I718567

(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 I718567 B**

(45)公告日： 中華民國 110 (2021) 年 02 月 11 日

(21)申請案號：108121717　(22)申請日： 中華民國 108 (2019) 年 06 月 21 日

(51)Int. Cl.：　*G06F21/36　(2013.01)*　*H04L9/30　(2006.01)*

(30)優先權：2018/08/24　中國大陸　201810974011.8

(71)申請人：開曼群島商創新先進技術有限公司 (開曼群島) ADVANCED NEW TECHNOLOGIES CO., LTD.　(KY)
開曼群島

(72)發明人：黃琪 (CN) ；趙生波 (CN) ；廖暉 (CN) ；王志偉 (CN) ；魏亞文 (CN)

(74)代理人：林志剛

(56)參考文獻：

TW	201610742A	CN	103295046A
CN	106100850A	CN	107146124A
CN	107194695A	CN	108256869A

審查人員：黃同慶

申請專利範圍項數：23 項　圖式數：6　共 36 頁

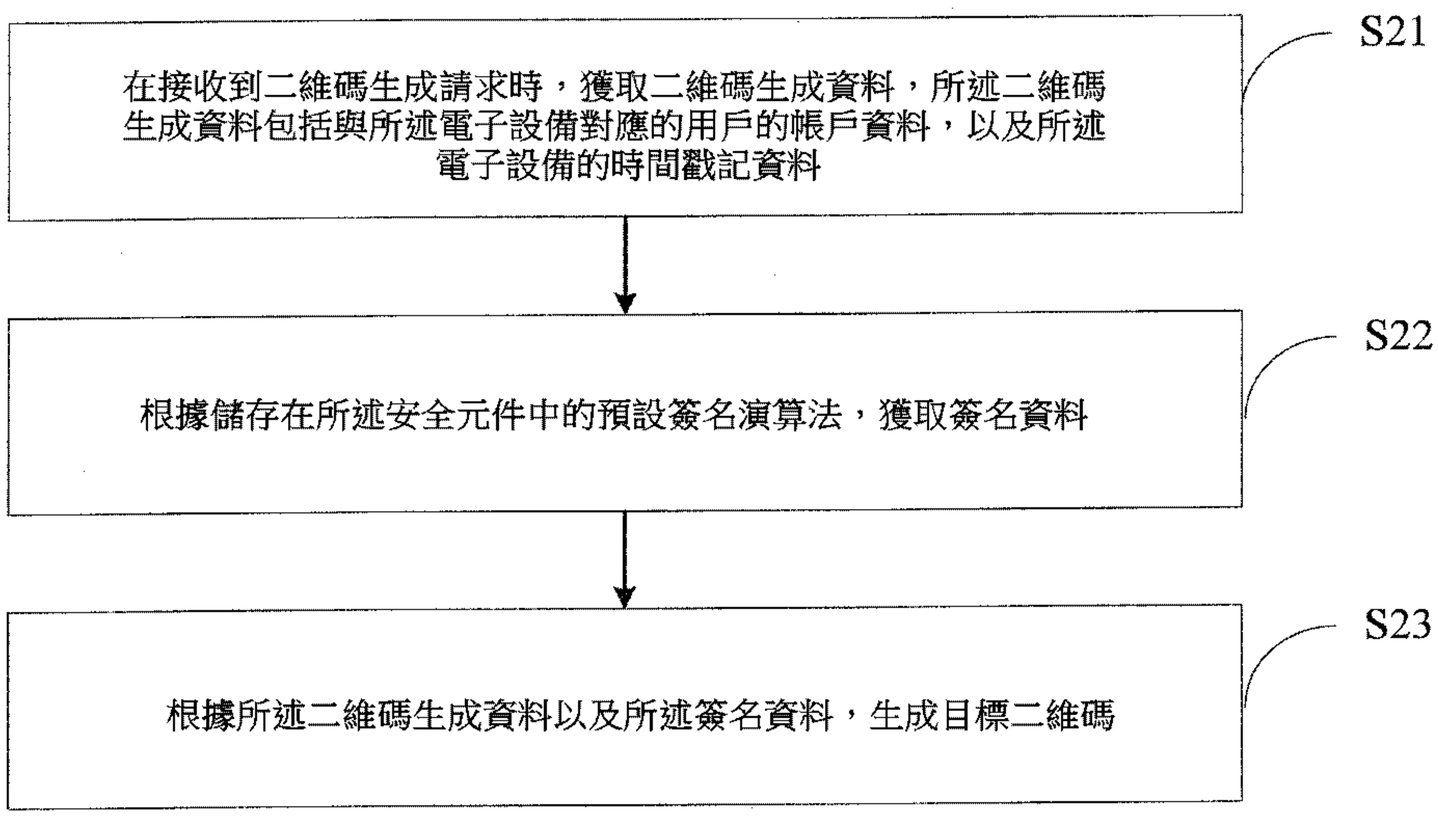
(54)名稱

二維碼生成方法、資料處理方法、裝置、伺服器及計算機可讀儲存媒體

(57)摘要

本發明公開一種二維碼生成方法、資料處理方法、裝置及伺服器，所述二維碼生成方法應用於電子設備中，所述電子設備設置有安全元件，在所述二維碼生成方法中，獲取二維碼生成資料，以及透過儲存在所述安全元件中的預設簽名演算法獲取簽名資料，根據所述二維碼生成資料以及所述簽名資料生成目標二維碼，保證了目標二維碼的安全。

指定代表圖：


在接收到二維碼生成請求時，獲取二維碼生成資料，所述二維碼生成資料包括與所述電子設備對應的用戶的帳戶資料，以及所述電子設備的時間戳記資料
S21
根據儲存在所述安全元件中的預設簽名演算法，獲取簽名資料
S22
根據所述二維碼生成資料以及所述簽名資料，生成目標二維碼
S23

【圖 2】

I718567 第 108121717 號

公告本

民國 109 年 7 月 29 日修正

【發明摘要】

【中文發明名稱】

二維碼生成方法、資料處理方法、裝置、伺服器及計算機可讀儲存媒體

【中文】

本發明公開一種二維碼生成方法、資料處理方法、裝置及伺服器，所述二維碼生成方法應用於電子設備中，所述電子設備設置有安全元件，在所述二維碼生成方法中，獲取二維碼生成資料，以及透過儲存在所述安全元件中的預設簽名演算法獲取簽名資料，根據所述二維碼生成資料以及所述簽名資料生成目標二維碼，保證了目標二維碼的安全。

第 108121717 號　　民國 109 年 7 月 29 日修正

【指定代表圖】第(2)圖。
【代表圖之符號簡單說明】無

【特徵化學式】無

第 108121717 號　　民國 109 年 7 月 29　日修正

【發明說明書】

【中文發明名稱】

二維碼生成方法、資料處理方法、裝置、伺服器及計算機可讀儲存媒體

【技術領域】

本發明涉及計算機技術領域，尤其涉及一種二維碼生成方法、資料處理方法、裝置及伺服器。

【先前技術】

二維碼是透過某種特定的幾何圖形按照一定規律，在平面上形成的黑白相間的圖形來記錄資料符號資訊。隨著科學技術的不斷發展，二維碼得到了越來越廣泛的應用。例如在收付款時，可以透過掃描收款二維碼和付款二維碼來完成交易。但是二維碼資料是以明文進行儲存的，容易受到攻擊者的篡改、攻擊等。

【發明內容】

本說明書實施例提供及一種二維碼生成方法、資料處理方法、裝置及伺服器。

第一態樣，本說明書實施例提供一種二維碼生成方法，應用於電子設備中，所述電子設備設置有安全元件，所述方法包括：

在接收到二維碼生成請求時，獲取二維碼生成資料，所述二維碼生成資料包括與所述電子設備對應的用戶的帳

戶資料，以及所述電子設備的時間戳記資料；

根據儲存在所述安全元件中的預設簽名演算法，獲取簽名資料；

根據所述二維碼生成資料以及所述簽名資料，生成目標二維碼。

第二態樣，本說明書實施例提供一種資料處理方法，所述資料處理方法包括：

接收目標電子設備掃描目標二維碼得到的二維碼掃描資料，其中，所述目標二維碼為採用申請專利範圍第1至5項任一項所述的方法生成的二維碼，所述二維碼掃描資料中包括所述生成所述目標二維碼的簽名資料以及二維碼生成資料；

