結合近端通訊系統之線上遊戲帳號驗證機制

The Authentication Mechanism of Online Game with Near Field Communication System

陳炳彰
南臺科技大學資訊傳播學系
台南市永康區南台街一號
bcchen@mail.stust.edu.tw

Bing-Chang Chen
Department of Information and Communication, Southern Taiwan University of Science and Technology
No.1, Nantai St., Yongkang Dist., Tainan City 710, Taiwan (R.O.C.)
bcchen@mail.stust.edu.tw

吳權勳
南臺科技大學資訊傳播學系
台南市永康區南台街一號
ma0f0206@stust.edu.tw

Chiuan-Shiun Wu
Department of Information and Communication, Southern Taiwan University of Science and Technology
No.1, Nantai St., Yongkang Dist., Tainan City 710, Taiwan (R.O.C.)
ma0f0206@stust.edu.tw

摘要

近年來，智慧型行動裝置發展快速，持有人口也逐年增加。科技的發展，相對提高了智慧型行動裝置的便利性，因此 SONY、Philips 及 Nokia 以非接觸式射頻識別（RFID）爲基礎共同開發出近端通訊。近端通訊的特點爲耗電量低、一次只和一台機器連結並且擁有較高的保密性與安全性，因此目前近端通訊的應用大都以門禁及付款爲主。本研究以線上遊戲帳號爲例，架構出一套以內建近端通訊功能的行動裝置結合 NFC Tag 的雙因素驗證機制。

隨著線上遊戲的盛行，遊戲裡面的虛擬寶物也漸漸被賦予實體的價值，因此也衍生出很多盜取帳號或虛擬寶物的案件。目前許多遊戲公司也開始提供雙因素身分驗證的機制，雖然提供的機制能讓遊戲帳號多一層的保護，但使用者可能要付出額外的驗證器材費用或是使用不夠人性化的驗證方式。本研究將線上遊戲帳號結合 NFC 手機及 NFC Tag，進行雙因素身分認證，使用者使用行動裝置靠近方便攜帶的 NFC Tag，經過驗證伺服器驗證後，再輸入遊戲帳號密碼，即可立即登入遊戲。

關鍵詞：近端通訊、線上遊戲、雙因素驗證

Abstract

With technology development, the number of users of smart mobile devices has also grown steadily in recent years. This is mainly due to the convenience offered by smart mobile devices. Based on the wireless non-contact Radio-Frequency Identification (RFID) technology, SONY, Philips, and Nokia jointly developed the Near-Field Communication (NFC) technology. NFC, characterized by lower power consumption, connectivity with one device at a time, and higher confidentiality and security, is mainly used in door access and payment applications. This study used online game and Telecom Based Micropayment as examples to develop a two-factor authentication mechanism for mobile devices built with NFC functionality.

With the increasing popularity of online games, virtual goods in the games have gradually been given a value like physical goods. Many problems such as account fraud and thievery of virtual goods have therefore derived. In the present, many gaming companies have used two-factor authentication of user identity. Although such mechanism offers additional protection of user accounts, the verification is not user-friendly enough, and extra cost of the verification device may be incurred. This study proposed to integrate online gaming accounts and NFC tags for two-factor authentication. Users only need to use their mobile device built with an NFC sensor to communicate with portable NFC tags for server authentication. Later, they can input their account and password to log into the game.

Keyword：Near Field Communication, Online Game, two-factor authentication, NFC

一、前言

根據資策會 MIC 的研究，2011 年全球遊戲人數超過 3 億人，產值約 600 億美元，其中線上遊戲佔 30%；而台灣電腦遊戲人數約爲 500 萬人，2011 年台灣線上遊戲產值約爲 159 億元，較 2010 年成長 4%，預估未來的成長率爲 4.8%[3]。由此可見，有越來越多的人沉浸在虛擬的世界裡，因此線上遊戲中的帳號及虛擬寶物在現實社會中也漸漸有了實體價值，形成新的交易市場[6]。因爲遊戲帳號跟虛擬寶物在現實中都有了價值，所以一些盜取帳號或虛擬寶物的案件也跟著發生。因此內政部警政署在 2011 年 7 月起，與網路業者合作「緊急封鎖被盜用帳號」機制，來阻止帳號遭盜用後衍生的網路詐欺犯罪行爲及損害；雖然這個機制讓網路犯罪發生數大幅下降，但根據內政部警政署統計，2012 年 1 至 10 月網路犯罪數爲 11712 件以「妨礙電腦使用」7282 件最多，詐欺居次[2]。行政院消費者保護會公開在 2011 年春節假期的消費爭議，其中以「線上遊戲爭議」的案件最多，其中糾紛內容又以帳號被鎖及寶物被盜較多[9]。由數據可以知道，國人在遊戲帳號安全的認知與保護還是稍嫌不足。

目前許多線上遊戲廠商爲了減少因遊戲帳號被盜而衍生出來的糾紛，都推出雙因素驗證的工具或功能，當玩家申請雙因素驗證服務後，遊戲帳號會立即鎖定，必須使用雙因素驗證工具，經過驗證伺服器驗證後，才能解除鎖定。目前遊戲廠商提供許多雙因素驗證的工具，例如需額外購買讀卡機及晶片卡的雙因素驗證或是需要購買動態密碼安全

