



(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 I636412 B

(45)公告日：中華民國 107 (2018) 年 09 月 21 日

(21)申請案號：103110483

(22)申請日：中華民國 103 (2014) 年 03 月 20 日

(51)Int. Cl. : G06Q20/32 (2012.01)

G06Q20/38 (2012.01)

H04B5/00 (2006.01)

(30)優先權：2013/10/30

中國大陸

201310526656.2

(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：葉東 (CN)

(74)代理人：林志剛

(56)參考文獻：

TW 201250481A

CN 101140545A

US 2007/0118891A1

US 2011/0169654A1

審查人員：馮耀嘉

申請專利範圍項數：12 項 圖式數：4 共 32 頁

(54)名稱

針對應用程式的驗證方法、終端和系統

(57)摘要

本發明涉及一種針對應用程式的驗證方法、終端和系統。該方法應用於具有近場通信功能的終端中，該方法包括：當特定操作被觸發時，檢測距所述終端一定距離內的近場設備；獲取所述近場設備的標識，並向伺服器發送所述標識，以請求伺服器根據所述標識驗證所述近場設備是否是與所述特定操作對應的特定近場設備；接收所述伺服器根據所述標識進行驗證的結果；以及根據驗證結果，對所述特定操作進行下一步處理。採用本發明的技術方案，能夠保證終端上應用程式的使用安全性。

指定代表圖：

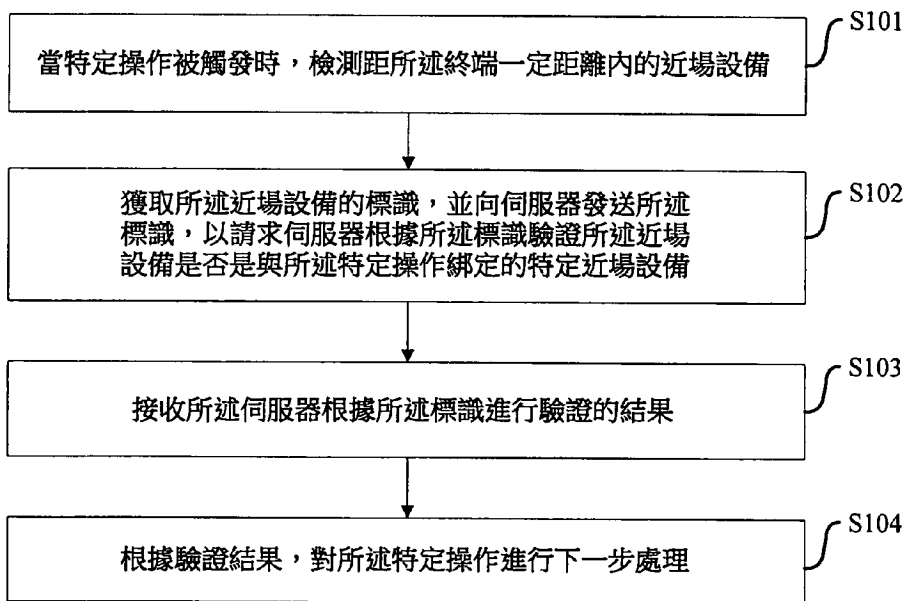


圖 1

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)

針對應用程式的驗證方法、終端和系統

【技術領域】

本發明涉及通訊領域，尤其涉及一種針對應用程式的驗證方法、終端和系統。

【先前技術】

隨著通信技術的發展，行動終端越來越受到廣大使用者的青睞，而行動終端的功能也越來越強大，尤其是手機，已經發展到了可以與電腦相媲美的智慧型手機階段。目前，為各種行動終端所開發的各種應用程式（App）層出不窮。然而，當使用者使用手機等行動終端上的應用程式（App）時，往往需要進行各種驗證操作，例如，登錄用戶帳號時需輸入登錄密碼進行驗證，與其他使用者進行資料互動時，需要輸入協力廠商互動平臺發送的驗證碼等。

現有的使用終端上的應用程式或透過終端上的應用程式進行資料互動時的驗證方案一般包括以下幾種：

1) 使用者密碼：由使用者設置使用者帳號的登錄密碼或資料互動密碼，當使用者登錄帳號或進行資料互動時需輸入預先設置的密碼，協力廠商互動平臺確認該密碼正

確後才放行使用者的登錄操作或資料交互動操作。但行動終端上的應用程式經常會被設置成記憶密碼，以方便使用者快捷的進行操作。然而，當使用者的行動終端由於遺失等原因，被他人使用時，由於該應用程式記憶了密碼，很可能會被他人濫用，造成用戶個人利益的損失。

2) 動態密碼 (OTP, One-time Password) 驗證：使用者在確認進行資料互動時，需要輸入動態密碼卡或硬體權杖上的動態密碼 (例如，包含數位、字母的一串字元)，協力廠商互動平臺確認該動態密碼正確後才放行資料互動。此方案需要使用者在正常的資料互動流程中，多增加一次輸入動態密碼的過程，複雜度增加，用戶體驗較差。

3) 基於簡訊的動態密碼驗證：這種方式是動態密碼 (OTP, One-time Password) 驗證方式中的一種，其主要用於手機終端中，使用者確認進行資料互動時，需要從事先與使用者帳戶綁定的手機中獲得協力廠商互動平臺以短資訊等形式下發的動態密碼，並在互動頁面上填寫正確動態密碼才能完成資料互動，然而當使用者的手機遺失後，這種驗證方式顯然就不能使用了，還可能會造成短時間內無法進行資料互動。

綜上所述，需要一種能夠保障使用者終端上應用程式的使用安全的驗證方法。

【發明內容】

本發明的主要目的在於提供一種針對應用程式的驗證方法、終端和系統，以解決現有技術存在的終端上的應用程式的使用安全問題，其中：

本發明提供的一種針對應用程式的驗證方法，應用於具有近場通信功能的中，包括：當特定操作被觸發時，檢測距所述終端一定距離內的近場設備；獲取所述近場設備的標識，並向伺服器發送所述標識，以請求伺服器根據所述標識驗證所述近場設備是否是與所述特定操作對應的特定近場設備；接收所述伺服器根據所述標識進行驗證的結果；以及根據驗證結果，對所述特定操作進行下一步處理。