根據所述簽名資料的簽名方式，對所述簽名資料進行驗簽，獲得驗簽結果。

第三態樣，本說明書實施例提供一種二維碼生成裝置，所述二維碼生成裝置設置有安全元件，所述二維碼生成裝置包括：

二維碼生成資料獲取模組，用於在接收到二維碼生成請求時，獲取二維碼生成資料，所述二維碼生成資料包括與所述電子設備對應的用戶的帳戶資料，以及所述電子設備的時間戳記資料；

簽名資料獲取模組，用於根據儲存在所述安全元件中的預設簽名演算法，獲取簽名資料；

二維碼生成模組，用於根據所述二維碼生成資料以及

所述簽名資料，生成目標二維碼。

第四態樣，本說明書實施例提供一種資料處理裝置，包括：

接收模組，用於接收目標電子設備掃描目標二維碼得到的二維碼掃描資料，其中，所述目標二維碼為採用申請專利範圍第1至5項任一項所述的方法生成的二維碼，所述二維碼掃描資料中包括所述生成所述目標二維碼的簽名資料以及二維碼生成資料；

處理模組，用於根據所述簽名資料的簽名方式，對所述簽名資料進行驗簽，獲得驗簽結果。

第五態樣，本說明書實施例提供一種二維碼生成裝置，包括記憶體、處理器及儲存在記憶體上並可在處理器上運行的計算機程式，所述處理器執行第一態樣所述的二維碼生成方法的步驟。

第六態樣，本說明書實施例提供一種伺服器，包括記憶體、處理器及儲存在記憶體上並可在處理器上運行的計算機程式，所述處理器執行第二態樣所述的資料處理方法的步驟。

第七態樣，本說明書實施例提供一種計算機可讀儲存媒體，其上儲存有計算機程式，該程式被處理器執行時實現上述任一項所述方法的步驟。

本說明書實施例有益效果如下：

在本說明書實施例中，在接收到二維碼生成請求時，獲取二維碼生成資料，所述二維碼生成資料包括與所述電

子設備對應的用戶的帳戶資料，以及所述電子設備的時間戳記資料；根據儲存在所述安全元件中的預設簽名演算法，獲取簽名資料；根據所述二維碼生成資料以及所述簽名資料，生成目標二維碼。上述方案中，由於安全元件能夠提供獨立的運行空間，保證資料安全，透過儲存在安全元件中的預設簽名演算法進行數位簽名資料，並基於二維碼生成資料以及數位簽名資料生成目標二維碼，保證了目標二維碼的安全，另外，只有在目標二維碼被認證中心驗簽成功時，才表明目標二維碼未被篡改，因此有效的保證了資料傳輸的安全。

【圖式簡單說明】

透過閱讀下文優選實施方式的詳細描述，各種其他的優點和益處對於本領域普通技術人員將變得清楚明瞭。附圖僅用於示出優選實施方式的目的，而並不認為是對本發明的限制。而且在整個附圖中，用相同的參考符號表示相同的部件。在附圖中：

圖1為本說明書實施例提供的資料處理方法的應用場景示意圖；

圖2為本說明書實施例第一態樣提供的一種二維碼生成方法的流程圖；

圖3為本說明書實施例第二態樣提供的一種資料處理方法的流程圖；

圖4為本說明書實施例第三態樣提供的一種二維碼生

成裝置的示意圖；

圖5為本說明書實施例第四態樣提供的一種資料處理裝置的示意圖；

圖6為本說明書實施例示出的一種伺服器的示意圖。

【實施方式】

為了更好的理解上述技術方案，下面透過附圖以及具體實施例對本說明書實施例的技術方案做詳細的說明，應當理解本說明書實施例以及實施例中的具體特徵是對本說明書實施例技術方案的詳細的說明，而不是對本說明書技術方案的限定，在不衝突的情況下，本說明書實施例以及實施例中的技術特徵可以相互組合。

第一態樣，本說明書實施例提供一種二維碼生成方法，如圖1所示，為本說明書實施例提供的資料處理方法的應用場景示意圖。圖1中，終端設備可以為支付機具、二維碼生成器等設備。終端設備的個數可以為多個，每個終端設備均與伺服器通信連接。在每個終端設備中，均可以設置有安全元件(Secure Element，SE)，透過安全元件獲取生成二維碼的資料。由於安全元件提供了與設備中微控制單元(Microcontroller Unit，MCU)隔離的運行空間，所以運行或儲存在安全元件上的程式及資料不能被攻擊者讀取或篡改，保證了資料的安全性。終端設備還可以設置有顯示單元，能夠進行二維碼顯示。

掃碼設備可以為手機、平板電腦等設備，用於對終端

設備顯示的二維碼進行掃描，獲得掃碼結果。掃碼設備還可以將掃碼結果發送至伺服器，以使伺服器對掃碼結果進行驗簽，確定該二維碼是否被篡改。

伺服器可以包括CA認證中心伺服器、TSM(Trusted Service Management，可信服務管理)伺服器等。其中，CA認證中心伺服器可以對接收到的掃描資料進行驗簽，TSM伺服器可以對終端設備上的安全元件進行管理，如完成安全元件的初始化、終端設備入網等。

如圖2所示，為本說明書實施例提供的一種二維碼生成方法的流程圖，該方法應用於一電子設備中，電子設備內設置有安全元件，該方法包括以下步驟。

步驟S21：在接收到二維碼生成請求時，獲取二維碼生成資料，所述二維碼生成資料包括與所述電子設備對應的用戶的帳戶資料，以及所述電子設備的時間戳記資料；

本說明書實施例中，電子設備可以為支付機具、二維碼生成器等設備，電子設備內設置有安全元件。二維碼可以為收款碼、訂單碼、付款碼等，二維碼生成請求可以是定時請求，也可以是透過用戶的操作觸發生成的請求。在一個實施例中，電子設備為支付機具，二維碼為收款碼，收款碼生成請求可以由定時更新任務來發送，例如，每隔1min發送一次收款碼更新請求。在另一實施例中，支付機具可以設置有用於顯示二維碼的操作按鍵，當用戶按下該操作按鍵後，發送二維碼生成請求。當然還可以透過其他方式發送二維碼生成請求，如在當前二維碼被掃描之後，

可以發送二維碼生成請求，以更新二維碼。

本說明書實施例中，二維碼生成資料可以保存在電子設備的安全元件中，也可以保存在安全元件以外的儲存空間內。二維碼生成資料包括與電子設備對應的用戶的帳戶資料，以及電子設備的時間戳記資料，當然，二維碼生成資料還可以包括其他資料，這裡不做限定。時間戳記資料能夠表明電子設備的時間資訊，可以對二維碼的生成時間進行標記，由於時間戳記資料是實時變化的，進而使得二維碼生成資料也為動態的，因此，根據二維碼生成資料獲得的二維碼圖形也是動態變化的。應理解的是，每個電子設備可以與用戶的帳戶進行綁定，用戶的帳戶資料可以是銀行帳戶資料、支付寶帳戶資料等。在一個實施例中，當二維碼為收款碼時，用戶的帳戶資料可以是用戶的收款帳號。

步驟S22：根據儲存在所述安全元件中的預設簽名演算法，獲取簽名資料；

本說明書實施例中，電子設備在出廠前可以將預設簽名演算法寫入安全元件中。預設簽名演算法可以根據實際需要進行選擇，例如，PKI(Public Key Infrastructure，公鑰基礎設施)演算法、HOTP(HMAC-based One-Time Password，基於HMAC演算法加密的一次性密碼)演算法等，本說明書實施例不做限定。

應理解的是，採用不同簽名演算法得到的簽名資料也可以是不同的。另外，由於簽名演算法本身的特性，同一

簽名演算法在每次進行數位簽名的過程中，得到的簽名資料也可以是不同的，例如，在預設簽名演算法為橢圓曲線公鑰密碼演算法時，每次得到的簽名資料是動態變化的。

由於SE能夠給資料提供安全的空間，在一個實施例中，數位簽名的處理過程均可以在SE中完成，生成簽名資料。

步驟S23：根據所述二維碼生成資料以及所述簽名資料，生成目標二維碼。

在獲得了二維碼生成資料以及簽名資料之後，將這些資料轉換為二維碼圖像，生成目標二維碼。在一個實施例中，電子設備中可以保存有資料轉換為二維碼圖像的對應模板，如二維碼的版本資訊、二維碼的結構組成等，將二維碼生成資料以及簽名資料作為二維碼的資料內容填充在二維碼圖像中的資料區域中，可以得到目標二維碼。

