



(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 I802084 B

(45)公告日：中華民國 112 (2023) 年 05 月 11 日

(21)申請案號：110142618

(22)申請日：中華民國 110 (2021) 年 11 月 16 日

(51)Int. Cl. : G06Q20/34 (2012.01)

G06Q20/38 (2012.01)

G06Q20/40 (2012.01)

(30)優先權：2020/12/15

中國大陸

202011469593.8

(71)申請人：大陸商中國銀聯股份有限公司(中國大陸) CHINA UNIONPAY CO., LTD. (CN)

中國大陸

(72)發明人：劉剛(CN)；彭程(CN)；孫權(CN)；鄒震中(CN)；詹成初(CN)；才華(CN)

(74)代理人：廖俊龍

(56)參考文獻：

TW M590733U

CN 109842605A

CN 111932245A

US 2020/0034830A1

審查人員：沈佳瑾

申請專利範圍項數：27 項 圖式數：23 共 63 頁

(54)名稱

卡管理方法、用戶終端、伺服器、系統及存儲介質

(57)摘要

本發明公開了一種卡管理方法、用戶終端、伺服器、系統及存儲介質，屬於資料處理領域。用戶終端的安全元件存儲有第一類通用卡實例和第二類通用卡實例，第一匹配通用卡實例用於綁定卡的交易驗證，第一匹配通用卡實例包括第一匹配通用卡標識，第一匹配通用卡標識為與綁定卡的卡類型匹配的第一類通用卡標識或第二類通用卡標識。該方法包括：向伺服器發送卡綁定消息，卡綁定消息包括安全元件標識和綁定卡認證資訊，以使伺服器為綁定卡分配卡交易標識，並建立第一映射關係；接收伺服器發送的綁定卡的卡交易標識；將綁定卡的卡交易標識存儲至安全元件。根據本發明實施例，能夠降低卡管理流程的繁瑣程度。

指定代表圖：

符號簡單說明：

S201,S202,S203:步驟

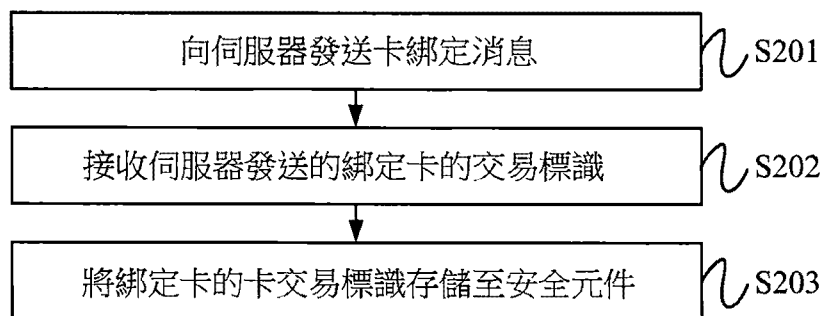


圖 4

※ 申請案號：110142618

※ 申請日：110年11月16日 ※IPC 分類：G06Q 20/34 (2012.01)  
G06Q 20/38 (2012.01)  
G06Q 20/40 (2012.01)

**【發明名稱】（中文/英文）**

卡管理方法、用戶終端、伺服器、系統及存儲介質

**【中文】**

本發明公開了一種卡管理方法、用戶終端、伺服器、系統及存儲介質，屬於資料處理領域。用戶終端的安全元件存儲有第一類通用卡實例和第二類通用卡實例，第一匹配通用卡實例用於綁定卡的交易驗證，第一匹配通用卡實例包括第一匹配通用卡標識，第一匹配通用卡標識為與綁定卡的卡類型匹配的第一類通用卡標識或第二類通用卡標識。該方法包括：向伺服器發送卡綁定消息，卡綁定消息包括安全元件標識和綁定卡認證資訊，以使伺服器為綁定卡分配卡交易標識，並建立第一映射關係；接收伺服器發送的綁定卡的卡交易標識；將綁定卡的卡交易標識存儲至安全元件。根據本發明實施例，能夠降低卡管理流程的繁瑣程度。

**【英文】**

**【代表圖】**

**【本案指定代表圖】**：圖 4。

**【本代表圖之符號簡單說明】**：

S201,S202,S203：步驟

# 發明專利說明書

(本說明書格式、順序，請勿任意更動)

## 【發明名稱】 (中文/英文)

卡管理方法、用戶終端、伺服器、系統及存儲介質

## 【技術領域】

【0001】 本發明屬於資料處理領域，尤其涉及一種卡管理方法、用戶終端、伺服器、系統及存儲介質。

## 【先前技術】

【0002】 隨著資訊技術的不斷發展，用戶可通過安裝有應用程式的用戶終端完成支付交易。在進行支付交易前，用戶需要將自己用於進行支付交易的卡如銀行卡等在應用程式中進行綁定，使得在通過應用程式進行支付交易的過程中可使用該卡。

【0003】 用戶可根據需求的變化，對卡進行管理，例如增加應用程式中綁定的卡，或刪除應用程式中綁定的卡等。為了使卡能夠進行支付交易，在多次綁定卡的情況下，需要頻繁地進行增加的綁定的卡對應的程式資料包和個人化資料的下載和存儲，使卡管理流程更加繁瑣。

## 【發明內容】

【0004】 本發明實施例提供一種卡管理方法、用戶終端、伺服器、系統及存儲介質，能夠降低卡管理流程的繁瑣程度。

【0005】 第一方面，本發明實施例提供一種卡管理方法，應用於用戶終端，用戶終端包括安全元件，安全元件存儲有第一類通用卡實例和第二類通用卡實例，第一類通用卡實例包括第一類通用卡標識和第一類通用個人化資料，第二類通用卡實例包括第二類通用卡標識和第二類通用個人化資料；

【0006】 方法包括：向伺服器發送卡綁定消息，卡綁定消息包括安全元件的安全元件標識和綁定卡的卡認證資訊，以使伺服器為綁定卡分配卡交易標識，並建立第一映射關係，第一映射關係包括安全元件標識、第一匹配通用卡標識和綁定卡的卡交易標識的映射關係，第一匹配通用卡標識為與綁定卡的卡類型匹配的第一類通用卡標識或第二類通用卡標識；接收伺服器發送的綁定卡的卡交易標識；將綁定卡的卡交易標識存儲至安全元件，第一匹配通用卡實例用於

綁定卡的交易驗證，第一匹配通用卡實例包括第一匹配通用卡標識。

**【0007】** 第二方面，本發明實施例提供一種卡管理方法，其特徵在於，應用於伺服器，伺服器存儲有用戶終端的第一類通用卡實例和第二類通用卡實例，第一類通用卡實例包括第一類通用卡標識和第一類通用個人化資料，第二類通用卡實例包括第二類通用卡標識和第二類通用個人化資料，第一類通用卡實例用於用戶終端進行卡類型為第一類型的卡的交易驗證，第二類通用卡實例用於用戶終端進行卡類型為第二類型的卡的交易驗證；

**【0008】** 方法包括：接收用戶終端發送的卡綁定消息，卡綁定消息包括安全元件標識和綁定卡認證資訊，綁定卡認證資訊包括綁定卡的卡認證資訊；回應於卡綁定消息，為綁定卡分配卡交易標識，並建立第一映射關係，第一映射關係包括安全元件標識、第一匹配通用卡標識和綁定卡的卡交易標識的映射關係，第一匹配通用卡標識為與綁定卡的卡類型匹配的第一類通用卡標識或第二類通用卡標識；向用戶終端發送綁定卡的卡交易標識，第一匹配通用卡實例用於綁定卡的交易驗證，第一匹配通用卡實例包括第一匹配通用卡標識。

**【0009】** 第三方面，本發明實施例提供一種用戶終端，其特徵在於，用戶終端具有安全元件，安全元件存儲有第一類通用卡實例和第二類通用卡實例，第一類通用卡實例包括第一類通用卡標識和第一類通用個人化資料，第二類通用卡實例包括第二類通用卡標識和第二類通用個人化資料，第一類通用卡實例用於用戶終端進行卡類型為第一類型的卡的交易驗證，第二類通用卡實例用於用戶終端進行卡類型為第二類型的卡的交易驗證；

**【0010】** 用戶終端包括：發送模組，用於向伺服器發送卡綁定消息，卡綁定消息包括安全元件標識和綁定卡認證資訊，綁定卡認證資訊包括綁定卡的卡認證資訊，以使伺服器為綁定卡分配卡交易標識，並建立第一映射關係，第一映射關係包括安全元件標識、第一匹配通用卡標識和綁定卡的卡交易標識的映射關係，第一匹配通用卡標識為與綁定卡的卡類型匹配的第一類通用卡標識或第二類通用卡標識，第一匹配通用卡實例用於綁定卡的交易驗證，第一匹配通用卡實例包括第一匹配通用卡標識；接收模組，用於接收伺服器發送的綁定卡的卡交易標識；處理模組，用於將綁定卡的卡交易標識存儲至安全元件。

**【0011】** 第四方面，本發明實施例提供一種伺服器，其特徵在於，伺服器

存儲有用戶終端的第一類通用卡實例和第二類通用卡實例，第一類通用卡實例包括第一類通用卡標識和第一類通用個人化資料，第二類通用卡實例包括第二類通用卡標識和第二類通用個人化資料，第一類通用卡實例用於用戶終端進行卡類型為第一類型的卡的交易驗證，第二類通用卡實例用於用戶終端進行卡類型為第二類型的卡的交易驗證；

**【0012】** 伺服器包括：接收模組，用於接收用戶終端發送的卡綁定消息，卡綁定消息包括安全元件標識和綁定卡認證資訊，綁定卡認證資訊包括綁定卡的卡認證資訊；處理模組，用於回應於卡綁定消息，為綁定卡分配卡交易標識，並建立第一映射關係，第一映射關係包括安全元件標識、第一匹配通用卡標識和綁定卡的卡交易標識的映射關係，第一匹配通用卡標識為與綁定卡的卡類型匹配的第一類通用卡標識或第二類通用卡標識，第一匹配通用卡實例用於綁定卡的交易驗證，第一匹配通用卡實例包括第一匹配通用卡標識；發送模組，用於向用戶終端發送綁定卡的卡交易標識。

**【0013】** 第五方面，本發明實施例提供一種用戶終端，包括：處理器以及存儲有電腦程式指令的記憶體；處理器執行電腦程式指令時實現第一方面中的卡管理方法。

**【0014】** 第六方面，本發明實施例提供本發明實施例提供一種伺服器，包括：處理器以及存儲有電腦程式指令的記憶體；處理器執行電腦程式指令時實現第二方面中的卡管理方法。

**【0015】** 第七方面，本發明實施例提供一種卡管理系統，包括第五方面的用戶終端和第六方面的伺服器。

**【0016】** 第八方面，本發明實施例提供一種電腦存儲介質，電腦存儲介質上存儲有電腦程式指令，電腦程式指令被處理器執行時實現第一方面中的卡管理方法或第二方面中的卡管理方法。

**【0017】** 本發明實施例提供一種卡管理方法、用戶終端、伺服器、系統及存儲介質，用戶終端的安全元件中存儲有第一類通用卡實例和第二類通用卡實例。用戶終端通過向伺服器發送卡綁定消息，使伺服器為綁定卡分配卡交易標識，並建立安全元件標識、第一匹配通用卡標識和分配的卡交易標識的映射關係。用戶終端自身可利用綁定卡對應的第一匹配通用卡實例進行交易驗證，伺

服务器利用确定的第一匹配通用卡实例进行交易验证。第一匹配通用卡实例为与绑定卡的卡类型匹配的第一类通用卡实例或第二类通用卡实例。即利用第一类通用卡实例或第二类通用卡实例即可完成交易验证。在绑定卡的过程中，服务器并不需要为每张卡分配对应的个人化资料，因此不需要在每次绑卡的过程中下载个人化资料，从而避免频繁地进行个人化资料的下载和存储，降低了卡管理流程的繁琐程度。

## 【圖式簡單說明】

### 【0018】

為了更清楚地說明本發明實施例的技術方案，下面將對本發明實施例中需要使用的圖式作簡單的介紹，對於本領域普通技術人員來講，在不付出創造性勞動的前提下，還可以根據這些圖式獲得其他的圖式。

圖 1 為本發明實施例提供的卡管理方法的應用場景的一示例的示意圖；

圖 2 為本發明實施例提供的用戶終端的安全元件中存儲內容的一示例的示意圖；

圖 3 為本發明實施例提供的伺服器中存儲的映射關係的一示例的示意圖；

圖 4 為本發明第一方面提供的卡管理方法的一示例的流程圖；

圖 5 為本發明第一方面提供卡管理方法的另一實施例的流程圖；

圖 6 為本發明第一方面提供的卡管理方法的又一實施例的流程圖；

圖 7 為本發明第一方面提供的卡管理方法的再一實施例的流程圖；

圖 8 為本發明第一方面提供的卡管理方法的又再一實施例的流程圖；

圖 9 為本發明第二方面提供的卡管理方法的一實施例的流程圖；

圖 10 為本發明第二方面提供的卡管理方法的另一實施例的流程圖；

圖 11 為本發明第二方面提供的卡管理方法的又一實施例的流程圖；

圖 12 為本發明第二方面提供的卡管理方法的再一實施例的流程圖；

圖 13 為本發明第二方面提供的卡管理方法的又再一實施例的流程圖；

圖 14 為本發明實施例提供的初始化流程的一示例的流程圖；

圖 15 為本發明實施例提供的卡綁定流程的一示例的流程圖；

圖 16 為本發明實施例提供的卡刪除流程的一示例的流程圖；

圖 17 為本發明實施例提供的卡刪除流程的另一示例的流程圖；

- 圖 18 為本發明第三方面提供的用戶終端的一實施例的結構示意圖；  
圖 19 為本發明第三方面提供的用戶終端的另一實施例的結構示意圖；  
圖 20 為本發明第四方面提供的伺服器的一實施例的結構示意圖；  
圖 21 為本發明第四方面提供的伺服器的另一實施例的結構示意圖；  
圖 22 為本發明第五方面提供的用戶終端的一實施例的結構示意圖；  
圖 23 為本發明第六方面提供的伺服器的一實施例的結構示意圖。

### 【實施方式】

**【0019】** 下面將詳細描述本發明的各個方面的特徵和示例性實施例，為了使本發明的目的、技術方案及優點更加清楚明白，以下結合圖式及具體實施例，對本發明進行進一步詳細描述。應理解，此處所描述的具體實施例僅意在解釋本發明，而不是限定本發明。對於本領域技術人員來說，本發明可以在不需要這些具體細節中的一些細節的情況下實施。下面對實施例的描述僅僅是為了通過示出本發明的示例來提供對本發明更好的理解。

**【0020】** 隨著資訊技術的不斷發展，用於可通過用戶終端中安裝的應用程式來完成支付交易。應用程式會與用戶的卡如銀行卡等綁定，在支付交易的過程中，支付交易過程中的資源從應用程式綁定的一張卡中轉出。利用每張卡進行支付交易的過程中，需要進行交易驗證。為了能夠實現交易驗證，會為每張卡分配對應的程式資料包和個人化資料，並存儲在用戶終端。每綁定一張卡，用戶終端都需要下載和存儲為這一張卡分配的程式資料包和個人化資料。在應用程式綁定多張卡的情況下，用戶終端需要多次下載和存儲卡對應的程式資料包和個人化資料。在應用程式刪除卡的情況下，用戶終端需要將該卡對應的程式資料包和個人化資料刪除。程式資料包和個人化資料頻繁的下載、刪除，使得卡管理流程更加繁瑣。尤其是在用戶將刪除的卡重新綁定的情況下，用戶終端需要將該卡對應的程式資料包和個人化資料重新下載，卡管理流程的繁瑣程度更加嚴重。

**【0021】** 本發明實施例提供一種卡管理方法、終端設備、伺服器、系統及存儲介質，能夠避免個人化資料頻繁的下載和刪除，從而簡化卡管理流程，降低卡管理流程的繁瑣程度。

**【0022】** 圖 1 為本發明實施例提供的卡管理方法的應用場景的一示例的示

意圖。如圖 1 所示，本發明實施例提供的卡管理方法可涉及用戶終端 11 和伺服器 12，在此並不限定。

**【0023】** 用戶終端 11 可包括手機、平板電腦、可穿戴設備、各類異形卡等具有支付交易功能的終端設備，在此並不限定。用戶終端 11 中可安裝有用於進行支付交易的應用程式。用戶可通過應用程式實現支付交易。

**【0024】** 用戶終端 11 可包括安全元件，安全元件為用戶終端 11 中設置的安全保護元件，可包括具體的硬體電路，也可包括搭建的安全環境，在此並不限定。例如，安全元件可包括安全元件（Secure Element，SE）、可信執行環境（Trusted Execution Environment，TEE）、SE+TEE、主機의卡類比（Host-based Card Emulation，HCE）等。在本發明實施例中，安全元件中存儲有第一類通用卡實例和第二類通用卡實例。具體的，可在初次進行卡綁定的過程中，通過初始化操作將第一類通用卡實例和第二類通用卡實例下載至安全元件中；也可在用戶終端出廠前將第一類通用卡實例和第二類通用卡實例預置在安全元件中，在此並不限定。

**【0025】** 第一類通用卡實例包括第一類通用卡標識和第一類通用個人化資料。第一類通用卡實例用於用戶終端進行卡類型為第一類型的卡的交易驗證。第一類通用卡標識包括卡類型為第一類型的卡的通用標識。第一類通用個人化資料包括卡類型為第一類型的卡的通用的個人化資料。在卡類型為第一類型的卡進行支付交易的情況下，可利用第一類通用卡實例進行交易驗證計算。

**【0026】** 第二類通用卡實例包括第二類通用卡標識和第二類通用個人化資料。第二類通用卡實例用於用戶終端進行卡類型為第二類型的卡的交易驗證。第二類通用卡標識包括卡類型為第二類型的卡的通用標識。第二類通用個人化資料包括卡類型為第二類型的卡的通用的個人化資料。在卡類型為第二類型的卡進行支付交易的情況下，可利用第二類通用卡實例進行交易驗證計算。

**【0027】** 安全元件中還可存儲應用程式中綁定的卡的卡交易標識。不同的卡的卡交易標識不同。卡的卡交易標識可在綁定卡的過程中由管理伺服器分配，用戶終端接收卡的卡交易標識並存儲於安全元件。通過不同的卡交易標識可在卡中資源轉移、清算等過程中，區分進行支付交易的具體卡。

**【0028】** 第一類通用卡標識與第二類通用卡標識的格式可以不同。例如，

第一類通用卡標識為借記通用卡標識，借記通用卡標識可為 19 位元標識；第二類通用卡標識為貸記通用卡標識，貸記通用卡標識可為 16 為標識。卡類型不同的卡的卡交易標識的格式也可以不同。例如，借記卡的卡交易標識可為 19 位元標識，貸記卡的卡交易標識可為 16 位元標識。

**【0029】** 在一些示例中，安全元件中還可存儲有一個程式資料包。該程式資料包包括安全元件運行所需的程式，在此並不限定。該程式資料包具體可為 Cap 包形式。安全元件中對卡的相關資訊、第一類通用卡實例和第二類通用卡實例等的內部操作可共用這一個程式資料包，且該程式資料包存儲至安全元件後，不再刪除，避免程式資料包的頻繁下載和刪除。具體地，該程式資料包可在初次進行卡綁定的過程中通過初始化操作下載至安全元件中；也可在用戶終端出廠前將該程式資料包預置在安全元件中，在此並不限定。

