國 立 交 通 大 學

管理學院（資訊管理學程）碩士班

碩　士　論　文

數位社會資訊安全密碼政策初探

Cryptography's Policy in Securing the Information Society

研 究 生：王美靜

指導教授：陳安斌　博士

樊國楨　博士

中　華　民　國　九　十　五　年　七　月

數位社會資訊安全密碼政策初探

Cryptography's Policy in Securing the Information Society

研 究 生：王美靜　　Student：Mei-Jing Wang

指導教授：陳安斌博士　　Advisor：Dr. An-Pin Chen

樊國楨博士　　Dr. Kwo-Jean Farn

國 立 交 通 大 學

管理學院（資訊管理學程）碩士班

碩 士 論 文

A Thesis

Submitted to Institute of Information Management

College of Management

National Chiao Tung University

In Partial Fulfillment of the Requirements

For the Degree of

Master of Science

in

Information Management

July 2006

Hsinchu, Taiwan, the Republic of China

中　華　民　國　九　十　五　年　七　月

數位社會資訊安全密碼政策初探

研究生：王美靜　　指 導 教 授：陳安斌 博士

共同指導教授：樊國楨　博士

國立交通大學資訊管理研究所

摘要

政府對於人民的秘密應該知道多少？這是一個古今中外永無定論的大問題。然而，在今日資訊化的時代，這個問題將對未來的個人隱私與群體安全，產生根本及深遠的影響。在數位社會中，日常生活各個層面的活動均迅速透明化與數位化，無論從個人隱私、群體安全、身分鑑別、交易安全、授權驗證等，密碼裝置都是最基本的組件之一。

隨著密碼技術應用的日益普及，密碼裝置已逐漸成為消費商品，如何確保其安全之品質已成為國際間共同解決的議題，工業界已共同制定內嵌於主機板中之「密碼模組及其應用」的可信賴平台模組（Trusted Platform Module，簡稱 TPM），做為對抗惡意軟體（Malware）攻擊之個人電腦、個人數位助理、行動通訊裝置等的可信賴計算平台（Trusted Computing Platform，簡稱 TCP）之核心組件。國際標準組織自 1998 年 6 月 15 日起，除公布密碼裝置鑑測相關系列標準中，並逐步建立密碼技術及其應用「使用便捷，遺失不懼」的機制。

根基於此，遵循國際發展趨勢，審慎衡量我國實際現況，在可操作的面向，為數位社會奠定密碼技術及其應用之可信賴的使用環境，提出：

1. 遵循 ISO 公布之標準，制定我國密碼技術及其應用宜遵循之規範。
2. 建立能對抗海峽對岸網軍威脅之我國密碼技術及其應用的研發能量。

二項政策與下列 5 項行動方案：

1. 「密碼技術及其應用」之「認知、訓練與教育」的課程規劃及實作。
2. 「公開金鑰基礎建設（Public Key Infrastructure，簡稱 PKI）」之安全評鑑、檢討與改進。
3. 我國金鑰管理基礎建設（Key Management Infrastructure，簡稱 KMI）之建置。
4. 建立我國密碼技術及其應用之資訊安全保證的鑑測機制。
5. 研發能對抗海峽對岸網軍攻擊之 TPM。

期能奠定我國密碼技術及其應用之「堅若磐石，使用便捷；依法取用，遺失不懼。」的基礎。

關鍵詞：密碼裝置/模組(Cryptographic Device/Module)，數位社會(Cyberspace)，深度防禦(Defense in Depth)，資訊保證(Information Assurance)，政策(Policy)，可信賴平台模組(Trusted Platform Module)

Cryptography's Policy in Securing the Information Society

Student：Mei-Jing Wang　　Advisor：Dr. An-Pin Chen
Dr. Kwo-Jean Farn

Institue of Information Management
National Chiao Tung University
Hsinchu, Taiwan, Republic of China

Abstract

How much can and should the government look into someone's personal life? This has been a highly debatable topic for a long time. In this Information Age, the outcome of this issue will influence people's individual privacy and group safety deep and far in the future. Activities of each aspect of daily life have become transparent on the internet. Cryptographic Devices/Modules are one of the most basic and necessary tool to provide individual privacy, group safety, authentication, trade safety, and authorization, etc.

