M505130

(19)中華民國智慧財產局

(12)新型說明書公告本 **(11)證書號數：TW M505130 U**

(45)公告日： 中華民國 104 (2015) 年 07 月 11 日

(21)申請案號：104206633 (22)申請日： 中華民國 104 (2015) 年 04 月 30 日

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

(71)申請人：臺灣網路認證股份有限公司(中華民國) TAIWAN-CA INC. (TW)
臺北市中正區延平南路 85 號 10 樓

(72)新型創作人：杜宏毅 TU, HUNG YI (TW)；連子清 LIEN, TZU CHING (TW)；林志能 LIN, CHIH NENG (TW)

(74)代理人：林鼎鈞

(NOTE)備註： 相同的創作已於同日申請發明專利(Another patent application for invention in respect of the same creation has been filed on the same date)

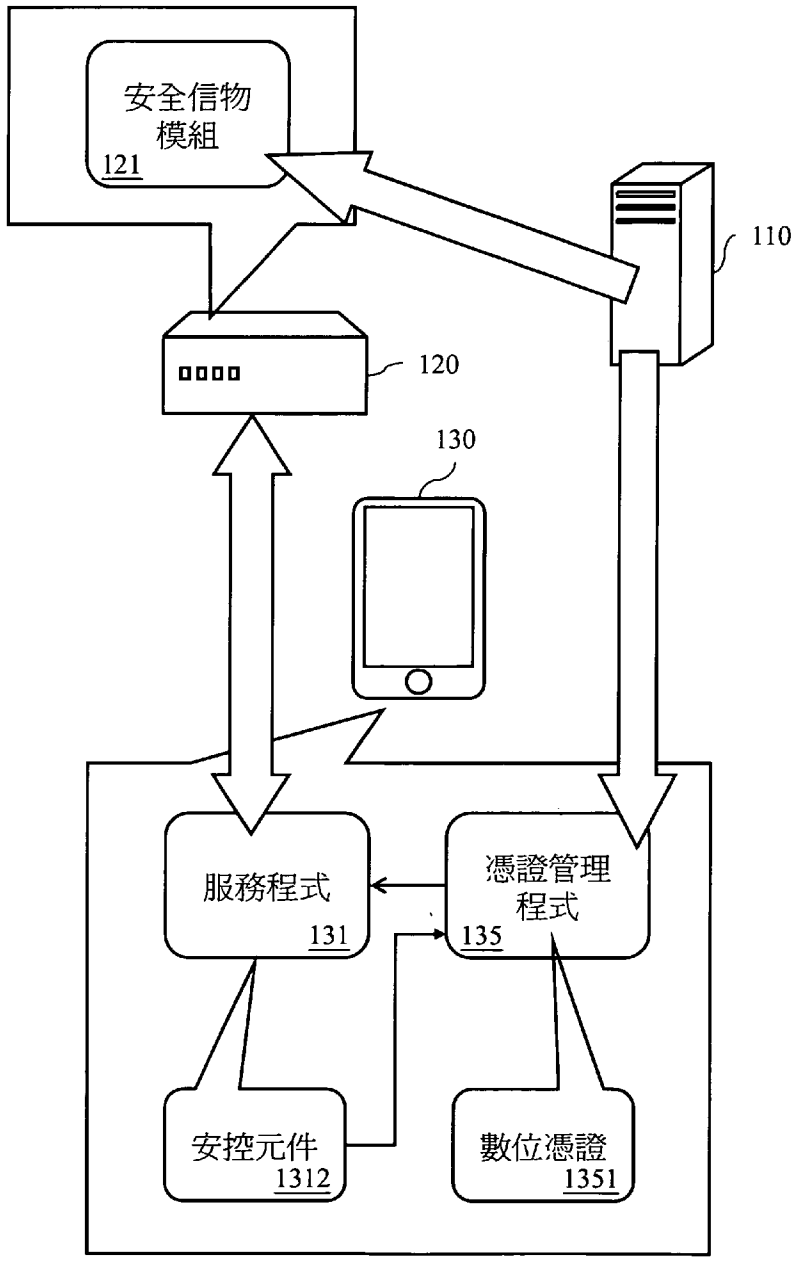
申請專利範圍項數：10 項 圖式數：2 共 17 頁

(54)名稱

在行動裝置上以安全信物使相異程式獲得數位憑證簽署之系統

(57)摘要

一種在行動裝置上以安全信物使相異程式獲得數位憑證簽署之系統，其透過服務主機中之安全信物單元下載憑證管理伺服器所產生的安全信物，並在服務程式至服務主機下載安全信物後，由服務程式透過所包含之安控元件呼叫憑證管理程式，使得憑證管理程式驗證安全信物，並在安全信物通過驗證時，使用與數位憑證對應之私鑰對目標資料簽章，並將簽章結果傳回服務程式，使服務程式可以傳送目標資料與目標資料的簽章結果至服務主機的技術手段，可以讓應用程式共用數位憑證，並達成減少使用者所維護之數位憑證之數量的技術功效。