卡的雙因素驗證，甚至提供手機或市話撥打免付費電話的雙因素驗證服務。而這些服務通常需要購買額外的驗證器材，或是需要撥打免付費電話才能進行帳號解鎖，在線上遊戲改版初期，免付費電話通常會是滿線的狀態，造成玩家因爲電話滿線，而無法登入遊戲。

近端通訊從 2004 年開始發展，NOKIA 於 2006 年推出第一支結合 NFC(Near Field Communication)功能的手機，因爲當時的應用比較貧乏，所以這個技術一直沒有受到青睞，直到 2011 年 Samsung 推出支援 NFC 的手機 Samsung Galaxy Nexus，並提供完整的 NFC 功能，讓使用者來開發 NFC 系統。近端通訊可以傳輸有價值的訊息、票卷或是進行小額付款等[12]，因此許多手機大廠也都推出支援 NFC 功能的手機，如 HTC 的 One 系列、SONY 的 XPERIA 系列以及 Samsung 的 Galaxy 系列。近年來，NFC 應用越來越廣泛，通常被用來行動付以及門禁等應用，例如中華電信在 2010 年台北國際花卉博覽會推出的「花珀」即是使用近端通訊技術傳輸使用者所想要瀏覽的資訊。

辜志雄(2012)發表的碩士論文—以整合性科技接受模式探討線上遊戲玩家對廠商提供之身分驗證機制滿意度之探討[8]，該研究分析統計玩家對六項線上遊戲驗證機制的滿意度。分析結果顯示，玩家對於只需要輸入帳號密碼的驗證機制滿意度最高，而使用智慧晶片卡與讀卡機的機制滿意度最低，顯示玩家還是偏向使用簡單的驗證機制。表一爲玩家對驗證機制的滿意程度之統計。

表一、玩家對驗證機制的滿意程度之統計

題項	樣本數	平均數	標準差	排名
1.玩線上遊戲只需輸入一組固定帳號與密碼登入，作爲驗證。	127	3.583	1.171	1
2.登入線上遊戲時，除須輸入一組固定帳號外，如果另須由遊戲廠商經手手機簡訊傳送一組一次性密碼，提供登入。	127	3.339	1.298	2
3.登入線上遊戲帳號時，如果另須將廠商販售的驗證卡片插入晶片讀卡機中，並輸入密碼。	127	2.795	1.311	6
4.如果線上遊戲會鎖定登入電腦的網路位置或是電腦硬體號碼，登入時除輸入帳密外，遊戲會自動辨認登入者電腦是否爲允許名單之中的電腦。	127	3.291	1.273	3
5.如果線上遊戲登入畫面會出現一組鍵盤，玩家使用滑鼠在鍵盤上進行點選輸入帳號密碼進行登入。	127	3.252	1.285	4
6.在輸入遊戲帳號後，還須對照遊戲所提供的亂數密碼卡，輸入對應的正確密碼，才能進行登入。	127	2.961	1.281	5

(資料來源：辜志雄，2012)

本文將遊戲帳號結合近端通訊系統，使用者只需要將近端通訊行動裝置靠近遊戲驗證專用的 NFC Tag，即可進行帳號解鎖，不僅讓使用者方便快速的解鎖帳號、減少花費在雙因素驗證工具的費用，也避免因爲線上遊戲改版初期，因爲免付費電話系統滿線，而玩家無法登入遊戲的窘境。在安全性方面，解鎖過程的資料傳輸皆使用對稱式金鑰做爲加密，在解鎖時限內，如果被有心人士重複登入，系統會立即凍結帳號，並傳送簡訊至使用者手機，提供一組解鎖序號，供使用者在遊戲官方網站進行解除凍結帳號及更改遊戲密碼，確保使用者的帳號安全。

二、文獻探討

2.1 近端通訊(Near Field Communication)

近端通訊(Near Field Communication；NFC)是一種短距離的無線通訊，以無線射頻識別(Radio Frequency Identification; RFID)爲基礎開發的技術[14][15]，讓電子設備透過無線連接，進行非接觸式點對點的資料傳輸[13][16]，在 10 公分的距離內，進行資料交換；此技術是由 SONY、Philips 及 Nokia 共同開發，並在 2004 年創立 NFC Forum，負責訂定 NFC 的協定與推廣等。近端通訊有主動以及被動兩種傳輸模式，傳輸速率爲 106 Kbps、212 Kbps 以及 424 Kbps 三種[10]，工作模式分爲三種[1][7]：

1. 裝置互連模式(Peer-to-Peer Mode)：將兩個具有 NFC 功能的裝置，進行無線連結，可在 10 公分的距離內進行資料交換，如名片交換，資料下載等。
2. 讀寫模式(Read/Write Mode)：讓具有 NFC 功能的裝置，成爲非接觸式的讀取器，藉由編輯程式的輔助，可讀取或編寫 NFC Tag 裡的資訊，如 NFC 電子海報。
3. 卡片模擬模式(Card Emulation Mode)：讓具有 NFC 功能的裝置成爲卡片模式，可藉由 NFC 非接觸式讀取器，進行讀取或編寫資訊，當 NFC 裝置成爲模擬卡片模式時，裝置不需供電也能進行工作。

