出國報告（出國類別：會議）

參加 2007 國際資訊認證安全研討會

服務機關：內政部
姓名職稱：參事兼資訊中心主任沈金祥
派赴國家：英　國
出國期間：96 年 8 月 26 日至 96 年 9 月 2 日
報告日期：95 年 11 月 30 日

摘要

系統編號：C09603322

出國報告名稱：參加第三屆國際資訊認證安全研討會

出國計畫主辦機關：內政部資訊中心

出國人員姓名：內政部參事兼資訊中心主任

出國類別：會議

出國期間：96 年 08 月 26 日至 9 月 2 日

出國地區：英 國 曼徹斯特

內容摘要：

爲規劃本部自然人憑證業務後續之推動方向，汲取國際 PKI（公開金鑰）相關發展經驗及最新技術應用趨勢，乃參加國際資訊認證及安全組織（ IAS - Information Assurance and Security）在英國曼徹斯特大學所舉辦之「2007 國際資訊認證安全研討會」。與會期間所獲心得及建議有：一)國現行 GPKI 政策下核發之 PKI 憑證，其有效安全期限面臨挑戰，相關憑證使用 RSA 長度及 SHA1 方法盡速予以檢視；二)資安策略措施及效益宜予檢討；三)研討改進自然人憑證之載具設計；四)加強國際資安合作與交流。

目　　次

壹 參加會議目的

爲規劃本部自然人憑證業務後續之推動方向，汲取國際 PKI（公開金鑰）相關發展經驗及最新資訊安全技術應用趨勢，乃參加國際資訊認證及安全組織（ IAS - Information Assurance and Security）在英國曼徹斯特大學所舉辦之「2007 國際資訊認證安全研討會」。

由於本部負責自然人憑證推廣規劃、維運督導及自然人憑證應用系統推動等工作項目，第一階段將於今（96）年辦理完竣，自明（97）年起將推動第二階段（97 至 100 年）工作，亟須汲取各國相關經驗並獲取如何在關鍵性的資訊基礎架構下保護資訊系統、網路及機敏資料的最新技術，以順利研討推動本項業務之後續計畫、強化資訊安全、提升便民服務品質。

「第三屆國際資訊認證安全研討會」研討會係由國際資訊認證及安全組織（IAS）所舉辦，會中安排 PKI 憑證簽發及身份確認技術專題討論、密碼協定專題討論、網際網路認證及支付安全專題報告等，各項研討主題符合本部推展自然人憑證 PKI 機制需要；並值得供國內推動電子化政府之資訊安全借鏡；同時爲充分運用時機，並在正式會議期程前參訪曼徹斯特大學在資訊安全相關領域之研究成果，俾供強化本部資訊安全規劃參考。

貳　參加會議過程

「2007 國際資訊認證安全研討會」（ IAS - Information Assurance and Security）係於民國 96 年 8 月 26 日至 96 年 9 月 2 日間在英國曼徹斯特大學舉辦，計有 22 國 200 餘人參加；會中共有 61 篇論文發表。

本研討會旨在藉邀請各方資安研究人員、電腦工作者、系統發展者、及決策者齊聚一堂，交換心得並共同研習此重大課題的最新發展。本年研討會邀集在資安領域德高望重的專家及學者討論在網路及分散式資訊分享的環境的以下的重要議題：

- 代理人及流動代碼(Mobile Code)安全
- 匿名及使用者隱私
- 憑證簽發及身分管理
- 授權及存取控制
- 生物辨識安全及應用
- 電腦辯論術
- 密碼協定
- 資料完整性及應用
- 資料完整性及隱私性
- 資料庫安全

- 阻斷式服務入侵偵測
- 分散式系統安全安全
- 電子商務及電子化政府安全
- 詐騙管制
- 資訊戰爭及網路恐怖份子
- 智慧財產保護
- 網路及網頁服務安全
- 金鑰管理及復原
- 行動及專屬網路安全
- 網路安全
- 安全新知及範例
- 作業系統安全
- 安全硬體及智慧卡
- 安全軟體技術
- 安全教育及訓練
- 安全管理和策略
- 安全模式和架構
- 安全驗證、評估和量度
- 偵測器網路安全

- 信託溝通、建立及管理
- 到處可見的電腦安全

IAS 2007 受到國際傳輸科學及技術協會和 CREATE-NET 的聯合技術支援，由歐洲幾個主要的大學和研究中心創辦於意大利的 Trento 城。這裡每一篇的文稿都是由至少 3 個以上的計畫委員會成員評審後，最後選出 61 篇。

茲將本人參與本次研討會各項議題之重點摘要說明如下：

一、主題演講 -- 生物鑑識智慧資訊系統及應用

本場次爲講座，由我國旅美教授 Dr. Patrick Wang 主講，本主題討論某些生物鑑識技術及其應用的一些基本問題。它包括以下幾方面：(1)綜覽生物測定的技術和應用，(2)安全的重要：以恐怖份子的攻擊的情節，(3)生物鑑識技術，(4)生物測定術：分析和合成，(5)分析：模式識別觀念，(6)指紋取得及核對，眼球及臉型分析，(7)識別應用，(8)温度影像：心情辨識，(9)生物鑑識合成，(10)模式化及模擬，和(11)應用實例。

二、實務教學 -- 現代電腦網路加密協定－結合憑證簽發及安全機制

本主題爲教學場次，由國際著名 PKI（公開金鑰）專家 DR Milan

Markovic 主講（因本主題與本部推展自然人憑證及 PKI 機制之應用相符合，特將講稿全文翻譯於附件三，以提供相關單位參考）。

現代 TCP/IP 電腦網路的加密方法主要着眼於以下方面：以非對稱式加密演算法爲基礎的數位簽章技術、用對稱式加密系統保護資料的私密性、及 PKI 系統。本文首先考慮 TCP/IP 網路的弱點及其改良方法。文中指出只有透過通盤且多層的網路防禦架構才能因應對電腦網路的可能攻擊。本文評估 ISO/OSI 應用層、傳輸層和網路層的安全機制，並舉例說明在各層網路中今日最常見的安全協定應用(如 S/MIME、SSL、和 IPSec)。本文也特別強調以數位憑證和 PKI 爲基礎的使用者強勢的認證程序。並評估僅用軟體、軟硬體組合使用、和僅用硬體模組間的差異，因而選用了到處可見的智慧卡和硬體模組。硬體安全模組(HSM)代表著近代電腦網路的重要安全面向。HSMs 主要是用在伺服器的應用上，但也可能用於特殊的客戶端應用(如政府、軍事、警政等)。對於大量的個人使用，智慧卡是較合適的硬體安全模組，至於在大規模的用途上，爲了效能，最佳的的方案爲智慧卡及軟體的組合，也就是說，智慧卡增加安全性，而軟體增進整體處理速度。依此而言，最適合的大規模解決方案爲：使用軟體處理大量的對稱式資料加解密，而智慧卡則用來產生數位簽章和讀取數位信封。

本文簡述了 PKI 系統的主要元件，強調憑證簽發機構及其建立以

ITU-T X.509v3 數位憑證標準爲基礎在系統中的合法使用者身分加密唯一性的角色。對 ITU-T X.509 標準而言，PKI 系統是用被定義爲用來製作、管理、儲存、或取出那建基於公鑰密碼的硬體集合、軟體集合、角色、和程序。PKI 系統提供在合理技術及組織安全環境下，可實現以下四個企業主要的安全功能：認證、保護資料完整性、不可否認性、保護資料的私密性。

此外，本文綜覽使用數位簽章的法律層面，歐盟各國在採用了根據歐盟條例及其他法案所制訂的電子簽章法及相關規定之後，歐洲各國分別建立一個專責的國家級機構負責監督電子簽章的執行。因爲和人工簽章具同等法律效力，文中也考量合格電子簽章的可能應用、不同 CA 的授權和監督機制、有關使用安全簽章產生器(SSCD)方面的問題、發出合格憑證的 CA 的必要條件等等。

最後，本文也簡述了 EMV 改進過程的主要特徵，如由磁卡轉換到晶片卡。此外，本文也綜覽 3D 安全系統和晶片認證程式(CAP)。事實上，本文會考量憑證簽發和安全付款機制在多用途 DDA 付款卡上的可能組合，這種卡片至少有三方面的應用：付款、CAP 和 PKI。

三、代理人及系統安全（Agent & System Security）

1、智慧型的互動分散系統

（荷蘭阿姆斯特丹 VU 大學 Martijn Warnier Frances Brazier）

在分散的代理人系統如電子商務和網拍裡，匿名是很重要的。本論文分析建議對組織化代理人的匿名方式的一種新方法 － 使用假名。一個創新的命名方式提出來，令代理人平台中的代理人能使用該平台中的自動命名系統，也可說是因應需求而生的匿名。本論文也介紹一項新技巧，就是使用可以完全整合至代理人平台的「把手」，在 AgentScape 平台所使用匿名服務的效能量測也提供了對其中所涉及的資源消耗的瞭解。

2、比較行動代理人的信託及安全模式

（希臘 Piraeus 大學 Michail Fragkakis 及 Nikolaos Alexandris）

行動代理人系統運用一些安全功能來解釋各種的威脅。儘管這是一個安全的共同需求，目前似乎並不存在有一個通用的信託安全模式能涵盖所有的運作而成爲一個標準做法，本文旨在提出現代信託及安全模式的進展，以比較四個主要的現代行動代理人平台的安全架構。所得到結論能指出目前技術的缺失及未來研究所應注意到的問題。

3、程式支解得以變形保護軟體

（網際空間研究中心 Bobby D. Birrer, Richard A. Raines, Rusty O.

