以「共同準則」的方法探討「WebATM」系統之安全目標*

李　怡　昌　撰**

摘　要

「WebATM」系統除為銀行自動化服務的新通路外，亦為銀行對抗木馬駭客的利器，但「WebATM」系統安全嗎？尤其是在威脅來自四面八方的網際網路環境中，安全在本質上是一種既抽象且難以具體衡量的表述，尤其在資訊安全的領域中，資訊安全代表的是多重工程跨越時空的持續協同運作結果，它更難以衡量；「共同準則」（Common Criteria）是國際上一個評估「資訊產品或系統安全」的準則，其目的即在使資訊安全變成可以共同的語言具體表達及評量。

本文嘗試依照「共同準則」的方法，探討「WebATM」系統之安全目標，第一章說明「WebATM」系統之源起並簡單介紹「共同準則」；第二章說明評估標的系統-「WebATM」系統之運作模型及組成元素，評估標的系統為從晶片金融卡至客戶個人電腦以迄銀行伺服主機之子系統；第三章描述評估標的系統之安全環境，包括五種假設、九種威脅及十三條組織的安全政策等；第四章則依照第三章評估之安全環境需求訂定「WebATM」系統之安全目標共四十九條。最後綜合研究過程之心得，臚列於第五章為結論，簡略如下：

一、依照最近一期知名網路安全專業公司 Symantec 2005/01 -2005/06 網路安全威脅報告指出，網路威脅持續增加，更多的敵意程式（木馬程式）是有計畫的為獲得金融利益而潛伏，在這樣的網路環境下提供網路銀行服務，銀行資訊技術服務管理階層對網路威脅更應持續有效的監控及有效管理。

二、銀行於構建晶片金融卡系統之初，即應於符合銀行公會所訂規格之前提下，審慎規劃其獨特的晶片卡安全控管方式及加密政策，這樣才不會因一家銀行的安全機制被破解，所有銀行都遭殃。

* 本文定稿於 94 年 12 月。本文觀點純屬作者個人意見，與服務單位無關，文中如有任何疏漏或謬誤，一律由作者自行負責。

** 作者為中央銀行金融業務檢查處副稽核。

三、就「WebATM」系統之服務言，銀行不應於契約上規範客戶責任即已了事，而應具體評估規劃客戶計算環境中安全控管的具體策略，並持續有計劃的教育顧客，甚至支援顧客建立安全計算環境的技術或直接提供顧客安全的計算環境。

四、為有效防堵網路駭客以木馬程式攻擊，應考量採用適當的雙重驗證方法。

五、銀行應務實考量不可否認的機制，在完成一筆轉帳交易的過程中，客戶獨自掌控的只有晶片金融卡密碼，而密碼也是在銀行提供的軟體下輸入的。

壹、前　言

金融支付系統為金融業進行資金收付之核心業務，支付系統之安全、效率直接影響銀行對客戶服務之品質，也關係著整體金融體制之健全與穩定，因此維持安全、穩定及高效率之支付系統，一直是巴塞爾銀行監理委員會之主張，也是本行主管支付系統的重要課題。

一、WebATM 系統源起

本國銀行大概於民國 70 年代即推出磁條式金融卡的服務，而科技的持續發展，屢有不法之徒利用截取、盜取、側錄、盜錄等技術偽造金融卡進行智慧型犯罪，造成持卡人與金融機構莫大的損失。由於磁條式金融卡易被偽造、側錄，保密安全機制不足，安全性屢遭質疑，又受其原始設計功能所限，無法成為新興商業模式之有效支付工具。

我國銀行公會鑒於磁條金融卡之安全性已不符時宜，且晶片取代磁條已是當今世界各國卡片應用之市場趨勢，為提供社會大眾更安心、安全地、廣泛地應用金融卡作為日常生活資金調度、消費、理財等用途之支付工具，遂於 90 年 2 月著手評估金融卡晶片化之可行性，並於 91 年 7 月起由各金融機構陸續規劃進行系統轉置與卡片換發作業，原擬於 93 年 12 月底完成全國各金融卡全面晶片化工作，除可徹底解決磁條式金融卡的安全性問題外，金融機構亦可善用晶片卡功能強大之特性，來拓展卡片消費通路增加收益，並為企業金流電子化之過程中提供解決方案，使銀行與客戶均蒙其利創造雙贏局面。

「WebATM」系統即是在此背景下被推出的新種銀行自動化服務；由於在網路銀行上演的「特洛伊木馬屠城記」- 駭客在銀行客戶電腦植入木馬程式，進而竊取帳號、密碼盜領存戶存款；銀行公會甚至緊急決議，要求先關閉網路銀行非約定帳戶轉帳功能，於是銀行紛紛加緊推出「WebATM」系統作為銀行的新通路以為對抗木馬駭客的利器，目前全國已有二十餘家銀行建置。

