



(19)中華民國智慧財產局

(12)發明說明書公告本

(11)證書號數：TW I700603 B

(45)公告日：中華民國 109 (2020) 年 08 月 01 日

(21)申請案號：107130315

(22)申請日：中華民國 107 (2018) 年 08 月 30 日

(51)Int. Cl. : **G06F21/30 (2013.01)****G06Q10/10 (2012.01)**

(30)優先權：2017/10/30 中國大陸

201711036776.9

(71)申請人：香港商阿里巴巴集團服務有限公司 (香港地區) ALIBABA GROUP SERVICES
LIMITED (HK)

香港

(72)發明人：魏亞文 (CN)

(74)代理人：林志剛

(56)參考文獻：

CN 108985361A

CN 109104441A

US 8010469B2

US 8763127B2

審查人員：施廷岳

申請專利範圍項數：17 項 圖式數：9 共 43 頁

(54)名稱

數位證書使用的實現方法和用於執行上述方法的電腦設備及電腦可讀儲存媒體

(57)摘要

本說明書提供一種數位證書使用的實現方法，所述方法包括：接收用戶端的證書使用請求，所述證書使用請求中包括用戶端的設備標識和所述證書的核身要求；所述核身要求指定至少一種要素核身方式；根據所述對應關係，查找與所述設備標識對應的、並且滿足核身要求的已有證書標識；所述滿足核身要求的已有證書標識為：已通過核身方式中包括核身要求指定的每種要素核身方式的已有證書標識；向用戶端發送證書使用指令，所述證書使用指令中包括滿足核身要求的已有證書標識。

指定代表圖：

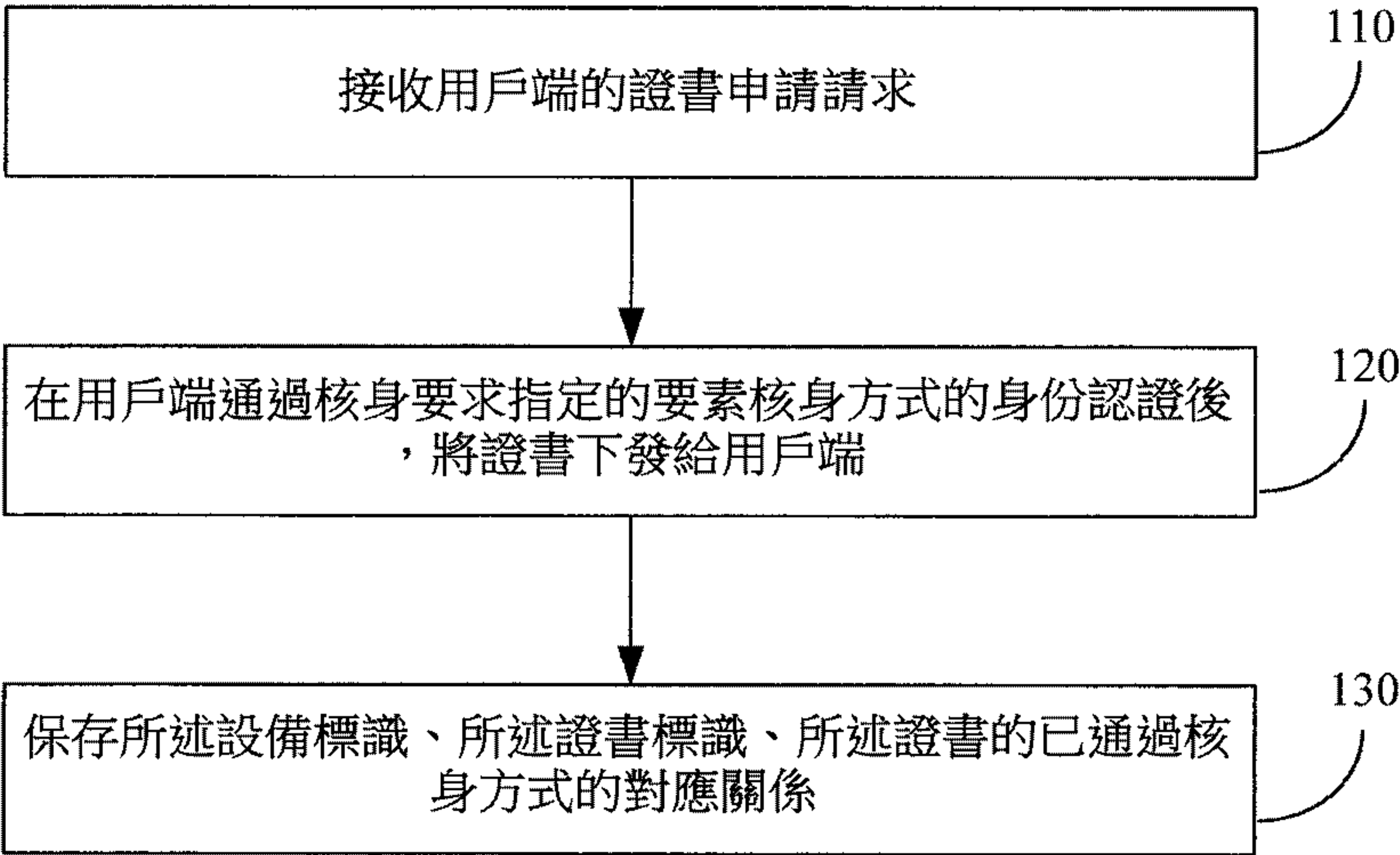


圖 1

【發明摘要】**【中文發明名稱】**

數位證書使用的實現方法和用於執行上述方法的電腦設備及電腦可讀儲存媒體

【中文】

本說明書提供一種數位證書使用的實現方法，所述方法包括：接收用戶端的證書使用請求，所述證書使用請求中包括用戶端的設備標識和所述證書的核身要求；所述核身要求指定至少一種要素核身方式；根據所述對應關係，查找與所述設備標識對應的、並且滿足核身要求的已有證書標識；所述滿足核身要求的已有證書標識為：已通過核身方式中包括核身要求指定的每種要素核身方式的已有證書標識；向用戶端發送證書使用指令，所述證書使用指令中包括滿足核身要求的已有證書標識。

【指定代表圖】第(1)圖。

【代表圖之符號簡單說明】無

【特徵化學式】無

【發明說明書】

【中文發明名稱】

數位證書使用的實現方法和用於執行上述方法的電腦設備及電腦可讀儲存媒體

【技術領域】

本說明書關於網路通訊技術領域，尤其關於一種數位證書申請的實現方法和裝置、一種數位證書使用的實現方法和裝置。

【先前技術】

資訊技術的飛速發展，使網際網路滲入到社會生活的各個態樣。在電子商務、網路金融、網路政務等對參與各方之間的互動有資訊完整性、不可更改、不可抵賴等要求的應用場景中，通常採用數位證書來滿足這些要求。

數位證書是一種權威性的電子文件，相當於網路環境中的一種身份證，用於證明在網上進行資訊交流及商務活動的各主體（如人、伺服器等）的身份。數位證書由權威機構發行，每一個數位證書包含了主體身份的部分資訊、主體所持有的公開金鑰及認證機構的數位簽章。

隨著電子商務、網路金融的業務種類日益豐富，應用數位證書的業務也不斷增加。不同的業務對安全性的要求可能有所不同，因此安裝在設備上每個應用程式中通常都有多張不同可信度的數位證書。如何以少量的證書來滿足不同業務的需求，成為數位證書發展中面臨的問題。

【發明內容】

有鑑於此，本說明書提供一種數位證書申請的實現方法，包括：

接收用戶端的證書申請請求，所述證書申請請求中包括用戶端的設備標識和所述證書的核身要求；所述核身要求指定至少一種要素核身方式；

在用戶端通過核身要求指定的要素核身方式的身份認證後，將證書下發給用戶端；

保存所述設備標識、所述證書標識、所述證書的已通過核身方式的對應關係。

本說明書提供的一種電腦設備，包括：記憶體和處理器；所述記憶體上儲存有可由處理器運行的電腦程式；所述處理器運行所述電腦程式時，執行上述數位證書申請的實現方法所述的步驟。

本說明書提供的一種電腦可讀儲存媒體，其上儲存有電腦程式，所述電腦程式被處理器運行時，執行上述數位證書申請的實現方法所述的步驟。

本說明書提供的一種數位證書使用的實現方法，伺服器端維護有用戶端的設備標識、所述用戶端的已有證書標識、所述已有證書的已通過核身方式的對應關係，所述方法包括：

接收用戶端的證書使用請求，所述證書使用請求中包括用戶端的設備標識和所述證書的核身要求；所述核身要

求指定至少一種要素核身方式；

根據所述對應關係，查找與所述設備標識對應的、並且滿足核身要求的已有證書標識；所述滿足核身要求的已有證書標識為：已通過核身方式中包括核身要求指定的每種要素核身方式的已有證書標識；

向用戶端發送證書使用指令，所述證書使用指令中包括滿足核身要求的已有證書標識。

本說明書提供的一種電腦設備，包括：記憶體和處理器；所述記憶體上儲存有可由處理器運行的電腦程式；所述處理器運行所述電腦程式時，執行上述數位證書使用的實現方法所述的步驟。

本說明書還提供了一種電腦可讀儲存媒體，其上儲存有電腦程式，所述電腦程式被處理器運行時，執行上述數位證書使用的實現方法所述的步驟。

本說明書提供的一種數位證書使用的實現方法，應用在用戶端，所述方法包括：

向伺服器發送證書使用請求，所述證書使用請求中包括用戶端的設備標識和所述證書的核身要求；所述核身要求指定至少一種要素核身方式，供伺服器根據維護的用戶端的設備標識、已有證書標識、所述已有證書的已通過核身方式的對應關係，查找已通過核身方式中包括所述核身要求指定的每種要素核身方式的、與所述證書使用請求中設備標識對應的已有證書標識；

從伺服器接收證書使用指令，所述證書使用指令中包

括滿足核身要求的已有證書標識；

採用具有證書使用指令中已有證書標識的證書進行簽名。

本說明書提供的一種電腦設備，包括：記憶體和處理器；所述記憶體上儲存有可由處理器運行的電腦程式；所述處理器運行所述電腦程式時，執行數位證書使用的實現方法所述的步驟。

本說明書還提供了一種電腦可讀儲存媒體，其上儲存有電腦程式，所述電腦程式被處理器運行時，執行上述數位證書使用的實現方法所述的步驟。

由以上技術方案可見，本說明書的實施例中，在數位證書申請時，在伺服器保存用戶端的設備標識、證書標識、該證書的已通過核身方式的對應關係，使得當該證書的已通過核身方式能夠滿足某項業務對證書的核身要求時，該項業務可以使用該證書而不需申請新的證書，從而在滿足業務需求的條件下將證書多工於多項業務，節約了設備的資源，減少了用戶操作；