近年來，NFC 被運用在各個領域裡，如付款、門禁管理或是倉庫管理，而 NFC 的應用類型大概可分爲以下四種[1][7]：

1. 接觸即通過(Touch and Go)：此類型通常使用卡片模擬模式，使用者的裝置裡存有通行碼或票卷做爲通關的驗證，不需供電，就能完成工作，常運用在門禁管理。
2. 接觸即支付(Touch and Pay)：爲目前最常見且討論最多的運用，將具有 NFC 功能的裝置靠近內崁 NFC 裝置的 POS 機，即可進行交易，如中華電信的 Hami 電子錢包。
3. 接觸即連接(Touch and Connect)：將兩個具有 NFC 功能的裝置互相靠近，即可透過無線進行連接，常運用在名片交換及傳輸檔案。
4. 接觸即瀏覽(Touch and Explore)：將具有 NFC 功能的裝置靠近 NFC 標籤來瀏覽標籤裡內存的各種訊息。

2.2 PlaySAFE 數位安全卡

PlaySAFE 數位安全卡是遊戲橘子數位科技公司與全景軟體公司在 2005 年合作推出的雙因素身分驗證工具，採用採用金鑰基礎建設(PKI，public key infrastructure)憑證技術的實體晶片卡，每一張卡片都擁有獨一無二的金鑰，且所有資料的傳輸都是經過加密的，持有正確金鑰才能解開資訊，當晶片卡被拆解時，線路也會自動燒毀，因此以現今的技術是無法以暴力破解或是複製。而且每張晶片卡都會搭配一組 PIN 碼，要同時竊取晶片卡及 PIN 碼的可能性極低。PlaySAFE 數位安全卡除了使用最高安全規格的 PKI 技術外，在資料的傳輸過程中也使用了 SSL 加密，同時驗證伺服器每次皆會回傳不同的 OTP 給晶片卡再次確認，因此，玩家如果沒有使用實體晶片卡，進行雙因素身分驗證，並無法進入遊戲。

2.3 OTP 動態密碼安全卡

OTP(One Time Password)動態密碼安全卡是遊戲橘子數位科技公司與歐柏系統公司合作共同導入的雙因素驗證工具，提供遊戲玩家一個安全的登入機制，避免玩家因爲遊戲端的電腦被植入木馬程式、間諜程式或鍵盤側錄程式等危害玩家遊戲帳號安全的不法程式，導致玩家的遊戲帳號密碼遭竊取。此機制導入的 Even-Based OTP 動態密碼系統，玩家使用離線式的專用讀卡機與晶片卡來產生 OTP 動態密碼，不需要在電腦上安裝任何的硬體驅動程式。當玩家要進行身分驗證時，利用讀卡機與晶片卡來產生 OTP 動態密碼，當需要產生 OTP 動態密碼時玩家需輸入晶片卡之 PIN 碼，且產生 OTP 動態密碼爲離線方式，讀卡機與晶片卡並無跟玩家電腦連結，因此駭客並無法利用網路產生 OTP 動態密碼。

2.4 IP 行動鎖

以網路卡 MAC address 作爲雙因素驗證的因素之一，使用者不需要購買額外的驗證工具，也不需要安裝其他的驗證軟體，透過簡單的步驟，讓玩家輕鬆保護自己的遊戲帳號安全。IP 行動鎖是藉由遊戲帳號綁定玩家電腦上的網路卡來保護玩家的遊戲帳號。雖然只有經註冊成功的電腦才有權限登入遊戲，可降低帳號被盜用的可能性，但是也限制了玩家進行遊戲的地點，並不能在網咖或朋友家的電腦上進行遊戲。

2.5 通訊安全鎖

通訊安全鎖是目前遊戲廠商最常建置的雙因素驗證工具，驗證方式爲玩家使用註冊的手機號碼或市內電話號碼做爲雙因素驗證的因素之一。玩家申請服務時可自行註冊 3 組個人手機或市內電話號碼做爲憑證，完成申請步驟後，所綁定的遊戲帳號立即凍結，當玩家要進行遊戲時，須先撥打通訊安全鎖開通專線，而且手機號碼不能設定爲隱藏，開通專線撥通後，玩家會聽見電話鈴聲 2 到 5 次，接著系統會自動掛斷來電，帳號也立即開通 100 秒，玩家可利用這 100 秒內登入遊戲，100 秒後，帳號會恢復成凍結狀態。若撥打電話不是註冊的電話，則系統會立即掛斷，帳號也不會開通。

2.6 Battle.net 手機驗證器

Battle.net 手機驗證器是網路遊戲公司暴風雪所開發，用來保護旗下網路遊戲的裝

置。驗證方式是透過手機驗證器隨機產生一組亂數數字代碼，與伺服器時間做校對。驗證器使用一套公開演算法的公式，結合代碼和系統的時間做運算後，得到一組驗證碼，運算出的驗證碼無法反推數字代碼，驗證碼也隨著時間不同，每 30 秒變換一次，且驗證碼使用一次或 3 分鐘後即失效。圖 2.9 爲 Battle.net 手機驗證器。

2.7 對稱式金鑰加密法

加密演算法或解密演算法使用一把相同的秘密金鑰，將明文做各種不同的取代或換位，且解密演算法必須是加密演算法的反向[5]。常見的演算法如 DES 以及 AES。

2.8 雙因素認證

雙因素認證(Two-Factor Authentication) 從密碼學的理論來說，有三個要素可供進行身份認證時使用[4]：

1. 使用者需記憶的認證內容：例如帳號密碼和通行碼等等。
2. 使用者擁有之特殊認證裝置：例如動態密碼卡(Token)、智慧卡(Smart Card)等等。
3. 使用者本身擁有的唯一生物特徵：例如指紋、瞳孔等等。