【第1圖】

110・・・憑證管理伺服器

120・・・服務主機

121・・・安全信物單元

130・・・目標裝置

131・・・服務程式

1312・・・安控元件

135・・・憑證管理程式

1351・・・數位憑證

M505130
專利案號：104206633

公告本

申請日：104. 4. 30

IPC分類：H04L 9/32 (2006.01)

【新型摘要】

【中文新型名稱】　在行動裝置上以安全信物使相異程式獲得數位憑證簽署之系統

【中文】

一種在行動裝置上以安全信物使相異程式獲得數位憑證簽署之系統，其透過服務主機中之安全信物單元下載憑證管理伺服器所產生的安全信物，並在服務程式至服務主機下載安全信物後，由服務程式透過所包含之安控元件呼叫憑證管理程式，使得憑證管理程式驗證安全信物，並在安全信物通過驗證時，使用與數位憑證對應之私鑰對目標資料簽章，並將簽章結果傳回服務程式，使服務程式可以傳送目標資料與目標資料的簽章結果至服務主機的技術手段，可以讓應用程式共用數位憑證，並達成減少使用者所維護之數位憑證之數量的技術功效。

【指定代表圖】　第（1）圖。

【代表圖之符號簡單說明】

110	憑證管理伺服器
120	服務主機
121	安全信物單元
130	目標裝置
131	服務程式
1312	安控元件
135	憑證管理程式
1351	數位憑證

【新型說明書】

【中文新型名稱】　在行動裝置上以安全信物使相異程式獲得數位憑證簽署之系統

【技術領域】

【0001】一種在行動裝置上使程式獲得數位憑證簽署之系統，特別係指一種經由安全信物使相異程式獲得數位憑證簽署之系統。

【先前技術】

【0002】數位憑證，又稱爲電子憑證，是一種用於電腦系統的身分識別機制。數位憑證是身份認證機構加在數位身份證上的一個簽名，這一行爲表示身份認證機構已認定擁有數位身分證的使用者。數位憑證是一個或一組電腦檔案，其中記載了擁有人的身份資料及一組公開密碼匙。電子憑證的擁有人可向電腦系統認證自己的身分，從而存取或使用某一特定的數位服務。

【0003】然而，在部分的數位裝置上，例如智慧型手機等行動裝置，應用程式所擁有的資料並無法共用，因此，即使使用者爲某一個應用程式申請了數位憑證，被這個數位憑證只能讓該應用程式使用，並無法讓其他應用程式使用，這導致使用者需要爲每一個需要使用數位憑證的應用程式都申請數位憑證，容易造成使用者維護數位憑證上的複雜度。

【0004】綜上所述，可知先前技術中長期以來一直存在部分數位裝置上之應用程式無法共用數位憑證的問題，因此有必要提出改進的技術手段，來解決此一問題。

【新型內容】

【0005】有鑒於先前技術存在部分數位裝置上之應用程式無法共用數位憑證的問題，本創作遂揭露一種在行動裝置上以安全信物使相異程式獲得數位憑證簽署之系統，其中：

【0006】本創作所揭露之在行動裝置上以安全信物使相異程式獲得數位憑證簽署之系統，至少包含：憑證管理伺服器，用以產生安全信物；服務主機，包含安全信物單元，安全信物單元用以至憑證管理伺服器下載安全信物；服務程式，包含安控元件，服務程式用以至服務主機下載安全信物，及用以產生目標資料；憑證管理程式，提供服務程式透過安控元件進行呼叫，用以接收安控元件所傳送之安全信物及目標資料，並驗證安全信物，及用以於安全信物通過驗證時，使用與數位憑證對應之私鑰（private key）對目標資料簽章，並傳送簽章結果至服務程式，使服務程式傳送目標資料及簽章結果至服務主機，藉以讓服務主機在依據簽章結果成功驗證目標資料後，依據目標資料提供對應服務。

【0007】本創作所揭露之系統如上，與先前技術之間的差異在於本創作透過服務主機中之安全信物單元下載憑證管理伺服器所產生的安全信物，並在服務程式至服務主機下載安全信物後，由服務程式透過所包含之安控元件呼叫憑證管理程式，使得憑證管理程式驗證安全信物，並在安全信物通過驗證時，使用與數位憑證對應之私鑰對目標資料簽章，並將簽章結果傳回服務程式，使服務程式可以傳送目標資料與目標資料的簽章結果至服務主機，藉以解決先前技術所存在的問題，並可以達成減少使用者所維護之數位憑證之數量的技術功效。