Baldwin,）

未經授權的程式和演算法逆向工程是軟體業的一大問題。逆向工程師找尋程式的安全漏洞以利用或竊取競爭者的重要演算法。爲了不讓逆向工程得逞，程式發展者運用各種保護軟體的方法來弄亂他們的軟體。

程式支解軟體保護在傳統的弄亂技術加上另一層的保護，這樣改變保護的方式迫使逆向工程師必須調整他們的攻擊。程式支解是由兩種混亂技術所組成的，經由大綱化並弄亂參照表使成爲一個新變形的保護，程式的片段由主程式流程中移至各區的記憶體，減少程式的群聚性，這些碎片程式再經由弄亂參照表來呼叫執行，這樣就不易被看懂程式的流程。本研究評估一程式支解引擎所帶來的效能成本並分析其對抗逆向工程技術的有效性。結果顯示效能成本低且能有效混淆使用兩種常見的反組譯/除錯工具的反組譯程式。

4、程式執行碼正確的應用軟體沙盒機制

（Stony Brook 大學電腦科學系、Wei Li Lap-chung Lam Tzi-cker Ciueh）

將網路應用的系統呼叫程序饋入沙盒機制做爲偵測是否有駭客入侵取得掌控權是常見的方法，這類的駭客攻擊利用軟體弱點如緩衝區溢出來取得對受攻擊軟體甚或是其所在機器的控制。這種以監控系

統呼叫的方法長久以來難以被接受的原因在於對無法取得原始程式碼的視窗應用軟體如何能正確的建立沙盒機制。實際上很多資安軟體公司利用這個理由去建立一套有如防毒軟體公司的病毒碼更新的生意經，就是說客戶要付沙盒機制的定期更新費用。本論文也敍述了一個名叫 BASS 的沙盒系統的設計、應用、和評量，該系統能自動從 Win32/X86 程式執行碼中萃取出非常正確針對特定應用系統的沙盒機制，而且在執行程式時強制應用該機制的效能降低很有限。BASS 是建立在一個稱爲 BIRD 的程式執行碼詮釋及分析架構上的系統，能處理應用軟體的程式碼，包括其動態連結庫、例外處理、和多執行緒，其也已證實了能在許多視窗版的分散式網路商業應用中正確執行，包含 IIS 和 Apache。在所有測試的軟體中，僅有一個超過 8%的效能降低。

四、風險評估（Risk Assessment)

1. 資訊基礎架構下動態緩和風險

（Stanford 大學資訊工程管理學系 R. Ann Miura-Ko Nicholas Bambos）

本篇論文做了一個創新的分析架構去緩和及模型化會動態改變安全等級的資訊系統及網路。當風險入侵系統時(病毒、蠕蟲等)，風險值會在各元件/節點累加(主機、伺服器、資料庫等)，風險指標器就

進行監控。風險管理者動態性選擇防衛方式，將參數重新調整並分配既有的保護資源至各基礎架構的元件/節點。問題就在於如何進行能回應各處隨時變動的風險指標而分派合適防護能力的動態風險控管。

設計本架構旨在對模型中的成員併行執行排隊規則，映射存積/擁塞至風險層次/壓力。這揭露了動態風險管理和排隊理論兩者間的有趣關係，也允許運用存積管理的一些結果去做風險緩和，以及發展新方法來抓住風險管理的效能折衝。

2、營運風險：接受度原則

（曼徹斯特國家電算中心 Daniel Gideon Dresner J. Robert (Bob) G.. Wood）

英文有句諺語說「某人吃的肉可能是另一人的毒藥」，對本文應付風險的方法可能是貼切的。有些人熱衷滑雪或高空彈跳，也有些人對於在平地搭車都感到難以接受。有些組織允許員工無限的使用網際網路，另有些公司不但以技術性的監控或阻擋來限制員工網路的使用，還在心理上以解聘爲要脅。本文中我們檢視是否存在一種方法可適合對風險胃口不同的各個組織間，能有保證的分享彼此的資料和資源。我們是否有可能定義一種對風險態度的模式容許組織間彼此交流？本文提出只要有爲了管理風險而有意或無意制訂的標準，就一定

有辦法找到能建立互信的共同基礎。

3、結盟網路的風險管理

（皇家軍事學院訊號及影像中心 Wim Mees）

在現代的軍事行動中，多國參與結盟一項行動。爲了要快速的執行命令，一國軍隊的資訊系統要和盟國中其他成員國的資訊系統建立起通訊連結。互通結果也不可避免會帶來風險，而對這些風險要加以管理。一國以自己的風險管理方法及工具去整合結盟國對風險評估的結果，而這種整合過程仍是定期手動的作業方式。本篇中我們首先討論在單一組織中的風險管理方法，並說明爲何採用不中斷的風險管理方法是很重要的。接著再闡明在結盟環境中實現不中斷風險管理的想法。

五、信託管理 (Trust Management)

1、HPRS：使用檔案及同僚評價的混種 P2P 評價系統

（印度工學院電腦雷機科學院 Srinivasan T, Varun Ramachandran, Arun Vedachalam, S.K. Ghosh）

使用點對點網路檔案分享的人與日俱增，但因廣泛的使用難免會有惡意的點以不合規定的檔案氾濫網路、破壞網路。這種情況使得發

展針對惡意點和檔案的牢靠評價系統的需求應運而生。而僅對點評價的系統早已存在且很多人都有一些使用心得。本篇提出一種結合點和檔案評價的混合 P2P 評價系統(HPRS)的創新架構。 這個組合評價能使優良點對個別檔案評價以去除不良檔案下載。也能幫助點從系統中得到最大的好處，一方面能從壞點得到偶爾的好檔案，另一方面又能拒絕從好點來的意外壞檔案。HPRS 在網路模擬測試的結果顯示其在效能上有顯著的改善。

2、在網站服務中以資源分類爲基礎的溝通協調

（法國電話公司 Diala Abi Haidar(1,2), Nora Cuppens(2), Fr’ ed’ eric Cupens(2), Her’ e Debar(1)）

信託的建立在不同安全領域間的每個溝通協調是必須的，它被視爲是獲得保護資源存取權的第一步，在本論文中，我們介紹對保護資源的新分類方法，並利用這種分類法去定義在以狀態爲基礎的溝通協調過程的個體行爲，這個過程由兩個模組去運作的：溝通協調模式和例外處理模式，前者攔截存取的要求，它蒐集私密資料並根據現有的溝通政策交換政策規定。後者是在有例外事件發生時才會被前者呼叫到。所謂例外是指無法溝通而被拒絕或鎖定。

3、使用品質保證的統計方法在網格中管理行爲信託

（Marburg 大學電腦科學及數學系 Elvis Papalilo and Bernd Freisleben）

本篇中提出在網格運算環境中管理成員行爲信託的一種方法。它和產業生產過程一樣，在網格環境中考量成員的互動過程，本文認爲使用品質保證的統計方法就可以監控網格成員的行爲而能够發現誤差來獲得成員的行爲信託。

六、入侵偵測 (Intrusion Detection)

1、用偵測和蜜罐爲基礎的轉向 - ISP 用來防衛分散式阻斷服務攻擊的方式

（印度技術學院 Anjali Sardana，Krishan Kumar，R.C. Joshi）

TCP/IP 架構與生俱來的弱點造成了分散式阻斷服務攻擊者的機會，而能在瞬時間偵測到這些攻擊林林總總的方法不外乎針對低次數或高頻寬的攻擊，低次數攻擊會使網路服務品質慢慢下降而使之不容易被查覺，本文中用三道防線的方式來防衛。第一道防線是藉偵測小段時間內的低次數或高頻寬攻擊的熵(能量變化所造成的產能降低)的變化，第二道防線能在瞬時鑑別並標記攻擊動線，最後一道防線則將攻擊轉向到蜜罐伺服器阻延攻擊而能維持 ISP 應有的服務品質水準。本文在 Linux 平台的 ns-2 上模擬驗證了本方法的有效性。

2、IP 保護：偵測 Email 爲基礎的信心裂縫

（英國 Survey 大學 Neil Cooke Lee Gillam Ahmet Kondoz）

本文探討利用 email 來破壞信心是如何的容易，因爲公司的秘密和商業機密被洩露出去的情形愈來愈多，故也提出一套智慧型的外寄郵件篩選系統以防止秘密流出，本文在實驗了 50 萬封 Enron 郵件並運用語言學文集的一些技巧來減少由單純關鍵字篩選系統所做出的誤判警訊之後，提出以下詳細的報告，文中也考量了適當訊息可能因此被遺露的危險。

3、入侵偵測系統的非固定式 Markov 模型與異常事件增加分析

（Binghamton 大學電腦電機系 Arthur G. Tokhtabayev 及 Victor A. Skormin）

本文提出一個能夠減少誤判率的異常狀況入侵偵測系統，它利用以主機爲基礎的系統呼叫領域的新方法，就是將各個主機的相關異常情形報告給 IDS 伺服器知道。

在主機層級的一個創新偵測異常作法是將一項應用服務視爲非固定式的隨機過程，而以非固定的 Markov 鏈去建立模型，就可大大的提高模型的正確性。其利用伺服器程序偵測異常事件的增加；在網

路內誤判的警訊沒有增加的情況下，被偵測到的異常事件增加幾乎可確認是出於電腦蠕蟲所爲。否則警訊往往要被視爲誤判了。

4、立可信賴的由虛擬機器反推入侵偵測機制

（Pisa 大學資訊系 Fabrizio Baiardi, Daniele Sgandurra, Polo G. Marconi La Spezia）

Psyco-Virt 是一個高度有效的入侵偵測工具，因其連結主機及以虛擬機器反推的網路入侵偵測技術。Psyco-Virt 架構包含一組的虛擬機器 - 其由一些在上面跑預定的作業系統和應用軟體的被監控的虛擬機器，和一個更進一步的虛擬機器 – 反推型者所組成，分佈在被監控虛擬機器上的許多代理人執行網路及主機入侵偵測系統的工具以發掘嚐試入侵被監控虛擬機器的攻擊行爲。此反推虛擬機器運用一個反推器和導引器去發掘任何惡意改變核心程式、代理人程式或在受監控虛擬機器上運行的入侵偵測系統的企圖，如此偵測工具方值得信賴。在每個被監控的虛擬機器上都有一個蒐集器收集代理人程式發出的警訊，再透過控制網路轉寄給導引器，此控制網路乃代理人和反推虛擬機器間專門用交換資料用的，在反推虛擬機器上的導引器再篩選所有的警訊，如有偵測到企圖改變入侵偵測系統時會指派合適的行動給通知者去處理。在這種情況下，此受監控的虛擬機器不是被停止就

是被凍結，目前的狀態儲存到一個檔案後再來深入檢視。說明了 Psyco-Virt 後，本文再來討論一些使用反推的代理人和功能並展示了第一個雛型系統的初步結困和效能數據。