With the advances in the cryptographic technology, applications that utilize this technology have gain popularity and widely adapted. However, the question is how to maintain security standard on these cryptographic devices has developed into an international discussion topic. The industry created the Trusted Platform Module (TPM), which combines cryptographic module and application into one and embedded on the motherboard of computer. TPM would be the core component of Trusted Computing Platform's (TCP) to prevent malware attack on personal computers, personal digital assistant, mobile telecommunication device, and any other digital devices may contain personal information. Since June 15, 1998, International Standards Organization (ISO) not only announced related standards of "Cryptographic Technology and Application", but also established a mechanism which is *convenient of using, no fear of losing* progressively.

Observing the international trend, and information security needs of our country, we propose the following policies and procedures to create the foundation for a trusted computing environment using "Cryptographic Technology and Application".

Two policies:

1. Follow ISO standards, and make the norms that our country's Cryptographic Technology and Application should be followed.
2. Increase our country's researching and developing capability on Cryptographic Technology and Application to guard against threats and attack.

The five action schemes:

1. Planning and practicing the "cognition, training and education" courses of "Cryptographic Technology and Application".
2. Security evaluation, review and improvement of Public Key Infrastructure (PKI).
3. Setup our country's Key Management Infrastructure (KMI).
4. Setup the authentication and test mechanism for "Cryptographic Technology and Application".
5. Researching and developing the TPM which can against the China Network Army' attack.

We need follow these steps to establish the foundation of our country's "Cryptographic Technology and Application" and a *convenient of using, no fear of losing* environment.

誌　謝

感謝樊國楨老師的耐心與悉心指導，使我在資訊安全領域的知識成長許多；感謝林樹國學長、徐正民同學的幫助及鼓勵，和陳安斌所長、彭仁岡處長、黃仁俊老師三位口試委員對論文的建議和指教，使我能順利完成論文。

感謝家人們的支持、體諒與關心，同學及好友們的扶持，不論在學業上、精神上及生活上。

感謝我生命中的貴人，尤其在這人生階段中，伴隨、支持我成長的每一位，你們無限的關愛及付出是我所負荷的溫柔壓力與動力。

感謝每一位使我生命更完整、更充滿豐富、美麗回憶的你們。

目錄

表目錄

圖目錄

一、前言：

資訊化的浪潮席捲全球，一種全新先進技術之出現，把人類的生活帶引至知識經濟之數位社會。資訊技術的應用，催化人們工作方式、生活環境與思維觀念之巨大變化，大步地推動著人類社會的發展及世界文明的進步，把人類帶入新時代。然而，人們在享受數位社會帶來之巨大利益的同時，也面臨著資訊安全問題之嚴峻考驗。

數位社會中的資訊系統是頗具誘惑力之攻擊標的，宜具備防護駭客團體、組織犯罪等全方位威脅個體攻擊的能量。應健全侷限遭如表 1.1 中各類攻擊損害之能力與在攻擊後快速回復的反應處理機制。

表 1.1：惡意軟體(Malware)層次簡述

類型	入侵層次	功能描述	舉例說明—以亞瑟王之城堡為例	現況
後門	應用層	繞過常規之安全防護，為攻擊者提供隱密取存通道。	入侵者在城堡外之村莊的圍牆打開缺口，攻城掠地。	已是事實
木馬	應用層	看起來是一個正常之程序，實際上是惡意的程式。	入侵者進入城堡外之村莊，偽裝成良民俟機犯案。	已是事實
使用者模組之根盒(Root Kit)	作業系統之執行層	替換或修改作業系統關聯之程序與指令，提供後門通道並隱藏攻擊者。	入侵者攻佔了城堡外之護城河，使自己可以進出城堡外的村莊並隱藏行蹤。	已是事實
核心模組之根盒	作業系統之核心層	控制作業系統之核心模組，提供後門通道並隱藏攻擊者。	入侵者攻陷了城堡，隨時可以改變亞瑟王對村民的所有命令。	已是事實
BIOS 級惡意軟體	BIOS	從 BIOS 起動系統時，加載惡意軟體之核心模組以控制作業系統。	入侵者選出亞瑟王之圓桌武士，經由這些武士控制亞瑟王的城堡。	攻防實作階段
CPU 級惡意軟體	BIOS 與 CPU	改變 BIOS 與 CPU 之程式碼，為攻擊者提供完全的秘密行動及控制作業系統。	入侵者俘虜並控制了亞瑟王，城堡已實質易幟。	攻防研究階段

