I744267

(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 I744267 B

(45)公告日： 中華民國 110 (2021) 年 11 月 01 日

(21)申請案號：105142083 (22)申請日： 中華民國 105 (2016) 年 12 月 19 日

(51)Int. Cl.： *G06F21/34 (2013.01)*

(30)優先權：2016/01/05 中國大陸 201610006062.2

(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：修超 (CN) ；王磊 (CN) ；施晨杰 (CN)

(74)代理人：林志剛

(56)參考文獻：

CN 104182870A

審查人員：吳鴻鎮

申請專利範圍項數：8 項 圖式數：6 共 29 頁

(54)名稱

智慧卡應用安全驗證方法及裝置

(57)摘要

本發明係關於資訊安全技術領域，特別係關於一種智慧卡應用安全驗證方法及裝置，其中方法包括在智慧卡應用與外界進行業務的處理過程中，獲取當前業務相關資料；將所述當前業務相關資料與安全參數進行判斷；若所述當前業務相關資料不符合所述安全參數，則終止本次業務。方法相應的裝置可以內置於虛擬智慧卡應用中或者獨立於 eSE 晶片中的智慧卡應用執行上述方法，透過本發明實施例的方法和裝置對業務進行時地理位置、時間、交易資訊等內容的判斷，可以進一步的確保使用智慧卡應用進行業務時的安全性。

指定代表圖：

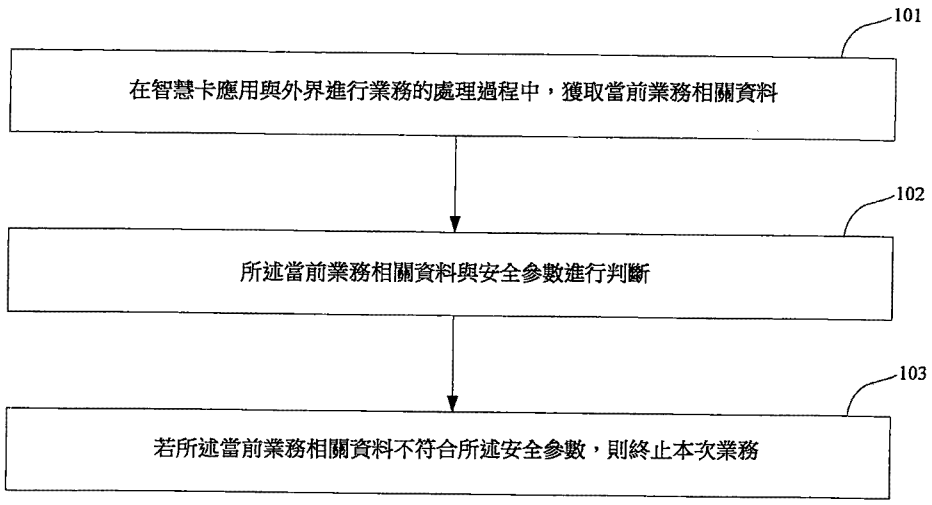

圖 1

第 105142083 號　　民國 108 年 10 月 18 日修正

I744267

發明摘要

公告本

※申請案號：105142083

※申請日：105 年 12 月 19 日　　※IPC 分類：*G06F 21/34* (2013.01)

【發明名稱】(中文/英文)

智慧卡應用安全驗證方法及裝置

【中文】

本發明係關於資訊安全技術領域，特別係關於一種智慧卡應用安全驗證方法及裝置，其中方法包括在智慧卡應用與外界進行業務的處理過程中，獲取當前業務相關資料；將所述當前業務相關資料與安全參數進行判斷；若所述當前業務相關資料不符合所述安全參數，則終止本次業務。方法相應的裝置可以內置於虛擬智慧卡應用中或者獨立於 eSE 晶片中的智慧卡應用執行上述方法，透過本發明實施例的方法和裝置對業務進行時地理位置、時間、交易資訊等內容的判斷，可以進一步的確保使用智慧卡應用進行業務時的安全性。

【英文】

【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

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)

智慧卡應用安全驗證方法及裝置

【技術領域】

本發明係關於資訊安全技術領域，特別係關於一種智慧卡應用安全驗證方法及裝置。

【先前技術】

隨著行動網際網路的發展，越來越多的業務可以透過智慧終端機的智慧卡應用來實現，例如透過在智慧終端機實現行動支付、實現乘坐公共交通工具、實現進入自己的工作區域等，均可以透過給智慧終端機增加近場通信晶片來實現上述智慧卡應用。但是，智慧終端機的通途越來越廣，在使用者生活中所扮演的角色也越來越重要，如果智慧終端機遺失後被惡意盜用可能會給使用者甚至公司、社會造成嚴重後果。現在極需一種增強智慧終端機智慧卡應用安全性的技術方案。

【發明內容】

為了解決現有技術中智慧終端機被盜用後無法保證智慧卡應用安全性的問題，提出了一種智慧卡應用安全驗證方法及裝置，用於根據使用者的設定或者使用者的使用習

慣限制智慧卡應用的使用，從而保證了智慧卡應用的安全性。

本發明實施例具體提供了一種智慧卡應用安全驗證方法，包括，

在智慧卡應用與外界進行業務的處理過程中，獲取當前業務相關資料；

將所述當前業務相關資料與安全參數進行判斷；

若所述當前業務相關資料不符合所述安全參數，則終止本次業務。

本發明實施例還提供了一種智慧卡應用安全驗證裝置，包括，

獲取單元，用於在智慧卡應用與外界進行業務的處理過程中，獲取當前業務相關資料；

判斷單元，用於將所述當前業務相關資料與安全參數進行判斷；

處理單元，用於若所述當前業務相關資料不符合所述安全參數，則終止本次業務。

由以上本發明實施例提供的技術方案可見，對業務進行時地理位置、時間、交易資訊等內容的判斷，可以進一步的確保使用智慧卡應用進行業務時的安全性；並且在根據了智慧卡應用的不同種類（eSE 晶片或者 HCE 等），設計了適用於不同種類智慧卡應用的安全驗證方法，例如獲取 eSE 晶片內的智慧卡應用與通信模組之間的業務過程，從而進行驗證，或者透過內置於 HCE 智慧卡應用中