二、WebATM 系統安全嗎？

「WebATM」系統安全嗎？尤其是在威脅來自四面八方的網際網路環境中，安全在

本質上是一種既抽象且難以具體衡量的表述，尤其在資訊安全的領域中，資訊安全代表的是多重工程跨越時空的持續協同運作結果，它更難以衡量；「共同準則」（Common Criteria）是國際上一個評估「資訊產品或系統安全」的準則，其目的即在於當特定資訊產品或系統之資訊安全目標為多數人、個體所共同關切時，則藉由大家共同認可的評估準則、評估程序及評估機構去評估其資訊安全，其評估結果將很容易被大家瞭解，當資訊安全變成可以共同的語言具體表達及評量時，對資訊產品或系統之消費者（使用者）、開發者及評估者均將具正面價值。

三、「共同準則」（Common Criteria）簡介

「共同準則」（Common Criteria）是國際上資訊技術主流國家，包括美國、英國、法國、德國、加拿大及紐西蘭等國家之資訊安全相關機構共同發展制定的一個供評估「資訊產品或系統安全」的準則，目前相當多的國家已設有合格的評鑑機構，也有相當多的國家承認前述評鑑機構的評鑑結果。

在「共同準則」中 TOE-評估標的系統(Target Of Evaluaion)是一個專有名詞，它代表被評估的資訊系統或產品，在本文中也就是WebATM系統，TOE的文件必須清楚的界定、表示其安全功能範疇，從安全環境的評估開始，訂定安全目標後再發展為安全需求，安全需求區分為功能性需求(Functional requirements) 及保證性需求(Assurance requirements)，功能性需求定義所需要的安全行為，保證需求則是對其所宣稱安全方法正確及有效執行的信心基礎（簡單的講即開發過程的嚴謹度）。安全功能需求及保證需求被運用來做為安全評估之基礎，評估的進程建立了對資訊產品或系統之安全功能、保證措施之信心等級。

本文嘗試依照「共同準則」的方法，但將僅探討至「WebATM」系統之安全目標，在第二章說明評估標的「WebATM」系統之運作模型及組成元素，第三章描述評估標的系統之安全環境，包括假設、威脅及組織的安全政策等，第四章評估「WebATM」系統之安全目標，最後在第五章綜合研究過程心得做成結論。

四、研究目的

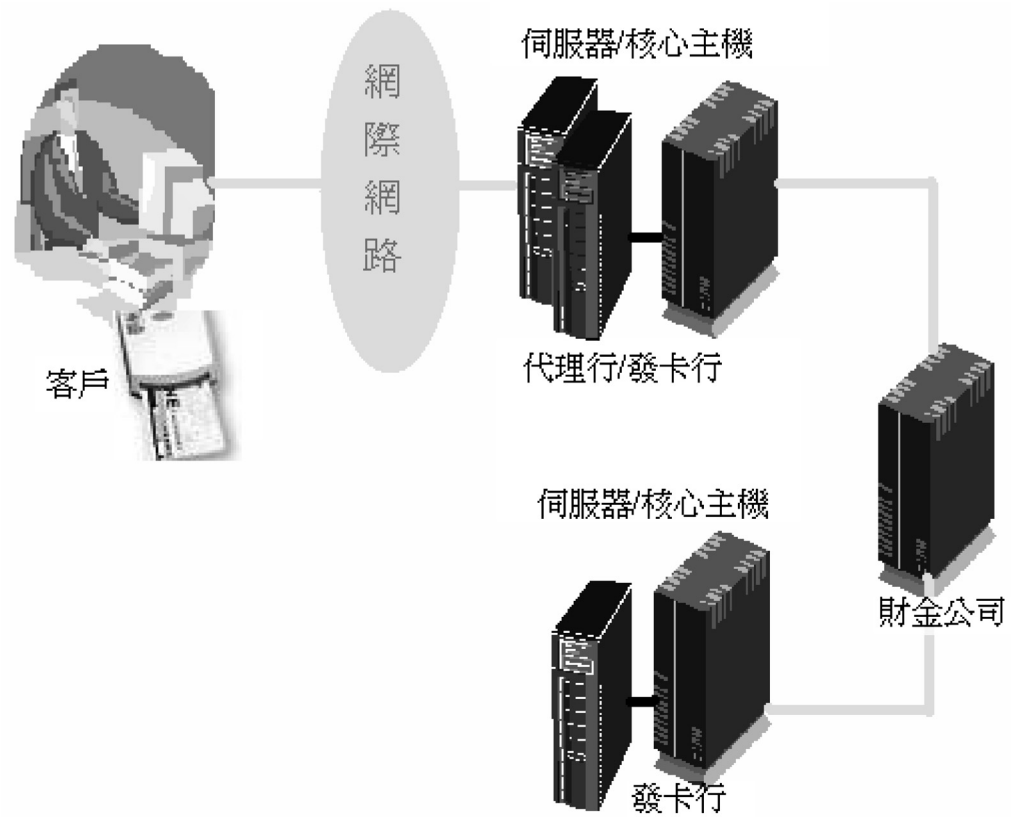
安全目標說明TOE -「WebATM」系統為對抗威脅、滿足其安全環境的具體措施，可供銀行建置或維護其「WebATM」系統參考使用，若銀行擬建置一個符合「共同準則」之「WebATM」系統，亦可循此發展後續的安全需求文件，另主管機關亦可藉以評估銀行「WebATM」系統之安全考量是否周延。

