/D)轉換。一接收到之訊號的A/D轉換允許在DSP 160中執行更複雜的通信功能，諸如解調變及解碼。在類似方式中，DSP 160處理(包括調變及編碼)擬傳輸的訊號。彼等經DSP處理之訊號被輸入至發射器152，以供數位轉類比(D/A)轉換、增頻轉換、濾波、放大以及經由天線156透過網路200傳輸。DSP 160不僅處理通信訊號，而且還提供接收器150及發射器152控制。例如，可透過實作在DSP 160中的自動增益控制演算法，來調節地控制施加至通信訊號的增益。

介於行動裝置100與一網路200之間的無線鏈路可包含一或多個不同之頻道(典型是不同的RF頻道)，以及介於行動裝置100與網路200之間使用的相關聯協定。一RF頻道是一必須節約的有限資源，典型係由於整體頻寬之限制及行動

裝置100之有限電池電力所致。

當行動裝置100係完全操作中時，發射器152典型僅當其正在傳送至網路200時才予以調諧或開啟，否則關閉發射器152以節約資源。同樣地，除非在指定之時期期間(如果隨時)需要接收器150來接收訊號或資訊，否則接收器150被週期性關閉以節約電力。

現在請參考圖3，圖中將一無線網路之一節點的方塊圖繪示為202。實務上，網路200包括一或多個節點202。行動裝置100在無線網路200內與一節點202通信。在圖3之實例實施方式中，節點202係依照通用封包無線電服務(General Packet Radio Service；GPRS)及行動通信全球定位系統(Global System for Mobile；GSM)技術予以組態。節點202包括一含一相關聯塔台206之基地台控制器(BSC) 204、一用於在GSM中支援GPRS所附加之封包控制單元(PCU) 208、一行動交換中心(MSC) 210、一本籍位置暫存器(Home Location Register；HLR) 212、一訪客位置暫存器(Visitor Location Registry；VLR) 214、一伺服GPRS支援節點(Serving GPRS Support Node；SGSN) 216、一閘道GPRS支援節點(Gateway GPRS Support Node；GGSN) 218以及一動態主機組態協定(Dynamic Host Configuration Protocol；DHCP) 220。此組件清單並非旨在列出一GSM/GPRS網路內所有節點202的詳盡組件清單，而是旨在列出透過網路200通信方面常用的組件清單。

在GSM網路中，MSC 210被耦合到BSC 204以及耦合到

一基地台222，並可進一步耦合到有線網路(landline network)，諸如公共交換電話網路(PSTN) 222，藉以滿足電路交換需求。通過PCU 208、SGSN 216及GGSN 218至公共或私有網路(網際網路)224(本文中也普遍稱為一共用網路基礎設施)的連接代表具GPRS能力之行動裝置的資料路徑。在經擴充而具有GPRS能力之GSM網路中，BSC 204也包含一封包控制單元(PCU) 208，該封包控制單元(PCU) 208連接至SGSN 216，藉以控制分段(segmentation)、無線電頻道配置以及滿足封包交換需求。為了追蹤行動裝置位置以及電路交換和封包交換管理之可用性，MSC 210與SGSN 216共用HLR 212。存取VLR 214係受控於MSC 210。

塔台206係一固定式收發站。塔台206與BSC 204共同構成固定式收發器設備。該固定式收發器設備提供用於一特定涵蓋區域(通常被統稱為「細胞」)的無線網路涵蓋範圍。該固定式收發器設備經由塔台206，在其細胞內傳輸通信訊號至行動裝置以及接收來自行動裝置的通信訊號。該固定式收發器設備通常在其控制器之控制下，依照特定(通常係預先決定)通信協定及參數來執行多項功能，諸如擬傳輸至行動裝置之訊號的調變以及可能的編碼及/或加密。該固定式收發器設備同樣地解調變以及可能的解碼和解密(若有需要)在其細胞內接收自行動裝置100的任何通信訊號。不同節點之間的通信協定及參數可有所不同。例如，一節點可採用一不同的調變方案且以不同於其他節點

的頻率運作。

對於向一特定網路註冊的所有行動裝置100，諸如一使用者設定檔等永續性組態資料被儲存在HLR 212中。HLR 212也包含每個已註冊之行動裝置的位置資訊，並且可能受到查詢以決定一行動裝置的目前位置。MSC 210負責一含多個位置區域的群組，並且在VLR 214中儲存目前在其負責區塊內之行動裝置的資料。進一步，VLR 214也包含關於正造訪其他網路之行動裝置的資訊。VLR 214中的資訊包括從HLR 212傳輸至VLR 214的永續性行動裝置資料之部分，以便加速存取。藉由將額外資訊一遠端HLR 212節點移至VLR 214，介於節點之間的流量可被減少，所以能夠以加速的回應時間來提供語音及資料服務，並且同時需要使用較少的計算資源。

SGSN 216及GGSN 218係為了在GSM內支援GPRS (即，封包交換資料支援)所附加之元件。在無線網路200內，SGSN 216及MSC 210持續追蹤每個行動裝置100的位置，而具有相似的責任。SGSN 216也執行對於網路200上之資料流量的安全性功能及存取控制。GGSN 218提供連至外部封包交換式網路的網路間連接，並且經由運作在網路200內的一網際網路協定(IP)骨幹網路而連接至一或多個SGSN 216。於正常操作期間，一既定行動裝置100必須執行「GPRS Attach」，藉以獲得一IP位址且藉以存取資料服務。在電路交換式語音頻道不存在此需求，原因在於整合服務數位網路(Integrated Services Digital Network；ISDN)

位址係用來投送傳入及傳出之呼叫。目前，所有具備GPRS能力之網路皆使用私有、動態指派之IP位址，因此需要一連接至該GGSN 218的DHCP伺服器220。有許多用於動態IP指派之機制，包括使用一遠端鑑認撥接使用者服務(Remote Authentication Dial-In User Service；RADIUS)伺服器及DHCP伺服器之組合。一旦GPRS Attach完成，隨即建置一從一行動裝置100、通過PCU 208和SGSN 216至一在GGSN 218內之存取點節點(Access Point Node；APN)的邏輯連接。該APN代表一IP鑿通道(IP tunnel)的一邏輯端，其可存取直接網際網路相容之服務或私有網路連接。該APN也代表網路200的安全性機制，原因為每個行動裝置100皆必須被指派給一或多個APN，並且行動裝置100在未先執行GPRS Attach至一經授權使用的APN之情況下，就無法交換資料。該APN可被視為類似於一網際網路網域名稱，諸如"myconnection.wireless.com"。

一旦GPRS Attach完成，隨即建置一鑿通道，並且使用可支援IP封包的任何協定，在標準IP封包內交換所有流量。這包括諸如IP over IP之類的鑿通道方法，如同配合虛擬私有網路(Virtual Private Network；VPN)使用的某些IPSecurity (IPsec)連接的案例。這些鑿通道也稱為封包資料協定(Packet Data Protocol；PDP)內容，並且網路200中有數量有限的PDP內容可供使用。為了最大程度地使用PDP內容，網路200將對於每個PDP內容來執行一閒置計時器，藉以決定是否有活動不足。當一行動裝置100未正在

使用其PDP內容時，PDP內容可能被解除配置，並且IP位址傳回至由DHCP伺服器220所管理的IP位址集區。

現在請參考圖4，圖中繪示在一實例組態中之一主機系統的組件之方塊圖。主機系統250典型是一公司辦公室或其他區域網路(LAN)，但替代地可能是一家用辦公室或某其他私有系統，例如，在變化版實施方式中。在圖4所示之此項實例中，主機系統250被描繪為一行動裝置100之使用者所屬之組織的LAN。

LAN 250包括藉由LAN連接260而互相連接的數個網路組件。例如，一使用者的桌上型電腦262a (其含有適用於使用者之行動裝置100的隨附傳輸基座(cradle) 264)係位於LAN 250上。例如，可藉由一序列或通常序列匯流排(USB)連接，將行動裝置100的傳輸基座264耦合至電腦262a。其他使用者電腦262b也是位於LAN 250上，並且每部電腦可配備或可不配備一適用於一行動裝置的隨附傳輸基座。傳輸基座264促進將資訊(例如，PIM資料、用以促進行動裝置100與LAN 250之間安全通信的私用對稱式加密金鑰)從使用者電腦262a下載至行動裝置100，並且對於在初始化擬使用之行動裝置100過程中通常執行之大量資訊更新尤其有用。下載至行動裝置100的資訊可包括在交換訊息過程中使用憑證。熟悉此項技術者應明白，使用者電腦262a、262b典型地也被連接至未明確繪示於圖4中的其他周邊裝置。

據此，對於此項實例組態，為了易於解說，圖4中僅繪

示LAN 250的網路組件子集，並且熟悉此項技術者應明白，LAN 250將包括未明確繪示於圖4中的其他額外組件。一般而言，LAN 250可代表組織之一較大型網路的一較小部分，並且可包括不同的組件及/或係以不同於圖4之實例中所示之拓樸予以佈置。

在此實例中，行動裝置100透過無線網路200的一節點202及一共用網路基礎設施224 (諸如服務提供者網路或公共網際網路)來與LAN 250通信。可透過一或多個路由器來提供對LAN 250之存取，並且LAN 250的計算裝置可從一防火牆或代理(proxy)伺服器266後端運作。

在一變化版實施方式中，LAN 250包括一無線VPN路由器(圖中未繪示)，藉以促進介於LAN 250與行動裝置100之間的資料交換。在無線產業中，一無線VPN路由器概念是新概念，並且意謂著可建置直接通過一特定無線網路至行動裝置100的一VPN連接。使用一無線VPN路由器可能性已在最近實現，並且可在新網際網路協定(Internet Protocol；IP)版本6 (IPV6)送達IP架構無線網路時予以使用。此新協定將提供足夠的IP位址，藉以使一IP位址專用於所有行動裝置，促使可隨時將資訊發送至一行動裝置。使用一無線VPN路由器的優點在於，其可能是一現成(off-the-shelf) VPN組件，不需要使用一分開的無線閘道及分開的無線基礎設施。在此變化版實施方式中，較佳方式為，一VPN連接係一傳輸控制協定(Transmission Control Protocol；TCP)/IP或使用者資料元協定(User Datagram

Protocol；UDP)/IP連接，藉由將訊息直接傳遞至行動裝置100。

預定給一行動裝置100之使用者的訊息起始時係由LAN 250的一訊息伺服器268予以接收。此類訊息可源自於若干來源中之任何來源。舉例而言，一寄件者已經從LAN 250內的一電腦262b、從連接至無線網路200或連接至一不同無線網路的一不同之行動裝置(圖中未繪示)、從一具備傳送訊息能力的不同計算裝置或其他裝置，經由該共用網路基礎設施224，且例如可能通過一應用服務提供者(ASP)或網際網路服務提供者(ISP)來傳送一訊息。

訊息伺服器268典型係當作用於在組織內且透過共用網路基礎設施224來交換訊息(尤其是電子郵件訊息)的主要介面。組織中已設定傳送及接收訊息的每位使用者期型係相關聯於由訊息伺服器268所管理的一使用者帳戶。訊息伺服器268的一實例係Microsoft Exchange™ Server。在某些實施方式中，LAN 250可包括多個訊息伺服器268。訊息伺服器268也可被調整以提供除訊息管理外的額外功能，例如，包括相關聯於行事曆及工作清單之資料管理。

當訊息伺服器268接收到訊息時，典型將訊息儲存在一訊息儲存區(圖中未明確繪示)中，可從該訊息儲存區檢索訊息且傳遞至使用者。舉例而言，正在一使用者電腦262a上執行的一電子郵件用戶端應用程式，可要求訊息伺服器268上所儲存之相關聯於該使用者帳戶的電子郵件訊息。接著，典型從訊息伺服器268檢索彼等訊息，且將所檢索