**【0030】** 例如，圖 2 為本發明實施例提供的用戶終端的安全元件中存儲內容的一示例的示意圖。如圖 2 所示，安全元件中存儲有 Cap 包、第一類通用卡實例、第二類通用卡實例和綁定的各個銀行卡的卡交易標識。第一類型的卡為銀行卡中的借記卡，第一類通用卡標識可作為與應用程式綁定的卡中的所有借記卡通用的卡標識，第一類通用卡標識記為 Token A，第一類通用個人化資料記為 Data A。第二類型的卡為銀行卡中的貸記卡，第二類通用卡標識可作為與應用程式綁定的卡中的所有貸記卡通用的卡標識，第二類通用卡標識記為 Token B，第二類通用個人化資料記為 Data B。設應用程式綁定有銀行卡 C1、C2、C3 和 C4。其中，銀行卡 C1 和 C2 為借記卡，銀行卡 C1 和 C2 各自的卡交易標識分別為 Token 1 和 Token 2。銀行卡 C3 和 C4 為貸記卡，銀行卡 C3 和 C4 各自的卡交易標識分別為 Token 3 和 Token 4。

**【0031】** 需要說明的是，在此並不限定卡類型的數量，例如，在存在卡類型為第三類型的卡、卡類型為第四類型的卡等的情況下，安全元件中還可存儲有第三類通用卡實例、第四類通用卡實例等，第三類通用卡實例、第四類通用卡實例等與第一通用卡實例、第二通用卡實例類似，作用和卡管理流程中的使用可參考第一通用卡實例、第二通用卡實例，在此不再贅述。

**【0032】** 用戶終端存儲通用卡實例，並不需要下載、存儲每張卡對應的實例，可減小用戶終端中存儲資源的佔用率，減少下載所佔用的運行資源，優化

存儲資源和運行資源。

**【0033】** 伺服器 12 可包括管理伺服器 121 和應用程式的後臺伺服器 122，在此並不限定。在一些示例中，管理伺服器 121 可包括信託服務管理平臺（Trusted Service Manager，TSM）伺服器 1211 和內容服務提供者（Telematics Service Provider，TSP）伺服器 1212。管理伺服器 121 和後臺伺服器 122 之間可進行交互。TSM 伺服器 1211 與 TSP 伺服器 1212 也可進行交互。

**【0034】** 伺服器 12 中可存儲有與伺服器 12 進行交互的各個用戶終端對應的第一類通用卡實例和第二類通用卡實例。用戶終端的安全元件中的第一類通用卡實例和第二類通用卡實例與伺服器中存儲的第一類通用卡實例和第二類通用卡實例相同。需要說明的是，不同用戶終端對應的第一類通用卡實例和第二類通用卡實例不同，可由伺服器統一分配。

**【0035】** 伺服器 12 中可存儲與該伺服器 12 進行交互的各個終端設備的綁定卡的安全元件標識、匹配通用卡標識和綁定卡的卡交易標識的映射關係。匹配通用卡標識為與綁定卡的卡類型匹配的第一類通用卡標識或第二類通用卡標識。在一些示例中，該映射關係中涉及的元素還可包括與安全元件標識對應的卡生產生命週期資料（Card Production Life Cycle Data，CPLC）中的其他資訊，在此並不限定。

**【0036】** 例如，設伺服器 12 與三個不同的用戶終端 UE1、UE2 和 UE3 分別進行交互。用戶終端 UE1 中安全元件的安全元件標識為 SEID 1。用戶終端 UE1 對應的借記類通用卡標識為 Token A，貸記類通用卡標識為 Token B。用戶終端 UE1 對應綁定有兩張銀行卡，兩張銀行卡包括一張借記卡和一張貸記卡，借記卡的卡交易標識為 Token 1，貸記卡的卡交易標識為 Token 2。用戶終端 UE2 中安全元件的安全元件標識為 SEID 2。用戶終端 UE2 對應的借記類通用卡標識為 Token C，貸記類通用卡標識為 Token D。用戶終端 UE2 對應綁定有一張銀行卡，該銀行卡為借記卡，該借記卡的卡交易標識為 Token 3。用戶終端 UE3 中安全元件的安全元件標識為 SEID 3。用戶終端 UE3 對應的借記類通用卡標識為 Token E，貸記類通用卡標識為 Token F。用戶終端 UE3 對應綁定有三張銀行卡，三張銀行卡包括兩張借記卡和一張貸記卡，借記卡的卡交易標識分別為 Token 4 和 Token 5，貸記卡的卡交易標識為 Token 6。圖 3 為本發明實施例

提供的伺服器中存儲的映射關係的一示例的示意圖，示出了上述各個終端設備的綁定卡的安全元件標識、匹配通用卡標識和綁定卡的卡交易標識的映射關係。

**【0037】** 在一些示例中，為了便於用戶終端與管理伺服器之間的交互，可在用戶終端安裝管理伺服器的功能控制項，用戶終端可通過該功能控制項與管理伺服器進行交互。例如，用戶終端可通過該功能控制項與 TSM 伺服器進行交互。

**【0038】** 下面將具體說明本發明提供的卡管理方法、用戶終端、伺服器、系統及存儲介質。

**【0039】** 本發明第一方面提供一種卡管理方法，可應用於用戶終端。圖 4 為本發明第一方面提供的卡管理方法的一示例的流程圖。如圖 4 所示，該卡管理方法可包括步驟 S201 至步驟 S203。

**【0040】** 在步驟 S201 中，向伺服器發送卡綁定消息。

**【0041】** 具體地，用戶終端設備可回應於用戶對用戶終端的應用程式的輸入觸發卡綁定消息的發送，在此並不限定。

**【0042】** 卡綁定消息包括安全元件標識和綁定卡認證資訊。安全元件標識用於標識安全元件。不同的用戶終端中的安全元件的安全元件標識不同。安全元件標識可在初次進行卡綁定的過程中通過初始化操作寫入安全元件；也可在用戶終端出廠前將安全元件標識預置入安全元件。

**【0043】** 綁定卡認證資訊包括綁定卡的卡認證資訊。卡綁定消息請求綁定的卡即為綁定卡。卡認證資訊可用於標識卡。例如，在卡為銀行卡的情況下，卡認證資訊具體可包括銀行卡的卡號，還可包括密碼、卡所屬人手機號、卡有效期、信用卡鑒別密碼等，在此並不限定。不同的卡的卡認證資訊不同。卡認證資訊可通過用戶輸入或掃描得到，在此並不限定。

**【0044】** 伺服器接收到卡綁定消息，可根據卡綁定消息中的卡認證資訊為綁定卡分配卡交易標識。卡交易標識用於標識卡，與卡認證資訊不同。同一張卡的卡交易標識和卡認證資訊均可標識該卡，但由於卡認證資訊為敏感資訊，在進行支付交易的過程中，通過卡交易標識來進行交易，以避免用戶隱私洩露。

**【0045】** 在伺服器接收到卡綁定消息的情況下，伺服器還可建立第一映射關係。第一映射關係包括安全元件標識、第一匹配通用卡標識和綁定卡的卡交

易標識的映射關係。第一匹配通用卡標識為與綁定卡的卡類型匹配的第一類通用卡標識或第二類通用卡標識。在綁定卡的卡類型為第一類型的情況下，綁定卡的第一匹配通用卡標識為第一類通用卡標識。在綁定卡的卡類型為第二類型的情況下，綁定卡的第一匹配通用卡標識為第二類通用卡標識。

**【0046】** 在步驟 S202 中，接收伺服器發送的綁定卡的卡交易標識。

**【0047】** 卡交易標識可用於該綁定卡進行交易。

**【0048】** 在步驟 S203 中，將綁定卡的卡交易標識存儲至安全元件。

**【0049】** 為了保證卡交易標識的安全性，將綁定卡的卡交易標識存儲至安全元件中。安全元件中存儲有綁定的各個卡對應的卡交易標識。

**【0050】** 用戶終端的安全元件中存儲的第一匹配通用卡實例可用於該綁定卡的交易驗證。第一匹配通用卡實例包括第一匹配通用卡標識。即第一匹配通用卡實例為與綁定卡的卡類型匹配的第一類通用卡實例或第二類通用卡實例。

**【0051】** 在本發明實施例中，用戶終端的安全元件中存儲有第一類通用卡實例和第二類通用卡實例。用戶終端通過向伺服器發送卡綁定消息，使伺服器為綁定卡分配卡交易標識，並建立安全元件標識、第一匹配通用卡標識和分配的卡交易標識的映射關係。用戶終端自身可利用綁定卡對應的第一匹配通用卡實例進行交易驗證，伺服器利用確定的第一匹配通用卡實例進行交易驗證。第一匹配通用卡實例為與綁定卡的卡類型匹配的第一類通用卡實例或第二類通用卡實例。即利用第一類通用卡實例或第二類通用卡實例即可完成交易驗證。在綁定卡的過程中，伺服器並不需要為每張卡分配對應的個人化資料，因此不需要在每次綁卡的過程中下載個人化資料，從而避免頻繁地進行個人化資料的下載和存儲，降低了卡管理流程的繁瑣程度，簡化卡管理流程，還可提高卡綁定的速度，減少卡綁定所花費的時間。

**【0052】** 在用戶終端將綁定卡的卡交易標識存儲至安全元件後，完成了卡綁定的申請階段，還需要將綁定卡啟動。圖 5 為本發明第一方面提供卡管理方法的另一實施例的流程圖。圖 5 與圖 4 的不同之處在於，圖 5 所示的卡管理流程還可包括步驟 S204 至步驟 S207。

**【0053】** 在步驟 S204 中，向伺服器發送驗證碼獲取請求消息。

**【0054】** 用戶終端在存儲綁定卡的卡交易標識後，可通過向伺服器發送驗

證碼獲取請求，觸發綁定卡啟動流程。驗證碼獲取請求消息用於請求動態驗證碼。

**【0055】** 在步驟 S205 中，接收伺服器回應於驗證碼獲取請求消息回饋的第一動態驗證碼。

**【0056】** 伺服器回應於驗證碼獲取請求消息，向用戶終端發送第一動態驗證碼。第一動態驗證碼用於綁定卡啟動。第一動態驗證碼可通過短信、即時通信消息、通話等回饋至用戶終端，在此並不限定。用戶終端可通過顯示文字圖像或發出聲音以向用戶展示第一動態驗證碼，在此並不限定。

**【0057】** 在步驟 S206 中，接收輸入的第二動態驗證碼。

**【0058】** 第二動態驗證碼可為用戶輸入的動態驗證碼，也可為通過應用程式根據第一動態驗證碼獲取並輸入的動態驗證碼，在此並不限定。

**【0059】** 在步驟 S207 中，向伺服器發送驗證碼請求消息，以使伺服器在第二動態驗證碼驗證成功的情況下啟動第一映射關係。

**【0060】** 驗證碼請求消息包括第二動態驗證碼。在第一動態驗證碼與第二動態驗證碼相同的情況下，確定第二動態驗證碼驗證成功。伺服器在第二動態驗證碼驗證成功的情況下，啟動第一映射關係。在第一映射關係未啟動的情況下，第一映射關係中卡交易標識對應的綁定卡處於不可用狀態。在第一映射關係啟動的情況下，第一映射關係中卡交易標識對應的綁定卡處於可用狀態。

**【0061】** 在一些示例中，在第一映射關係啟動的情況下，用戶終端可將第一映射關係中卡交易標識對應的綁定卡的生命狀態設置為可用狀態。

**【0062】** 在用戶終端初次進行卡綁定的情況下，用戶終端需要進行卡管理的初始化流程。圖 6 為本發明第一方案提供的卡管理方法的又一實施例的流程圖。圖 6 與圖 4 的不同之處在於，圖 6 所示的卡管理方法還可包括步驟 S208 至步驟 S210。

**【0063】** 在步驟 S208 中，向伺服器發送初始化請求消息。

**【0064】** 初始化請求消息用於觸發卡管理的初始化流程。

**【0065】** 在用戶終端還安裝有與伺服器的功能控制項的情況下，在用戶終端向伺服器發送初始化請求消息之前，用戶終端還可通過應用程式調用功能控制項進行初始化。為了保證初始化的合法性，在用戶終端向伺服器發送初始化

請求資訊前，用戶終端可與伺服器之間先進行用戶終端進行卡綁定的應用程式的合法性。

**【0066】** 在步驟 S209 中，與伺服器建立安全元件與伺服器之間的秘密頻道。

**【0067】** 秘密頻道具體可為 GP 通道，在此並不限定。用戶終端中安全元件還可與伺服器相互進行認證，在認證成功後，伺服器即可通過秘密頻道與安全元件進行交互。秘密頻道能夠提高用戶終端與伺服器之間交互的安全性。

**【0068】** 在步驟 S210 中，通過秘密頻道接收伺服器下發的初始化資訊，並將初始化資訊存儲至安全元件。

**【0069】** 在本示例中，在未進行初始化流程的情況下，用戶終端中安全元件處於原始狀態，無安全元件標識，也未存儲第一類通用卡實例和第二類通用卡實例等資訊。在進行初始化流程的過程中，通過秘密頻道傳輸的初始化資訊可包括但不限於安全元件標識、加密公開金鑰、第一類通用卡實例和第二類通用卡實例。加密公開金鑰可在後續的卡綁定流程中，對用戶終端與伺服器之間傳輸的資料進行加密。

**【0070】** 在一些示例中，初始化資訊還可包括安全元件中用於存儲與卡管理流程相關資料的交易功能區域的區域初始金鑰。

**【0071】** 在一些示例中，程式資料包可在用戶終端出廠前預置於用戶終端的安全元件中。

**【0072】** 在另一些示例中，在安全元件未存儲有程式資料包的情況下，初始化資訊還可包括程式資料包。即在卡管理的初始化過程中，將程式資料包下載至用戶終端的安全元件中。在後續過程中，若不需更新，則不需要重複下載程式資料包。

**【0073】** 在又一些示例中，在安全元件中存儲的程式資料包需要更新的情況下，初始化資訊還包括更新後的程式資料包。即在卡管理的初始化過程中，可對安全元件中的程式資料包進行更新，如利用更新後的程式資料包替換更新前的程式資料包。

**【0074】** 需要說明的是，安全元件中存儲的程式資料包的更新也可在除初始化過程外的其他過程中進行，在此並不限定。在安全元件中存儲的程式資料

包需要更新的情況下，用戶終端可向伺服器發送更新請求消息。更新請求消息用於請求更新後的程式資料包。該更新請求消息可以是伺服器檢測到安全元件中存儲的程式資料包需要更新，通知用戶終端發起更新請求消息，請求更新後的程式資料包。該更新請求消息也可以是用戶終端接收用戶更新輸入操作，向伺服器發起更新請求消息，請求更新後的程式資料包。

**【0075】** 在安全元件中存儲的程式資料包的版本低於伺服器中存儲的程式資料包的最新版本的情況下，可認為安全元件中存儲的程式資料包需要更新。或者，在安全元件中存儲的程式資料包的版本低於伺服器中存儲的程式資料包的最新版本，且得到用戶終端的用戶授權的情況下，可認為安全元件中存儲的程式資料包需要更新。

**【0076】** 在一些示例中，在用戶終端非初次進行卡綁定的情況下，伺服器可利用與上述初始化過程存儲入安全元件中的加密公開金鑰成對的加密私密金鑰對綁定的卡交易標識進行加密。即用戶終端接收到的綁定卡的卡交易標識可為利用與加密公開金鑰成對的加密私密金鑰加密的卡交易標識。加密公開金鑰和加密私密金鑰為成對的非對稱金鑰。在用戶終端與伺服器之間傳輸加密的卡交易標識，可在未建立秘密頻道的基礎上保證資料傳輸的安全性，不需要建立秘密頻道，從而節省了建立秘密頻道所需佔用的資源及花費的時間。

**【0077】** 對應地，用戶終端接收到加密的卡交易標識，可在安全元件內利用加密公開金鑰對綁定卡的卡交易標識解密，在安全元件中存儲解密後的綁定卡的卡交易標識。

**【0078】** 在綁定卡綁定成功後，可利用綁定卡進行交易支付。交易可分為聯網交易和離線交易兩種。聯網交易即為交易設備如 POS 機、刷卡機等具有交易功能的設備處於聯網狀態下的交易。離線交易即為交易設備處於離線狀態下的交易。圖 7 為本發明第一方面提供的卡管理方法的再一實施例的流程圖。圖 7 與圖 4 的不同之處在於，圖 7 所示的卡管理方法還可包括步驟 S211、步驟 S212。

**【0079】** 在步驟 S211 中，在利用綁定卡進行聯網交易的情況下，利用第一匹配通用卡實例進行交易驗證計算，向交易設備提供第一交易驗證資訊，以通過交易設備使伺服器根據第一映射關係，利用與綁定卡的卡交易標識對應的

第一匹配通用卡實例進行交易驗證計算。

**【0080】** 在利用綁定卡進行支付交易的情況下，第一交易驗證資訊包括綁定卡的卡交易標識。

**【0081】** 用戶終端和交易設備在聯網狀態下進行交易，用戶終端和伺服器需要進行交易驗證。具體地，用戶終端利用第一匹配通用卡實例進行交易驗證計算。交易設備可將接收到的第一交易驗證資訊向伺服器發送。伺服器根據存儲的第一映射關係，可確定與綁定卡的卡交易標識對應的第一匹配通用卡標識。伺服器基於第一匹配通用卡標識，可確定與綁定卡的卡交易標識對應的第一匹配通用卡實例，並利用該第一匹配通用卡實例進行交易驗證計算。第一匹配通用卡實例包括第一匹配通用卡標識，即第一匹配通用卡實例為與綁定卡的卡類型匹配的第一類通用卡實例或第二類通用卡實例。交易驗證計算具體可由 TSP 伺服器執行。在用戶終端的交易驗證計算結果與伺服器的交易驗證計算結果一致的情況下，確定交易驗證成功。例如，用戶終端和伺服器之間進行的交易驗證具體可包括但不限於授權請求報文（Authenticate Request cryptogram，ARQC）驗證。

**【0082】** 用戶終端與交易設備在聯網支付交易的情況下，用戶終端提供的第一交易驗證資訊包括用於交易的綁定卡的卡交易標識。第一交易驗證資訊可通過交易設備傳輸至伺服器，伺服器能夠根據卡交易標識識別出本次支付交易所使用的卡，使得收單方能夠區分不同的卡進行的支付交易。

**【0083】** 在步驟 S212 中，在利用綁定卡進行離線交易的情況下，利用第一匹配通用卡實例進行交易驗證計算，向交易設備提供第二交易驗證資訊，以使交易設備利用第一匹配通用卡實例進行交易驗證計算。

**【0084】** 第二交易驗證資訊包括第一匹配通用卡實例。在離線交易情況下，用戶終端與交易設備需要進行離線資料認證（Offline Data Authentication，ODA）。具體地，用戶終端可利用第一匹配通用卡實例進行交易驗證計算，交易設備可利用第二交易驗證資訊中的第一匹配通用卡實例進行交易驗證計算，在用戶終端的交易驗證計算結果與伺服器的交易驗證計算結果一致的情況下，確定離線資料認證成功。例如，用戶終端和交易設備進行的交易驗證具體可為交易證書（Transaction Certificate，TC）驗證，在此並不限定。

**【0085】** 需要說明的是，在交易設備再次聯網的情況下，交易設備會將本次離線交易的資料向伺服器發送。離線交易的資料可包括交易時間、第一匹配通用卡標識等，在此並不限定。

**【0086】** 用戶終端的應用程式可能會綁定多張卡，在綁定多張卡的情況下，會在綁定的多張卡中設置一張默認卡，使用該默認卡進行支付交易。默認卡可更改。圖 8 為本發明第一方案提供的卡管理方法的又一實施例的流程圖。圖 8 與圖 5 的不同之處在於，圖 8 所示的卡管理方法還可包括步驟 S213 至步驟 S216。