本發明的另一態樣提供了一種具有近場通信功能的終端，包括：檢測模組，用於當特定操作被觸發時，檢測距所述終端一定距離內的近場設備；獲取模組，用於獲取所述近場設備的標識；發送模組，用於向伺服器發送所述標識，以請求伺服器根據所述標識驗證所述近場設備是否是與所述特定操作對應的特定近場設備；接收模組，用於接收所述伺服器根據所述標識進行驗證的結果；以及處理模組，用於根據驗證結果，對所述特定操作進行下一步處理。

本發明的再一態樣提供了一種終端系統，包括：具有近場通信功能的終端以及與所述終端對應的特定近場設備，其中，所述終端包括：檢測模組，用於當特定操作被觸發時，檢測距所述一定距離內的特定近場設備；獲取模

組，用於獲取所述近場設備的標識；發送模組，用於向伺服器發送所述標識，以請求伺服器根據所述標識驗證所述近場設備是否是與所述特定操作對應的特定近場設備；接收模組，用於接收所述伺服器根據所述標識進行驗證的結果；以及處理模組，用於根據驗證結果，對所述特定操作進行下一步處理；並且其中，所述特定近場設備與所述具有相同的近場通信功能。

與現有技術相比，根據本發明的技術方案，可以透過檢測與特定操作對應的近場設備是否存在來驗證使用者的當前的操作是否為正常操作（用戶本人的操作），如果近場設備驗證失敗，則終止當前的操作，並執行預設的安全操作，以保證上應用程式的使用安全性。

【圖式簡單說明】

此處所說明的圖式用來提供對本發明的進一步理解，構成本發明的一部分，本發明的示意性實施例及其說明用於解釋本發明，並不構成對本發明的不當限定。在圖式中：

圖 1 是本發明實施例的一種針對應用程式的驗證方法的流程圖；

圖 2 是本發明實施例的針對應用程式的驗證方法的一種實施方式的流程圖；

圖 3 是本發明實施例的一種具有近場通信功能的終端的結構方塊圖；以及

圖 4 是本發明實施例的一種終端系統的結構方塊圖。

【實施方式】

本發明的主要思想在於，提供一種針對應用程式的驗證方法，利用終端的近場通信功能，當啟動終端上某一應用程式的特定操作時，透過檢測所述終端近場通信有效距離內是否存在與所述特定操作對應的特定近場設備，以確定是否可以放行所述特定操作，進而保證終端上應用程式的使用的安全性。

為使本發明的目的、技術方案和優點更加清楚，下面將結合本發明具體實施例及相應的圖式對本發明技術方案進行清楚、完整地描述。顯然，所描述的實施例僅是本發明一部分實施例，而不是全部的實施例。基於本發明中的實施例，所述技術領域中具有通常知識者在沒有做出創造性勞動前提下所獲得的所有其他實施例，都屬於本發明保護的範圍。

根據本發明的實施例，提供了一種針對應用程式的驗證方法，該方法可以適用於具有近場通信功能的終端中，尤其是例如，手機、平板電腦等行動終端。所述近場通信功能可以包括但不限於：藍牙通信（Bluetooth）功能、近距離無線通訊（NFC）功能、射頻識別（RFID）功能。所述終端可以為具有上述任意一項或多項近場通信功能的終端。

參考圖 1，圖 1 是本發明實施例的一種針對應用程式

的驗證方法的流程圖。

如圖 1 所示，在步驟 S101 中，當特定操作被觸發時，檢測距所述終端一定距離內的近場設備。也就是說，搜尋該終端的近場通信有效距離內，是否有與該終端近場通信類型相同的近場設備。

在步驟 S102 中，獲取所述近場設備的標識，並向伺服器發送所述標識，以請求伺服器根據所述標識驗證所述近場設備是否是與所述特定操作對應的特定近場設備。

在步驟 S103 中，接收所述伺服器根據所述標識進行驗證的結果。即，接收所述伺服器返回的關於所述檢測到的近場設備是否是與所述特定操作對應的特定近場設備的驗證結果。

在步驟 S104 中，根據驗證結果，對所述特定操作進行下一步處理。即，根據伺服器根據所述標識驗證所述近場設備是否是與所述特定操作對應的特定近場設備而返回的驗證結果，對所述特定操作進行下一步處理。

其中，當所述驗證結果為所述近場設備是與所述特定操作對應的特定近場設備時，執行所述特定操作；當所述驗證結果為所述近場設備不是與所述特定操作對應的特定近場設備時，執行預設安全操作。

為了更清楚地描述本發明實施例的技術方案，下面將參考圖 2 進行更詳細的說明。

圖 2 是本發明的一種針對應用程式的驗證方法的較佳實施方式的流程圖，如圖 2 所示，在步驟 S201 中，當特

定操作被觸發時，確定針對所述特定操作是否需要進行近場設備驗證。即，首先確定針對該特定操作是否需要進行近場設備驗證。

其中，針對所述特定操作是否需要進行近場設備驗證，可以預先進行設置並儲存在伺服器。並且，該特定操作是否需要進行近場設備驗證，可以預先由使用者透過其他終端利用使用者帳號登錄該應用程式進行設置。其他終端可以為桌上型電腦、可攜式電腦等設備，例如，使用者可以透過桌上型電腦登錄該應用程式，設置該應用程式針對特定操作需要進行近場設備驗證。並且，可以預先設置與該特定操作對應的特定近場設備，即，該特定操作與該特定近場設備的標識具有對應關係。實際上，也就是將設置該特定操作需要進行近場設備驗證的使用者帳號與該特定近場設備綁定（應理解，將該特定操作與特定近場設備的標識的對應關係是由用戶透過登錄應用程式帳號進行設置的，因此，該特定近場設備也是與使用者帳號對應的），所述特定近場設備可以由使用者指定。並且透過該終端與伺服器的互動來設置該特定近場設備與該特定操作的對應關係，其中，伺服器是該應用程式的資料資訊在後臺的存放裝置，該應用程式的資訊展示及處理均須透過與伺服器的資料互動來實現。在伺服器可以儲存該特定近場設備的標識，從而認為該標識所標識的該特定近場設備為該特定操作所對應的特定近場設備。其中，近場通信功能可以包括但不限於：藍牙通信（Bluetooth）功能、近距離