本文所述子系統及交易模式並未以特定銀行之「WebATM」系統為樣版模型。

貳、評估標的系統（TOE）說明

「WebATM」系統是一台在網際網路上不會吐鈔的ATM，只要一部個人電腦、一台晶片讀卡機、加上一張晶片金融卡即能使用，除了吐鈔，其他 ATM 的功能，「WebATM」系統都有，就等於把ATM搬到自家的個人電腦上，基本上它是網路銀行的另一種呈現，而和傳統網路銀行不同的是，「WebATM」系統使用者驗證方法改為以晶片金融卡為基礎的驗證程序，只要銀行均遵循銀行公會及財金公司所訂規範，就如同傳統的共用實體ATM系統，「WebATM」系統亦能被他行的客戶所使用。

一、「WebATM」系統整體構成示意圖:



在大部份的情況下，銀行客戶通常會使用其晶片金融卡發卡行的「WebATM」系統，這樣的「WebATM」系統包括下列計算環境:

1. 晶片金融卡
2. 使用者個人電腦
3. 網際網路
4. 發卡行「WebATM」系統網站

⑴網站伺服器

⑵安全伺服器（亂碼化設備）

⑶交易伺服器

5. 發卡行帳務主機

⑴安全伺服器（亂碼化設備）

但仍然有發卡行本身不建置「WebATM」系統，其客戶持有的晶片金融卡須使用他行（代理行）的「WebATM」系統，則整個「WebATM」系統計算環境包括:

1. 晶片金融卡

2. 使用者個人電腦

3. 網際網路

4. 代理行「WebATM」系統網站

⑴網站伺服器

⑵安全伺服器（亂碼化設備）

⑶交易伺服器

5. 代理行帳務主機

⑴安全伺服器（亂碼化設備）

6. 跨行中介服務主機（財金公司）

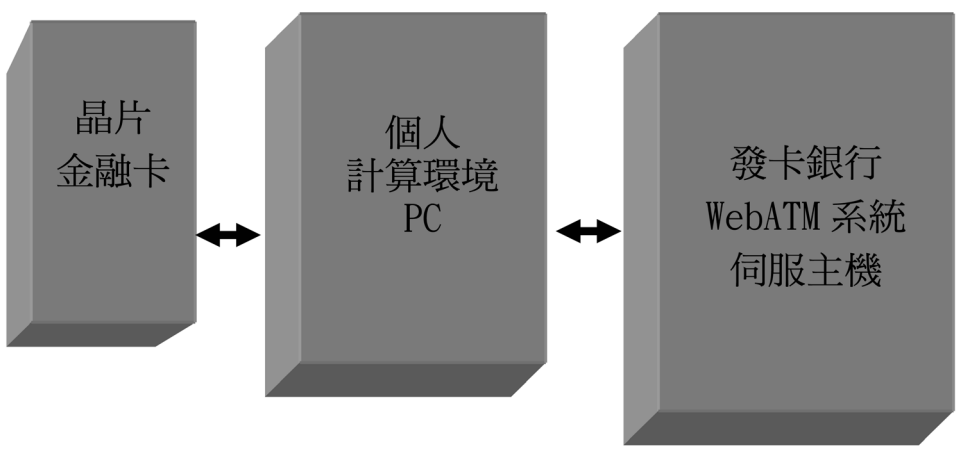
⑴安全伺服器（亂碼化設備）

7. 發卡行帳務主機

⑴安全伺服器（亂碼化設備）

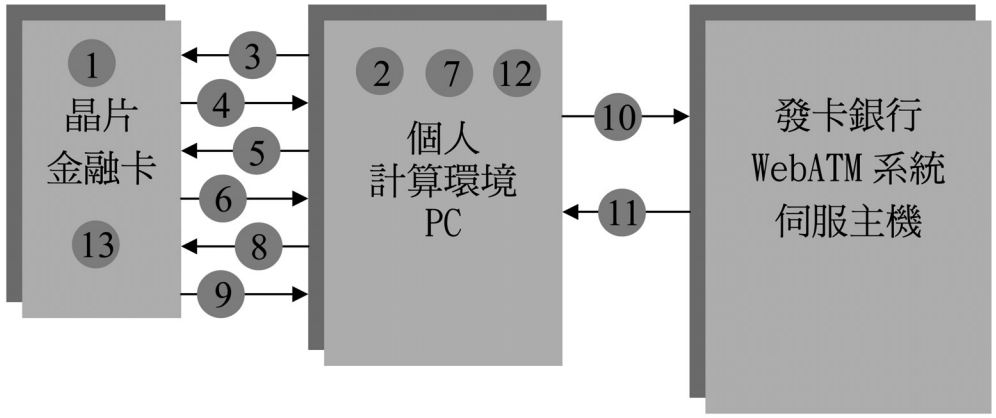
代理行帳務主機至發卡行帳務主機間屬既有跨行作業環境，本文主要探討將僅涵及晶片金融卡至發卡行（代理行）「WebATM」系統網站間之子系統環境。

二、子系統構成



三、交易模型

在「WebATM」系統中交易模型通常因功能而異，同一個功能也會因銀行不同而異，但因各銀行均須遵循銀行公會及財金公司所訂規範，大抵均在同一框架下運作，本文以安全需求較嚴格的轉帳交易為基準，描繪典型的「WebATM」交易模型如下:



交易模型說明：

1.客戶於 PC 連接之讀卡機插入晶片金融卡。

2.客戶啟動銀行「WebATM」系統，「WebATM」系統要求客戶輸入晶片金融卡密碼。

3.「WebATM」系統將客戶輸入晶片金融卡密碼傳送晶片金融卡驗證。

4.晶片金融卡傳回驗證結果。

5.「WebATM」系統要求讀取客戶帳戶基本資料。

6. 晶片金融卡傳回客戶之帳戶基本資料。

7.「WebATM」系統顯示帳戶基本資料並引導客戶完成交易資料輸入。

8.「WebATM」系統將交易資料傳送晶片金融卡，要求產生交易驗證碼。

9.晶片金融卡計算交易驗證碼，將相關資料寫入交易授權明細記錄檔，並傳回交易驗證碼。

10.「WebATM」系統產生交易資料送銀行伺服主機處理並等待主機傳回處理結果。

11.銀行伺服主機傳回處理結果。

12.「WebATM」系統顯示交易處理結果。

13.客戶取出晶片金融卡，交易完成。

四、子系統互通性

不同銀行的「WebATM」系統基本上並未直接互通，但是各銀行就晶片金融卡基本規格、存取介面規格均須遵循銀行公會及財金公司所訂規範，則每一銀行「WebATM」子系統均可依其自行所訂交易處理程序，透過既有跨行網路，提供他行客戶「WebATM」系統基本服務。

五、系統參與者及其角色

(一)銀行：系統的建置者、管理者。

(二)客戶：系統使用者。

(三)IT 提供廠商：包括晶片卡廠商、電

腦軟、硬體設備提供廠商。

六、評估標的系統（Target Of Evaluation）

TOE 包括子系統、交易模型及參與者等相關範疇，相關系統軟、硬體設備之開發、製造，及銀行每日清算、結帳等程序並不屬 TOE 之範圍，但為 TOE 運作所必需者均為 TOE 之環境。

參、TOE 之安全環境

此章節的目的主要在描述「共同準則」第 21 條所定義之 TOE 安全環境，包括：

(一)一個 TOE 環境必須符合的假設性陳述（Assumptions），惟有在假設的條件下，TOE 才可被認為是安全的，這個假設性陳述可以當成 TOE 被評估之基礎。

(二)一個對資產安全威脅的陳述，辨識在 TOE 的安全分析過程中所查覺到所有的威脅。

(三)一個對可被應用的組織安全政策、規定的陳述。

在後面的說明中，每一種假設、威脅及組織安全政策均會賦予名稱放於[ ]中，名稱的主要用途係於後續「共同準則」的相關進程中供識別使用。

一、假設

假設說明 TOE 將被使用或預期被使用和安全相關的環境：

(一)所有系統參與者充分的瞭解及並履行他們在契約上（或準契約上）有關於法規、財務及安全的責任義務，如晶片金融卡持有者必須要善盡保護卡片的責任－有一個合約說明晶片金融卡持有者的責任義務及好處。[假設.責任]

(二)所有系統參與者均具備足夠的工具、方法、訓練及資訊去表現它的功能，其內容包括規格、使用者手冊、維護手冊及作業規範等文件，以及按時更新文件、常態的訓練及演練模擬例外事件。[假設.能力]

(三)子系統執行正常管理或維護工作時，各類伺服器及安全機制相關設備均被裝置於實體保護的環境。[假設.信任的位置]

(四)就個別帳務交易與銀行間的應收、應付款項資料，存在特定的方法可確保資料之連貫與正確性。[假設.資料]

(五)所有的安全相關事件均被記錄追蹤。[假設.記錄]

