具身份保護之違法事件線上舉報系統

施再繁
朝陽科技大學副教授
e-mail：
tfshih@cyut.edu.tw

許博硯
朝陽科技大學研究生
e-mail：
charlie23567@gmail.com

摘要

現今社會充斥不法行為，其中食安問題應是最熱門的議題，例如：近幾年的毒牛奶、毒麵粉、毒豆干、…等各種有毒食物案件層出不窮，而剛被揭發的「毒油事件」更是震撼人心，大多數人雖心有不滿與想正義的挺身向政府單位舉發，但隨著社會的變遷，在充滿病態的社會結構，到頭來人們常害怕因舉發不法事件而影響自身安全，最後總是向現實低頭放棄舉報的想法，在惡性循環下，不法事件始終得不到有效的遏止，因此激勵我們設計一個適用於各種違規、不法事件的舉報系統，以達成檢舉人的隱私與安全獲得保障，可放心檢舉不法、安心領獎勵金，又不濫用此系統之方便性，進行謊報為害他人與擾亂承辦單位之行政。

關鍵詞：自然人憑證、公鑰、私鑰、加密、傳輸層安全協議(SSL)。

Abstract

Recently, social crime is rampant, and amongst all that come to focus is the issue about food security. In recent years, poisoned milk powder, poisoned flour and poisoned dried tofu are the most representative examples of such endless toxic food events. And the recent poisoned oil event was particularly shocking. Most people would want to come forward against such corrupted corporations and its product to send a message of anger to the government. But as social changes with its structure in an ill fashion, people started to be afraid of the consequences that might affect their own safety reporting the illegal activities. As a result, people tend to give up the fight against the misconduct of the corporations, and ending up with a vicious circle that the justice can never be upheld. In light of the situation, we are motivated to design a system that can process various reports of illegal activities, and ensure safety, security, anonymity and convenience of the user. The system is designed to be robust to abusive use, and is able to preclude false reports.

Keywords: Citizen Digital Certificate, Public key, Private key, Encryption, Secure Sockets Layer (SSL).

1. 前言

現今社會犯罪不法行為氾濫，其中食安問題是最熱門的議題，例如：近幾年的毒牛奶、毒麵粉、毒豆干…各種有毒食物事件層出不窮，尤其最近的「毒油事件」更是震撼人心，大多數人雖心懷不滿想挺身舉發，但人們常害怕因舉發不法事件而使自己的人身安全受到威脅，最後總是向現實低頭並打消舉報的念頭，只能視而不見讓不法行為持續存在，默默承受為害，即使民眾有勇氣向相關單位舉發不法，也常因外力介入而發生吃案或拖延審理，讓案件石沉大海不了了之，在惡性循環下，不法事件始終得不到有效的遏止。近期「毒油事件」的檢舉人，先是被吃案，再者檢舉成功後又受盡恐嚇，乃因檢舉獲得獎勵，又因高額獎勵金曝光，再次受到各種不肖份子之覬覦與恐嚇，凡此種種威脅勢力的壓迫，若非有毅志和膽識過人早就放棄，讓為害者繼續存在與傷害所有人。有鑑於近期的「黑油」影響眾人健康、「違建」大火葬送許多無辜生命，讓我們深知不能再縱容不法事件，更激勵我們設計一個適用於各種違規以及不法事件之安全、有效的線上舉報系統，達成如電子公文依法限期回覆與處理之功效，使舉報流程更簡單、快速且安全，讓檢舉人的隱私獲得充份保障，安心地檢舉不法行為與領取獎勵金，此外，此系統可有效防止惡意濫用系統進行謊報，為害他人與擾亂承辦單位行政之情事發生。

為了確保舉報者的安全，讓舉報者的身分受到高度保護，此系統採用電子憑證驗證技術，達成資料的完整性、私密性與不可偽造之目標與保障，進行身份驗證與確認，透過網路

進行線上舉報作業流程，不但功效高且成本低，對承辦人而言，無法得知舉報者的真實身份，讓舉發者身分獲得完全保密，若屬於有獎勵金之案件，一旦舉發成功，將可以透過多把聯合確認舉發者身份的鑰匙，進行舉發者之身份確認，而頒發應得的獎金給舉發者，透過此多鑰匙聯合確認的機制，可防止單一人士即能惡意查詢舉發者身份之風險，藉以提高舉報者人身安全的保障，避免舉報者受到威脅，降低不肖人士之犯罪動機，透過此系統之建置，可望促進舉報人更勇於舉發不當行為，讓人人更守法並促進眾人的生活品質。