**【0087】** 在步驟 S213 中，接收默認卡設置輸入。

**【0088】** 默認卡設置輸入用於選定默認卡。默認卡設置輸入可為用戶對用戶終端的輸入，在此並不限定。默認卡為預設進行交易支付的卡。

**【0089】** 在步驟 S214 中，在聯網的情況下，向伺服器發送默認卡設置消息，以使伺服器將第二映射關係的使用狀態設置為預設使用狀態。

**【0090】** 默認卡設置消息包括默認卡的卡交易標識。第二映射關係包括安全元件標識、第二匹配通用卡標識和默認卡的卡交易標識的映射關係。第二匹配通用卡標識為與默認卡的卡類型匹配的第一類通用卡標識或第二類通用卡標識。在默認卡的卡類型為第一類型的情況下，默認卡的第二匹配通用卡標識為第一類通用卡標識。在默認卡的卡類型為第二類型的情況下，默認卡的第二匹配通用卡標識為第二類通用卡標識。

**【0091】** 伺服器可根據默認卡的卡交易標識，查找到包括默認卡的卡交易標識的第二映射關係。伺服器將第二映射關係的使用狀態設置為預設使用狀態，對應地，在進行支付交易的過程中，伺服器會默認利用第二映射關係包括的安全元件標識、第二匹配通用卡標識和默認卡的卡交易標識進行支付交易流程。

**【0092】** 在步驟 S215 中，接收伺服器發送的默認卡應答消息。

**【0093】** 在將第二映射關係的使用狀態設置為預設使用狀態的情況下，伺服器向用戶終端發送默認卡應答消息，以通知用戶終端。默認卡應答消息用於表徵第二映射關係的使用狀態已設置為預設使用狀態。

**【0094】** 在步驟 S216 中，回應於默認卡應答消息，通過默認卡設置指令，將安全元件中默認卡的卡交易標識的使用狀態設置為預設使用狀態，將安全元

件中與默認卡的卡交易標識對應的第二匹配通用卡實例的生命狀態設置為生效狀態。

**【0095】** 第二匹配通用卡實例為與默認卡的卡類型匹配的第一類通用卡實例或第二類通用卡實例。在默認卡的卡類型為第一類型的情況下，默認卡的第二匹配通用卡實例為第一類通用卡實例。在默認卡的卡類型為第二類型的情況下，默認卡的第二匹配通用卡實例為第二類通用卡實例。

**【0096】** 用戶終端接收到默認卡應答消息，可確定伺服器中第二映射關係的使用狀態已設置為預設使用狀態，可對應設置安全元件中的默認卡的卡交易標識的使用狀態，以及設置第二匹配通用卡實例的生命狀態，從而保證用戶終端中默認卡的設置與伺服器中默認卡的設置的一致。

**【0097】** 默認卡設置指令為用戶終端向安全元件發送的控制指令。在此並不限定默認卡設置指令的具體形式，例如，默認卡設置指令可為應用協定資料單元（Application Protocol Data Unit，APDU）指令，在此並不限定。

**【0098】** 需要說明的是，安全元件可識別的默認卡設置指令可包括不同版本模式下的指令。安全元件接收到默認卡設置指令，可優先執行新版本模式的指令，若指令無效，再執行舊版本的指令。新、舊版本模式下的指令相互獨立，保證新、舊版本模式下的指令的執行具有相容性。

**【0099】** 在一些示例中，在進行支付交易所使用的卡即為默認卡。在進行支付交易的過程中需要利用與默認卡的卡類型相同的第一類通用卡實例或第二類通用卡實例進行交易驗證。可將與默認卡的卡類型相同的第一類通用卡實例或第二類通用卡實例即第二匹配通用卡實例的生命狀態設置為生效狀態，在進行支付交易的過程中，會預設利用生命狀態設置為生效狀態的第二匹配通用卡實例進行交易驗證。

**【0100】** 在使用上述實施例中某張綁定卡進行交易支付的情況下，該綁定卡即為默認卡。在利用某綁定卡進行離線交易後，在交易設備再次聯網的情況下，交易設備會將本次離線交易的資料向伺服器發送。離線交易的資料可包括交易時間、第一匹配通用卡標識等。在這種情況下，第一匹配通用卡標識與第二匹配通用卡標識相同，即第一匹配通用卡實例與第二匹配通用卡實例相同。

**【0101】** 伺服器可通過交易時間，查詢在交易時間使用狀態為預設使用狀

態的映射關係中的卡交易標識，利用卡交易標識進行結算等流程，即本次交易的金額從該卡交易標識對應的卡中轉出，從而保證離線交易的結算的準確性。

**【0102】** 在再一些實施例中，還可根據需求，將用戶終端的應用程式中已綁定的卡刪除，即執行卡刪除流程。用戶終端可接收卡刪除消息，回應於卡刪除消息，在安全元件中刪除卡刪除消息指示的待刪除卡的卡交易標識，或者，將卡刪除消息指示的待刪除卡的卡交易標識的生命狀態設置為失效狀態。

**【0103】** 卡交易標識的生命狀態為失效狀態，表示該卡交易標識處於不可用狀態，無法被調用。在該卡被刪除又再次需要綁定的情況下，可將該卡的卡交易標識的生命狀態設置為有效狀態，從而快速實現再次綁卡。

**【0104】** 需要注意的是，在這種情況下，安全元件中刪除了待刪除卡的卡交易標識，或者並不刪除待刪除卡的卡交易標識，只將待刪除卡的卡交易標識的生命狀態設置為失效狀態。不會刪除第一類通用卡實例和第二類通用卡實例，也不會刪除程式資料包。第一類通用卡實例和第二類通用卡實例還可用於其他未刪除的卡的交易驗證。

**【0105】** 在一些示例中，卡刪除流程可由用戶通過用戶終端發起。具體地，用戶可通過對用戶終端的應用程式的操作，發起卡刪除流程。用戶終端向伺服器發送卡刪除申請消息，通知伺服器請求刪除待刪除卡。回應於卡刪除申請消息，伺服器可生成卡刪除消息，向用戶終端發送卡刪除消息。用戶終端回應於卡刪除消息，在安全元件中刪除待刪除卡的卡交易標識，或者，將待刪除卡的卡交易標識的生命狀態設置為失效狀態。卡刪除消息可指示待刪除卡，例如，卡刪除消息包括待刪除卡的卡交易標識。用戶終端可向伺服器發送卡刪除請求消息，卡刪除請求消息可包括待刪除卡的卡交易標識。伺服器回應於卡刪除請求消息，將包括待刪除卡的卡交易標識的映射關係刪除。伺服器還可向用戶終端發送刪除卡應答消息，刪除卡應答消息用於表徵伺服器中已刪除包括待刪除卡的卡交易標識的映射關係。用戶終端可發出卡刪除成功提示資訊，以提示用戶待刪除卡刪除成功。

**【0106】** 在另一些示例中，卡刪除流程可由卡組織通過伺服器發起，例如，由銀行發起。伺服器接收卡組織發出的卡刪除請求消息。卡刪除請求消息用於指示待刪除卡，例如，卡刪除請求消息可包括待刪除卡的卡交易標識。回應於

卡刪除請求消息，伺服器刪除包括待刪除卡的卡交易標識的映射關係，並向用戶終端發送卡刪除消息。卡刪除消息用於指示待刪除卡，例如，卡刪除消息可包括待刪除卡的卡交易標識。用戶終端回應於卡刪除消息，在安全元件中刪除待刪除卡的卡交易標識，或者，將待刪除卡的卡交易標識的生命狀態設置為失效狀態。用戶終端可向伺服器發送卡刪除應答消息，以通知伺服器安全元件中待刪除卡刪除成功。

**【0107】** 需要說明的是，在待刪除卡為默認卡的情況下，需要指定綁定的另外一張卡為默認卡後，再進行待刪除卡的刪除。

**【0108】** 本發明實施例中，在刪除卡的情況下，應用終端並不刪除第一類通用卡實例和第二類通用卡實例，也不刪除程式資料包，避免了個人化資料和程式資料包的頻繁刪除。尤其是在再次綁定之前刪除過的卡的情況下，可避免再次綁定的過程中個人化資料和程式資料包的再次下載，從而進一步降低綁定卡過程、刪除卡過程的繁瑣程度。

**【0109】** 本發明第二方面還提供一種卡管理方法，可應用於伺服器。圖 9 為本發明第二方面提供的卡管理方法的一實施例的流程圖。如圖 9 所示，該卡管理方法可包括步驟 S301 至步驟 S303。

**【0110】** 在步驟 S301 中，接收用戶終端發送的卡綁定消息。

**【0111】** 卡綁定消息包括安全元件標識和綁定卡認證資訊。安全元件標識用於標識用戶終端中的安全元件。綁定卡認證資訊包括綁定卡的卡認證資訊。綁定卡為需要與用戶終端中的應用程式綁定的卡。

**【0112】** 在步驟 S302 中，回應於卡綁定消息，為綁定卡分配卡交易標識，並建立第一映射關係。

**【0113】** 伺服器為不同的卡分配不同的卡交易標識。具體地，伺服器可根據卡綁定消息中的綁定卡認證資訊，為綁定卡分配卡交易標識。

**【0114】** 第一映射關係包括安全元件標識、第一匹配通用卡標識和綁定卡的卡交易標識的映射關係。第一匹配通用卡標識為與綁定卡的卡類型匹配的第一類通用卡標識或第二類通用卡標識。第一匹配通用卡實例用於綁定卡的交易驗證。第一匹配通用卡實例包括第一匹配通用卡標識。

**【0115】** 在步驟 S303 中，向用戶終端發送綁定卡的卡交易標識。

**【0116】** 上述步驟 S301 至步驟 S303 中的具體內容可參見上述實施例中的相關說明，在此不再贅述。

**【0117】** 在本發明實施例中，伺服器回應於用戶終端發送的卡綁定消息，為綁定卡分配卡交易標識，並建立安全元件標識、第一匹配通用卡標識和分配的該卡交易標識的第一映射關係。伺服器將為綁定卡分配的卡交易標識向用戶終端發送，以使用戶終端獲取該卡交易標識。第一匹配通用卡實例用於進行綁定卡的交易驗證計算。對於用戶終端的應用程式綁定的卡類型相同的卡，用戶終端與伺服器利用相同的匹配通用卡實例進行交易驗證，因此伺服器不需要為每張卡單獨配置用於交易驗證的個人化資料，避免了每次卡綁定伺服器都需要將該卡對應的個人化資料傳輸給用戶終端的情況，降低了卡管理流程的繁瑣程度，簡化卡管理流程，還可提高卡綁定的速度，減少卡綁定所花費的時間。

**【0118】** 在用戶終端將綁定卡的卡交易標識存儲至安全元件後，完成了卡綁定的申請階段，還需要將綁定卡啟動。圖 10 為本發明第二方面提供的卡管理方法的另一實施例的流程圖。圖 10 與圖 9 的不同之處在於，圖 10 所示的卡管理方法還可包括步驟 S304 至步驟 S307。

**【0119】** 在步驟 S304 中，接收用戶終端發送的驗證碼獲取請求消息。

**【0120】** 在步驟 S305 中，回應驗證碼獲取請求消息，向用戶終端回饋第一動態驗證碼。

**【0121】** 在步驟 S306 中，接收用戶終端發送的驗證碼請求消息，驗證碼請求消息包括第二動態驗證碼。

**【0122】** 在步驟 S307 中，在第二動態驗證碼驗證成功的情況下啟動第一映射關係。

**【0123】** 步驟 S304 至步驟 S307 的具體內容可參見上述實施例中的相關說明，在此不再贅述。

**【0124】** 在用戶終端初次進行卡綁定的情況下，用戶終端需要進行卡管理的初始化流程。圖 11 為本發明第二方面提供的卡管理方法的又一實施例的流程圖。圖 11 與圖 9 的不同之處在於，圖 11 所示的卡管理方法還可包括步驟 S308 至步驟 S310。

**【0125】** 在步驟 S308 中，接收用戶終端發送的初始化請求消息。

**【0126】** 初始化請求消息用於觸發卡管理的初始化流程。

**【0127】** 在步驟 S309 中，回應於初始化請求消息，與用戶終端建立用戶終端中安全元件與伺服器之間的秘密頻道。

**【0128】** 在步驟 S310 中，通過秘密頻道向安全元件下發初始化資訊。

**【0129】** 初始化資訊包括安全元件標識、加密公開金鑰、第一類通用卡實例和第二類通用卡實例。

**【0130】** 伺服器還可記錄第一類通用個人化資料和第二類通用個人化資料的版本，在第一類通用個人化資料和第二類通用個人化資料出現新版本的情況下，可更新用戶終端的安全元件存儲的第一類通用個人化資料和第二類通用個人化資料。

**【0131】** 上述步驟 S308 至步驟 S310 的具體內容可參見上述實施例中的相關說明，在此不再贅述。

**【0132】** 在一些示例中，初始化資訊還可包括安全元件中用於存儲與卡管理流程相關資料的區域的區域初始金鑰。

**【0133】** 在一些示例中，程式資料包可在用戶終端出廠前預置於用戶終端的安全元件中。

**【0134】** 在另一些示例中，在安全元件未存儲有程式資料包的情況下，初始化資訊還包括程式資料包。

**【0135】** 在又一些示例中，在安全元件中存儲的程式資料包需要升級的情況下，初始化資訊還包括升級後的程式資料包。

**【0136】** 在一些示例中，不限於初始化過程，在其他過程中，在安全元件中存儲的程式資料包需要更新的情況下，伺服器可接收用戶終端發送的更新請求消息。伺服器回應更新請求消息，向用戶終端下發更新後的程式資料包，以實現安全元件中程式資料包的更新。程式資料包更新的具體內容可參見上述實施例中的相關說明，在此不再贅述。

**【0137】** 在一些示例中，在伺服器非初次接收到卡綁定消息的情況下，伺服器可利用與加密公開金鑰成對的加密私密金鑰對綁定卡的卡交易標識加密；向用戶終端發送加密後的綁定卡的卡交易標識。

**【0138】** 在綁定卡綁定成功後，可利用綁定卡進行交易支付。交易可分為

聯網交易和離線交易兩種。聯網交易即為交易設備如 POS 機、刷卡機等具有交易功能的設備處於聯網狀態下的交易。離線交易即為交易設備處於離線狀態下的交易。圖 12 為本發明第二方面提供的卡管理方法的再一實施例的流程圖。圖 12 與圖 9 的不同之處在於，圖 12 所示的卡管理方法還可包括步驟 S311、步驟 S312。

**【0139】** 在步驟 S311 中，在利用綁定卡進行聯網交易的情況下，通過交易設備接收用戶終端提供的第一交易驗證資訊，根據第一映射關係，利用與綁定卡的卡交易標識對應的第一匹配通用卡實例進行交易驗證計算。

**【0140】** 第一交易驗證資訊包括綁定卡的卡交易標識。根據第一映射關係，可確定與綁定卡的卡交易標識對應的第一匹配通用卡實例，進而利用第一匹配通用卡實例進行交易驗證計算。第一匹配通用卡實例包括第一匹配通用卡標識，即第一匹配通用卡實例為與綁定卡的卡類型匹配的第一類通用卡實例或第二類通用卡實例。在用戶終端的交易驗證計算結果與伺服器的交易驗證計算結果一致的情況下，確定交易驗證成功。

**【0141】** 用戶終端與交易設備在聯網支付交易的情況下，伺服器通過交易設備從用戶終端獲取的第一交易驗證資訊包括用於交易的綁定卡的卡交易標識。伺服器能夠根據該卡交易標識識別出本次支付交易所使用的卡，使得收單方能夠區分不同的卡進行的支付交易。

**【0142】** 在步驟 S312 中，在用戶終端利用綁定卡與交易設備進行離線交易後，在聯網的情況下，獲取第一匹配通用卡實例，根據第一匹配通用卡實例進行交易驗證計算。

**【0143】** 具體地，在發生離線交易後，若交易設備再次聯網，伺服器可獲取到與該綁定卡對應的第一匹配通用卡實例，利用第一匹配通用卡實例進行交易驗證計算。

**【0144】** 用戶終端的應用程式可能會綁定多張卡，在綁定多張卡的情況下，會在綁定的多張卡中設置一張默認卡，使用該默認卡進行支付交易。默認卡可更改。圖 13 為本發明第二方面提供的卡管理方法的又再一實施例的流程圖。圖 13 與圖 10 的不同之處在於，圖 11 所示的卡管理方法還可包括步驟 S313 至步驟 S315。

**【0145】** 在步驟 S313 中，在聯網的情況下，接收用戶終端發送的默認卡設置消息。

**【0146】** 默認卡設置消息包括選定的默認卡的卡交易標識。

**【0147】** 在步驟 S314 中，回應於默認卡設置消息，將第二映射關係的使用狀態設置為預設使用狀態。

**【0148】** 第二映射關係包括安全元件標識、第二匹配通用卡標識和默認卡的卡交易標識的映射關係。

**【0149】** 在步驟 S315 中，向用戶終端發送默認卡應答消息。

**【0150】** 默認卡應答消息用於表徵第二映射關係的使用狀態已設置為預設使用狀態。

**【0151】** 在使用上述實施例中某張綁定卡進行交易支付的情況下，該綁定卡即為默認卡。在利用某綁定卡進行離線交易後，在交易設備在此聯網的情況下，伺服器會接收到交易設備發送的離線交易的相關資訊，該相關資訊可包括交易時間。伺服器可根據交易時間，確定在交易時間使用狀態為預設使用狀態的第二映射關係。利用該第二映射關係中默認卡的卡交易標識進行結算，即從該默認卡的帳戶中將交易金額轉出，能夠避免利用錯誤的帳戶進行結算，提高了離線交易的準確性。

**【0152】** 在交易支付過程的結算流程中，可利用第二映射關係中默認卡的卡交易標識進行結算。伺服器與用戶終端的默認卡的設置只能在聯網狀態下進行，從而使得能夠通過交易時間，來確定交易時間對應的默認卡。

**【0153】** 步驟 S313 至步驟 S315 的具體內容可參見上述實施例中的相關說明，在此不再贅述。

**【0154】** 在再一些實施例中，還可根據需求，將用戶終端的應用程式中已綁定的卡刪除，即執行卡刪除流程。伺服器可接收卡刪除請求消息，回應於卡刪除請求消息，刪除第三映射關係，或者，將第三映射關係的生命狀態設置為失效狀態。

**【0155】** 卡刪除請求消息用於指示待刪除卡。第三映射關係包括安全元件標識、第三匹配通用卡標識與待刪除卡的卡交易標識的對應關係。第三匹配通用卡標識為與待刪除卡的卡類型匹配的第一類通用卡標識或第二類通用卡標識。

在綁定卡的卡類型為第一類型的情況下，待刪除卡的第三匹配通用卡標識為第一類通用卡標識。在待刪除卡的卡類型為第二類型的情況下，綁定卡的第三匹配通用卡標識為第二類通用卡標識。

**【0156】** 第三映射關係的生命狀態為失效狀態，表示第三映射關係處於不可用狀態，無法被調用。在該卡被刪除又再次需要綁定的情況下，可將第三映射關係的生命狀態設置為有效狀態，從而快速實現再次綁卡。

**【0157】** 卡刪除流程可由用戶通過用戶終端的應用程式發起，也可由卡組織發起，在此並不限定，具體內容可參見上述實施例中的相關說明，在此不再贅述。

**【0158】** 為了進一步說明卡管理方法中涉及到的各個流程，下面以用戶終端包括安全元件，用戶終端安裝有應用程式以及功能控制項，伺服器包括應用程式的後臺伺服器、TSM 伺服器和 TSP 伺服器，以及卡類型包括借記卡和貸記卡為例進行說明。應用程式具體可為電子錢包應用程式。功能控制項為 TSM 伺服器對應的控制項。