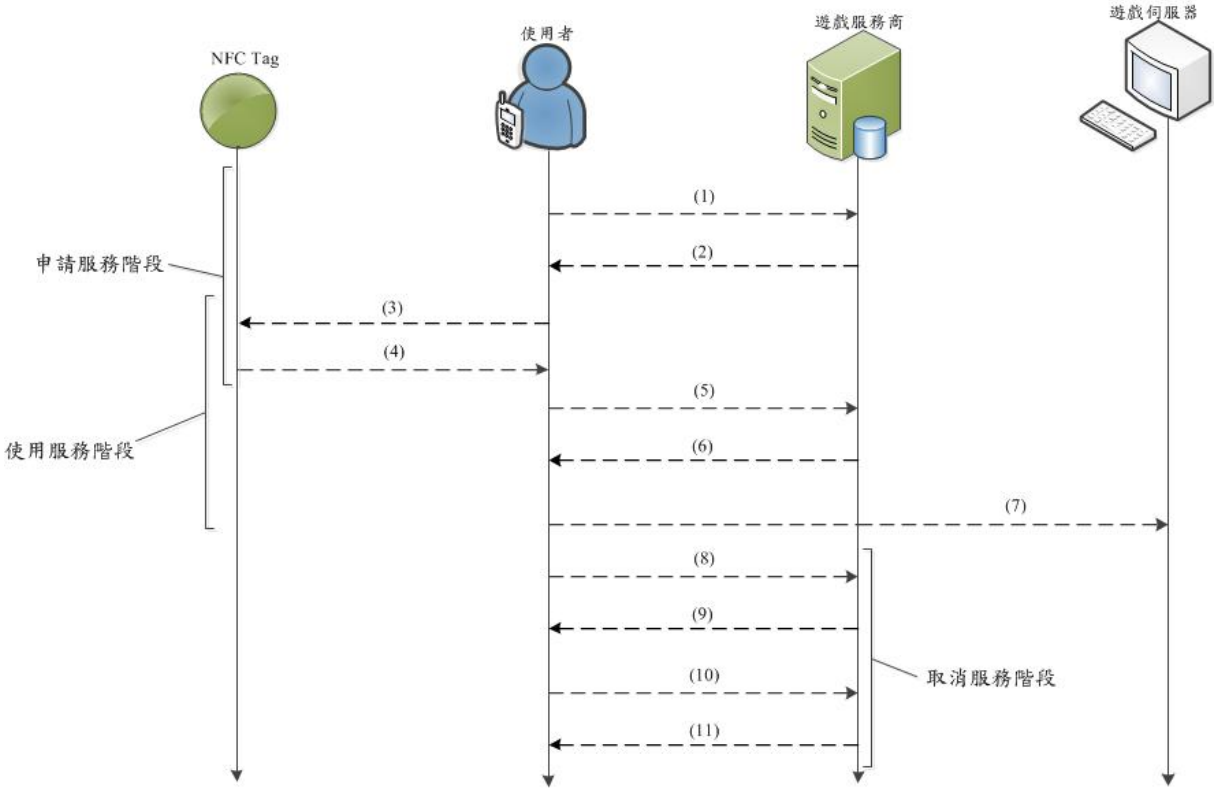
當使用者進行身分識別時，若同時使用三種要素中的其中兩種，就稱爲雙因素身份認證。例如網路 ATM 系統就是一種雙因素身份認證，使用者必須擁有金融卡及自己設定的密碼，才能進行交易。使用者使用網路 ATM 系統時，必須先插入金融卡作爲身份認證的第一個要素，再輸入使用者自行設定的密碼，作爲身份認證的第二個要素，當這兩個要素皆正確，使用者才能順利的使用服務。

只要是用作身分認證的裝置產品都可稱之爲 Token，而 Token 依形式區分大致可分爲下列三種：

1. Smart Card :又稱智慧卡，是指一種崁入積體電路的卡片，卡片包含了微處理器、I/O 介面及記憶體，可提供了資料的運算及儲存功能，例如，金融卡。
2. USB Token :使用時需與電腦系統連接，內建晶片及記憶體，進行身份認證程序。
3. Off-Line Token : Token 本身內含電池，不需要直接與電腦系統及應用程式相連接，由機身內建的晶片，來計算產生身份認證所需的 OTP。例如遊戲橘子聰明鎖及 Battle.net 驗證器[4]。

三、系統架構

目前許多線上遊戲廠商都推出自己的雙因素驗證方法及工具，但有些方法及工具需要額外的安裝或操作步驟才能進行雙因素驗證。本文提出的方法，需先購買產品包，產品包內附一組產品碼，使用者再至遊戲官方網站輸入產品碼申請服務，申請完畢後，只需要將 NFC 手機感應 NFC Tag 後即可解鎖。圖一爲系統流程圖。