2. 方法

我們設計的電子憑證身份認證線上舉報平台預期可達成下列功能：避免因身份曝光人身安全遭受威脅的情況、線上自動發放獎金給舉報者，以保護舉報者身份與權益、線上舉發視同電子公文處理可防止吃案情事。平台使用分類為：舉報、承辦、上層審核。舉報人如果要使用該平台進行舉報，必須先上平台進行帳號註冊，註冊時會員必需持有電子憑證，在此論文中，我們選擇採用內政部的自然人憑卡，註冊時也將填寫銀行帳戶等個人資料，一旦完成註冊即可登入系統進行舉發或其他作業，此系統最大的特色是只會將舉報事件的內容傳送給相關承辦單位，不會洩漏舉報者的身分。

承辦單位收件後，進行查證，如果真的有違規，系統將會向上呈報至共同持有金鑰成員，進行二次確認，系統經過金鑰成員們確認屬實後，系統將通知約定之金融單位自動匯撥獎金至舉報者帳戶。

系統因避免執法人員吃案或不偵辦，當承辦單位判定承辦的違規事件為未屬實時，將會自動通知上層審核端，由上層長官們再次審查該事件是否重新偵辦。

本節將一一介紹平台各部分的運作流程與驗證機制，而文中所使用的相關符號及說明如表 1 所示。

表 1 符號表

符號	說明
U_i	平台使用者 i 可分為三類： 舉報者(Informer) 承辦人(Promoter) 上司(Superior)
I_i	舉報者(Informer)
P_i	承辦人(Promoter)
S_i	上司(Superior)
$Server_{IN}$	舉報平台伺服器
$Server_{CA}$	MOICA 憑證驗證伺服器
$Cash$	金流平台(Cash Flow Platform)
ID_i	舉報系統之登入帳戶
PW_i	舉報系統之登入密碼
$E(x)$	將 x 加密
$D(x)$	將 x 解密
D_i	註冊資料(如: 匯款帳戶等)
$Salt$	亂數
ID_NO	自然人憑證卡所存身分證後四碼
SN_i	自然人憑證卡之序號
$X \rightarrow Y$	表示從 X 傳送訊息到 Y [5]
MSC_i	驗證自然人憑證之回傳資訊
$Bank\_ACC$	匯款帳戶
OK_i	上司回傳之事件確認回覆訊息