的安全驗證方法來對業務進行安全驗證。

當然實施本發明的任一產品或者方法必不一定需要同時達到以上所述的所有優點。

【圖式簡單說明】

為了更清楚地說明本發明實施例或現有技術中的技術方案，下面將對實施例或現有技術描述中所需要使用的圖式作簡單地介紹，顯而易見地，下面描述中的圖式僅僅是本發明中記載的一些實施例，對於本領域通常知識者來講，在不付出創造性勞動性的前提下，還可以根據這些圖式獲得其他的圖式。

圖 1 所示為本發明實施例一種智慧卡應用安全驗證方法的流程圖；

圖 2 所示為本發明實施例一種智慧卡應用安全驗證裝置的結構示意圖；

圖 3 所示為本發明實施例一種智慧卡應用安全驗證方法的具體流程圖；

圖 4 所示為本發明實施例安裝智慧卡應用到 eSE 晶片中的系統結構圖；

圖 5 所示為本發明實施例另一種智慧卡應用安全驗證方法的具體流程圖；

圖 6 所示為本發明實施例安裝智慧卡應用到智慧手機中的系統結構圖。

【實施方式】

本發明實施例提供一種智慧卡應用安全驗證方法及裝置。

為了使本技術領域的人員更好地理解本發明中的技術方案，下面將結合本發明實施例中的圖式，對本發明實施例中的技術方案進行清楚、完整地描述，顯然，所描述的實施例僅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，本領域通常知識者在沒有作出創造性勞動前提下所獲得的所有其他實施例，都應當屬於本發明保護的範圍。

在本發明中的智慧卡應用包括了例如門禁、交通卡、銀行卡等應用，在智慧終端機中設置 eSE 晶片（嵌入式安全元件），在該 eSE 晶片中置入所述智慧卡應用，或者透過 HCE（卡模擬）的技術來實現智慧卡應用，以上兩種方式均為現有技術，在本發明中不再贅述。

如圖 1 所示為本發明實施例一種智慧卡應用安全驗證方法的流程圖，在本實施例中，智慧終端機與交易終端進行業務處理的過程中，在智慧終端機根據判斷規則判斷當前業務是否安全，如果不安全則中斷該業務，否則允許業務繼續進行，其中的判斷規則可以為根據位置資訊、時間資訊、業務內容等諸多資訊的判斷，可以由使用者自行設定，或者有系統端統計分析後給所述智慧終端機，透過上述方式可以對智慧卡應用進行安全控制，防止智慧終端機遺失後的危害。

該圖具體包括步驟 101，在智慧卡應用與外界進行業務的處理過程中，獲取當前業務相關資料。

步驟 102，將所述當前業務相關資料與安全參數進行判斷。

步驟 103，若所述當前業務相關資料不符合所述安全參數，則終止本次業務。

根據本發明的一個實施例，還包括若所述當前業務相關資料符合所述安全參數，則允許繼續進行本次業務。透過對當前業務相關資料的判斷，可以中斷或者授權本次業務，從而可以進一步保證智慧卡應用所進行的本次業務的安全性。

根據本發明的一個實施例，所述當前業務相關資料至少包括當前位置資訊、當前時間資訊、交易資訊中的一個或者多個的組合。其中，透過當前位置資訊可以與安全參數中設定的位置資訊進行判斷，如果超出所述安全參數中設定的位置範圍，則不應當允許業務的繼續進行，例如，當智慧卡應用正在進行業務的當前位置為天津，而使用者設定的安全參數中的位置範圍為北京，則認為智慧卡應用所進行的本次業務是不安全的；或者，當智慧卡應用正在進行業務的交易為付款 1000 元，而使用者設定的安全參數的交易資訊中為 800 元，則認為智慧卡應用所進行的本次業務是不安全的。

所述當前業務相關資料可以透過智慧終端機的 GPS 模組或者基地台的定位方式獲得當前位置資訊，透過系統

時鐘或者網路時鐘獲得當前時間資訊，透過交易訂單獲得交易資訊。其中定位的具體方法可以參考現有技術中的定位技術，獲取當前時間資訊也可以參考現有技術中的具體方案，在此不再贅述。

根據本發明的一個實施例，在智慧卡應用與外界進行業務的處理過程中，獲取當前業務相關資料之中還包括，在內置於 eSE 晶片（嵌入式安全元件）的智慧卡應用與 NFC（近場通信單元）控制器的通信過程中，監測雙方的通信過程，並獲取當前業務相關資料。

在本步驟的實施例中，本發明實施例中的方法可以以軟體方式或者以硬體模組的方式實施，該獲取當前業務相關資料以及後面的判斷分析等處理過程構成的方法是以監測 eSE 晶片中智慧卡應用與 NFC 控制器（或者類似其它智慧卡應用所使用的通信模組）之間的通信過程而啟動的，或者還可以由 NFC 控制器在進行某個業務過程中通知本發明的安全驗證應用，也就是說本發明實施例的安全驗證方法監測 eSE 晶片中智慧卡應用與 NFC 控制器之間是否正在進行業務處理，如果出現業務處理，則啟動安全驗證。

本實施例還可以在智慧卡應用與 NFC 控制器通信的任意過程中獲取當前業務相關資料以及後繼步驟，例如在 NFC 控制器向智慧卡應用轉發業務指令之前進行安全驗證。

根據本發明的一個實施例，在智慧卡應用與外界進行

業務的處理過程中，獲取當前業務相關資料之中還包括，在虛擬智慧卡的應用（HCE）與 NFC 控制器的通信過程中，在虛擬智慧卡的應用中監測雙方的通信過程，並獲取當前業務相關資料。

在本步驟中的實施例中，當智慧卡應用是透過模擬智慧卡的應用（HCE）來實現的，那麼可以在該應用中加入本發明的安全驗證方法，可以在該模擬智慧卡的應用進行業務過程中的任意步驟之前或者之後進行本發明實施例的安全驗證方法，當透過安全驗證，則可以繼續業務過程，否則將中斷業務過程。