無線通訊（NFC）功能、射頻識別（RFID）功能。特定近場設備與該終端具有相同的近場通信功能，以便能與該終端進行近場通信。例如，對於具有藍牙通信功能的行動終端，該特定近場設備可以為具有藍牙功能的藍牙耳機、藍牙滑鼠等具有藍牙功能的設備。該特定近場設備還可以為與該終端類型相同的設備，例如，該終端為具有藍牙功能的手機時，該特定近場設備也可以為具有藍牙功能的手機，在這種情況下，兩個終端還可以互為特定近場設備，即，在其中一個終端上使用該應用程式時，另一個終端可以作為特定近場設備，反之亦然。該特定近場設備可以為一個或一個以上，即，與該特定操作（以帳號標識使用者身份的應用程式的特定操作）對應的特定近場設備可以設置一個也可以設置多個，並可以透過該特定近場設備的標識來綁定該特定操作與該特定近場設備的對應關係，所述標識可以為該近場設備的實體位址（MAC 位址）、使用者對該近場設備的命名等。例如，可以透過該特定近場設備的 MAC 位址綁定，具體地，可以將該特定近場設備的 MAC 位址儲存在伺服器端，當進行近場設備驗證時，終端獲取待驗證的近場設備的 MAC 位址，並上傳至伺服器，由伺服器查詢待驗證的近場設備的 MAC 位址與伺服器端儲存的與該特定操作對應的特定近場設備的 MAC 位址是否一致，從而驗證該待驗證的近場設備是否為該特定近場設備。當該設備為藍牙設備時，該標識還可以為藍牙設備位址（Bluetooth Device Address）。每個藍牙收發器

都會被分配唯一的一個 48 位元的設備位址，該設備位址包括 24 位元的 LAP 域，16 位的 NAP 域和一個 8 位的 UAP 域。可以將該藍牙設備位址儲存在伺服器端，當進行近場設備驗證時，終端獲取待驗證的藍牙設備的設備位址，並上傳至伺服器，由伺服器查詢待驗證的藍牙設備的設備位址與伺服器端儲存的與該特定操作對應的藍牙設備的設備位址是否一致，從而驗證該待驗證的藍牙設備是否為與該特定操作對應的藍牙設備。

根據本發明的一個實施例，所述特定操作是否需要進行近場設備驗證，不透過當前所使用的終端來進行設置，以保證用戶的由於遺失或其他原因被他人操作時，操作者不能隨意更改該設置。其中，所述其他終端可以為個人電腦（桌上型電腦、可攜式電腦等）、智慧型手機、平板電腦等。較佳地，該其他終端為個人電腦。當使用者透過某終端來設置針對該應用程式的特定操作是否需要進行近場設備驗證時，伺服器可以識別該終端的設備類型，並根據設備類型判斷該設置是否可以生效，即，判斷該終端類型是否是指定的可以設置針對應用程式的特定操作是否需要進行近場設備驗證的設備類型，如果是，則可以在伺服器端儲存該設置，否則該設置無效。

根據本發明的一個實施例，可以預先設置所述特定操作與特定近場設備的標識的對應關係，即，透過該特定近場設備的標識，將該特定操作與該特定近場設備進行預先綁定，以便當用戶再次觸發該特定操作時，針對該特定操

作進行近場設備驗證。預先設置的所述特定操作與所述特定近場設備的標識的對應關係儲存在伺服器。

具體地，在伺服器端可以存儲使用者對該應用程式的設置，而針對特定操作進行近場設備驗證可以設置為該應用程式的一個功能，這裡我們可以稱之為近場設備驗證功能，並且在伺服器端可以存儲使用者對該應用程式的特定操作的近場設備驗證功能進行的設置（或設置資料），例如，儲存針對特定操作的近場設備驗證功能開啟關閉狀態（或狀態資料）、儲存預先與該終端綁定的特定近場設備的標識等，當使用者透過所述其他終端觸發了該應用程式的特定操作時，伺服器檢查用戶對該應用程式的近場設備驗證功能的設置，如果用戶沒有開啟針對特定操作的近場設備驗證功能，例如，在用戶第一次觸發了該應用程式的特定操作時（用戶必然沒有開啟針對特定操作的近場設備驗證功能），則提示用戶是否要設置針對該特定操作進行近場設備驗證，即，提示用戶是否開啟針對該特定操作的近場設備驗證功能，使用者如果選擇是，則提示用戶設置一個（或多個）與該特定操作對應的特定近場設備。需注意，設置針對該應用程式的特定操作是否需要進行近場設備驗證，並不僅限於使用者透過所述其他終端在第一次觸發該應用程式的特定操作時進行設置，也就是說，使用者可以在其他終端上根據個人的需要更改針對特定操作是否需要進行近場設備驗證的設置。

所述特定操作可以為所述應用程式的一項或多項操

作，例如，登錄某一應用程式時的登錄操作、使用支付應用程式的進行支付時的確認支付操作等，並且，可以透過登錄該應用程式，將該應用程式的一項或多項操作設置為特定操作。當用戶開啟該應用程式並觸發了任意一項操作時，如果該操作是預先設置的特定操作，即可透過查詢針對該特定操作是否需要進行近場設備驗證，來確定是否對該特定操作進行近場設備的驗證。