可選地，在根據所述儲存在所述安全元件中的預設簽名演算法，獲取簽名資料之前，所述方法還包括：獲取待簽名資料；所述根據儲存在所述安全元件中的預設簽名演算法，獲取簽名資料，包括：根據所述預設簽名演算法，對所述待簽名資料進行數位簽名，獲取所述簽名資料。

本說明書實施例中，待簽名資料可以根據實際需要進行設定，待簽名資料可以保存在安全元件中，也可以是經過資料處理得到的。在一個實施例中，待簽名資料可以是預設好的資料，在進行簽名操作時直接讀取。

在另一個實施例中，根據所述二維碼生成資料，生成

與所述二維碼生成資料對應的摘要資料，所述摘要資料為所述待簽名資料。在該實施例中，在二維碼生成資料的資料量較大時，為了減少數位簽名的計算量，可以先對二維碼生成資料進行處理，如透過對二維碼生成資料進行哈希運算得到與二維碼生成資料對應的摘要資料，然後再對摘要資料進行數位簽名。當然也可以透過其他方式得到摘要資料，這裡不做限定。

可選地，所述預設簽名演算法為基於公鑰基礎設施的簽名演算法時，所述根據所述預設簽名演算法，對待簽名資料進行數位簽名，獲取所述簽名資料，包括：獲取所述安全元件生成的私鑰；根據所述私鑰，對所述待簽名資料進行數位簽名，得到所述簽名資料。

本說明書實施例中，電子設備在投入使用時可以進行入網操作，在設備入網的過程中，電子設備可以向TSM伺服器發送生成請求CSR(Cerificate Signing Request，證書請求)指令，該指令中包含有該電子設備中設置的SE的標識，以用來唯一的表示發送請求的電子設備。TSM伺服器將請求CSR指令下發給該電子設備，以使該電子設備中的SE生成公私鑰對，並將公私鑰對與SE的標識進行關聯。

在SE生成公私鑰對並與SE的標識關聯之後，TSM伺服器向CA認證中心請求CA認證證書，CA認證中心根據SE生成的公鑰以及其他資訊生成證書文件，將證書進行儲存，並將證書資料返回為TSM伺服器，TSM伺服器向電子設備下發寫證書指令，電子設備將證書儲存到SE中，以完成設備入

網過程。SE中保存有私鑰和證書。

當SE使用私鑰對待簽名資料進行簽名時，SE可以直接讀取私鑰對待簽名資料進行簽名。對應的，當CA認證中心在對簽名資料進行驗簽時，可以根據SE的標識，確定該SE生成的公鑰，並利用該公鑰對簽名資料進行驗簽。

在一個實施例中，待簽名資料為二維碼生成資料進行哈希運算得到的摘要資訊，SE利用私鑰對摘要資訊進行數位簽名，得到簽名資料，將二維碼生成資料以及簽名資料轉換為目標二維碼。當掃碼設備對目標二維碼進行掃描後，獲得掃碼結果，掃碼結果包括二維碼生成資料以及簽名資料。掃碼設備將交掃碼結果發送給CA認證中心，CA認證中心透過對二維碼生成資料做哈希運算得到第一摘要資料，並利用SE的標識找到與該私鑰對應的公鑰，透過公鑰對簽名資料進行驗簽，得到第二摘要資料，當第一摘要資料與第二摘要資料相同時，表明該目標二維碼為與SE的標識對應的電子設備生成的，未經過篡改。

可選地，所述預設簽名演算法為基於一次性加密的簽名演算法時，所述預設簽名演算法為基於一次性加密的簽名演算法時，所述根據儲存在所述安全元件中的預設簽名演算法，獲取簽名資料，包括：根據儲存在所述安全元件中的共享密鑰，獲得一次性加密密碼，所述一次性加密密碼為所述簽名資料。

本說明書實施例中，當預設簽名演算法為基於一次性加密的簽名演算法時，該簽名演算法可以為HTOP演算法

時。SE中可以儲存有共享密鑰，該密鑰是SE和認證伺服器共享的。根據共享密鑰，可以生成一個一次性加密密碼。在一個實施例中，電子設備中設置有一計數器，根據共享密鑰，以及計數器值，透過HMAC(Hash-based Message Authentication Code，哈希運算消息認證碼)運算，得到一次性加密密碼。應理解的是，每次生成的一次性加密密碼均是不同的，因此能夠保證每次簽名過程的安全性。同時，在認證伺服器上，也會根據共享密鑰以及計數器值生成一個密碼，當這個密碼與SE生成的一次性加密密碼相同時，則表明資料沒有被篡改。

當簽名資料為一次性加密密碼時，根據二維碼生成資料以及一次性加密密碼，生成目標二維碼。

可選地，在所述根據所述私鑰，對所述待簽名資料進行數位簽名，得到所述簽名資料之後，所述方法還包括：根據儲存在所述安全元件中的共享密鑰，生成一次性加密密碼；所述根據所述二維碼生成資料以及所述簽名資料，生成目標二維碼，包括：根據所述二維碼生成資料、所述簽名資料以及所述一次性加密密碼，生成所述目標二維碼。

本說明書實施例中，為了加強資料的安全性，可以先透過SE中儲存的私鑰對待簽名資料進行數位簽名，得到簽名資料然後透過一次性加密密碼對二維碼生成資料以及簽名資料進行加密保護。在生成目標二維碼的過程中，將二維碼生成資料、簽名資料以及一次性加密密碼進行處理，

轉換為目標二維碼的圖像資訊。對應的，當認證伺服器接收到該目標二維碼資料時，先根據一次性加密密碼對目標二維碼資料進行解密，在根據公鑰對待簽名資料進行驗簽。

在生成目標二維碼時，可以根據電子設備中預設好的二維碼資訊來進行資料轉換。二維碼資訊可以包括二維碼的版本資訊、二維碼的結構資訊等。在一個實施例中，可以將二維碼生成資料、簽名資料進行編碼處理，得到資料碼字序列，再進行糾錯編碼、分塊處理、構造矩陣等步驟，得到最終的完整的目標序列，將完整的目標序列填充到相對的二維碼矩陣區域中，得到目標二維碼圖像。

第二態樣，本說明書實施例提供一種資料處理方法，該資料處理方法可以應用於伺服器側。如圖3所示，該資料處理方法包括以下步驟。

步驟S31：接收目標電子設備掃描目標二維碼得到的二維碼掃描資料，其中，所述目標二維碼為採用本說明書實施例中第一態樣提供的二維碼生成方法生成的二維碼，所述二維碼掃描資料中包括所述生成所述目標二維碼的簽名資料以及二維碼生成資料；

本說明書實施例中，目標電子設備可以是手機、平板電腦等能夠掃描二維碼的設備。目標二維碼是採用本說明書實施例中第一態樣提供的二維碼生成方法生成的二維碼。目標電子設備在掃描目標二維碼之後，可以將目標二維碼由圖像資訊轉換成碼字序列，並對碼字序列進行處

理，得到與目標二維碼對應的簽名資料以及二維碼生成資料。二維碼掃描資料可以是上述碼字序列，也可以使處理後得到的二維碼生成資料以及簽名資料，還可以是其他形式的資料，這裡不做限定。目標電子設備將得到的二維碼掃描資料發送給伺服器，在一個實施例中，目標電子設備將二維碼掃描資料發送給CA認證中心伺服器。

步驟S32：根據所述簽名資料的簽名方式，對所述簽名資料進行驗簽，獲得驗簽結果。

由於簽名資料可以是由不同的簽名演算法生成的，例如，PKI(Public Key Infrastructure，公鑰基礎設施)演算法、HOTP(HMAC-based One-Time Password，基於HMAC演算法加密的一次性密碼)演算法等。不同的簽名方式，對應不同的驗簽方式。在一個實施例中，所述簽名方式為基於公鑰基礎設施的簽名方式時，所述根據所述簽名資料的簽名方式，對所述簽名資料進行驗簽，獲得驗簽結果，包括：根據與所述簽名資料對應的公鑰，對所述簽名資料進行驗簽，獲得驗簽結果。在另一實施例中，所述預設簽名演算法為基於一次性加密的簽名方式時，所述根據所述簽名資料的簽名方式，對所述簽名資料進行驗簽，獲得驗簽結果，包括：根據與所述簽名資料對應的共享密鑰，獲取目標一次性加密密碼；根據所述目標一次性加密密碼，對所述簽名資料進行驗簽，獲得驗簽結果。由於上述兩種驗簽方式在本說明書實施例的第一態樣提供的二維碼生成方法的實施例中進行了描述，此處就不做贅述了。