根據本發明的一個實施例，在將所述當前業務相關資料與安全參數進行判斷之前還包括，接收並保存使用者輸入的安全參數；

或者，接收並保存伺服器根據使用者的相關資料分析得到的安全參數。

在本步驟的實施例中，安全參數可以由使用者自行設定，也可以透過伺服器基於使用者歷史行為的分析確定，例如透過統計分析該使用者從而出現在 A 區域，而本次業務的位置資訊為 A 區域，則認為該業務可能存在安全風險，可以拒絕使用者的本次業務，再進一步的實施例中，例如當業務為門禁認證時，該使用者從來未要求進入過 A 區，本次要求進入 A 區，可能是由於具有門禁智慧卡應用的手機遺失，被人撿到後的行為。

透過本發明實施例的方法，對業務進行時地理位置、

時間、交易資訊等內容的判斷，可以進一步的確保使用智慧卡應用進行業務時的安全性；並且在根據了智慧卡應用的不同種類（eSE 晶片或者 HCE 等），設計了適用於不同種類智慧卡應用的安全驗證方法，例如獲取 eSE 晶片內的智慧卡應用與通信模組之間的業務過程，從而進行驗證，或者透過內置於 HCE 智慧卡應用中的安全驗證方法來對業務進行安全驗證。

如圖 2 所示為本發明實施例一種智慧卡應用安全驗證裝置的結構示意圖，在本實施例中的裝置可以內置並運行於智慧終端機上，其中智慧終端機例如包括智慧手機、平板電腦等設備，所述智慧卡應用驗證裝置可以由可程式設計邏輯器件（FPGA）等專用晶片實現，或者在類比智慧卡應用（HCE）中透過軟體實現。

該圖具體包括獲取單元 201，用於在智慧卡應用與外界進行業務的處理過程中，獲取當前業務相關資料。

判斷單元 202，用於將所述當前業務相關資料與安全參數進行判斷。

處理單元 203，用於若所述當前業務相關資料不符合所述安全參數，則終止本次業務。

根據本發明的一個實施例，所述處理單元還用於若所述當前業務相關資料符合所述安全參數，則允許繼續進行本次業務。

根據本發明的一個實施例，所述當前業務相關資料至少包括當前位置資訊、當前時間資訊、交易資訊中的一個

或者多個的組合。

其中，所述當前位置資訊可以透過智慧終端機內部的GPS 模組獲得，所述當前時間資訊可以透過網路通信模組獲得，或者透過智慧終端機內部的時鐘晶體諧振器獲得，所述交易資訊可以透過智慧終端機的交易訂單獲得。

根據本發明的一個實施例，所述獲取單元監測內置於eSE 晶片（嵌入式安全元件）的智慧卡應用與 NFC（近場通信單元）控制器的通信過程，並獲取當前業務相關資料。

根據本發明的一個實施例，所述獲取單元內置於虛擬智慧卡的應用中，獲取虛擬智慧卡的應用（HCE）與 NFC控制器的通信過程中的當前業務相關資料。

根據本發明的一個實施例，還包括安全參數接收單元204，用於接收並保存使用者輸入的安全參數；

或者，接收並保存伺服器根據使用者的相關資料分析得到的安全參數。

透過本發明實施例的裝置，對業務進行時地理位置、時間、交易資訊等內容的判斷，可以進一步的確保使用智慧卡應用進行業務時的安全性；並且在根據了智慧卡應用的不同種類（eSE 晶片或者 HCE 等），設計了適用於不同種類智慧卡應用的安全驗證方法，例如獲取 eSE 晶片內的智慧卡應用與通信模組之間的業務過程，從而進行驗證，或者透過內置於 HCE 智慧卡應用中的安全驗證方法來對業務進行安全驗證。

如圖 3 所示為本發明實施例一種智慧卡應用安全驗證方法的具體流程圖，在該圖中的智慧卡應用內置於 eSE 安全晶片之中，本實施例中的智慧終端機可以為智慧手機，讀卡器可以為 POS 機上安裝的 NFC 讀卡器，NFC 控制器為智慧手機上的硬體，用於與 POS 機上的 NFC 讀卡器通信以完成支付業務。在智慧手機中內置本發明實施例中的裝置或者用軟體方式運行的方法，監測智慧卡應用與 NFC 控制器之間的支付業務處理過程，從而實現對支付業務進行安全驗證的目的。

具體包括步驟 301，內置於 eSE 晶片中的支付應用在 NFC 控制器上註冊，在 NFC 控制器中記錄有支付應用 ID。

在本實施例中智慧卡應用可以透過智慧卡應用管理終端安裝到 eSE 晶片中，或者透過空中發卡單元（可以內置於智慧手機的 eSE 晶片內部）透過網路安裝到 eSE 晶片中，具體系統結構圖可以如圖 4 所示，其中，POS 機上的 NFC 讀卡器透過近場通信的方式與智慧手機的 NFC 控制器進行通信，智慧卡應用管理終端也是透過該近場通信方式將智慧卡應用安裝於智慧手機的 eSE 晶片中，或者還可以透過空中發卡單元從遠端獲取智慧卡應用安裝於 eSE 晶片中，本發明中的安全驗證應用也內置於智慧手機中，監測 eSE 晶片和 NFC 控制器之間的通信，該安全驗證應用也可以透過 NFC 控制器中的通信介面監測 eSE 晶片和 NFC 控制器之間的通信。

在本步驟中或者在本步驟之前，使用者可以透過智慧手機的輸入裝置，例如觸控式螢幕、按鍵等方式，在內置於智慧手機的本發明的安全驗證應用中輸入安全參數，其中安全參數在智慧卡的支付應用中可以例如為限定位置地點或者範圍、交易金額臨界值等，或者可以根據實際的需要增加或者減少安全參數的設定，在本實施例中限定位置例如為 A 地區、B 地區、C 地區以及貫穿這三個地區的沿途都是允許使用智慧卡的支付應用，在其它地區禁止使用該支付應用，交易金額臨界值例如可以為 1000 塊，即無論在什麼地區，均不允許消費超過 1000 元，當然本領域技術人員透過上述本發明的公開可以聯想到其它組合的安全參數，例如交易金額與限定位置組合，即，在限定位置區域內交易金額可以不受限制，在限定位置以外的區域交易金額只能為 100，如果安全參數中考慮到時間參數，則可以出現更多種組合可能的安全參數，在本發明實施例中不能窮盡各種可能的組合，因此不再贅述。