備考：
1、BIOS：基本輸入/輸出系統(Basic Input/Output System)。
2、資料來源：Skoudis, E. and L. Zelter (2004) Malware: Fighting Malicious Code, Prentice-Hall 與本研究。

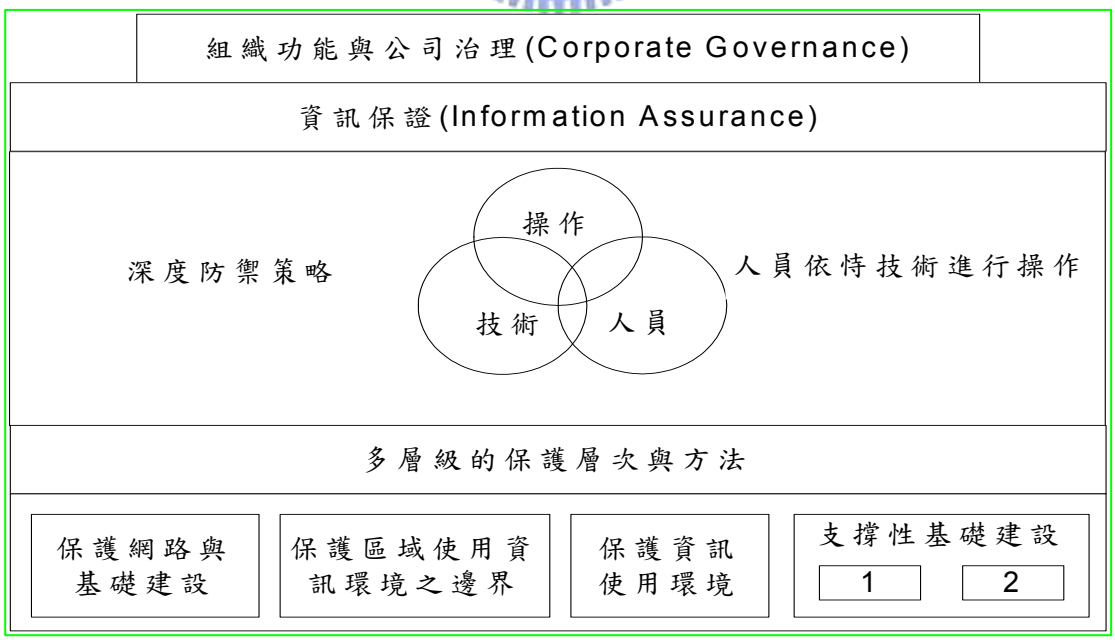
作業系統是一個資訊系統之基石，根據安全事故資料的分析，大約 50%之資訊安全問題的源池是作業系統之脆弱性。因此，作業系統的安全是資訊系統安全之必要條件。隨著電子科技之一日千里，如表 1.1 所示的資訊世界惡意程式碼日益猖獗，資訊安全專家根基於密碼模組、安全作業系統等技術冀期發現更有效之方法來面對駭客入侵等資訊安全問題；密碼技術已成為歷經資料保密－資訊安全的階段性任務後之 21 世紀資訊保證(Information Assurance)與深度防禦(Defense in Depth)的礎石。「他山之石，可以攻錯」，根基於此，本文分別在第 2 節、第 3 節、第 4 節與第 5 節簡介先進國家數位社會安全之密碼政策及其相關研發工作【5, 7, 12, 28, 52, 54, 76, 85~86】；在第 6 節，探討我國密碼政策擬案，並代為本文結論。