圖一、系統流程圖

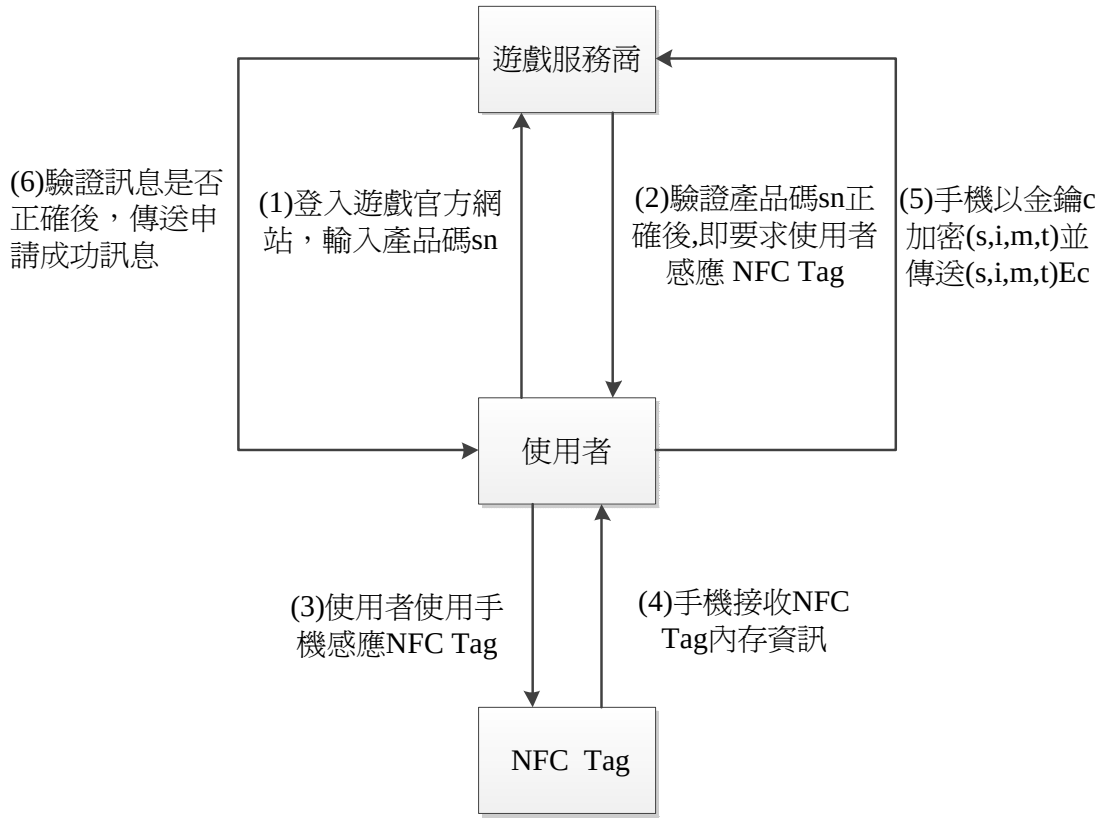
1. 使用者先至遊戲官方網站以遊戲帳號密碼登入遊戲帳戶，選取申請服務並輸入 NFC Tag 產品碼。
2. 遊戲服務商收到 NFC Tag 產品碼後，驗證 NFC Tag 產品碼的正確性，如正確即要求使用者一分鐘內感應 NFC Tag，反之，產品碼錯誤則跳回步驟一。
3. 使用者使用手機感應 NFC Tag。
4. 使用者手機讀取 NFC Tag 內存的通關序號及對稱式金鑰後，以對稱式金鑰加密通關序號、IMEI 碼、手機型號以及時戳，並發送至遊戲服務商。
5. 使用者手機傳送以對稱式金鑰加密過的通關序號、IMEI 碼、手機型號以及時戳至遊戲服務商。
6. 遊戲服務商以對稱式金鑰解密，驗證通關序號的正確性，如正確即傳送申請成功訊息至使用者端並記錄 IMEI 碼及手機型號作爲之後使用服務的驗證。
7. 當使用者使用服務時，需經過(3)(4)(5)流程後，遊戲服務商驗證通關序號、IMEI 碼以及手機型號的正確性，如正確即解鎖帳號 100 秒。
8. 當使用者要終止服務時，以遊戲帳號密碼登入遊戲帳戶，選取終止服務。
9. 遊戲服務商以簡訊傳送終止序號至使用者手機。
10. 使用者在遊戲服務商規定的頁面中輸入終止序號。
11. 遊戲服務商驗證終止序號的正確性，如正確即終止服務，並發送終止成功訊息至使用者端，反之，如終止序號輸入錯誤，則跳回步驟 10。

表二、符號表

符號	代表意義	符號	代表意義
c	金鑰	i	IMEI 碼
m	手機型號	e	終止序號
s	通關序號	t	時戳
Ec(x)	以金鑰 c 加密資訊 x	sn	產品碼

3.1 服務申請階段

使用者購買 NFC Tag 產品包後，取得產品包內附的產品碼 sn，再至遊戲官方網站以帳號密碼登入遊戲帳戶，選取服務申請後，輸入產品碼 sn，遊戲服務商驗證產品碼 sn 的正確性後，要求使用者一分鐘內使用手機感應 NFC Tag。使用者依照指示使用手機感應 NFC Tag 後，手機接收到 NFC Tag 裡面內存的金鑰 c 以及通關序號 s 後，以金鑰 c 加密通關序號 s、IMEI 碼 i、手機型號 m 以及時戳 t 並發送至遊戲供應商，遊戲供應商收到訊息後，以金鑰 c 解密，驗證通關序號 s 的正確性，如正確即發送申請成功訊息至使用者端並記錄 i 及 m 作爲之後使用服務的驗證。服務申請流程如圖二所示：