5、用時間數列平滑法和 Wavelet 分析及早偵測阻斷服務攻擊

（孟買 CDAC Pravin Shinde, Srinivas Guntupalli）

電腦網路的阻斷服務攻擊隨處可見，以氾濫爲手法的阻斷服務攻擊是很普遍的一種，偵測氾濫式阻斷服務攻擊的方法主要是找到資訊流量中忽然的改變而將之標記爲異常。本篇中我們提出考量網路流動爲時間序列的一種方法，並以指數移動平均將其平滑化，並以小波紋分析中的能量分佈法來分析此平滑曲線。本文使用的參數來代表流量的是每單位時間收到的字元數以及流入及流出字元數的比值，在分析了小波紋能量分佈的平滑時間序列、阻斷服務攻擊所帶來的流量增長後，就能很早就偵測到。本文所考慮的參數代表網路中各種不同的特性，偵測結果的正確性很高且少有誤判的情況。

6、實體環境偵測可疑樣態的安全模型

（澳門大學科學 Simon Fong, Shuang Yan）

破壞網頁外表是一種十分普遍的攻擊形式，但因網頁的動態性很

高，不同網頁間的動態性也差異很大，自動偵測這種未經授權的網頁改變是很困難的，本文一種創新的偵測方法，是以基因程式設計(GP)爲基礎。這種程式設計是爲了演算法能自動產生而建立的進化計算典範。在此領域內，GP 會顯得特別有吸引力的原因是它不需要倚靠任何領域專屬的知識，要分析描述這些知識永遠都是很困難的工作。在起初的學習階段，GP 是以讀入一序列監控中的遠端網頁和一組的攻擊行爲所建立的演算法，然後，本文在一定的時間區間應用該演算法監控遠端網頁，如有發現可疑的改變就發出警訊，以本文先前提出較廣泛的網頁偵測架構爲基礎，本文發展了雛型用本文的方法去測試 15 個動態網頁，觀察了約一個月，並蒐集了一些網頁遭改掉的實際案例。在和稍早本文發展的以領域專屬知識爲基礎的設計作了比較之後，顯示 GP 可能是做這種工作的有效方法。

七、入侵防阻 （Intrusion Prevention）

1、 學習式網路攻擊弱點評估圖之應用（ vulerability assessment by learning attacks specifications in graphs）

本文提出一種漸進式的演變方法，依據描述情節而學習網路攻擊的方式 。宗旨將發現網路弱點，使其一次攻擊減到最小的費用而達到最大衝擊。雖然本文集中於內部的威脅, 提出的方法適用於一般網路服務, 包括社會網路和電腦網絡。

2、自動元件修補器對緩衝器的溢位攻擊 (Automatic Patch Generation for Buffer Overflow Attacks)

控制攔截攻擊（*Control-hijacking attack*）利用作業系統的漏洞，最終控制或接管基礎的硬體設施。雖然多數的控制攔截攻擊（*Control-hijacking attack*）工作已事先被察覺或預防，但是大多數的網路服務的問題沒有被註記，以防止同樣攻擊事件一再重複發生。

觀念上，郵件式的網路攻擊的組成是由一個具有攻擊性的簽名元件，並創造一個規則可通過防火牆或闖入預防系統阻攔檢測攻擊，且爲了可成功的抵擋已偵測的攻擊以及其他的變種，修補產生器元件產生修補來持續的消除攻擊過的弱點。

本文描述設計, 完成及評估程式轉換及執行追蹤分析的系統稱爲 PASAN，此程式可以自動促成網路服務的程式偵測控制攔截攻擊（*Control-hijacking attack*） *且自動的經由*修補產生器元件產生修補。

本文執行了第一代 PASAN 雛型作爲 GNU C 編譯器的延伸，其目的在於以堆疊爲基礎造成**緩衝器**溢位攻擊，使其能達到與控制攔截攻擊（*Control-hijacking attack*）*相符的效果。利用網路的七層架構及已知的修補程式*，測試這個 PASAN 雛型可自動的修補成功。另外，這些自動化修補產生器都具有相似的結構並手工產生；除了二個程式

之外,ＣＵＰ消耗量在執行 PASAN 時僅約 10%-23%,。

3、從獨立式攻擊保護IP多媒體子系統服務傳遞平台（Protecting IP Multimedia Subsystem (IMS) Service Delivery Platform from Time Independent Attacks）

了整合使即將浮現的行動多媒體服務-例如多媒體簡訊服務，按一下即可撥出通話並橫跨網路連接多種不同的會議形式和*無縫多媒體串流服務。 這確定了手機中*聲音與資料綜合化，帶領總體網際網路電信合併。

IP 多媒體子系統(IMS)被視爲下一世代在這整合性的通訊世界中主要傳遞訊息的平台。其內容模組設計包含開放式使用者介面並經由 IP 技術,更靈活的提供多媒體服務的能力。

在這新興技術平行開放的同時，來自複合通訊平台如 IP，SIP 及 RTP 需要接受更多的安全性的挑戰。在這篇文章裡我們的宗旨將開發安全模型來保護 IMS 服務交付平臺(SDP)，免其受到 SQL injection 及媒體流(media flow)攻擊。這些攻擊最終還是回歸於增值服務等應用。

最後，本文將在 Fokus Fraunhofer testbed 展示目前的現實社會中最推薦最佳的解決方案。

4、使用HMM模型分析環境信息（Cyber Threat Trend Analysis Model Using HMM）

一般公認防禦惡意駭客或攻擊者最好的策略之一即是預防。渴望部署更好的預防機制激勵著許多研究威脅的趨勢分析模型的安全研究人員和實作者。然而，基於趨勢是隱性的本性上，威脅趨勢是不會從時間序列數據上直接顯示出來。此外，傳統的時間序列分析預測未來趨勢的模式靠的僅僅在過去的趨勢模式，並不適合去預測動態網絡環境下（例如，網際網路）的趨勢模式。因此，爲了從隱藏原始數據資料上發現趨勢模式，補充環境信息是必須的。在本篇論文中，我們將補充環境信息帶入*隱馬爾可夫模型(HMM)*趨勢分析來提出本文*之網絡威脅的趨勢分析模型*。

5、以隱藏的馬爾可夫模型(Markov)和線上自動控制風險評估做分散式入侵預報和預防之架構（DIPS: A Framework for Distributed Intrusion Prediction and Prevention Using Hidden Markov Models and Online Fuzzy Risk Assessment）

本文提出了一種分散式入侵預防系統(DIPS)，透過大網絡中的幾個入侵預防系統(IPS)所組成，所有系統都互相或與中央伺服器溝通，有利於進一步的網絡監測。隱藏的馬爾可夫(Markov)模型提出在

分佈式環境的入侵的檢知、檢出時，並先一步預測以防止可能出現的嚴重入侵。分散式入侵預防系統(DIPS)基於預測到威脅級別和被保護的資產有評估到風險時被啓動。入侵意圖被阻擋依據是：(1)已發生嚴重的攻擊事件(2)封包流量速率 (3)預測到可能的嚴重入侵(者)(4)線上風險評估資產可能被入侵者取得。本篇論文針對入侵企圖的分散式監控，採用模糊推理系統先一步預測這樣的企圖以及做線上風險評估。初步實驗結果表明，該架構能有效的做即時分散式入侵監測和預防。

八、資料安全與隱私 （Data Security and Privacy）

1、執行隱私性透過規格化方式來驅動XACML(eXtensible Access Control Markup Language，以XML爲基底提供在網際網路上資訊存取呈現的控制策略)架構：

現今於企業中執行隱私性被認爲是件衝擊性議題，實際上在軟體系統中，要去適用於規範的條文及規則是件很大的挑戰，包括要將企業中的各式條文及規則正式化，因爲在單一狀態下某一規則就可能影響整體隱私性。傳統存取控制爲了指派權利給個別使用者或規則而提供普遍性方法，但對隱私性來說這是不適合的方式，而且沒有提供工具滿足某些情況，就像限制某段時間讓隱密性資料能夠儲存。爲了在企業中執行隱私性，我們需要更好的存取控制方法在資料本身能保

證隱私性的各個情況可被反映。在文件中提供了新的解決方式就是透過規格化的方式，本文的規格化處理方法不同於去協定出單一作法，是將焦點放在產生存取控制政策，而在本文的軟體架構中更適合提供良好的存取從多樣的資料來源。

2、卡片包(CardSpace)中滿足隱私性議題

CardSpace(類似資訊卡)爲微軟最近所採用的數位認證管理系統，在此資料中本文針對CardSpace發現2項安全性缺點將引起嚴重隱私性侵犯。第1項缺點是網際網路使用者對於服務供應者可信賴性判斷的信賴度，第2項缺點是系統單一層認證的信賴度，本文也提出滿足這2項缺點的解決方案。我們的解決方案可相容於現行的CardSpace認證轉移系統，並在CasrdSpace架構下以較小幅度的更動來加強系統隱私性，本文也同時提供此解決方案的安全性及效能性分析。

3、委外商業流程中保護品質的模式化

有許多研究文件與標準對於委外資料安全性多有涉略，然而大部分文件所提出新的控制方法是針對存取及保護資料，而不是評估現行整體流程保證標準。此文件主要提出的方法是藉由匯集複雜商業流程中獨特工作的安全特性而整理出可接受的整體流程保證標準，此方法

所考慮的是商業流程中可被委外的工作項目而非評估可靠的合作夥伴，並從已建立的理想商業流程模式中選擇出具有較高保證的商業流程。

4、格網運算輕量級中等設備 (Lightweight Middleware for Grid Computing, gLite)的安全性儲存服務

格網運算輕量級中等設備的安全性儲存服務提供使用者多種工具透過安全路徑與加密資料(如：醫療及金融資料)存放於格網儲存環境，資料的儲存透過所提供之工具只可被有認證過的使用者取得與讀取。此外，能解決內部人員濫用問題也預防儲存環境的管理者以非加密格式存取機密資料，在TriGrid 虛擬實驗室(TriGrid VL)專案內容中，這樣的服務已爲歐盟的e-sicence格網計畫(EGGE)專案的格網運算輕量級中等設備所設計與發展

九、認證及輸入管制（Authentication/Access Control）

1、使用非交替半群法則的驗證結構

本文提出一份新雙驗證結構，這是依據公／私密金鑰對問題(Diffie-Hellman conjugacy problem)所演化自 Sibert-Dehornoy-Girault 的驗證結構概念，在上述結構中的一些參數能有更有效率的乘法規律，本