另外，當二維碼掃描資料表明該資料同時包含有一次性加密資訊和簽名資訊時，根據目標一次性加密密碼對二維碼掃描資料進行解密，對解密後的資料使用對應的驗簽方式進行驗簽。

可選地，所述接收目標電子設備掃描目標二維碼得到的二維碼掃描資料之後，所述方法還包括：獲取接收所述二維碼掃描資料的目標時間戳記資料；獲取所述二維碼生成資料中的初始時間戳記資料；根據所述目標時間戳記資料與所述初始時間戳記資料之間的目標時間差，以及預設時間差，確定所述二維碼是否有效，其中，在所述目標時間差小於或等於所述預設時間差時，確定所述目標二維碼有效；在所述目標時間差大於所述預設時間差時，確定所述目標二維碼無效。

為了保證資料的安全性，本說明書實施例中為二維碼設置了有效時長，即在有效時長內二維碼是有效的，超出了有效時長，二維碼則無效。本說明書實施例中，二維碼生成資料包括生成二維碼時的初始時間戳記資料，根據伺服器接收到二維碼掃描資料時的目標時間戳記資料，目標時間戳記資料與初始時間戳記資料之間的目標時間差可以表示目標二維碼的持續時間。預設時間差用來表示二維碼的有效時長，可以根據實際需要進行設定，如30s、1min等。當目標時間差大於預設時間差時，表明目標二維碼已經超時，確定目標二維碼失效，反之，則表明目標二維碼有效。

可選地，在所述目標二維碼為收款碼時，在所述獲得驗簽結果之後，所述方法還包括：在所述驗證結果為驗證成功時，獲取所述二維碼生成資料中的帳戶資料；根據所述收款碼對應的收款金額，對所述帳戶資料中的金額進行更新。

為了更好的理解本說明書實施例提供的方法，下面以二維碼為收款碼為例，對目標二維碼的生成以及掃描過程進行說明。在該實施例中，電子設備為支付機具，二維碼為收款碼，二維碼生成資料中的帳戶資料為該支付機具的使用用戶的收款帳戶資料，電子設備內的SE中儲存有PKI演算法。目標電子設備為進行掃碼的手機。伺服器端包括CA認證中心伺服器，以及交易平台，其中交易平台用於管理用戶的帳戶資料。

當支付機具接收到二維碼生成請求時，獲取收款帳戶資料，以及支付機具的時間戳記資料。SE透過PKI演算法，使用私鑰對收款帳戶資料以及時間戳記資料進行數位簽名，生成簽名資料。將收款帳戶資料、時間戳記資料以及簽名資料進行處理，轉換為目標二維碼，並在支付機具上進行顯示。

當手機對支付機具上的目標二維碼進行掃碼時，獲得二維碼掃描資料(包括收款帳戶資料、時間戳記資料以及簽名資料)。同時，手機可以跳轉至支付頁面，手機用戶在支付頁面上填寫支付的金額，填寫完畢後，手機將二維碼掃描資料以及支付金額發送至CA認證中心伺服器。

CA認證中心伺服器根據時間戳記資料判斷目標二維碼是否有效，當目標二維碼有效時，根據與支付機具對應的公鑰，對簽名資料進行驗簽。當驗簽成功時，可以將收款帳戶資料以及支付金額發送至交易平台，交易平台根據支付金額對收款帳戶中的總金額進行更新。

第三態樣，本說明書實施例提供一種二維碼生成裝置，如圖4所示，所述二維碼生成裝置設置有安全元件，所述二維碼生成裝置包括：

二維碼生成資料獲取模組41，用於在接收到二維碼生成請求時，獲取二維碼生成資料，所述二維碼生成資料包括與所述電子設備對應的用戶的帳戶資料，以及所述電子設備的時間戳記資料；

簽名資料獲取模組42，用於根據儲存在所述安全元件中的預設簽名演算法，獲取簽名資料；

二維碼生成模組43，用於根據所述二維碼生成資料以及所述簽名資料，生成目標二維碼。

在一種可選實現方式中，所述裝置還包括：

第一獲取模組，用於獲取待簽名資料；

所述簽名資料獲取模組，包括：

第二獲取模組，用於根據所述預設簽名演算法，對所述待簽名資料進行數位簽名，獲取所述簽名資料。

在一種可選實現方式中，所述預設簽名演算法為基於公鑰基礎設施的簽名演算法時，所述第一獲取模組，包括：

私鑰獲取模組，用於獲取所述安全元件生成的私鑰；

第一處理模組，用於根據所述私鑰，對所述待簽名資料進行數位簽名，得到所述簽名資料。

在一種可選實現方式中，所述預設簽名演算法為基於一次性加密的簽名演算法時，簽名資料獲取模組42，包括：

第二處理模組，用於根據儲存在所述安全元件中的共享密鑰，獲得一次性加密密碼，所述一次性加密密碼為所述簽名資料。

在一種可選實現方式中，所述裝置還包括：

第三處理模組，用於根據儲存在所述安全元件中的共享密鑰，生成一次性加密密碼；

所述二維碼生成模組，包括：

第四處理模組，用於根據所述二維碼生成資料、所述簽名資料以及所述一次性加密密碼，生成所述目標二維碼。

關於上述裝置，其中各個模組的具體功能已經在本發明實施例提供的二維碼生成方法的實施例中進行了詳細描述，此處將不做詳細闡述說明。

第四態樣，本說明書實施例提供一種資料處理裝置，如圖5所示，所述資料處理裝置包括：

接收模組51，用於接收目標電子設備掃描目標二維碼得到的二維碼掃描資料，其中，所述目標二維碼為採用本說明書實施例第一態樣提供的二維碼生成方法生成的二維

碼，所述二維碼掃描資料中包括所述生成所述目標二維碼的簽名資料以及二維碼生成資料；

處理模組52，用於根據所述簽名資料的簽名方式，對所述簽名資料進行驗簽，獲得驗簽結果。

可選地，所述簽名方式為基於公鑰基礎設施的簽名方式時，處理模組52，包括：

第一處理模組，用於根據與所述簽名資料對應的公鑰，對所述簽名資料進行驗簽，獲得驗簽結果。

可選地，所述預設簽名演算法為基於一次性加密的簽名方式時，處理模組52，包括：

第一獲取模組，用於根據與所述簽名資料對應的共享密鑰，獲取目標一次性加密密碼；

第二處理模組，用於根據所述目標一次性加密密碼，對所述簽名資料進行驗簽，獲得驗簽結果。

可選地，所述資料處理裝置還包括：

第二獲取模組，用於獲取接收所述二維碼掃描資料的目標時間戳記資料；

第三獲取模組，用於獲取所述二維碼生成資料中的初始時間戳記資料；

第三處理模組，用於根據所述目標時間戳記資料與所述初始時間戳記資料之間的目標時間差，以及預設時間差，確定所述二維碼是否有效，其中，在所述目標時間差小於或等於所述預設時間差時，確定所述目標二維碼有效；在所述目標時間差大於所述預設時間差時，確定所述

目標二維碼無效。

可選地，所述裝置還包括：

第四獲取模組，用於在所述驗證結果為驗證成功時，獲取所述二維碼生成資料中的帳戶資料；

第四處理模組，用於根據所述收款碼對應的收款金額，對所述帳戶資料中的金額進行更新。

關於上述裝置，其中各個模組的具體功能已經在本發明實施例提供的資料處理方法的實施例中進行了詳細描述，此處將不做詳細闡述說明。

第五態樣，基於與前述實施例中二維碼生成方法同樣的發明構思，本發明還提供一種二維碼生成裝置，包括記憶體、處理器及儲存在記憶體上並可在處理器上運行的計算機程式，所述處理器執行所述程式時實現前文所述二維碼生成方法的任一方法的步驟。

第六態樣，基於與前述實施例中資料處理方法同樣的發明構思，本發明還提供一種伺服器，如圖6所示，包括記憶體604、處理器602及儲存在記憶體604上並可在處理器602上運行的計算機程式，所述處理器602執行所述程式時實現前文所述資料處理方法的任一方法的步驟。

其中，在圖11中，匯流排架構(用匯流排600來代表)，匯流排600可以包括任意數量的互聯的匯流排和橋，匯流排600將包括由處理器602代表的一個或多個處理器和記憶體604代表的記憶體的各種電路鏈接在一起。匯流排600還可以將諸如外圍設備、穩壓器和功率管理電路等之