2.1 註冊流程與驗證機制

使用者初次使用舉報平台必須先進行註冊，其主要步驟說明如(1)~(4)，圖 1 為註冊流程示意圖。

(1) 使用者 U_i 至舉報平台入口網站填寫資料，並插入自然人憑證卡輸入 PIN 碼進行註冊。

(2) 將由自然人憑證驗證伺服器 $Server_{CA}$ 對該使用者自然人憑證卡進行驗證。

(3) 自然人憑證驗證伺服器 $Server_{CA}$ 傳送驗證後的結果至舉報平台伺服器 $Server_{IN}$。

(4) 當舉報平台伺服器 $Server_{IN}$ 收到驗證的結果，若是該憑證有效，舉報平台伺服器將該使用者填寫的資料存放至資料庫，即可完成註冊程序。

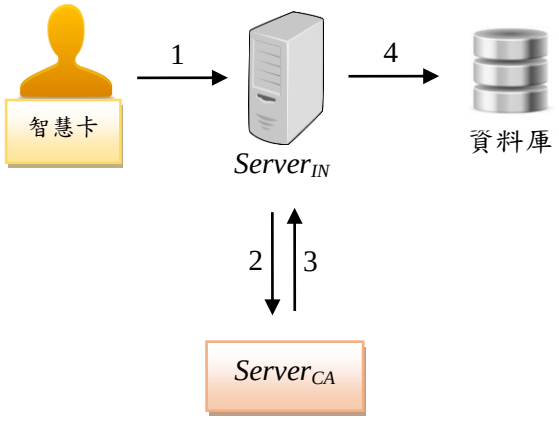

圖 1 註冊流程

下列步驟(1)~(4)將詳細說明註冊流程，而使用者與伺服器之間的驗證機制如圖 2 所示。

(1) U_i → $Server_{IN}$
使用者 U_i 首次使用系統時，必須先進行註冊，填寫註冊相關基本資料(ID_i, PW_i, D_i, SN_i)，其中 ID_i, PW_i, D_i, SN_i 分代表使用者 U_i 之帳號、密碼、個人資料、自然人憑證卡序號，填寫完成後，會將所填寫的資料 ID_i, PW_i, D_i, SN_i 傳送至舉報平台伺服器 $Server_{IN}$ 進行下一步處理。

(2) $Server_{IN}$ → $Server_{CA}$
$Server_{IN}$ 接收到 U_i 傳送過來的 ID_i, PW_i, D_i, SN_i 後，$Server_{IN}$ 會將其中的 SN_i 透過自然人憑證管理中心伺服器 $Server_{CA}$ 的 OSCP 服務，驗證此 SN_i 憑證是否有效。

(3) $Server_{CA}$ → $Server_{IN}$
$Server_{CA}$ 將驗證結果 MSC_i 回傳至 $Server_{IN}$。

(4) $Server_{IN}$
當 $Server_{IN}$ 接收到自然人憑證驗證伺服器 $Server_{CA}$ 回傳的 MSC_i 後，可據以判斷憑證是否有效。若是憑證有效，則表示 U_i 為合法的使用者，$Server_{IN}$ 即會將使用者 U_i 填寫的 D_i 及 PW_i 加密並寫入資料庫。PW_i 加密處理方式如公式(1)，使用 MD5 和 SHA 並加入 *Salt* 增強密碼的強度；另外，會利用公式(2)以 $Server_{IN}$ 的金鑰將使用者 U_i 的 D_i 加密。

$$E(PW_i||Salt)=\text{MD5}(\text{SHA}(Salt+PWi)) \quad (1)$$

$$E(D_i)=\text{MD5}(D_i) \quad (2)$$

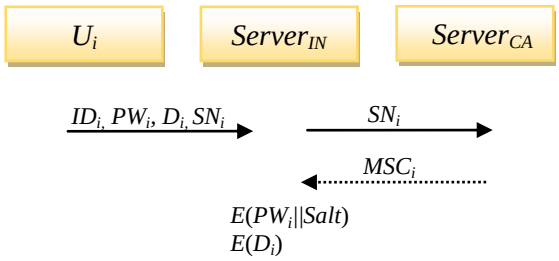

圖 2 註冊驗證

2.2 登入舉報流程與驗證機制

(1)~(6)為舉報者 U_i 登入舉報平台進行舉報之步驟，圖 3 則為舉報平台之登入及舉報運作流程。

(1) 於登入階段，使用者 U_i 至該平台輸入帳號、密碼，由伺服器進行驗證是否為合法的使用者。

(2) 若帳號、密碼經舉報平台伺服器 $Server_{IN}$ 驗證成功，舉報平台伺服器將透過自然人憑證驗證伺服器 $Server_{CA}$ 驗證該使用者 U_i 自然人憑證卡是否有效。