本說明書的實施例中，在數位證書使用時，在伺服器維護用戶端所在設備標識、已有證書標識、已有證書的已通過核身方式的對應關係，在收到用戶端證書使用請求後，根據證書核身要求指定的要素核身方式，基於對應關係查找滿足核身要求的已有證書標識，並指令用戶端使用滿足核身要求的已有證書，使得當用戶端的已有證書能夠滿足某項業務對證書的核身要求時，該項業務可以使用已

有證書而不需申請新的證書，從而在滿足業務需求的條件下將證書多工於多項業務，節約了設備的資源，減少了用戶操作。

【圖式簡單說明】

圖1是本說明書實施例一中一種應用在伺服器端的數位證書申請的實現方法的流程圖；

圖2是本說明書實施例二中一種應用在伺服器端的數位證書使用的實現方法的流程圖；

圖3是本說明書實施例二中一種應用在用戶端的數位證書使用的實現方法的流程圖；

圖4是本說明書應用示例中一種在申請數位證書時，證書SDK模組、證書管理伺服器、核身伺服器和CA伺服器之間的互動流程圖；

圖5是本說明書應用示例中一種在使用數位證書時，證書SDK模組、證書管理伺服器和核身伺服器之間的互動流程圖；

圖6是用戶端或伺服器端所在設備的一種硬體結構圖；

圖7是本說明書實施例中一種應用在伺服器端的數位證書申請的實現裝置的邏輯結構圖；

圖8是本說明書實施例中一種應用在伺服器端的數位證書使用的實現裝置的邏輯結構圖；

圖9是本說明書實施例中一種應用在用戶端的數位證書使用的實現裝置的邏輯結構圖。

【實施方式】

數位證書的可信度通常由頒發證書時用戶需要通過的核身方式（身份認證方式）來決定，例如，如果用戶在申請證書 A 時需要通過帳戶密碼和簡訊兩種核身方式的身份認證，在申請證書 B 時需要通過帳戶密碼、簡訊和人臉三種核身方式的身份認證，則證書 B 的可信度高於證書 A。很多應用場景中，業務對證書的要求通常也是指定證書要通過的核身方式。如果用戶在使用第一項業務時申請的證書能夠滿足第二項業務對證書的要求，第二項業務可以直接使用該證書而不必申請新的證書，從而減少用戶需要申請、用戶端需要維護的證書數量。此外，如果已有的證書不能滿足一項業務對證書的要求，可以以已有證書的已通過核身方式為基礎，由用戶補充新的核身方式來已有證書進行升級，使已有證書滿足該業務的要求，而無需申請新的證書和令用戶重複已經通過的身份認證，進一步減少了用戶操作和用戶端的證書數量。

本說明書的實施例一提出一種新的數位證書申請的實現方法，用戶端在證書申請請求中攜帶設備標識和證書的核身要求，伺服器下發證書並保存設備標識、證書標識和已通過核身方式的對應關係，該對應關係由伺服器用來在某個證書的已通過核身方式滿足某項業務的核身要求時，將該證書用於該項業務，從而使得證書能夠多工於多項業務，減少了用戶端的證書數量，也減少了用戶申請證書的

操作。

本說明書的實施例一和實施例二中，用戶端和伺服器端通過網路相互可存取。其中，用戶端可以是設備作業系統中的一個用來在設備層管理證書的功能模組，可以是一個App（應用程式），也可以是App中的一個用來管理該App內證書的功能模組，不做限定。用戶端可以運行在各種設備上，如手機、平板電腦、PC（Personal Computer，個人電腦）、筆記型電腦、伺服器設備。伺服器端可以運行在一個實體或邏輯伺服器上，也可以是由兩個或兩個以上分擔不同職責的實體或邏輯伺服器、相互協同來實現本說明書實施例中伺服器端的各項功能。本說明書的實施例一和實施例二對用戶端、伺服器端所在設備的種類，以及用戶端與伺服器端之間通訊網路的類型、協定等均不做限定。

本說明書的實施例一和實施例二中，證書的核身要求用來指定一種到多種核身方式，區別起見以下將這些核身方式稱之為要素核身方式。例如，一個證書的核身要求為簡訊和人臉，則該證書有兩個要素核身方式，分別是簡訊和人臉。要素核身方式表達了證書的可信度，在申請該證書時需要通過每種要素核身方式的身份認證。當第一個證書的要素核身方式包含了所有第二個證書的要素核身方式時，第一個證書已經滿足了第二證書的核身要求，第一個證書具有的可信度至少不低於第二個證書，用第一個證書代替第二個證書進行數位簽章所具有的效率同樣至少不低於採用第二個證書的數位簽章。

在本說明書的實施例一和實施例二的一些應用場景中，證書的核身要求可以由一個到多個核身方式組構成，每個核身方式組指定一種到多種要素核身方式，證書的核身要求可以由任意一個核身方式組內的所有要素核身方式來構成；也就是說，當核身要求的任意一個核身方式組內的每種要素核身方式都曾經通過身份認證時，即滿足了該核身要求。例如，一個證書的核身要求包括2個核身方式組，第一個核身方式組有三個要素核身方式（帳戶密碼、簡訊和人臉），第二個核身方式組有兩個要素核身方式（人臉和指紋），則用戶通過帳戶密碼、簡訊和人臉的身份認證，即滿足了該證書的核身要求；用戶通過人臉和指紋的身份認證，也同樣滿足了該證書的核身要求；但是用戶只通過了帳戶密碼和人臉的身份認證，由於這兩種核身方式的組合與該證書指定的要素核身方式不同，不滿足該證書的核身要求。

本說明書的實施例一中，數位證書申請的實現方法的流程如圖1所示，該方法應用在伺服器端。

步驟110，接收用戶端的證書申請請求。

當用戶端申請新的數位證書時，將用戶端所在設備的標識、所申請證書的核身要求封裝在證書申請請求中，發送給伺服器端。證書的核身要求通常由用戶端所在設備上要進行的業務來決定。設備標識可以是任何能夠唯一代表該設備的資訊，如IMEI（International Mobile Equipment Identity，國際移動設備身份碼）、UUID（Universally

Unique Identifier，通用唯一識別碼）、MAC（Media Access Control，媒體介入控制）位址等。

伺服器從接收的證書申請請求中提取用戶端設備標識和證書的核身要求，按照核身要求指示該用戶端進行身份認證。

步驟 120，在用戶端通過核身要求指定的要素核身方式的身份認證後，將證書下發給用戶端。

用戶在用戶端逐一進行證書的核身要求指定的每種要素核身方式的身份驗證。在用戶成功完成上述每個身份認證過程後，伺服器可以獲知用戶端已經通過每種要素核身方式的身份認證，已經滿足核身要求，伺服器將用戶端的證書下發給用戶端。

在步驟 110 和 120 中，根據實際應用場景中伺服器 and 用戶端的實現、以及對證書申請的安全性要求，伺服器指示用戶端進行身份認證、用戶端進行身份認證、伺服器獲知用戶端通過認證、伺服器下發證書的具體過程可以採用不同的互動流程實現，例如現有技術中證書申請過程中的各種互動流程，不再贅述。

步驟 130，保存用戶端設備標識、下發的證書標識、下發證書的已通過核身方式的對應關係。

伺服器將接收下發證書的用戶端的設備標識、下發證書的證書標識、和下發證書的已通過核身方式（包括用戶在證書申請過程中在用戶端通過的每種要素核身方式）的對應關係，保存在可存取的儲存位置。其中，證書標識是

在伺服器端能夠唯一代表一個證書的資訊，例如可以是證書的序號、證書在伺服器端證書資料庫中的索引等。

在一些應用場景中，可能有不同的用戶使用同一個設備來進行業務，或者同一個用戶在同一個設備上使用不同的帳戶來進行業務。在這些應用場景中，用戶端在證書申請請求中封裝用戶標識、所在設備的設備標識和所申請證書的核身要求，伺服器端保存用戶標識、用戶端所在設備標識、下發證書標識、和下發證書的已通過核身方式的對應關係。其中，用戶標識是在伺服器端能夠唯一代表一個用戶帳戶的資訊，例如，用戶帳戶名稱、用戶帳戶在伺服器端的識別碼等。這些應用場景中，用戶端需要提供用戶標識和設備標識，伺服器端才能在保存的對應關係中查找到已經下發給具有相同設備標識的用戶端、並且屬於具有該用戶標識的用戶的證書（即用戶端的已有證書）。

可見，本說明書的實施例一中，伺服器端從用戶端在證書申請請求中提取設備標識和證書的核身要求，在用戶端通過每種要素核身方式的身份認證後，下發證書並保存設備標識、證書標識和已通過核身方式的對應關係，該對應關係能夠在某個證書的已通過核身方式滿足某項業務對證書的核身要求時，將該證書多工於該項業務，在滿足業務需求的條件下減少了證書數量，節約了設備的資源，減少了用戶操作。

本說明書的實施例二提出一種新的數位證書使用的實現方法，伺服器端根據用戶端發送的證書核身要求指定的要

素核身方式，在該用戶端所在設備的已有證書中查找滿足核身要求的已有證書標識，並指令用戶端使用滿足核身要求的已有證書，從而使得已有證書能夠在滿足業務需求的前提下多工於多項業務，減少了用戶端的證書數量，也減少了用戶申請證書的操作。

本說明書的實施例二中，伺服器維護有用戶端所在設備的設備標識、用戶端的已有證書標識和該已有證書的已通過核身方式的對應關係。其中，已有證書是伺服器已經下發給該用戶端的證書；某個已有證書的已通過核身方式包括在申請和使用該證書的過程中，用戶通過身份認證的每種核身方式。

類似於實施例一，在可能有不同的用戶使用同一個設備來進行業務，或者同一個用戶在同一個設備上使用不同的帳戶來進行業務的應用場景中，伺服器維護有使用用戶端的用戶標識、用戶端所在設備的設備標識、用戶端的已有證書標識和該已有證書的已通過核身方式的對應關係。在這些應用場景中，伺服器同時採用用戶標識和設備標識來查找對應的已有證書標識。

本實施例中，對設備標識、已有證書標識（一種證書標識）、核身要求、要素核身方式的說明請參見實施例一，不再重複。

本說明書的實施例二中，數位證書使用的實現方法運行在伺服端的流程如圖2所示，運行在用戶端的流程如圖3所示。

在用戶端，步驟 310，向伺服器發送證書使用請求。

在伺服器端，步驟 210，接收用戶端的證書使用請求。

當用戶端所在設備進行某項業務，需要使用數位證書時，用戶端將所在設備的設備標識（或用戶標識及設備標識）、和該項業務對證書的核身要求封裝在證書使用請求中，發送給伺服器端。

在伺服器端，步驟 220，根據維護的對應關係，查找與設備標識對應的、並且滿足核身要求的已有證書標識。

伺服器端從接收的證書使用請求中提取設備標識（或用戶標識及設備標識）、和證書的核身要求，在本端維護的對應關係中，找到對應於證書使用請求中設備標識（或對應於用戶標識及設備標識）的每個已有證書標識，如果某個已有證書標識的已通過核身方式中包括該證書使用請求攜帶的核身要求指定的每種要素核身方式，則該已有證書標識為滿足該核身要求的已有證書標識。