類的各種其他電路鏈接在一起，這些都是本領域所公知的，因此，本文不再對其進行進一步描述。匯流排介面606在匯流排600和接收器601和發送器603之間提供介面。接收器601和發送器1103可以是同一個元件，即收發機，提供用於在傳輸媒體上與各種其他裝置通信的單元。處理器602負責管理匯流排600和通常的處理，而記憶體604可以被用於儲存處理器602在執行操作時所使用的資料。

第七態樣，基於與前述實施例中基於二維碼生成方法以及資料處理方法的發明構思，本發明還提供一種計算機可讀儲存媒體，其上儲存有計算機程式，該程式被處理器執行時實現前文所述基於二維碼生成方法以及資料處理方法的任一方法的步驟。

本說明書是參照根據本說明書實施例的方法、設備(系統)、和計算機程式產品的流程圖及／或方框圖來描述的。應理解可由計算機程式指令實現流程圖及／或方框圖中的每一流程及／或方框、以及流程圖及／或方框圖中的流程及／或方框的結合。可提供這些計算機程式指令到通用計算機、專用計算機、嵌入式處理機或其他可編程資料處理設備的處理器以產生一個機器，使得透過計算機或其他可編程資料處理設備的處理器執行的指令產生用於實現在流程圖一個流程或多個流程及／或方框圖一個方框或多個方框中指定的功能的設備。

這些計算機程式指令也可儲存在能引導計算機或其他可編程資料處理設備以特定方式工作的計算機可讀記憶體

中，使得儲存在該計算機可讀記憶體中的指令產生包括指令設備的製造品，該指令設備實現在流程圖一個流程或多個流程及／或方框圖一個方框或多個方框中指定的功能。

這些計算機程式指令也可裝載到計算機或其他可編程資料處理設備上，使得在計算機或其他可編程設備上執行一系列操作步驟以產生計算機實現的處理，從而在計算機或其他可編程設備上執行的指令提供用於實現在流程圖一個流程或多個流程及／或方框圖一個方框或多個方框中指定的功能的步驟。

儘管已描述了本發明的優選實施例，但本領域內的技術人員一旦得知了基本創造性概念，則可對這些實施例作出另外的變更和修改。所以，所附申請專利範圍意欲解釋為包括優選實施例以及落入本發明範圍的所有變更和修改。

顯然，本領域的技術人員可以對本發明進行各種改動和變型而不脫離本發明的精神和範圍。這樣，倘若本發明的這些修改和變型屬於本發明申請專利範圍及其等同技術的範圍之內，則本發明也意圖包含這些改動和變型在內。

【符號說明】

41：二維碼生成資料獲取模組

42：簽名資料獲取模組

43：二維碼生成模組

51：接收模組

52：處理模組

600：匯流排

601：接收器

602：處理器

603：發送器

604：記憶體

606：匯流排介面

第 108121717 號　　民國 109 年 7 月 29　日修正

【發明申請專利範圍】

【第1項】

一種二維碼生成方法，應用於電子設備中，該電子設備設置有安全元件，該方法包括：

在接收到二維碼生成請求時，獲取二維碼生成資料，該二維碼生成資料包括與該電子設備對應的用戶的帳戶資料，以及該電子設備的時間戳記資料；

根據儲存在該安全元件中的預設簽名演算法，獲取簽名資料；

根據該二維碼生成資料以及該簽名資料，生成目標二維碼；

其中，該電子設備在入網過程中，向可信服務管理伺服器發送生成證書請求的指令，該指令中包含有該電子設備中設置的安全元件的標識，並接收可信服務管理伺服器下發的證書請求，以使安全元件生成公私鑰對，透過該安全元件生成的私鑰生成該簽名資料。

【第2項】

根據申請專利範圍第1項所述的二維碼生成方法，在根據所述儲存在該安全元件中的預設簽名演算法，獲取該簽名資料之前，該方法還包括：獲取待簽名資料；

所述根據儲存在該安全元件中的預設簽名演算法，獲取該簽名資料，包括：根據該預設簽名演算法，對該待簽名資料進行數位簽名，獲取該簽名資料。

【第3項】

根據申請專利範圍第2項所述的二維碼生成方法，該預設簽名演算法為基於公鑰基礎設施的簽名演算法時，所述根據該預設簽名演算法，對該待簽名資料進行數位簽名，獲取該簽名資料，包括：

獲取該安全元件生成的私鑰；

根據該私鑰，對該待簽名資料進行數位簽名，得到該簽名資料。

【第4項】

根據申請專利範圍第1項所述的二維碼生成方法，該預設簽名演算法為基於一次性加密的簽名演算法時，所述根據儲存在該安全元件中的預設簽名演算法，獲取該簽名資料，包括：

根據儲存在該安全元件中的共享密鑰，獲得一次性加密密碼，該一次性加密密碼為該簽名資料。

【第5項】

根據申請專利範圍第3項所述的二維碼生成方法，在所述根據該私鑰，對該待簽名資料進行數位簽名，得到該簽名資料之後，該方法還包括：根據儲存在該安全元件中的共享密鑰，生成一次性加密密碼；

所述根據該二維碼生成資料以及該簽名資料，生成目標二維碼，包括：根據該二維碼生成資料、該簽名資料以及該一次性加密密碼，生成該目標二維碼。

【第6項】

一種資料處理方法，該資料處理方法包括：

接收目標電子設備掃描目標二維碼得到的二維碼掃描資料，其中，該目標二維碼為採用申請專利範圍第1-5項任一項所述的方法生成的二維碼，該二維碼掃描資料中包括所述生成該目標二維碼的簽名資料以及二維碼生成資料；

根據該簽名資料的簽名方式，對該簽名資料進行驗簽，獲得驗簽結果。

【第7項】

根據申請專利範圍第6項所述的資料處理方法，該簽名方式為基於公鑰基礎設施的簽名方式時，所述根據該簽名資料的簽名方式，對該簽名資料進行驗簽，獲得驗簽結果，包括：

根據與該簽名資料對應的公鑰，對該簽名資料進行驗簽，獲得驗簽結果。

【第8項】

根據申請專利範圍第6項所述的資料處理方法，該預設簽名演算法為基於一次性加密的簽名方式時，所述根據該簽名資料的簽名方式，對該簽名資料進行驗簽，獲得驗簽結果，包括：

根據與該簽名資料對應的共享密鑰，獲取目標一次性加密密碼；

根據該目標一次性加密密碼，對該簽名資料進行驗簽，獲得驗簽結果。

【第9項】

根據申請專利範圍第6項所述的資料處理方法，所述接收目標電子設備掃描目標二維碼得到的二維碼掃描資料之後，該方法還包括：

獲取接收該二維碼掃描資料的目標時間戳記資料；

獲取該二維碼生成資料中的初始時間戳記資料；

根據該目標時間戳記資料與該初始時間戳記資料之間的目標時間差，以及預設時間差，確定該二維碼是否有效，其中，在該目標時間差小於或等於該預設時間差時，確定該目標二維碼有效；在該目標時間差大於該預設時間差時，確定該目標二維碼無效。

【第10項】

根據申請專利範圍第9項所述的資料處理方法，在該目標二維碼為收款碼時，在該獲得驗簽結果之後，該方法還包括：

在該驗證結果為驗證成功時，獲取該二維碼生成資料中的帳戶資料；

根據該收款碼對應的收款金額，對該帳戶資料中的金額進行更新。

【第11項】

一種二維碼生成裝置，該二維碼生成裝置設置有安全元件，該二維碼生成裝置包括：

二維碼生成資料獲取模組，用於在接收到二維碼生成請求時，獲取二維碼生成資料，該二維碼生成資料包括與該電子設備對應的用戶的帳戶資料，以及該電子設備的時

間戳記資料；

簽名資料獲取模組，用於根據儲存在該安全元件中的預設簽名演算法，獲取簽名資料；

二維碼生成模組，用於根據該二維碼生成資料以及該簽名資料，生成目標二維碼；

其中，電子設備在入網過程中，向可信服務管理伺服器發送生成證書請求的指令，該指令中包含有該電子設備中設置的安全元件的標識，並接收可信服務管理伺服器下發的證書請求，以使安全元件生成公私鑰對，該簽名資料獲取模組用於基於該安全元件生成的私鑰生成該簽名資料。