二、威脅

針對資產的威脅，特定的保護於 TOE 裡或其環境是需要的，在這裡僅列出和 TOE 作業安全相關者。

(一)在此 TOE 中，將被保護的資產有：

1. 和 TOE 安全功能相關的軟、硬體設備。

2. 終端使用者資料，如系統正常作業使用的資料。

3. 和 TOE 安全機制相關資料，如亂碼化基碼、密碼、驗證資料等。

(二)威脅的來源

系統必須針對所有可能的威脅來源保護自己，不管威脅是來自其內部職員、客戶或系統外部的個體，「WebATM」系統之威脅來源依照他們的目的可分為下列五種:

1. 竊盜：為遂其金融利益企圖，滲入系統竊取秘密資料，進而盜轉客戶存款者。

2. 騙子：為遂其利益企圖，滲入系統竊取客戶基本或帳戶資料，以遂行其詐騙目的者。

3. 破壞者：為特定不法目的破壞所有或部份系統者。

4. 攻擊者：企圖展現其對系統安全技能的瞭解者。

5. 其他：濫用系統以促成其非法行動的任務。

另外，「WebATM」系統亦必須考量因管理上的疏忽而導致的可能障礙，擬訂因應措施。

(三)威脅清單

「WebATM」系統是在開放的網際網路上作業，其面臨的可能威脅亦如同一般傳統的網路銀行系統，這些威脅主要有：

1. 偽造轉帳交易：

偽造轉帳交易是「WebATM」系統所面對最嚴重的威脅，它直接導致銀行及客戶資產的損失，偽造轉帳交易可能經由下列途徑達成：

⑴在網路上惡意的入侵者於客戶電腦設備（PC）植入木馬程式，竊取客戶晶片金融卡密碼，並憑以要求晶片金融卡產生交易驗證碼（Transaction Authentication Code）等，再依序完成偽造轉帳交易。[威脅.偽造-竊取晶片金融卡密碼]

⑵在網路上惡意的入侵者於客戶電腦設備（PC）植入木馬程式，於客戶進行轉帳交易時，於晶片金融卡產生交易驗證碼（Transaction Authentication Code）及交易序號之前，竄改轉入帳號、轉帳金額等資料，再依序完成偽造轉帳交易。[威脅.偽造-竄改轉帳資料]

⑶竊取客戶晶片金融卡內產生交易驗證押碼之基碼及計算公式，憑以產生偽造轉帳交易之驗證碼等，再依程序完成偽造轉帳交易。[威脅.偽造-竊取秘密]

2. 客戶惡意否認轉帳交易：

⑴客戶竊取或非授權取得晶片金融卡片作業系統的秘密（Secrets），刪除晶片金融卡上之轉帳交易記錄，再訴求轉帳交易非其所為。[威脅.否認-刪除轉帳記錄]

⑵客戶銷毀晶片金融卡，再訴求轉帳交易非其所為。[威脅.否認-銷毀卡片]

3. 詐騙客戶身分識別或交易驗證資料

在網路上詐騙身分識別資料案件持續增加，歹徒經由下列途徑騙取客戶身分識別或交易驗證資料，憑以進行其他詐騙行為：

⑴利用釣魚技術，以假的電子郵件引導客戶進入其所設的網頁，騙取客戶身分識別資料或交易驗證資料。[威脅.詐騙-假郵件]

⑵設立假網站，套取誤入其網站的客戶之身分識別資料或交易驗證資料。[威脅.詐騙-假網站]

4. 干擾交易或破壞系統

⑴攻擊者於網路上發動癱瘓攻擊，導致系統無法提供服務。[威脅.干擾-癱瘓]

⑵攻擊者於網路上發動破壞攻擊，導致系統無法提供服務。[威脅.干擾-破壞]

三、組織的安全政策(Organizational Security Policies,簡稱 OSP)

在「共同準則」架構中，組織的安全政策為 TOE 必須遵從的安全規則、程序、辦法或指引：

(一)監控 TOE 的安全，偵測已發生或即將發生的故障。[OSP.監測]

(二)監控 TOE 的安全，偵測已發生或即將發生的故障，並採取適當的反應去限制或抑制故障之影響。[OSP.反應]

(三)適當的記錄秘密的建立、更新及廢止等安全事件，俾可以被追蹤。[OSP.記錄]

秘密泛指基碼、密碼、驗證資料等具機密性資料。

(四)TOE 的安全架構須基於已標準化、公開的、被大量覆核過、最先進的亂碼化邏輯及亂碼化基碼管理，TOE 不使用為安全理由須予保密的亂碼化邏輯，使用亂碼化之功能強度必須為高。[OSP.亂碼]

(五)TOE 的通信架構須基於已標準化的協定及安全程序。[OSP.通訊協定]

(六)軟、硬體設備及組織的程序已通過功能合格的測試及安全測試。[OSP.合格的設備]