之訊息本機儲存在電腦262a上。

當操作行動裝置100時，使用者會想要檢索電子郵件訊息，以便傳遞至手持裝置。一正在行動裝置100上執行的電子郵件用戶端應用程式，也可向訊息伺服器268要求相關聯於該使用者帳戶的訊息。該電子郵件用戶端可被組態(可能按照組織的資訊技術(IT)政策，由使用者進行組態，或由系統管理員進行組態)，用以按該使用者之指示、在某預定義之時間間隔或發生某預定義事件時提出此項要求。在某些實施方式中，行動裝置100被指派屬於自己的電子郵件位址，並且當訊息伺服器268接收到已明確定址至行動裝置100的訊息時，自動將訊息重新導向至行動裝置100。

為了促進在行動裝置100與LAN 250的組件之間的訊息及訊息相關資料的無線通信，可提供若干無線通信支援組件270。在此實例實施方式中，例如，無線通信支援組件270包括一訊息管理伺服器272。訊息管理伺服器272係用來明確提供對於管理由行動裝置所處置之訊息(例如，電子郵件訊息)的支援。一般而言，雖然訊息仍然係儲存在訊息伺服器268上，但是可使用訊息管理伺服器272來控制何時、是否及如何應將訊息傳送至行動裝置100。訊息管理伺服器272也促進行動裝置100上所撰寫之訊息的處置，彼等訊息被傳送至訊息伺服器268，以便隨後傳遞。

例如，訊息管理伺服器272可：監視使用者的用於新電子郵件訊息的「信箱」(例如，訊息伺服器268上相關聯於

該使用者帳戶的訊息儲存區)；將使用者定義之篩選器套用至新訊息，藉以決定是否及如何將訊息中繼至使用者的行動裝置100；壓縮及加密新訊息(例如，使用加密技術，諸如資料加密標準(Data Encryption Standard；DES)或三重DES (Triple DES))，並且經由該共用網路基礎設施224及無線網路200將訊息發送至行動裝置100；以及接收行動裝置100上撰寫的訊息(例如，已使用Triple DES予以加密)、解密及解壓縮該等撰寫之訊息，重新格式化該等撰寫之訊息(如果想要重新格式化該等撰寫之訊息，使訊息似乎是源自於使用者電腦262a)，並且將該等撰寫之訊息投送至訊息伺服器268，以便傳遞。

訊息管理伺服器272可定義(例如，按照IT政策，由系統管理員進行定義)且強制實行相關聯於訊息(擬從行動裝置100傳送及/或由行動裝置100接收之訊息)的某些屬性或限制。例如，彼等屬性或限制可包括：行動裝置100是否可接收已加密及/或已簽名的訊息；最小加密金鑰大小；傳出之訊息是否必須多以加密及/或簽名；以及從行動裝置100傳送的所有安全訊息之複本是否要傳送至一預定義複本位址。

訊息管理伺服器272也可被調整以提供其他控制功能，諸如僅將某訊息資訊或訊息伺服器268上所儲存之一訊息的預定義部分(例如，「區塊」)發送至行動裝置100。例如，當起始時由行動裝置100從訊息伺服器268檢索一訊息時，訊息管理伺服器272被調整以僅發送一訊息之第一部

分至行動裝置100，該部分屬於一預定義大小(例如，2 KB)。接著，使用者可要求該訊息的更多部分，擬由訊息管理伺服器272以相似大小之區塊傳遞至行動裝置100，可能多達一最大預定義訊息大小。

因此，訊息管理伺服器272促進對於傳達至行動裝置100之資料類型及資料量的最佳控制，並且可有助於最小化潛在的頻寬或其他資源浪費。

熟悉此項技術者應明白，未必在LAN 250或其他網路中的一分開之實體伺服器上實施訊息管理伺服器272。例如，相關聯於訊息管理伺服器272的某些或所有功能可能與訊息伺服器268或LAN 250中的某其他伺服器整合在一起。另外，LAN 250可包括多個訊息管理伺服器272，尤其在必須支援大量行動裝置的變化版實施方式中。

本發明具體實施例通常係關於在處理已編碼之訊息(諸如已加密及/或已簽名的電子郵件訊息)過程中使用的憑證。雖然可使用簡易郵件傳送協定(Simple Mail Transfer Protocol；SMTP)、RFC822標頭及多用途網際網路郵件延伸標準(Multipurpose Internet Mail Extensions；MIME)本文部分來定義一不要求編碼之電子郵件訊息的格式，但是在傳達已編碼之訊息過程中(即，在安全傳訊應用程式中)，可使用屬於MIME協定之一版本的Secure/MIME (S/MIME)。S/MIME實現端對端鑑認及可信度，並且從一訊息之寄件者傳送一訊息之時間開始，直到該訊息之收件者解碼及讀取該訊息為止，保護資料完整性及私密性。可

採用其他已知的標準及協定來促進安全訊息通信，諸如極佳隱私性(Pretty Good Privacy™；PGP)、OpenPGP及其他此項技術已知的標準及協定。

安全傳訊協定(諸如S/MIME)依賴於公開與私密加密金鑰來提供可信度及完整性，並且依賴於一公開金鑰基礎結構(Public Key Infrastructure；PKI)來傳達提供鑑認及授權的資訊。使用一私密金鑰/公開金鑰對中之私密金鑰所加密的資料僅能使用該私密金鑰/公開金鑰對中之該相對應公開金鑰予以解密，反之亦然。私密金鑰資訊永不公開，而公開金鑰資訊則為共用。

例如，如果一寄件者想要以已加密形式將一訊息傳送至一收件者，則使用該收件者的公開金鑰來加密一訊息，接著僅限於使用該收件者的私密金鑰才能將訊息解密。或者，在某些編碼技術中，產生並使用一次會期金鑰(one-time session key)來加密一訊息之本文，典型係運用一種對稱式加密技術(例如，Triple DES)。接著，使用該收件者的公開金鑰來加密該會期金鑰(例如，使用諸如RSA等公開金鑰加密演算法)，接著僅限於使用該收件者的私密金鑰才能將該會期金鑰解密。然後，使用該已解密之會期金鑰來解密該訊息本文。可使用訊息標頭來指定擬解密該訊息所必須使用的特定加密方案。在變化版實施方式中，可使用以公開金鑰密碼編譯為基礎的其他加密技術。然而，在每一案例中，僅限於可使用該收件者的私密金鑰才能促進該訊息之解密，並且在此方式中，得以維持訊息之可信

度。

作為一進一步實例，一寄件者可使用一數位簽名來簽名於一訊息。一數位簽名係使用該收件者的私密金鑰所編碼之訊息的摘要(例如，該訊息的雜湊)，接著可將該摘要附加至該傳出之訊息。為了當接收時檢驗該訊息的數位簽名，該收件者使用相同於該寄收者的技術(例如，使用相同的標準雜湊演算法)，藉以獲得該接收到之訊息的摘要。該收件者也使用該寄件者的公開金鑰來解碼該數位簽名，以便獲得應是該接收到之訊息的匹配摘要。如果該接收到之訊息的該等摘要不匹配，則暗示著該訊息內容在傳輸期間有所變更及/或該訊息不是源自於檢驗所使用之公開金鑰的寄件者。數位簽名演算法之設計方式，係促使僅限於知道寄件者之私密金鑰的某人才能夠編碼一簽名，收件者將使用該寄件者的公開金鑰來解碼該簽名。因此，藉由以此方式來檢驗一數位簽名，得以維護該寄件者之鑑認及訊息完整性。

一已編碼之訊息可被加密、簽名或被加密及簽名。彼等作業中所使用之公開金鑰的確實性係使用憑證予以驗證。一憑證係由一憑證授權機構(CA)所發行的一數位文件。憑證係用來鑑認介於使用者與其公開金鑰之間的關聯性，並且最終提供使用者之公開金鑰的確實性方面的信任程度。憑證包含關於憑證持有者之資訊，連同憑證內容(典型係按照一已接受之標準(例如，X.509)予以格式化)。

請參閱圖5，圖中繪示一實例憑證鏈300。發行給「John

信任。

然而，在圖5所示的實例中，還需要憑證330以檢驗憑證310之信任狀態。憑證330是自我簽署的憑證，並且被稱為「根憑證」(root certificate)。因此，在憑證鏈300中，憑證320可被稱為一「中間憑證」(intermediate certificate)；假設對於一特定終端實體憑證，可決定一至該根憑證的鏈結，鏈結至一根憑證的任何既定憑證可包含零個、一個或多個中間憑證。如果憑證330是一受信任來源所發行的根憑證(例如，來自諸如Verisign或Entrust等大型憑證授權機構)，則由於憑證310鏈結至一受信任之憑證而可被視為受信任。這意謂著訊息的寄件者及收件者皆信任該根憑證330的來源。如果無法將一憑證鏈結至一受信任憑證，則該憑證可被視為「不受信任」。

憑證伺服器儲存關於憑證的資訊以及識別已撤銷之憑證的清單。可存取彼等憑證伺服器，藉以獲取憑證並且檢驗憑證確實性及廢止狀態。例如，可使用一輕量型目錄存取協定(Lightweight Directory Access Protocol；LDAP)伺服器來獲取憑證，以及可使用線上憑證狀態協定(Online Certificate Status Protocol；OCSP)伺服器來檢驗憑證廢止狀態。

標準電子郵件安全性協定典型地促進介於非行動計算裝置(例如，圖4之電腦262a、262b、遠端桌上型裝置)之間的安全訊息傳輸。請再次參考圖4，為了可從行動裝置100讀取從寄件者接收到的已簽名訊息，行動裝置100被調整以

儲存其他個體的憑證及相關聯之公開金鑰。典型地，例如，透過傳輸基座264將使用者電腦262a上所儲存的憑證從電腦262a下載至行動裝置100。

儲存在電腦262a上且載入至行動裝置100的憑證不限於相關聯於個體的憑證，而是還可包括(例如)發行至CA的憑證。使用者也可將儲存在電腦262a或行動裝置100上的某些憑證明確指定為「受信任」。因此，當使用者在行動裝置100上接收一憑證時，可藉由比對該憑證與行動裝置100上儲存的憑證來檢驗該憑證，並且指定為受信任，或以其他方式決定為已鏈結至一受信任憑證。

行動裝置100也可被調整，以儲存相關聯於該使用者的公開金鑰/私密金鑰對的該私密金鑰，促使行動裝置100的使用者可簽名於在行動裝置100上撰寫的傳出之訊息，並且對傳送至該使用者且以該使用者之公開金鑰所加密的訊息進行解密。例如，可透過傳輸基座264將私密金鑰從該使用者電腦262a下載至行動裝置100。較佳在電腦262a與行動裝置100之間交換該私密金鑰，促使該使用者可共同一個身份及一種存取訊息之方法。

使用者電腦262a、262b可從若干來源獲取憑證，以便儲存在使用者電腦262a、262b上及/或儲存在行動裝置上(例如，行動裝置100)。例如，彼等憑證來源可能是私有(例如，專用於一組織內部)或公共、可本機或遠端駐存，並且可從一組織的私有網路或透過網際網路進行存取。在圖4所示的實例中，相關聯於該組織的多個PKI伺服器280駐

存在LAN 250上。PKI伺服器280包括：一用於發行憑證的CA伺服器282；一用於搜尋及下載憑證(例如，對於組織內的個體)的LDAP伺服器284；以及一用於檢驗憑證之廢止狀態的OCSP伺服器286。