(3) 自然人憑證驗證伺服器將驗證結果傳送至 $Server_{IN}$。

(4) 當舉報平台伺服器收到 $Server_{CA}$ 回傳的驗證結果後，若是身分正確，$Server_{IN}$ 將允許使用者登入系統進行後續作業。

(5) 舉報者 I_i 即可進行舉報、查看歷史事件及變更資料等相關作業。

(6) 舉報平台伺服器會將舉報者所傳送過來的資料存入資料庫中。

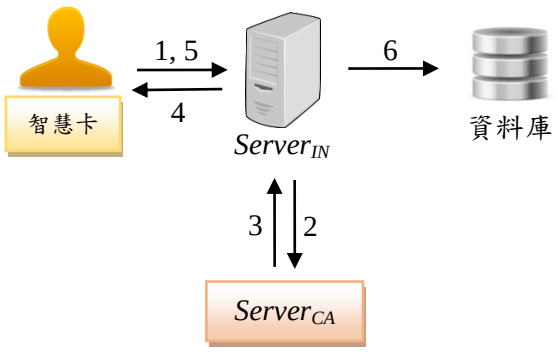

圖 3 登入及舉報流程

下面步驟(1)~(4)，將詳細說明使用者登入平台之身分驗證機制，其運作如圖 4 所示。

(1) U_i → $Server_{IN}$
當舉報平台伺服器收到 U_i 傳送輸入的 ID_i 和 PW_i，會將使用者 U_i 的 PW_i 使用系統的金鑰以加密公式 $E(PW_i||Salt)$進行加密，接著將加密後的 ID_i 及 PW_i 與存放於資料庫的資料進行比對，若是相符，$Server_{IN}$ 將要求 U_i 插入自然人憑證卡，並透過自然人憑證驗證伺服器 $Server_{CA}$ 驗證 U_i 憑證。
接著會驗證 PIN 碼是否正確，若正確，則透過 MOICA 所提供的 LDAP 協定取得使用者 U_i 卡片裡的 SN_i [3]。

(2) $Server_{IN}$ → $Server_{CA}$
$Server_{IN}$ 將取得的 SN_i，透過 OSCP 驗證該憑證有效性。

(3) $Server_{CA}$ → $Server_{IN}$
經 $Server_{CA}$ 驗證 U_i 身分後，如果為合法的使用者，則將 U_i 的憑證資訊 MSC_i 傳送至 $Server_{IN}$，若 $Server_{IN}$ 收到此人身分合法的驗證結果，則會將先前透過 LDAP 取得的身份證後四碼(ID_NO)與資料庫所存放的資料進行比對，若比對成功，才可允許登入系統[2] [6]。

(4) $Server_{IN}$ → U_i
$Server_{IN}$ 比對後若是帳號身份相符，則可允許使用者 U_i 登入系統。

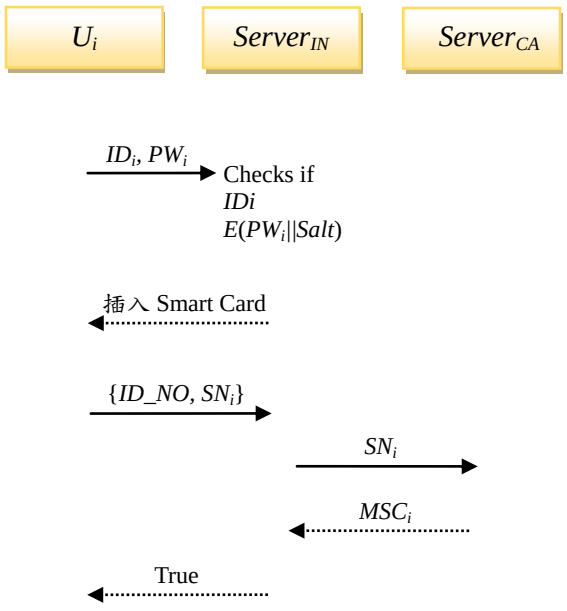

圖 4 登入驗證

2.3 舉報事件審核流程

經 $Server_{IN}$ 確認舉報者 I_i 身分後，即可填寫違規事件，當事件填寫完畢送出，$Server_{IN}$ 只傳送該事件內容及相關文件至 $Server_{IN}$ 並通知承辦人 P_i，並不會傳送 I_i 身分相關資料，由於 $Server_{IN}$ 先前已對該使用者的自然人憑證卡及身分進行認證，故可確定其為合法使用者。

