IC卡晶片作業系統實作--從符記保護剖繪談起

楊中皇
國立高雄師範大學 資訊教育研究所
高雄市苓雅區和平一路116號
http://crypto.nknu.edu.tw/

摘要

我國使用IC卡已有十多年的歷史，隨著電話IC卡、金融IC卡、大哥大IC卡、健保IC卡等的使用，可見IC卡與我們日常生活逐漸息息相關。IC卡與目前常用的磁條卡比較起來具有難以偽造與記憶體容量較高的優點，然而IC卡的晶片猶如電腦，外觀可能相似但實際上有多種差異性極大的規格。IC卡系統設計不善或管理不良時，依舊可能產生弊端。本文以美國國防部公佈的符記保護剖繪為藍圖 ，討論IC卡內部晶片作業系統的實作，並探討IC卡的安全管理。
關鍵字： 保護剖繪， 符記，IC卡，智慧卡，安全管理

一、前言

美國國防部於2002年三月公佈第三版的公開金鑰基礎建設(Public Key Infrastructure，以下簡稱PKI)與金鑰管理基礎建設(Key Management Infrastructure, KMI)符記(Token)保護剖繪(Protection Profile) [1]。此保護剖繪是以ISO 15408 [2] 標準之資訊技術安全評估共通準則(Common Criteria for Information Technology Security Evaluation，簡稱CC)為基礎，提出一套詳盡的規範來確認美國國防部推動公開金鑰基礎建設與金鑰管理機建設兩者所使用的符記硬體裝置的安全需求。PKI/KMI符記是一個硬體裝置用來儲存密碼學金鑰與公開金鑰憑證，且用來提供使用者身份認證(user identity authentication)的功能。依據美國國防部該保護剖繪的定義，此符記可達到CC安全等級的EAL第四級要求，而且此符記的安全功能可涵蓋美國國防部所有人員與供應商的金融(電子商務及付款)、安全電子訊息、身分識別、安全資訊儲存、存取控制等多種應用。

使用者身份認證是資訊或網路應用最基本的安全需求。近年來國內屢次發生的信用卡或銀行提款卡被盜用案件，明顯暴露出磁條卡儲存的資料無法被有效地保護，而磁條卡與個人識別碼(PIN)的結合僅能提供薄弱的單向使用者身份認證功能。PKI/KMI符記內建數位簽章、對稱式與非對稱式加解密、等多種安全機制，不僅可直接用來支援高安全性的互動式使用者身份認證，且可用於電子公文、電子商務等應用。國人有能力自製符合此規範的此PKI/KMI符記，若國內相關單位在擬定IC卡規格時能有效地引導廠商提供適合國人長期使用之IC卡。

符合PKI/KMI符記的裝置目前已有四種外觀不同的種類，如表一所示。表一所列的PKI/KMI符記硬體裝置涵蓋硬體及內部相關作業系統及應用程式。接觸式IC卡[4-5]讀卡機的介面目前有USB、RS-232、PCMCIA、3.5吋磁片等，隨著Windows2000/XP的內建PC/SC讀卡機驅動程式庫，同時IC卡讀卡機(內政部自然人憑證IC卡[6]適用的USB介面IC卡讀卡機一台僅須NT$350)的價格也日益便宜，這使得IC卡越來越適合網路安全應用。IC卡除了資料傳輸速度較慢外，方便性與內部功能都能符合PKI/KMI符記的要求，且接觸式IC卡與讀卡機價格低廉，所以目前接觸式IC卡可說是PKI/KMI符記的最合適裝置。以下我們對符記保護剖繪的討論也將限於接觸式IC卡。

表一、美國國防部PKI/KMI符記的硬體裝置種類

符記外觀	說明
1. IC卡	大小如信用卡的接觸式或非接觸式智慧卡
2. USB碟	外觀如USB隨身碟，但內含智慧卡晶片
3. PCMCIA卡	大小如筆記型電腦PCMCIA介面卡，但內含安全晶片，資料傳輸速度高
4. iButton鈕扣	達拉斯半導體公司[3]的非接觸式硬體裝置, 通常外觀如同鈕扣或戒指