當應用程式的特定操作被觸發時，向伺服器發送查詢針對所述特定操作是否需要進行近場設備驗證的請求，並根據伺服器返回的查詢結果確定所述特定操作是否需要進行近場設備驗證。所述特定操作是否需要進行近場設備驗證，是預先進行設置並儲存在所述伺服器的，伺服器收到該查詢請求後，查詢該用戶是否設置了針對該特定操作進行近場設備驗證，並返回查詢的結果，從而可以根據伺服器返回的查詢結果，確定是否需要對於該特定操作進行近場設備的驗證。

例如，當用戶使用上的支付應用程式進行支付操作時，當用戶點擊表示“確認支付”的按鈕後（該“確認支付”操作為一項特定操作），該應用程式可以向伺服器發起查詢請求，請求伺服器查詢該用戶是否設置了針對該“確認支付”操作需要進行近場設備驗證，以確定是否需要對於該“確認支付”的操作進行近場設備的驗證。

如果針對所述特定操作不需要進行近場設備驗證，則執行步驟 S206，執行所述特定操作。即，執行用戶所觸

發的操作。

如果針對所述特定操作需要進行近場設備驗證，則執行步驟 S202。

在步驟 S202 中，檢測距所述終端一定距離內的近場設備。也就是說，搜尋該終端的近場通信有效距離內，是否存在近場設備。

其中，所述終端與所述近場設備採用同樣的近場通信方式，終端可能具有不只一種近場通信方式（例如，可能同時具有藍牙功能和 NFC 功能），因此，該終端需要與該近場設備的近場通信方式相同，雙方才能在進行近場設備驗證時進行近場通信。例如，該近場通信方式可以為藍牙通信，該近場設備可以為藍牙耳機。所述一定距離為所述終端的近場通信有效距離，該終端，需要與要互相進行通信的近場設備保持在一定的距離範圍內，才能搜尋到該近場設備，進而與該近場設備配對並進行通信，即，近場通信的有效距離。也就是說，當與該特定操作對應的近場設備與該終端的距離在該終端近場通信有效距離以內時，該終端才能夠搜尋到該近場設備。

例如，在具有藍牙功能的手機上開啟應用程式時，由於藍牙通信的有效距離一般約為 10 公尺，因此，當使用該應用程式的特定操作時，需要將與該特定操作綁定的藍牙設備與該手機保持 10 公尺以內的距離，手機才能搜尋到該藍牙設備，並且透過與該設備配對獲取該設備的設備資訊，如設備標識等資訊。由於藍牙通信有效距離約為

10 公尺，因此，用戶只需要隨身攜帶與該手機對應的藍牙設備（例如，藍牙耳機），而不需要特意將藍牙耳機靠近該手機。

如果距所述終端一定距離記憶體在近場設備，則執行步驟 S203。

在步驟 S203 中，獲取所述近場設備的標識，並向伺服器發送所述標識，以請求伺服器根據所述標識驗證所述近場設備是否是與所述特定操作對應的特定近場設備。

伺服器儲存有預先設置的所述特定操作與所述特定近場設備的標識的對應關係，如果搜尋到該終端的近場通信有效距離記憶體在近場設備，可以透過與近場該設備配對，從而與近場該設備進行近場通信，進而獲取該近場設備的標識。獲取到該近場設備的標識後，可以向伺服器發送該標識，請求伺服器查詢該近場設備是否為與所述特定操作對應的特定近場設備，即，預先與該特定操作綁定的特定近場設備。

伺服器接收到驗證所述近場設備是否是與所述特定操作對應的特定近場設備的請求時，可以根據接收到的由所述終端發送的所述標識及所述儲存的預先設置的所述特定操作與所述特定近場設備的標識的對應關係進行驗證，並返回驗證結果。

具體地，伺服器可以儲存預先設置的所述特定操作與所述特定近場設備的標識的對應關係，當接收到該終端發送的該近場設備的標識，伺服器端透過將該標識與伺服器

端儲存的與該特定操作對應的特定近場設備的標識進行比對，來驗證該近場設備是否是與該特定操作對應的特定近場設備，並返回驗證的結果。如果一致，則說明該近場設備是與該特定操作對應的特定近場設備，即，該的近場通信有效距離記憶體在與該特定操作對應的特定近場設備。如果比對的結果為不一致，則該近場設備不是與該特定操作對應的特定近場設備，即，該終端的近場通信有效距離內不存在與該特定操作對應的特定近場設備。所述標識可以為該近場設備的物理位址（MAC 位址）、使用者對該近場設備的命名等。並且可以將該標識儲存在伺服器端。例如，可以透過該近場設備的 MAC 位址綁定該近場設備與該終端，可以將該設備的 MAC 位址儲存在伺服器端，當進行近場設備驗證時，向伺服器發送該 MAC 位址，請求伺服器驗證該搜尋到的近場設備是否是與該特定操作綁定的特定近場設備，伺服器則根據該的 MAC 位址以及伺服器端儲存的與該特定操作對應的特定近場設備的對應關係，驗證該近場設備是否為與該特定操作對應的特定近場設備，並返回驗證結果。

在步驟 S204 處，接收所述伺服器根據所述標識進行驗證的結果。即，接收所述伺服器返回的驗證所述檢測到的近場設備是否是與所述特定操作對應的特定近場設備的驗證結果。