在伺服器端，步驟 230，向用戶端發送證書使用指令，證書使用指令中包括滿足核身要求的已有證書標識。

在用戶端，步驟 320，從伺服器端接收證書使用指令。

在用戶端，步驟 330，採用具有證書使用指令中已有證書標識的證書進行簽名。

如果伺服器端找到滿足該證書使用請求中核身要求的已有證書標識，則向用戶端發送證書使用指令，在證書使用指令中攜帶滿足核身要求的已有證書標識。用戶端在收到證書使用指令後，採用證書使用指令中伺服器端指定的已有

證書來進行簽名。

如果伺服端找到的滿足核身要求的已有證書標識超過一個，伺服端可以將其中的一個在證書使用指令中發送給用戶端；也可以將其中的部分或全部在證書使用指令中發送給用戶端，由用戶端選擇其中的一個已有證書標識，用具有該標識的已有證書來進行簽名。

如果與證書使用請求中設備標識對應的（或與用戶標識及設備標識對應的）每個已有證書標識都不滿足核身要求，伺服端在與設備標識對應的（或與用戶標識及設備標識對應的）已有證書標識中，查找已通過核身方式與證書使用請求中核身要求指定的要素核身方式中至少有一種核身方式相同的已有證書標識。如果存在這樣的已有證書標識，伺服端在其中確定一個到多個來將其作為可升級證書標識，可升級證書標識的已通過核身方式與核身要求指定的要素核身方式中有一種到多種核身方式是相同的。如果伺服端找不到可升級證書標識，也即當所有已有證書標識的已通過核身方式都與核身要求指定的每種要素核身方式均不相同時，伺服端可以指令用戶端進行新證書的申請流程（參見實施例一）。

伺服端在確定可升級證書標識時，可以將與證書使用請求中設備標識對應的（或與用戶標識及設備標識對應的）、升級核身方式數量最少的已有證書標識作為可升級證書標識。如果核身要求包括兩個或兩個以上的核身方式組，則可以遍歷每個核身方式組來發現升級核身方式數量

最少的已有證書標識。在一種實現方式中，可以在伺服器端採用貪婪演算法、A*演算法（一種用於查找最優解的演算法）或Top K演算法（一種用來查找最符合要求的K個目標物件的演算法）來選擇出升級核身方式數量最少的已有證書標識，並確定其中的至少一個作為可升級證書標識。

對每種可升級證書標識，伺服器端比較證書使用請求中核身要求指定的要素核身方式、與可升級證書標識的已通過核身方式，將要素核身方式中不同於已通過核身方式的所有核身方式作為該可升級證書的升級核身方式。也就是說，升級核身方式是滿足核身要求所需要、但某個可升級證書尚未通過的核身方式。

伺服器端將可升級證書標識的升級核身方式發送給用戶端。如果可升級證書標識超過一個，可以由伺服器端選擇其中一個的可升級證書標識的升級核身方式發送給用戶端；也可以由伺服器端將至少兩個可升級證書標識及其升級核身方式發送給用戶端，當用戶端從伺服器端接收的可升級證書標識超過一個時，可以選擇其中一個可升級證書標識，採用所選擇的可升級證書標識的每種升級核身方式進行身份認證。在用戶端可以由業務運行功能模組來選擇可升級證書標識，也可以由用戶來選擇，本實施例中不做限定。

在一個例子中，當與設備標識對應的（或與用戶標識及設備標識對應的）已有證書標識不滿足核身要求、並且伺服器端發現存在可升級證書標識時，向用戶端發送已有證書可升級的通知。用戶端收到已有證書可升級的通知，提

示用戶可以對已有的證書採用附加身份認證的方式來進行升級，向用戶詢問是否進行升級。如果用戶端收到用戶的確認操作，則向伺服器端發送已有證書升級的確認；如果收到用戶的拒絕操作，則啟動新證書的申請流程。伺服器端收到用戶端進行已有證書升級的確認後，再向用戶端發送可升級證書標識的升級核身方式。

用戶端在從伺服器端收到至少一個可升級證書標識的升級核身方式後，採用一個可升級證書標識的升級核身方式來進行身份認證。在用戶端通過該可升級證書標識的每種升級核身方式的身份認證後，該可升級證書標識已滿足證書使用請求中的核身要求，伺服器端將該可升級證書標識封裝在證書使用指令中發送給用戶端。用戶端收到證書使用指令，採用具有證書使用指令中具有證書使用指令中可升級證書標識的證書進行簽名。

這樣，當已有證書不能滿足某項業務的核身要求時，如果已有證書的已通過核身方式中有與核身要求指定的要素核身方式相同的核身方式，可以通過令用戶進行升級核身方式的身份認證，對已有證書進行升級，使其稱為滿足該項業務核身要求的證書，避免了申請新的證書，並且用戶只需進行部分要素核身方式的身份認證，也減少了用戶的操作，提高了用戶的效率。

類似於實施例一，本實施例中，根據實際應用場景中伺服器端和用戶端的實現、以及對證書申請的安全性要求，用戶端進行身份認證、伺服器端獲知用戶端通過認證、伺服

端下發證書使用指令的具體過程可以採用不同的互動流程實現，例如現有技術中證書使用過程中的各種互動流程，不再贅述。

在用戶端通過某個可升級證書標識的每種升級核身方式的身份認證後，伺服器根據用戶端通過的升級核身方式，更新所維護的對應關係中該可升級證書標識的已通過核身方式，在該可升級證書標識的已通過核身方式中添加用戶端通過的所有升級核身方式。

可見，在本說明書的實施例二中，在伺服器維護用戶端所在設備標識、已有證書標識、和已有證書的已通過核身方式的對應關係，伺服器根據用戶端發送的證書核身要求指定的要素核身方式，在該用戶端所在設備的已有證書中查找滿足核身要求的已有證書標識，並指令用戶端使用滿足核身要求的已有證書，使得當用戶端的已有證書能夠滿足某項業務對證書的核身要求時，該項業務可以使用已有證書而不需申請新的證書，減少了用戶端的證書數量，也減少了用戶申請證書的操作。

上述對本說明書特定實施例進行了描述。其它實施例在所附申請專利範圍的範圍內。在一些情況下，在申請專利範圍中記載的動作或步驟可以按照不同於實施例中的順序來執行並且仍然可以實現期望的結果。另外，在附圖中描繪的過程不一定要求顯示的特定順序或者連續順序才能實現期望的結果。在某些實施方式中，多工處理和並行處理也是可以的或者可能是有利的。

在本說明書的一個應用示例中，第三方支付平臺的伺服器端包括證書管理伺服器和核身伺服器。第三方支付平臺的用戶端 App 運行在用戶終端上，App 中包括證書 SDK（Software Development Kit，軟體開發套件）模組。本應用實例中，新的證書由負責發放、管理和廢除數位證書的 CA（Certificate Authority，證書認證）機構的 CA 伺服器來發放。

當用戶在用戶端 App 內申請證書時，證書 SDK 模組、證書管理伺服器、核身伺服器和 CA 伺服器之間的互動流程如圖 4 所示。

證書 SDK 模組將用戶標識、用戶端所在設備的標識、業務對證書的核身要求封裝在證書申請請求中，發送給證書管理伺服器。

證書管理伺服器提取證書申請請求中證書核身要求指定的要素核身方式，向核身伺服器查詢該用戶和該設備可用的核身方式。如果核身伺服器返回的可用核身方式包括核身要求指定的要素核身方式，證書管理伺服器向證書 SDK 模組返回可用核身方式清單，否則告知 SDK 模組不支援當前證書的申請。

證書 SDK 模組收到可用核身方式清單，如果核身要求包括超過一個核身方式組，則按照可用核身方式清單選擇一個核身方式組的要素核身方式作為核身要求指定的要素核身方式，告知用戶申請證書需要進行哪幾項核身方式的身份認證。

通過用戶的操作，證書 SDK 模組與核身伺服器逐個採用核身要求指定的要素核身方式進行身份認證。

在用戶通過每種要素核身方式的身份認證後，證書 SDK 模組向證書管理伺服器發送核身通過通知。證書 SDK 模組在核身通過通知中攜帶證書申請資訊，證書申請資訊包括所申請證書要求提供的各種資訊，如 CSR（Certificate Signing Request，證書請求檔）、公開金鑰等。

證書管理伺服器向核身伺服器查詢用戶要素核身方式的身份認證結果，在收到核身伺服器的確認後，向 CA 伺服器提交證書請求，證書請求中攜帶 CSR、公開金鑰、證書 SDK 模組所在設備的標識等。

在收到 CA 伺服器頒發的證書後，證書管理伺服器記錄用戶標識、設備標識、已有證書序號（一種已下發證書的證書標識）和該已有證書的要素核身方式的對應關係，並將證書發送給證書 SDK 模組。

證書 SDK 模組安裝收到的證書，在安裝成功後向證書管理服務發送證書安裝成功的通知。在收到證書安裝成功的通知後，證書管理伺服器將記錄的對應關係持久化保存起來。

當用戶在用戶端 App 內運行某項業務，該業務需要使用證書時，證書 SDK 模組、證書管理伺服器和核身伺服器之間的互動流程如圖 5 所示。

用戶通過用戶端 App 向證書 SDK 模組申請數位證書簽名，將用戶標識、證書的核身要求和待簽名原文傳遞給證

書 SDK 模組。其中，證書的核身要求可以包括兩個或兩個以上的核身方式組，每個核身方式組可以指定一個到多個要素核身方式。

證書的核身要求可以採用核身方式的邏輯運算式來轉義，例如，運算式 [SMS && FACE || IDCARD && EMAIL && FINGERPRINT]，表示核身要求包括兩個核身方式組，第一個核身方式組的要素核身方式是簡訊和人臉，第二個核身方式組的要素核身方式是身份證、郵件和指紋。

證書 SDK 模組向證書管理伺服器發送證書使用請求，證書使用請求中攜帶用戶標識、設備標識、證書的核身要求和待簽名原文。

證書管理伺服器在維護的對應關係中，查詢對應於用戶標識及設備標識的已有證書序號中，是否有滿足核身要求的已有證書序號。對包括若干核身方式組的核身要求，當已有證書序號的已通過核身方式包括任意一個核身方式組指定的每種要素核身方式時，該已有證書序號滿足核身要求。證書管理伺服器通過動態指令碼語言將核身要求轉換為可運行的決策邏輯，來對已有證書序號是否滿足核身要求進行判斷。

如果存在滿足核身要求的已有證書序號，證書管理伺服器向證書 SDK 模組發送證書使用指令（圖 5 中未顯示），攜帶滿足核身要求的已有證書序號。證書 SDK 模組使用證書管理伺服器在證書使用指令中指定序號的已有證書進行數位簽章（圖 5 中未顯示）。