當 P_i 收到違規案件，P_i 可依照審核結果來判定發放獎金或濫用系統與否。

2.4 獎金審核及發放流程與驗證機制

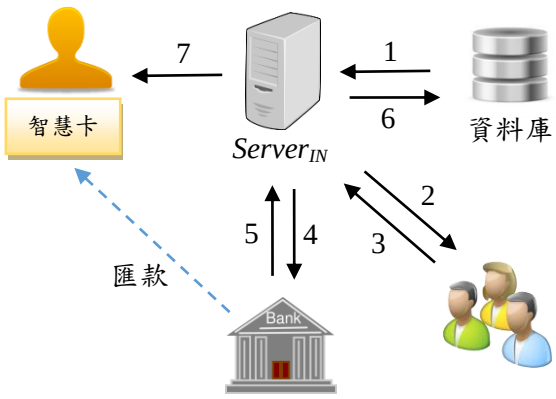

圖 5 獎金審核及發放流程

獎金審核及發放流程如圖 5 所示，下面步驟(1)~(7)，將詳細說明其運作流程。

(1) 若經承辦人 P_i 調查後，確認該案件之調查結果屬實且為有獎金的獎勵案，接下來將進行獎金發放審核，承辦人只需按下【獎金發放審核】按鈕，即可將審核事件送給上層審核者，此後即進入審核流程。

(2) 舉報平台伺服器 $Server_{IN}$ 將通知上司 S_i 們進行獎金核發確認。

(3) 在審查完畢後，若所有上司 S_i 們確認案件應予以核發獎金，只需按下【確認】按鈕即可核准獎金發放作業。

(4) 當舉報平台伺服器收到所有上司核准獎金發放確認訊息後，$Server_{IN}$ 將通知金流平台 *Cash* 進行匯款。

(5) 金流平台匯款完成後會通知舉報平台伺服器已完成匯款。

(6) 當舉報平台伺服器收穫金流平台匯款完成通知後，將通知承辦人 P_i 已完成匯款並標示結案。

(7) 舉報平台伺服器發送 E-MAIL 通知舉報者 I_i 已獲的獎金。

以下步驟(1)~(2)為所有上司$\{S_1, S_2, \ldots, S_i\}$審核案件獎金核發之流程，其驗證機制如圖 6 所示。步驟(3)~ (5)則為系統發放獎金的流程，圖 7 為其驗證機制。

(1) $Server_{IN} \rightarrow S_i$
當 $Server_{IN}$ 收到 P_i 調查結果需核發獎金後，$Server_{IN}$ 將傳送該案件至 S_i 再次確認。

(2) $S_i \rightarrow Server_{IN}$
若 $Server_{IN}$ 收到 OK_1，則表示 S_1 已確認過案件，當 $Server_{IN}$ 收到$\{OK_1, OK_2, \ldots, OK_i\}$表示$\{S_1, S_2, \ldots, S_i\}$已確認過該案件，此時 $Server_{IN}$ 將啟動獎金發放機制。

(3) $Server_{IN} \rightarrow Cash$
$Server_{IN}$ 將使用系統金鑰，利用公式 $D(D_i)$ 解密得到舉報者 I_i 的匯款帳號 $Bank\_ACC$，$Server_{IN}$ 將 $Bank\_ACC$ 及舉報獎勵金額傳送至金流平台 $Cash$ 進行匯款作業。

(4) $Cash \rightarrow Server_{IN}$
金流平台匯款完成後，將傳送回覆訊息通知 $Server_{IN}$ 匯款完成，並修改該案件之處理狀態為已匯款完成並結案。