(七)每一筆轉帳交易進行前均須先經雙方互相驗證，驗證的程序可確保交易的不可否認性。[OSP.身份驗證]

(八)每一筆轉帳交易均被詳細記錄，俾可在事後檢查相關的細節。[OSP.交易驗證]

(九)所有 TOE 中使用的秘密的生命週期均有期限，並依照它們的期限適時更新。[OSP.秘密生命週期]

(十)「WebATM」系統功能所需之軟硬體設備必須定期辦理安全更新。[OSP.定期維護更新]

(十一)所有秘密均得予更換，子系統亦可整個或局部更換，更換必須以對可用性衝擊最小的方式辦理。[OSP.安全設備更新]

(十二)僅有權限人員方能辦理建置、管理、操作所有子系統的相關設備，銀行必須強制以組織上或技術上之程序，確保僅有權限人員方能存取資產。[OSP.存取控制]

(十三)管理階層須有明確的資訊安全風險辨識及管理能力，尤其對網際網路上的威脅更應持續有效的監控與有效管理。[OSP. 資訊風險辨識與管理]

肆、TOE之安全目標

本章節定義TOE及其環境的安全目標，安全目標之目的在對付所辨識的威脅，並滿足所辨識的組織安全政策及假設。

一、安全目標的分類

安全目標的目的在對付所有的安全考慮，並宣告那些安全問題已直接由TOE或由其環境來滿足，安全目標區分如下：

(一)TOE的安全目標：追蹤TOE將對付被辨識的威脅及/或TOE必須符合的組織安全策略。

(二)環境的安全目標：追蹤TOE未完全對付被辨識的威脅及/或TOE未完全符合的組織安全策略或假設。

二、安全目標應用的領域

安全目標的範圍包括下列三個領域：

(一)系統：其目標相關於「WebATM」系統。

(二)秘密：這些目標相關於基碼、密碼、驗證資料及它們的管理及使用。

(三)交易：這些目標相關於交易的領域。

三、安全目標命名原則

安全目標依下列原則命名：

OT|OE . <領域> . <一般目標> [.<特定目標>]

* OT|OE　：表示此目標和TOE (OT)或環境 (OE) 相關

* <領域>　：以<系統>|<秘密>|<交易>|<監控> 表示

* <一般目標>：一般目標的分類

* <特定目標>：可選擇性的對一般目標再加修飾

四、安全目標

在本章節說明安全目標，每一個說明標題中，[]中即為一般目標，而在詳細的說明中，再針對特定的目標說明，並組成一個完整的名稱附加於後。

(一)資料完整性 [完整性]

維持資料的完整性。

1. 每一個子系統維持資料之完整性。[OT.系統.完整性.整體]

2. 每一轉帳交易必須同時完成借、貸方之加計。[OT.系統.完整性.借貸平衡]

3. 惟授權的交易、功能才能更新帳務資料。[OT.系統.完整性.授權功能]

(二)資料機密性 [機密性]

必須保持機密的資產均應保持。

1. TOE 對所有的秘密均保持機密。[OT.秘密.機密性.保持]

2. 惟有被授權的人才能知悉機密。[OE.秘密.機密性.授權]

(三)識別性 [識別性]

一個唯一的識別是必須的，TOE 中下列每一個的元素均須被唯一的識別所定義。[OT.系統.識別性]

1. 子系統

2. 晶片金融卡/帳號

3. 交易序號

4. 交易類別

5. 秘密

(四)驗證 [驗證]

下列訊息溝通必須驗證對方的身分：

1. 個人計算環境與銀行伺服主機間。[OT.交易.驗證.訊息]

2. 晶片金融卡與客戶間。[OT.交易.驗證.客戶與晶片卡]

3. 晶片金融卡與個人計算環境程式間。[OT.交易.驗證.晶片卡與程式]

4. 晶片金融卡與銀行伺服主機間。[OT.交易.驗證.晶片卡與伺服主機]

5. 適當的提供雙重驗證機制。[OT.交易.驗證.雙重驗證]

(五)存取控制 [存取控制]

非授權地存取所有資產必須被防止，包括系統處於故障時或是在管理秘密時，每一個被識別的角色均有一組很清楚的存取權限：

1. TOE 實施安全控制，俾防範非法存取秘密。[OT.秘密.存取控制.秘密]

2. 在系統中每一被識別之角色，均有一組清楚的存取權限。 [OE.系統.存取控制.角色權限]

(六)交易正確性 [正確]

交易僅能正確完成或取消，交易如未正常結束，TOE 強制的安全功能允許該交易被完成或取消。[OT.交易.正確]

(七)限制 [限制]

「WebATM」系統中對轉帳交易金額必須要訂限制。[OT.系統.限制]

1. 每筆轉帳交易限額

2. 每日轉帳交易限額

3. 待確認轉帳交易限額

(八)可追蹤性 [追蹤]