當不存在滿足核身要求的已有證書序號時，證書管理伺服器在已有證書序號中，查找已通過核身方式與核身要求指定的要素核身方式至少有一個相同的已有證書序號，採用貪婪演算法在這些已有證書序號中挑選出升級核身方式數量最少的作為可升級證書序號（一種可升級證書標識）。證書管理伺服器將可升級證書序號及其升級核身方式發送給證書 SDK 模組。

證書 SDK 模組告知用戶有一個已有證書可用來簽名，不需要再重新安裝，但是需要額外再做一些身份認證，來升級證書。在得到用戶的確認操作後，證書 SDK 模組啟動身份認證流程，通過用戶的操作，證書 SDK 模組與核身伺服器逐個採用一個可升級證書序號的升級核身方式進行身份認證。

在用戶通過每種升級核身方式的身份認證後，證書 SDK 模組向證書管理伺服器發送核身通過通知。

證書管理伺服器向核身伺服器查詢用戶升級核身方式的身份認證結果，在收到核身伺服器的確認後，證書管理伺服器更新維護的對應關係，將用戶通過的升級核身方式添加到對應關係中與用戶標識、設備標識對應的已有證書序號的已通過核身方式中。

證書管理伺服器向用戶端發送證書使用指令，其中攜帶伺服端生成的簽名內容、待簽名原文、用戶標識、滿足核身要求的已有證書序號、伺服端證書簽名等。

證書 SDK 模組在收到證書使用指令後，使用其中指定

序號的已有證書，對簽名內容進行簽名。

與上述流程實現對應，本說明書的實施例還提供了一種數位證書申請的實現裝置、一種應用在伺服器端的數位證書使用的實現裝置、和一種應用在用戶端的數位證書使用的實現裝置。這三種裝置均可以通過軟體實現，也可以通過硬體或者軟硬體結合的方式實現。以軟體實現為例，作為邏輯意義上的裝置，是通過用戶端或伺服器端所在設備的CPU（Central Process Unit，中央處理器）將對應的電腦程式指令讀取到記憶體中運行形成的。從硬體層面而言，除了圖6所示的CPU、記憶體以及記憶體之外，數位證書申請的實現裝置或數位證書使用的實現裝置所在的設備通常還包括用於進行無線訊號收發的晶片等其他硬體，和/或用於實現網路通訊功能的板卡等其他硬體。

圖7所示為本說明書實施例提供的一種數位證書申請的實現裝置，應用在伺服器端，所述裝置包括證書申請請求接收單元、證書下發單元和對應關係保存單元，其中：證書申請請求接收單元用於接收用戶端的證書申請請求，所述證書申請請求中包括用戶端的設備標識和所述證書的核身要求；所述核身要求指定至少一種要素核身方式；證書下發單元用於在用戶端通過核身要求指定的要素核身方式的身份認證後，將證書下發給用戶端；對應關係保存單元用於保存所述設備標識、所述證書標識、所述證書的已通過核身方式的對應關係。

可選的，所述核身要求包括至少一個核身方式組，每

個核身方式組指定至少一種要素核身方式；所述核身要求指定的要素核身方式，包括：核身要求的一個核身方式組指定的所有要素核身方式。

可選的，所述證書申請請求中還包括：用戶標識；所述保存設備標識、所述證書標識、所述證書的已通過核身方式的對應關係；包括：保存用戶標識、所述設備標識、所述證書標識、所述證書的已通過核身方式的對應關係。

圖8所示為本說明書實施例提供的一種數位證書使用的實現裝置，伺服器維護有用戶端的設備標識、所述用戶端的已有證書標識、所述已有證書的已通過核身方式的對應關係，所述裝置包括證書使用請求接收單元、可用證書查找單元和證書多工指令發送單元，其中：證書使用請求接收單元用於接收用戶端的證書使用請求，所述證書使用請求中包括用戶端的設備標識和所述證書的核身要求；所述核身要求指定至少一種要素核身方式；可用證書查找單元用於根據所述對應關係，查找與所述設備標識對應的、並且滿足核身要求的已有證書標識；所述滿足核身要求的已有證書標識為：已通過核身方式中包括核身要求指定的每種要素核身方式的已有證書標識；證書多工指令發送單元用於向用戶端發送證書使用指令，所述證書使用指令中包括滿足核身要求的已有證書標識。

一種實現方式中，所述裝置還包括可升級證書標識單元、升級核身方式發送單元和升級證書使用指令發送單元，其中：可升級證書標識單元用於當與所述設備標識對

應的已有證書標識不滿足核身要求時，確定至少一個與所述設備標識對應的已有證書標識作為可升級證書標識，所述可升級證書標識的已通過核身方式與所述要素核身方式中至少有一種相同；升級核身方式發送單元用於向用戶端發送可升級證書標識的升級核身方式，所述升級核身方式為所述要素核身方式中與所述可升級證書標識的已通過核身方式不同的所有核身方式；升級證書使用指令發送單元用於在用戶端通過一個可升級證書標識的每種升級核身方式的身份認證後，向用戶端發送證書使用指令，所述證書使用指令中包括滿足核身要求的可升級證書標識。

上述實現方式中，所述裝置還可以包括對應關係更新單元，用於根據用戶端通過的升級核身方式，更新所維護的對應關係中所述滿足核身要求的可升級證書標識對應的已通過核身方式。

上述實現方式中，所述可升級證書標識單元具體用於：當所述設備標識對應的已有證書標識不滿足核身要求時，確定至少一個與所述設備標識對應的、升級核身方式數量最少的已有證書標識作為可升級證書標識。

上述實現方式中，所述可升級證書標識單元確定至少一個與所述設備標識對應的升級核身方式數量最少的已有證書標識，包括：採用貪婪演算法、A*演算法或Top K演算法選擇升級核身方式數量最少的已有證書標識。

上述實現方式中，所述可升級證書標識單元具體用於：當與所述設備標識對應的已有證書標識不滿足核身要

求、並且存在與所述設備標識對應的可升級證書標識時，向用戶端發送已有證書可升級的通知；在收到用戶端進行已有證書升級的確認後，確定至少一個與所述設備標識對應的已有證書標識作為可升級證書標識。

上述實現方式中，所述升級核身發送單元具體用於：向用戶端發送至少兩個可升級證書標識及其升級核身方式，供用戶端選擇其中一個可升級證書標識，採用所選擇的可升級證書標識的升級核身方式進行身份認證。

上述實現方式中，所述對應關係包括：用戶標識、用戶端的設備標識、所述用戶端的已有證書標識、所述已有證書的已通過核身方式的對應關係；所述證書使用請求中還包括：用戶標識；所述與設備標識對應的已有證書標識包括：所述用戶標識、所述設備標識對應的已有證書標識。

可選的，所述核身要求包括至少一個核身方式組，每個核身方式組指定至少一種要素核身方式；所述由核身要求指定的至少一種要素核身方式，包括：核身要求的一個核身方式組指定的所有要素核身方式。

圖9所示為本說明書實施例提供的一種數位證書使用的實現裝置，包括證書使用請求發送單元、證書多工指令接收單元和證書多工單元，其中：證書使用請求發送單元用於向伺服器發送證書使用請求，所述證書使用請求中包括用戶端的設備標識和所述證書的核身要求；所述核身要求指定至少一種要素核身方式，供伺服器根據維護的用戶

端的設備標識、已有證書標識、所述已有證書的已通過核身方式的對應關係，查找已通過核身方式中包括所述核身要求指定的每種要素核身方式的、與所述證書使用請求中設備標識對應的已有證書標識；證書多工指令接收單元用於從伺服端接收證書使用指令，所述證書使用指令中包括滿足核身要求的已有證書標識；證書多工單元用於採用具有證書使用指令中已有證書標識的證書進行簽名。

一種實現方式中，所述裝置還可以包括升級核身方式接收單元、升級證書使用指令接收單元和升級證書使用單元，其中：升級核身方式接收單元用於從伺服端接收至少一個可升級證書標識的升級核身方式；所述可升級證書標識為已通過核身方式與所述要素核身方式中至少有一種相同的、與所述設備標識對應的已有設備標識；所述升級核身方式為所述要素核身方式中與所述可升級證書標識的已通過核身方式不同的所有核身方式；升級證書使用指令接收單元用於在通過一個可升級證書標識的每種升級核身方式的身份認證後，從伺服端接收證書使用指令，所述證書使用指令中包括滿足核身要求的可升級證書標識；升級證書使用單元用於採用具有證書使用指令中可升級證書標識的證書進行簽名。

上述實現方式中，所述升級核身方式接收單元具體用於：從伺服端接收已有證書可升級的通知；在收到用戶的確認操作後，向伺服端發送已有證書升級的確認；從伺服端接收至少一個可升級證書標識的升級核身方式。

上述實現方式中，所述裝置還可以包括可升級證書選擇單元，用於當從伺服端接收的可升級證書標識超過一個時，選擇其中一個可升級證書標識，採用所選擇的可升級證書標識的每種升級核身方式進行身份認證。

上述實現方式中，所述伺服端維護的對應關係包括：用戶標識、用戶端的設備標識、所述用戶端的已有證書標識、所述已有證書的已通過核身方式的對應關係；所述證書使用請求中還包括：用戶標識；所述與設備標識對應的已有證書標識包括：所述用戶標識、所述設備標識對應的已有證書標識。

可選的，所述核身要求包括至少一個核身方式組，每個核身方式組指定至少一種要素核身方式；所述由核身要求指定的至少一種要素核身方式，包括：核身要求的一個核身方式組指定的所有要素核身方式。

本說明書的實施例提供了一種電腦設備，該電腦設備包括記憶體和處理器。其中，記憶體上儲存有能夠由處理器運行的電腦程式；處理器在運行儲存的電腦程式時，執行本說明書實施例中應用在伺服端的數位證書申請的實現方法的各個步驟。對應用在伺服端的數位證書申請的實現方法的各個步驟的詳細描述請參見之前的內容，不再重複。

本說明書的實施例提供了一種電腦設備，該電腦設備包括記憶體和處理器。其中，記憶體上儲存有能夠由處理器運行的電腦程式；處理器在運行儲存的電腦程式時，執

行本說明書實施例中應用在伺服器端的數位證書使用的實現方法的各個步驟。對應用在伺服器端的數位證書使用的實現方法的各個步驟的詳細描述請參見之前的內容，不再重複。

本說明書的實施例提供了一種電腦設備，該電腦設備包括記憶體和處理器。其中，記憶體上儲存有能夠由處理器運行的電腦程式；處理器在運行儲存的電腦程式時，執行本說明書實施例中應用在用戶端的數位證書使用的實現方法的各個步驟。對應用在用戶端的數位證書使用的實現方法的各個步驟的詳細描述請參見之前的內容，不再重複。

本說明書的實施例提供了一種電腦可讀儲存媒體，該儲存媒體上儲存有電腦程式，這些電腦程式在被處理器運行時，執行本說明書實施例中應用在伺服器端的數位證書申請的實現方法的各個步驟。對應用在伺服器端的數位證書申請的實現方法的各個步驟的詳細描述請參見之前的內容，不再重複。