(5) $Server_{IN} \rightarrow I_i$
$Server_{IN}$ 將會發送 E-MAIL 通知舉報者 I_i 獎勵金已匯入其帳戶。

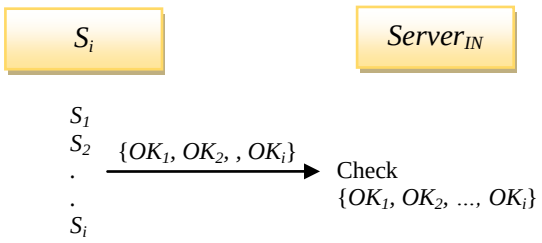

圖 6 獎金審核驗證機制

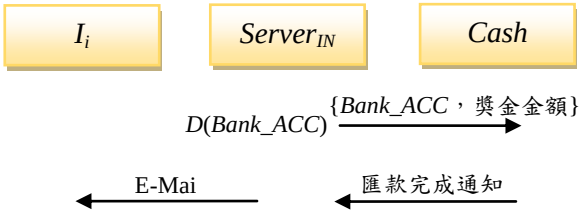

圖 7 獎金發放驗證機制

2.5 濫用系統之判定與懲罰

以下將介紹上司們如何再次確認承辦人員初步判定為濫用案件是否真的歸為濫用案件處置，其程序如圖 8 所示，步驟說明如下：

(1) 經由承辦人 P_i 查詢後，若認定該案件為濫用系統，即可按下【濫用系統審核】按鈕，將重新審核通知送至舉報平台伺服器 $Server_{IN}$ 由上司們再進一步審核。

(2) 伺服器 $Server_{IN}$ 將通知上司$\{S_1, S_2, \ldots, S_i\}$，再次進行確認該案件是否為濫用事件。

(3) 上司$\{S_1, S_2, \ldots, S_i\}$將根據所認定的結果，選擇按下【濫用系統】或【重新偵辦】中的一個按鈕回報再次確認的結果。

(4) 當舉報平台伺服器收到任一位上司 S_i 按下【重新偵辦】的按鈕，表示案件必須重新調查，$Server_{IN}$ 將重新指派該案件給新的承辦人員。

(5) 當舉報平台伺服器收到所有上司$\{S_1, S_2, \ldots, S_i\}$按下【濫用系統】的按鈕，伺服器將暫停該用戶繼續使用系統一段指定的時間或永久停權。

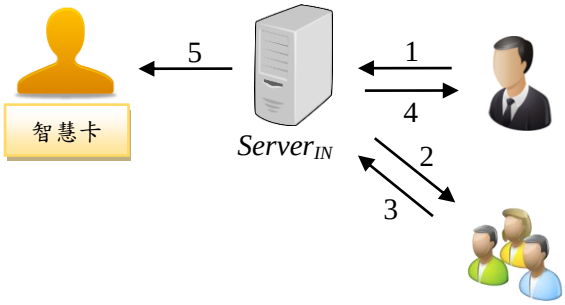

圖 8 濫用系統判定流程

接著將進一步說明濫用系統之判定流程，首先這個程序，先由所有上司$\{S_1, S_2, \ldots, S_i\}$再次審核該事件，如果 *Si* 判定此事件為濫用，S_i將按下【濫用系統】按鈕，即會回傳 OK_i 至 $Server_{IN}$，若是認為該事件有疑慮必須重查，則按下【重新偵辦】按鈕，將傳送 NO_i 至 $Server_{IN}$，以下步驟 1~2 將說明當舉報平台伺服器($Server_{IN}$)收到 *Si* 結果後的處理機制。

S_i → $Server_{IN}$:

$Server_{IN}$收到所有上司回傳之審核結果若為$\{OK_1, OK_2, \ldots, OK_i\}$，表示所有上司$\{S_1, S_2, \ldots, S_i\}$均已判定該舉報為濫用事件，$Server_{IN}$ 會自動停用該帳號，濫用系統之驗證如圖 9 所示。

反之，當 $Server_{IN}$ 收到$\{S_1, S_2, \ldots, S_i\}$，只要有任一位上司 *i* 傳送 NO_i，則表示該案件需重新偵辦，此時 $Server_{IN}$ 會將該事件重新指派給另一位 P_i 重查以防吃案或誤判，圖 10 顯示重新偵辦之驗證。