文概略地描述所提的驗證結構證明是安全的。

2、存取控制與安全保證的安全模式理論

先進的駭客技術同時也促進網路安全更有效率的防護，在近幾年來由研究者與企業提出許多安全性解決方案，大部分的焦點放於如何加強安全模式的功能與性能，但少部分強調安全模式保證評估。安全性保證打算提供安全性等級以代替系統有多安全的真實測量，安全性保證應能被數據化與可被控制於安全管理週期流程。在這文件中，本文提出一個安全模式－物件連結聚合(OAB)，可將多個存取控制政策一致化，並提供客觀性評估作爲網路安全保證的信賴標準。基於 OAB 的設計原則，透過 OAB 的標準(稱爲網路安全政策輔助工具, NSPA)來執行。

3、效果性基礎存取控制模式

在資料分享電腦化環境中要達成隱私性保護是件有挑戰性的問題。維持資料存取政策隱私性的需求應該要專業化，這是爲了使隱私性政策與實際上執行之間能夠建立一致性，以這概念作爲存取控制的基礎，將使隱私性政策更具體化。隱私性政策應該要保證資料能達成其預期性效果，而存取效果也應隨同資料的預期性效果來達成。這文

件透過虛擬作業系統機器(Virtual DOS Machine, VDM)來呈現這方式如何將隱私性政策具體化，效果性基礎存取控制模式中的本質是可被具體化的，在隱私性政策中的隱私性需求也是可被具體化，而模式中的運算與證明法可被設計與研究。

4、範圍管理模式作爲混合階層式的角色基礎存取控制

因爲使用角色基礎存取控制(RBAC)方法可有多種好處，故最近這樣的系統管理方式很盛行，這樣的控制方式依各個角色管理其控制政策，所以其管理功能以分散式管理且更有效率。然而，現有RBAC管理模式卻無法處理混合階層式的角色基礎存取控制特別在於具體性的細微RBAC政策需求。文件中我們所提範圍管理模式作爲混合階層式的角色基礎存取控制(SARBAC07)，這是最早以管理式範圍的概念應用於這樣的模式中。本文所提的此一模式除保有原始模式的優點外，更能處理混合階層式所需的複雜狀態。

叁、心得與建議

茲將與會期間所獲心得及建議分述報告如下：

一、國現行 GPKI 政策下核發之 PKI 憑證，其有效安全期限面臨挑戰，相關憑證使用 RSA 長度及 SHA1 方法盡速予以檢視

DR Milan Markovic 於現代電腦網路的加密協定專題中指出，美國所公布的 NIST SP800-57-A 與 SP800-78 報告提出：RSA 1024 bits 金鑰，對將於 2010 年有被破解風險機率，並明確的建議在 2010 年 12 月 31 日以後不要再使用 RSA 1024 bits 金鑰對，必須就改用 RSA 2048 bits，以提高安全強度。另依據 NIST SP800-57-A 的報告 RSA 2048 bits 這樣的密碼安全強度預估可以用到 2030 年，且依目前行政院研考會所訂 GPKI 憑證政策的規範，RSA 2048 bits 金鑰使用期限可達 10 年。

爲提高安全性及延長 PKI 憑證 IC 卡使用期限，一方面可以節省民眾購卡的費用，一方面可以減少民眾換發 IC 卡的不便，自然人憑證等政府機關核發之 PKI 憑證實有必要即刻著手規劃更換金鑰長度爲 2048bits 之相關事宜，並修改 GPKI 之 CP 及 CPS 俾利通盤研討金鑰期限。

二．資安策略措施及效益宜予檢討

防毒軟體、防火牆及入侵偵測（IDS）爲各機關建構資安體系的鐵三角，但隨著駭客入侵型態的快速演化，及資安設備功能的日新月異，政府機關之資安防護措施，實有定期檢討改進的必要，進而研訂資安政策，落實實質以資安設備而言，前述之鐵三角已不足以有效防止惡意攻擊事件，而須要再依資訊系統架構功能，研擬細步防護工作，如：

(1)防毒應包含信件防毒牆、網頁瀏覽防毒牆及個人端防毒牆裝置；(2)網路監控除入侵偵測系統外，尚應包含流量管制及高危險網站之過濾與阻擋措施;(3)建置 AP 防火牆以攔截駭客利用網路應用程式之漏洞進行入侵攻擊。而建立資安區域聯防機制，事先蒐集資安攻擊資訊，須爲建立防患網及特定回復流程，皆可有效強化資安措施。

此外，人的因素（human factors）也不可忽視，從教育訓練到資安稽核，到內部自我檢測（包含資安通報演練、弱點掃瞄、滲透測試及內部監控），都爲資訊安全整體防護作爲的主要工作之一。

三・研討改進自然人憑證之載具設計

自然人憑證爲現階政府提供民眾申請核發具有 PKI 機制的憑證，民眾可利用其具有網路身份認證及確保資料傳輸安

全的功能，享受政府部門的各項網路申辦業務。惟鑑於資訊科技日新月異，且個人化資訊產品不斷推陳出新，有關自然人憑證載具之設計與選用，宜隨資訊社會之潮流不斷研討創新。就現有載具 IC 卡之設計是否改採可移動性方式，以因應個人化需求；IC 卡除採現行接觸性 IC 卡外，可研究以雙卡設計方式，另增加非接觸性 IC 卡，以提昇應用之方便性（如具感應功能之間員工卡）；同時，使用讀卡機爲目前自然人憑證推動主要阻力之一，若能研究以 USB 爲載具供民眾選用，將有助於憑證之推廣應用。

四．加強國際資安合作與交流

資安事件資訊之蒐集，發生後之系統回復作業及駭客之查察，有賴國際合作；資訊安全科技之發展與應用更須隨時與海外學者專家相互交流，故邀請海外 PKI 專家學者參與國內相關研討會，除可客觀檢視我ＧＰＫＩ運作方式、並可將我推展自然人憑證之成果向國際宣傳。

就參加 ISA2007 之學者專家而言，下列人士皆可供作相關研討會邀請參考對象。 (1)Patrick Wang 是美國東北大學的全職教授及其他著名大學的客座或訪問教授，並著有 20 幾本資

安專書和 120 多篇的資安論文，同時也享有多項歐美的專利權，目前也是「模式鑑識和人工智慧期刊(IJPRAI)」的主編。

(2) DR Milan Markovic 主講「現代電腦網路加密協定－結合憑證簽發及安全機制」，目前任教於 Belgrade 大學，爲國際著名 PKI（公開金鑰）專家，且爲歐洲 FESA forum of European Supervision Authorities）會員。

(3) DR Ajith Abraham 係「2007 國際資訊認證安全研討會」主席，爲挪威科技大學教授，也爲歐洲 IEEE 協會成員。此三位皆國際資訊安全技術理論及實務經驗豐富人士，若能與保持進一步合作，透過渠等與國際相關團體進行交流活動，非但可客觀檢視我現有自然人憑證運作方式，並可將我推展 PKI 成果向國際宣傳。

肆、附件

附件一　照片

IAS 2007 於英國曼徹斯特大學之會議場所

與大會主席 Dr. Ajith Abraham 等人交換資安措施意見

我國旅美教授 Dr.Patrick Wang 報告「生物鑑識智慧資訊系統及應用」

Dr. Milan Markovic 講授「現代電腦網路加密協定」情形

各種不同 PKI 憑證與 IC 卡之讀卡機

GISCO 公司報告資安策略圖照

德國報告網格電腦之資安架構

會後與 Dr. Milan Markovic 交換 PKI 憑證應用經驗

附件二 研討會議程

IAS 2007 Final Programme

* Workshops (for the full programmes please refer to their respective Web sites):

- 2007 International Workshop on Data Hiding for Information and Multimedia Security (Thursday 30th August 2007, Location: Boardroom Level 6)
- 2007 International Workshop on Computational Forensics (Friday 31st August 2007, Location: Boardroom Level 6)

* Conference (click here for the pdf version):

Wednesday, August 29, 2007		
Time	**Activity**	
8:00 - 9:00	Reception	
9:00 - 9:15	Opening remarks Location: Cockcroft Theatre	
9:15 - 10:15	Keynote speech 1: Biometrics Intelligent Information Systems and Applications, *Patrick Wang* Location: Cockcroft Theatre Chair: Ajith Abraham	
10:15 - 10:45	Coffee/Tea break (Location: The Hub)	
Time	**Session A.1.1: Agent & System Security** Location: Cockcroft Theatre Chair: Jose Romero-Mariona	**Session B.1.1: Network Security 1** Location: Conference Room 6 Chair: Hannan Xiao
10:45 - 12:25	Organized Anonymous Agents *Martijn Warnier* and *Frances Brazier* Comparing the Trust and	Towards an Autonomic Security System for Mobile Ad Hoc Networks *Mohamad Aljnidi* and *Jean*

	Security Models of Mobile Agents *Michail Fragkakis* and *Nikolaos Alexandris* Program Fragmentation as a Metamorphic Software Protection *Bobby D. Birrer*, *Richard A. Raines*, *Rusty O. Baldwin*, *Barry E. Mullins* and *Robert W. Bennington* Accurate Application-Specific Sandboxing for Win32/Intel Binaries *Wei Li*, *Lap-chung Lam* and *Tzi-cker Chiueh*	*Leneutre* A Secure Authenticated Key Agreement Protocol for Wireless Communications *Pierre E. ABI-CHAR*, *Abdallah MHAMED* and *Bachar EL-HASSAN* Hierarchical Multi-Party Key Agreement for Wireless Networks *Sigurd Eskeland* and *Vladimir Oleshchuk* Applying Secure Data Aggregation Techniques for a Structure and Density Independent Group Based Key Management Protocol *Kashif Kifayat*, *Madjid Merabti* , *Qi Shi* and *David Llewellyn-Jones*
12:25 - 13:45	Lunch break (Location: The Hub)	
13:45 - 14:45	Keynote speech 2: How Cisco protects Cisco, *Paul King* Location: Cockcroft Theatre Chair: Ning Zhang	
14:45 - 15:00	Coffee/Tea break (Location: The Hub)	
Time	**Session A.1.2: Risk Assessment** Location: Cockcroft Theatre Chair: Tzi-cker Chiueh	**Session B.1.2: Panel** Location: Conference Room 6 Chair: Ning Zhang
15:00 - 16:40	Dynamic Control Approach to Risk Mitigation in Computing	Levels of Authentication Assurance: an Investigation