一使用者電腦262a可從LDAP伺服器284檢索憑證，例如，擬將彼等憑證經由傳輸基座264下載至行動裝置100。但是，在一變化版實施方式中，行動裝置100可直接存取LDAP伺服器284 (即，在此上下文中係「以無線方式」(over the air))，並且行動裝置100可透過一行動資料伺服器288來搜尋及檢索個體的憑證。同樣地，行動資料伺服器288可被調整以允許行動裝置100直接查詢OCSP伺服器286，藉以檢驗憑證的廢止狀態。

在變化版實施方式中，僅限於所選之PKI伺服器280才供行動裝置存取(例如，允許僅從一使用者電腦262a、262b下載憑證，同時允許從行動裝置100檢查憑證的廢止狀態)。

在變化版實施方式中，例如，也許按照IT政策，按一系統管理員所指定，僅限於註冊給特定使用者的行動裝置才能存取某些PKI伺服器280。

例如，其他憑證來源(圖中未繪示)可包括一Windows憑證儲存區、在LAN 250上或外部的另一安全憑證儲存區以及智慧卡。

現在請參考圖6，一已編碼訊息之實例的組成之方塊圖係一般地繪示為350，該已編碼訊息可能係由一訊息伺服

器(例如，圖4之訊息伺服器268)所接收。已編碼訊息350典型包括下列一或多項：一標頭部分352、一已編碼之本文部分354、選用之一或多個已編碼之附件356、一或多個已加密之會期金鑰358以及簽名和簽名相關之資訊360。例如，標頭部分352典型包括定址資訊，諸如「To」、「From」及「CC」位址，並且還可包括(例如)訊息長度指示項以及寄件者加密和簽名方案識別項。實際的訊息內容通常包括一訊息本文或資料部分354，並且也許包括一或多個附件356，該寄件者可使用一會期金鑰將訊息內容加密。如果使用一會期金鑰，則典型地使用每個收件者的各自公開金鑰來針對每個預定之收件者將該會期金鑰加密，並且被包含在該訊息的358之處。如果該訊息被簽名，則還包括一簽名和簽名相關之資訊360。例如，這可包括該寄件者的憑證。

僅以舉實例方式來提供如圖6所示之一已編碼訊息的格式，並且熟悉此項技術者應明白，可存在其他格式之已編碼訊息。例如，依據使用的特定傳訊方案，一已編碼訊息的組成可按不同於圖6所示之順序出現，並且一已編碼訊息可包括較少、額外或不同的組成，這可取決於該已編碼訊息是否被加密、簽名或被加密及簽名。

本發明具體實施例一般係針對一種系統及方法，其藉由儲存簽名檢驗作業中所採用的某資訊以供再次使用，促進更高效率檢驗憑證上的數位簽名。在建置憑證鏈過程中(如圖5之實例中之論述)，通常必須檢驗該鏈上之該等憑證

的數位簽名。對於在一使用者計算裝置上處理多個憑證，相同的數位簽名通常會遭受到一次以上檢驗。這可能對於形成含交互憑證的憑證鏈尤其普遍。下文參考圖7B來進一步詳細論述交互憑證。

請先參考圖7A，圖中繪示兩個實例憑證鏈的方塊圖。該等兩個實例憑證鏈被廣泛繪示為400a及400b。熟悉此項技術者應明白，係舉實例而提供憑證鏈400a及400b。具體而言，一交互憑證可包括少於或多於圖中所繪示之實例的憑證數量。

許多組織建置自己的CA，其明確發行憑證給其組織內的個體。發行給一特定組織內之個體的終端實體憑證不需要係由相關聯於該組織的一單一CA所發行。一終端實體憑證通常係由一CA階層架構(CA hierarchy)內的若干次級(subordinate)或中級(intermediate) CA之一所發行，而CA階層架構的最上層係該組織的一根CA (root CA)。此根CA可提供一擬作為一「信任錨點」(trust anchor)使用的自我簽署根憑證 – 這是用於驗證該組織內所發行之憑證的起點。

憑證鏈400a描繪用以驗證發行給「user1」(組織「ABC」內的一個體)之一憑證402a所形成的一實例憑證鏈。憑證402a係經由該組織之一根CA發行給該組織之一中級CA的一中級憑證406a鏈結至一自我簽署根憑證404a(由該根CA所發行且被該user1所信任)。例如，可能從組織ABC所維護的一LDAP伺服器(例如，圖4之LDAP伺服器

284)，搜尋及檢索該組織內所發行的憑證。

同樣地，憑證鏈400b描繪用以驗證發行給「user2」(一不同組織「XYZ」內的一個體)之一憑證402b所形成的一實例憑證鏈。憑證402b係經由一中級憑證406b鏈結至一自我簽署根憑證404b (由組織XYZ的一根CA所發行且被該user2所信任)。例如，可能從組織XYZ所維護的一LDAP伺服器，搜尋及檢索組織XYZ內所發行的憑證。

請考量一實例情況，其中組織ABC之user1接收到一來自組織XYZ之user2的已編碼之訊息。即使user2已將其憑證402b附加至該訊息，user1仍然無法僅僅使用該憑證來檢驗user2之憑證402b的信任狀態(假設user1尚未儲存user2之憑證402b且未將user2之憑證402b標記為受信任)。如果user1不信任來自組織XYZ的憑證，則由於user2之憑證402b未鏈結至一受信任之憑證，所以無法驗證user2之憑證402b。

為了促進不同組織之使用者之間的安全通信，可能希望允許在組織之間使用及信任憑證。可在兩組織之間執行一種稱為交互憑證的鑑認方法，其中某組織的一CA檢定另一組織的一CA。

用詞「交互憑證」可用來廣泛表示兩項作業。第一作業(典型地相對不常執行)係關於建置兩CA之間的一信任關係(例如，跨組織或在同一組織內)，其方式為在一稱為交互憑證的憑證中，由某CA來簽名於另一CA的公開金鑰。第二作業(典型地相對經常執行)涉及透過形成一包括至少一此種交互憑證的憑證鏈來檢驗一使用者的憑證。

現在請參考圖7B，圖中繪示連結兩個實例憑證鏈之交互憑證實例的方塊圖。在此實例中，繪示組織XYZ之根CA發行給組織ABC之根CA的一交互憑證410。同樣地，繪示組織ABC之根CA發行給組織XYZ之根CA的一交互憑證412。

圖7B之實例闡明兩個根CA之間彼此的交互憑證。但是，在變化版實施方式中，其他的交互憑證方法是可能的。例如，交互憑證可能係由某組織中的一次級CA發行給另一組織之根CA。舉進一步實例而言，一第一組織之一CA可發行一交互憑證給一第二組織之一CA，即使該第二組織不回覆發行一交互憑證給該第一組織。

再者，例如，可按一組織的IT政策之指示，來限制跨組織的憑證使用方式。舉例而言，某組織的IT政策可指示：僅限於為了處理已編碼之電子郵件訊息之用途，才能信任來自其他組織的憑證。而且，某組織的一發行方CA可撤銷交互憑證，以終止與其他組織之間的信任關係。這可促進更高效率控制介於跨不同組織之個體之間的安全電子郵件通信。

交互憑證促進介於已建置一信任關係之組織之個體之間的安全通信。請再次考量組織ABC之user1接收到一來自組織XYZ之user2的已編碼之訊息的情況。User1將能夠檢驗user2之憑證402b的信任狀態，其方式為檢索一鏈中的憑證，該鏈係從user2的憑證402b至user1之組織的一根CA且被user1所信任的根憑證404a。具體而言，如圖7B之實例

中所示，該鏈包括ABC的根憑證404a、交互憑證412、XYX的根憑證404b、中級憑證40b及user2的憑證402b。

對於user1檢驗user2之憑證402b的信任狀態，user1必須獲得憑證402b。這將按慣例附隨從user2至user1的訊息；但是，舉例而言，假使未提供憑證402b且未以其他方式儲存在user1的計算裝置上，則必須從組織XYZ所維護的一LDAP伺服器或其他認證伺服器檢索該憑證。再者，還必須檢索該鏈中的每個其餘憑證，以檢驗憑證402b的信任狀態。必須從ABC的LDAP伺服器、XYZ的LDAP伺服器或的LDAP伺服器user1可存取的其他LDAP伺服器檢索該鏈中的其他憑證(在此實例中，包括一根憑證及一交互憑證)。

如參考圖5、7A和7B之論述，當建置憑證鏈時，通常必須檢驗憑證上的發行方CA的數位簽名。當驗證憑證時也可能執行其他任務，例如，諸如檢查一憑證日期的有效性，或檢查可由一組織按照一IT政策所建置的其他驗證準則。

檢驗一憑證上之一數位簽名係一項處理程序，其需要發行方CA的公開金鑰。當一CA數位簽名於一憑證時，典型地使用該CA的私密金鑰來編碼憑證資訊(例如，包括憑證持有者的名字及公開金鑰，或透過套用一雜湊演算法所獲得之該資訊的一雜湊)。該發行方CA簽名於一憑證所使用的演算法典型係在該憑證中予以識別。接著，在類似於檢驗一使用者所簽名之一訊息的數位簽名中採用的方式中，可藉由使用CA的公開金鑰來解碼已編碼之資訊或雜湊，

以及分別比較該結果與所預期之憑證資訊或其雜湊，來檢驗一憑證上的CA之公開金鑰。一成功匹配指示出該CA已檢驗該憑證持有者的公開金鑰可被有效地繫結至該憑證持有者，並且建議如果該CA受到信任，則可信任該憑證持有者的公開金鑰。

檢驗憑證簽名可能是耗時且高成本(例如，就計算資源使用量而論)的處理程序，尤其是在較小型裝置(例如，諸如行動裝置)上執行檢驗時。本發明具體實施例一般係針對一種系統及方法，其藉由儲存簽名檢驗作業中所採用的某資訊以供再次使用，促進更高效率檢驗憑證上的數位簽名。

在至少一具體實施例中，使已發行一特定憑證的一CA之一或多個公開金鑰相關聯於該憑證，且予以快取或儲存。如上文所述，當嘗試檢驗一CA所發行之一憑證上的一數位簽名時，需要該CA的公開金鑰。但是，可存在有似乎屬於該同一CA的多個憑證(各憑證含有一附加之公開金鑰)。例如，如果數個憑證具有相同或相似的主旨資料(即，識別憑證持有者的憑證資料)，或如果CA已發行多個公開金鑰(某些公開金鑰可能不再有效)，則可能發生此情況。據此，追蹤曾經用來成功檢驗一特定憑證的公開金鑰可能是有所助益。

請參考圖8，在本發明一具體實施例中之檢驗憑證上之數位簽名之方法中的步驟之流程圖係一般地繪示為420。

在本發明一項具體實施例中，該方法的至少某些步驟係

由在一行動裝置所駐存及執行的一憑證驗證應用程式予以執行。在變化版具體實施例中，該憑證驗證應用程式可能係駐存在除一行動裝置外的一計算裝置上及在該計算裝置上執行。再者，該憑證驗證應用程式不需要係一獨立的應用程式，並且該憑證驗證應用程式的功能可被實作在行動裝置或其他計算裝置上所駐存及執行的一或多個應用程式中。

一般而言，在方法420中，當在成功檢驗一憑證上的數位簽名過程中使用一既定公開金鑰時，該公開金鑰的一複本被快取，或以其他方式儲存在一記憶體儲存區中。例如，該公開金鑰可能係連同相關聯於該憑證的憑證資料一起予以儲存，或該公開金鑰被儲存在一調適用以儲存成功簽名檢驗中所採用之公開金鑰的分開記憶體儲存區(例如，一查詢表)中。當進行一後續嘗試以檢驗該同一憑證上之該數位簽名時，不執行至少需要使用一公開金鑰來解碼某資料的高費用簽名檢驗作業，而是起始時再比較已用於檢驗該數位簽名的該公開金鑰與該儲存之公開金鑰。如果該等公開金鑰匹配，則由於擬使用的公開金鑰匹配先前在簽名檢驗作業中已成功使用的一金鑰，所以該檢驗將被視為成功。這是考量到不需要對於該同一數位簽名來再次執行一實際的簽名檢驗作業。據此，至少某些後續簽名檢驗作業可被更高效率(例如，位元組陣列)比較作業予以取代。下文進一步說明這方法420的步驟。