步驟 302，POS 機的 NFC 讀卡器與智慧手機的 NFC 控制器近距離通信進行支付業務。

在本步驟中，NFC 讀卡器與 NFC 控制器之間的支付業務處理過程可以參考現有技術中的方案，例如，NFC 讀卡器選擇 NFC 控制器中註冊的支付應用 ID，然後執行相應的智慧卡支付業務流程。

步驟 303，NFC 控制器向安全驗證應用發送支付業務的提示，以啟動安全驗證應用。

步驟 304，內置於智慧手機中的安全驗證應用獲取支付業務相關資料。

在本步驟中安全驗證應用可以透過 NFC 控制器的介面獲得支付業務相關資料，此時支付應用不會獲得該支付業務相關資料。

所述支付業務相關資料包括當前的位置資訊和當前交易金額。其中，安全驗證應用透過智慧手機中的 GPS 模組獲取當前的位置資訊，或者可以透過基地台定位的方式或者網路定位的方式獲得當前位置資訊，透過截獲的業務處理結果可以獲得本次交易金額。

步驟 305，根據安全參數驗證當前位置資訊和當前交易金額。

在本實施例中，截獲的位置資訊為 D 區域，交易金額為 2000 元，將支付業務相關資料與安全參數中的限定位置和交易金額臨界值進行比較，判斷結果為不符合安全參數。

步驟 306，安全驗證應用終止本次支付業務，並將本次支付業務失敗的執行結果發送給 NFC 控制器。

在本步驟中，還可以將安全驗證的結果透過智慧手機的螢幕向使用者進行提示。

若上述步驟 305 中的判斷結果為符合安全參數，則允許本次支付業務繼續進行（即不作為），不干擾 NFC 控制器和 eSE 晶片中智慧卡應用進行的支付業務過程，在圖中以虛線的方式顯示允許支付業務繼續進行時支付應用進

行業務處理的過程，NFC 控制器將支付業務指令轉發給內置於 eSE 晶片中的支付應用，支付應用進行業務處理，並透過 NFC 控制器向 NFC 讀卡器返回業務處理結果，支付應用可能與 NFC 讀卡器之間還具有多次的通信，以使得支付業務流程順利進行，但是這部分內容作為現有技術中不在本實施例中贅述。

步驟 307，NFC 控制器將本次支付業務失敗的執行結果發送給 POS 機 NFC 讀卡器，本次支付失敗。

透過上述實施例，本發明的技術方案可以根據使用者設定的安全參數控制進行智慧卡應用，當進行未授權（即安全參數以外）的業務時，將會及時終止不安全的智慧卡應用的業務處理，保證了使用者財產、資訊的安全，避免由於智慧終端機遺失後被他人惡意使用而造成的損失。

如圖 5 所示為本發明實施例另一種智慧卡應用安全驗證方法的具體流程圖，在該實施例中以虛擬智慧卡應用為例介紹本發明的技術方案，虛擬智慧卡主要是針對一些沒有內置 eSE 晶片的智慧終端機，使這種智慧終端機可以支援智慧卡應用，本發明的安全驗證方法或者裝置可以內置於虛擬智慧卡應用中，從而可以實現對該虛擬智慧卡應用進行安全驗證的目的。在本實施例中還是以支付業務作為說明，智慧終端機為智慧手機，POS 機讀卡器還是 NFC 讀卡器，智慧手機透過 NFC 控制器與 NFC 讀卡器進行通信，當然，在其它實施例中，還可以採用其它模式的近場通信技術進行通信，在此不做限定。

具體包括步驟 501，虛擬智慧卡應用在 NFC 控制器中註冊支付應用 ID。

在本實施例中虛擬智慧卡應用可以透過智慧卡應用管理終端安裝到智慧手機的記憶體中，具體系統結構圖可以如圖 6 所示，其中，POS 機上的 NFC 讀卡器透過近場通信的方式與智慧手機的 NFC 控制器進行通信，智慧卡應用管理終端也是透過該近場通信方式將虛擬智慧卡應用安裝於智慧手機的記憶體中，或者還可以透過智慧手機的聯網功能從遠端獲取虛擬智慧卡應用安裝於智慧手機中，本發明的安全驗證應用可以內置於所述虛擬智慧卡應用中。

步驟 502，POS 機的 NFC 讀卡器與 NFC 控制器通信，選擇虛擬智慧卡應用 ID 進行支付業務。

步驟 503，NFC 控制器將進行支付業務的指令發送給虛擬智慧卡應用。

步驟 504，虛擬智慧卡應用中的安全驗證應用可以獲取當前位置資訊、當前時間資訊。

其中，獲取當前位置資訊可以透過智慧手機中的 GPS 模組獲取當前的位置資訊，或者可以透過基地台定位的方式或者網路定位的方式獲得當前位置資訊；當前時間資訊可以透過智慧手機的系統時間中獲得，或者也可以透過智慧手機的聯網功能從網際網路中獲取。

步驟 505，透過智慧手機的通信模組從遠端伺服器中獲取該使用者的安全參數。

在本步驟中的安全參數是透過網際網路，從遠端伺服

器中獲得，所述遠端伺服器透過對使用者的歷史資料進行分析，或者透過對該使用者相關的大數據分析得到相應安全參數，例如透過該使用者日常的支付交易習慣、金額、地點、時間、商品類別等資料中分析得到該使用者安全參數，根據使用者的資料判斷本次交易的安全風險在電子交易領域中有很多實現方法，本發明中所係關於的具體安全參數計算方法可以參考現有技術中的內容，此處只是利用到該部分的現有技術。

本實施例中獲取安全參數的方法和圖 3 所示實施例中由使用者設定安全參數的方法可以互換。

步驟 506，根據安全參數驗證本次支付業務的當前位置資訊和當前時間資訊。

若安全參數中的位置資訊與當前位置資訊不同，並且安全參數中的時間資訊與當前時間資訊不同，即說明該使用者通常不會在當前時間、當前位置進行支付業務，該支付業務可能不是使用者本人實施，可能存在風險。

步驟 507，終止本次支付業務，產生相應業務處理結果，並傳送給 NFC 控制器。

若上述步驟 506 的判斷結果為安全支付業務，則繼續執行虛擬智慧卡應用的支付業務流程，期間可能透過 NFC 控制器與 POS 級的 NFC 讀卡器進行一次或者數次通信，已完成支付業務流程。