二、IC卡及晶片作業系統

我國政府積極推行IC卡已有十多年的歷史，IC卡在國內各界的應用也日趨廣泛。IC卡與目前常用的磁條提款卡與信用卡比較起來具有難以偽造與記憶體容量較高的優點。然而如果我們檢視金融IC卡(十多年前的第一代與目前的第二代)、電子公文IC卡、自然人憑證IC卡、以及健保IC卡等的規格，可知IC卡外觀相似但實際上有多種差異性極大的規格，不僅在通信協定與內部密碼學演算法的功能有差異，而且在安全管理等級也有極大的差異。

符合PKI/KMI符記的IC卡必須為具備執行程式的微處理機及其內部的晶片作業系統等。IC卡晶片內部至少有個八(或十六或三十二)位元中央處理器(CPU)，唯讀記憶體(ROM)、電流可消除可程式唯讀記憶體(EEPROM)、及隨機存取記憶體(RAM)等。晶片的ROM記憶體區域是用來儲存作業系統程式和儲存密碼運算法程式或其他固定的應用程式；EEPROM記憶體區域是用來儲存個人化的資料(如私密金鑰、公開金鑰憑證)或其他易更動的應用程式；RAM則是供暫時性運算變數資料儲存用。IC卡晶片作業系統(chip operating system)的功能包括提供外界通信協定(T=0, T=1等)，儲存密碼學金鑰於晶片內部EEPROM記憶區域，接受晶片外部呼叫資料加解密及數位簽章等演算法的命令，監控命令的執行過程，及命令錯誤特殊狀況的處理等。

IC卡有它的生命週期(life cycle)，包括使用者需求、設計、製造、發行、使用、結束等六個階段。每個階段都有安全管理上的需求[7]，且每個階段的活動與IC卡的種類有關。能執行程式的IC卡(有時稱之為智慧卡)可分為表二所示的四種[7]，每種IC卡有自己的生命週期階段活動也有可能受到攻擊的弱點與安全管理需求。

表二、IC卡的種類

IC卡種類	說明
1. 軟罩(Soft Mask) IC卡	應用程式放在EEPROM區域執行
2. 硬罩(Hard Mask) IC卡	應用程式放在ROM區域執行
3. 特定(Proprietary) IC卡	針對某一特定系統設計的IC卡
4. 可重組(Reconfigurable) IC卡	允許高階語言的應用程式於IC卡發行後透過卡片內的虛擬機器(virtual machine)執行。例如：MultOS卡、Java卡、Smart Card for Windows

三、IC卡內部的密碼學演算法與密碼模組

密碼學[8]技術是目前所知唯一能有效地在不安全的網路上安全傳遞訊息的成熟技術。IC卡內的晶片猶如一部具有運算能力的電腦，可以透過密碼學演算法保護儲存的內部資料，同時能提供數位簽章等的資訊安全功能。PKI/KMI符記要求具備表三所列的密碼學演算法功能。亦即在IC卡內部必須透過軟硬體具體實現RSA [9]、DSA [10]、ECDSA

[10]、Diffie-Hellman [11]、KEA [12]、ECKEA [12]、AES [13]、DES [14]、Triple DES [14]、Skipjack [12]、SHA-1 [15]、MD5 [16]、SHA 256 [15]、SHA 384 [15]、SHA 512 [15]等15種演算法。

表三、PKI/KMI符記內部必須具有的密碼學演算法

演算法種類	說明
1. 數位簽章演算法	包括1024/2048位元RSA、 1024位元DSA、384位元ECDSA
2. 金鑰交換演算法	包括1024/2048位元RSA、1024位元Diffie - Hellman、1024位元KEA、以及384位元ECKEA橢圓曲線金鑰交換演算法
3. 對稱式演算法	包括128/192/256位元AES、DES、Triple DES、Skipjack
4. 雜湊演算法	包括SHA-1、MD-5、SHA 256、SHA 384、SHA 512

由於PKI/KMI符記要求能實現RSA、ECDSA等公開金鑰密碼學演算法，這意味著IC卡內部必須有特殊的輔助處理器(coprocessor)，提供快速的數論相關基礎運算。三種數位簽章演算法中RSA公開金鑰密碼系統可用數位簽章或金鑰交換，但RSA用於數位簽章時速度慢，而美國國家技術標準局(NIST)於1991年公佈數位簽章專用的DSA（Digital Signature Algorithm，DSA）演算法用於數位簽章時速度較快。橢圓曲線密碼系統（elliptic curve cryptosystem，ECC）[16-17]則是近年開始被採用的密碼學演算法技術，且近年來已被廣泛地制訂於國際標準如ISO 11770-3、ANSI X 9.62、IEEE P1363等。在相同的安全強度下，ECC的密碼學參數可遠較諸如RSA的其他公開金鑰密碼系統為小，這代表IC卡儲存ECC演算法的金鑰或公開金鑰憑證時能節省EEPROM的空間。ECDSA是將DSA內部的數學運算改用橢圓曲線的一種數位簽章標準。