在步驟 S205 處，根據驗證結果，對所述特定操作進行下一步處理。即，根據伺服器根據所述標識驗證所述近

場設備是否是與所述特定操作綁定的特定近場設備而返回的驗證結果，對所述特定操作進行下一步處理。

步驟 S205 可以包括兩種情況，其中，一種情況為：當所述驗證結果為所述近場設備是與所述特定操作對應的特定近場設備時，執行所述特定操作。

另一種情況為：當所述驗證結果為所述近場設備不是與所述特定操作對應的特定近場設備時，執行預設安全操作。

例如，使用者透過一個終端啟動應用程式，與特定應用程式綁定的特定近場設備為一個藍牙耳機，當使用者開啟終端上的應用程式並觸發了登錄操作（該登錄操作為一項特定操作）時，並且，向伺服器發起查詢請求返回的結果為針對該登錄操作需要進行近場設備驗證，則檢測該終端的一定距離內是否存在近場設備，其中，該終端採用與該近場設備相同的近場通信方式。即，搜尋該終端的近場通信有效距離內有沒有藍牙設備，如果搜尋到該終端的近場通信有效距離記憶體在藍牙設備，則獲取該藍牙設備的 MAC 位址，並將該 MAC 位址向伺服器發送，以請求伺服器查詢該藍牙設備是否為與該特定操作對應的藍牙耳機，伺服器接收到該 MAC 位址後與之前儲存的與該終端的藍牙耳機的 MAC 位址進行比對，如果伺服器返回的結果為這兩個 MAC 位址一致，說明該設備是與該特定操作對應的藍牙耳機，即近場設備驗證成功；如果伺服器返回的結果為兩個 MAC 位址不一致，則說明該近場設備不是與該

特定操作對應的藍牙耳機，即，近場設備驗證失敗，則執行預設安全操作。

例如，當使用者使用終端上的支付應用程式時，當用戶點擊表示“確認支付”的按鈕後（該“確認支付”操作為一項特定操作），如果該用戶設置了針對該支付應用程式需要進行近場設備驗證，則搜尋該終端的近場通信有效距離內是否有與該終端具有相同的近場通信功能的近場設備，並獲取搜尋到的近場設備的標識向伺服器發送，以請求伺服器驗證該設備是否是與該確認支付操作對應的特定近場設備，實際上，也就是搜尋該終端的近場通信有效距離內是否存在與該操作對應的特定近場設備，不存在（該終端的近場通信有效距離內沒有搜尋到近場通信類型相同的近場設備，或所搜尋到的近場設備經查詢並不是與該操作綁定的特定近場設備，則說明該“確認支付”操作，為異常操作（例如，使用者終端丟失的情況、他人濫用該使用者的終端的情況），即，驗證失敗，此時執行預設安全操作。

在步驟 S202 中，如果檢測距所述終端一定距離內不存在近場設備，也就是說，該終端的近場通信有效距離內不存在與該特定操作對應的特定近場設備，則執行步驟 S207，執行預設安全操作。

其中，所述預設安全操作可以包括以下任意一項或多項：鎖定所述終端、清除所述終端中記憶的密碼、通知其他的終端。

當在終端近場通信有效距離內沒有搜尋到與其綁定的特定近場設備，即，近場設備驗證失敗時，可以鎖定該終端，例如，該終端為手機時，可以終止當前的被觸發的特定操作，並鎖定該手機的螢幕，即，需要輸入預設的鎖螢幕密碼才能解鎖，使當前的操作者不能繼續使用該手機。

或者，還可以清除終端中記憶的密碼或刪除（卸載）該應用程式，例如，用戶在登錄手機上應用程式的時候，為了方便下次登錄，經常會將該應用程式設置成記憶登錄密碼，如果使用者的手機不慎遺失，那麼，該應用程式則極容易被他人使用手機中儲存的密碼進行登錄並使用，因此，可以在近場設備驗證失敗時，終止當前的操作，並清除記憶的密碼，此時，雖然登錄密碼是正確的，但由於在手機端的近場設備驗證失敗，手機端已經終止了當前被觸發的特定操作（即，並沒有向伺服器發送登錄該應用程式的請求），因此，當前的操作者仍然不能成功登錄用戶的應用程式帳號。

或者，還可以通知其他終端，使用者可以設置當近場設備驗證失敗時，自動向其他終端發送提醒。例如，當用戶的手機不慎丟失，當有人使用該用戶手機上的該應用程式的該特定操作時，由於沒有與該手機對應的特定近場設備（例如，藍牙耳機），則近場設備驗證就會失敗，用戶手機會透過簡訊等形式自動向其他終端發出提醒，例如，用戶可以設置的其他手機的號碼為發送提醒簡訊的手機號碼，當近場設備驗證失敗時，自動向該手機號碼發送提醒

簡訊，這樣一方面不但可以保證應用程式的使用安全，另一方面當用戶在不知道自己的手機已經遺失的時候，還可以起到提醒用戶的作用。另外，還可以設置當近場設備驗證失敗時，開啟 GPS 定位或前置攝像頭進行拍攝，並將定位得到的該終端當前的位置資訊或前置攝像頭拍攝的照片以提醒簡訊的形式發送給該其他終端，從而還能獲取該終端當前所在的地點等資訊，以方便使用者尋回該終端。

根據本發明的一個實施例，上述的近場設備驗證過程可以設置為隱藏過程，即在驗證過程中，不在該應用程式的頁面上顯示任何有關近場設備驗證的提示，因此，當前的操作者也不會感知到正在進行的驗證操作。

本發明還提供了一種具有近場通信功能的終端。

圖 3 示意性地示出了根據本發明一個實施例的一種終端 300 的結構方塊圖。根據本發明的一個實施例，該終端 300 可以包括：檢測模組 301、獲取模組 302、發送模組 303、接收模組 304 以及處理模組 305。

其中，檢測模組 301 可以用於當特定操作被觸發時，檢測距所述終端一定距離內的近場設備。

獲取模組 302 可以用於獲取所述近場設備的標識。

發送模組 303 可以用於向伺服器發送所述標識，以請求伺服器根據所述標識驗證所述近場設備是否是與所述特定操作對應的特定近場設備。

接收模組 304 可以用於接收所述伺服器根據所述標識進行驗證的結果。

處理模組 305 可以用於根據驗證結果，對所述特定操作進行下一步處理。

根據本發明的一個實施例，處理模組 305 可以進一步用於：當所述驗證結果為所述近場設備是與所述特定操作對應的特定近場設備時，執行所述特定操作；以及當所述驗證結果為所述近場設備不是與所述特定操作對應的特定近場設備時，執行預設安全操作。