步驟 508，NFC 控制器將支付業務處理結果發送給 POS 機的 NFC 讀卡器。

透過上述本發明實施例中的方法及裝置，對業務進行時地理位置、時間、交易資訊等內容的判斷，可以進一步的確保使用智慧卡應用進行業務時的安全性；並且在根據了智慧卡應用的不同種類（eSE 晶片或者 HCE 等），設計了適用於不同種類智慧卡應用的安全驗證方法，例如獲取 eSE 晶片內的智慧卡應用與通信模組之間的業務過程，從而進行驗證，或者透過內置於 HCE 智慧卡應用中的安全驗證方法來對業務進行安全驗證。

對於一個技術的改進可以很明顯地區分是硬體上的改進（例如，對二極體、電晶體、開關等電路結構的改進）還是軟體上的改進（對於方法流程的改進）。然而，隨著技術的發展，當今的很多方法流程的改進已經可以視為硬體電路結構的直接改進。設計人員幾乎都透過將改進的方法流程程式設計到硬體電路中來得到相應的硬體電路結構。因此，不能說一個方法流程的改進就不能用硬體實體模組來實現。例如，可程式設計邏輯器件（Programmable Logic Device, PLD）（例如現場可程式設計閘陣列（Field Programmable Gate Array，FPGA））就是這樣一種積體電路，其邏輯功能由使用者對器件程式設計來確定。由設計人員自行程式設計來把一個數位系統“整合”在一片 PLD 上，而不需要請晶片製造廠商來設計和製作專用的積體電路晶片 2。而且，如今，取代手工地製作積體電路晶片，這種程式設計也多半改用“邏輯編譯器（logic compiler）”軟體來實現，它與程式開發撰寫時所用的軟

體編譯器相類似，而要編譯之前的原始代碼也得用特定的程式設計語言來撰寫，此稱之為硬體描述語言（Hardware Description Language，HDL），而 HDL 也並非僅有一種，而是有許多種，如 ABEL（Advanced Boolean Expression Language）、AHDL（Altera Hardware Description Language）、Confluence、CUPL（Cornell University Programming Language）、HDCal、JHDL（Java Hardware Description Language）、Lava、Lola、MyHDL、PALASM、RHDL（Ruby Hardware Description Language）等，目前最普遍使用的是 VHDL（Very-High-Speed Integrated Circuit Hardware Description Language）與 Verilog2。本領域通常知識者也應該清楚，只需要將方法流程用上述幾種硬體描述語言稍作邏輯程式設計並程式設計到積體電路中，就可以很容易得到實現該邏輯方法流程的硬體電路。

控制器可以按任何適當的方式實現，例如，控制器可以採取例如微處理器或處理器以及儲存可由該（微）處理器執行的電腦可讀程式碼（例如軟體或韌體）的電腦可讀媒體、邏輯閘、開關、專用積體電路（Application Specific Integrated Circuit，ASIC）、可程式設計邏輯控制器和嵌入微控制器的形式，控制器的例子包括但不限於以下微控制器：ARC 625D、Atmel AT91SAM、Microchip PIC18F26K20 以及 Silicone Labs C8051F320，記憶體控制器還可以被實現為記憶體的控制邏輯的一部分。

本領域通常知識者也知道，除了以純電腦可讀程式碼方式實現控制器以外，完全可以透過將方法步驟進行邏輯程式設計來使得控制器以邏輯閘、開關、專用積體電路、可程式設計邏輯控制器和嵌入微控制器等的形式來實現相同功能。因此這種控制器可以被認為是一種硬體部件，而對其內包括的用於實現各種功能的裝置也可以視為硬體部件內的結構。或者甚至，可以將用於實現各種功能的裝置視為既可以是實現方法的軟體模組又可以是硬體部件內的結構。

上述實施例闡明的系統、裝置、模組或單元，具體可以由電腦晶片或實體實現，或者由具有某種功能的產品來實現。

為了描述的方便，描述以上裝置時以功能分為各種單元分別描述。當然，在實施本發明時可以把各單元的功能在同一個或多個軟體和/或硬體中實現。

透過以上的實施方式的描述可知，本領域的通常知識者可以清楚地瞭解到本發明可借助軟體加必需的通用硬體平臺的方式來實現。基於這樣的理解，本發明的技術方案本質上或者說對現有技術做出貢獻的部分可以以軟體產品的形式體現出來，該電腦軟體產品可以儲存在儲存媒體中，如 ROM/RAM、磁碟、光碟等，包括若干指令用以使得一台電腦設備（可以是個人電腦，伺服器，或者網路設備等）執行本發明各個實施例或者實施例的某些部分所述的方法。

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。尤其，對於系統實施例而言，由於其基本相似於方法實施例，所以描述的比較簡單，相關之處參見方法實施例的部分說明即可。

本發明可用於眾多通用或專用的電腦系統環境或配置中。例如：個人電腦、伺服器電腦、手持設備或可攜式設備、平板型設備、多處理器系統、基於微處理器的系統、機上盒、可程式設計的消費電子設備、網路 PC、小型電腦、大型電腦、包括以上任何系統或設備的分散式運算環境等等。

本發明可以在由電腦執行的電腦可執行指令的一般上下文中描述，例如程式模組。一般地，程式模組包括執行特定任務或實現特定抽象資料類型的常式、程式、物件、元件、資料結構等等。也可以在分散式運算環境中實踐本發明，在這些分散式運算環境中，由透過通信網路而被連接的遠端處理設備來執行任務。在分散式運算環境中，程式模組可以位於包括存放裝置在內的本地和遠端電腦儲存媒體中。

雖然透過實施例描繪了本發明，本領域通常知識者知道，本發明有許多變形和變化而不脫離本發明的精神，希望所附的申請專利範圍包括這些變形和變化而不脫離本發明的精神。

【符號說明】

201：獲取單元

202：判斷單元

203：處理單元

204：安全參數接收單元

申請專利範圍

1. 一種智慧卡應用安全驗證方法，包括，

在智慧卡應用與外界進行業務的處理過程中，獲取當前業務相關資料，其中包括：

在內置於嵌入式安全晶片(eSE 晶片)的所述智慧卡應用與 NFC 控制器的通信過程中，監測雙方的通信過程，並獲取所述當前業務相關資料，或在以 HCE（卡模擬）來實現的虛擬智慧卡的應用與所述 NFC 控制器的通信過程中，在所述虛擬智慧卡的應用中監測雙方的通信過程，並獲取所述當前業務相關資料；