在步驟430，起始檢驗一憑證上的一數位簽名(例如，藉

由憑證驗證應用程式)。舉例而言，當建置憑證鏈以便驗證一使用者所接收的特定憑證時，可能執行檢驗憑證上的數位簽名(例如，如參考圖5所論述示之檢驗附加至一所接收訊息之憑證的信任狀態)。在此具體實施例中，正被檢驗的憑證上之數位簽名係已發行各自憑證的憑證授權機構之數位簽名。如上文所述，在一簽名檢驗作業中，需要發行該憑證的該憑證授權機構之一公開金鑰。在此步驟，如果該憑證授權機構之(多個)憑證及(多個)尚未被儲存在行動裝置或其他計算裝置上中的一憑證儲存區中，也許需要(例如，從一LDAP伺服器)檢索該憑證授權機構之(多個)憑證及(多個)金鑰。

在步驟440，對於一既定公開金鑰，在使用此公開金鑰來執行簽名檢驗作業之前，先決定先前是否曾經使用此公開金鑰而成功檢驗該主題憑證上的數位簽名。如上文所述，可完成此項決定的方式為，比較先前成功檢驗該主題憑證上之數位簽名所使用的該憑證發行者的一儲存之公開金鑰(如果該儲存之公開金鑰存在，如在步驟470中儲存於快取區或其他記憶體儲存區中之公開金鑰)與即將用於檢驗該數位簽名的公開金鑰，並且接著決定是否有一匹配。在此具體實施例中，由於僅限於成功檢驗嘗試中所採用之公開金鑰才被儲存在快取區或其他記憶體儲存區，所以如果一匹配被決定，則將建議該主題憑證上的數位簽名已曾經予以成功檢驗。

如果先前使用該既定公開金鑰未曾成功檢驗該主題憑證

上的數位簽名，則在步驟450，以已知方式使用此公開金鑰來檢驗該數位簽名。根據此具體實施例，如果依照步驟460之決定係使用此公開金鑰而成功檢驗該簽名，則在步驟470，在此成功檢驗中所使用的該公開金鑰被儲存在快取區或其他記憶體儲存區，以供未來使用。例如，在步驟470儲存的該公開金鑰可能係連同相關聯於該主題憑證的資料一起予以儲存，或儲存在按憑證編索引的一公開金鑰中央記憶體儲存區(例如，一查詢表)中(例如，藉由連同該公開金鑰一起儲存該憑證的發行者名稱及序號)。

另一方面，如果按步驟440之決定係，先前使用該既定公開金鑰曾經成功檢驗該主題憑證上的數位簽名，則在步驟480，提供該檢驗係成功的一指示。其完成方式為，不執行一至少需要使用一公開金鑰來解碼某資料的實際簽名檢驗作業，藉以使簽名檢驗處理程序更具效率。這可有助於節省電池電力且更具使用者吸引力，例如，尤其是對於如行動裝置等小型裝置。

對於額外公開金鑰，可重複方法420的彼等步驟。

現在請參考圖8B，在本發明另一具體實施例中之檢驗憑證上之數位簽名之方法中的步驟之流程圖係一般地繪示為420b。

方法420b類似於方法420，除外之處在於，與將成功簽名檢驗中採用的公開金鑰儲存快取區或其他記憶體儲存區中的方法420形成對比，在方法420b中，任何簽名檢驗嘗試(無論成功與否)中使用的公開金鑰係連同檢驗嘗試結果

一起儲存在快取區或其他記憶體儲存區中。

一般而言，在方法420b中，當在檢驗一憑證上的數位簽名過程中使用一既定公開金鑰時，該公開金鑰的一複本係連同該作業之結果一起予以快取，或以其他方式儲存在一記憶體儲存區中。例如，該公開金鑰及相關聯之結果可能係連同相關聯於該憑證的憑證資料一起予以儲存，或該公開金鑰及相關聯之結果被儲存在一分開記憶體儲存區(例如，一查詢表)中。當進行一後續嘗試以使用該既定公開金鑰來檢驗該同一憑證上之該數位簽名的時，不執行至少需要使用該公開金鑰來解碼某資料的高費用簽名檢驗作業，而是起始時再比較已用於檢驗該數位簽名的該公開金鑰與該(等)儲存之公開金鑰。如果該既定公開金鑰匹配於一儲存之公開金鑰匹配，則依據相關聯於該儲存之公開金鑰的所儲存之結果，該目前的檢驗嘗試將被視為成功或未成功。如果該儲存之結果指示出，先前用該儲存之公開金鑰的檢驗嘗試係成功，則該目前的檢驗嘗試將被視為成功。如果該儲存之結果指示出，先前用該儲存之公開金鑰的檢驗嘗試係未成功，則該目前的檢驗嘗試將被視為未成功。據此，以其他方式需要使用公開金鑰來解碼某資料的後續簽名檢驗作業可被更高效率(例如，位元組陣列)比較作業予以取代。

在步驟430，起始檢驗一憑證上的一數位簽名(例如，藉由憑證驗證應用程式)，如參考方法420所論述。

在步驟440b，對於一既定公開金鑰，在使用此公開金鑰

來執行簽名檢驗作業之前，先決定先前是否曾經使用此公開金鑰來檢驗該主題憑證上的數位簽名。如上文所述，可完成此項決定的方式為，比較先前檢驗該主題憑證上之數位簽名所使用的該憑證發行者的一公開金鑰(如果該公開金鑰存在，如在步驟470中儲存於快取區或其他記憶體儲存區中之公開金鑰)與即將用於檢驗該數位簽名的公開金鑰，並且決定是否有一匹配。如果一匹配被決定，則將建議先前已進行一檢驗該主題憑證上的數位簽名的嘗試。

如果先前未進行一檢驗該主題憑證上的數位簽名的嘗試，則在步驟430，以已知方式來執行一簽名檢驗作業，類似於如參考方法420所論述。根據此具體實施例，在步驟470b，該檢驗中所使用的該公開金鑰及該檢驗嘗試之結果(即，成功或未成功檢驗該數位簽名的一指示項)皆被儲存在快取區或其他記憶體儲存區，以供未來使用。例如，在步驟470儲存的該公開金鑰及結果皆可能係連同相關聯於該主題憑證的資料一起予以儲存，或儲存在按憑證編索引的一公開金鑰中央記憶體儲存區(例如，一查詢表)中(例如，藉由連同該公開金鑰一起儲存該憑證的序號)。

如果按步驟440b之決定係，先前使用該既定公開金鑰曾經成功檢驗該主題憑證上的數位簽名，則在步驟472，從該快取區或其他記憶體儲存區檢索先前使用此金鑰的檢驗嘗試結果，並且決定該儲存之結果是否指示出先前使用此金鑰的檢驗嘗試係成功。若是，則在步驟480，提供該目前之檢驗係成功的一指示；若否，則步驟490，提供該目

前之檢驗係未成功的一指示。

對於額外公開金鑰，可重複方法420b的彼等步驟。

不執行一至少需要使用一既定公開金鑰來解碼某資料的簽名檢驗作業，而是使用先前檢驗嘗試結果來決定是否使用此公開金鑰的一檢驗應為未成功，藉以使簽名檢驗處理程序更具效率。具體而言，如果一使用者要求使用相同之無法公開金鑰，來檢驗一憑證之數位簽名多次，則至少需要使用該公開金鑰來解碼某資料的高費用簽名檢驗作業僅需要被執行一次，並且後續嘗試將在執行一相對高效率(例如，位元組陣列)比較作業之後立即失敗。這可進一步有助於節省電池電力且更具使用者吸引力，例如，尤其是對於如行動裝置等小型裝置。

熟悉此項技術者應明白，在變化版具體實施例中，若有需要，除了上文所述之公開金鑰及檢驗嘗試結果以外，還可在快取區或其他記憶體儲存區中儲存其他資訊。

在本發明一變化版具體實施例中，快取區或其他記憶體儲存區中所儲存的公開金鑰及其他資訊(例如，檢驗嘗試結果)，可僅被允許在一有限持續時期期間內運用於公開金鑰比較，之後，所儲存的公開金鑰及其他資訊可被視為過期且從快取區或其他記憶體儲存區予以刪除。這可為了安全性用途而完成，促使必須不時地重新執行一至少需要使用一公開金鑰來解碼某資料的實際簽名檢驗作業。例如，可依照IT政策來設定此持續時期。同樣地，在本發明另一變化版具體實施例中，快取區或其他記憶體儲存區中

所儲存的某些或所有公開金鑰及其他資訊可被標記為過期，或按一使用者或系統管理員的手動指示予以刪除，促使必須重新執行簽名檢驗作業。例如，為了更提高安全性，還可執行驗證作業，以確保公開金鑰(例如，先前成功檢驗一憑證簽名的公開金鑰)在儲存後未變成無效。

在本發明多項具體實施例中，一種用於檢驗憑證上的數位簽名之方法的步驟可被提供為電腦可讀媒體(其可包括傳輸型媒體)上所儲存的可執行之軟體指令。

已關於數項具體實施例來說明本發明。但是，熟悉此項技術者應明白，可進行其他變化及修改，而不會脫離如本發明所隨附之申請專利範圍中定義的本發明範疇。

【圖式簡單說明】

為了最佳理解本發明具體實施例並且更清楚展示實施方式，【實施方式】將以舉實例方式且參考附圖來進行說明，圖式中：

圖1繪示在一實例實施方式中之一行動裝置的方塊圖；

圖2繪示圖1所示之行動裝置的通信子系統組件之方塊圖；

圖3繪示一無線網路之一節點的方塊圖；

圖4繪示在一實例組態中之一主機系統的組件之方塊圖；

圖5繪示一憑證鏈實例的方塊圖；

圖6繪示一已編碼訊息之實例的組成之方塊圖；

圖7A繪示兩個實例憑證鏈的方塊圖；

圖7B繪示連結圖7A之該等憑證鏈之交互憑證的方塊圖；

圖8A繪示在本發明一具體實施例中之檢驗一憑證上的一數位簽名之方法中的步驟之流程圖；以及

圖8B繪示在本發明另一具體實施例中之檢驗一憑證上的一數位簽名之方法中的步驟之流程圖。

【主要元件符號說明】

100	行動裝置
102	微處理器
104	通信子系統
106	隨機存取記憶體(RAM)
108	快閃記憶體
110	顯示器
112	輔助輸入/輸出(I/O)子系統
114	序列埠
116	鍵盤
118	揚聲器
120	麥克風
122	短矩離通信子系統
124	其它裝置子系統
126	SIM卡
128	SIM介面
130	可充電式電池
132	電池介面

150	接收器
152	發射器
154, 156	天線元件
158	本機振盪器(LO)
160	數位訊號處理器(DSP)
200	無線網路
202	節點
204	基地台控制器(BSC)
206	塔台
208	封包控制單元(PCU)
210	行動交換中心(MSC)
212	本籍位置暫存器(Home Location Register；HLR)
214	訪客位置暫存器(Visitor Location Registry；VLR)
216	伺服GPRS支援節點(Serving GPRS Support Node；SGSN)
218	閘道GPRS支援節點(Gateway GPRS Support Node；GGSN)
220	動態主機組態協定(Dynamic Host Configuration Protocol；DHCP)
222	公共交換電話網路(PSTN)
224	公共或私用網路(網際網路)
250	主機系統(LAN)