根據本發明的一個實施例，終端 300 還可以包括：確定模組，用於當特定操作被觸發時，向伺服器發送查詢針對所述特定操作是否需要進行近場設備驗證的請求，並根據伺服器返回的驗證結果確定所述特定操作是否需要進行近場設備驗證。

根據本發明的一個實施例，檢測模組 301 可以進一步用於：檢測距所述終端一定距離內的近場設備。獲取模組 302 可以進一步用於：如果存在近場設備，則獲取所述近場設備的標識；以及處理模組 305 可以進一步用於：如果不存在近場設備，則執行預設安全操作。

根據本發明的實施例，所述一定距離為所述終端的近場通信有效距離。

根據本發明的實施例，所述預設安全操作包括以下操作中的一個或多個：鎖定所述終端、清除所述終端中記憶的密碼、通知其他的終端。

參考圖 4，為本發明的一種終端系統 400 的結構方塊圖，如圖 4 所示，終端系統 400 包括：具有近場通信功能

的終端 410 以與所述特定操作對應的特定近場設備 420；

其中，所述終端包括：

檢測模組 411，可以用於當特定操作被觸發時，檢測距所述終端一定距離內的近場設備。

獲取模組 412，可以用於獲取所述近場設備的標識。

發送模組 413，可以用於向伺服器發送所述標識，以請求伺服器根據所述標識驗證所述近場設備是否是與所述特定操作對應的特定近場設備。

接收模組 414，可以用於接收所述伺服器根據所述標識進行驗證的結果。

處理模組 415，可以用於根據驗證結果，對所述特定操作進行下一步處理。

並且其中，所述特定近場設備 420 與所述終端 410 具有相同的近場通信功能。

根據本發明的一個實施例，所述近場通信為可以藍牙通信，所述特定近場設備可以為藍牙耳機。

由於本實施例的終端和終端系統所實現的功能基本相應於前述圖 1、圖 2 所示的方法實施例，故本實施例的描述中未詳盡之處，可以參見前述實施例中的相關說明，在此不做贅述。

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存儲。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。電腦的存儲媒體的例子包括，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）、電子抹除式可複寫唯讀記憶體（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）或其他光學存儲、磁盒式磁帶，磁帶磁磁片存儲或其他磁性存放裝置或任何其他非傳輸媒體，可用於存儲可以被計算設備訪問的資訊。按照本文中的界定，電腦可讀媒體不包括非暫存電腦可讀媒體（transitory media），如調製的資料信號和載波。

還需要說明的是，術語“包括”、“包含”或者其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。

本領域中具有通常知識者應明白，本發明的實施例可提供為方法、系統、或電腦程式產品。因此，本發明可採用完全硬體實施例、完全軟體實施例、或結合軟體和硬體方面的實施例的形式。而且，本發明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存儲媒體（包括但不限於磁碟記憶體、CD-ROM、光學儲存器等）上實施的電腦程式產品的形式。

以上所述僅為本發明的實施例而已，並不用於限制本發明，對於本領域中具有通常知識者來說，本發明可以有各種更改和變化。凡在本發明的精神和原則之內，所作的任何修改、等同替換、改進等，均應包含在本發明的申請專利範圍範圍之內。

【符號說明】

S101~S104：步驟

S201~S207：步驟

300：終端

301：檢測模組

302：獲取模組

303：發送模組

304：接收模組

305：處理模組

400：終端系統

410：終端

411：檢測模組

412：獲取模組

413：發送模組

414：接收模組

415：處理模組

420：特定近場設備

I636412

發明摘要

※申請案號：103110483

※申請日：103 年 03 月 20 日

※IPC 分類：

【發明名稱】(中文/英文)

針對應用程式的驗證方法、終端和系統

【中文】

本發明涉及一種針對應用程式的驗證方法、終端和系統。該方法應用於具有近場通信功能的終端中，該方法包括：當特定操作被觸發時，檢測距所述終端一定距離內的近場設備；獲取所述近場設備的標識，並向伺服器發送所述標識，以請求伺服器根據所述標識驗證所述近場設備是否是與所述特定操作對應的特定近場設備；接收所述伺服器根據所述標識進行驗證的結果；以及根據驗證結果，對所述特定操作進行下一步處理。採用本發明的技術方案，能夠保證終端上應用程式的使用安全性。