將所述當前業務相關資料與安全參數進行判斷，其中所述安全參數是使用者輸入的安全參數或是伺服器根據使用者的相關資料分析得到的安全參數；

若所述當前業務相關資料不符合所述安全參數，則終止本次業務。

2. 根據申請專利範圍第 1 項所述的方法，其中，還包括若所述當前業務相關資料符合所述安全參數，則允許繼續進行本次業務。

3. 根據申請專利範圍第 1 項所述的方法，其中，所述當前業務相關資料至少包括當前位置資訊、當前時間資訊、交易資訊中的一個或者多個的組合。

4. 根據申請專利範圍第 1 項所述的方法，其中，在將所述當前業務相關資料與所述安全參數進行判斷之前還包括，接收並保存所述使用者輸入的所述安全參數；

或者，接收並保存所述伺服器所述根據所述使用者的相關資料分析得到的所述安全參數。

5. 一種智慧卡應用安全驗證裝置，包括，

獲取單元，用於在智慧卡應用與外界進行業務的處理過程中，獲取當前業務相關資料，其中，所述獲取單元監測內置於嵌入式安全晶片的智慧卡應用與 NFC 控制器的通信過程，並獲取所述當前業務相關資料，其中，所述獲取單元內置於虛擬智慧卡的應用中，獲取以 HCE 來實現的所述虛擬智慧卡的應用與所述 NFC 控制器的通信過程中的所述當前業務相關資料；

判斷單元，用於將所述當前業務相關資料與安全參數進行判斷，其中所述安全參數是使用者輸入的安全參數或是伺服器根據使用者的相關資料分析得到的安全參數；

處理單元，用於若所述當前業務相關資料不符合所述安全參數，則終止本次業務。

6. 根據申請專利範圍第 5 項所述的裝置，其中，所述處理單元還用於若所述當前業務相關資料符合所述安全參數，則允許繼續進行本次業務。

7. 根據申請專利範圍第 5 項所述的裝置，其中，所述當前業務相關資料至少包括當前位置資訊、當前時間資訊、交易資訊中的一個或者多個的組合。

8. 根據申請專利範圍第 5 項所述的裝置，其中，還包括安全參數接收單元，用於接收並保存所述使用者輸入的所述安全參數；

或者，接收並保存所述伺服器根據所述使用者的相關資料分析得到的所述安全參數。

圖 式

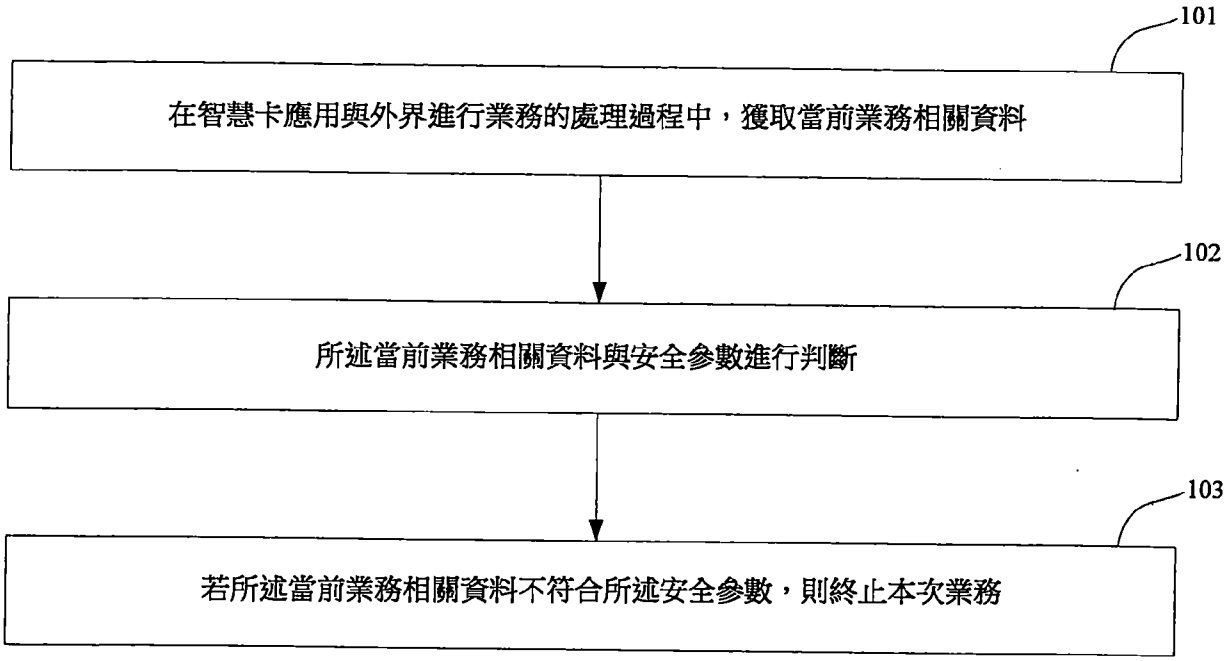
101
在智慧卡應用與外界進行業務的處理過程中，獲取當前業務相關資料
102
所述當前業務相關資料與安全參數進行判斷
103
若所述當前業務相關資料不符合所述安全參數，則終止本次業務