二、美國資訊保證框架與可信賴平台模組簡介：

自 1985 年美國正式公布可信賴電腦系統安全評估準則(以下簡稱橘皮書)後，由於其僅考慮傳統之單一電腦獨立於階層分明的作業環境，隨著資訊科技的日新月異，於其實作時均已改弦更張，使用安全機制強度(Strength Mechanism Level，簡稱 SML)與評估保證等級(Evaluation Assurance Level，簡稱 EAL)等整合之資訊保證(Information Assurance，簡稱 IA)強健性程度(Degree of Robustness)的方案【29】，已成為國家資通安全會報自 2006 年 1 月正式實施之「政府機關(構)資訊安全責任等級分級作業」的參考標的。美國已進行建置之資訊保證技術框架(Information Assurance Technical Framework，簡稱 IATF)立基於如表 2.1 與圖 2.1 所示深度防禦實作原則，2005 年 6 月，行政院國家資通安全會報參照 IATF 之 SML，頒布政府機關(構)資訊安全責任等級分級作業施行計畫【72】中「防禦機制強度」的要求，於 IATF 中 SML 之存取控制、可歸責性、可用性、機密性、識別與鑑別、完整性與不可否認性 7 項分類要求，密碼技術已成為圖 2.1 中多層級的保護層次與方法之基石。可信賴平台模組已溶入作業系統中，提供作業系統安全功能計算的核心組件(Component)，成為數位社會資訊保證作業鏈條中，最重要之環節。

表 2.1：深度防禦定義【29】

這個安全的方法是為了建立適度安全的系統，藉由多層保護的方式來滿足安全形勢上的需要；這種策略的觀念係植基於攻擊必須要突破安置於整系統的多重保護措施才能得以成功。 The security approach whereby layers op protection and needed to establish and adequate security posture for a system; strategy is based on concept that attacks must penetrate multiple protections that have been placed throughout the system to be successful.



說明：1.公開金鑰基礎建設(Public Key Infrastructure，簡稱 PKI)／金鑰管理基礎建設(Key Management Infrastructure，簡稱 KMI)。
2.偵測與回應。

圖 2.1：深度防禦示意說明【11】

作業系統直接與電腦硬體交互工作，是電腦系統軟體之基石，欠缺作業系統的安全性，資訊系統之安全保證就不可能達到想定之標的。作業系統安全性的功能很多，僅從可信賴計算基底(Trusted Computing Base，簡稱 TCB)及可信賴計算路徑(Trusted Computing Path，簡稱 TCP)兩個構面，就足以看出其在資訊系統安全不可或缺之作用。

2.1、可信賴計算基底(Trusted Computing Base，簡稱 TCB)：

一般而言，TCB 宜具備：

(1). 確保作業系統中物件之身分、權限與工作室間的完整性、可靠性；

(2). 確保儲存、處理及傳輸資訊之機密性、完整性；

(3). 確保硬體組態、作業系統核心模組、服務與應用過程的完整性；

(4). 確保密碼金鑰儲存及作業之安全性；以及，

(5). 確保 TCB 能具備防止惡意程式碼與駭客的免疫能力。

等功能，提供作業系統安全之基礎。

2.2、可信賴計算路徑(Trusted Computing Path，簡稱 TCP)：

TCP 是實作使用者與可信賴軟體之間進行直接交互作用的機制，TCP 僅能由使用者或可信賴軟體起動，不能由其他軟體仿冒。TCP 之標的在於保證資訊系統關鍵功能不被假冒，是確保兩個實體(Entity)間之相互驗證通道的一種機制。