【圖式簡單說明】

【0008】

第1圖爲本創作所提之在行動裝置上以安全信物使相異程式獲得數位憑證簽署之系統架構圖。

第2A圖爲本創作所提之在行動裝置上以安全信物使相異程式獲得數位憑證簽署之方法流程圖。

第2B圖爲本創作所提之使用數位憑證對目標資料簽章之詳細方法流程圖。

【實施方式】

【0009】以下將配合圖式及實施例來詳細說明本創作之特徵與實施方式，內容足以使任何熟習相關技藝者能夠輕易地充分理解本創作解決技術問題所應用的技術手段並據以實施，藉此實現本創作可達成的功效。

【0010】本創作可以讓憑證管理程式對服務程式所產生的目標資料進行簽章，使得服務程式可以傳送目標資料與目標資料的簽章結果至服務主機。其中，本創作之目標資料爲可以讓服務主機進行對應服務的資料，例如，當服務主機爲投票伺服器時，目標資料爲投票內容，又如服務主機爲帳號伺服器時，目標資料爲服務識別碼等，但本創作並不以上述爲限。

【0011】以下先以「第1圖」本創作所提之在行動裝置上以安全信物使相異程式獲得數位憑證簽署之系統架構圖來說明本創作的系統運作。如「第1圖」所示，本創作之系統含有憑證管理伺服器110、服務主機120、目標裝置130。

【0012】憑證管理伺服器110負責產生安全信物，並將所產生的安全信物傳送到服務主機120。憑證管理伺服器110所產生的安全信物會與服務主機120相對應。在部分的實施例中，憑證管理伺服器110可以加密所產生的安全信物。

【0013】憑證管理伺服器110可以預先產生安全信物，並在服務主機120請求下載時將預先產生的安全信物傳送到服務主機120，憑證管理伺服器110也可以在服務主機120請求下載安全信物時才產生安全信物。

【0014】憑證管理伺服器110可以維護一份程式允許清單，並提供憑證管理程式135下載程式允許清單。憑證管理伺服器110所維護之程式允許清單包含一個或多個服務程式的程式識別資料。其中，程式識別資料包含但不限於服務程式的程式名稱，或是憑證管理伺服器110分配給服務程式的識別碼等。

【0015】服務主機120負責接收目標資料，並依據所接收到的目標資料提供相對應的服務。例如，當服務主機120爲投票伺服器時，服務主機120可以提供線上投票的服務，又如服務主機120爲帳號伺服器時，服務主機120可以提供登入的服務，但本創作所提之服務主機120並不以上述爲限。

【0016】在部分的實施例中，服務主機120在提供服務前，還可以先驗證目標資料的簽章結果，並在目標資料的簽章結果通過驗證後，才依據目標資料提供對應服務。其中，目標資料的簽章結果通常會隨著目標資料一同被傳送到服務主機120，但本創作並不以此爲限。

【0017】服務主機120可以包含安全信物單元121，安全信物單元121負責到憑證管理伺服器110下載安全信物，使得服務主機120可以取得安全信物。一般而言，安全信物單元121可以定期或每隔特定時間或在預定時間至憑證管理伺服器110下載安全信物。

【0018】服務程式131與憑證管理程式135被安裝在目標裝置130，目標裝置130可以執行服務程式131與憑證管理程式135。其中，服務程式131與服務主機120相對應。

【0019】服務程式131負責在目標裝置130執行後產生目標資料。服務程式131所產生的目標資料可以是服務程式131在收集特定的資料後產生，或是依據目標裝置130之使用者的操作產生，本創作沒有特別的限制。

【0020】服務程式131負責到服務主機120下載安全信物。其中，服務程式131可以在需要傳送所產生的目標資料至服務主機120時，至服務主機120下載安全信物，但本創作並不以此爲限。

【0021】服務程式131可以包含安控元件1312。安控元件1312提供服務程式131呼叫憑證管理程式135，安控元件1312也負責將服務程式131所下載的安全信物與服務程式131所產生的目標資料傳送到憑證管理程式135。一般而言，安控元件1312可以在呼叫憑證管理程式135時，一併將安全信物與目標資料傳送給憑證管理程式135，例如透過參數的方式傳遞等，但本創作並不以此爲限。

【0022】服務程式131可以接收憑證管理程式135所傳回的簽章結果，並可以將所產生的目標資料與所接收之簽章結果傳送到服務主機120。

【0023】憑證管理程式135負責接收安控元件1312所傳送的安全信物及目標資料，並驗證所接收到的安全信物。憑證管理程式135可以判斷安全信物的有效性以及判斷安全信物內的簽章值是否正確來驗證安全信物。當憑證管理程式135判斷安全信物有效且安全信物內的簽章值正確時，表示安全信物可以通過驗證，當安全信物無效或安全信物內的簽章值不正確時，表示安全信物無法通過驗證。但憑證管理程式135驗證安全信物之方式並不以上述爲限。