**【0159】** 圖 14 為本發明實施例提供的初始化流程的一示例的流程圖。圖 14 省略了一些交互的流程文字說明，但在圖 14 中以箭頭示出這些交互。如圖 14 所示，初始化流程可包括步驟 S401 至步驟 S420。

**【0160】** 在步驟 S401 中，應用程式向功能控制項發起初始化請求。

**【0161】** 在步驟 S402 中，功能控制項將初始化請求向 TSM 伺服器發送。

**【0162】** 在步驟 S403 中，TSM 伺服器驗證應用程式的合法性。

**【0163】** TSM 伺服器向功能控制項返回應答消息，以通知功能控制項建立秘密頻道。

**【0164】** 在步驟 S404 中，在合法性驗證結果表徵應用程式的合法性驗證成功的情況下，建立功能控制項與安全元件之間秘密頻道，相當於建立 TSM 伺服器與安全元件之間秘密頻道。

**【0165】** 安全元件向功能控制項返回應答消息，以通知功能控制項秘密頻道建立成功。功能控制項向 TSM 伺服器發送驗證請求，以使 TSM 伺服器驗證安全元件中交易功能區域的合法性。

**【0166】** 在步驟 S405 中，TSM 伺服器驗證安全元件中交易功能區域的合

法性。

**【0167】** 在步驟 S406 中，在合法性驗證結果表徵交易功能區域的合法性驗證成功的情況下，將交易功能區域的區域初始金鑰和為安全元件分配的安全元件標識向功能控制項發送。

**【0168】** 在步驟 S407 中，功能控制項將區域初始金鑰和安全元件標識寫入安全元件。

**【0169】** 安全元件向功能控制項返回應答消息，功能控制項向 TSM 返回該應答消息，以通知 TSM 伺服器區域初始金鑰和安全元件標識寫入成功。

**【0170】** TSM 伺服器向功能控制項發送第一觸發消息，功能控制項向應用程式發送第一觸發消息，以通知應用程式可進程式資料包的下載。

**【0171】** 應用程式向功能控制項發送下載觸發消息，功能控制項向 TSM 伺服器發送下載觸發消息。該下載觸發下次用於觸發下載程式資料包和通用卡標識。通用卡標識可包括通用借記卡標識和通用貸記卡標識。可選的，該下載觸發還可觸發下載通用個人化資料。通用個人化資料可包括借記卡通用個人化資料和貸記卡通用個人化資料。

**【0172】** 在步驟 S408 中，TSM 伺服器將程式資料包向功能控制項發送。

**【0173】** 在步驟 S409 中，功能控制項將程式資料包寫入安全元件。

**【0174】** 安全元件向功能控制項返回應答消息，功能控制項向 TSM 伺服器返回應答消息，以通知 TSM 伺服器程式資料包寫入成功。

**【0175】** TSM 伺服器向功能控制項發送第二觸發消息，以觸發功能控制項觸發下載通用卡標識，或者觸發下載通用卡標識和通用個人化資料。本示例中以觸發下載通用卡標識、通用個人化資料和加密公開金鑰為例。功能控制項向 TSM 伺服器發送下載請求，以請求下載通用卡標識、通用個人化資料和加密公開金鑰。

**【0176】** 在步驟 S410 中，TSM 伺服器向功能控制項發送通用卡標識、通用個人化資料和加密公開金鑰。

**【0177】** 在步驟 S411 中，功能控制項向安全元件發送通用卡標識、通用個人化資料和加密公開金鑰。

**【0178】** 安全元件向功能控制項返回應答消息，功能控制項向 TSM 伺服

器返回應答消息，以通知 TSM 伺服器通用卡標識、通用個人化資料和加密公開金鑰寫入成功。

**【0179】** 在步驟 S412 中，TSM 伺服器建立安全元件標識、通用卡標識、通用個人化資料的映射關係。

**【0180】** TSM 伺服器與 TSP 伺服器進行交互，以使 TSP 伺服器建立安全元件標識、通用卡標識、通用個人化資料的映射關係。

**【0181】** 在步驟 S413 中，TSP 伺服器建立安全元件標識、通用卡標識、通用個人化資料的映射關係。

**【0182】** TSP 伺服器向 TSM 伺服器返回應答消息，TSM 伺服器向功能控制項返回應答消息，功能控制項向應用程式返回應答消息，以通知用戶終端映射關係建立完畢。

**【0183】** 在步驟 S414 中，應用程式獲取銀行卡的卡號。

**【0184】** 在步驟 S415 中，應用程式將卡號向功能控制項發送。

**【0185】** 功能控制項對卡號進行加密，將加密的卡號返回應用程式。應用程式將加密的卡號向後臺伺服器發送。後臺伺服器將加密的卡號向 TSM 伺服器發送。TSM 伺服器根據卡號，確定卡的類型和發卡行，將卡類型和發卡行回饋給後臺伺服器。後臺伺服器將卡的類型和發卡行向應用程式發送。

**【0186】** 在步驟 S416 中，應用程式根據卡類型，獲取卡認證資訊，如貸記卡的有效期、信用卡安全碼（即 CVN2）、所屬人手機號碼，或者，如借記卡的卡密碼、所屬人手機號碼等。

**【0187】** 應用程式將卡認證資訊傳輸至功能控制項。功能控制項對卡認證資訊加密，將加密的卡認證資訊返回應用程式。應用程式將加密的卡認證資訊向後臺伺服器發送。

**【0188】** 在步驟 S417 中，後臺伺服器向 TSM 伺服器發送卡認證資訊。

**【0189】** 在步驟 S418 中，TSM 伺服器向卡組織發送卡認證資訊，以使卡組織對該卡進行認證。

**【0190】** 在步驟 S419 中，TSM 伺服器接收卡組織發送的認證結果。

**【0191】** 在步驟 S420 中，在認證結果表徵認證成功的情況下，TSM 伺服器向後臺伺服器發送通知資訊，以通知後臺伺服器可開始卡綁定流程。

**【0192】** 圖 15 為本發明實施例提供的卡綁定流程的一示例的流程圖。圖 15 省略了一些交互的流程文字說明，但在圖 15 中以箭頭示出這些交互。如圖 15 所示，卡綁定流程可包括步驟 S501 至步驟 S518。

**【0193】** 在步驟 S501 中，後臺伺服器向應用程式發送卡綁定消息。

**【0194】** 在步驟 S502 中，應用程式向功能控制項發送卡綁定消息。

**【0195】** 在步驟 S503 中，功能控制項向 TSM 伺服器發送卡綁定消息。

**【0196】** 在步驟 S504 中，TSM 伺服器回應於卡綁定消息，向功能控制項發送利用加密私密金鑰加密的卡交易標識。

**【0197】** 在步驟 S505 中，功能控制項向安全元件發送加密的卡交易標識。

**【0198】** 在步驟 S506 中，利用加密公開金鑰對加密的卡交易標識解密，並存儲。

**【0199】** 安全元件向功能控制項發送應答消息，功能控制項向 TSM 伺服器發送應答消息，以通知 TSM 伺服器已將卡交易標識寫入安全元件。

**【0200】** 在步驟 S507 中，TSM 伺服器建立安全元件標識、第一匹配通用卡標識和卡交易標識的映射關係。

**【0201】** TSM 伺服器與 TSP 伺服器交互，以使 TSP 伺服器建立安全元件標識、第一匹配通用卡標識和卡交易標識的映射關係。

**【0202】** 在步驟 S508 中，TSP 伺服器建立安全元件標識、第一匹配通用卡標識和卡交易標識的映射關係。

**【0203】** TSP 伺服器向 TSM 伺服器發送應答消息，TSM 伺服器向功能控制項發送應答消息，功能控制項向應用程式發送應答消息，以通知應用程式映射關係建立完畢。

**【0204】** 在步驟 S509 中，應用程式向後臺伺服器發送驗證碼獲取請求消息。

**【0205】** 在步驟 S510 中，後臺伺服器向 TSM 伺服器發送驗證碼獲取請求消息。

**【0206】** 在步驟 S511 中，TSM 伺服器向卡組織發送驗證碼獲取請求消息。

**【0207】** 在步驟 S512 中，卡組織向 TSM 伺服器發送第一動態驗證碼。

**【0208】** 在步驟 S513 中，TSM 伺服器向後臺伺服器發送第一動態驗證碼。

**【0209】** 在步驟 S514 中，後臺伺服器向應用程式發送第一動態驗證碼。

**【0210】** 在步驟 S515 中，應用程式向後臺伺服器發送第二動態驗證碼。

**【0211】** 在步驟 S516 中，後臺伺服器向 TSM 伺服器發送第二動態驗證碼。

**【0212】** 在步驟 S517 中，TSM 伺服器向卡組織發送第二動態驗證碼，以使卡組織進行動態驗證碼驗證。

**【0213】** 卡組織向 TSM 伺服器發送驗證應答消息。

**【0214】** 在步驟 S518 中，在驗證應答消息表徵驗證成功的情況下，TSM 伺服器根據驗證結果啟動映射關係。

**【0215】** TSM 伺服器向後臺伺服器發送驗證應答消息，後臺伺服器向應用程式發送驗證應答消息。

**【0216】** 圖 16 為本發明實施例提供的卡刪除流程的一示例的流程圖。圖 16 省略了一些交互的流程文字說明，但在圖 16 中以箭頭示出這些交互。如圖 16 所示，卡刪除流程可包括步驟 S601 至步驟 S608。

**【0217】** 在步驟 S601 中，應用程式回應於用戶輸入，向後臺伺服器發送卡刪除申請消息。

**【0218】** 在步驟 S602 中，後臺伺服器向 TSM 伺服器發送卡刪除申請消息。

**【0219】** 在步驟 S603 中，TSM 伺服器向後臺伺服器發送卡刪除消息。

**【0220】** 在步驟 S604 中，後臺伺服器向功能控制項發送卡刪除消息。

**【0221】** 在步驟 S605 中，功能控制項向安全元件發送卡刪除消息。

**【0222】** 在步驟 S606 中，安全元件刪除卡的卡交易標識。

**【0223】** 安全元件向功能控制項發送應答消息，功能控制項向 TSM 伺服器發送應答消息，以通知 TSM 伺服器安全元件已刪除卡的卡交易標識。

**【0224】** 在步驟 S607 中，TSM 伺服器刪除包括該卡的卡交易標識的映射關係。

**【0225】** TSM 伺服器與 TSP 伺服器交互，以使 TSP 伺服器刪除包括該卡的卡交易標識的映射關係。

**【0226】** 在步驟 S608 中，TSP 伺服器刪除包括該卡的卡交易標識的映射關係。

**【0227】** TSP 伺服器向 TSM 伺服器發送應答消息，以通知 TSM 伺服器

TSP 伺服器已刪除該映射關係。TSM 伺服器與卡組織交互，以使卡組織刪除包括該卡的卡交易標識的映射關係。卡組織刪除包括該卡的卡交易標識的映射關係後向 TSM 伺服器發送應答消息，TSM 伺服器向後臺伺服器發送應答消息，後臺伺服器向應用程式發送應答消息，以通知用戶刪卡成功。

**【0228】** 圖 17 為本發明實施例提供的卡刪除流程的另一示例的流程圖。圖 17 省略了一些交互的流程文字說明，但在圖 17 中以箭頭示出這些交互。如圖 17 所示，卡刪除流程可包括步驟 S701 至步驟 S705。

**【0229】** 在步驟 S701 中，TSM 伺服器回應於卡組織的卡刪除請求消息，刪除包括卡刪除請求消息指示刪除的卡的卡交易標識的映射關係。

**【0230】** TSM 伺服器與 TSP 伺服器交互，以使 TSP 伺服器刪除包括該卡的卡交易標識的映射關係。

**【0231】** 在步驟 S702 中，TSP 伺服器刪除包括該卡的卡交易標識的映射關係。

**【0232】** TSP 伺服器向 TSM 伺服器發送應答消息，以通知 TSM 伺服器 TSP 伺服器已刪除包括該卡的卡交易標識的映射關係。TSM 伺服器向卡組織發送應答消息，以通知卡組織 TSM 伺服器和 TSP 伺服器均已刪除包括該卡的卡交易標識的映射關係。

**【0233】** 在步驟 S703 中，TSM 伺服器向功能控制項發送卡刪除消息。

**【0234】** 在步驟 S704 中，功能控制項向安全元件發送卡刪除消息。

**【0235】** 在步驟 S705 中，回應於卡刪除消息，安全元件刪除該卡的卡交易標識。

**【0236】** 安全元件向功能控制項發送應答消息，功能控制項向 TSM 伺服器發送應答消息，以通知 TSM 伺服器安全元件已刪除該卡的卡交易標識。

**【0237】** 本發明第三方面提供一種用戶終端。該用戶終端具有安全元件。安全元件存儲有第一類通用卡實例和第二類通用卡實例。第一類通用卡實例包括第一類通用卡標識和第一類通用個人化資料。第二類通用卡實例包括第二類通用卡標識和第二類通用個人化資料。第一類通用卡實例用於用戶終端進行卡類型為第一類型的卡的交易驗證。第二類通用卡實例用於用戶終端進行卡類型為第二類型的卡的交易驗證。

**【0238】** 圖 18 為本發明第三方面提供的用戶終端的一實施例的結構示意圖。如圖 18 所示，該用戶終端 800 可包括發送模組 801、接收模組 802 和處理模組 803。

**【0239】** 發送模組 801 可用于向伺服器發送卡綁定消息，以使伺服器為綁定卡分配卡交易標識，並建立第一映射關係。

**【0240】** 卡綁定消息包括安全元件標識和綁定卡認證資訊。綁定卡認證資訊包括綁定卡的卡認證資訊。第一映射關係包括安全元件標識、第一匹配通用卡標識和綁定卡的卡交易標識的映射關係。第一匹配通用卡標識為與綁定卡的卡類型匹配的第一類通用卡標識或第二類通用卡標識。

**【0241】** 接收模組 802 可用於接收伺服器發送的綁定卡的卡交易標識。

**【0242】** 處理模組 803 可用於將綁定卡的卡交易標識存儲至安全元件。

**【0243】** 第一匹配通用卡實例用於綁定卡的交易驗證。第一匹配通用卡實例包括第一匹配通用卡標識。

**【0244】** 在本發明實施例中，用戶終端的安全元件中存儲有第一類通用卡實例和第二類通用卡實例。用戶終端通過向伺服器發送卡綁定消息，使伺服器為綁定卡分配卡交易標識，並建立安全元件標識、第一匹配通用卡標識和分配的卡交易標識的映射關係。用戶終端自身可利用綁定卡對應的第一匹配通用卡實例進行交易驗證，伺服器利用確定的第一匹配通用卡實例進行交易驗證。第一匹配通用卡實例為與綁定卡的卡類型匹配的第一類通用卡實例或第二類通用卡實例。即利用第一類通用卡實例或第二類通用卡實例即可完成交易驗證。在綁定卡的過程中，伺服器並不需要為每張卡分配對應的個人化資料，因此不需要在每次綁卡的過程中下載個人化資料，從而避免頻繁地進行個人化資料的下載和存儲，降低了卡管理流程的繁瑣程度，簡化卡管理流程，還可提高卡綁定的速度，減少卡綁定所花費的時間。

**【0245】** 在一些示例中，在用戶終端初次進行卡綁定的情況下，上述發送模組 801 還可用於向伺服器發送初始化請求消息。

**【0246】** 上述接收模組 802 還可用於與伺服器建立安全元件與伺服器之間的秘密頻道；以及用於通過秘密頻道接收伺服器下發的初始化資訊。初始化資訊包括安全元件標識、加密公開金鑰、第一類通用卡實例和第二類通用卡實例。

**【0247】** 處理模組 803 還可用於將初始化資訊存儲至安全元件。

**【0248】** 在一些示例中，在用戶終端非初次進行卡綁定的情況下，接收的綁定卡的卡交易標識為利用與加密公開金鑰成對的加密私密金鑰加密的卡交易標識。

**【0249】** 處理模組 803 可用于利用加密公開金鑰對綁定卡的卡交易標識解密，將解密後的綁定卡的卡交易標識存儲至安全元件內。

**【0250】** 在一些示例中，在安全元件未存儲有程式資料包的情況下，初始化資訊還包括程式資料包。

**【0251】** 在另一些示例中，在安全元件中存儲的程式資料包需要更新的情況下，初始化資訊還包括更新後的程式資料包。

**【0252】** 在一些示例中，不限於初始化過程，在安全元件中存儲的程式資料包需要更新的情況下，上述發送模組 801 還可用於向伺服器發送更新請求消息。更新請求消息用於請求更新後的程式資料包。

**【0253】** 在一些示例中，發送模組 801 還可用於向伺服器發送驗證碼獲取請求消息。

**【0254】** 接收模組 802 還可用於接收伺服器回應於驗證碼獲取請求消息回饋的第一動態驗證碼。

**【0255】** 接收模組 802 還可用於接收輸入的第二動態驗證碼。

**【0256】** 發送模組 801 還可用於向伺服器發送驗證碼請求消息，以使伺服器在第二動態驗證碼驗證成功的情況下啟動第一映射關係。

**【0257】** 驗證碼請求消息包括第二動態驗證碼。

**【0258】** 圖 19 為本發明第三方面提供的用戶終端的另一實施例的結構示意圖。圖 19 與圖 18 的不同之處在於，圖 19 所示的用戶終端 800 還可包括驗證模組 804 和輸出模組 805。

**【0259】** 驗證模組 804 可用於在利用綁定卡進行聯網交易的情況下，利用第一匹配通用卡實例進行交易驗證計算。

**【0260】** 輸出模組 805 可用於在利用綁定卡進行聯網交易的情況下，向交易設備提供第一交易驗證資訊，以通過交易設備使伺服器根據第一映射關係，利用與綁定卡的卡交易標識對應的第一匹配通用卡實例進行交易驗證計算。

**【0261】** 第一交易驗證資訊包括綁定卡的卡交易標識。第一匹配通用卡實例包括第一匹配通用卡標識。

**【0262】** 在用戶終端進行支付交易的情況下，用戶終端向交易設備提供第一交易驗證資訊，以使伺服器從交易設備獲取進行交易的綁定卡的卡交易標識，通過卡交易標識確定第一匹配通用卡實例。

**【0263】** 用戶終端與交易設備在聯網支付交易的情況下，用戶終端提供的第一交易驗證資訊包括用於交易的綁定卡的卡交易標識。第一交易驗證資訊可通過交易設備傳輸至伺服器，伺服器能夠根據卡交易標識識別出本次支付交易所使用的卡，使得收單方能夠區分不同的卡進行的支付交易。

**【0264】** 在另一些示例中，驗證模組 804 還可用於在利用綁定卡進行離線交易的情況下，利用第一匹配通用卡實例進行交易驗證計算。

**【0265】** 輸出模組 805 還可用於向交易設備提供第二交易驗證資訊，以使交易設備利用第一匹配通用卡實例進行交易驗證計算。

**【0266】** 第二交易驗證資訊包括第一匹配通用卡實例。

**【0267】** 在一些示例中，接收模組 802 還可用於接收默認卡設置輸入。

**【0268】** 默認卡設置輸入用於選定默認卡。

**【0269】** 發送模組 801 還可用於在聯網的情況下，向伺服器發送默認卡設置消息，以使伺服器將第二映射關係的使用狀態設置為預設使用狀態。

**【0270】** 默認卡設置消息包括默認卡的卡交易標識。第二映射關係包括安全元件標識、第二匹配通用卡標識和默認卡的卡交易標識的映射關係。第二匹配通用卡標識為與默認卡的卡類型匹配的第一類通用卡標識或第二類通用卡標識。

**【0271】** 接收模組 802 還可用於接收伺服器發送的默認卡應答消息。

**【0272】** 默認卡應答消息用於表徵第二映射關係的使用狀態已設置為預設使用狀態。

**【0273】** 處理模組 803 還可用於回應於默認卡應答消息，通過默認卡設置指令，將安全元件中默認卡的卡交易標識的使用狀態設置為預設使用狀態，將安全元件中與默認卡的卡交易標識對應的第二匹配通用卡實例的生命狀態設置為生效狀態。

**【0274】** 第二匹配通用卡實例為與默認卡的卡類型匹配的第一類通用卡實例或第二類通用卡實例。

**【0275】** 需要說明的是，在利用某張綁定卡進行交易支付的情況下，該綁定卡即為默認卡。

**【0276】** 在一些示例中，處理模組 803 還可用於回應於接收的卡刪除消息，在安全元件中刪除待刪除卡的卡交易標識，或將待刪除卡的卡交易標識的生命狀態設置為失效狀態。

**【0277】** 卡刪除消息用於指示待刪除卡。

**【0278】** 本發明第四方面提供一種伺服器。該伺服器存儲有用戶終端的第一類通用卡實例和第二類通用卡實例。第一類通用卡實例包括第一類通用卡標識和第一類通用個人化資料。第二類通用卡實例包括第二類通用卡標識和第二類通用個人化資料。第一類通用卡實例用於用戶終端進行卡類型為第一類型的卡的交易驗證。第二類通用卡實例用於用戶終端進行卡類型為第二類型的卡的交易驗證。