260	LAN連接
262a, 262b	使用者電腦
264	傳輸基座(cradle)
266	代理(proxy)伺服器
268	訊息伺服器
270	無線通信支援組件
272	訊息管理伺服器
280	PKI伺服器
282	CA伺服器
284	LDAP伺服器
286	OCSP伺服器
288	行動資料伺服器
300	憑證鏈
310	憑證(終端實體憑證)
312	憑證持有者
314	憑證發行者
316	發行者的數位簽章
318	憑證持有者的公開金鑰
320	憑證
330	憑證
350	已編碼訊息
352	標頭部分
354	已編碼之本文部分
356	已編碼之附件

358	已加密之會期金鑰
360	簽章和簽章相關之資訊
400a, 400b	憑證鏈
402a, 402b	憑證
404a, 404b	自我簽署根憑證
406a, 406b	中級憑證
410, 412	交互憑證

五、中文發明摘要：

一種用於檢驗一憑證上的一數位簽名之系統及方法，其可運用在處理已編碼之訊息。在一具體實施例中，當在一簽名檢驗作業中成功檢驗一數位簽名時，快取用於檢驗該數位簽名的公開金鑰。當進行一後續嘗試以檢驗該數位簽名時，比較擬用於檢驗該數位簽名的該公開金鑰與該快取之金鑰。如果該等金鑰匹配，則可以成功檢驗該數位簽名，而不需要執行一簽名檢驗作業，在該簽名檢驗作業中，使用該公開金鑰來解碼某些資料。

六、英文發明摘要：

十一、圖式：

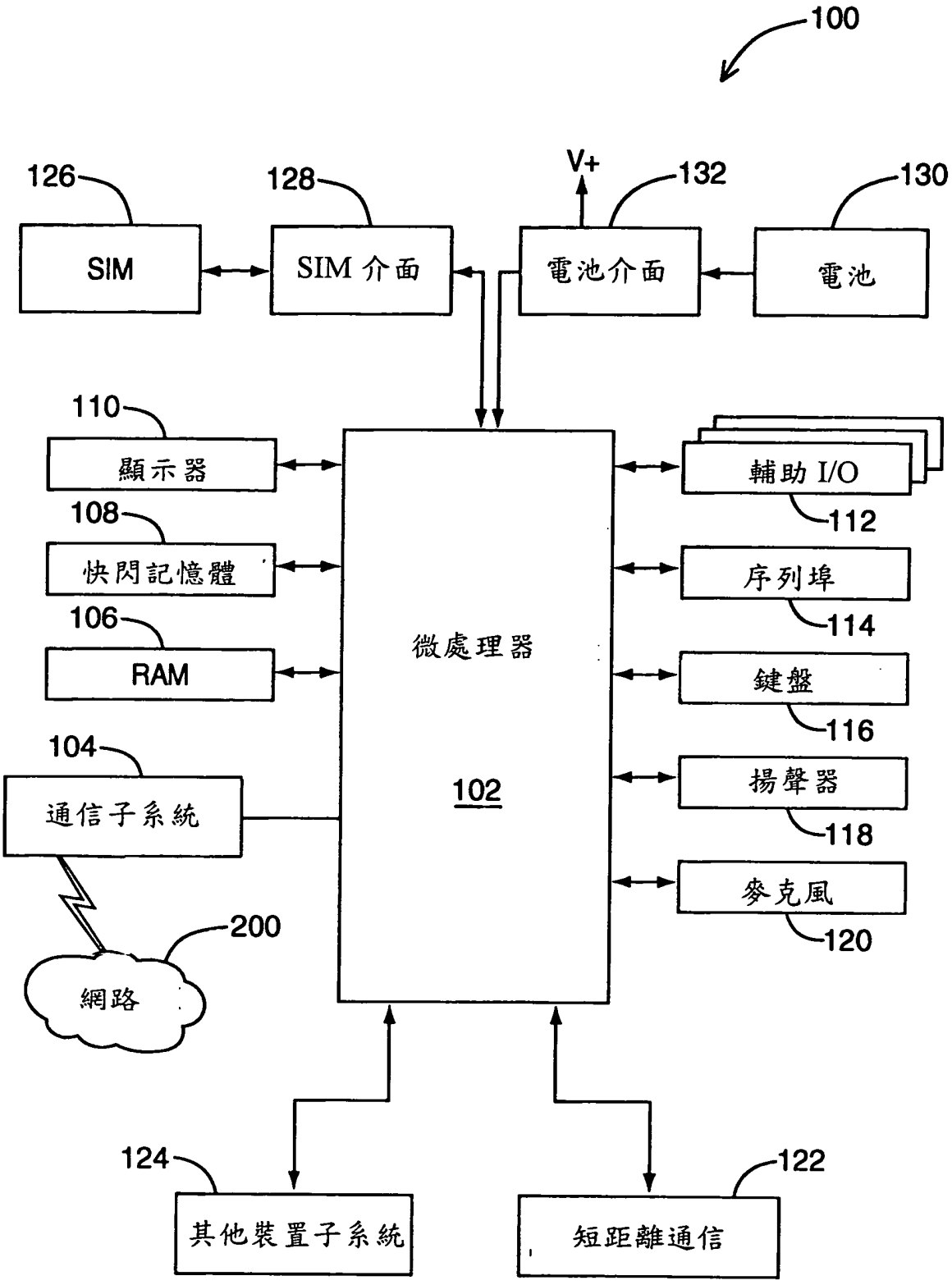
100
126
SIM
128
SIM 介面
V+
132
電池介面
130
電池
110
顯示器
108
快閃記憶體
106
RAM
104
通信子系統
200
網路
微處理器
102
輔助 I/O
112
序列埠
114
鍵盤
116
揚聲器
118
麥克風
120
124
其他裝置子系統
122
短距離通信

圖 1

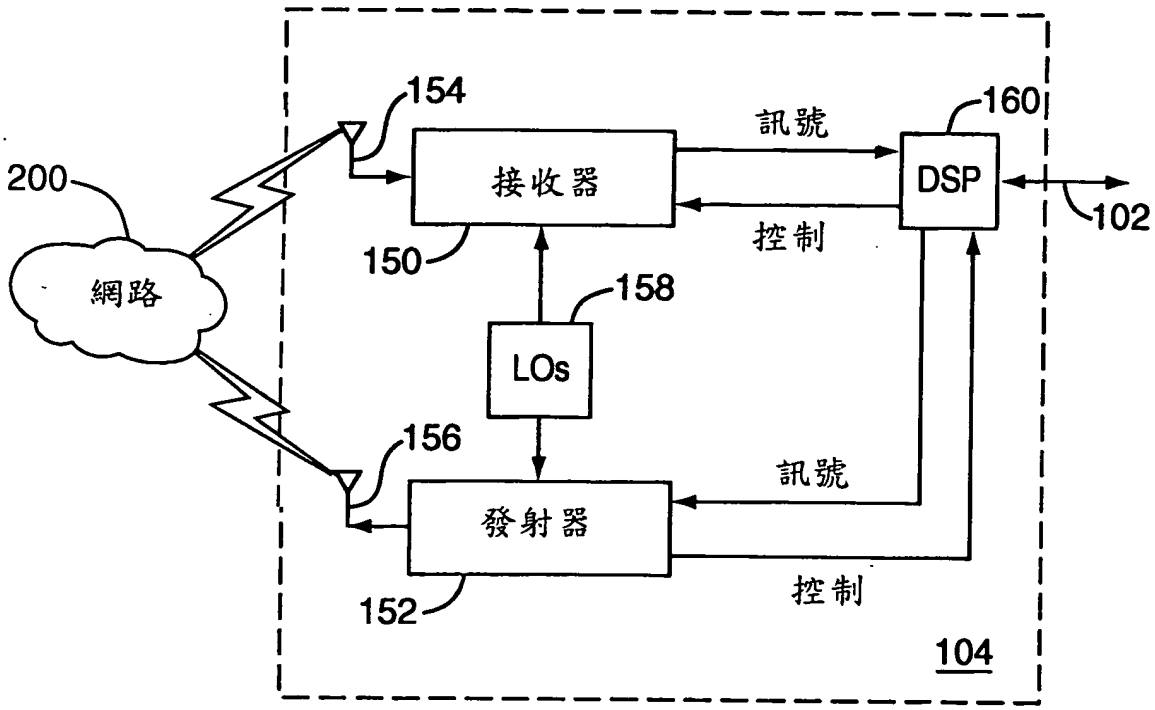

圖 2

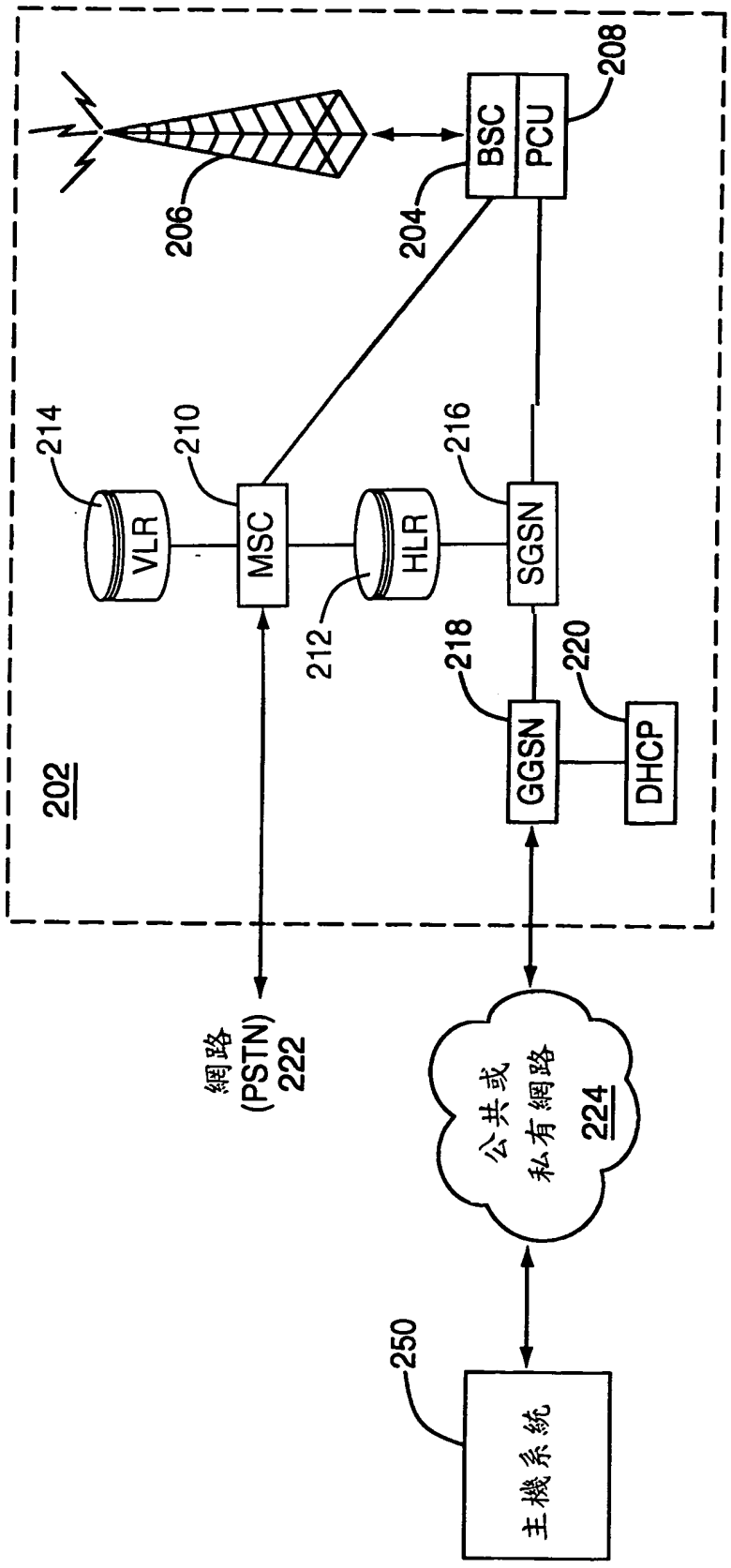
202
206
204
208
BSC
PCU
214
210
216
VLR
MSC
HLR
SGSN
212
218
220
GGSN
DHCP
網路
(PSTN)
222
公共或
私有網路
224
250
主機系統