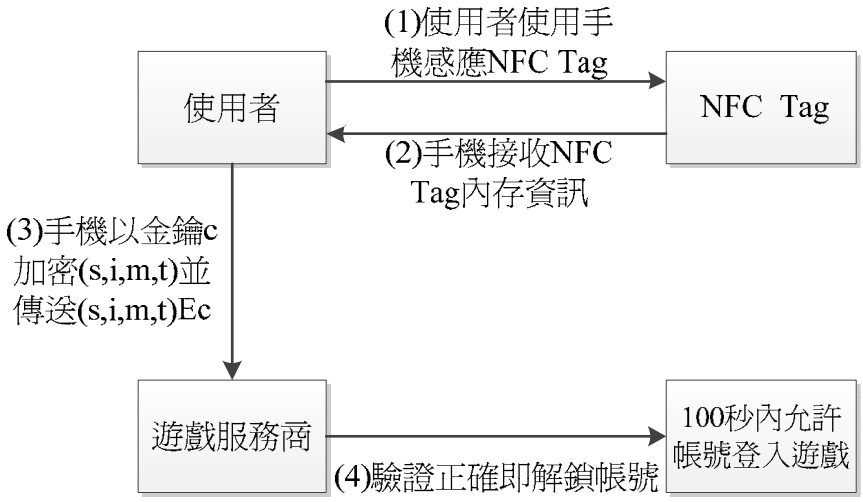
圖二、服務申請階段

1. 使用者先至遊戲官方網站以遊戲帳號密碼登入帳戶，並選取註冊 NFC Tag 服務後，輸入產品碼 sn，sn 爲產品碼，附在產品包裝內並以銀漆保護。每一組產品碼皆有一組相對應金鑰。

2. 遊戲服務商收到產品碼 sn，驗證產品碼 sn 的正確性，如果正確即要求使用者在一分鐘內使用手機感應 NFC Tag，反之，如產品碼 sn 輸入錯誤，則跳回步驟一。
3. 使用者使用手機感應 NFC Tag。
4. 手機讀取 NFC Tag 內存的通關序號 s 及對稱式金鑰 c 後，以金鑰 c 加密通關序號 s、IMEI 碼 i、手機型號 m 以及時戳 t 並發送至遊戲服務商。金鑰 c 以及驗證序號 s 的資訊是儲存在 NFC Tag 裡面。
5. 使用者傳送(s,i,m,t)Ec 至遊戲服務商。
6. 遊戲服務商以金鑰 c 解密，驗證通關序號 s 的正確性，如正確即傳送註冊成功訊息至使用者端並記錄 IMEI 碼 i 及手機型號 m 作爲之後使用服務的驗證。

3.2 服務使用階段

使用者已經申請服務，並要進行遊戲時，需將 NFC 手機感應 NFC Tag，讀取 NFC Tag 內存的通關序號 s 及對稱式金鑰 c 後，以 NFC Tag 內存的金鑰 c 加密通關序號 s、IMEI 碼 i、手機型號 m 以及時戳 t 並發送至遊戲供應商。遊戲供應商收到訊息後，以金鑰 c 解密，驗證通關序號 s、IMEI 碼 i 以及手機型號 m 的正確性，皆正確則解鎖帳號，在一百秒內允許使用者帳號登入遊戲。服務使用流程如圖三所示：

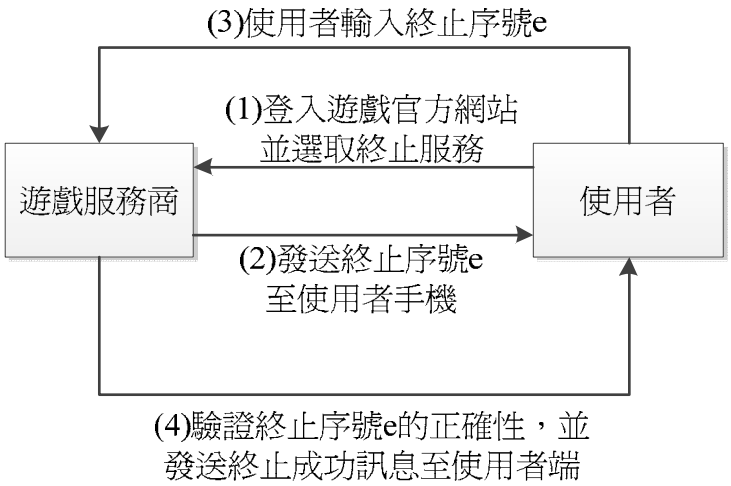


圖三、服務使用階段

1. 使用者已經完成帳號綁定作業，欲使用 NFC Tag 進行雙因素驗證時，需使用 NFC 手機感應 NFC Tag。
2. NFC 手機讀取 NFC Tag 內存的通關序號 s 及對稱式金鑰 c 後，以金鑰 c 加密通關序號 s、IMEI 碼 i、手機型號 m 以及時戳 t 並發送至遊戲供應商。
3. 使用者手機以金鑰 c 加密(s,i,m,t)並傳送(s,i,m,t)Ec 至遊戲服務商。
4. 遊戲服務商以金鑰 c 解密，驗證通關序號 s、IMEI 碼 i 以及手機型號 m 是否正確，如果正確則允許使用者一百秒內使用遊戲帳號密碼登入遊戲伺服器。