**【0279】** 圖 20 為本發明第四方面提供的伺服器的一實施例的結構示意圖。如圖 20 所示，該伺服器 900 可包括接收模組 901、處理模組 902 和發送模組 903。

**【0280】** 接收模組 901 可用於接收用戶終端發送的卡綁定消息。

**【0281】** 卡綁定消息包括安全元件標識和綁定卡認證資訊。綁定卡認證資訊包括綁定卡的卡認證資訊。

**【0282】** 處理模組 902 可用於回應於卡綁定消息，為綁定卡分配卡交易標識，並建立第一映射關係。

**【0283】** 第一映射關係包括安全元件標識、第一匹配通用卡標識和綁定卡的卡交易標識的映射關係。第一匹配通用卡標識為與綁定卡的卡類型匹配的第一類通用卡標識或第二類通用卡標識。

**【0284】** 發送模組 903 可用於向用戶終端發送綁定卡的卡交易標識。

**【0285】** 第一匹配通用卡實例用於綁定卡的交易驗證。第一匹配通用卡實例包括第一匹配通用卡標識。

**【0286】** 在本發明實施例中，伺服器回應於用戶終端發送的卡綁定消息，

為綁定卡分配卡交易標識，並建立安全元件標識、第一匹配通用卡標識和分配的該卡交易標識的第一映射關係。伺服器將為綁定卡分配的卡交易標識向用戶終端發送，以使用戶終端獲取該卡交易標識。伺服器利用第一匹配通用卡實例進行交易驗證計算，第一匹配通用卡實例包括第一匹配通用卡標識。對於用戶終端的應用程式綁定的卡類型相同的卡，用戶終端與伺服器利用相同的匹配通用卡實例進行交易驗證，因此伺服器不需要為每張卡單獨配置用於交易驗證的個人化資料，避免了每次卡綁定伺服器都需要將該卡對應的個人化資料傳輸給用戶終端的情況，降低了卡管理流程的繁瑣程度，簡化卡管理流程，還可提高卡綁定的速度，減少卡綁定所花費的時間。

**【0287】** 在一些示例中，接收模組 901 還可用於接收用戶終端發送的初始化請求消息。

**【0288】** 發送模組 903 還可用於回應於初始化請求消息，與用戶終端建立用戶終端中安全元件與伺服器之間的秘密頻道。

**【0289】** 發送模組 903 還可用於通過秘密頻道向安全元件下發初始化資訊。

**【0290】** 初始化資訊包括安全元件標識、加密公開金鑰、第一類通用卡實例和第二類通用卡實例。

**【0291】** 在一些示例中，在伺服器非初次接收到卡綁定消息的情況下，處理模組 902 還可用於利用與加密公開金鑰成對的加密私密金鑰對綁定卡的卡交易標識加密。

**【0292】** 發送模組 903 還可用於向用戶終端發送加密後的綁定卡的卡交易標識。

**【0293】** 在一些示例中，在安全元件未存儲有程式資料包的情況下，初始化資訊還包括程式資料包；

**【0294】** 在另一些示例中，在安全元件中存儲的程式資料包需要升級的情況下，初始化資訊還包括升級後的程式資料包。

**【0295】** 在一些示例中，不限於初始化過程，在安全元件中存儲的程式資料包需要更新的情況下，上述接收模組還可用於接收用戶終端發送的更新請求消息。

**【0296】** 上述發送模組 903 還可用於回應更新請求消息，向用戶終端下發

更新後的程式資料包。

**【0297】** 在一些示例中，接收模組 901 還可用於接收用戶終端發送的驗證碼獲取請求消息。

**【0298】** 發送模組 903 還可用於回應驗證碼獲取請求消息，向用戶終端回饋第一動態驗證碼。

**【0299】** 接收模組 901 還可用於接收用戶終端發送的驗證碼請求消息。

**【0300】** 驗證碼請求消息包括第二動態驗證碼。

**【0301】** 處理模組 902 還可用於在第二動態驗證碼驗證成功的情況下啟動第一映射關係。

**【0302】** 圖 21 為本發明第四方面提供的伺服器的另一實施例的結構示意圖。圖 21 與圖 20 的不同之處在於，圖 21 所示的伺服器 900 還可包括驗證模組 904。

**【0303】** 上述接收模組 901 還可用於在利用綁定卡進行聯網交易的情況下，通過交易設備接收用戶終端提供的第一交易驗證資訊。

**【0304】** 第一交易驗證資訊包括綁定卡的卡交易標識。

**【0305】** 驗證模組 904 可用於根據第一映射關係，利用與綁定卡的卡交易標識對應的第一匹配通用卡實例進行交易驗證計算。

**【0306】** 在聯網交易的情況下，伺服器可通過交易設備接收到用戶終端設備提供的第一交易驗證資訊。第一驗證資訊包括綁定卡的卡交易標識。伺服器可根據該卡交易標識，確定第一映射關係中的第一匹配通用卡實例，從而利用第一匹配通用卡實例進行交易驗證計算。

**【0307】** 而且，用戶終端與交易設備在聯網支付交易的情況下，伺服器通過交易設備從用戶終端獲取的第一交易驗證資訊包括用於交易的綁定卡的卡交易標識。伺服器能夠根據該卡交易標識識別出本次支付交易所使用的卡，使得收單方能夠區分不同的卡進行的支付交易。

**【0308】** 在另一些示例中，處理模組 902 還可用於在用戶終端利用綁定卡與交易設備進行離線交易後，在聯網的情況下，獲取第一匹配通用卡實例，利用第一匹配通用卡實例進行交易驗證計算。

**【0309】** 在一些示例中，接收模組 901 還可用於在聯網的情況下，接收用

戶終端發送的默認卡設置消息。

**【0310】** 默認卡設置消息包括選定的默認卡的卡交易標識；

**【0311】** 處理模組 902 還可用於回應於默認卡設置消息，將第二映射關係的使用狀態設置為預設使用狀態。

**【0312】** 第二映射關係包括安全元件標識、第二匹配通用卡標識和默認卡的卡交易標識的映射關係；

**【0313】** 發送模組 903 還可用於向用戶終端發送默認卡應答消息，默認卡應答消息用於表徵第二映射關係的使用狀態已設置為預設使用狀態。

**【0314】** 在一些示例中，驗證模組 904 還可用於在用戶終端與交易設備進行離線交易後，在聯網的情況下，根據第二匹配通用卡實例進行交易驗證計算。

**【0315】** 第二匹配通用卡實例為與默認卡的卡類型匹配的第一類通用卡實例或第二類通用卡實例。

**【0316】** 在一些示例中，在利用某張綁定卡進行交易支付的情況下，該綁定卡即為默認卡。處理模組 902 還可用於在用戶終端與交易設備進行離線交易後，在聯網的情況下，確定使用狀態為預設使用狀態的第二映射關係；以及，用於利用第二映射關係中默認卡的卡交易標識進行結算。

**【0317】** 在一些示例中，接收模組 901 還可用於接收卡刪除請求消息。

**【0318】** 卡刪除請求消息用於指示待刪除卡。

**【0319】** 處理模組 902 還可用於回應於卡刪除請求消息，刪除第三映射關係，或者，將第三映射關係的生命狀態設置為失效狀態。

**【0320】** 第三映射關係包括安全元件標識、第三匹配通用卡標識與待刪除卡的卡交易標識的對應關係。第三匹配通用卡標識為與待刪除卡的卡類型匹配的第一類通用卡標識或第二類通用卡標識。

**【0321】** 本發明第五方面提供了一種用戶終端。圖 22 為本發明第五方面提供的用戶終端的一實施例的結構示意圖。如圖 22 所示，用戶終端 1000 包括記憶體 1001、處理器 1002 及存儲在記憶體 1001 上並可在處理器 1002 上運行的電腦程式。

**【0322】** 在一個示例中，上述處理器 1002 可以包括中央處理器（Central Processing Unit，CPU），或者特定應用積體電路（Application Specific

Integrated Circuit ，ASIC） ，或者可以被配置成實施本發明實施例的一個或多個積體電路。

**【0323】** 記憶體可包括唯讀記憶體（Read-Only Memory ，ROM） ，隨機存取記憶體（Random Access Memory ，RAM） ，磁片存儲介質設備，光存儲介質設備，快閃記憶體設備，電氣、光學或其他物理/有形的記憶體存放裝置。因此，通常，記憶體包括一個或多個編碼有包括電腦可執行指令的軟體的有形（非暫態）電腦可讀存儲介質（例如，記憶體設備） ，並且當該軟體被執行（例如，由一個或多個處理器）時，其可操作來執行參考根據本發明第一方面的卡管理方法所描述的操作。

**【0324】** 處理器 1002 通過讀取記憶體 1001 中存儲的可執行程式碼來運行與可執行程式碼對應的電腦程式，以用於實現上述實施例中第一方面的卡管理方法。

**【0325】** 在一個示例中，用戶終端 1000 還可包括通信介面 1003 和匯流排 1004。其中，如圖 22 所示，記憶體 1001、處理器 1002、通信介面 1003 通過匯流排 1004 連接並完成相互間的通信。

**【0326】** 通信介面 1003，主要用於實現本發明實施例中各模組、裝置、單元和/或設備之間的通信。也可通過通信介面 1003 接入輸入裝置和/或輸出設備。

**【0327】** 匯流排 1004 包括硬體、軟體或兩者，將用戶終端 1000 的部件彼此耦接在一起。舉例來說而非限制，匯流排 1004 可包括加速圖形埠（Accelerated Graphics Port ，AGP）或其他圖形匯流排、增強工業標準架構（Enhanced Industry Standard Architecture ，EISA）匯流排、前側匯流排（Front Side Bus ，FSB）、超傳送標準（Hyper Transport ，HT）互連、工業標準架構（Industry Standard Architecture ，ISA）匯流排、無限頻寬互連、低引腳數（Low pin count ，LPC）匯流排、記憶體匯流排、微通道架構（Micro Channel Architecture ，MCA）匯流排、外部連結標準（Peripheral Component Interconnect ，PCI）匯流排、快速週邊組件互連（PCI-Express ，PCI-E）匯流排、序列先進技術附件（Serial Advanced Technology Attachment ，SATA）匯流排、視電標準協會局部（Video Electronics Standards Association Local Bus ，VLB）匯流排或其他合適的匯流排或者兩個或更多個以上這些的組合。在合適的情況下，

匯流排 1004 可包括一個或多個匯流排。儘管本發明實施例描述和示出了特定的匯流排，但本發明考慮任何合適的匯流排或互連。

**【0328】** 本發明第六方面提供了一種伺服器。圖 23 為本發明第六方面提供的伺服器的一實施例的結構示意圖。如圖 23 所示，伺服器 1100 包括記憶體 1101、處理器 1102 及存儲在記憶體 1101 上並可在處理器 1102 上運行的電腦程式。

**【0329】** 在一個示例中，上述處理器 1102 可以包括中央處理器（Central Processing Unit，CPU），或者特定應用積體電路（Application Specific Integrated Circuit，ASIC），或者可以被配置成實施本發明實施例的一個或多個積體電路。

**【0330】** 記憶體可包括唯讀記憶體（Read-Only Memory，ROM），隨機存取記憶體（Random Access Memory，RAM），磁片存儲介質設備，光存儲介質設備，快閃記憶體設備，電氣、光學或其他物理/有形的記憶體存放裝置。因此，通常，記憶體包括一個或多個編碼有包括電腦可執行指令的軟體的有形（非暫態）電腦可讀存儲介質（例如，記憶體設備），並且當該軟體被執行（例如，由一個或多個處理器）時，其可操作來執行參考根據本發明第二方面的卡管理方法所描述的操作。

**【0331】** 處理器 1102 通過讀取記憶體 1101 中存儲的可執行程式碼來運行與可執行程式碼對應的電腦程式，以用於實現上述實施例中第二方面的卡管理方法。

**【0332】** 在一個示例中，伺服器 1100 還可包括通信介面 1103 和匯流排 1104。其中，如圖 23 所示，記憶體 1101、處理器 1102、通信介面 1103 通過匯流排 1104 連接並完成相互間的通信。

**【0333】** 通信介面 1103，主要用於實現本發明實施例中各模組、裝置、單元和/或設備之間的通信。也可通過通信介面 1103 接入輸入裝置和/或輸出設備。

**【0334】** 匯流排 1104 包括硬體、軟體或兩者，將伺服器 1100 的部件彼此耦接在一起。舉例來說而非限制，匯流排 1104 可包括加速圖形埠（Accelerated Graphics Port，AGP）或其他圖形匯流排、增強工業標準架構（Enhanced Industry Standard Architecture，EISA）匯流排、前側匯流排（Front Side Bus，

FSB)、超傳送標準(Hyper Transport, HT)互連、工業標準架構(Industrial Standard Architecture, ISA)匯流排、無限頻寬互連、低引腳數(Low pin count, LPC)匯流排、記憶體匯流排、微通道架構(Micro Channel Architecture, MCA)匯流排、外部連結標準(Peripheral Component Interconnect, PCI)匯流排、快速週邊組件互連(PCI-Express, PCI-X)匯流排、序列先進技術附件(Serial Advanced Technology Attachment, SATA)匯流排、視電標準協會局部(Video Electronics Standards Association Local Bus, VLB)匯流排或其他合適的匯流排或者兩個或更多個以上這些的組合。在合適的情況下，匯流排 1104 可包括一個或多個匯流排。儘管本發明實施例描述和示出了特定的匯流排，但本發明考慮任何合適的匯流排或互連。

**【0335】** 本發明第七方面還提供了一種卡管理系統。該卡管理系統可包括上述實施例中的用戶終端和伺服器，具體內容可參見上述實施例中的相關說明，在此不再贅述。

**【0336】** 本發明第八方面還提供一種電腦存儲介質，該電腦存儲介質上存儲有電腦程式，該電腦程式被處理器執行時可實現上述實施例中的卡管理方法，且能達到相同的技術效果，為避免重複，這裡不再贅述。其中，上述電腦存儲介質可包括非暫態電腦可讀存儲介質，如唯讀記憶體(Read-Only Memory, 簡稱 ROM)、隨機存取記憶體(Random Access Memory, 簡稱 RAM)、磁碟或者光碟等，在此並不限定。

**【0337】** 需要明確的是，本說明書中的各個實施例均採用遞進的方式描述，各個實施例之間相同或相似的部分互相參見即可，每個實施例重點說明的都是與其他實施例的不同之處。對於交換設備實施例、伺服器實施例、電腦存儲介質實施例而言，相關之處可以參見方法實施例的說明部分。本發明並不局限於上文所描述並在圖中示出的特定步驟和結構。本領域的技術人員可以在領會本發明的精神之後，作出各種改變、修改和添加，或者改變步驟之間的順序。並且，為了簡明起見，這裡省略對已知方法技術的詳細描述。

**【0338】** 上面參考根據本發明的實施例的方法、裝置(系統)和電腦程式產品的流程圖和/或框圖描述了本發明的各方面。應當理解，流程圖和/或框圖中的每個方框以及流程圖和/或框圖中各方框的組合可以由電腦程式指令實現。

這些電腦程式指令可被提供給通用電腦、專用電腦、或其它可程式設計資料處理裝置的處理器，以產生一種機器，使得經由電腦或其它可程式設計資料處理裝置的處理器執行的這些指令使能對流程圖和/或框圖的一個或多個方框中指定的功能/動作的實現。這種處理器可以是但不限於是通用處理器、專用處理器、特殊應用處理器或者現場可程式設計邏輯電路。還可理解，框圖和/或流程圖中的每個方框以及框圖和/或流程圖中的方框的組合，也可以由執行指定的功能或動作的專用硬體來實現，或可由專用硬體和電腦指令的組合來實現。

**【0339】** 本領域技術人員應能理解，上述實施例均是示例性而非限制性的。在不同實施例中出現的不同技術特徵可以進行組合，以取得有益效果。本領域技術人員在研究圖式、說明書及專利請求範圍的基礎上，應能理解並實現所揭示的實施例的其他變化的實施例。在專利請求範圍中，術語“包括”並不排除其他裝置或步驟；數量詞“一個”不排除多個；術語“第一”、“第二”用於標示名稱而非用於表示任何特定的順序。請求項中的任何圖式標記均不應被理解為對保護範圍的限制。請求項中出現的多個部分的功能可以由一個單獨的硬體或軟體模組來實現。某些技術特徵出現在不同的從屬請求項中並不意味著不能將這些技術特徵進行組合以取得有益效果。本發明公開了一種卡管理方法、用戶終端、伺服器、系統及存儲介質，屬於資料處理領域。用戶終端的安全元件存儲有第一類通用卡實例和第二類通用卡實例，第一匹配通用卡實例用於綁定卡的交易驗證，第一匹配通用卡實例包括第一匹配通用卡標識，第一匹配通用卡標識為與綁定卡的卡類型匹配的第一類通用卡標識或第二類通用卡標識。該方法包括：向伺服器發送卡綁定消息，卡綁定消息包括安全元件標識和綁定卡認證資訊，以使伺服器為綁定卡分配卡交易標識，並建立第一映射關係；接收伺服器發送的綁定卡的卡交易標識；將綁定卡的卡交易標識存儲至安全元件。根據本發明實施例，能夠降低卡管理流程的繁瑣程度。

### **【符號說明】**

#### **【0340】**

1000：用戶終端

1001：記憶體

1002：處理器

1003：通信介面  
1004：匯流排  
11：用戶終端  
1100：伺服器  
1101：記憶體  
1102：處理器  
1103：通信介面  
1104：匯流排  
12：伺服器  
121：管理伺服器  
122：後臺伺服器  
1211：TSM 伺服器  
1212：TSP 伺服器  
800：用戶終端  
801：發送模組  
802：接收模組  
803：處理模組  
804：驗證模組  
805：輸出模組  
900：伺服器  
901：接收模組  
902：處理模組  
903：發送模組  
904：驗證模組  
C1,C2,C3,C4：銀行卡  
Data A：第一類通用個人化資料  
Data B：第二類通用個人化資料  
SEID 1,SEID 2：安全元件標識

S201,S202,S203,S204,S205,S206,S207,S208,S209,S210,S211,S212,S213,S214,S215,S216,S301,S302,S303,S304,S305,S306,S307,S308,S309,S310,S311,S312,S313,S314,S315,S401,S402,S403,S404,S405,S406,S407,S408,S409,S410,S411,S412,S413,S414,S415,S416,S417,S418,S419,S420,S501,S502,S503,S504,S505,S506,S507,S508,S509,S510,S511,S512,S513,S514,S515,S516,S517,S518,S601,S602,S603,S604,S605,S606,S607,S701,S702,S703,S704,S705 : 步驟

Token A : 第一類通用卡標識

Token B : 第二類通用卡標識

Token C, Token D, Token E,Token F : 卡標識

Token 1,Token 2,Token 3,Token 4, Token 5,Token 6 : 交易標識

UE1,UE2,UE3 : 用戶終端

## 申請專利範圍

**【請求項1】** 一種卡管理方法，其特徵在於，應用於用戶終端，所述用戶終端包括安全元件，所述安全元件存儲有第一類通用卡實例和第二類通用卡實例，所述第一類通用卡實例包括第一類通用卡標識和第一類通用個人化資料，所述第二類通用卡實例包括第二類通用卡標識和第二類通用個人化資料，所述第一類通用卡實例用於所述用戶終端進行卡類型為第一類型的卡的交易驗證，所述第二類通用卡實例用於所述用戶終端進行卡類型為第二類型的卡的交易驗證；