在金鑰交換演算法方面，PKI/KMI符記要求具備傳統常用的RSA及Diffie/Hellman演算法，但也包括美國軍方慣用的KEA與橢圓曲線ECKEA。對稱式加解密演算法則有傳統的DES及Triple DES演算法、軟體速度較快亦較安全的AES、及美國軍方慣用的Skipjack演算法。

NIST於1995年修訂公佈SHA-1的雜湊演算法可以計算產生160位元的訊息摘要(或訊息指紋)。此演算法常用於數位簽章或訊息認證碼。由於雜湊函數的安全度取決於訊摘要的長度，160位元的SHA-1安全度約為2^{80}。2002年公佈的FIPS 180-2提出SHA 256、SHA 384、SHA 512三個訊息摘要長度各為256位元、384位元、512位元的雜湊函數演算法，它們的安全性各約為2^{128}、2^{192}、2^{256}，訊息摘要長度較大時，雖較安全但執行速度會較慢。

為了要確保演算法的具體實現無誤，便有賴於密碼模組的檢驗。依據NIST的定義密碼模組可以是硬體元件或模組、軟體韌體程式或模組、或它們的組合。美國於於2001年修正通過FIPS 140-2規範[18]，並為目前國際上業界公認的密碼模組標準。FIPS 140-2 標準訂定密碼模組的四種安全等級，從最低要求的第一級到最高階的第四級，每個安全等級各須滿足11個安全要件。每個安全等級的共同基本需求包括模組輸出入及控制與狀態介面的描述、至少須實現一個核定的密碼學演算法、模組啟動時自我測試密碼學演算法、模組安全政策的定義、授權角色與安全服務的說明、驗證機制的選擇、以及模組須以有限狀態機器描述等。PKI/KMI 符記要求密碼模組必須通過FIPS 140-2第二級的檢測。

四、IC卡安全管理需求

成熟的密碼學技術須輔以合適的安全管理規範與合適的說明文件，否則就算要求廠商提供(數以千計的)原始程式碼，我們又能如何研讀？雖然資訊技術安全評估共通準則[2]安全等級的高低無法用來代表產品的絕對安全性，然而安全等級至少代表產品從設計到製造到安全評估的嚴謹程度。

PKI/KMI符記的CC安全等級達到EAL 4。從符記(IC卡)的軟硬體描述開始，表四簡單說明符記安全管理的步驟。由於符記與IC卡保護剖繪[1,7]文件甚為冗長，限於篇幅，我們在這裡僅擇要描述。

表四、PKI/KMI符記安全管理

步驟	說明
1. IC卡描述	● 微處理器硬體規格 ● 記憶體種類(ROM、EEPROM、RAM等)、大小與位址配置 ● 實體IC積體電路佈局圖 ● 所有啟動與未啟動的硬體安全功能 ● 所有啟動的硬體安全功能 ● 軟體規格 ● 所有啟動與未啟動的軟體體安全功能 ● 所有啟動的軟體體安全功能 ● 狀態圖
2. 安全環境	● 操作時的環境假設 ● 可能受到的威脅 ● 安全政策
3. 安全目的	● 保護資料避免被揭露或竄改 ● 使用者與系統管理者身分認證 ● 應用程式的控制管理 ● ... ...
4. 安全需求	● 功能需求 ● 安全確保需求

IC卡描述裡的狀態圖包括“電源加入狀態”、“未初始化狀態”、“未定義狀態”、“未認證狀態”、“認證狀態”、“封鎖狀態”等IC卡在與外界聯繫時自我偵測到的狀態。IC卡的某些高安全性功能必須在合適的認證狀態才可被執行。