系統監督者能夠依照其所需的時間，追蹤和稽核所有策略上重要的事件，子系統應記錄並保存系統監督者所需的資料，可追蹤的資料必須能正確的反應記錄的事件。

1. 建立、刪除、撤銷及更換秘密是重要的事件，這些事件被記錄俾利系統監督者之稽核。[OT.秘密.追蹤.異動記錄]

2. 更改子系統運跑控制參數，如轉帳交易限額等。[OT.系統.追蹤.參數變更]

3. 正確的記錄成功及失敗的交易。[OT.交易.追蹤.交易記錄]

4. TOE 提供方法，俾可於需要時及時通報稽核記錄予系統監督者。[OT.系統.追蹤.提供方法]

(九)偵測 [偵測]

系統具有偵測下列事件之能力。

1. TOE 提供方法，供偵測企圖或已發生的非法存取秘密、修改或使用秘密。[OT.監控.秘密存取]

2. TOE 提供方法，供偵測企圖或已發生的非法存取資產。[OT.監控.資產存取]

3. TOE 提供方法，供偵測企圖或已發生的偽造交易，提供予系統監督者俾使其可追蹤該等異常事件至其來源。[OT.監控.偽造交易]

(十)反應 [反應]

系統對因異常或非法行為所致之傷害，提供迅速反應之方法。

1. TOE 對非法存取、修改或使用秘密所致之傷害，備有方法、程序能迅速反應以確保服務的持續性。[OT.秘密.反應]

2. TOE 對非法或錯誤功能造成錯誤的資產交易，提供方法去執行系統監督者所下之反應命令。[OT.交易.反應]

3. TOE 可取消涉及錯誤功能之每一筆交易。[OT.交易.反應.取消]

(十一)亂碼學及通信協定 [亂碼協定]

最先進的亂碼學、通信協定及安全程序是必須的。

1. TOE 的安全架構係基於標準化、公開、廣泛的覆審、最先進的亂碼演算法及亂碼化的基碼管理，TOE 不使用仍須為安全理由而保密的亂碼演算法。[OT.系統.亂碼協定.亂碼]

2. 所使用的亂碼學及或然率機制之功能強度須為高。[OT.系統.亂碼協定.功能強度]

3. TOE 的通信架構須基於標準化的協定及安全程序。[OT.系統.亂碼協定.協定程序]

(十二)秘密管理 [秘密管理]

保持秘密的機密性及完整性，以正確的產生、分送、實體儲存保護、有限的生命週期及換新。

1. TOE 產生及分送秘密係依照標準化的程序。[OT.秘密.秘密管理.初始化]

2. 秘密的產生方法必須是它的值不可被預測。 [OT.秘密.秘密管理.可預測性]

3. 每一秘密依照其用途均有一有限的生命週期。 [OT.秘密.秘密管理.生命週期]

4. TOE 提供方法，可於任何時間產生新的值去更換秘密 [OT.秘密.秘密管理.更新]

5. 對特屬於某一安全功能的秘密須僅限該功能使用 [OE.秘密.秘密管理.唯一性]

6. 秘密被傳輸及存放於可抗實體損壞、修改及干擾的適當設備中，且在設備外永不以明碼呈現，私人的及秘密的亂碼基碼須儘量避免於設備外使用，且不應是對安全很重要的，非對稱性的私密基碼、對稱性的主基碼及在階層式基碼架構下的根基碼等對安全都很重要。[OT.秘密.秘密管理.損害]

7. 所有用來產生秘密之程序及相關元素，均僅限於那些需要的人才能知曉，秘密亦僅分送予需要的人。[OE.秘密.秘密管理.授權人員]

(十三)信任的路徑 [信任路徑]

和系統交易訊息經由受保護的通信方法一樣，TOE 提供一個被信任的路徑，俾保護交易訊息免被惡意的修改或揭露。[OT.系統.信任路徑]

(十四)信任的位置 [信任的位置]

對某些敏感的設備，實體保護的環境是必須的，在管理者或操作者執行工作時，安全設備應放置於實體保護的環境。 [OE.系統.信任的位置]

(十五)能力與責任 [能力與責任]

參與系統者均知悉並遵循其合約上的責任，並且具備足夠的工具、訓練及資訊去扮演他的角色。

1. 系統參與者知悉並遵循其合約上的責任，及他們彼此間相互的規約、財務及安全上的責任。[OE.系統.能力與責任.責任]

2. 管理秘密及操作子系統的人必須具備相關領域上的能力及專業，並具備充足的工具、訓練及資訊去扮演他們的角色。[OE.系統.能力與責任.能力]

3. 應有一個合時的僱用政策、公司營業場所進出控制及適用於全公司員工的安全體認計畫。[OE.系統.能力與責任.人事管理]

(十六)合格及測試 [合格測試]