	Infrastructures *Reiko Ann Miura-Ko* and *Nicholas Bambos* Risk Management in Coalition Networks *Wim Mees* Operational Risk: Acceptability Criteria *Daniel Gideon Dresner* and *Robert Wood* Modeling Security Protocols as Games *Mohamed Saleh* and *Mourad Debbabi*	*Aleksandra Nenadic*, *Ning Zhang*, *Li Yao*, *Terry Morrow*
16:40 - 17:00	Coffee/Tea break (Location: The Hub)	
Time	**Session A.1.3: Trust Management** Location: Cockcroft Theatre Chair: Nick Bambos	**Session B.1.3: Network Security 2** Location: Conference Room 6 Chair: Martijn Warnier
17:00 - 18:15	HPRS: A Hybrid P2P Reputation System Using File and Peer Rating *Srinivasan T*, *Varun Ramachandran* and *Arun Vedachalam* Resource Classification Based Negotiation in Web Services *Diala Abi Haidar*, *Nora Cuppens*, *Frederic Cuppens* and *Herve Debar*	A Performance Comparison of Wireless Ad Hoc Network Routing Protocols under Security Attack *Su Mon Bo*, *Hannan Xiao*, *Aderemi Adereti* and *James A. Malcolm* On Detecting Selfish Packet Droppers in MANET: A Novel Low Cost Approach *Tarag Fahad*, *Djamel*

	Managing Behaviour Trust in Grids Using Statistical Methods of Quality Assurance *Elvis Papalilo* and *Bernd Freisleben* *Djenouri* and *Robert Askwith* Binding Update Authentication Scheme for Mobile IPv6 *Irfan Ahmed*, *Usman Tariq*, *Shoaib Mukhtar*, *Kyung-suk Lhee*, *S.W. Yoo*, *Piao Yanji and ManPyo Hong*	
19:00 - 22:00	Conference Reception (Location: Weston Room 1)	
Thursday, August 30, 2007		
Time	**Session A.2.1: Intrusion Detection 1** Location: Conference Room 5 Chair: Cor Veenman	**Session B.2.1: Tutorial A 1** Location: Conference Room 6 Chair: Patrick Wang
9:00 - 10:15	Detection and Honeypot Based Redirection to Counter DDoS Attacks in ISP *Anjali Sardana*, *Krishan Kumar Saluja* and *R. C. Joshi* IP Protection: Detecting Email Based Breaches of Confidence *Neil Cooke*, *Lee Gillam* and *Ahmet Kondoz* Non-Stationary Markov Models and Anomaly Propagation Analysis in IDS *Arnur G. Tokhtabayev* and *Victor A. Skormin*	Intelligent Pattern Recognition and Applications *Patrick Wang*
10:15 - 10:45	Coffee/Tea break (Location: The Hub)	

Time	**Session A.2.2: Intrusion Detection 2** Location: Conference Room 5 Chair: Sandro Bartolini	**Session B.2.2: Tutorial A 2** Location: Conference Room 6 Chair: Patrick Wang
10:45 - 12:25	Building Trustworthy Intrusion Detection through VM Introspection *Fabrizio Baiardi* and *Daniele Sgandurra* Early DoS Attack Detection Using Smoothened Time-Series and Wavelet Analysis *Pravin Shinde* and *Srinivas Guntupalli* A Security Model for Detecting Suspicious Patterns in Physical Environment *Simon Fong* Detection of Web Defacements by Means of Genetic Programming *Eric Medvet*, *Cyril Fillon* and *Alberto Bartoli*	Intelligent Pattern Recognition and Applications (continued) *Patrick Wang*
12:25 - 13:45	Lunch break (Location: The Hub)	
Time	**Session A.2.3: Cryptography & Applications 1** Location: Conference Room 5 Chair: Tzi-cker Chiueh	**Session B.2.3: Security Requirements & Policies** Location: Conference Room 6 Chair: Danny Dresner
13:45 - 15:00	Threshold SKI Protocol for ID-based Cryptosystems	On the Definition and Policies of Confidentiality

	Ashutosh Saxena An LSB Data Hiding Technique Using Prime Numbers *Sandipan Dey*, *Ajith Abraham* and *Sugata Sanyal* Low-cost Anonymous Timed-Release Encryption *Dimitrios Hristu-Varsakelis*, *Konstantinos Chalkias* and *George Stephanides*	*Johs Hansen Hammer* and *Gerardo Schneider* Enhanced Availability and Security by Rate Control Using Extended Policy Framework in SELinux *Pravin Shinde*, *Priyanka Sharma* and *Srinivas Guntupalli* CCARCH: Architecting Common Criteria Security Requirements *Jose Romero-Mariona*, *Hadar Ziv* and *Debra J. Richardson*
15:00-15:30	Tea/Coffee break (Location: The Hub)	
Time	**Session A.2.4: Cryptography & Applications 2** Location: Conference Room 5 Chair: Sergio Damas	**Session B.2.4: Intrusion Prevention** Location: Conference Room 6 Chair: Mario Refice
15:30 - 17:35	Integrating Multi-Modal Circuit Features within an Efficient Encryption System *Evangelos Papoutsis*, *Gareth Howells*, *Andrew B. Hopkins* and *Klaus McDonald-Maier* A Secure Authenticated Key Agreement Protocol Based on Elliptic Curve Cryptography *Pierre E. ABI-CHAR*, *Abdallah MHAMED* and *Bachar EL-HASSAN*	Vulnerability Assessment by Learning Attack Specifications in Graphs *Virginia N. L. Franqueira* and *Raul H. C. Lopes* Automatic Patch Generation for Buffer Overflow Attacks *Alexey Smirnov* and *Tzi-cker Chiueh* Protecting IP Multimedia Subsystem Service

	Inclusion of a Montgomery Multiplier Unit into an Embedded Processor's Datapath to Speed-up Elliptic Curve Cryptography *S. Bartolini*, *G. Castagnini* and *E. Martinelli*	Delivery Platform from Time Independent Attacks *Muhammad Sher* and *Thomas Magedanz* Cyber Threat Trend Analysis Model Using HMM *Do Hoon Kim*, *Taek Lee*, *Sung Oh D. Jung*, *Hee Jo Lee* and *Hoh Peter In* DIPS: A Framework for Distributed Attack Prediction and Intrusion Prevention Using Hidden Markov Models and Online Fuzzy Risk Assessment *Kjetil Haslum* and *Ajith Abraham*
19:00 - 21:30	Conference Banquet (Location: Albert's Shed Restaurant, 20 Castle Street, Manchester M3 4LZ - see it on a map)	
Friday, August 31, 2007		
Time	**Session A.3.1: Data Security and Privacy 1** Location: Conference Room 5 Chair: Robert McAdoo	**Session B.3.1: Security Analysis** Location: Conference Room 6 Chair: Elvis Papalilo
9:00 - 10:15	Enforcing Privacy by Means of an Ontology Driven XACML Framework *Dhiah el Diehn I.Abou-Tair*, *Stefan Berlik* and *Udo Kelter* Addressing Privacy Issues in CardSpace	Team Edit Automata for Testing Security Property *Zhenrong Yang*, *Aiman Hanna* and *Mourad Debbabi* Analysing Security Threats against Network Convergence Architectures

	Waleed A. Alrodhan Second-LSB-Dependent Robust Watermarking for Relational Database *Xiangrong Xiao*, *Xingming Sun* and *Minggang Chen*	*Patroklos Argyroudis*, *Robert McAdoo*, *Stephen Toner*, *Linda Doyle* and *Donal O'Mahony* Modelling Quality of Protection in Outsourced Business Processes *Fabio Massacci* and *Artsiom Yautsiukhin*
10:15 - 10:45	Coffee/Tea break (Location: The Hub)	
Time	**Session A.3.2: Authentication/Access Control** Location: Conference Room 5 Chair: Milan Markovic	**Session B.3.2: E-commerce Security** Location: Conference Room 6 Chair: Sandro Bartolini
10:45 - 12:25	An Authentication Scheme Using Non-Commutative Semigroups *Milton Chowdhury* SARBAC-HH: A Scoped Administration Model for RBAC with Hybrid Hierarchy *Yue Zhang* and *James B.D. Joshi* A Theoretical Security Model for Access Control and Security Assurance *Bo-Chao Cheng*, *Huan Chen* and *Ryh-Yuh Tseng* A Purpose-Based Access Control Model *Naikuo Yang*, *Howard Barringer*	Secure M-commerce Transactions: A Third Party Based Signature Protocol *Lisha He*, Ning Zhang, *Lirong He* and *Ian Rogers* Secure E-Commerce Protocol for Purchase of E-Goods *Satish RDevane*, *Madhumita Chatterjee* and *Deepak Phatak* An Effective and Secure Buyer-Seller Watermarking Protocol *Ibrahim M. Ibrahim*, *Sherif Hazem Nour El-Din* and *Abdel Fatah A. Hegazy*

	and *Ning Zhang*	
12:25 - 13:45	Lunch break (Location: Weston Restaurant)	
Time	**Session A.3.3: Data Security and Privacy 2** Location: Conference Room 5 Chair: Robert McAdoo	**Session B.3.3: Tutorial B 1** Location: Conference Room 6 Chair: Milan Markovic
13:45 - 15:00	A Secure Storage Service for the gLite Middleware *Diego Scardaci* and *Giordano Scuderi* An Architecture for Privacy Preserving Collaborative Filtering on Web Portals *Waseem Ahmad* and *Ashfaq Khokhar*	Cryptographic Protocols in Modern Computer Networks - Combining Authentication and Secure Payment *Milan Markovic*
15:00 - 15:30	Coffee/Tea break (Location: The Hub)	
Time		**Session B.3.4: Tutorial B 2** Location: Conference Room 6 Chair: Milan Markovic
15:30 - 17:00		Cryptographic Protocols in Modern Computer Networks - Combining Authentication and Secure Payment (continued) *Milan Markovic*