【英文】

圖式

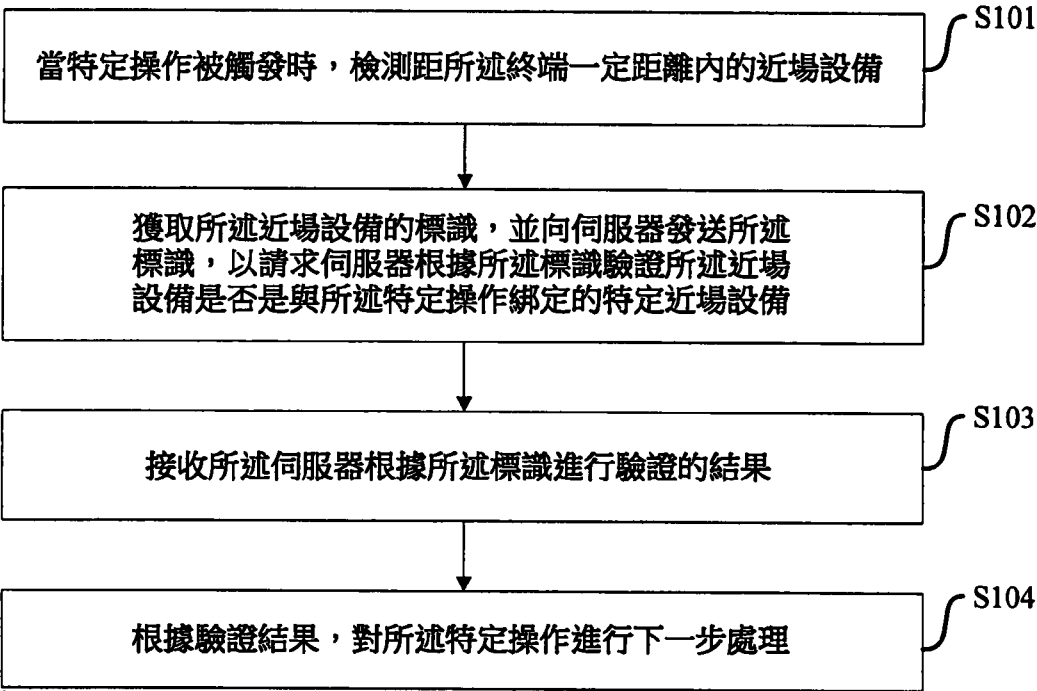


圖 1

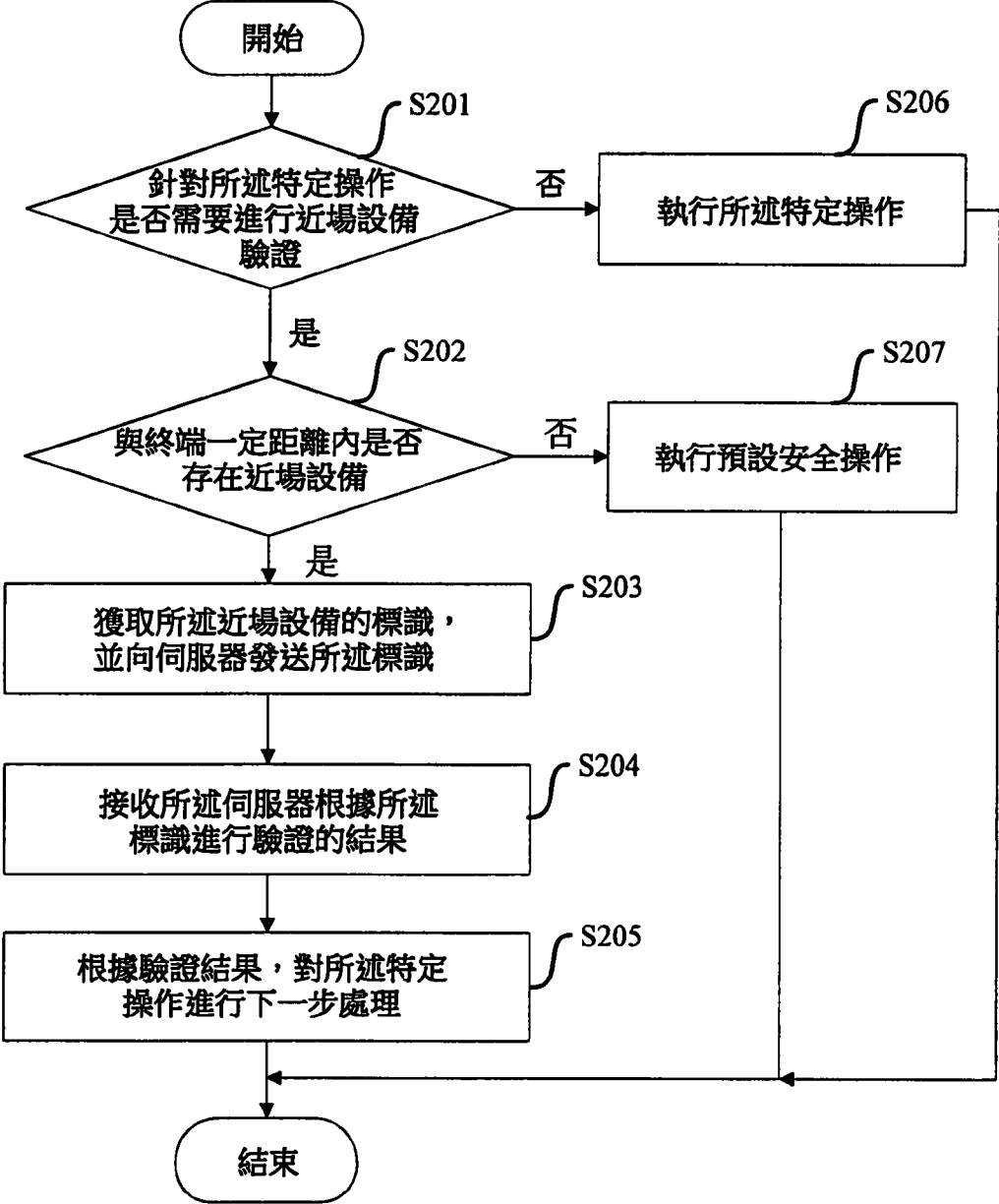


圖 2

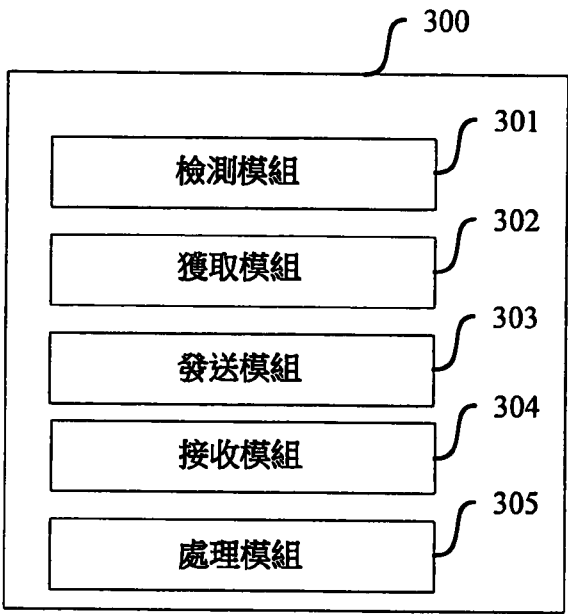


圖 3

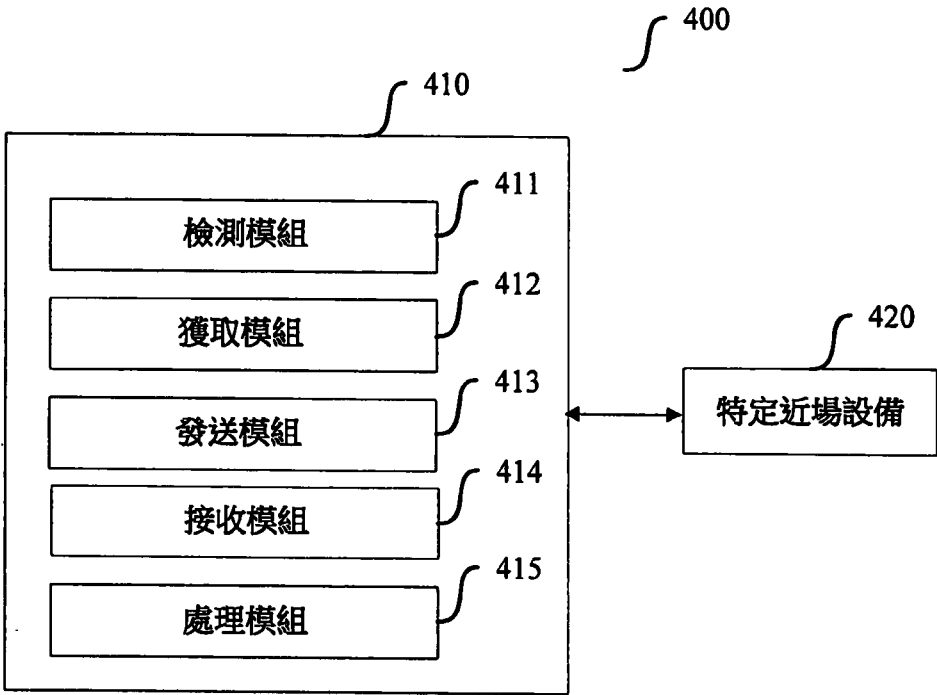


圖 4

【代表圖】

【本案指定代表圖】：第(1)圖。

【本代表圖之符號簡單說明】：無

【本案若有化學式時，請揭示最能顯示發明特徵的化學式】：
無

申請專利範圍

1. 一種針對應用程式的驗證方法，應用於具有近場通信功能的終端中，其特徵在於，包括：

當特定操作被觸發時，檢測距該終端一定距離內的近場設備；

獲取該近場設備的標識，並向伺服器發送該標識，以請求伺服器根據該標識驗證該近場設備是否是與該特定操作對應的特定近場設備；

接收該伺服器根據該標識進行驗證的結果；以及
根據驗證結果，對該特定操作進行下一步處理，
其中，進一步包括：

向伺服器發送查詢針對該特定操作是否需要進行近場設備驗證的請求，並根據伺服器返回的查詢結果確定該特定操作是否需要進行近場設備驗證，且
其中，該特定操作是否需要進行近場設備驗證，是預先儲存在該伺服器的。

2. 根據申請專利範圍第 1 項所述的方法，其中，根據驗證結果，對該特定操作進行下一步處理，包括：

當該驗證結果為該近場設備是與該特定操作對應的特定近場設備時，執行該特定操作；

當該驗證結果為該近場設備不是與該特定操作對應的特定近場設備時，執行預設安全操作。

3. 根據申請專利範圍第 1 項所述的方法，其中，檢測距該終端一定距離內的近場設備，包括：

檢測距該終端一定距離內的近場設備；

如果存在近場設備，則獲取該近場設備的標識；以及
如果不存在近場設備，則執行預設安全操作。

4. 根據申請專利範圍第 1 項所述的方法，其中，該伺服器儲存有該特定操作與該特定近場設備的標識的對應關係。