所述方法包括：

向伺服器發送卡綁定消息，所述卡綁定消息包括所述安全元件的安全元件標識和綁定卡的卡認證資訊，以使所述伺服器為所述綁定卡分配卡交易標識，並建立第一映射關係，所述第一映射關係包括所述安全元件標識、第一匹配通用卡標識和所述綁定卡的卡交易標識的映射關係，所述第一匹配通用卡標識為與所述綁定卡的卡類型匹配的所述第一類通用卡標識或所述第二類通用卡標識；

接收所述伺服器發送的所述綁定卡的卡交易標識；

將所述綁定卡的卡交易標識存儲至所述安全元件，第一匹配通用卡實例用於所述綁定卡的交易驗證，所述第一匹配通用卡實例包括所述第一匹配通用卡標識，所述第一匹配通用卡實例為與所述綁定卡的卡類型匹配的所述第一類通用卡實例或所述第二類通用卡實例。

**【請求項2】** 如請求項 1 所述的方法，其中，還包括：

在利用所述綁定卡進行聯網交易的情況下，利用所述第一匹配通用卡實例進行交易驗證計算，向交易設備提供第一交易驗證資訊，所述第一交易驗證資訊包括所述綁定卡的卡交易標識，以通過所述交易設備使所述伺服器根據所述第一映射關係，利用與所述綁定卡的卡交易標識對應的所述第一匹配通用卡實例進行交易驗證計算。

**【請求項3】** 如請求項 1 所述的方法，其中，還包括：

在利用所述綁定卡進行離線交易的情況下，利用所述第一匹配通用卡實例進行交易驗證計算，向交易設備提供第二交易驗證資訊，所述第二交易驗證資

訊包括所述第一匹配通用卡實例，以使所述交易設備利用所述第一匹配通用卡實例進行交易驗證計算。

**【請求項4】** 如請求項 1 所述的方法，其中，在所述用戶終端初次進行卡綁定的情況下，在所述向伺服器發送卡綁定消息之前，還包括：

向所述伺服器發送初始化請求消息；

與所述伺服器建立所述安全元件與所述伺服器之間的秘密頻道；

通過所述秘密頻道接收所述伺服器下發的初始化資訊，並將所述初始化資訊存儲至所述安全元件，所述初始化資訊包括所述安全元件標識、加密公開金鑰、所述第一類通用卡實例和所述第二類通用卡實例。

**【請求項5】** 如請求項 4 所述的方法，其中，在所述用戶終端非初次進行卡綁定的情況下，接收的所述綁定卡的卡交易標識為利用與所述加密公開金鑰成對的加密私密金鑰加密的卡交易標識，

所述將所述綁定卡的卡交易標識存儲至所述安全元件，包括：

在所述安全元件內利用所述加密公開金鑰對所述綁定卡的卡交易標識解密，存儲解密後的所述綁定卡的卡交易標識。

**【請求項6】** 如請求項 4 所述的方法，其中，

在所述安全元件未存儲有程式資料包的情況下，所述初始化資訊還包括程式資料包；

在所述安全元件中存儲的程式資料包需要更新的情況下，所述初始化資訊還包括升級後的程式資料包。

**【請求項7】** 如請求項 1 所述的方法，其中，還包括：

在所述安全元件中存儲的程式資料包需要更新的情況下，向所述伺服器發送更新請求消息，所述更新請求消息用於請求更新後的程式資料包。

**【請求項8】** 如請求項 1 所述的方法，其中，在所述將所述綁定卡的卡交易標識存儲至所述安全元件之後，還包括：

向所述伺服器發送驗證碼獲取請求消息；

接收所述伺服器回應於所述驗證碼獲取請求消息回饋的第一動態驗證碼；

接收輸入的第二動態驗證碼；

向所述伺服器發送驗證碼請求消息，所述驗證碼請求消息包括所述第二動

態驗證碼，以使所述伺服器在所述第二動態驗證碼驗證成功的情況下啟動所述第一映射關係。

**【請求項9】** 如請求項 1 所述的方法，其中，還包括：

接收默認卡設置輸入，所述默認卡設置輸入用於選定默認卡；

在聯網的情況下，向所述伺服器發送默認卡設置消息，所述默認卡設置消息包括所述默認卡的卡交易標識，以使所述伺服器將第二映射關係的使用狀態設置為預設使用狀態，所述第二映射關係包括所述安全元件標識、第二匹配通用卡標識和所述默認卡的卡交易標識的映射關係，所述第二匹配通用卡標識為與所述默認卡的卡類型匹配的所述第一類通用卡標識或所述第二類通用卡標識；

接收所述伺服器發送的默認卡應答消息，所述默認卡應答消息用於表徵所述第二映射關係的使用狀態已設置為預設使用狀態；

回應於所述默認卡應答消息，通過默認卡設置指令，將所述安全元件中所述默認卡的卡交易標識的使用狀態設置為預設使用狀態，將所述安全元件中與所述默認卡的卡交易標識對應的第二匹配通用卡實例的生命狀態設置為生效狀態，所述第二匹配通用卡實例為與所述默認卡的卡類型匹配的所述第一類通用卡實例或所述第二類通用卡實例。

**【請求項10】** 如請求項 1 所述的方法，其中，還包括：

回應於接收的卡刪除消息，在所述安全元件中刪除待刪除卡的卡交易標識，或將所述待刪除卡的卡交易標識的生命狀態設置為失效狀態，所述卡刪除消息用於指示所述待刪除卡。

**【請求項11】** 一種卡管理方法，其特徵在於，應用於伺服器，所述伺服器存儲有用戶終端的第一類通用卡實例和第二類通用卡實例，所述第一類通用卡實例包括第一類通用卡標識和第一類通用個人化資料，所述第二類通用卡實例包括第二類通用卡標識和第二類通用個人化資料，所述第一類通用卡實例用於所述用戶終端進行卡類型為第一類型的卡的交易驗證，所述第二類通用卡實例用於所述用戶終端進行卡類型為第二類型的卡的交易驗證；

所述方法包括：

接收所述用戶終端發送的卡綁定消息，所述卡綁定消息包括安全元件標識和綁定卡認證資訊，所述綁定卡認證資訊包括綁定卡的卡認證資訊；

回應於所述卡綁定消息，為所述綁定卡分配卡交易標識，並建立第一映射關係，所述第一映射關係包括所述安全元件標識、第一匹配通用卡標識和所述綁定卡的卡交易標識的映射關係，所述第一匹配通用卡標識為與所述綁定卡的卡類型匹配的所述第一類通用卡標識或所述第二類通用卡標識，第一匹配通用卡實例用於所述綁定卡的交易驗證，所述第一匹配通用卡實例包括所述第一匹配通用卡標識，所述第一匹配通用卡實例為與所述綁定卡的卡類型匹配的所述第一類通用卡實例或所述第二類通用卡實例；

向所述用戶終端發送所述綁定卡的卡交易標識。

**【請求項12】** 如請求項 11 所述的方法，其中，還包括：

在利用所述綁定卡進行聯網交易的情況下，通過交易設備接收所述用戶終端提供的第一交易驗證資訊，所述第一交易驗證資訊包括所述綁定卡的卡交易標識，根據所述第一映射關係，利用與所述綁定卡的卡交易標識對應的第一匹配通用卡實例進行交易驗證計算。

**【請求項13】** 如請求項 11 所述的方法，其中，還包括：

在所述用戶終端利用所述綁定卡與交易設備進行離線交易後，在聯網的情況下，獲取所述第一匹配通用卡實例，利用所述第一匹配通用卡實例進行交易驗證計算。

**【請求項14】** 如請求項 11 所述的方法，其中，在所述接收所述用戶終端發送的卡綁定消息之前，還包括：

接收所述用戶終端發送的初始化請求消息；

回應於所述初始化請求消息，與所述用戶終端建立所述用戶終端中安全元件與所述伺服器之間的秘密頻道；

通過所述秘密頻道向所述安全元件下發初始化資訊，所述初始化資訊包括所述安全元件標識、加密公開金鑰、所述第一類通用卡實例和所述第二類通用卡實例。

**【請求項15】** 如請求項 14 所述的方法，其中，在所述伺服器非初次接收到所述卡綁定消息的情況下，所述向所述用戶終端發送所述綁定卡的卡交易標識，包括：

利用與所述加密公開金鑰成對的加密私密金鑰對所述綁定卡的卡交易標識

加密；

向所述用戶終端發送加密後的所述綁定卡的卡交易標識。

【請求項16】 如請求項 14 所述的方法，其中，

在所述安全元件未存儲有程式資料包的情況下，所述初始化資訊還包括程式資料包；

在所述安全元件中存儲的程式資料包需要更新的情況下，所述初始化資訊還包括更新後的程式資料包。

【請求項17】 如請求項 11 所述的方法，其中，還包括：

在所述安全元件中存儲的程式資料包需要更新的情況下，接收所述用戶終端發送的更新請求消息；

回應所述更新請求消息，向所述用戶終端下發更新後的程式資料包。

【請求項18】 如請求項 11 所述的方法，其中，所述綁定卡分配卡交易標識，並建立第一映射關係之後，還包括：

接收所述用戶終端發送的驗證碼獲取請求消息；

回應所述驗證碼獲取請求消息，向所述用戶終端回饋第一動態驗證碼；

接收所述用戶終端發送的驗證碼請求消息，所述驗證碼請求消息包括第二動態驗證碼；

在所述第二動態驗證碼驗證成功的情況下啟動所述第一映射關係。

【請求項19】 如請求項 11 所述的方法，其中，還包括：

在聯網的情況下，接收所述用戶終端發送的默認卡設置消息，所述默認卡設置消息包括選定的默認卡的卡交易標識；

回應於所述默認卡設置消息，將第二映射關係的使用狀態設置為預設使用狀態，所述第二映射關係包括所述安全元件標識、第二匹配通用卡標識和所述默認卡的卡交易標識的映射關係；

向所述用戶終端發送默認卡應答消息，所述默認卡應答消息用於表徵所述第二映射關係的使用狀態已設置為預設使用狀態。

【請求項20】 如請求項 19 所述的方法，其中，還包括：

在所述用戶終端與交易設備進行離線交易後，在聯網的情況下，確定使用狀態為預設使用狀態的所述第二映射關係；

利用所述第二映射關係中所述默認卡的卡交易標識進行結算。

**【請求項21】** 如請求項 11 所述的方法，其中，還包括：

接收卡刪除請求消息，所述卡刪除請求消息用於指示待刪除卡；

回應於所述卡刪除請求消息，刪除第三映射關係，或者，將所述第三映射關係的生命狀態設置為失效狀態，所述第三映射關係包括所述安全元件標識、第三匹配通用卡標識與所述待刪除卡的卡交易標識的對應關係，所述第三匹配通用卡標識為與所述待刪除卡的卡類型匹配的所述第一類通用卡標識或所述第二類通用卡標識。

**【請求項22】** 一種用於卡管理的用戶終端，其特徵在於，所述用戶終端具有安全元件，所述安全元件存儲有第一類通用卡實例和第二類通用卡實例，所述第一類通用卡實例包括第一類通用卡標識和第一類通用個人化資料，所述第二類通用卡實例包括第二類通用卡標識和第二類通用個人化資料，所述第一類通用卡實例用於所述用戶終端進行卡類型為第一類型的卡的交易驗證，所述第二類通用卡實例用於所述用戶終端進行卡類型為第二類型的卡的交易驗證；

所述用戶終端包括：

發送模組，用於向伺服器發送卡綁定消息，所述卡綁定消息包括安全元件標識和綁定卡認證資訊，所述綁定卡認證資訊包括綁定卡的卡認證資訊，以使所述伺服器為所述綁定卡分配卡交易標識，並建立第一映射關係，所述第一映射關係包括所述安全元件標識、第一匹配通用卡標識和所述綁定卡的卡交易標識的映射關係，所述第一匹配通用卡標識為與所述綁定卡的卡類型匹配的所述第一類通用卡標識或所述第二類通用卡標識，第一匹配通用卡實例用於所述綁定卡的交易驗證，所述第一匹配通用卡實例包括所述第一匹配通用卡標識，所述第一匹配通用卡實例為與所述綁定卡的卡類型匹配的所述第一類通用卡實例或所述第二類通用卡實例；

接收模組，用於接收所述伺服器發送的所述綁定卡的卡交易標識；

處理模組，用於將所述綁定卡的卡交易標識存儲至所述安全元件。

**【請求項23】** 一種用於卡管理的伺服器，其特徵在於，所述伺服器存儲有用戶終端的第一類通用卡實例和第二類通用卡實例，所述第一類通用卡實例包括第一類通用卡標識和第一類通用個人化資料，所述第二類通用卡實例包括第

二類通用卡標識和第二類通用個人化資料，所述第一類通用卡實例用於所述用戶終端進行卡類型為第一類型的卡的交易驗證，所述第二類通用卡實例用於所述用戶終端進行卡類型為第二類型的卡的交易驗證；

所述伺服器包括：

接收模組，用於接收所述用戶終端發送的卡綁定消息，所述卡綁定消息包括安全元件標識和綁定卡認證資訊，所述綁定卡認證資訊包括綁定卡的卡認證資訊；

處理模組，用於回應於所述卡綁定消息，為所述綁定卡分配卡交易標識，並建立第一映射關係，所述第一映射關係包括所述安全元件標識、第一匹配通用卡標識和所述綁定卡的卡交易標識的映射關係，所述第一匹配通用卡標識為與所述綁定卡的卡類型匹配的所述第一類通用卡標識或所述第二類通用卡標識，第一匹配通用卡實例用於所述綁定卡的交易驗證，所述第一匹配通用卡實例包括所述第一匹配通用卡標識，所述第一匹配通用卡實例為與所述綁定卡的卡類型匹配的所述第一類通用卡實例或所述第二類通用卡實例；