【0024】在部分的實施例中，憑證管理程式135可以預先至憑證管理伺服器110下載程式允許清單，並可以在驗證安全信物時，判斷安全信物所包含之程式識別資料是否包含於所下載的程式允許清單中，若是，則表示安全信物可以通過驗證，反之，若安全信物所包含之程式識別資料沒有包含於程式允許清單中，則安全信物無法通過驗證。

【0025】若憑證管理程式135所接收到的安全信物經過憑證管理伺服器110的加密，則憑證管理程式135可以先解密安全信物再驗證安全信物。其中，若憑證管理伺服器110使用非對稱的加密演算法，則憑證管理程式135需要預先儲存與憑證管理伺服器110加密安全信物所使用之私密金鑰（私鑰；private key）相對應的公開金鑰（公鑰；public key）。

【0026】憑證管理程式135也負責在安全信物通過驗證時，取用相對應之數位憑證1351，並使用與數位憑證1351相對應之私密金鑰對所接收到的目標資料進行簽章而產生目標資料的簽章結果，並將所產生之簽章結果傳送到服務程式131，藉以讓服務程式131將所產生的目標資料與所接收之簽章結果傳送到服務主機120，使服務主機120可以驗證所接收到之目標資料的簽章結果，並在簽章結果成功通過驗證後，依據所接收到的目標資料提供對應服務。

【0027】其中，憑證管理程式135可以提供使用者介面，藉以提供目標裝置130的使用者輸入簽章密碼。若安控元件1312未指定數位憑證且目標裝置內有多張數位憑證時，憑證管理程式135可以先提供讓使用者選擇所欲使用之數位憑證的使用者介面，使得安控元件1312可以依據使用者的選擇指定目標裝置130所使用的數位憑證，再提供使用者輸入簽章密碼。而當安控元件1312已指定目標裝置130使用特定的數位憑證或在目標裝置130中僅有一張數位憑證時，則當使

用者透過憑證管理程式135所輸入的簽章密碼正確時，憑證管理程式135可以使用提供使用者輸入的簽章密碼來動用與該數位憑證相對應的私密金鑰進行簽章，而當使用者透過憑證管理程式135所輸入的簽章密碼錯誤時，則憑證管理程式135將無法動用與該數位憑證相對應的私密金鑰，也就是無法進行簽章作業。

【0028】 接著以一個實施例來解說本創作的運作系統，並請參照「第2A圖」本創作所提之在行動裝置上以安全信物使相異程式獲得數位憑證簽署之方法流程圖。在本實施例中，假設服務主機120爲股東投票系統，目標裝置130爲智慧型手機，服務程式131爲股票管理程式，但本創作並不以此爲限。

【0029】 首先，股東投票系統的管理者也需要先架設服務主機120，在服務主機120開始運作後，服務主機120中的安全信物單元121可以至憑證管理伺服器110下載憑證管理伺服器110所產生的安全信物（步驟210）。在本實施例中，假設安全信物單元121可以週期性的傳送下載安全信物的請求至憑證管理伺服器110，憑證管理伺服器110可以在接收到安全信物單元121的請求時，產生與服務主機120對應之安全信物，並將所產生的安全信物加密後傳回安全信物單元121。

【0030】 當目標裝置130的使用者希望使用目標裝置130連線至服務主機120進行股東線上投票時，使用者可以在目標裝置130安裝與本創作相容且對應服務主機120的服務程式131與憑證管理程式135，並可以執行服務程式131，且透過服務程式131進行線上投票，也就是在服務程式131上選擇投票的選項。

【0031】 在目標裝置130的使用者在服務程式131中完成投票的選擇後，服務程式131可以依據使用者的選擇產生相對應的目標資料。若服務主機120需要使用簽章來驗證目標資料的正確性，則服務程式131可以先至服務主機120下載

與服務主機120相對應的安全信物（步驟220），並透過服務程式131所包含的安控元件1312呼叫被安裝在同一目標裝置130中的憑證管理程式135（步驟230）。在本實施例中，假設安控元件1312可以將服務程式131所下載的安全信物與服務程式131所產生的目標資料作爲呼叫憑證管理程式135的參數。

【0032】 如此，在憑證管理程式135被呼叫後，便可以接收到服務程式131所下載的安全信物與服務程式131所產生的目標資料，接著，憑證管理程式135可以驗證所接收到的安全信物（步驟250）。在本實施例中，假設憑證管理程式135在被執行後，可以至憑證管理伺服器110下載程式允許清單（步驟202），則憑證管理程式135可以先解密所接收到的安全信物後，接著判斷安全信物中所表示的程式識別資料是否包含在所下載的程式允許清單中，並判斷安全信物的時效是否有效以及檢核安全信物內的簽章值是否正確，藉以進行安全信物的驗證。若安全信物中所表示的程式識別資料包含在所下載的程式允許清單中，同時安全信物有效且安全信物內的簽章值正確，則表示安全信物通過憑證管理程式135的驗證，而若安全信物中所表示的程式識別資料沒有包含在所下載的程式允許清單中或安全信物的時效已過或安全信物內的簽章值不正確，則表示安全信物沒有通過憑證管理程式135的驗證。