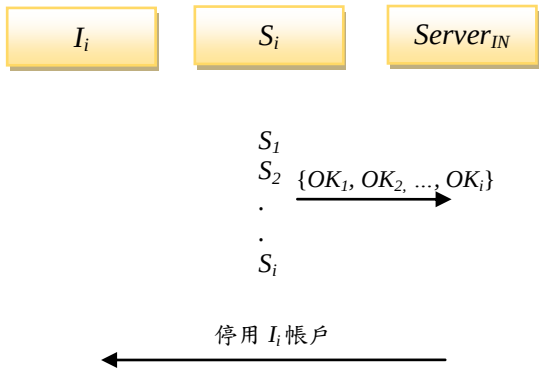

圖 9 濫用系統之驗證

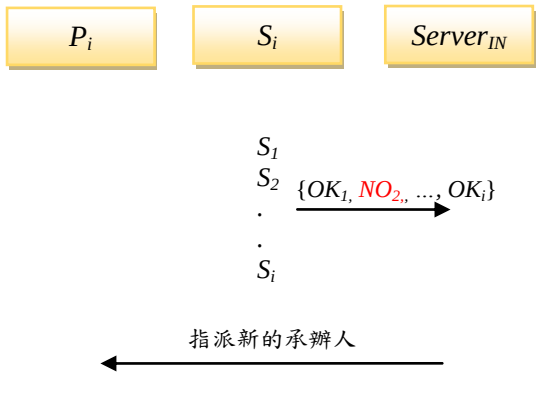

圖 10 重新偵辦之驗證

3. 系統安全分析

以下將分析隱匿舉報平台所符合資訊安全的特點: 首先舉報平台伺服器 $Server_{IN}$ 與各個單位在網路通訊上，採用 SSL(Secure Sockets Layer)傳輸層安全協議，將可以達到資料傳輸的機密性(Confidentiality)和完整性(Integrity)[8]。

註冊及登入階段，舉報平台伺服器除了對使用者輸入的身份及密碼進行確認外，為了確保使用者身分的合法性，此系統結合自然人憑證卡，透過公信第三方驗證伺服器 $Server_{CA}$ 再次驗證該使用者身分，因而達到雙重驗證。在資訊安全上將符合身份的鑑別性(Authentication)、不可否認性(Undeniability)及資料的完整性[1]。

另外在登入該平台通行密碼的安全上，採用 MD5 及 SHA。使用 MD5 主要理由為借重其效率及普遍性，能有效率驗證資料完整[4]。SHA 的選用則是因其單向雜湊的特性，使得訊息難以逆推，可有效預防暴力破解。此外，更在通行密碼上加上雜訊(*salt*)，由插入片段可大幅降低使用者密碼外洩造成的風險[7]。

4. 結論

由於氾濫的犯罪行為在社會上經常出現，人們常為了自身安全不敢舉發不法，縱容不法行為不斷發生。為解決此問題，在本論文中，我們提出以電子憑證作為身份識別之具有人身隱匿、安全保護及負責功能的違法舉報系統，提供大眾舉報違規事件之新管道，有效且迅速地向政府單位通報，以期最短的時間內予以處理與回覆，解決了人心的恐懼，不再害怕受到威脅，使民眾們可以放心的使用舉報系統達成全民共同打擊不法之目的。本論文所提出的系統，為結合自然人憑證卡，搭配現有的加解密技術，透過既有之具公信的第三方進行必要之認證，不僅可驗證舉報者身分的真實性，避免使用假人頭帳戶之問題，又可避免身份曝光受報負威脅，亦可確保名眾舉報及領獎金過程完全隱私。透過此簡單易用且安全的線上舉報系統，可讓全民放心地監督不法行為，使全民的生活品質得以受到保護與提昇。

參考文獻

[1] 內政部憑證管理中心 http://moica.nat.gov.tw/index.html。

[2] 林祝興、黃志雄，資訊安全實務：數位憑證技術與應用，全華。

[3] 吳志崧，“以自然人憑證實作一次性密碼之身份認證機制”，義守大學，資訊管理學系碩士在職專班，碩士論文，2012 年 5 月。

[4] 李南逸、王智弘、林峻立、張智超、溫翔 安、葉禾田，東華，網路安全與密碼學概論 。

[5] 蔡佳倫、李榮耀，“以 IC 卡強化網站使用者身份驗證之研究”，*資訊應用期刊第三期第一卷*，P43-58，2007/07/01。

[6] 蘇建興、王威傑，“運用政府機關數位憑證實現雙向驗證之研究”，***北商學報***，第 20 期 ，P83 – 98，2011 / 07 / 01。

[7] Best Practicing for Password Protection http://plainpass.com/2012/06/best-practicing-for-password-protection.html。

[8] SSL: Foundation for Web Security http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_1-1/ssl.html。