本說明書的實施例提供了一種電腦可讀儲存媒體，該儲存媒體上儲存有電腦程式，這些電腦程式在被處理器運行時，執行本說明書實施例中應用在伺服器端的數位證書使用的實現方法的各個步驟。對應用在伺服器端的數位證書使用的實現方法的各個步驟的詳細描述請參見之前的內容，不再重複。

本說明書的實施例提供了一種電腦可讀儲存媒體，該

儲存媒體上儲存有電腦程式，這些電腦程式在被處理器運行時，執行本說明書實施例中應用在用戶端的數位證書使用的實現方法的各個步驟。對應用在用戶端的數位證書使用的實現方法的各個步驟的詳細描述請參見之前的內容，不再重複。

以上所述僅為本說明書的較佳實施例而已，並不用以限制本發明，凡在本發明的精神和原則之內，所做的任何修改、等同替換、改進等，均應包含在本發明保護的範圍之內。

在一個典型的配置中，計算設備包括一個或多個處理器（CPU）、輸入/輸出介面、網路介面和記憶體。

記憶體可能包括電腦可讀媒體中的非永久性記憶體，隨機存取記憶體（RAM）和/或非揮發性記憶體等形式，如唯讀記憶體（ROM）或快閃記憶體（flash RAM）。記憶體是電腦可讀媒體的示例。

電腦可讀媒體包括永久性和非永久性、可移動和非可移動媒體可以由任何方法或技術來實現資訊儲存。資訊可以是電腦可讀指令、資料結構、程式的模組或其他資料。電腦的儲存媒體的例子包括，但不限於相變記憶體（PRAM）、靜態隨機存取記憶體（SRAM）、動態隨機存取記憶體（DRAM）、其他類型的隨機存取記憶體（RAM）、唯讀記憶體（ROM）、電可抹除可程式設計唯讀記憶體（EEPROM）、快閃記憶體或其他記憶體技術、唯讀光碟唯讀記憶體（CD-ROM）、數位多功能光碟

（DVD）或其他光學儲存、磁盒式磁帶，磁帶磁磁片儲存或其他磁性存放裝置或任何其他非傳輸媒體，可用於儲存可以被計算設備存取的資訊。按照本文中的界定，電腦可讀媒體不包括暫存電腦可讀媒體（transitory media），如調變的資料訊號和載波。

還需要說明的是，術語“包括”、“包含”或者任何其他變體意在涵蓋非排他性的包含，從而使得包括一系列要素的過程、方法、商品或者設備不僅包括那些要素，而且還包括沒有明確列出的其他要素，或者是還包括為這種過程、方法、商品或者設備所固有的要素。在沒有更多限制的情況下，由語句“包括一個……”限定的要素，並不排除在包括所述要素的過程、方法、商品或者設備中還存在另外的相同要素。

本領域技術人員應明白，本說明書的實施例可提供為方法、系統或電腦程式產品。因此，本說明書的實施例可採用完全硬體實施例、完全軟體實施例或結合軟體和硬體態樣的實施例的形式。而且，本說明書的實施例可採用在一個或多個其中包含有電腦可用程式碼的電腦可用儲存媒體（包括但不限於磁碟記憶體、CD-ROM、光學記憶體等）上實施的電腦程式產品的形式。

【符號說明】

110-130：步驟

210-230：步驟

310-330：步驟

【發明申請專利範圍】

【第 1 項】

一種數位證書使用的實現方法，伺服器維護有用戶端的設備標識、所述用戶端的已有證書標識、所述已有證書的已通過核身方式的對應關係，所述方法包括：

接收用戶端的證書使用請求，所述證書使用請求中包括用戶端的設備標識和所述證書的核身要求；所述核身要求指定至少一種要素核身方式；

根據所述對應關係，查找與所述設備標識對應的、並且滿足核身要求的已有證書標識；所述滿足核身要求的已有證書標識為：已通過核身方式中包括核身要求指定的每種要素核身方式的已有證書標識；

向用戶端發送證書使用指令，所述證書使用指令中包括滿足核身要求的已有證書標識；

當與所述設備標識對應的已有證書標識不滿足核身要求時，確定至少一個與所述設備標識對應的已有證書標識作為可升級證書標識，所述可升級證書標識的已通過核身方式與所述要素核身方式中至少有一種相同；

向用戶端發送可升級證書標識的升級核身方式，所述升級核身方式為所述要素核身方式中與所述可升級證書標識的已通過核身方式不同的所有核身方式；

在用戶端通過一個可升級證書標識的每種升級核身方式的身份認證後，向用戶端發送證書使用指令，所述證書使用指令中包括滿足核身要求的可升級證書標識。

【第2項】

根據申請專利範圍第1項所述的方法，所述方法還包括：根據用戶端通過的升級核身方式，更新所維護的對應關係中所述滿足核身要求的可升級證書標識對應的已通過核身方式。

【第3項】

根據申請專利範圍第1項所述的方法，所述當與設備標識對應的已有證書標識不滿足核身要求時，確定至少一個與所述設備標識對應的已有證書標識作為可升級證書標識，包括：當所述設備標識對應的已有證書標識不滿足核身要求時，確定至少一個與所述設備標識對應的、升級核身方式數量最少的已有證書標識作為可升級證書標識。

【第4項】

根據申請專利範圍第3項所述的方法，所述確定至少一個與所述設備標識對應的升級核身方式數量最少的已有證書標識，包括：採用貪婪演算法、A*演算法或Top K演算法選擇升級核身方式數量最少的已有證書標識。

【第5項】

根據申請專利範圍第1項所述的方法，所述當與設備標識對應的已有證書標識不滿足核身要求時，確定至少一個與所述設備標識對應的已有證書標識作為可升級證書標識，包括：當與所述設備標識對應的已有證書標識不滿足核身要求、並且存在與所述設備標識對應的可升級證書標識時，向用戶端發送已有證書可升級的通知；在收到用戶

端進行已有證書升級的確認後，確定至少一個與所述設備標識對應的已有證書標識作為可升級證書標識。

【第6項】

根據申請專利範圍第1項所述的方法，所述向用戶端發送的可升級證書標識的升級核身方式，包括：至少兩個可升級證書標識及其升級核身方式，供用戶端選擇其中一個可升級證書標識，採用所選擇的可升級證書標識的升級核身方式進行身份認證。

【第7項】

根據申請專利範圍第1項所述的方法，所述對應關係包括：用戶標識、用戶端的設備標識、所述用戶端的已有證書標識、所述已有證書的已通過核身方式的對應關係；

所述證書使用請求中還包括：用戶標識；

所述與設備標識對應的已有證書標識包括：所述用戶標識和所述設備標識對應的已有證書標識。

【第8項】

根據申請專利範圍第1項所述的方法，所述核身要求包括至少一個核身方式組，每個核身方式組指定至少一種要素核身方式；

所述由核身要求指定的至少一種要素核身方式，包括：核身要求的一個核身方式組指定的所有要素核身方式。

【第9項】

一種數位證書使用的實現方法，包括：

向伺服器發送證書使用請求，所述證書使用請求中包括用戶端的設備標識和所述證書的核身要求；所述核身要求指定至少一種要素核身方式，供伺服器根據維護的用戶端的設備標識、已有證書標識、所述已有證書的已通過核身方式的對應關係，查找已通過核身方式中包括所述核身要求指定的每種要素核身方式的、與所述證書使用請求中設備標識對應的已有證書標識；

從伺服器接收證書使用指令，所述證書使用指令中包括滿足核身要求的已有證書標識；

採用具有證書使用指令中已有證書標識的證書進行簽名；

從伺服器接收至少一個可升級證書標識的升級核身方式；所述可升級證書標識為已通過核身方式與所述要素核身方式中至少有一種相同的、與所述設備標識對應的已有設備標識；所述升級核身方式為所述要素核身方式中與所述可升級證書標識的已通過核身方式不同的所有核身方式；

在通過一個可升級證書標識的每種升級核身方式的身份認證後，從伺服器接收證書使用指令，所述證書使用指令中包括滿足核身要求的可升級證書標識；

採用具有證書使用指令中可升級證書標識的證書進行簽名。

【第10項】

根據申請專利範圍第9項所述的方法，所述從伺服器

接收至少一個可升級證書標識的升級核身方式，包括：從伺服器端接收已有證書可升級的通知；在收到用戶的確認操作後，向伺服器端發送已有證書升級的確認；從伺服器端接收至少一個可升級證書標識的升級核身方式。

【第11項】

根據申請專利範圍第9項所述的方法，所述方法還包括：當從伺服器端接收的可升級證書標識超過一個時，選擇其中一個可升級證書標識，採用所選擇的可升級證書標識的每種升級核身方式進行身份認證。

【第12項】

根據申請專利範圍第9項所述的方法，所述伺服器端維護的對應關係包括：用戶標識、用戶端的設備標識、所述用戶端的已有證書標識、所述已有證書的已通過核身方式的對應關係；

所述證書使用請求中還包括：用戶標識；

所述與設備標識對應的已有證書標識包括：所述用戶標識和所述設備標識對應的已有證書標識。

【第13項】

根據申請專利範圍第9項所述的方法，所述核身要求包括至少一個核身方式組，每個核身方式組指定至少一種要素核身方式；

所述由核身要求指定的至少一種要素核身方式，包括：核身要求的一個核身方式組指定的所有要素核身方式。

【 第 14 項 】

一種電腦設備，包括：記憶體和處理器；所述記憶體上儲存有可由處理器運行的電腦程式；所述處理器運行所述電腦程式時，執行如申請專利範圍第 1 到 8 項中任意一項所述的步驟。

【 第 15 項 】

一種電腦設備，包括：記憶體和處理器；所述記憶體上儲存有可由處理器運行的電腦程式；所述處理器運行所述電腦程式時，執行如申請專利範圍第 9 到 13 項中任意一項所述的步驟。