圖 3

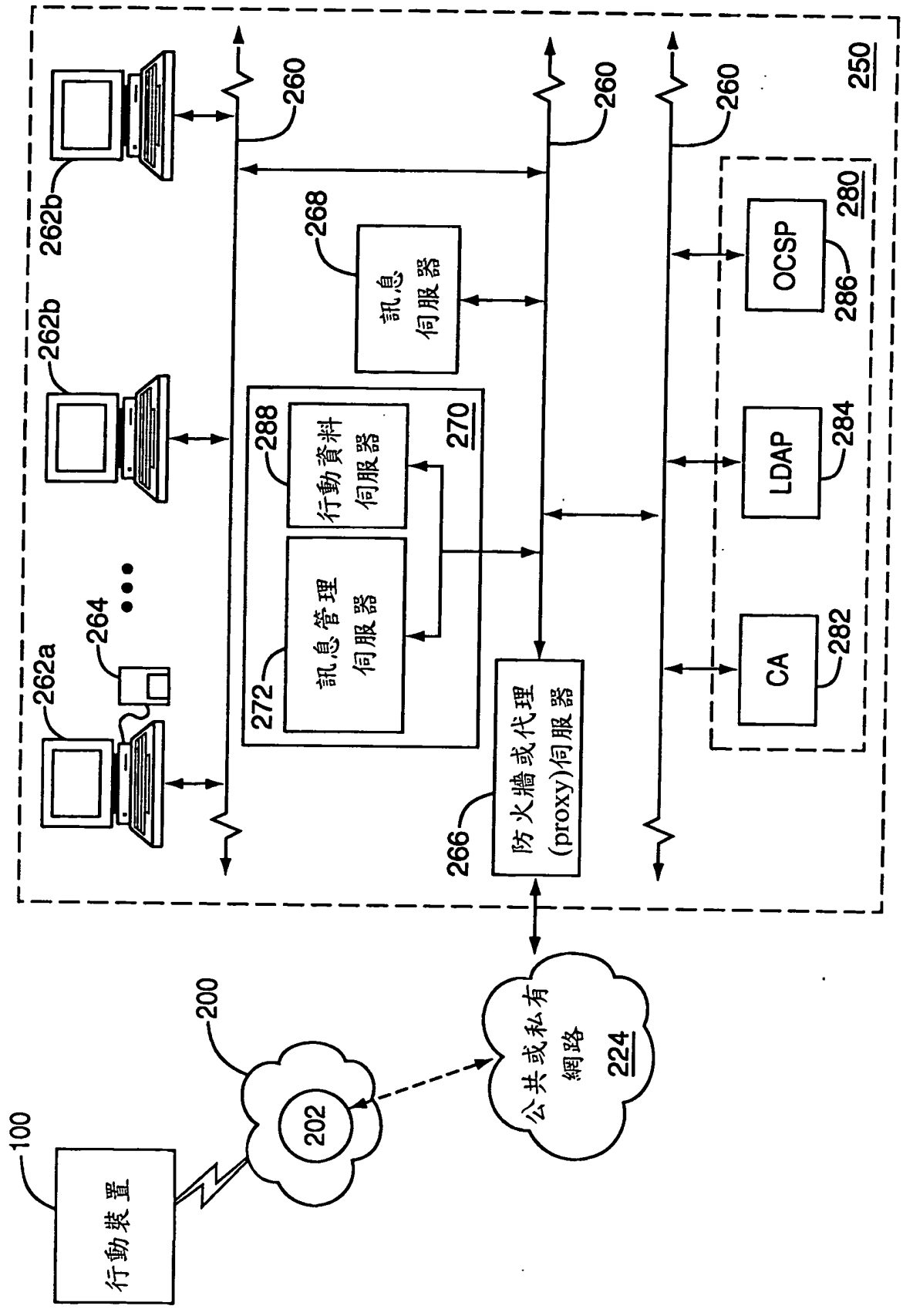
行動裝置
100
200
202
公共或私有網路
224
防火牆或代理(proxy)伺服器
266
訊息管理伺服器
272
行動資料伺服器
288
270
訊息伺服器
268
260
262a
262b
262b
262b
264
250
280
OCSP
286
LDAP
284
CA
282

圖 4

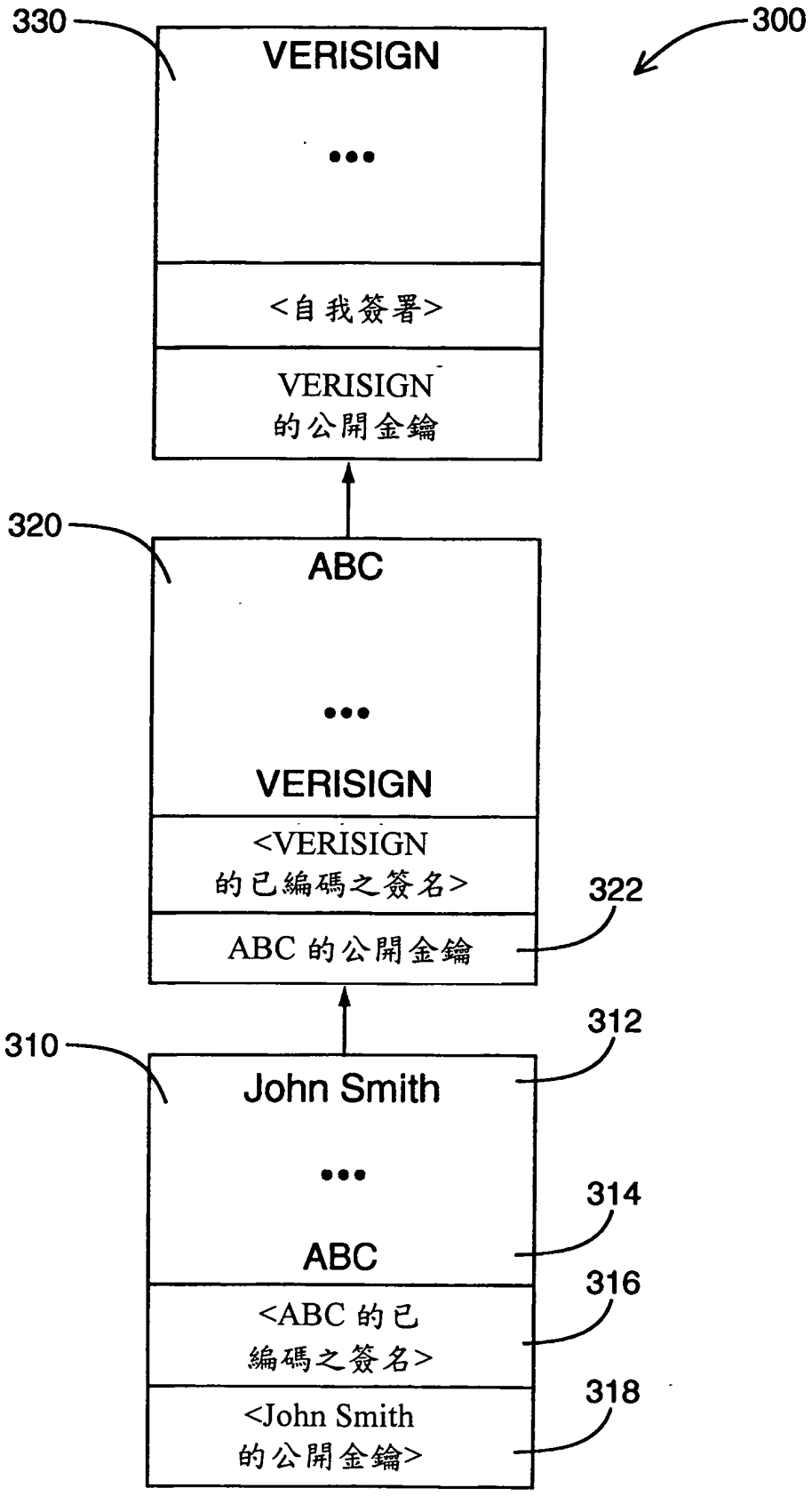
330
300
VERISIGN
•••
<自我簽署>
VERISIGN
的公開金鑰
320
ABC
•••
VERISIGN
<VERISIGN
的已編碼之簽名>
322
ABC 的公開金鑰
312
310
John Smith
•••
314
ABC
316
<ABC 的已
編碼之簽名>
318
<John Smith
的公開金鑰>

圖 5

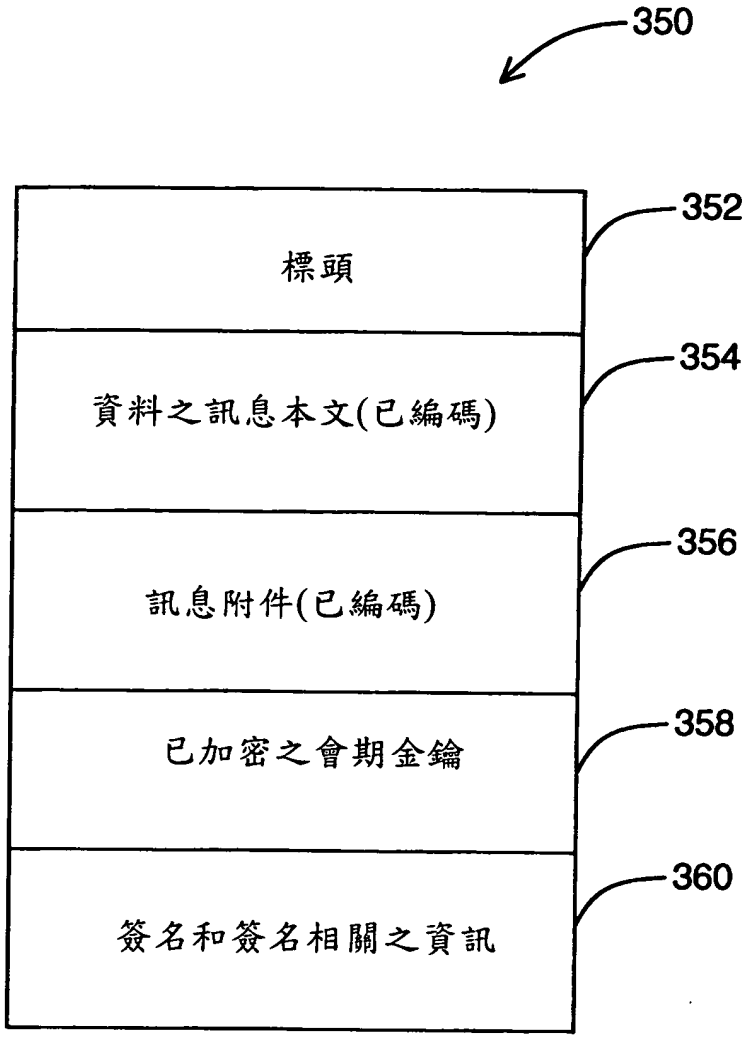
350
標頭
352
資料之訊息本文(已編碼)
354
訊息附件(已編碼)
356
已加密之會期金鑰
358
簽名和簽名相關之資訊
360