發送模組，用於向所述用戶終端發送所述綁定卡的卡交易標識。

**【請求項24】** 一種用於卡管理的用戶終端，其特徵在於，包括：處理器以及存儲有電腦程式指令的記憶體；

所述處理器執行所述電腦程式指令時實現如請求項 1 至 10 中任意一項所述的卡管理方法。

**【請求項25】** 一種用於卡管理的伺服器，其特徵在於，包括：處理器以及存儲有電腦程式指令的記憶體；

所述處理器執行所述電腦程式指令時實現如請求項 11 至 21 中任意一項所述的卡管理方法。

**【請求項26】** 一種卡管理系統，其特徵在於，包括如請求項 24 所述的用戶終端和如請求項 25 所述的伺服器。

**【請求項27】** 一種電腦存儲介質，其特徵在於，所述電腦存儲介質上存儲有電腦程式指令，所述電腦程式指令被處理器執行時實現如請求項 1 至 21 中任意一項所述的卡管理方法。

# 圖式

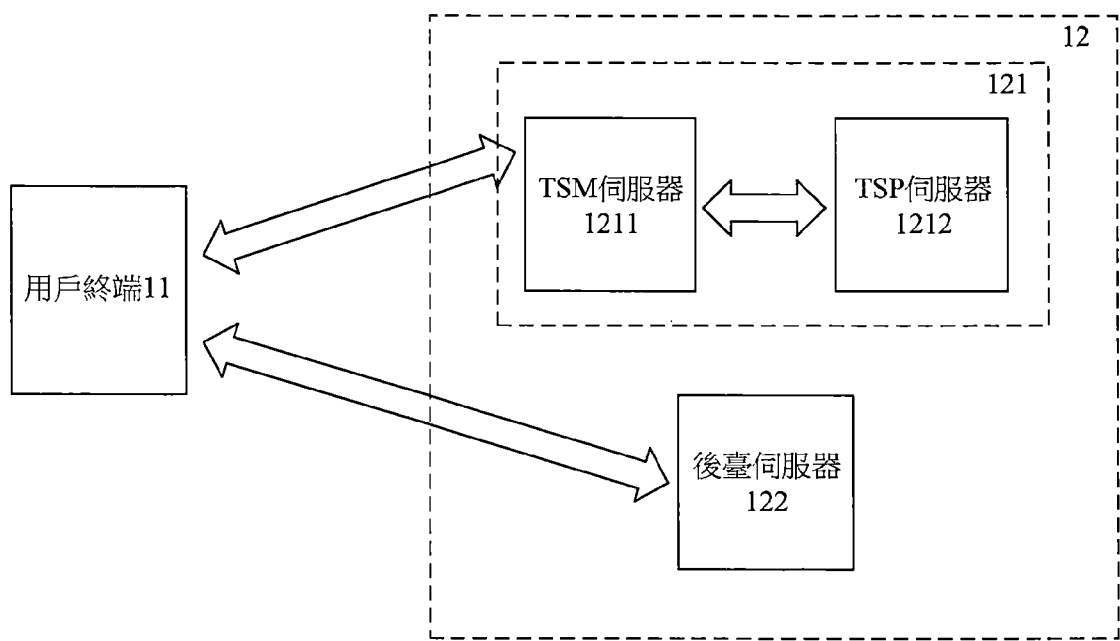


圖 1

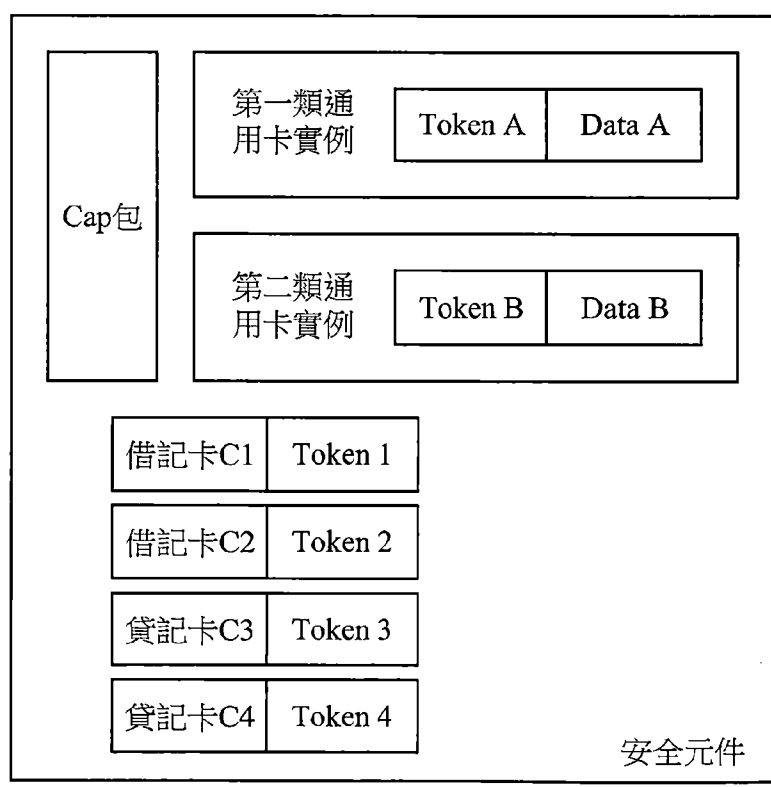


圖 2

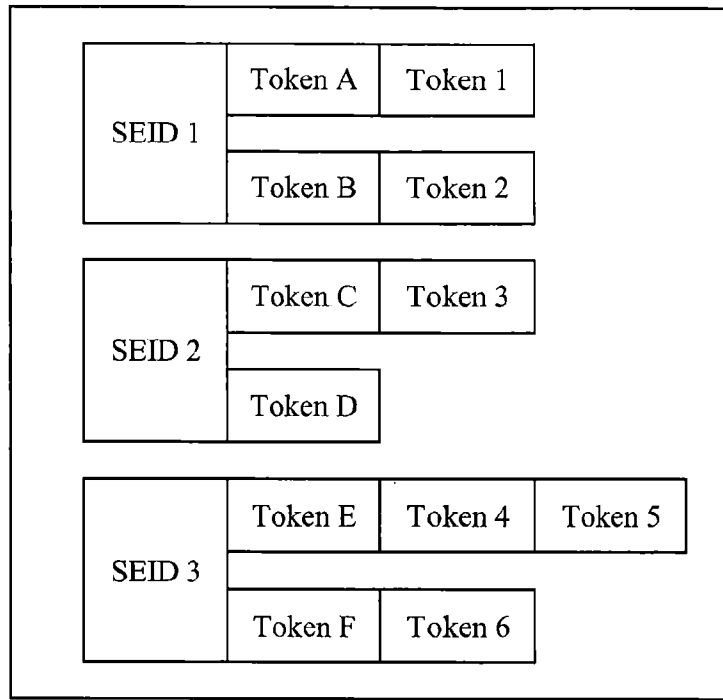


圖 3

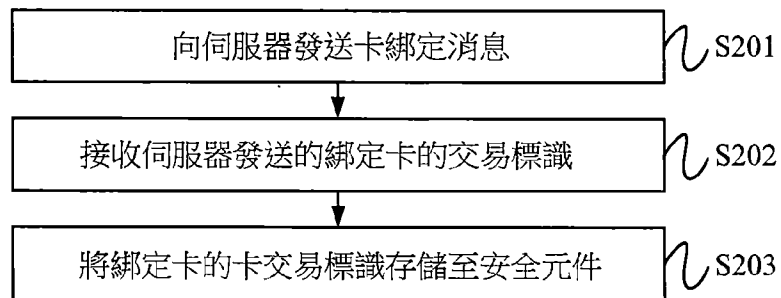


圖 4

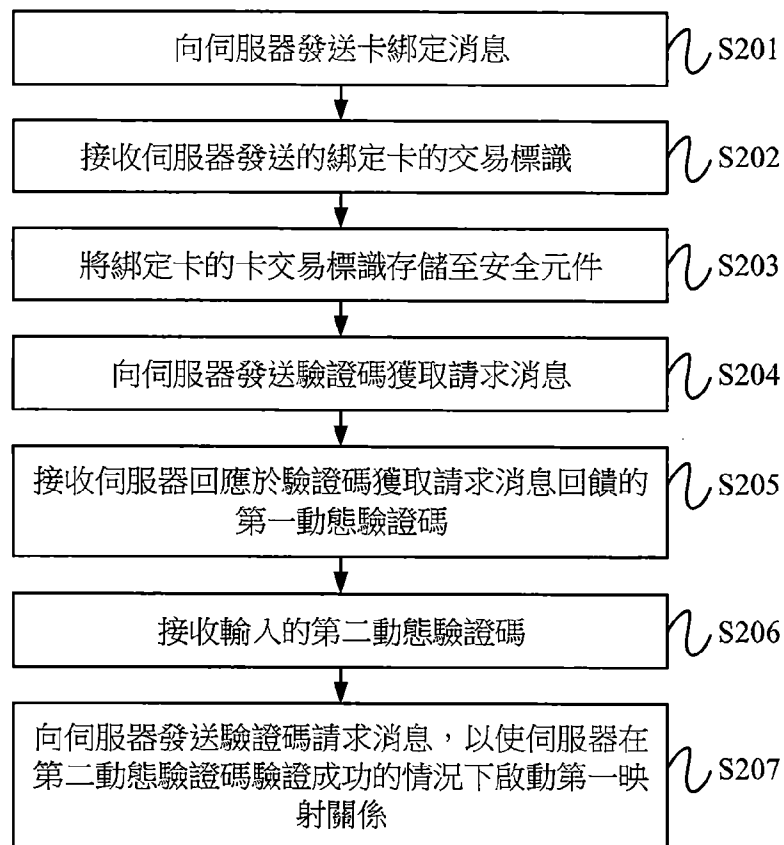


圖 5

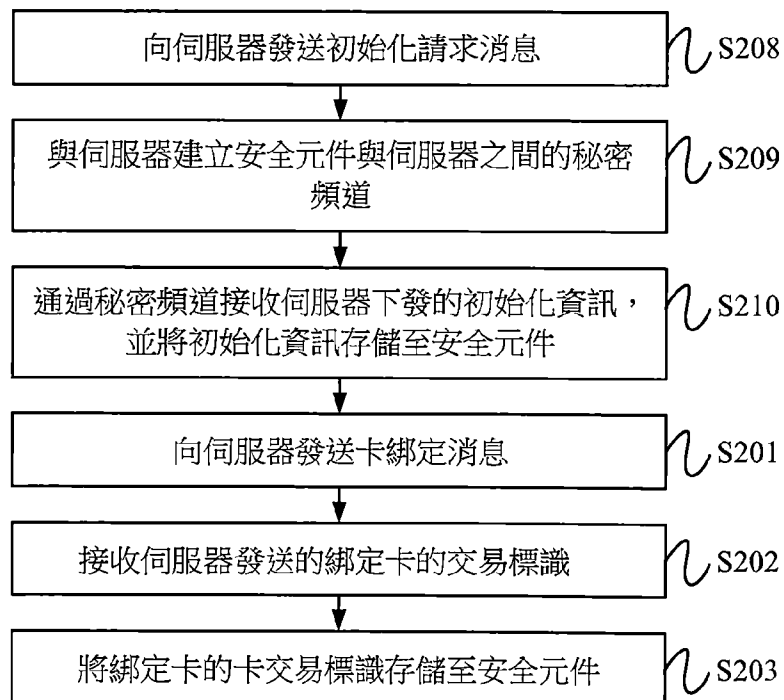


圖 6

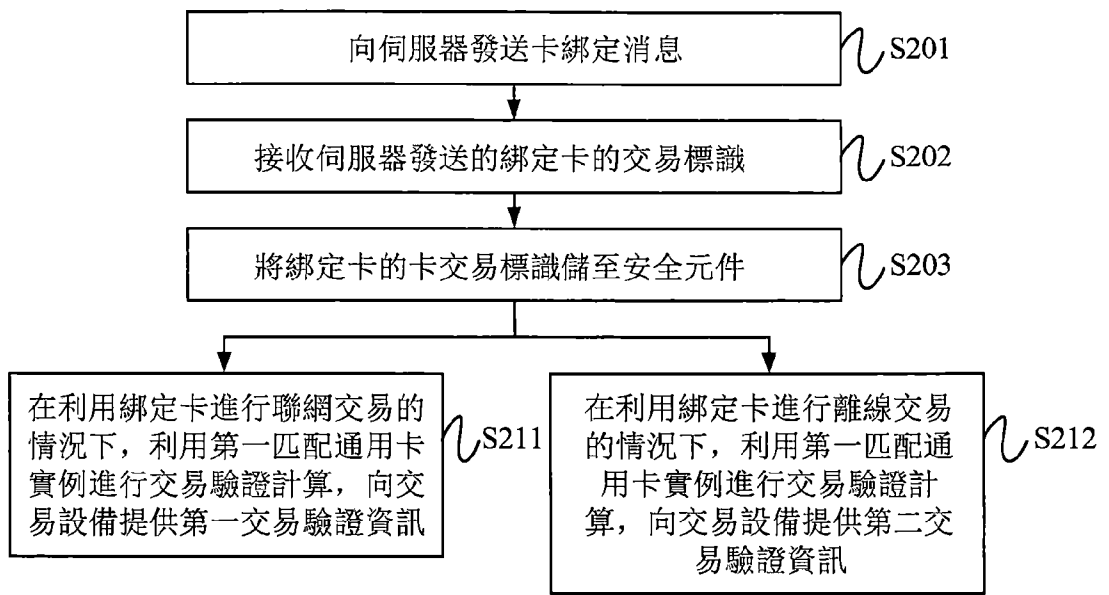


圖 7

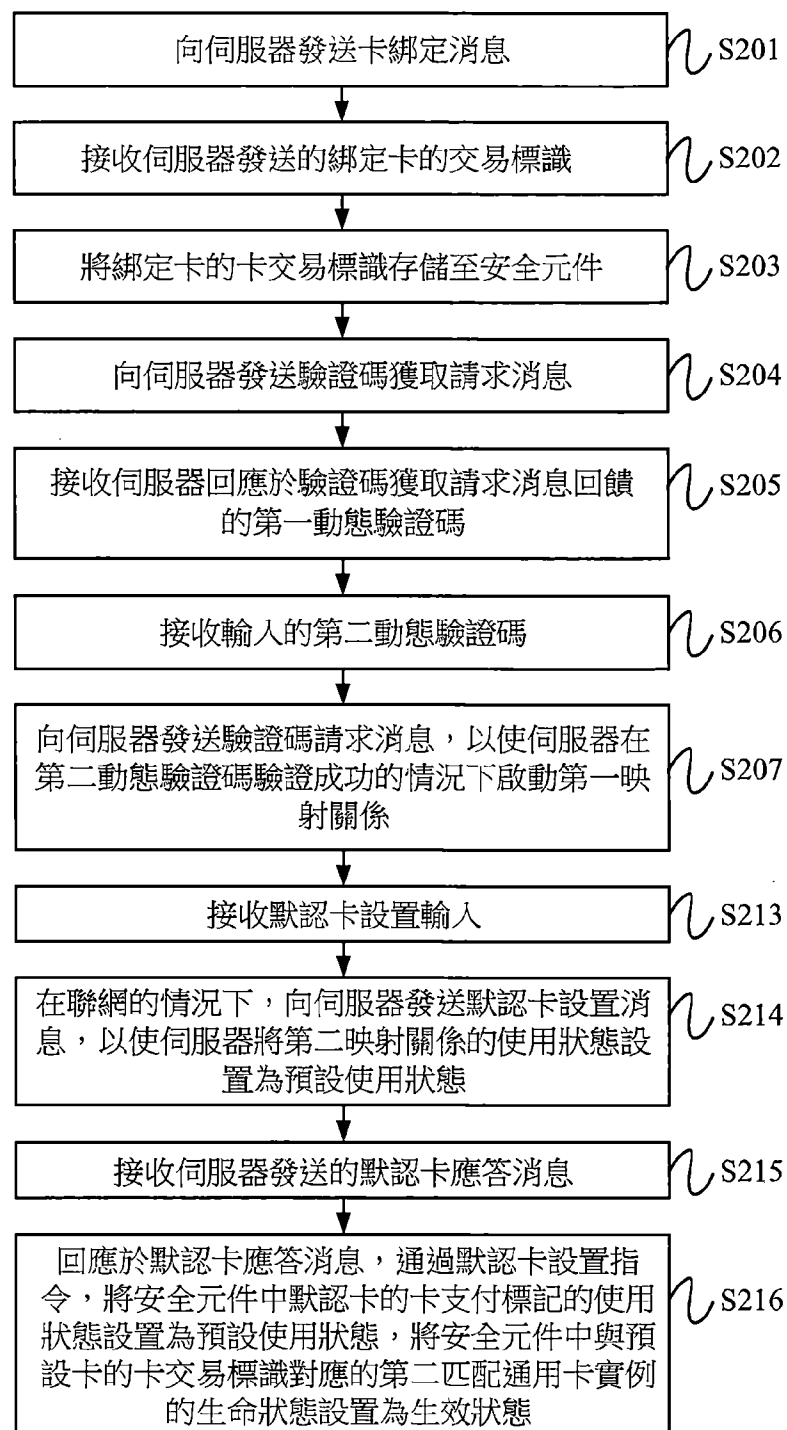