【0033】 若安全信物通過憑證管理程式135的驗證（步驟260），則憑證管理程式135可以對目標資料進行簽章，並將簽章所產生的簽章結果傳回透過安控元件1312呼叫憑證管理程式135的服務程式131（步驟270）。在本實施例中，假設憑證管理程式135可以如「第2B圖」的流程所示，憑證管理程式135可以依據安控元件1312所列條件取用相對應之數位憑證1351（步驟271），再顯示使用者介面，使得目標裝置130的使用者輸入欲使用之數位憑證1351的簽章密碼（步驟

273），使用被輸入之簽章密碼動用與數位憑證1351相對應的私密金鑰對所接收到的目標資料進行簽章（步驟275），並在完成簽章後產生目標資料的簽章結果，最後將所產生的簽章結果傳回服務程式131（步驟279）。

【0034】在憑證管理程式135將目標資料的簽章結果傳回服務程式131後，服務程式131可以將所接收到的簽章結果與所產生的目標資料傳送到服務主機120（步驟280），使得服務主機120可以接收到服務程式131所產生的目標資料與憑證管理程式135所產生的簽章結果，並依據所接收到之簽章結果對目標資料進行驗證，以及在目標資料成功被驗證後，依據目標資料提供相對應的服務（步驟290），在本實施例中，也就是儲存目標裝置130之使用者的投票選擇。

【0035】如此，透過本創作所提之憑證管理伺服器110、服務主機120中的安全信物單元121、服務程式131中的安控元件1312以及憑證管理程式135，服務程式131可以無需額外再安裝數位憑證也可以獲得需要使用數位憑證的服務。

【0036】綜上所述，可知本創作與先前技術之間的差異在於具有透過服務主機中之安全信物單元下載憑證管理伺服器所產生的安全信物，並在服務程式至服務主機下載安全信物後，由服務程式透過所包含之安控元件呼叫憑證管理程式，使得憑證管理程式驗證安全信物，並在安全信物通過驗證時，使用與數位憑證相對應的私密金鑰對目標資料簽章，並將簽章結果傳回服務程式，使服務程式可以傳送目標資料與目標資料的簽章結果至服務主機的技術手段，藉由此一技術手段可以解決先前技術所存在數位裝置上之應用程式可能無法共用數位憑證的問題，進而達成減少使用者所維護之數位憑證之數量的技術功效。

【0037】再者，本創作可實現於硬體、軟體或硬體與軟體之組合中，亦可在電腦系統中以集中方式實現或以不同元件散佈於若干互連之電腦系統的分散方式實現。

【0038】雖然本創作所揭露之實施方式如上，惟所述之內容並非用以直接限定本創作之專利保護範圍。任何本創作所屬技術領域中具有通常知識者，在不脫離本創作所揭露之精神和範圍的前提下，對本創作之實施的形式上及細節上作些許之更動潤飾，均屬於本創作之專利保護範圍。本創作之專利保護範圍，仍須以所附之申請專利範圍所界定者爲準。

【符號說明】

【0039】

110	憑證管理伺服器
120	服務主機
121	安全信物單元
130	目標裝置
131	服務程式
1312	安控元件
135	憑證管理程式
1351	數位憑證
步驟 206	憑證管理程式至憑證管理伺服器下載程式允許清單
步驟 210	服務主機之安全信物單元至憑證管理伺服器下載安全信物
步驟 220	服務程式至服務主機下載安全信物
步驟 230	服務程式透過所包含之安控元件呼叫憑證管理程式，並傳送安全信物及目標資料至憑證管理程式
步驟 250	憑證管理程式驗證安全信物
步驟 260	安全信物是否通過驗證