【 第 16 項 】

一種電腦可讀儲存媒體，其上儲存有電腦程式，所述電腦程式被處理器運行時，執行如申請專利範圍第 1 到 8 項中任意一項所述的步驟。

【 第 17 項 】

一種電腦可讀儲存媒體，其上儲存有電腦程式，所述電腦程式被處理器運行時，執行如申請專利範圍第 9 到 13 項中任意一項所述的步驟。

【發明圖式】

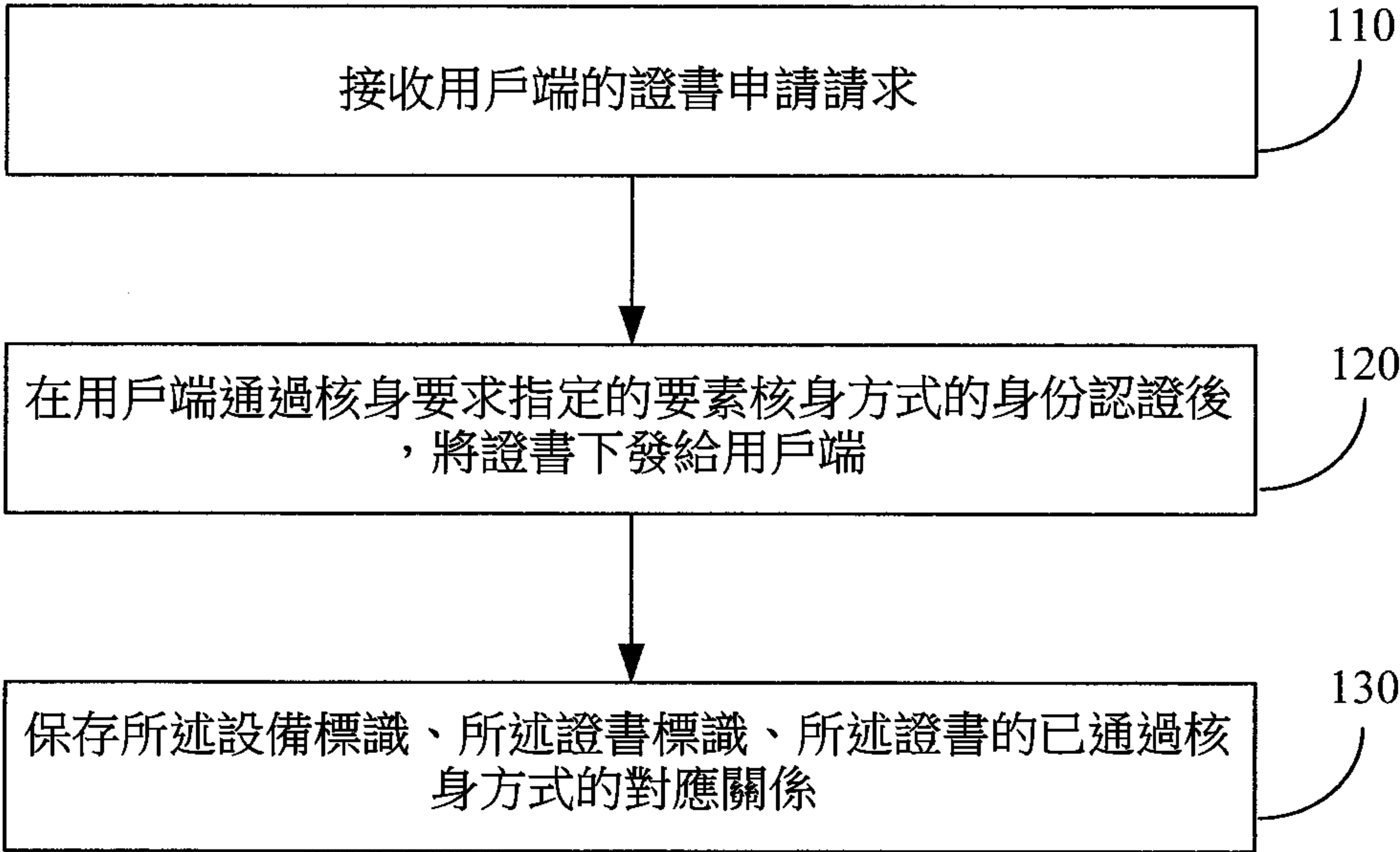