【第12項】

根據申請專利範圍第11項所述的二維碼生成裝置，該裝置還包括：

第一獲取模組，用於獲取待簽名資料；

該簽名資料獲取模組，包括：

第二獲取模組，用於根據該預設簽名演算法，對該待簽名資料進行數位簽名，獲取該簽名資料。

【第13項】

根據申請專利範圍第12項所述的二維碼生成裝置，該預設簽名演算法為基於公鑰基礎設施的簽名演算法時，該第一獲取模組，包括：

私鑰獲取模組，用於獲取該安全元件生成的私鑰；

第一處理模組，用於根據該私鑰，對該待簽名資料進

行數位簽名，得到該簽名資料。

【第14項】

根據申請專利範圍第11項所述的二維碼生成裝置，該預設簽名演算法為基於一次性加密的簽名演算法時，該簽名資料獲取模組，包括：

第二處理模組，用於根據儲存在該安全元件中的共享密鑰，獲得一次性加密密碼，該一次性加密密碼為該簽名資料。

【第15項】

根據申請專利範圍第13項所述的二維碼生成裝置，該裝置還包括：

第三處理模組，用於根據儲存在該安全元件中的共享密鑰，生成一次性加密密碼；

該二維碼生成模組，包括：

第四處理模組，用於根據該二維碼生成資料、該簽名資料以及該一次性加密密碼，生成該目標二維碼。

【第16項】

一種資料處理裝置，該資料處理裝置包括：

接收模組，用於接收目標電子設備掃描目標二維碼得到的二維碼掃描資料，其中，該目標二維碼為採用申請專利範圍第1至5項任一項所述的方法生成的二維碼，該二維碼掃描資料中包括所述生成該目標二維碼的簽名資料以及二維碼生成資料；