IC卡安全環境包括對操作環境的假設，例如IC卡的發展工具與生產製造過程可能假設是受到保護不被未授權使用或偷竊，IC卡與外界通信用的交換金鑰的產生也可能假設是安全的，外界傳送到IC卡的資料與程式碼亦可能假設是安全的。IC卡安全環境可能受到的威脅包括實體攻擊(例如利用電子探測棒去更改資料或是操控IC卡輸入的電壓與時鐘脈波)、邏輯攻擊(例如對IC卡輸入不正常的資料)、存取控制(例如試圖使用未經開卡的IC卡)、密碼學功能攻擊(例如以暴力攻擊法或分析加密過的資料)等。IC卡安全環境的安全政策指的是密碼學演算法的金鑰長度(例如ECDSA所用的質數域至少要384位元)、應用程式控制(例如ECDSA所用的質數域至少要384位元)等。

PKI/KMI符記(IC卡)想要達到的安全目的如圖一所示，安全需求的安全功能需求(functional requirements)與安全確保需求(assurance requirements)是取自ISO 15408文件第二部分與第三部分。安全功能需求分為七類；密碼學支援(Cryptographic support，FCS)、使用者資料保護(User data protection，FDP)、身分證明與確認(Identification and authentication，

FIA)、安全管理(Security management，FMT)、安全功能的保護(Protection of the security functions，FPT)、資源利用(Resource utilization，FRU)、可信賴的通道(Trusted path/channels，FTP)等。

圖二為PKI/KMI符記的安全功能需求，圖三為安全確保需求，圖二與圖三用到很多ISO 15408裡的專用術語與記號。

1. Protection of Authentication Data	**15. Logical Protection**
2. Authentication of Users and SSOs	**16. Multiple Applications**
3. Control of Applications	**17. Physical Protection**
4. Cryptography	**18. Resource Access**
5. Data Access Control	**19. Role Management**
6. Data Read Format	**20. User Data Control**
7. Enforce data exchange confidentiality	**21. Secure Host Communications**
8. Environmental Stress	**22. Self-Test**
9. Preservation of secure state for failures in critical components	**23. Set up Sequence**
10. Information Leak	**24. Respond to Tamper**
11. Initialization	**25. Trial-and-Error Resistance**
12. Probing by Selected Inputs	**26. Linkage**
13. Encryption of Stored Keys	**27. Destruction of Volatile Memory**
14. Life-Cycle Functions	

圖一、PKI/KMI符記的安全目的

1.	Cryptographic key generation	FCS	23.	Management of security functions behavior	FMT
2.	Cryptographic key distribution		24.	Management of security attributes	
3.	Cryptographic key access		25.	Secure security attributes	
4.	Cryptographic key destruction		26.	Static attribute initialization	
5.	Cryptographic operation		27.	Management of TSF data	
6.	Subset access control	FDP	28.	Management of limits of TSF data	
7.	Security attribute based access control		29.	Secure TSF data	
8.	Basic data authentication		30.	Revocation	
9.	Export of user data without security attributes		31.	Security roles	
10.	Subset information flow control		32.	Assuming roles	
11.	Simple security attributes		33.	Abstract machine testing	FPT
12.	Limited illicit information flows		34.	Failure with preservation of secure state	
13.	Import of user data without security attributes		35.	Inter-TSF detection of modification	
14.	Basic internal transfer protection		36.	Basic internal TSF data transfer protection	
15.	Subset residual information protection		37.	Passive detection of physical attack	
16.	Authentication failure handling	FIA	38.	Resistance to physical attack	
17.	User attribute definition		39.	Function recovery	
18.	Verification of secrets		40.	Non-bypassability of the TSP	
19.	Timing of authentication		41.	TSF domain separation	
20.	Re-authenticating		42.	TSF testing	
21.	Protected authentication feedback		43.	Maximum quotas	FRU
22.	User identification before any action		44.	Inter-TSF trusted channel	FTP

圖二、PKI/KMI符記的安全功能需求

安全確保等級	確保元件
ACM (Configuration Management)	ACM_AUT.1, ACM_CAP.4, ACM_SCP.2
ADO (Delivery and operation)	ADO_DEL.2, ADO_IGS.1
ADV (development)	ADV_FSP.2, ADV_HLD.2, ADV_IMP.1, ADV_LLD.1, ADV_RCR.1, ADV_SPM.1
AGD (Guidance documents)	AGD_ADM.1, AGD_USR.1
ALC (life cycle support)	ALC_DVS.1, ALC_LCD.1, ALC_TAT.3
ATE (test)	ATE_COV.2, ATE_DPT.1, ATE_FUN.1, ATE_IND.2
AVA (vulnerability assessment)	AVA_MSU.2, AVA_SOF.1, AVA_VLA.3