2003 年 4 月 8 日，70 個資訊技術(Information Technology，簡稱 IT)公司根基於：

(1)、使用增加之硬體組件，戲劇性的增進安全。

(2)、資料之最終防護僅由加密功能提供。

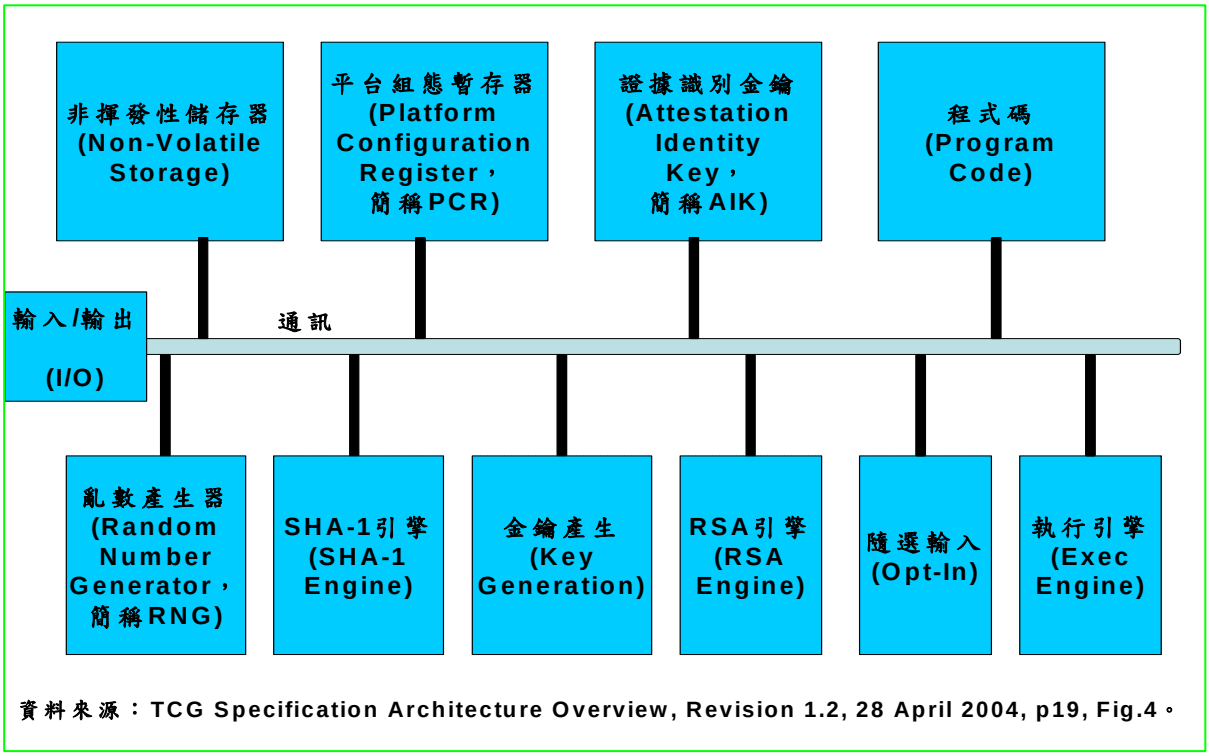
的假設，成立了可信賴計算集團(Trusted Computing Group，簡稱 TCG)。2003 年 5 月，TCG 公布其可信賴計算平台(Trusted Computing Platform，簡稱 TCP)的主要規範，如圖 2.2 與圖 2.3 所示之可信賴平台模組(Trusted Platform Module，簡稱 TPM)是其基石，圖 2.4 是 TCP 之框架示意。

2004 年 2 月，微軟(Microsoft)公司宣布其代號長角(Longhorn)之使用 TPM 的安全作業系統計畫，此安全作業系統組件名為下一代安全計算基底(Next Generation Secure Computing Base，簡稱 NGSCB)。

一般而言，TPM 是對抗表 1.1 所示惡意軟體層次中 BIOS 級與 CPU 級惡意軟體保證機制之礎石。

自 1999 年 10 月 TCG 之源池，AMD、HP、IBM、Intel、Microsoft、SONY 與 SUN 發起的可信計算平台聯盟(Trusted Computing Platform Alliance，簡稱 TCPA)嘗試廣泛使用基於 TPM 之 TCP 以提高數位社會整體的安全性起，以安全作業系統為核心，使用密碼技術實作，重視終端使用安全防護之可信賴計算技術，在 2005 年已勢不可當，即將進入普及階段，成為資訊保證方法實務的一個重要之里程碑。可信賴計算是否能治療資訊安全之沉疴，尚待驗證；惟 TCP 將可改善計算環境的安全問題，提供資訊社會更具信賴性之使用環境，已是資訊技術專家確認的事實【54】。