附件三　現代電腦網路的密碼協定 － 憑證簽發與安全機制的結合

內容

- 引言
- 現代電腦網路的潛在弱點
- 多層次安全機制的基礎架構
- 現代電腦網路的密碼協定
- PKI(公鑰基礎架構)系統
- 智慧卡與硬體安全模組(HSM)
- 一些安全機制的新趨勢
- 憑證簽發與安全付款機制的結合
- 結語

引言

- 本個別化的教學指引是針對現代電子商務領域逐漸形成的主題 － 植基於公鑰基礎架構(PKI)的電腦網路安全系統所作的討論。
- 本文會探討 TCP/IP 電腦網路的一些弱點及其可能的防範技術。
- 本文會指明僅有多層次安全機制能應付對網路安全系統的攻

擊。

- 本文也對 PKI 系統的主要元件做概略的介紹，強調憑證簽發機構在建立合法使用者的唯一加密身分時使用 ITU-T X.509v3 的數位憑證技術。
- 公鑰密碼學使用公開及私密金鑰、數位簽章、數位憑證和信任的第三人憑證簽發機構，以符合電子商務安全的主要規定。
- 應用此類的安全機制之前您得先回答以下問題：誰是你的 CA(憑證簽發機構)？你的私密金鑰置於何處？你如何知道你所交談的個人或伺服主機的私鑰是安全的？在那裡找得到憑證？
- 公鑰基礎架構(PKI)提供了上述問題的答案。

現代電腦網路的潛在弱點

- 沒有建置安全管制和方法，你的資料可能遭受攻擊。
- 有些攻擊是消極的，資訊僅被側錄或監聽。
- 有些攻擊則是積極的，資訊可被竄改，意圖破壞資料及網路本身。
- 如果沒有安裝安全機制，你的網路及資料的弱點可能遭到以下方式的 TCP/IP 網路攻擊。
    - 身分騙取，網路釣魚

- 網路竊聽
- 資料竄改
- 身分僞裝(IP 位址僞裝)
- 密碼基地攻擊
- 組斷服務攻擊
- 中間人攻擊
- 破解金鑰攻擊
- 嗅探器攻擊
- 應用程式層攻擊

身分騙取，網路釣魚

- 今日最常見的網路詐騙攻擊之一。
- 僞裝成某組織的網站發出正常的使用者身分通告(重設、管理者需要等)，要求使用者填寫身分確認(或信用卡號或其他)。
- 網路釣魚是針對銀行服務的新網路騙術。
- 此乃針對網路銀行或 email 的無人服務，攫取使用者的認證資料，用以從真正的網站偷取金錢。
- 網路釣魚是最早的一種安全破口，可利用簡單的方法騙取

大量的金額，吸引了對網路銀行的組織犯罪。

網路竊聽

- 大體來說，多數的網路傳輸都是以明文(非加密)格式的，使攻擊者能在可及的網路範圍內監聽及讀取資訊。
- 攻擊者的網路竊聽行爲也被稱爲嗅探或窺探。
- 企業主管面臨的最大的安全問題通常是網路竊聽者監控網路的能力。
- 沒有以密碼學爲後盾的強力加密服務，資料在網路傳遞時可能被其他人讀取。

資料竄改

- 攻擊者讀取資料後，最合情理的下一步就是竄改它。
- 攻擊者能改掉資料包內的資料而不被寄件者或收件者知悉。

身分僞裝

- 多數網路或作業系統使用 IP 位址作爲辨識電腦在網路上的真實身分。

- 有些情況 IP 位址可能被誤用，這種就稱爲身分僞裝。
- 攻擊者可能使用特別的程式建構 IP 封包使它看起來像某企業內部網路所發出來的。
- 在以正確的 IP 位址得到網路的存取權限後，攻擊者能夠修改、轉寄或刪除資料。

密碼基地攻擊

- 大多數的作業系統和網路安全規劃皆以密碼對群組做存取控制，就是以使用者帳號及密碼來決定對電腦及網路資源的使用權；早期的作業系統元件不一定對使用者身分資訊作加密保護而任其在網路上傳輸，用以識別使用者本身在網路上的身分。如此監聽者可以藉獲得正確的使用者名稱及密碼來控制網路，例如若使用者爲管理者時，攻擊者就能新增一些帳號以供其隨後使用。
- 於獲得正確帳號，攻擊者即能對網路進行以下動作：
  - 攫取正確使用者清單、電腦名稱、及網路資訊。
  - 修改伺服器及網路設定，包括如存取控制及路由表等。
  - 變更、重轉、或刪除資料。

組斷服務攻擊

- 和密碼基地攻擊不一樣，阻斷式服務攻擊會阻攔正確使用者正常使用電腦及網路。
- 在獲得網路使用權後，攻擊者可以進行以下的行動：
  - 干擾資訊管理者使其無法立即偵測到入侵事件，這樣攻擊者才有機會進行更多的攻擊。
  - 發送不正確的資訊給應用程式或網路服務，導致其關閉或不正常運作。
  - 發送大量資訊以癱瘓電腦或整個網路。
  - 阻斷網路使合法使用者無法使用網路資源。

中間人攻擊

- 如其名所示，中間人攻擊指某人嚴密監聽、攫取、控制兩個正在通訊中的使用者間的一切訊息而不被發現。
  - 例如中間人可以和兩使用者商討加密金鑰的方法。
  - 然後各使用者傳送加密資料給此能解密的攻擊者。
  - 當電腦進行較低層的網路傳輸時，電腦可能無法辨識和其交換資料的對方是誰。

破解金鑰攻擊

- 金鑰是一個密碼或數字用來加解密或驗證安全資訊。
- 雖然破解金鑰對攻擊者而言是曠日耗時的困難過程，但仍存在有破解的可能性。
- 一旦攻擊者找到了金鑰，那個金鑰就被稱爲破解金鑰。
- 攻擊者於是用破解金鑰去存取原以爲安全的通訊管道而不被收送兩方發現遭到攻擊。
- 攻擊者以破解金鑰來解開並更改加密資料。
- 攻擊者也可嚐試用破解金鑰來計算出更多的金鑰來，或許可藉此獲得更多安全通訊管道的存取權。

嗅探器攻擊

- 嗅探器是指能讀取、監控或攫取網路資訊交換或封包的應用程式或硬體裝置。
- 如果封包沒有加密，嗅探器就能提供封包內的完整資料內容。
- 沒有加密的資料包，即使有經過封裝(挖洞埋藏)，還是可以被打開來看的。

- 使用嗅探器，攻擊者能進行以下動作：
  - 分析網路及存取資訊，最後可讓網路停止回應或錯誤回應。
  - 讀取隱私資訊。

應用程式層攻擊

- 應用程式層攻擊的標的物是應用程式主機，意圖使該主機上的作業系統或應用程式產生錯誤。
- 這種錯誤的結果可令攻擊者躲開正常的存取管制。
- 攻擊者可趁機控制應用程式、主機或網路，再進行以下行動：
  - 讀取、新增、刪除、修改資料或作業系統。
  - 引入病毒並利用程式及網路擴散病毒。
  - 引入嗅探器程式分析網路獲取資訊，最後可讓網路停止回應或錯誤回應。
  - 異常關閉資料、程式或作業系統。
  - 解除其它的安全管制使之能發動下一波的攻擊。

- 防止攻擊的可能方式

- 加密 – 資料及密碼的隱私保護。
- 運用數位簽章技術 – 提供憑證簽發、完整性保護及不可否認性。
- 嚴格的憑證簽發程序 – 通訊雙方建立起安全的憑證簽發管道。
- 使用強固的金鑰及經常換鑰程序 – 防止破解密碼分析。
- 網路位址轉譯(保護) – 保護使不致遭阻斷服務攻擊。
- 使用 PKI 數位憑證 – 作爲通訊者的唯一電子 ID.
- 使用智慧卡 – 以產生金鑰、保護金鑰及產生數位簽章。
- 合宜的防毒、反垃圾信、反釣魚保護。
- 入侵偵測系統。

遠端交易需要私密性

遠端交易需要可認證性

遠端交易需要完整性

遠端交易需要不可否認性

安全技術

- 現代電腦 TCP/IP 網路的主要加密方式：
  - 以非對稱性加密技術爲基礎的數位簽章系統
  - 以對稱性加密技術爲基礎的密碼保全系統
  - PKI – 公鑰基礎架構

數位簽章

數位信封

雜湊函數

- 資料的雜湊函數值用來當作 ’ 數位指紋’ ，用來簽章及驗證。爲防止安全落差，此雜湊函數 H 必須滿足以下原則：
  - H 必須是抗碰撞的；就是說它在實務上是不可能發生碰撞的(兩個不同的數位文件映對到同一雜湊值視爲發生碰撞)。。
  - H 必須是單向函數；就是說它在實務上不可能由值域裡的

一已知字串去推出 H 在定義域的值。

- 碰撞的存在是無法免除的，但這僅是理論上的說法而已，然而更重要的是在實務上不可能找到碰撞(及定義域在映對前的值)。

合適的雜湊函數演算法

- 以下的雜湊函數有不同長度的映射值(SHA-224 是一種 224 位元的雜湊函數)，皆適合保證長期的安全性：
  - SHA-224，SHA-256，SHA-384，SHA-512[2]
  - 以上四個雜湊函數適合在往後六年(至少到 2011 年)運用於合格的電子簽章程序中。
- 下表針對雜湊函數作一總結說明。

適用至 2009 年底	與合格的憑證併用*: 適用至 2010 年底	適用至 2010 年底	適用至 20101 年底
SHA-1	SHA-1	RIPEMD-160	SHA-224, SHA-256, SHA-384, SHA-512

*即單指憑證的簽發和驗證，不含其它合格簽章資料的產生和驗證。

安全雜湊標準

演算法	訊息大小(位元)	團集大小(位元)	字元大小(位元)	訊息摘要大小(位元)	安全性[2](位元)
SHA-1	$<2^{64}$	512			
SHA-224	$<2^{64}$	512			
SHA-256	$<2^{64}$	512			
SHA-384	$<2^{128}$	1024			
SHA-512	$<2^{128}$	1024			

簽章程序

- 除了簽章金鑰的持有者以外不得由任何其他人來發出簽章。更明白的說，此意味著實務上無法經由對公開金鑰的運算後算出簽章金鑰。

RSA

■ 下表總結各有效年度所須的最小位元長度。

期別參數	至 2007 年底	至 2008 年底	至 2009 年底	至 2010 年底	至 2011 年底
n	1024(最小) 2048(建議)	1280(最小) 2048(建議)	1563(最小) 2048(建議)	1728(最小) 2048(建議)	1976(最小) 2048(建議)