圖 8

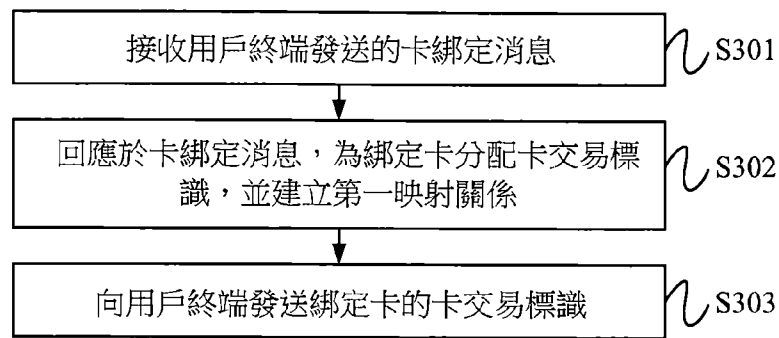


圖 9

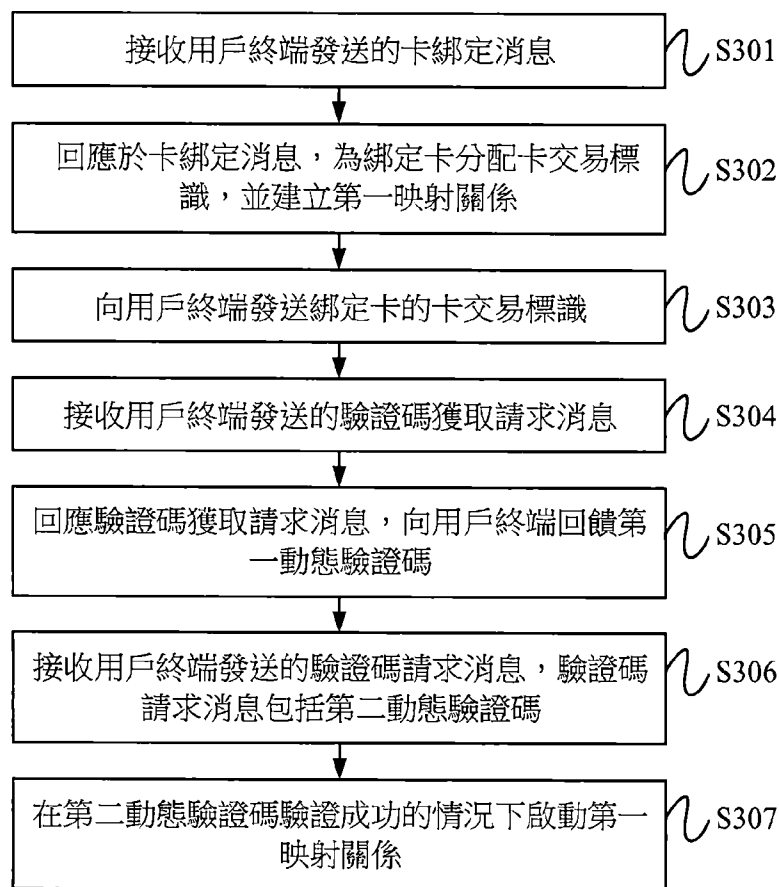


圖 10

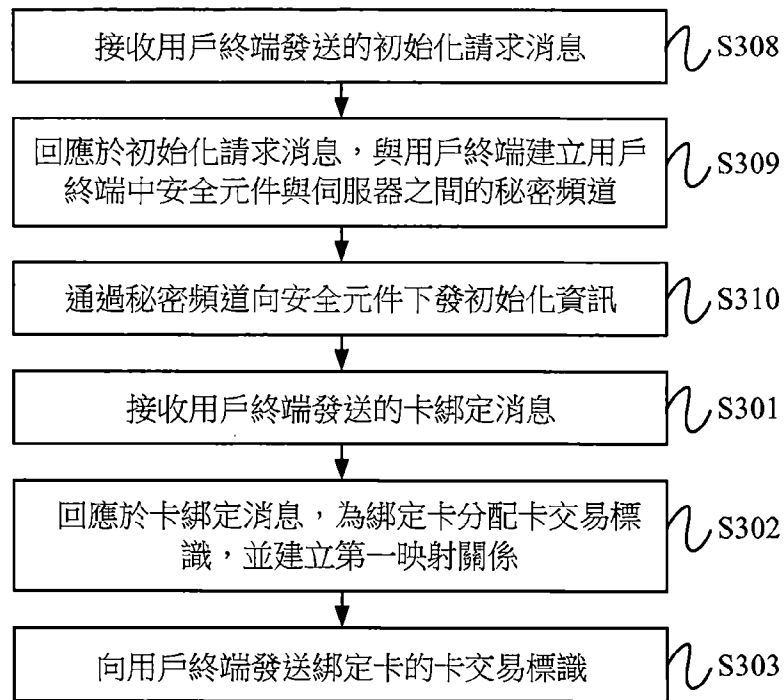


圖 11

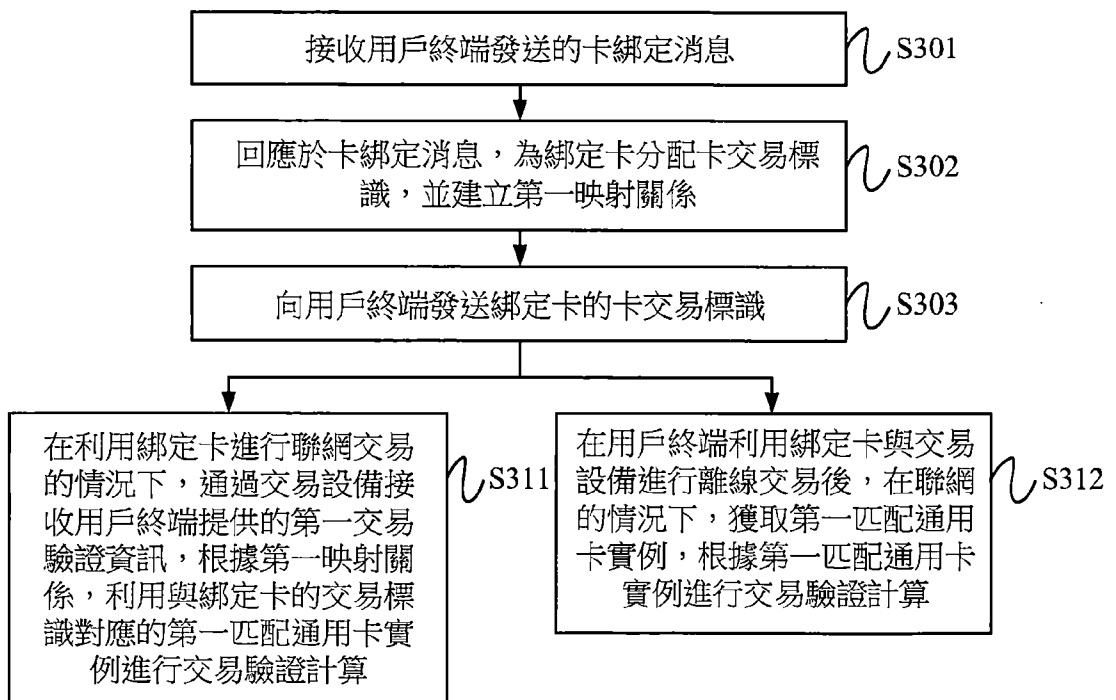


圖 12

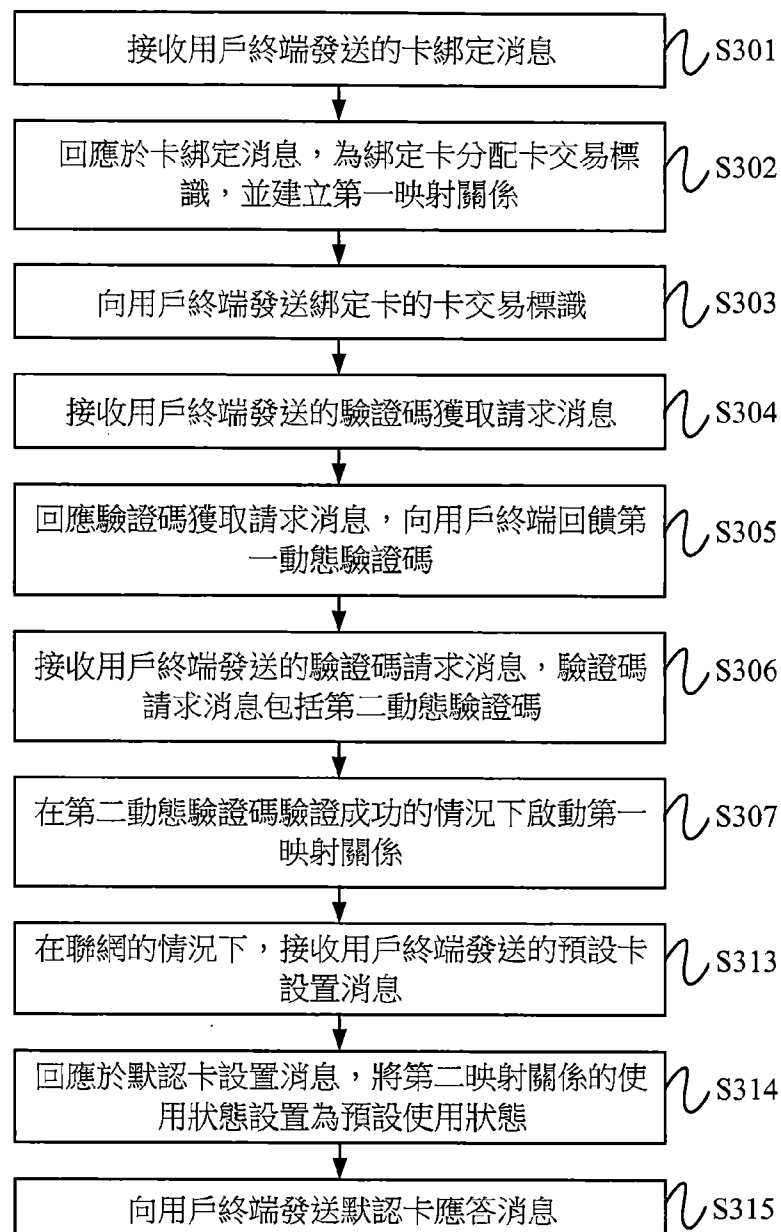


圖 13

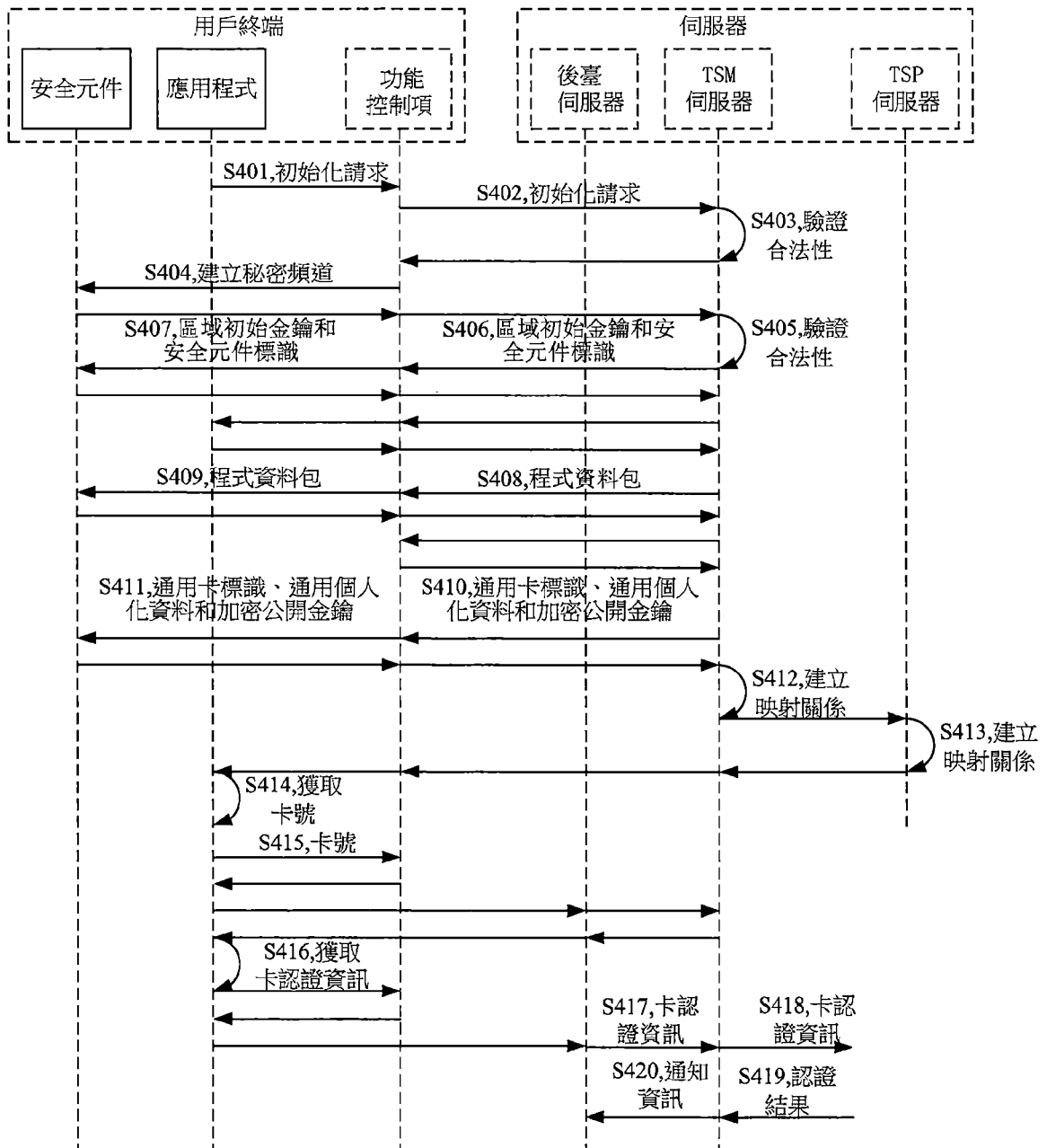


圖 14

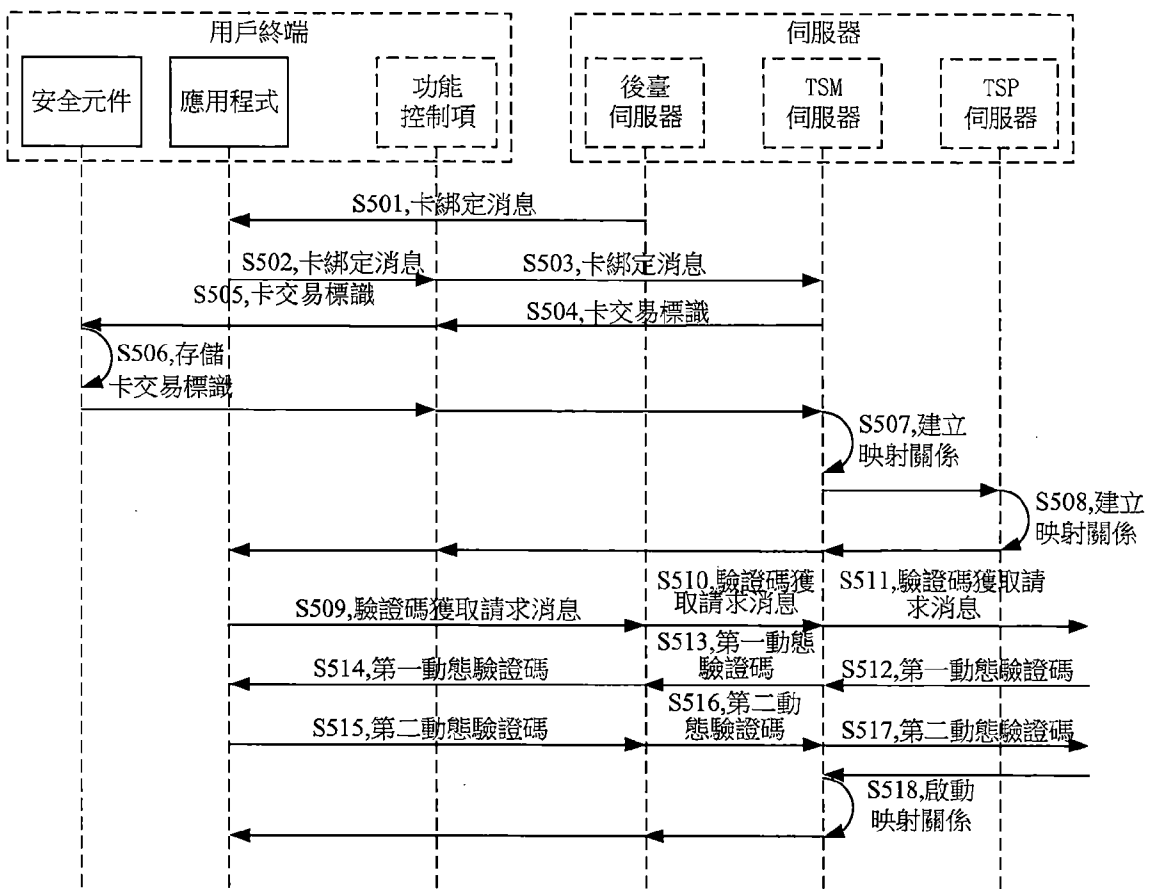


圖 15

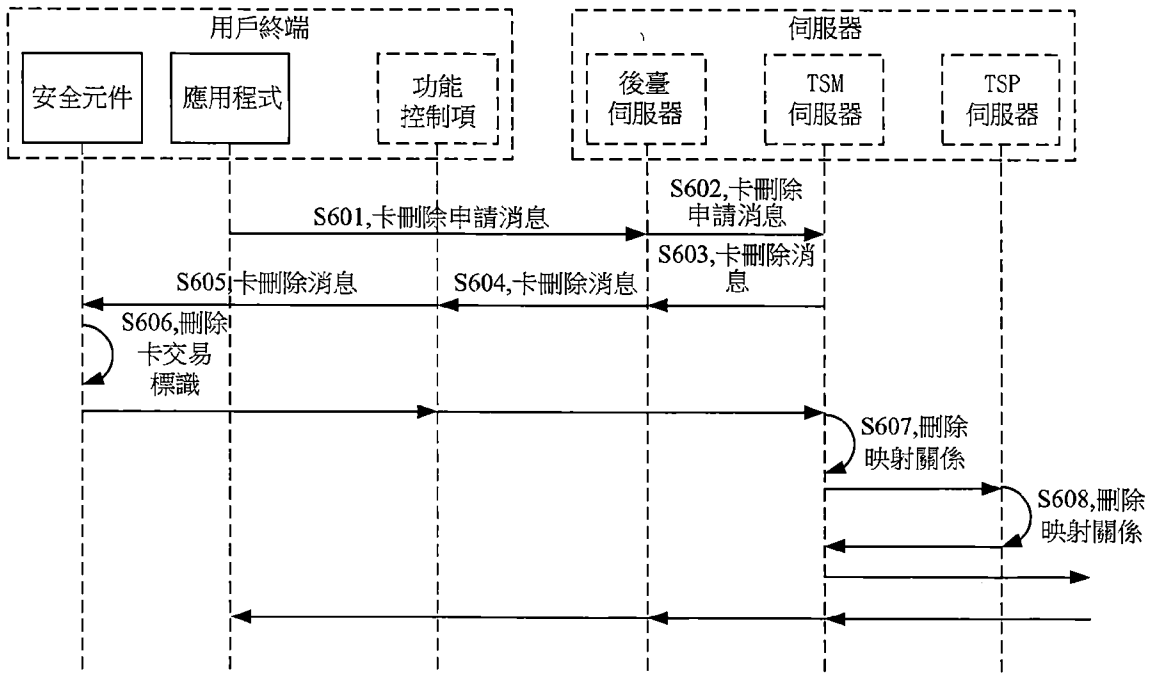


圖 16

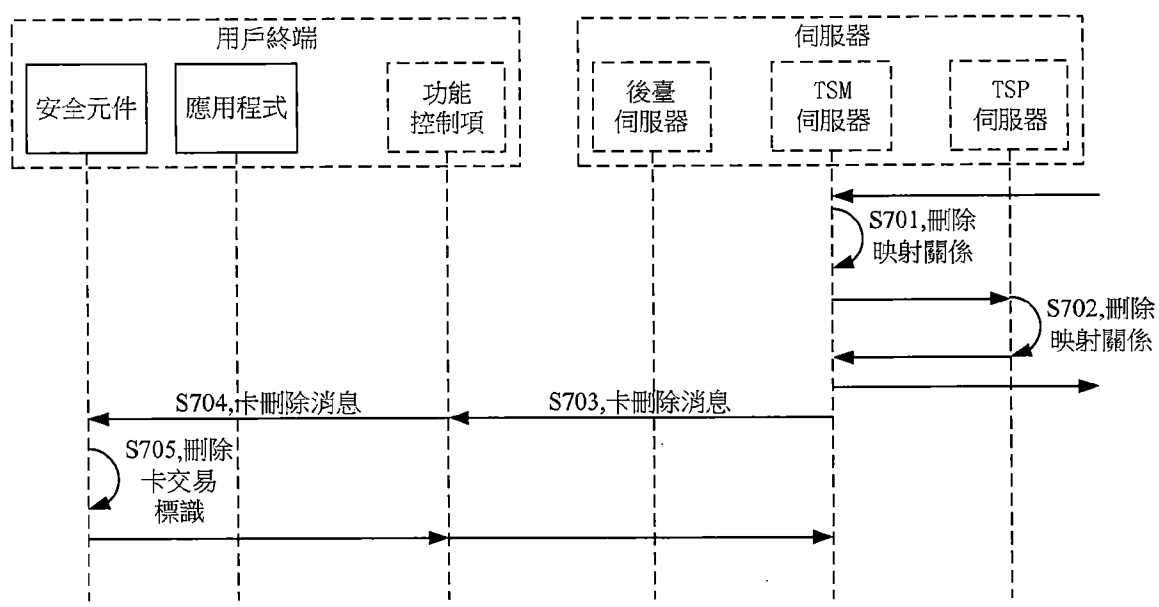


圖 17

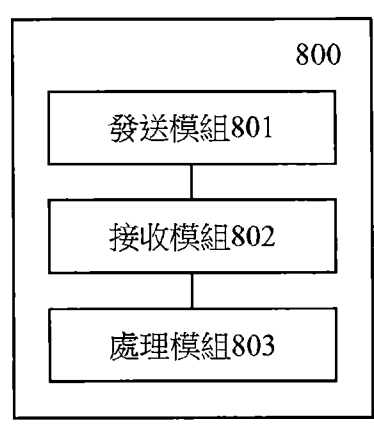


圖 18

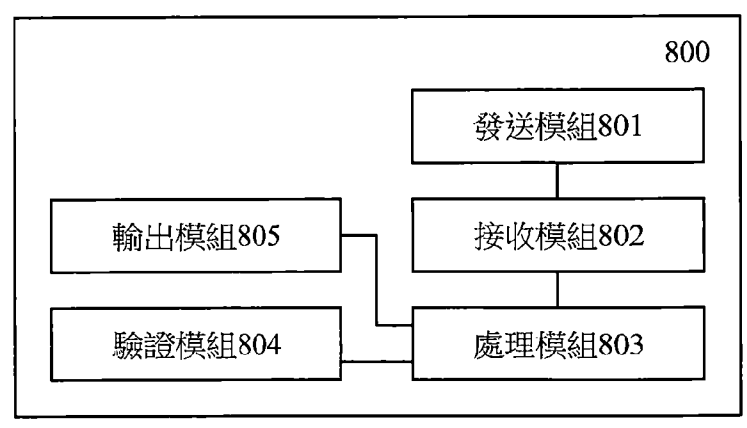


圖 19

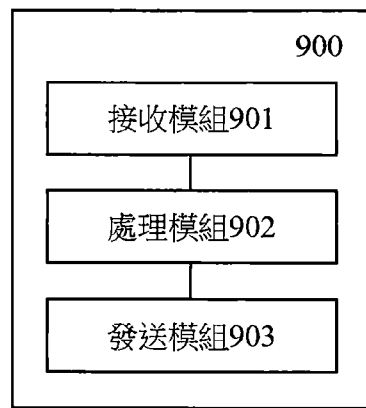


圖 20

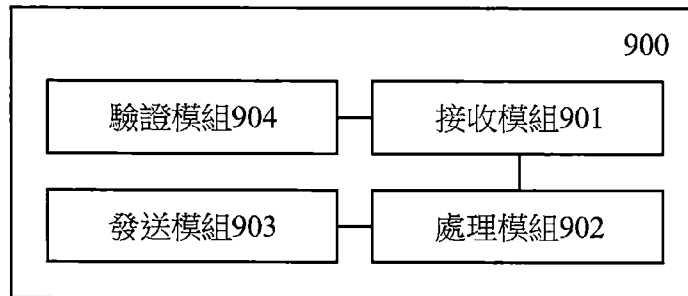


圖 21

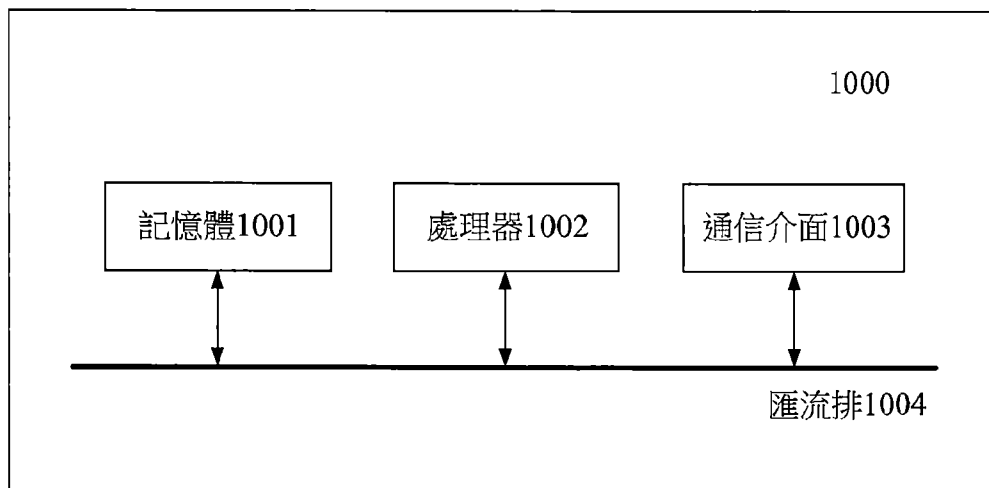


圖 22

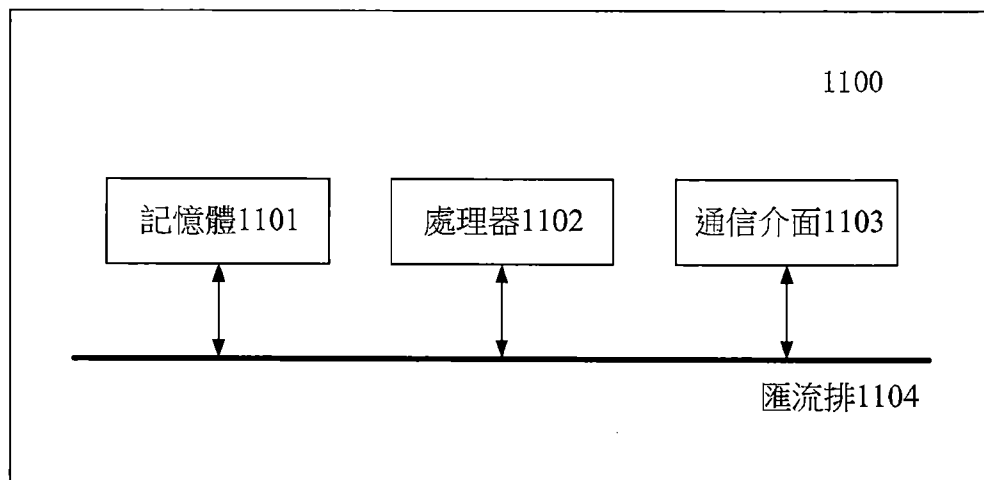


圖 23