步驟 270　憑證管理程式用數位憑證對目標資料簽章，並傳送簽章結果至服務程式

步驟 271　憑證管理程式依據安控元件所列條件取用相對應之數位憑證

步驟 273　憑證管理程式提供輸入簽章密碼

步驟 275　憑證管理程式使用簽章密碼動用與數位憑證對應之私鑰對目標資料簽章

步驟 279　憑證管理程式傳送簽章結果至服務程式

步驟 280　服務程式傳送目標資料及簽章結果至服務主機

步驟 290　服務主機依據簽章結果成功驗證目標資料後，依據目標資料提供服務

【新型申請專利範圍】

【第1項】一種在行動裝置上以安全信物使相異程式獲得數位憑證簽署之系統，該系統至少包含：

一憑證管理伺服器，用以產生一安全信物；

一服務主機，包含一安全信物單元，該安全信物單元用以至該憑證管理伺服器下載該安全信物；及

一目標裝置，其中更包含：

一服務程式，包含一安控元件，該服務程式用以至該服務主機下載該安全信物，及用以產生一目標資料；及

一憑證管理程式，提供該服務程式透過該安控元件進行呼叫，用以接收該安控元件所傳送之該安全信物及該目標資料，並驗證該安全信物，及用以於該安全信物通過驗證時，使用與一數位憑證相對應之私密金鑰對該目標資料簽章，並傳送簽章結果至該服務程式，使該服務程式傳送該目標資料及該簽章結果至該服務主機，藉以讓該服務主機在依據該簽章結果成功驗證該目標資料後，依據該目標資料提供對應服務。

【第2項】如申請專利範圍第1項所述之在行動裝置上以安全信物使相異程式獲得數位憑證簽署之系統，其中該憑證管理程式更用以至該憑證管理伺服器下載一程式允許清單，及判斷該安全信物所包含之程式識別資料是否包含於該程式允許清單中，藉以驗證該安全信物。

【第3項】如申請專利範圍第2項所述之在行動裝置上以安全信物使相異程式獲得數位憑證簽署之系統，其中該安全信物所包含之程式識別資料是該服務程式之程式名稱或該憑證管理伺服器分配給該服務程式之識別碼。

【第4項】如申請專利範圍第1項所述之在行動裝置上以安全信物使相異程式獲得數位憑證簽署之系統，其中該憑證管理伺服器更用以加密該安全信物，且該憑證管理程式更用以解密該安全信物。

【第5項】如申請專利範圍第1項所述之在行動裝置上以安全信物使相異程式獲得數位憑證簽署之系統，其中該憑證管理程式是判斷該安全信物之有效性以驗證該安全信物。

【第6項】如申請專利範圍第1項所述之在行動裝置上以安全信物使相異程式獲得數位憑證簽署之系統，其中該憑證管理程式是依據該安控元件所列條件取用相對應之該數位憑證，提供輸入一簽章密碼，並依據該簽章密碼動用與該數位憑證相對應之私密金鑰對該目標資料簽章。

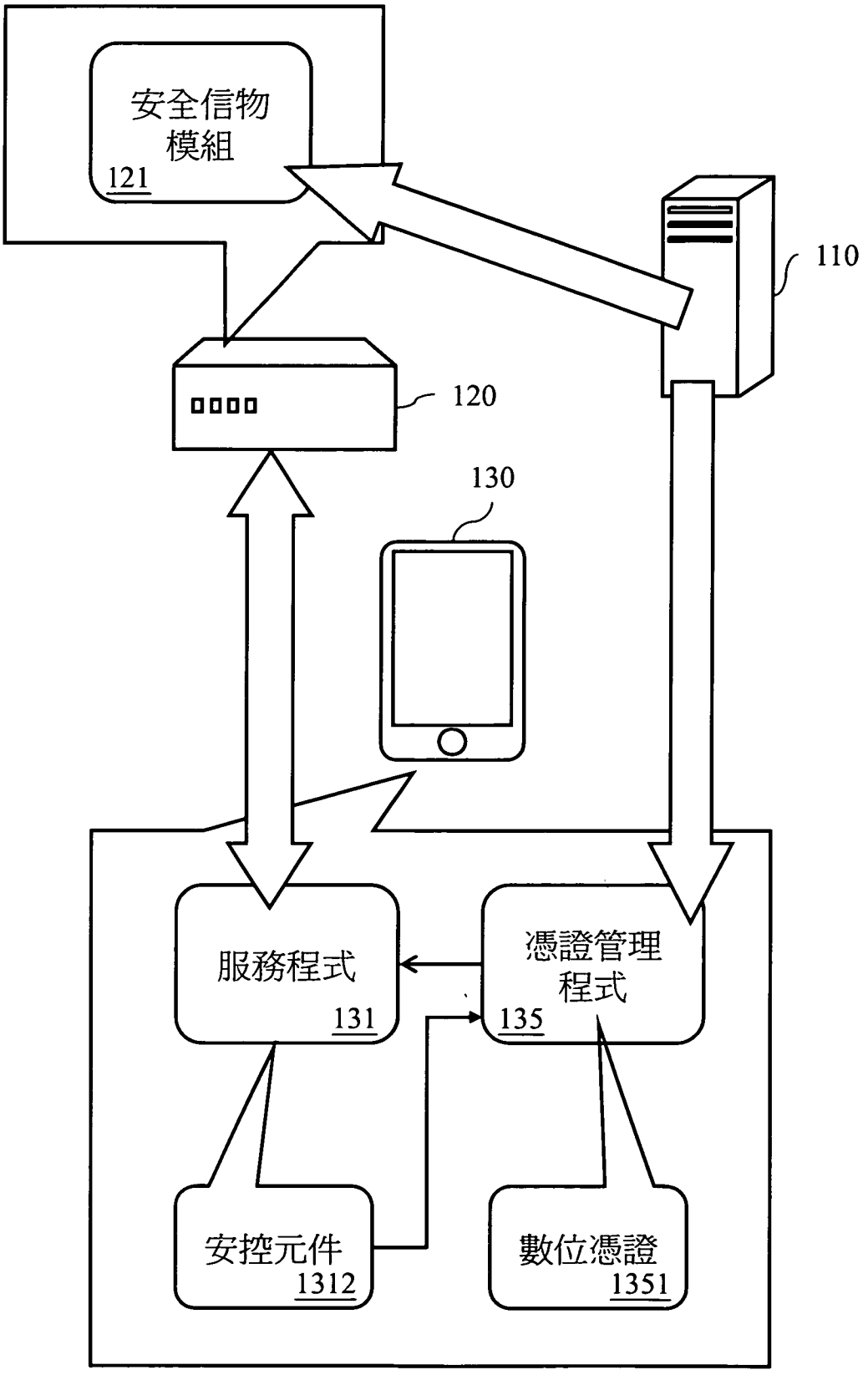
【第7項】如申請專利範圍第1項所述之在行動裝置上以安全信物使相異程式獲得數位憑證簽署之系統，其中該目標裝置爲智慧型手機。