圖 6

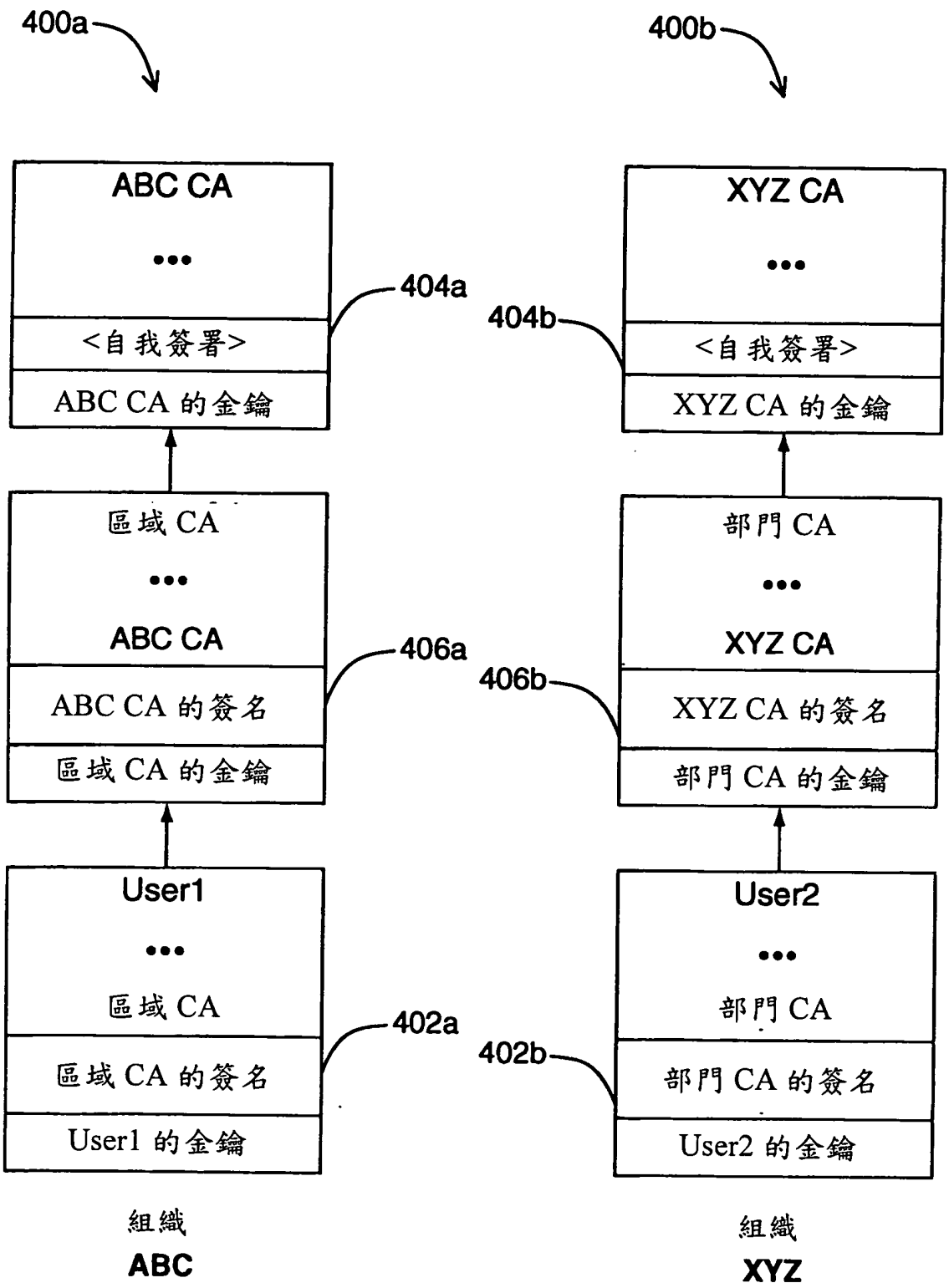
400a
400b
ABC CA
•••
<自我簽署>
ABC CA 的金鑰
404a
404b
XYZ CA
•••
<自我簽署>
XYZ CA 的金鑰
區域 CA
•••
ABC CA
ABC CA 的簽名
區域 CA 的金鑰
406a
406b
部門 CA
•••
XYZ CA
XYZ CA 的簽名
部門 CA 的金鑰
User1
•••
區域 CA
區域 CA 的簽名
User1 的金鑰
402a
402b
User2
•••
部門 CA
部門 CA 的簽名
User2 的金鑰
組織
ABC
組織
XYZ

圖 7A

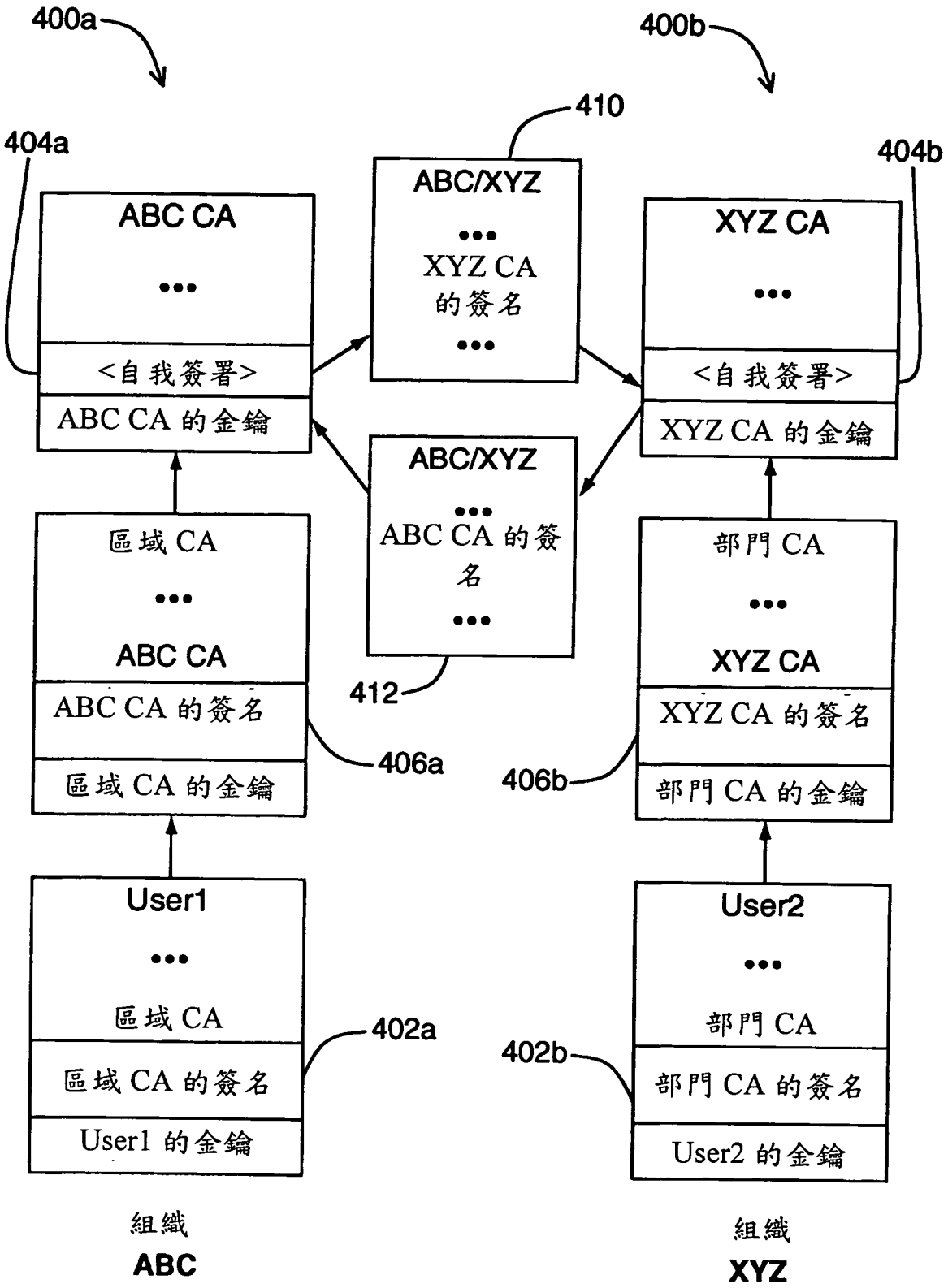
400a
400b
410
404a
404b
ABC/XYZ
•••
XYZ CA
的簽名
•••
ABC CA
•••
<自我簽署>
ABC CA 的金鑰
XYZ CA
•••
<自我簽署>
XYZ CA 的金鑰
ABC/XYZ
•••
ABC CA 的簽
名
•••
412
區域 CA
•••
ABC CA
ABC CA 的簽名
區域 CA 的金鑰
406a
部門 CA
•••
XYZ CA
XYZ CA 的簽名
部門 CA 的金鑰
406b
User1
•••
區域 CA
區域 CA 的簽名
User1 的金鑰
402a
User2
•••
部門 CA
部門 CA 的簽名
User2 的金鑰
402b
組織
ABC
組織
XYZ

圖 7B

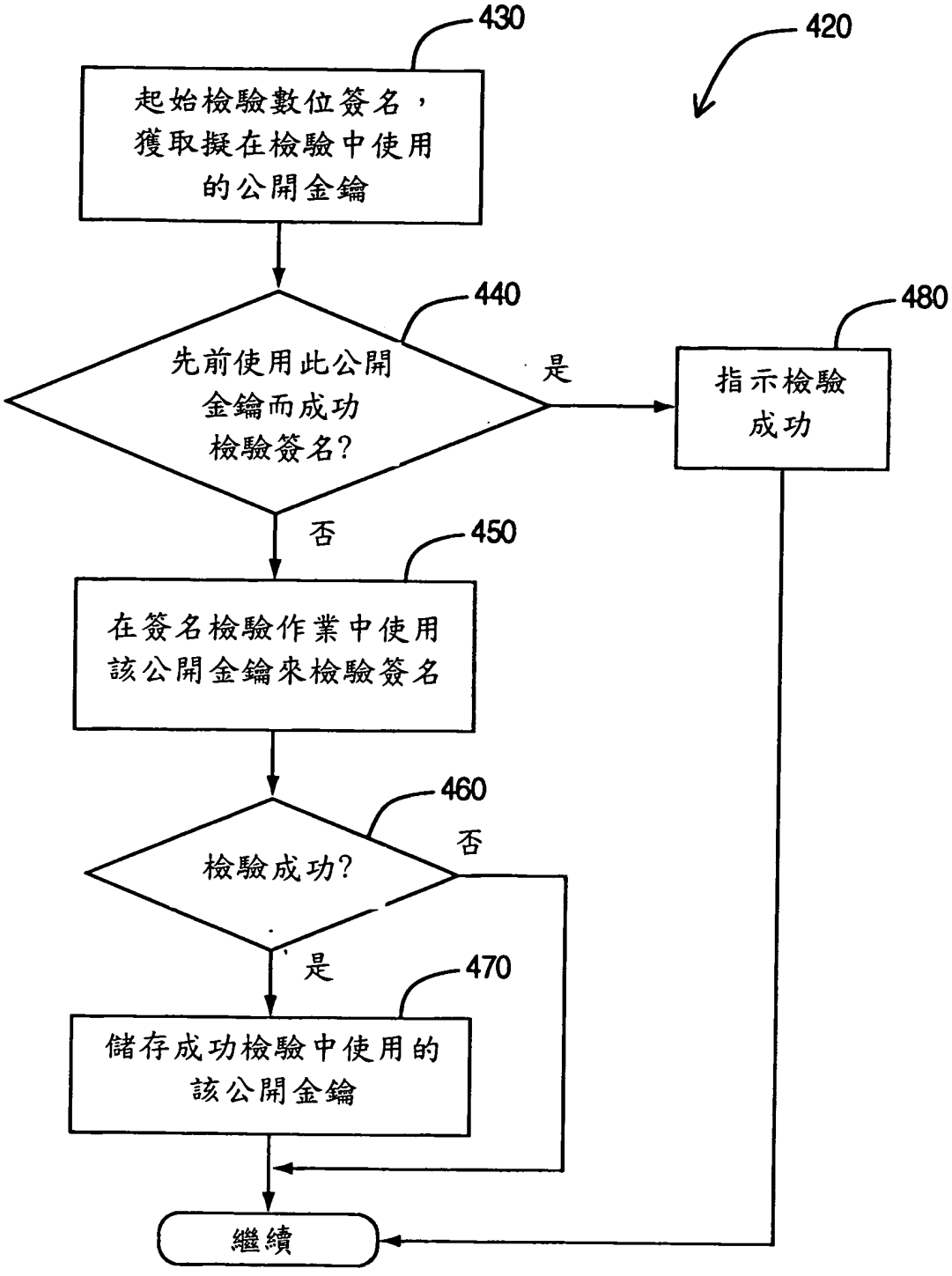
420
430
起始檢驗數位簽名，
獲取擬在檢驗中使用
的公開金鑰
440
先前使用此公開
金鑰而成功
檢驗簽名?
是
480
指示檢驗
成功
否
450
在簽名檢驗作業中使用
該公開金鑰來檢驗簽名
460
檢驗成功?
否
是
470
儲存成功檢驗中使用的
該公開金鑰
繼續