系統組件在作業前或作業中均經適當的測試。

1. 硬體設備、軟體及組織程序均通過功能合格之測試，硬體設備並經實體耐力測試。[OE.系統.合格測試.合格測試]

2. 於作業階段，每一設備亦能在不影響系統之可用性下承受功能測試。[OE.系統.合格測試.作業中測試]

3. 在其進入作業階段前，每一設備均經測試，首先是獨立測試，而後整合於 TOE 測試 [OE.系統.合格測試.整體測試]

(十七)評量 [評量]

重要的參與者均須被評量，管理者及操作者亦須被覆審，俾確保職務上能正確的反應安全政策。[OE.系統.評量]

(十八)安全更新 [維護]

為維持一個穩定的安全等級，定期對硬、軟體進行安全更新是必須的。[OE.系統.維護]

(十九)可用性 [可用性]

系統應確保服務的可用性，甚至在維護部分系統時。

1. 當更換一個或數個 TOE 秘密時，TOE 確保僅有微小的服務中斷。[OT.安全.可用性.可用性]

2.一個限制系統或其任何組件故障所導致衝擊之業務持續計畫。[OE.系統.可用性.可用性]

(二十)交易完成通知 [交易通知]

為儘速發現不法偽造轉帳交易，系統於完成轉帳交易後，應對客戶原申請指定之 e-mail 或手機，發出通知信函。[OT.監控.交易通知]

(二十一)客戶教育與支援[客戶支援]

應具體評估規劃客戶計算環境中安全控管的具體策略，並持續有計畫的教育顧客，甚至支援顧客建立安全計算環境的技術或直接提供顧客安全的計算環境。[OE.系統.客戶支援]

伍、結　論

現階段，晶片金融卡對偽造卡片有直接防止效用，而「WebATM」系統於網際網路上作業，使用晶片金融卡為交易驗證的工具，較傳統網路銀行使用個人密碼作為驗證之方法，已有長足的進步。本報告研究當時，國內媒體正大肆報導「網路 ATM 若遇駭，3 秒盜走 10 萬」事件，雖屬臆測性報導，後亦經銀行公會晶片金融卡專案小組負責人出面澄清，但隨著科技持續發展，網際網路上的威脅亦與日俱增卻是不爭的事實，臚列幾點心得如后：

一、依照最近一期知名網路安全專業公司 Symantec 2005/01 -2005/06 網路安全威脅報告指出，在這段期間相關網路系統軟體發現的弱點達 1,862 個，創歷年新高，自弱點發現至被利用為攻擊行為約需 6 天的時間，而發展出其安全更新軟體則需 54 天，更多的敵意程式（木馬程式）是有計畫的為獲得金融利益而潛伏，在這樣的網路環境下提供網路銀行服務，銀行資訊技術服務管理階層須有明確的資訊安全風險辨識及管理能力，尤其對網際網路上的威脅更應持續有效的監控及有效管理。

二、銀行於建構晶片金融卡系統之初，即應於符合銀行公會所訂規格之前提下，審慎規劃其獨特的晶片卡安全控管方式及加密政策，這樣才不會因一家銀行的安全機制被破解，所有銀行都遭殃。

三、相較於其他自動化服務，「WebATM」系統是相當低成本的服務，銀行不應一味的以為客戶應為自家個人電腦系統負責，於契約上規範客戶責任即已了事，畢竟客戶在網際網路上是最弱的一環，對駭客更毫無招架之力，銀行應具體評估規劃客戶計算環境中安全控管的具體策略，並持續有計劃的教育顧客，甚至支援顧客建立安全計算環境的技術或直接提供顧客安全的計算環境。

四、為有效防堵網路駭客木馬程式攻擊，應考量採用適當的雙重驗證方法。

五、銀行應務實的考量不可否認的機制，畢竟在完成一筆轉帳交易的過程中，客戶獨自掌控的只有晶片金融卡密碼，而密碼也是在銀行提供的軟體下輸入的。

參考文獻

1. Federal Reserve System USA. A summary of the roundtable discussion on the risk and security involving retail payments over the Internet. 2005/06.
2. Federal Financial Institutions Examination Council USA. Authentication in an Internet Banking Environment. 2005/10.
3. Electronic Banking Group of the Basel Committee on Banking Supervision. Risk Management Principles for Electronic Banking.

2003/07

4. Common Criteria Project Sponsoring Organisations.Common Criteria Part 1: Introduction and general model V2.2
5. Common Criteria Project Sponsoring Organisations.Common Criteria Part 2: Security functional requirements V2.2
6. Common Criteria Project Sponsoring Organisations.Common Criteria Part 3: Security Assurance Requirements V2.2
7. European Central Bank, ELECTRONIC MONEY SYSTEM SECURITY OBJECTIVES 2003/05
8. 財金公司晶片金融卡規格書 v2.1
9. Symantec, Internet Security Threat Report , 2005/09