3.3 服務終止階段

當使用者遺失 NFC Tag 或是損壞時，可至遊戲官方網站進行服務終止；使用者需先至遊戲官方網站輸入遊戲帳號密碼登入遊戲帳戶，選取 NFC Tag 服務終止後，遊戲服務商會傳送終止序號 e 至使用者手機，使用者在遊戲服務商規定的頁面輸入終止序號 e 後，遊戲服務商立即驗證終止序號 e 的正確性，如正確即終止服務並發送終止服務成功訊息至使用者端，反之，如終止序號錯誤，則發送失敗訊息。服務終止流程如圖四所示：



圖四、服務終止階段

1. 使用者先至遊戲官方網站登入遊戲帳戶，並選取 NFC Tag 服務終止。
2. 收到終止服務訊息後，遊戲服務商以簡訊發送終止序號 e 至使用者手機。
3. 使用者在遊戲官方網站規定的頁面中輸入終止序號 e。
4. 遊戲服務商驗證終止序號 e 的正確性，如正確即取消服務並發送取消服務成功訊息至使用者端，反之，如終止序號錯誤，則發送失敗訊息並跳回步驟 3。

四、分析與比較

在此節中，我們將討論與比較目前的雙因素驗證機制與本文提出的方法的差異，本文目的是讓使用者在雙因素身分驗證的機制有多一種的選擇，使用者可依照自己的喜好跟設備，選擇適合的雙因素驗證方式，因此我們假設使用者已經有 NFC 手機及手機門號採用無限上網方案。表三說明了本文提出的架構與目前的雙因素驗證機制之比較。

根據表三的比較，得到以下的結論：

1. 智慧安全卡因爲使用讀卡機及智慧安全卡作爲驗證工具，且需要安裝讀卡機及晶片卡的驅動程式，故在機動性方面是比較低的。而 IP 簡訊鎖是以網路卡 MAC address 作爲雙因素驗證的因素之一，使用者只能使用綁定 IP 的電腦進行遊戲，無法在網咖等其他地方進行遊戲，故機動性最低。而本文所提出的方法，是以使用者自行擁有的 NFC 手機爲媒介，搭配攜帶方便的 NFC Tag 即可進行遊戲帳號解鎖，故機動性是高的。
2. 智慧晶片卡及動態密碼卡皆需要高成本的驗證器材費用，因此廠商成本高，而通訊安全鎖雖然不用負擔高成本的驗證器材費用，但在設備建置費及通信費

上，需要較多的費用，故廠商成本高。本文提出的方法，廠商負擔 NFC Tag 的成本比智慧晶片卡及動態密碼卡的成本是較低的，而且也不需要負擔通信費，因此本文提出的方法，廠商成本低。

3. 目前智慧晶片卡，使用者需負擔的費用是 300 元以內，而動態密碼卡需負擔的費用是 300 元~600 元不等，而本文提出的方法，是假設使用者已經有 NFC 手機及手機門號採用無限上網方案，故只需要負擔 NFC Tag 百元以內的費用。
4. 雙因素驗證另一個風險就是在解鎖時限內，是否會遭到不明人士輸入使用者的帳號密碼重複登入。在 PLAYSAFE 數位安全卡中，使用者須使用讀卡機插入帳號綁定的 PLAYSAFE 數位安全卡，在輸入帳號以及設定的 PIN 碼，而 PIN 碼不會傳送到遊戲橘子做驗證，而是與 PLAYSAFE 數位安全卡進行驗證，驗證資料會經安全卡加密處理後，產生交易驗證碼，再傳送至遊戲橘子，且每次交易驗證碼均以動態方式產生，所以並無法複製安全卡，登入遊戲後即可拔出安全卡，帳號立即鎖定，並無重複登入問題。Battle.net 通訊安全鎖，雖然用綁定帳號的行動電話或市話撥打 0800 免付費專線，但在解鎖後的 100 秒內，使用者在遊戲內仍然可以被重複登入，這可能會危害使用者的帳號安全。本文提出的方法在資料的傳輸中皆使用對稱式金鑰加密，而在解鎖帳號的 100 秒內，如果重複登入會直接鎖定帳號並發送一組解鎖序號給使用者所註冊的手機，使用者只要在遊戲官方網站輸入這組序號並更改遊戲密碼，即可解除，而這組解鎖序號在解鎖後立即失效。
5. 在安全性方面，智慧安全卡除了使用最高安全規格的 PKI 技術外，在資料的傳輸過程中也使用了 SSL 加密，因此安全性爲最高。通訊安全鎖在使用者撥打帳號解鎖專線後，立即解鎖帳號 100 秒，但這 100 秒內可進行重複登入，並且造成原本已經登入遊戲的使用者斷線，造成使用者的損失，因此安全性比其他驗證方法較低。而本文提出的方法，資料傳輸使用對稱式金鑰加密，可避免解鎖資訊被有心人士複製，在重複登入方面，如果使用者在解鎖的 100 秒內被重複登入，系統會立即鎖定此帳號，並發送簡訊至使用者註冊的手機，提供解鎖序號，並要求使用者更改密碼，因此本文提出的方法，可讓使用者的遊戲帳號密碼受到更嚴密的保護。
6. 本文使用以近端通訊系統爲基礎的線上遊戲帳號驗證機制，在需要額外裝置進行雙因素驗證的情況下，本文提出的方法只需要在登入前，利用 NFC 手機感應 NFC Tag，NFC 手機即自動完成雙因素驗證的動作。如果在網路咖啡廳或其他電腦進行驗證時，其他的驗證方式，可能要攜帶讀卡機、安全卡等，可能會造成使用者的不便，而本文提出的方法只需要攜帶 NFC Tag 以及手機即可，可大大提升再次驗證的便利性。