RSA

■ n 的質因素 p 和 q 應該屬於同一位數，但不能太接近：

$$\varepsilon_1 < | \log2(p)-\log2(q) | < \varepsilon_2$$

■ 在此建議 ε_1 和 ε_2 的值分別爲 $\varepsilon_1 \fallingdotseq 0.1$， $\varepsilon_2 \fallingdotseq 30$。 質因數 p 和 q 是隨機且獨立的產生，但皆符合以上的限制條件。

■ 公開指數 e 是獨立於 n 被選出來的，但符合以下的限制式：

? [equation] ? 而由預選的 e 所計算出來的私密指數 d 其函式如下：

$ed \equiv 1 \bmod kgV(p-1, q-1)$

多層次安全基礎架構

- 金鑰安全在現代電腦網路應具備的功能有：
  - 使用者及資料認證
  - 資料完整性
  - 不可否認性
  - 私密性

多層次安全基礎架構

- 此意味著安全網路系統應包含以下功能：
  - 強固的使用者認證，
  - 無論經由有線或無線的 IP 網路傳輸都能確保資料的完整性，
  - 不可否認性，
  - 以上功能都可透過以非對稱式加密演算法爲基礎的數位簽章技術實現。
  - 此外，在整個流通過程中所傳輸資料的私密或機密性均可經由對稱性加密演算法來保護。
  - 現代電腦網路安全系統是由 ISO/OSI 的三層參照模式所組成的安全機制如下：
    - 應用層安全(後端對後端安全)機制建構於強固的使用者認證、數位簽章、機密保護、數位憑證、以及硬體代符

(如智慧卡)，

✧ 傳輸層安全機制建構於兩個網點間的密碼隧道(對稱式加密)以及強固的網點認證程序，

✧ 網路 IP 層安全機制提供網點間在網路層的大塊安全架構 – 保護使不遭外來的網路攻擊。

應用層安全機制

■ 應用層安全機制乃建基於對稱式及非對稱式的加密系統，它包含以下的功能：

- 可靠對應者的認證(非對稱式)
- 傳輸資料完整性的保護(非對稱式)
- 不可否認性(非對稱式)
- 應用層的保密措施(對稱式)
- 應用層安全領域最常見的通訊協定如下：S/MIME, PGP, Kerberos、應用層的代理伺服器、SET、主從式架構應用軟體的 API 加密系統等。
- 以上之通訊協定大多數是以 PKI X.509 數位憑證爲基礎，數位簽章技術以非對稱式演算法(如 RSA、DSA、ECDSA)爲基礎的，雜湊函數(MD5、RIPEND160、SHA-1、SHA-224、-256、

-384、-512)及保密方法則以對稱式演算法(如 DES、3DES、IDEA、AES、RC4 等)爲基礎的。

- 現代多數在主從式架構下的應用層安全協定如 S/MIME 及 API 加密系統是以數位簽章或數位信封的技術爲基礎的。

S/MIME – 認證需要 – 發送

S/MIME – 認證需要 – 接收

S/MIME – 私密需要 – 密碼

S/MIME – 私密需要 – 解碼

使用者認證

- 在應用層的安全系統也可由使用者認證程序所組成，此程序可能是一、二或三個元件的認證程序。
- 使用者認證程序有許多種，它們可能根據以下的元件所構成：
  - 使用者名稱/密碼 – PIN 碼 – 使用者已知的資訊，
  - 硬體代符 – 使用者所擁有的，
  - 生物特徵(如指紋) – 使用者身分識別。
- 有許多形式的認證程序是根據以上元件所組成的：
  - 以使用者名稱/密碼爲認證基礎 – 弱勢的認證，

- 使用者名稱 + 經由硬體代符所產生的動態密碼(一次有效)，這比上一個強點，但還不够格稱爲強勢使用者認證程序。
- 使用者名稱 + 經由硬體代符所產生的動態密碼 + 詢答程序 – 強勢使用者認證程序。
- 使用者名稱/密碼 + PKI 智慧卡 + 以 PKI X.509 數位憑證以及非對稱式密碼技術爲基礎的雙邊詢答程序 - 強勢使用者認證程序(比上一個更強)。
- PKI 智慧卡 + 生物特徵辨識 + 以 PKI X.509 數位憑證以及非對稱式密碼技術爲基礎的雙邊詢答程序 - 強勢使用者認證程序(比上一個更強)。
- 使用者名稱/密碼 + PKI 智慧卡 + 生物特徵辨識 + 以 PKI X.509 數位憑證以及非對稱式密碼技術爲基礎的雙邊詢答程序 – 最強勢的使用者認證程序。

強勢使用者認證程序

- 強勢使用者認證程序的等級是由兩個以上的元件程序並和雙邊詢答程序所組成。強勢使用者認證是合理安全性的一部份：
  - 資訊必須以適當的方法加以保護以確保僅通過識別、認證、或授權的人員能使用資訊。

- 使用者識別 – 由使用者 ID 確認身分的過程。
- 使用者認證 – 比對使用者提供的私密資料和已註冊資料以確認使用者身分的過程。
- 使用者授權 – 認證程序完成後，允許使用者使用其所要求的資訊的過程。

■ 以下爲強勢(2F)使用者認證系統的例子：

- 以 PKI X.509 爲基礎在使用者智慧卡上的 SSL 從屬認證。
- SSL 從屬認證 + 使用者名稱/密碼對應用軟體認證。
- SSL 從屬認證 + 使用者名稱/動態密碼(OTP)對應用軟體認證。
- 以 PKI X.509 爲基礎在應用層的專屬認證程序。

傳輸層的安全機制

■ 傳輸層的安全機制大多包含以對稱式加密演算法爲基礎的傳輸資料保護。

■ 這些系統大多在兩個網點間的傳輸層間建立起秘密通道，而此通道建立之前是要通過強勢認證程序的。

如此說來，這種系統是以對稱式演算法做成秘密通道，以非對稱式演算法做成雙邊詢答認證程序，而且以 PKI 數位憑證去認證兩

個網點間通道建立時的對稱會話金鑰。

- 傳輸層的安全系統最主要是用來保護使用者與網路瀏覽器程式或網頁伺服器間的通訊，而最常見的這類系統有：SOCKS(早期用的)，SSL/TLS，以及 WTLS。其中最多人使用的是 SSL(安全插座層)通訊協定，用來保護瀏覽器程式和網頁伺服器間的通訊。

第二部份內容 -

- 引言
- 現代電腦網路的潛在弱點
- 多層次安全機制的基礎架構
- 現代電腦網路的密碼協定
- PKI(公鑰基礎架構)系統
- 智慧卡與硬體安全模組(HSM)
- 一些安全機制的新趨勢
- 憑證簽發與安全付款機制的結合
- 結語

引言

- 對 ITU-T X.509 標準而言，PKI 系統是用被定義爲用來製作、管理、儲存、或取出那建基於公鑰密碼的硬體集合、軟體集合、角色、和程序。
- PKI 系統提供在合理技術及組織安全環境下可實現以下四個企業主要的安全功能：
  - 認證
  - 保護資料完整性
  - 不可否認性
  - 保護資料的私密性
- PKI 系統以數位憑證爲唯一的加密機制，在電腦網路中認證可靠的電子 ID

PKI 系統

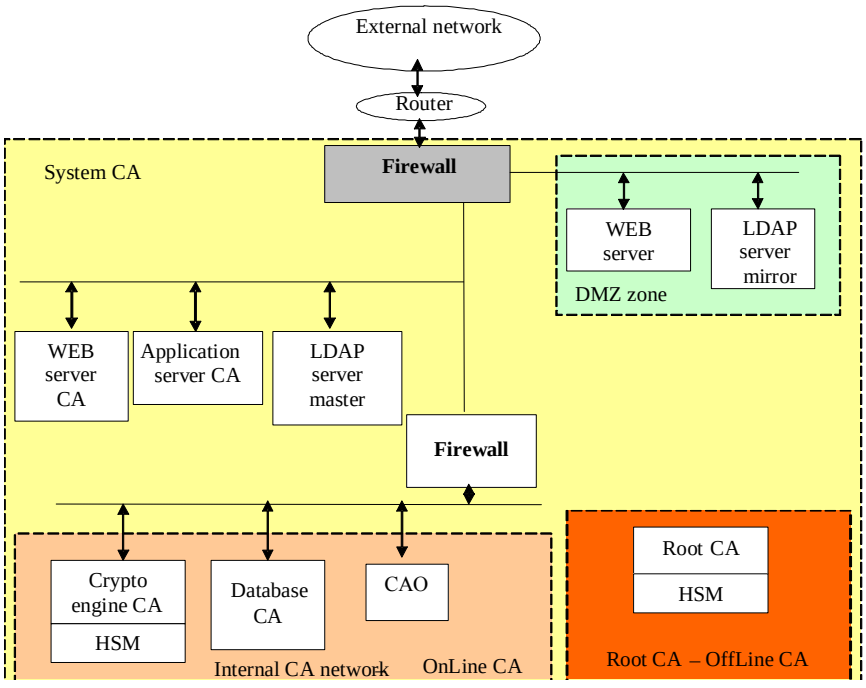
- PKI 系統包含以下的元件：
  - 憑證機構(CA) – 負責簽發、更新、收回憑證以及維護可收回憑證清單(CRLs)，
  - 註冊機構(RAs) – 負責接受憑證申請及驗證憑證持有者的身分識別，
  - 憑證發送系統 – 負責配送憑證給其持有人，

- 憑證持有者 – 被授與憑證的人、機器、或軟體，
- CP、CPS、使用者準則、其他基本的 CA 文件，
- 可收回憑證清單(CRLs)公告系統，
- PKI 應用系統(安全 WEB 交易、安全 E-mail、安全 FTP、VPN、安全網路付款機制、安全文件管理系統 – 安全數位儲存、邏輯存取控制系統等。)