處理模組，用於根據該簽名資料的簽名方式，對該簽

名資料進行驗簽，獲得驗簽結果。

【第17項】

根據申請專利範圍第16項所述的資料處理裝置，該簽名方式為基於公鑰基礎設施的簽名方式時，該處理模組，包括：

第一處理模組，用於根據與該簽名資料對應的公鑰，對該簽名資料進行驗簽，獲得驗簽結果。

【第18項】

根據申請專利範圍第16項所述的資料處理裝置，該預設簽名演算法為基於一次性加密的簽名方式時，該處理模組，包括：

第一獲取模組，用於根據與該簽名資料對應的共享密鑰，獲取目標一次性加密密碼；

第二處理模組，用於根據該目標一次性加密密碼，對該簽名資料進行驗簽，獲得驗簽結果。

【第19項】

根據申請專利範圍第16項所述的資料處理裝置，該資料處理裝置還包括：

第二獲取模組，用於獲取接收該二維碼掃描資料的目標時間戳記資料；

第三獲取模組，用於獲取該二維碼生成資料中的初始時間戳記資料；

第三處理模組，用於根據該目標時間戳記資料與該初始時間戳記資料之間的目標時間差，以及預設時間差，確

定該二維碼是否有效，其中，在該目標時間差小於或等於該預設時間差時，確定該目標二維碼有效；在該目標時間差大於該預設時間差時，確定該目標二維碼無效。

【第20項】

根據申請專利範圍第19項所述的資料處理裝置，該裝置還包括：

第四獲取模組，用於在該驗證結果為驗證成功時，獲取該二維碼生成資料中的帳戶資料；

第四處理模組，用於根據該收款碼對應的收款金額，對該帳戶資料中的金額進行更新。

【第21項】

一種二維碼生成裝置，包括記憶體、處理器及儲存在記憶體上並可在處理器上運行的計算機程式，該處理器執行該程式時實現申請專利範圍第1至5項任一項所述方法的步驟。

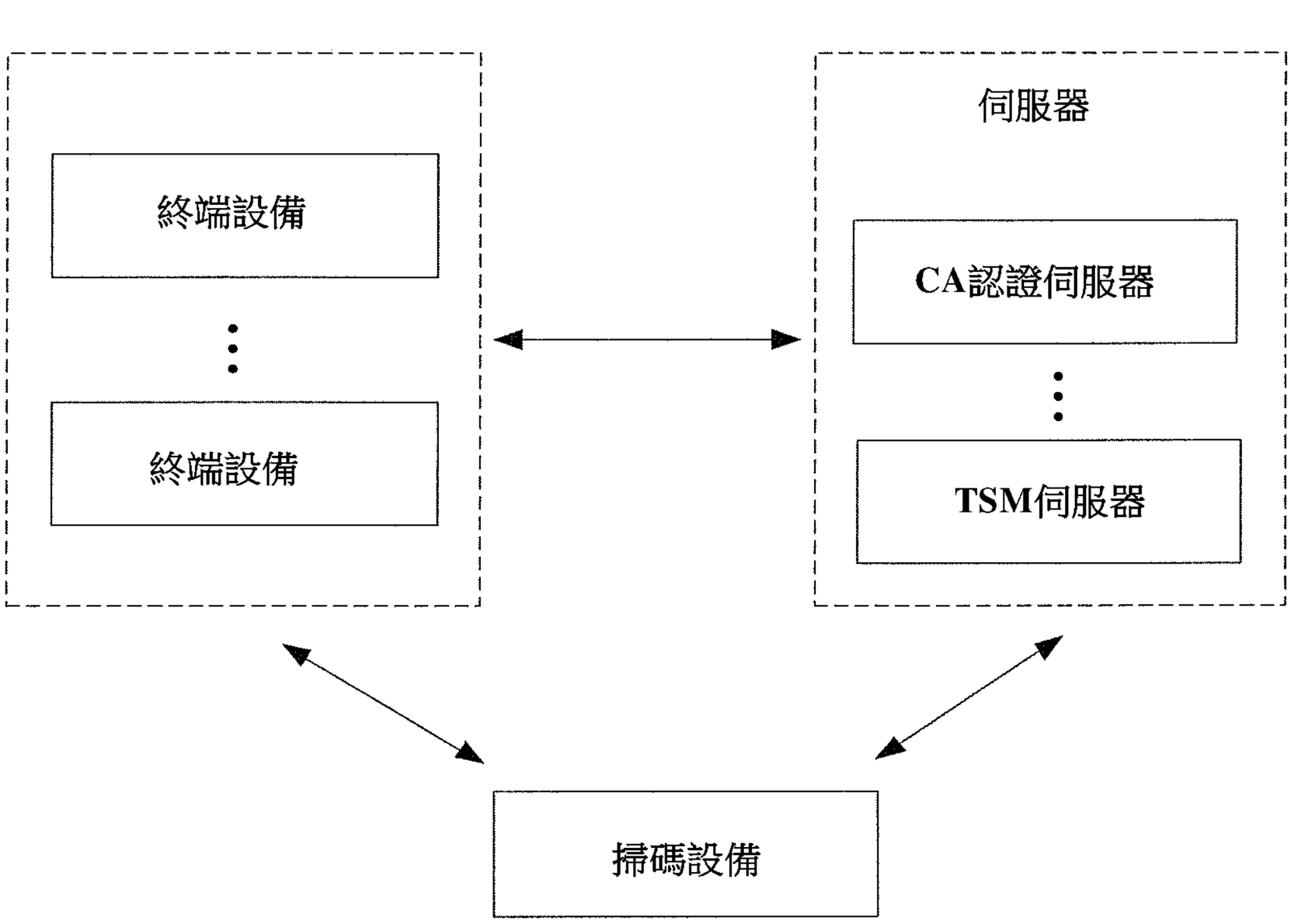