5. 根據申請專利範圍第 4 項所述的方法，其中，該伺服器根據該標識進行驗證的步驟，包括：該伺服器根據接收到的由該終端發送的該標識及該儲存的預先設置的該特定操作與該特定近場設備的標識的對應關係進行驗證。

6. 根據申請專利範圍第 1-5 項中任一項所述的方法，其中，該一定距離為該終端的近場通信有效距離。

7 根據申請專利範圍第 2 或 3 項所述的方法，其中，該預設安全操作包括以下操作中的一個或多個：鎖定該終端、清除該終端中記憶的密碼、通知其他的終端。

8. 根據申請專利範圍第 1 項所述的方法，其中：該終端與該近場設備採用同樣的近場通信方式。

9. 根據申請專利範圍第 8 項所述的方法，其中，該近場通信方式為藍牙通信，該近場設備為藍牙耳機。

10. 一種具有近場通信功能的終端，其特徵在於，包括：

檢測模組，用於當特定操作被觸發時，檢測距該終端一定距離內的近場設備；

獲取模組，用於獲取該近場設備的標識；

發送模組，用於向伺服器發送該標識，以請求伺服器根據該標識驗證該近場設備是否是與該特定操作對應的特定近場設備；

接收模組，用於接收該伺服器根據該標識進行驗證的結果；

處理模組，用於根據驗證結果，對該特定操作進行下一步處理；以及

確定模組，用於當特定操作被觸發時，向伺服器發送查詢針對該特定操作是否需要進行近場設備驗證的請求，並根據伺服器返回的查詢結果確定該特定操作是否需要進行近場設備驗證，

其中，該特定操作是否需要進行近場設備驗證，是預先儲存在該伺服器的。

11. 根據申請專利範圍第 10 項所述的終端，其中，該處理模組進一步用於：

當該驗證結果為該近場設備是與該特定操作對應的特定近場設備時，執行該特定操作；以及

當該驗證結果為該近場設備不是與該特定操作對應的特定近場設備時，執行預設安全操作。

12. 根據申請專利範圍第 10 項所述的終端，其中，

該檢測模組進一步用於：檢測距該終端一定距離內的近場設備；

該獲取模組進一步用於：如果存在近場設備，則獲取該近場設備的標識；以及

該處理模組進一步用於：如果不存在近場設備，則執行預設安全操作。