圖 1

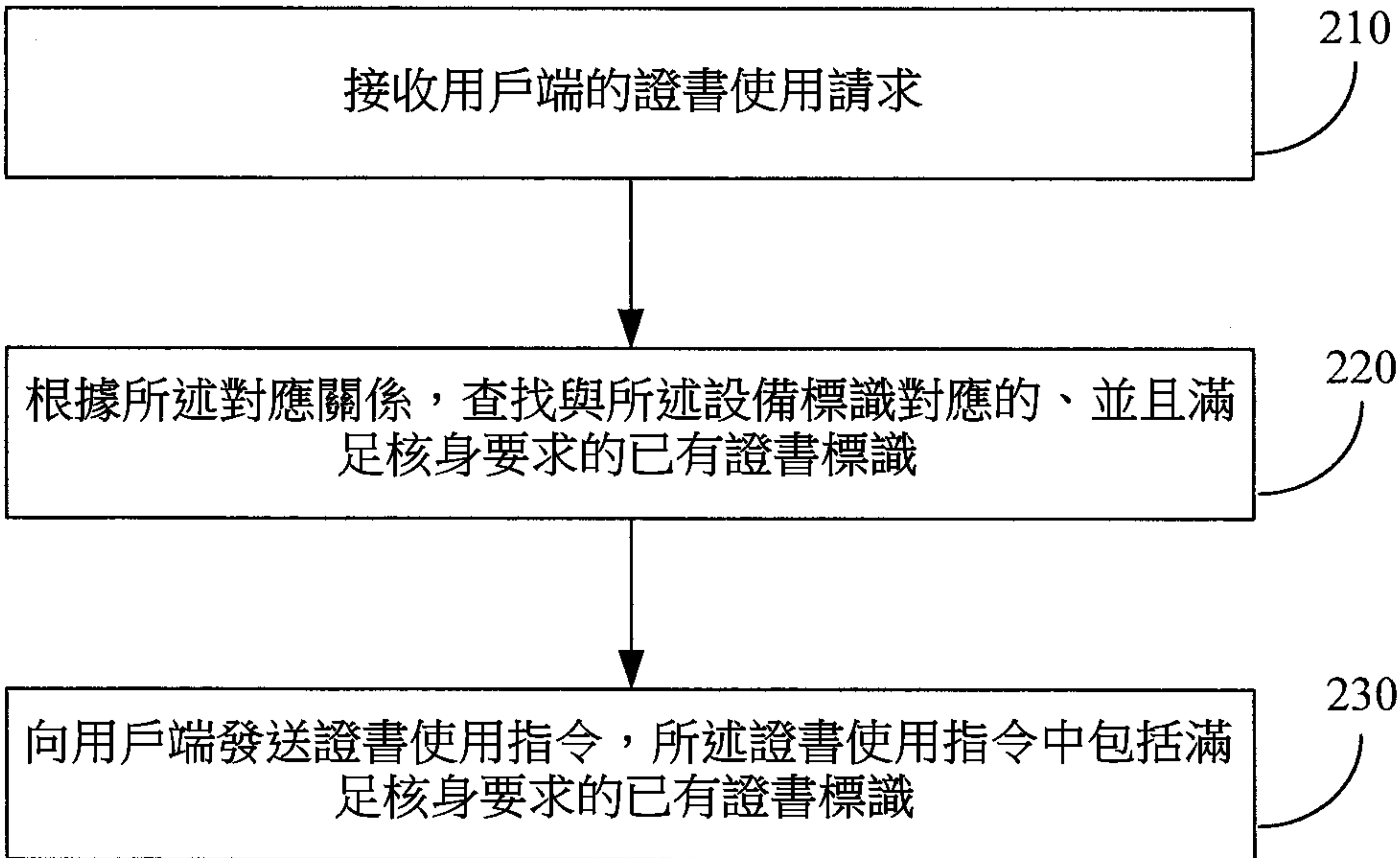


圖 2

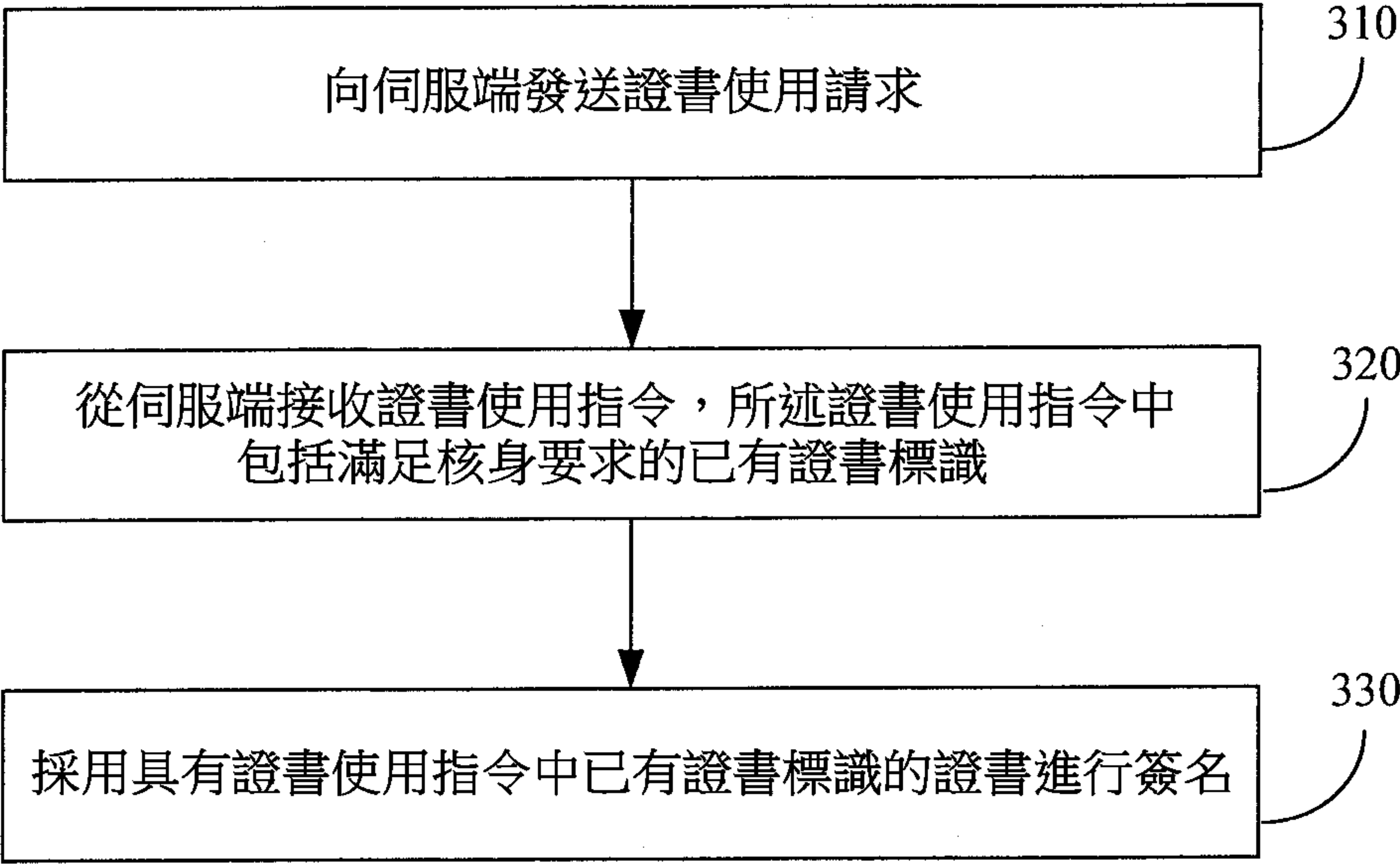


圖 3

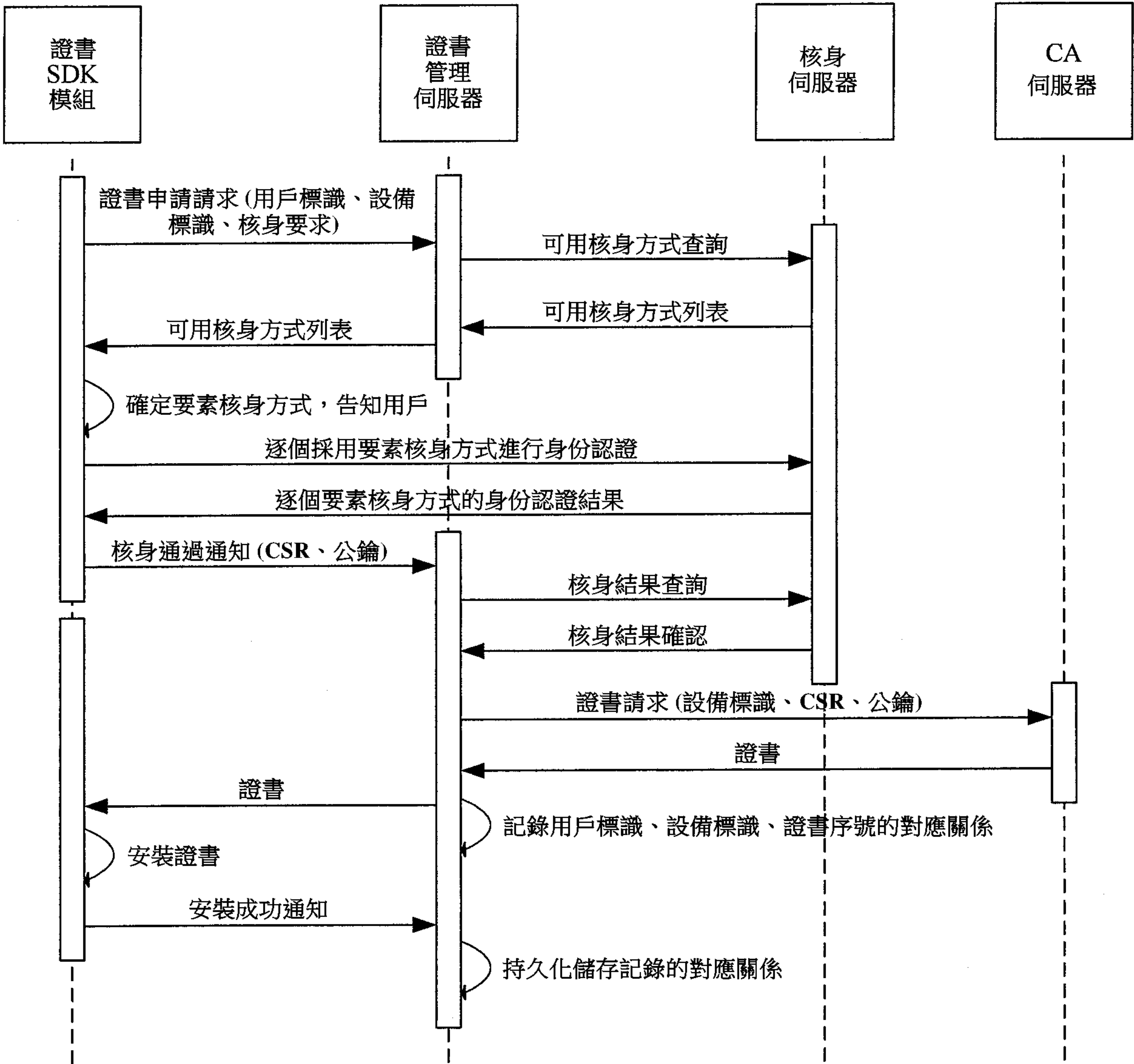


圖 4

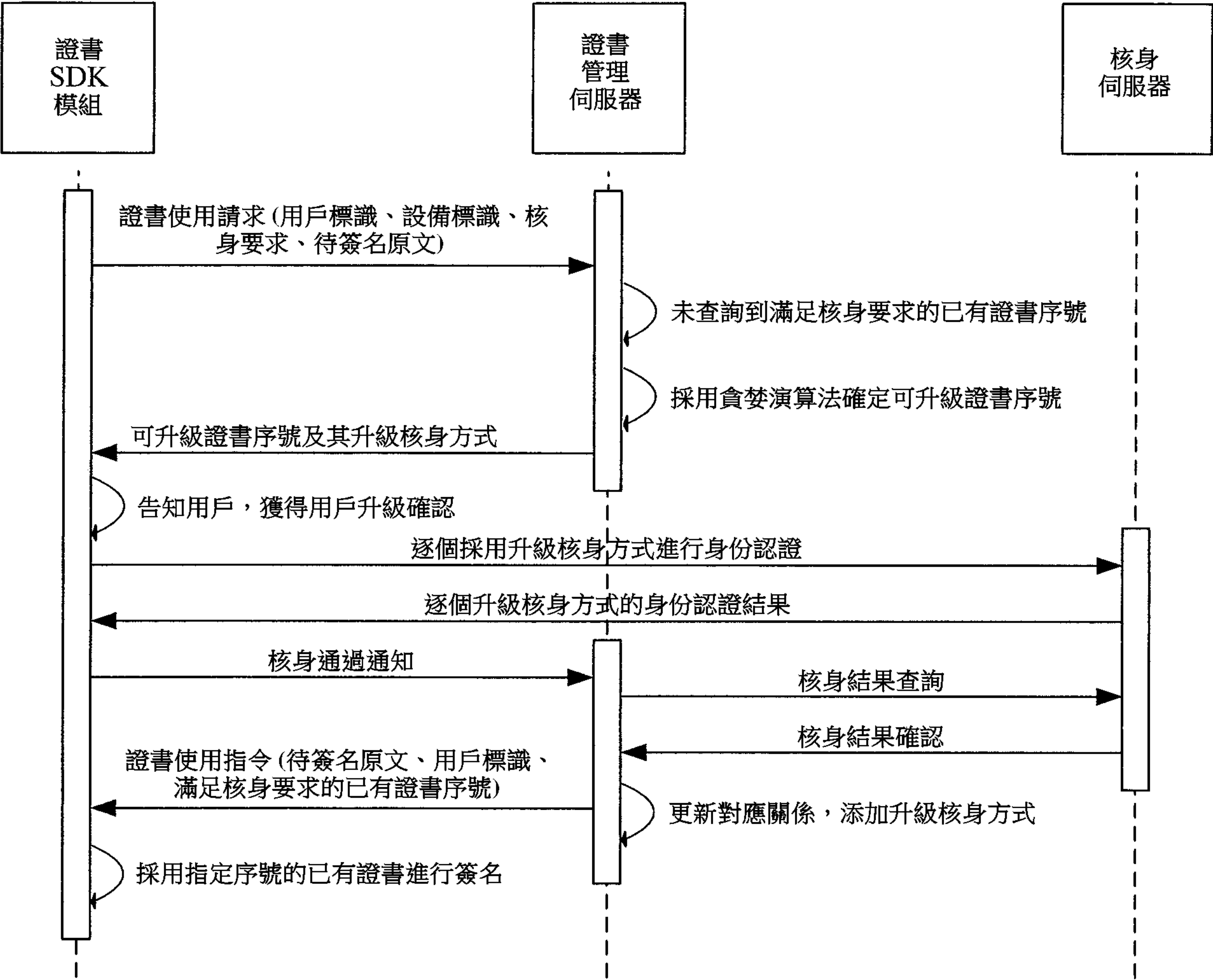