圖三、PKI/KMI符記的安全確保需求

PKI/KMI符記可支援多種應用，所以符記不僅儲存的是一個金鑰(對)而已，不同用途的金鑰與公開金鑰憑證也可事先規劃好空間，放在同一張IC卡內，達到一卡多功能的應用。表五為符記保護剖繪裡的一個範例，從這範例可針對使用用途大致瞭解需要使用多大EEPROM空間的IC卡。

表五、PKI/KMI符記內金鑰與憑證佔用空間估計表(假設使用2048位元RSA)

金鑰或憑證資料	EEPROM 佔用空間(位元組)
目前的根憑證中心（root CA）憑證	1,500
下次的根憑證中心憑證	1,500
簽章用金鑰對	768
建立共通金鑰用金鑰對	768
對稱式金鑰	32
符記儲存用金鑰	32
一般身分用金鑰與憑證	2,000
電子郵件加密用金鑰與憑證	2,000
網路登錄（log-on）用金鑰與憑證	2,000
KMI 管理員用金鑰與憑證	2,000
群體或組織用金鑰與憑證	2,000

五、結論

一卡多功能的IC卡具有成本低廉、攜帶方便以及安全性高的特性，目前可說是認證使用者身分的最合適裝置。美國國防部的PKI/KMI符記保護剖繪提出一套周密與嚴謹的安全管理需求規範，值得我們在擬定IC卡規格與使用IC卡時作為參考。

致謝

作者感謝中華資訊安全管理協會的邀請，參與該會所主辦的「堅實我國資訊安全

管理系統稽核作業相關標準討論會」，使作者有機會接觸此保護剖繪議題，特此致謝。

參考文獻

1. Department of Defense, *Public Key Infrastructure and Key Management Infrastructure Token Protection Profile V3.0*, http://www.niap.nist.gov/cc-scheme/PP_PKIKMITKNPP-MR_V3.0.pdf, March 2002.
2. ISO/IEC 15408 — *Information technology — Security techniques — Evaluation criteria for IT security (Common Criteria, CC, Version 2.1)* — Part 1: Introduction and general model, Part 2: Security functional requirements, Part 3: Security assurance requirements, 1999.
3. Dallas Semiconductor Corp., *iButton*, http://www.ibutton.com/
4. Wolfgang Rankl and Wolfgang Effing, *Smart Card Handbook*, 2nd edition, John Wiley & Sons,2000.
5. ISO/IEC 7816 Part 1 to 15, *Identification Cards – Integrated Circuit(s) Cards with Contact*,1987 to 2004.
6. 內政部憑證管理中心，http://moica.nat.gov.tw/
7. Smart Card Security User Group, *Smart Card Protection Profile* V3.0, http://niap.nist.gov/cc-scheme/PP_SCSUGSMPP_V3.0.pdf, September 2001.
8. A.J. Menezes, P.C. van Oorschot and S.A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996. http://www.cacr.math.uwaterloo.ca/hac/
9. R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", *Communications of the ACM*, Feb. 1978, Vol. 21, No. 2, pp. 120-126.
10. NIST, *Digital Signature Standard (DSS)*, FIPS 186-2, January 2000,http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf
11. W. Diffie and M.E. Hellman, "New directions in cryptography," *IEEE Trans. Information Theory*, Nov. 1976, pp. 644 – 654.
12. NIST, *SKIPJACK and KEA Algorithm Specifications*, May 1998, http://csrc.nist.gov/CryptoToolkit/skipjack/skipjack.pdf
13. NIST, *Advanced Encryption Standard (AES)*, FIPS 197, November 2001. http://csrc.nist.gov/publications/fips/fips197/ fips-197.pdf
14. NIST, *Data Encryption Standard (DES)*, FIPS 46-3, Data Encryption Standard, October 1999, http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf
15. NIST, *Secure Hash Standard (SHS)*, FIPS 180-2, August 2002, http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf
16. A. Menezes, *Elliptic curve public key cryptosystems*, Kluwer, 1993.
17. I. F. Blake, G. Seroussi and N. P. Smart, *Elliptic Curves in Cryptography*, London Mathematical Society Lecture Note Series, Vol. 265, Cambridge University Press, 1999.
18. NIST, FIPS 140-2, *Security Requirements for Cryptographic Modules*, June 2001. http://csrc.nist.gov/publications/ fips/fips140-2/fips1402.pdf