圖 1

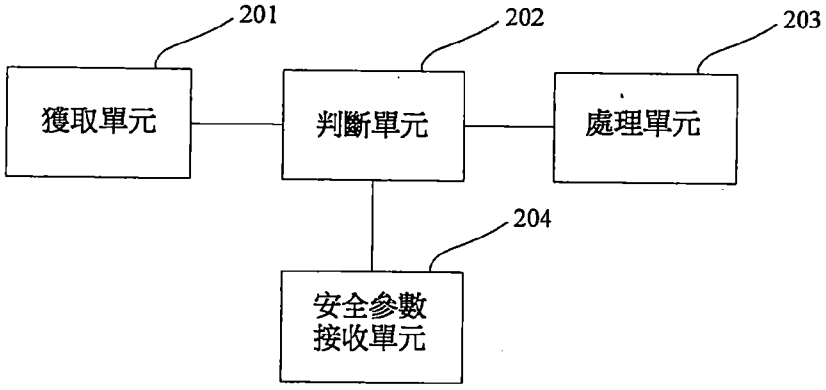
201
獲取單元
202
判斷單元
203
處理單元
204
安全參數
接收單元

圖 2

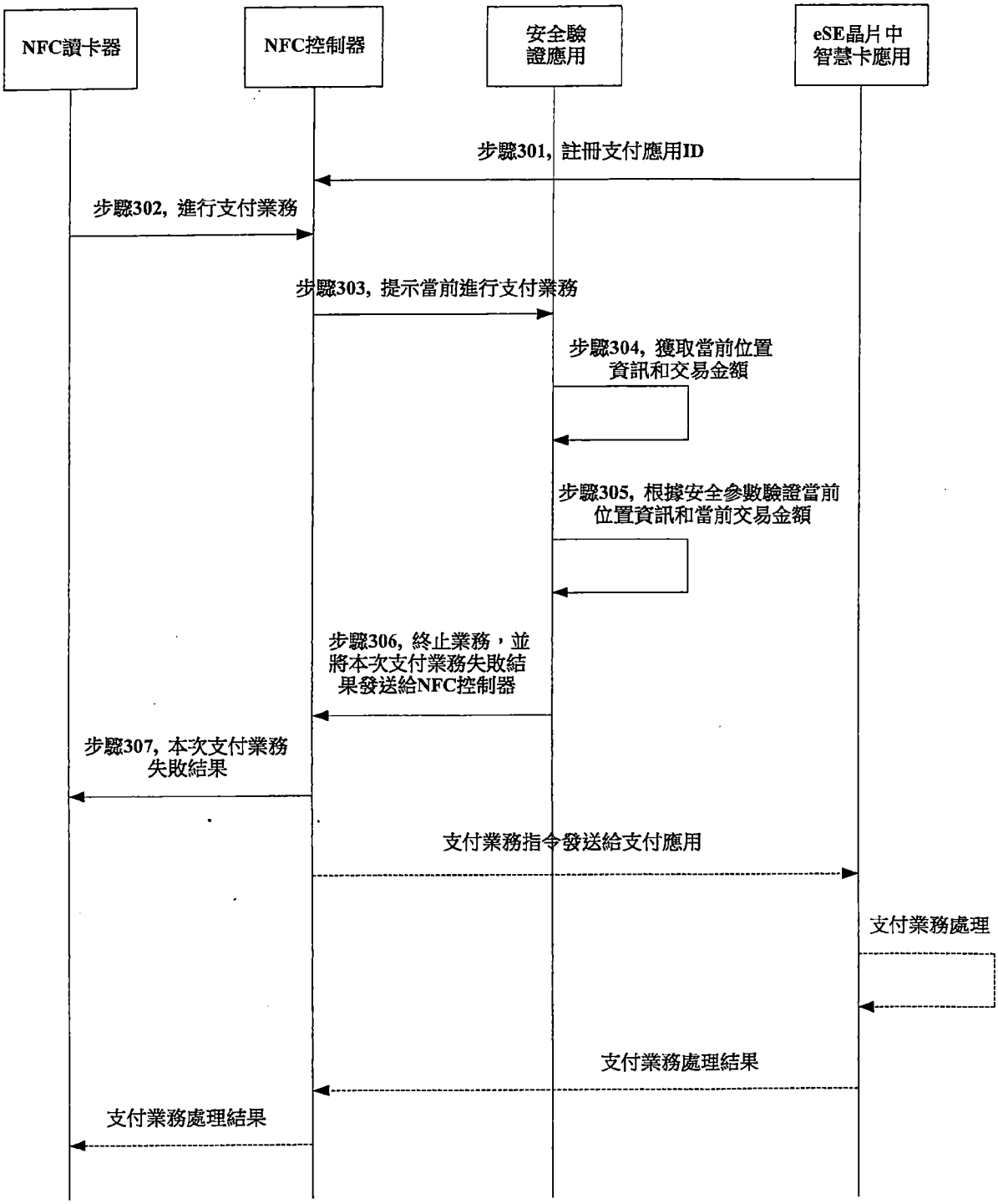
NFC讀卡器
NFC控制器
安全驗證應用
eSE晶片中智慧卡應用
步驟301，註冊支付應用ID
步驟302，進行支付業務
步驟303，提示當前進行支付業務
步驟304，獲取當前位置資訊和交易金額
步驟305，根據安全參數驗證當前位置資訊和當前交易金額
步驟306，終止業務，並將本次支付業務失敗結果發送給NFC控制器
步驟307，本次支付業務失敗結果
支付業務指令發送給支付應用
支付業務處理
支付業務處理結果
支付業務處理結果

圖 3

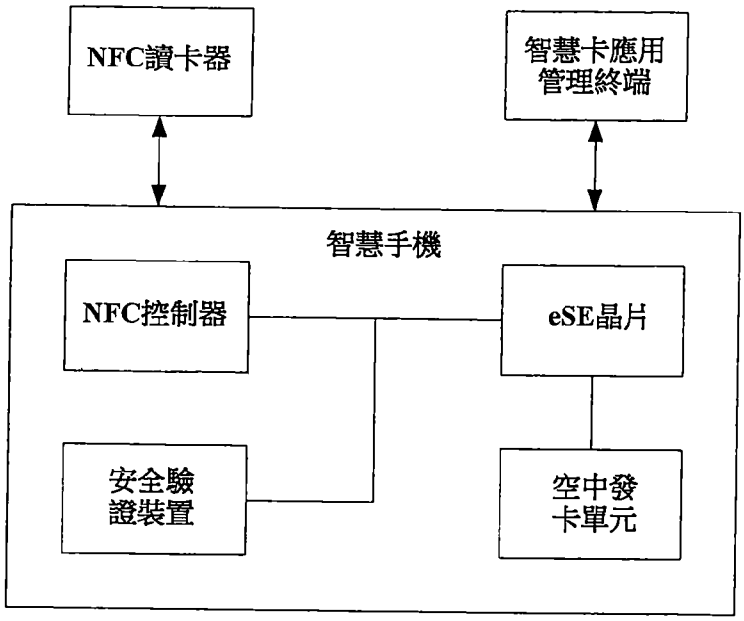
NFC讀卡器
智慧卡應用管理終端
智慧手機
NFC控制器
eSE晶片
安全驗證裝置
空中發卡單元