【第22項】

一種伺服器，包括記憶體、處理器及儲存在記憶體上並可在處理器上運行的計算機程式，該處理器執行該程式時實現申請專利範圍第6至10項任一項所述方法的步驟。

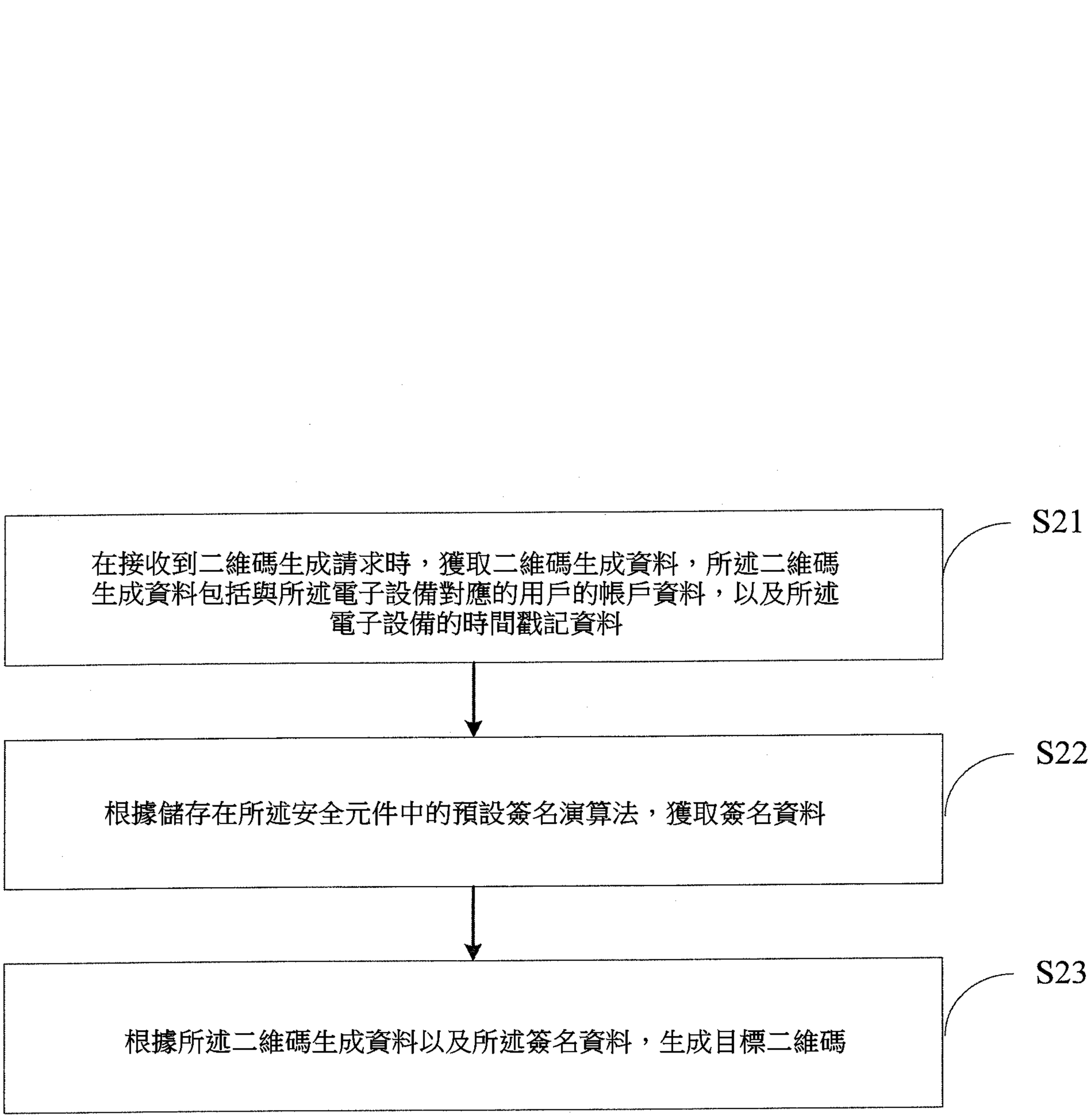
【第23項】

一種計算機可讀儲存媒體，其上儲存有計算機程式，該程式被處理器執行時實現申請專利範圍第1至10項任一項所述方法的步驟。

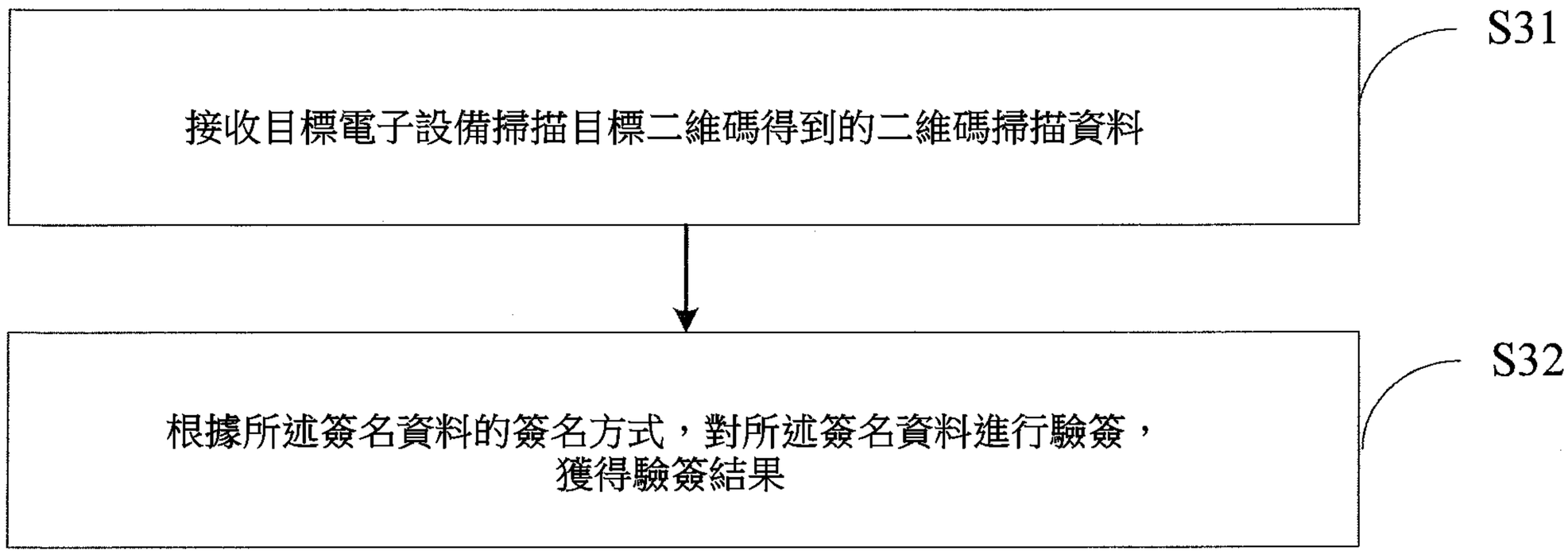
【發明圖式】



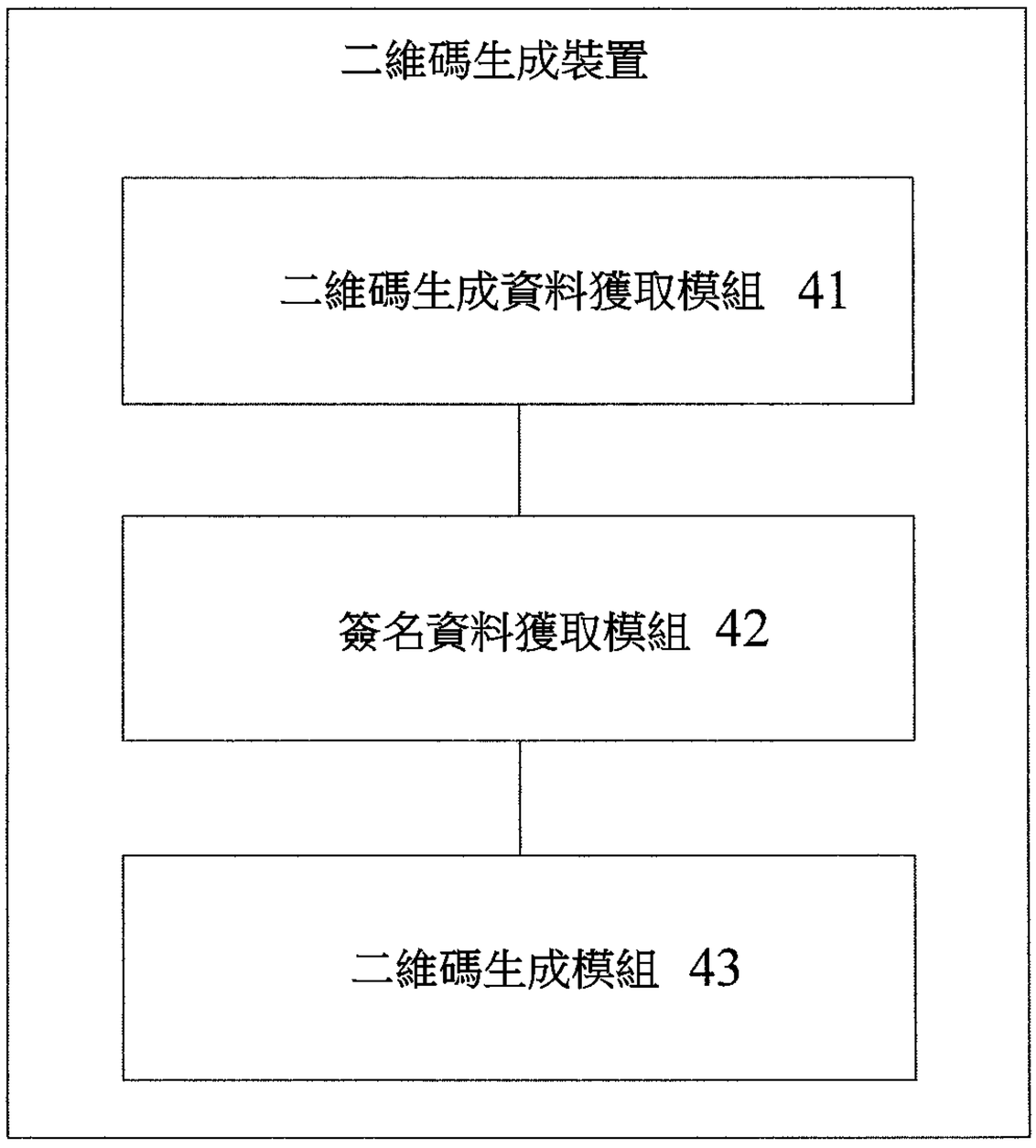
【圖 1】


S21
在接收到二維碼生成請求時，獲取二維碼生成資料，所述二維碼生成資料包括與所述電子設備對應的用戶的帳戶資料，以及所述電子設備的時間戳記資料
S22
根據儲存在所述安全元件中的預設簽名演算法，獲取簽名資料
S23
根據所述二維碼生成資料以及所述簽名資料，生成目標二維碼

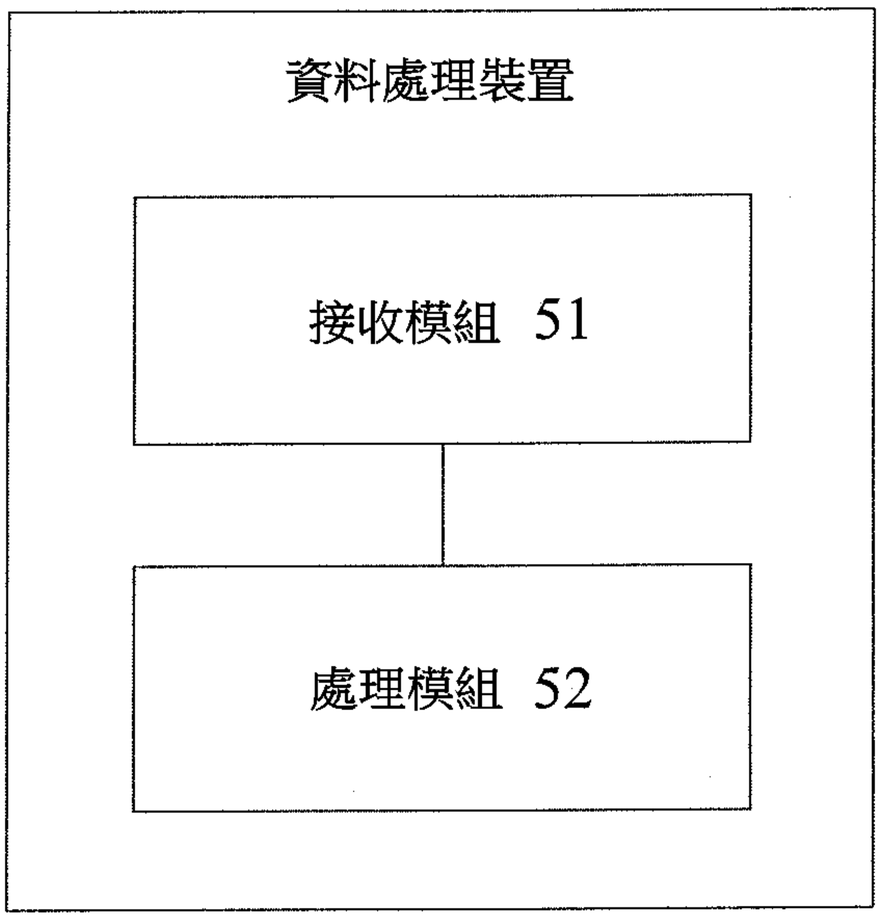
【圖 2】


S31
接收目標電子設備掃描目標二維碼得到的二維碼掃描資料
S32
根據所述簽名資料的簽名方式，對所述簽名資料進行驗簽，
獲得驗簽結果

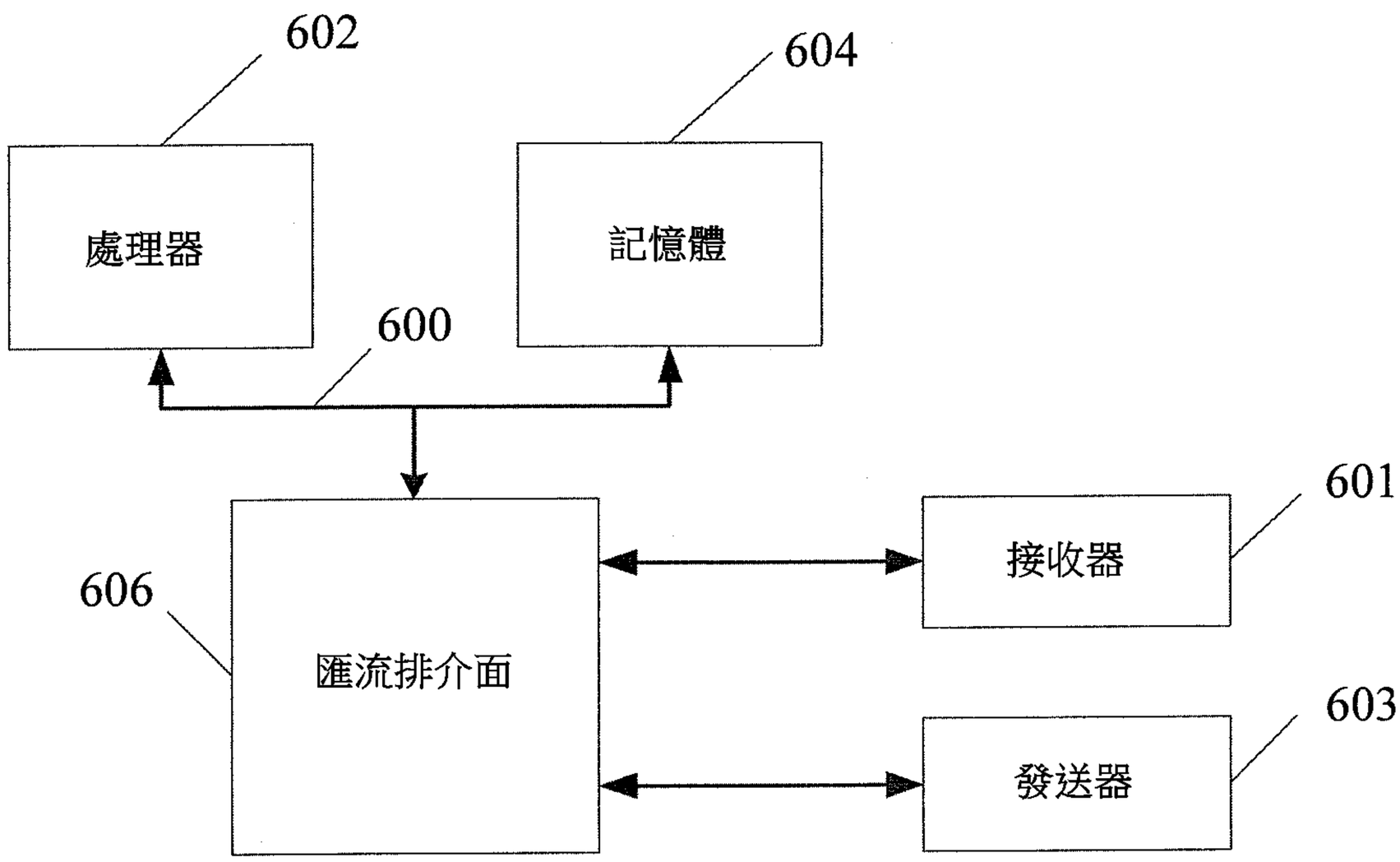
【圖 3】


二維碼生成裝置
二維碼生成資料獲取模組 41
簽名資料獲取模組 42
二維碼生成模組 43

【圖 4】


資料處理裝置
接收模組 51
處理模組 52

【圖 5】


602
604
處理器
記憶體
600
601
606
接收器
匯流排介面
603
發送器

【圖 6】