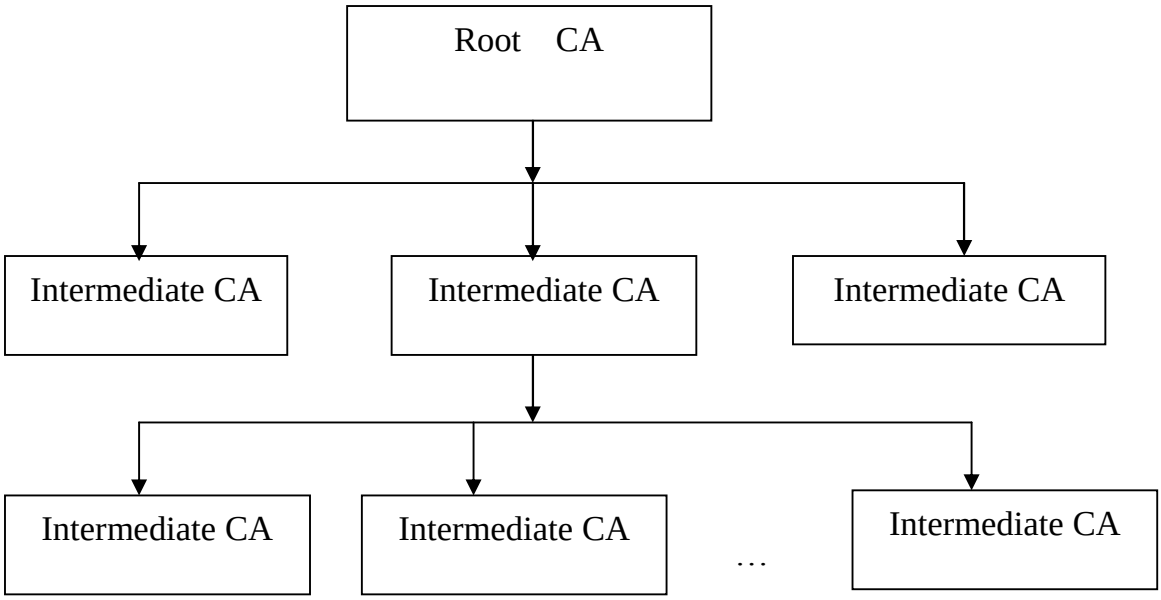
通用 PKI 系統

- 通用的 CA 是建基於 Web 憑證簽發系統，既可支援僅一兩個嚴密使用者設定檔的 PKI 封閉系統，亦可支援公鑰 PKI 系統的多使用者及不同的使用者註冊方式。
- 通用 CA 系統代表能處理不同使用者個別需求的客制化公開 CA 系統。

Generic PKI System - architecture



Generic PKI System - hierarchy



憑證生命週期管理

- 通用 CA 系統中，憑證生命週期管理包含以下程序執行：
  - 憑證更新，
  - 憑證停用及復用，
  - 憑證召回。
  - 這些功能是根據 CA 的憑證政策(CP)及憑證實務準則(CPS)所制訂的。

知慧卡和 HSMs

- 純軟體、純硬體及軟硬體組合間的安全系統之差異性。
- 因此，常見的智慧卡及硬體安全模組是較佳選擇。

- 硬體安全模組(HSM)爲近代電腦網路系統中很重要的安全性代表。
- 使用 HSM 有兩個主要的用意：加強系統的整體安全性並加速加密功能的執行(非對稱式及對稱式加密演算法、產生金鑰對等。)
- HSMs 主要是應用在伺服主機上，但在特別的資訊系統上(如政府、軍警)，也可用於終端電腦上。
- 在大量的個人使用上，智慧卡則爲較適合用的硬體安全模組。
- 然而，在大規模的用途上，爲了效能，最佳的的方案爲智慧卡及軟體的組合。
- 也就是說，智慧卡增加安全性，而軟體增進整體處理速度。依此而言，最適合的大規模解決方案爲：使用軟體處理大量的對稱式資料加解密，而智慧卡則用來產生數位簽章和讀取數位信封。

純軟體應用

純軟體安全限制….

- 憑證及私密金鑰儲存於傳統媒體

→ 不安全

- 消費者必須使用自己的電腦

→ 沒機動性

- 消費者要自己管理憑證

→ 不易使用

智慧卡和軟體模組的比較

- 智慧卡是安全性較佳組合型 …
- 軟體及智慧卡的組合可達最佳效能
- 用軟體來處理大量的資料加/解密
- 智慧卡用來讀取數位信封

- 發出簽章

軟體及智慧卡

應用

智慧卡架構 – 例子

軟體、硬體安全模組和智慧卡

應用

新的安全趨勢

- 合格的簽章
- 行動政府系統

- 智慧卡身分系統
- EMV 移植
- 多重應用的 EMV 付費卡

合格的電子簽章

- 根據 1999/93/EC 電子簽章條例於 2000 年 1 月 19 日所頒佈的，合格的電子簽章是含有如下進階功能的電子簽章：
- 是以符合 CCEAL4+標準(CWA14169)之安全簽章產生設備(SSCD)所簽發的，且
- 是由符合所有能簽發合格簽章需求的 CA 所簽發的合格簽章。
- 合格電子簽章和徒手簽章具同等法律效力。
- 憑證簽發機構是根據 ETSI ESI TS 101 862 “合格憑證資料檔”、 RFC 3739(網際網路 X.509 PKI：合格憑證資料檔)以及 RFC 3280(網際網路 X.509 PKI 憑證和憑證取回清單(CRL))簽發合格的電子憑證給使用者。
- 目前有許多歐盟國家運用合格電子簽章正進行建立國家級 PKI 系統的許多活動，而其中的建立程序有些差異。
- 多數先進國家具備強固的以國家 Root CA 爲基礎的 PKI 模式，它在該國扮演著大眾信賴機構，負責簽發合格憑證給各 CA(自

我授權)，而各 CA 再根據歐盟電子簽章條例及其他國內法規簽發合格憑證給使用者。

- 由於單一的國家級 Root CA，這個模式提供所有國內合格憑證擁有者間真正的互通性。
- 使用合格電子簽章的主要好處可近來逐漸形成的電子化政府、電子商務、電子化企業系統。

國家 PKI 機構

- 歐盟各國在採用了根據歐盟條例及其他法案所制訂的電子簽章法及相關規定之後，有必要建立一個專責的國家級機構負責監督(甚至指派)能簽發合格憑證的 CAs，也才能提供符合歐盟條例有關於電子簽章部分的必要法律基礎架構。
- 此國家級機構要在五個方面來制訂規範：
- 在國家級機構中建立 Root CA，
- 定義檢驗憑證機構(CAs)的權責主管機關。
- 定義能簽發合格憑證之 CAs 的條件。
- 定義安全簽章簽發設備(SSCDs)規格評量的權責主管機關。
- 定義安全簽章簽發設備(SSCDs)的條件。

國家級的認證機關

電子化政府的服務

- 採用 2001 年 3 月歐洲協會所羅列的 20 項(12 項人民和 8 項公司的)基本公眾電子化服務。
- 對每一項服務都有註記複雜度階段及可達到複雜度階段。
- 階段 1 – 資訊：有關大眾服務的線上資訊。
- 階段 2 – 互動：表單下載。
- 階段 3 – 雙向互動：包含認證的表單處理。
- 階段 4 – 交易：全程處理、決策及交付(付費)。

公民的電子化政府服務

公民的電子化政府 12 項服務如下：

1. 所得稅申報
2. 勞工就業服務
3. 社會安全
4. 個人文件資料
5. 汽車註冊登記
6. 建立網路簽入管制應用
7. 報案

8. 公立圖書館
9. 申請及派送證明書(出生、結婚)
10. 高等教育登記
11. 搬遷通報(更改地址)
12. 健康相關服務(如約時間至醫院看病)

企業的電子化政府服務

企業的 8 項電子化政府服務如下：

1. 員工的社會捐助
2. 公司稅：申報、通知
3. 加值稅：申報、通知
4. 新公司的註冊
5. 資料呈送統計機關
6. 關稅申報
7. 環境相關許可證
8. 大眾採購

M-政府

- 使用行動電話的民眾比使用電腦的民眾多。

- 在西 Balkan 半島國家這種關係更爲明顯。
- 發展適合行動電話應用的電子化服務。

M-政府 – 開放問題

- 行動螢幕的效能
- 可用的軟體工具及館藏
- 傳遞路徑的效能
- 安全性

PKI 應用

- 和許多在塞爾維亞的商業銀行一樣，Banca Intesa ad Beograd 這家銀行有對法人提供自己設計以 PKI 智慧卡及數位憑證爲基礎的電子化服務。
- 公司可使用這些銀行電子卡透過網路銀行的入口網站的安全交易系統進行付款。
- 此外，公司亦可離線準備交易資料，使用特別的離線軟體及銀行電子卡簽章及加密，之後再上傳至銀行端的網路服務。
- Banca Intesa ad Beograd 也針對個人提供安全家用銀行系統，以取代之前外包的 PKI 系統將憑證和非對稱式私密金鑰儲存於迷

你 CD 的做法。

- 當時在銀行有開戶的個人可藉由此 CD 在網路銀行的入口網站進行加密及簽章安全交易。
- 現在則使用更安全的 Maestro 智慧卡進行數位簽章及認證的付款系統。
- Maestro 卡上的 PKI 應用是啓用三組 2048 位元的 RSA 金鑰對。
- 此意味著這銀行卡還能用來做更多的 PKI 應用。
- Banca Intesa ad Beograd 也自行設計供銀行內部使用的智慧卡系統。
- 這些憑證和 Window 動態目錄整合起來，員工可使用智慧卡登入 Windows 後即可簽入銀行內部網路並使用安全電子郵件服務。

結語

- 本指引分析了現代電腦安全領域中的資料保護技術、加密協定和 PKI 系統。
- 結論是僅有多層次的安全架構能因應來自內部或外部的現代網路攻擊。
- 本文討論了最常用在應用層、傳輸層及網路層的安全機制。
- 結果告訴我們，合宜的安全機制能顧及系統全面的加密保護

至少要涵蓋超過一個層面。

■ 本文分析了有關安全的問題及對潛在弱點的對應之道。

■ 本文也作成了結論，在許多特定條件下的一個電子化企業個案，安全機制應該分布於客戶端、通訊面及中央資料庫端，在每一個環都應有合宜的安全措施。

■ 安全電子化企業的中心思想就是使用者的智慧卡，其使用數位簽章、數位信封及中央 PKI 系統。

全文完