圖 5

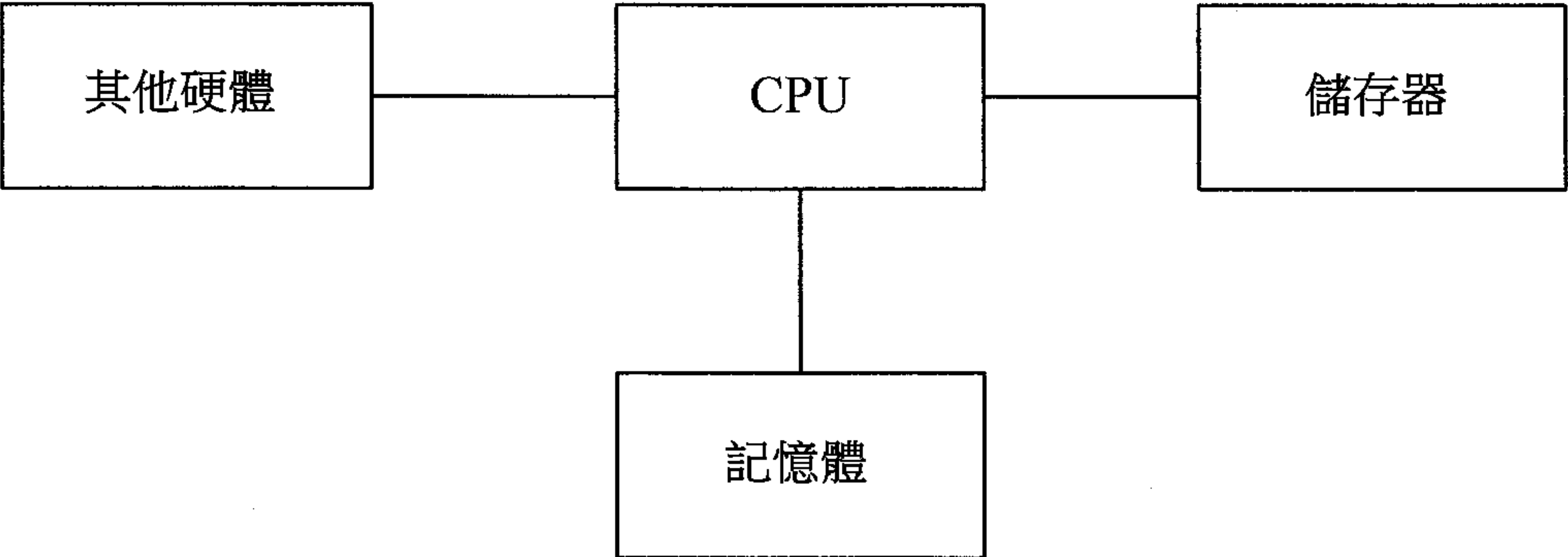


圖 6

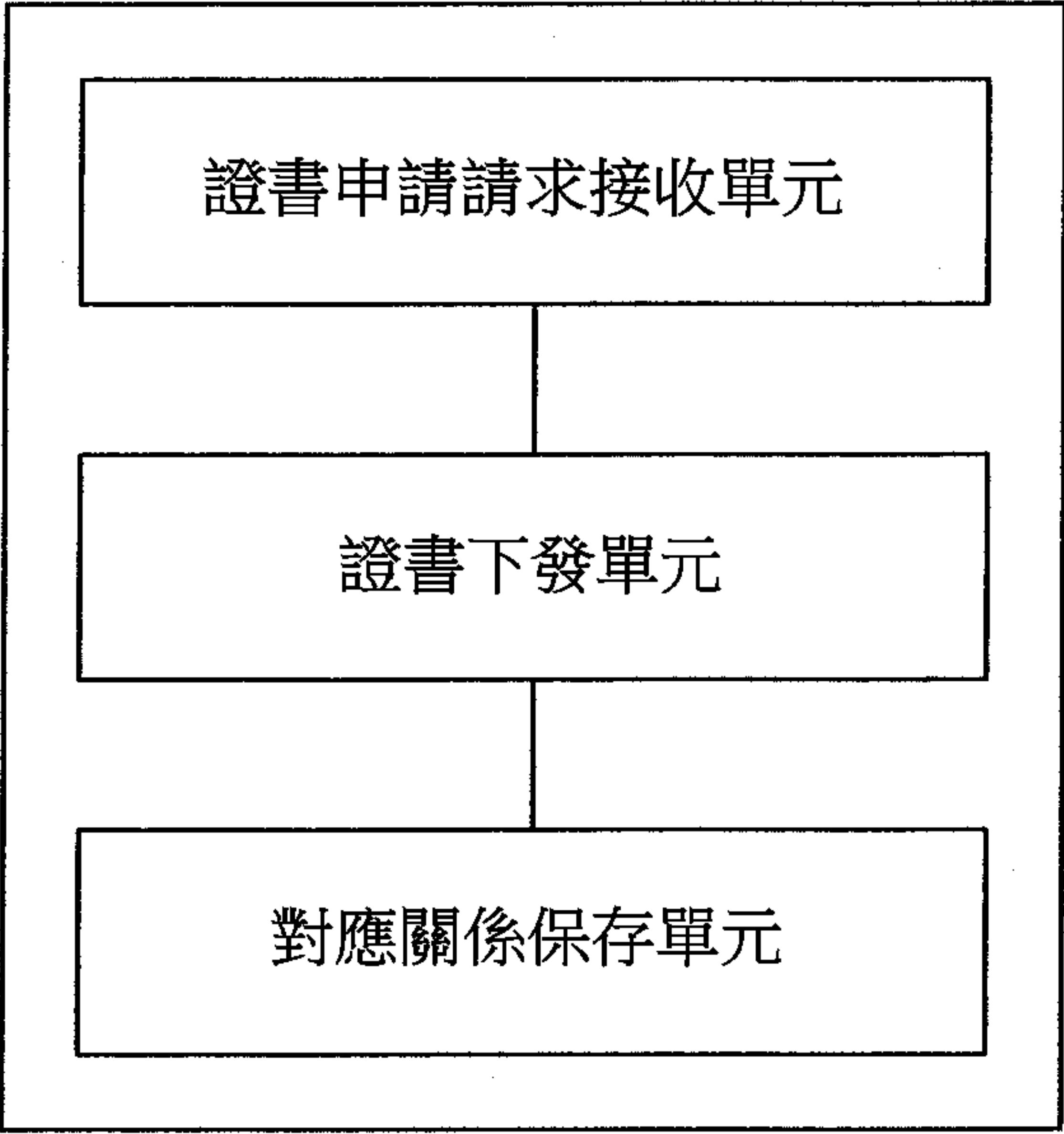


圖 7

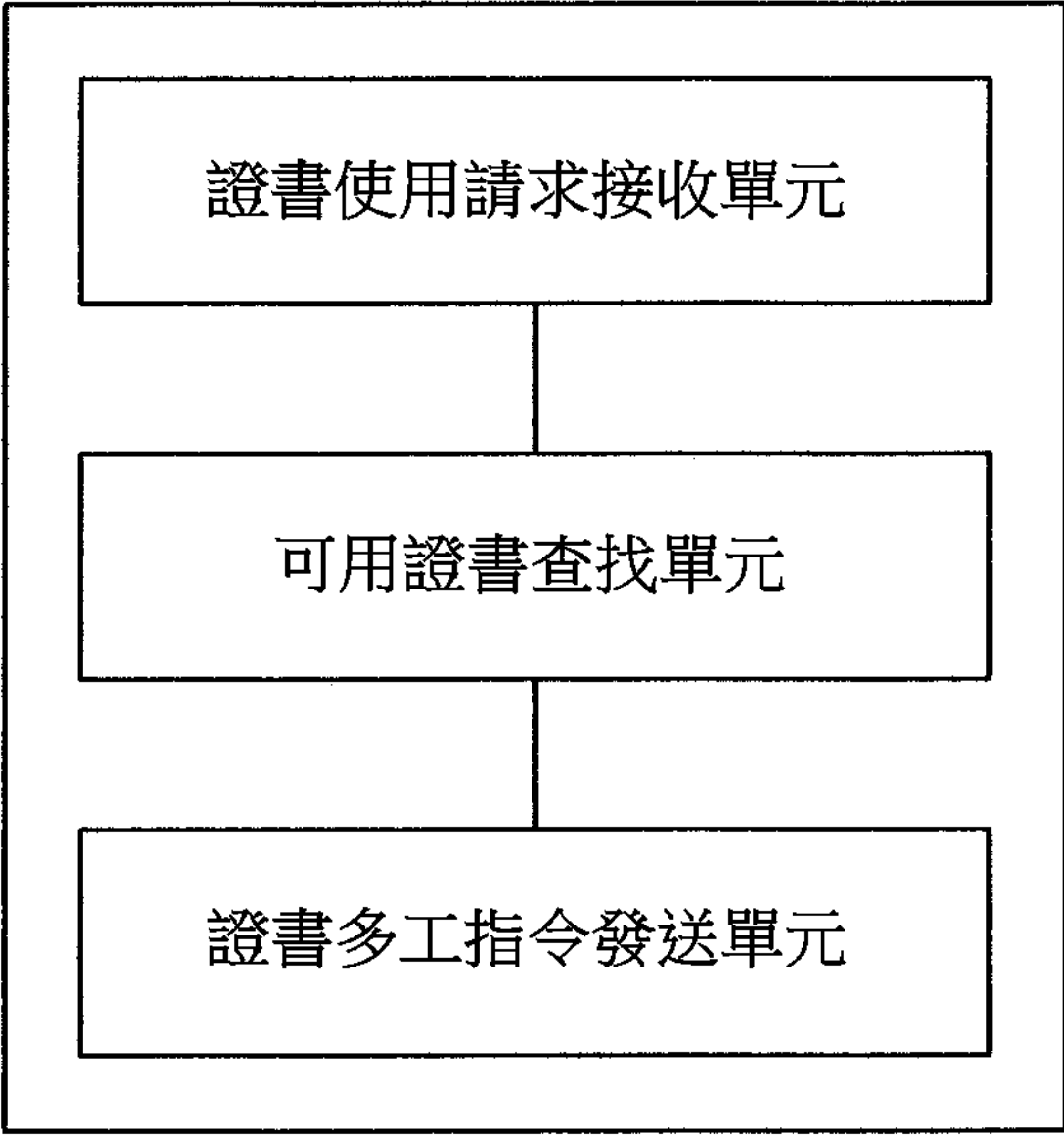


圖 8

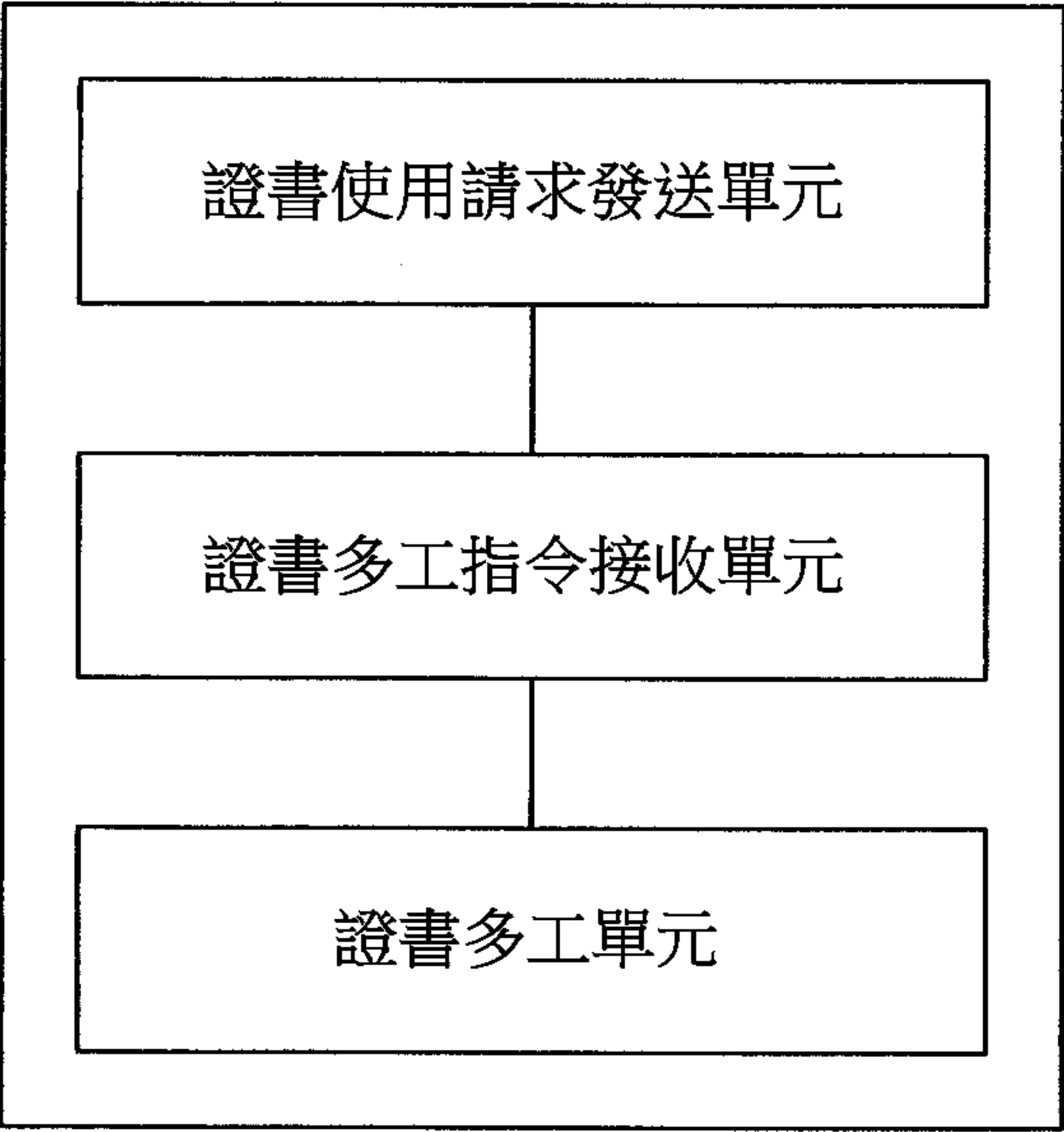


圖 9