圖 4

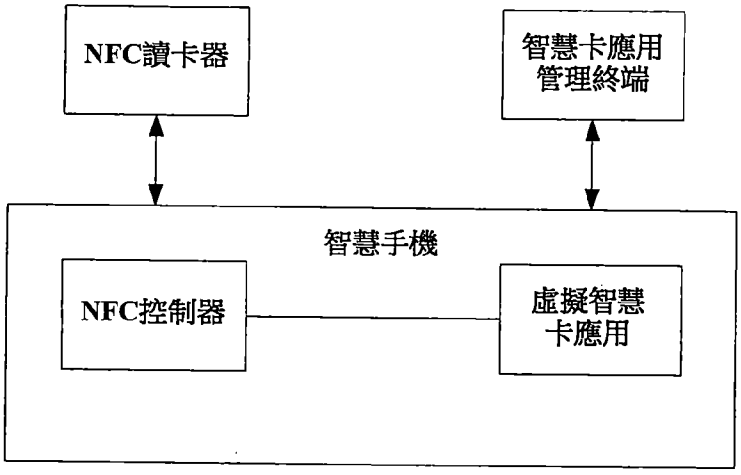
NFC讀卡器
智慧卡應用管理終端
智慧手機
NFC控制器
虛擬智慧卡應用

圖 6

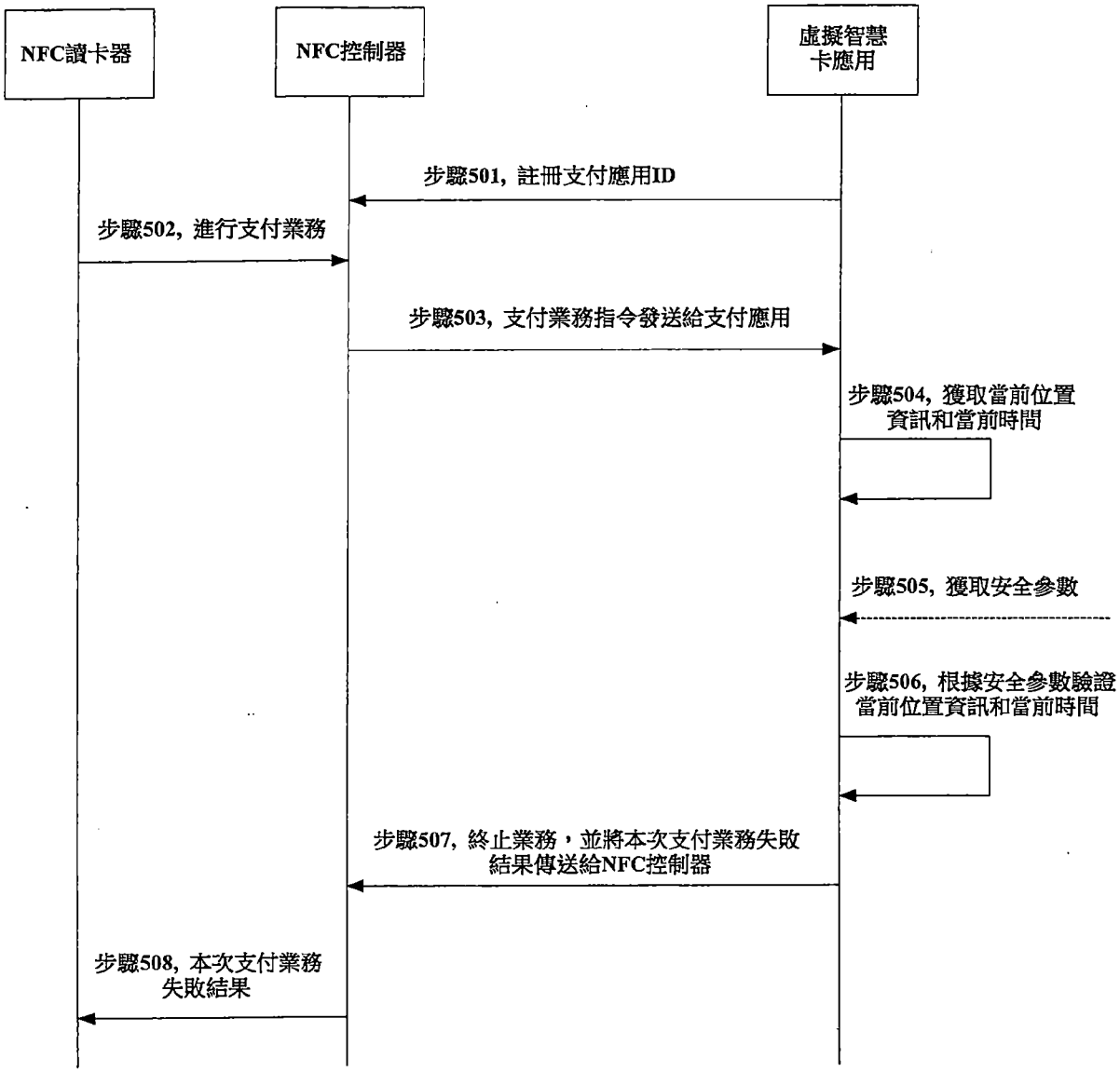
NFC讀卡器
NFC控制器
虛擬智慧卡應用
步驟501, 註冊支付應用ID
步驟502, 進行支付業務
步驟503, 支付業務指令發送給支付應用
步驟504, 獲取當前位置資訊和當前時間
步驟505, 獲取安全參數
步驟506, 根據安全參數驗證當前位置資訊和當前時間
步驟507, 終止業務，並將本次支付業務失敗結果傳送給NFC控制器
步驟508, 本次支付業務失敗結果

圖 5