【第8項】如申請專利範圍第1項所述之在行動裝置上以安全信物使相異程式獲得數位憑證簽署之系統，其中該安全信物是由該憑證管理伺服器預先產生或由該憑證管理伺服器在該服務主機請求時產生。

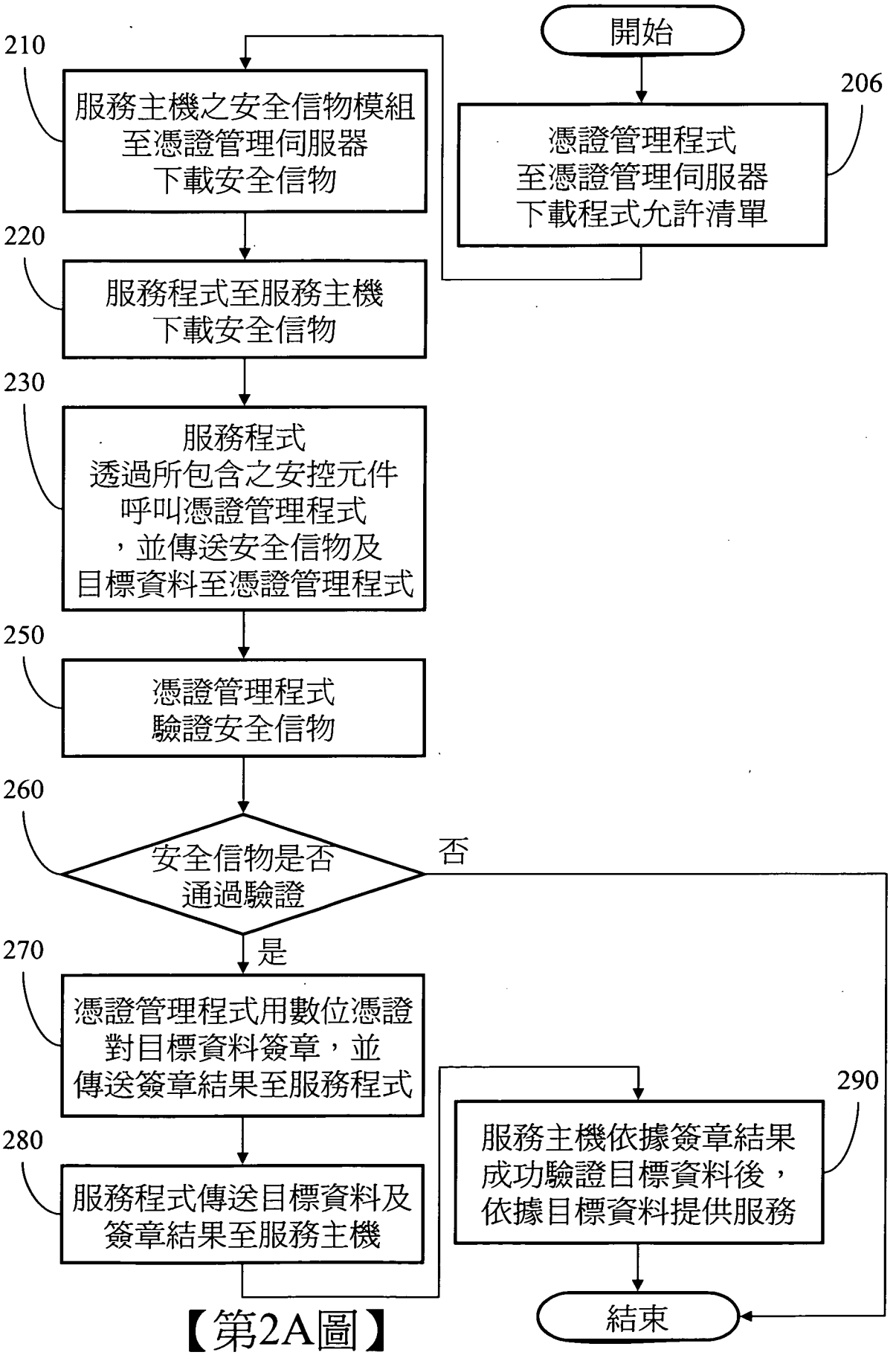
【第9項】如申請專利範圍第1項所述之在行動裝置上以安全信物使相異程式獲得數位憑證簽署之系統，其中該安全信物單元是定期或每隔一特定時間或在一預定時間至該憑證管理伺服器下載該安全信物。