五、結論

在本篇文章中，我們提出結合近端通訊系統之線上遊戲帳號驗證機制，透過 NFC Tag 裡面的金鑰、通關序號、手機 IMEI 碼以及手機型號做爲線上遊戲帳號之雙因素驗證的驗證憑證。使用者須先購買 NFC Tag 產品包，產品包內附一組產品碼，使用者再至遊戲

官方網站輸入產品碼申請服務，當要進行遊戲時，使用者只需將 NFC 手機在 NFC Tag 附近輕輕一晃，即可驅動手機以金鑰加密驗證資訊並傳送至遊戲服務商，驗證資訊包含通關序號、手機 IMEI 碼以及手機型號，手機遊戲服務商收到資訊，以金鑰解密後，驗證通關序號、手機 IMEI 碼以及手機型號是否正確，皆正確則立即解鎖帳號 100 秒，在這 100 秒內，如果遊戲帳號被重複登入，系統則會鎖定此帳號，並發送簡訊至使用者註冊的手機，並提供解鎖序號，使用者在遊戲官方網頁輸入解鎖序號並更改密碼後，即可解鎖，進行遊戲。本文提出的方法，是假設使用者已經有 NFC 手機及手機門號採用無限上網方案，因此只需要花少許的費用，就能讓線上遊戲帳號的安全更加安全，也減少使用者操作手機或其他驗證工具的步驟，讓使用者在帳號安全上有多一種的選擇。

表三、線上遊戲帳號驗證方式比較表

產品 比較	本文提出的 方法	智慧 晶片卡	動態 密碼卡	通訊 安全鎖	IP 行動鎖
機動性	高	低	高	高	最低
廠商成本	中	高	高	高	低
玩家負擔	百元以內	約數百元	約數百元	免費	免費
重複登入	不可	不可	不可	可	不可
安全性	高	最高	高	中	高

參考文獻

[1] 王建森，2012，“近端通訊之行動付費系統應用於智慧型行動裝置”，朝陽科技大學資訊工程系碩士論文。

[2] 內政部警政署，2012，“警政統計通報第46號”，2012年11月14日。

[3] 周樹林，2012，“數位遊戲產業發展趨勢”，MIC產業顧問學院學院專欄。

[4] 李武昌，2007，“植基於開放源碼軟體之雙因素認證系統之研究”，靜宜大學資訊管理學院碩士論文。

[5] 李南逸、王智弘、林峻立、張智超、溫翔安、葉禾田譯，Behrouz A. Forouzan著，2008，“*網路安全與密碼學概論*”，台北，美商麥格羅・希爾。

[6] 柯巧心、陳巧珮、陳志誠，2010，“線上遊戲犯罪模式分析之實證研究”，中央警察大學『資訊、科技與社會』學報，第十卷，第二期。

[7] 張智程，2010，“使用 NFC 手機建置校園應用資訊系統”，國立暨南國際大學資訊管理研究所碩士論文。

[8] 辜志雄，2012，“以整合性科技接受模式探討線上遊戲玩家對廠商提供之身分驗證機制滿意度之探討”，大同大學資訊經營研究所碩士論文。

[9] 楊久瑩，2012，“春節消費爭議 線上遊戲居首位”，自由時報電子報，2012年2月24日。

[10] Curran, K., Millar, A. and Garvey, C. M.：“Near Field Communication,”*International Journal of Electrical and Computer Engineering,* 2012, pp.371~382.

[11] Ghosal, P., Biswas, M. and Biswas, M.：“A Compact FPGA Implementation of Triple-DES Encryption System with IP Core Generation and On-Chip Verification,” *International Conference on Industrial Engineering and Operations Management*, 2010.

[12] Haselsteiner, E. and Breitfuß, K.：“Security in near field communication (NFC),” *Workshop on RFID Security RFIDSec* , 2006.

[13] Massoth, M. and Bingel, T.：“Performance of different mobile payment service concepts compared with a NFC-based solution,” *Fourth International Conference on Internet and Web Applications and Services*, 2009, pp.205~210.

[14] Ondrus, J. and Pigneur, Y.：“An assessment of NFC future mobile payment systems,” *International Conference on the Management of Mobile Business*, 2007, pp.43~49.

[15] Paills, J. C., Gaber, C., Alimi, V. and Pasquet, M.： “Payment and privacy: A key for the development of NFC mobile,” *International Symposium on Collaborative Technologies and Systems*, 2010, pp. 378~385.

[16] Pasquet, M., Reynaud, J. and Rosenberger C.：“Secure payment with NFC mobile phone in the SmartTouch project,”*International Symposium on Collaborative Technologies and Systems*, 2008, pp.121~126.

48 結合近端通訊系統之線上遊戲帳號驗證機制