圖 8A

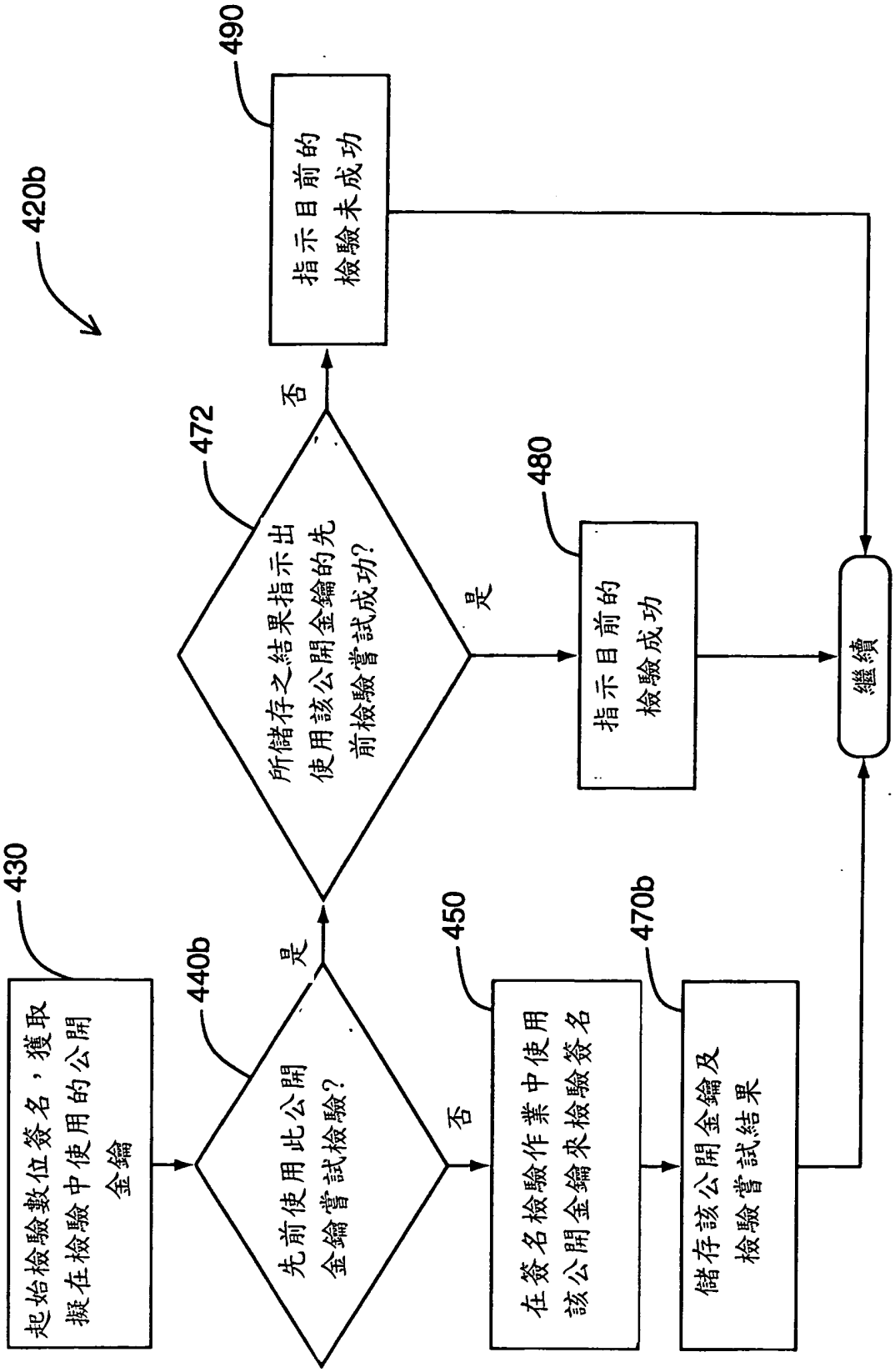
420b
430
起始檢驗數位簽名，獲取擬在檢驗中使用的公開金鑰
440b
先前使用此公開金鑰嘗試檢驗?
是
否
472
所儲存之結果指示出使用該公開金鑰的先前檢驗嘗試成功?
是
否
480
指示目前的檢驗成功
490
指示目前的檢驗未成功
450
在簽名檢驗作業中使用該公開金鑰來檢驗簽名
470b
儲存該公開金鑰及檢驗嘗試結果
繼續

圖 8B

七、指定代表圖：

(一)本案指定代表圖為：第（8B）圖。

(二)本代表圖之元件符號簡單說明：

(無元件符號說明)

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

(無)

Smith」的憑證310是一發行給一個體之憑證的實例，可稱為一終端實體憑證(end entity certificate)。終端實體憑證310典型地識別該憑證持有者312 (即，在此實例中為John Smith)及憑證的發行者314，並且包括該發行者的一數位簽名316及該憑證持有者的公開金鑰318。憑證310典型地還包括其他識別該憑證持有者的資訊及屬性(例如，電子郵件位址、組織名稱、組織單位名稱、位置等等)。當個體撰寫一擬傳送至一收件者的訊息時，按慣例連同該訊息包括該個體的憑證310。

對於一受信任之公開金鑰，其發行組織必須受到信任。介於一受信任CA與一使用者之公開金鑰之間的關係可藉由一連串相關憑證(也稱為一憑證鏈)予以表示。可遵循該憑證鏈來決定一憑證的有效性(validity)。

舉例而言，在圖5所示之實例憑證鏈300中，一宣稱係由John Smith所傳送之訊息的收件者，可能想要檢驗附加至該接收到之訊息的憑證310之信任狀態。例如，為了在一收件者的計算裝置(例如，圖4之使用者電腦262a)上檢驗憑證310之信任狀態，獲得發行者ABC的憑證320，並且用來檢驗該憑證310確實係由發行者ABC所簽名。憑證320可能已經儲存在該計算裝置的一憑證儲存區中，或可能需要從一憑證來源(例如，圖4之LDAP伺服器284，某其他公共或私有LDAP伺服器)。如果憑證320已經儲存在該收件者的計算裝置中，並且該憑證已被該收件者指定為受信任，則由於憑證310鏈結至一已儲存、受信任之憑證而被視為受

98年8月12日修正替換頁

十、申請專利範圍：

1. 一種用於在一計算裝置上檢驗一憑證上的一數位簽名之方法，該方法包括下列步驟：

a) 使用相關聯於該憑證之一發行者的一第一公開金鑰，執行一對於該數位簽名的第一簽名檢驗作業；

b) 決定在該第一簽名檢驗作業中是否成功檢驗該數位簽名；

c) 將該第一公開金鑰儲存於一記憶體儲存區中；

d) 接收一要求，以使用相關聯於該憑證之一發行者的一第二公開金鑰，執行一對於該數位簽名的第二簽名檢驗作業；

e) 比較該第二公開金鑰與該記憶體儲存區中所儲存的該第一公開金鑰，以決定該第一公開金鑰與該第二公開金鑰是否匹配；以及

f) 如果在該第一簽名檢驗作業中成功檢驗該數位簽名，並且如果在該比較步驟決定一匹配，則回應該要求而指示成功檢驗該數位簽名，藉以不需要執行該第二簽名檢驗作業。

2. 如請求項1之方法，其中只有在該第一簽名檢驗作業中成功檢驗該數位簽名，才會在該儲存步驟中將該第一公開金鑰儲存在該記憶體儲存區中。

3. 如請求項1之方法，其中該儲存步驟進一步包括：儲存一指示在該第一簽名檢驗作業中是否成功檢驗該數位簽名的結果，並且其中在該指示步驟，使用該結果來決定

在該第一簽名檢驗作業中是否成功檢驗該數位簽名。

4. 如請求項3之方法，進一步包括如果在該指示步驟中，決定在該第一簽名檢驗作業中未成功檢驗該數位簽名，並且如果在該比較步驟決定一匹配，則回應該要求而指示未成功檢驗該數位簽名之步驟。

5. 如請求項1、2或4之方法，其中該計算裝置是一行動裝置。

6. 一種用於在一計算裝置上執行之電腦可讀取媒體，其包括儲存於該電腦可讀取媒體上之複數個指令，該等指令係用於執行如請求項1至5中任一項之方法的該等步驟。

7. 一種用於檢驗一憑證上的一數位簽名之系統，包括至少一計算裝置，其中在該至少一計算裝置的一計算裝置上執行及駐存一憑證驗證應用程式，其中該憑證驗證應用程式被程式化以執行如請求項1至5中任一項之方法中的步驟。

8. 一種用於檢驗一憑證上的一數位簽名之計算裝置，包括：

a) 一第一驗證構件，用以使用相關聯於該憑證之一發行者的一第一公開金鑰，執行一對於該數位簽名的第一簽名檢驗作業；

b) 一第一決定構件，用以決定在該第一簽名檢驗作業中是否成功檢驗該數位簽名；

c) 一儲存構件，用以儲存該第一公開金鑰；

d) 一第二驗證構件，用以接收一要求，以使用相關聯於

該憑證之一發行者的一第二公開金鑰，執行一對於該數位簽名的第二簽名檢驗作業；

e) 一比較構件，用以比較該第二公開金鑰與該儲存構件中所儲存的該第一公開金鑰，以決定該第一公開金鑰與該第二公開金鑰是否匹配；以及

f) 一第一回應構件，如果在該第一簽名檢驗作業中成功檢驗該數位簽名，並且如果在該比較構件決定一匹配，則回應該要求而指示成功檢驗該數位簽名，藉以不需要執行該第二簽名檢驗作業。

9. 如請求項8之計算裝置，其中只有在該第一簽名檢驗作業中成功檢驗該數位簽名，才會將該第一公開金鑰儲存在該儲存構件中。

10. 如請求項8之計算裝置，其中該儲存構件進一步包括一第二決定構件，用以儲存一指示在該第一簽名檢驗作業中是否成功檢驗該數位簽名的結果，並且在其中，使用該結果來決定在該第一簽名檢驗作業中是否成功檢驗該數位簽名。

11. 如請求項10之計算裝置，進一步包括一第二回應構件，如果在該第二決定構件中，決定在該第一簽名檢驗作業中未成功檢驗該數位簽名，並且如果在該比較構件中決定一匹配，則回應該要求而指示未成功檢驗該數位簽名。

12. 如請求項8、9或11之計算裝置，其中該計算裝置是一行動裝置。