【第10項】如申請專利範圍第1項所述之在行動裝置上以安全信物使相異程式獲得數位憑證簽署之系統，其中該目標資料是該服務程式在收集特定資料後產生，或是該服務程式依據該目標裝置之使用者之操作產生。

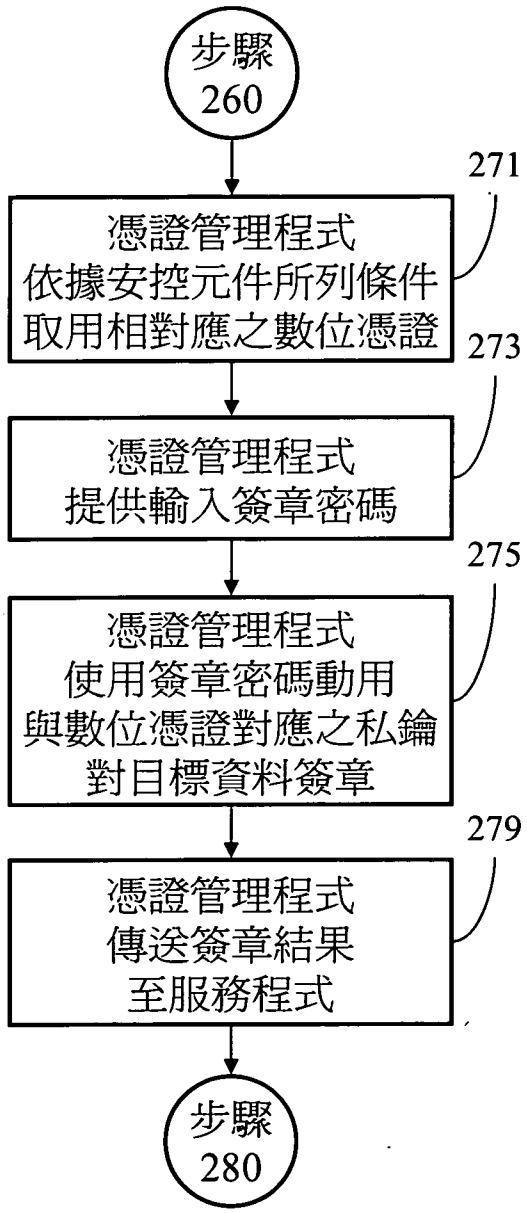
【新型圖式】


安全信物
模組
121
110
120
130
服務程式
131
憑證管理
程式
135
安控元件
1312
數位憑證
1351

【第1圖】


開始
206
憑證管理程式
至憑證管理伺服器
下載程式允許清單
210
服務主機之安全信物模組
至憑證管理伺服器
下載安全信物
220
服務程式至服務主機
下載安全信物
230
服務程式
透過所包含之安控元件
呼叫憑證管理程式
，並傳送安全信物及
目標資料至憑證管理程式
250
憑證管理程式
驗證安全信物
260
安全信物是否
通過驗證
否
是
270
憑證管理程式用數位憑證
對目標資料簽章，並
傳送簽章結果至服務程式
280
服務程式傳送目標資料及
簽章結果至服務主機
290
服務主機依據簽章結果
成功驗證目標資料後，
依據目標資料提供服務
結束

【第2A圖】


步驟
260
271
憑證管理程式
依據安控元件所列條件
取用相對應之數位憑證
273
憑證管理程式
提供輸入簽章密碼
275
憑證管理程式
使用簽章密碼動用
與數位憑證對應之私鑰
對目標資料簽章
279
憑證管理程式
傳送簽章結果
至服務程式
步驟
280

【第2B圖】