為保證 TCP 之安全，在 TCG 的規格書中無論是個人電腦、個人數位助理、行動通訊手機等之應用，均使用「參考平台」定義共同的系統架構，並使用共同準則(Common Criteria，簡稱 CC)與共同評估方法(Common Evaluation Methodology，簡稱 CEM)進行驗證【12, 28】，圖 2.5 是其架構示意；在第 5 節，我們將說明共同準則。



資料來源：TCG Specification Architecture Overview, Revision 1.2, 28 April 2004, p19, Fig.4。

說明：

1、輸入/輸出元件管理通訊匯流排中的資訊流動，負責外部與內部匯流排上的資訊編解碼，並將訊息傳送到其他適當的元件上。

2、非揮發性儲存器元件可用於儲存各種不同用途的金鑰、授權資訊與旗標等。

3、平台組態暫存器(PCR)元件為平台組態資訊的儲存位置，透過 PCR 所儲存的資料，管理人員可以瞭解哪些系統需要進行版本更新等作業。

4、AIK 中的資訊是必須持續存在的，TCG 的規格書中建議最好將 AIK 金鑰儲存在 TPM 以外的地方，等到執行時，才將 AIK 金鑰資訊載入 TPM 的揮發性記憶體中，以提升系統的執行速度。

5、程式碼元件中包含量測平台裝置的軟韌體。

6、TPM 的亂數產生器(RNG)元件主要是用於金鑰的產生、臨時亂數的建立等，以加強密碼系統的強度。

7、SHA-1 引擎元件可用於計算數位簽章值、建立金鑰資訊等。

8、RSA 金鑰產生器元件可用於建立數位簽章金鑰與儲存金鑰等。TPM 定義的 RSA 金鑰產生器可支援最高 2,048 位元的 RSA 金鑰。

9、RSA 引擎元件則負責利用簽章金鑰進行數位簽章、利用儲存金鑰進行加密/解密等。TPM 中的 RSA 引擎元件不受進出口管制的限制。

10、Opt-In 元件主要是負責制定 TCG 策略、TPM 模組狀態，以符合消費者的需求，例如，啟用或停用 TPM 模組中的其他元件等。

11、執行引擎元件的主要工作是負責執行程式碼，進行 TPM 初始化與量測作業。

圖 2.2：可信賴平台模組(Trusted Platform Module，簡稱 TPM)示意

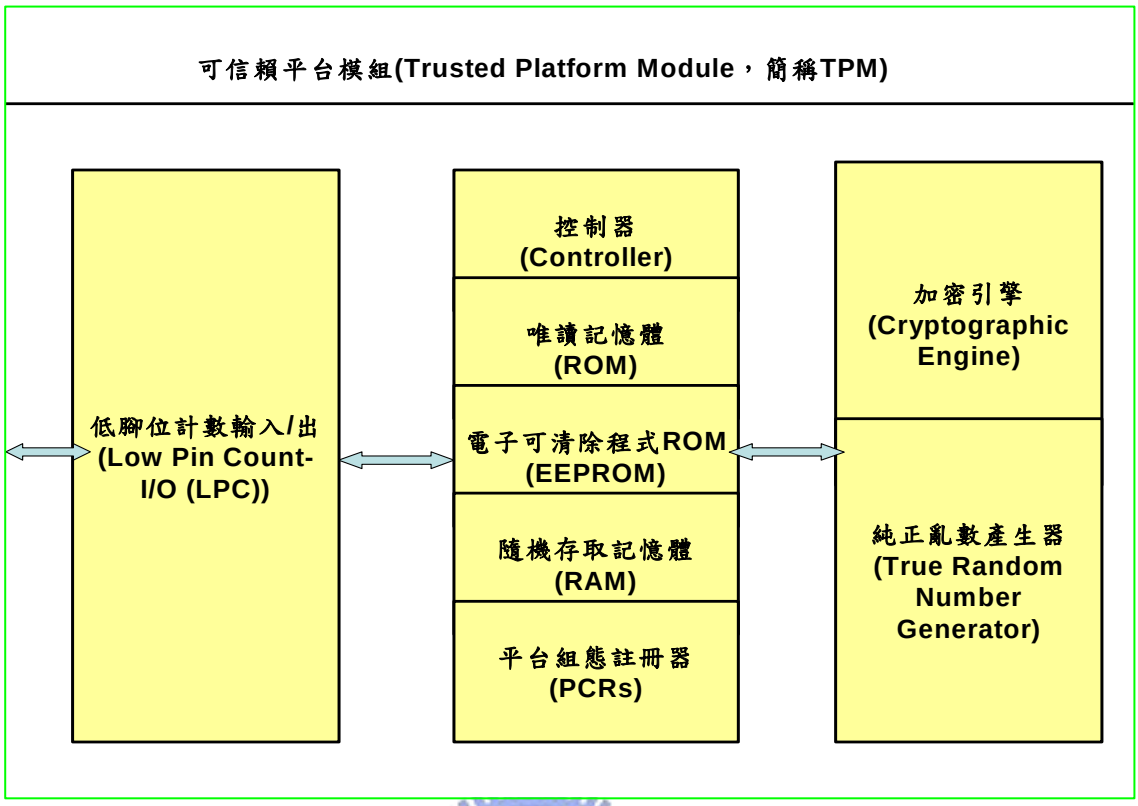


圖 2.3：TPM 架構示意

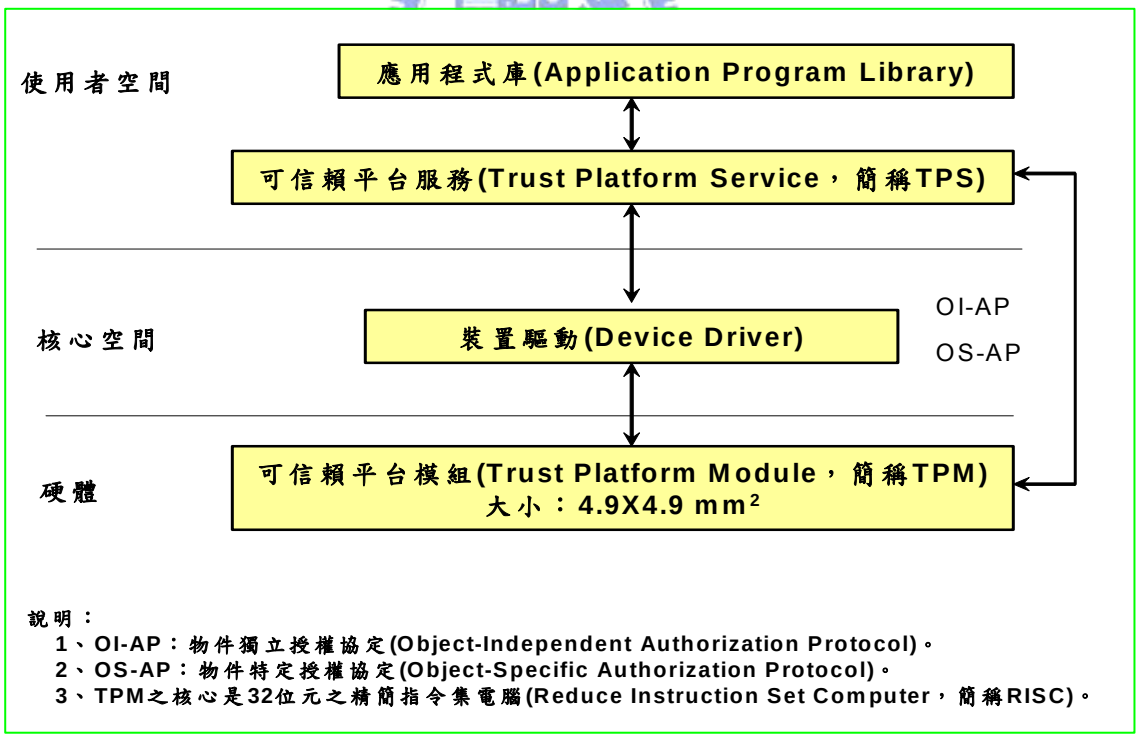


圖 2.4：TCP 安全次系統框架示意

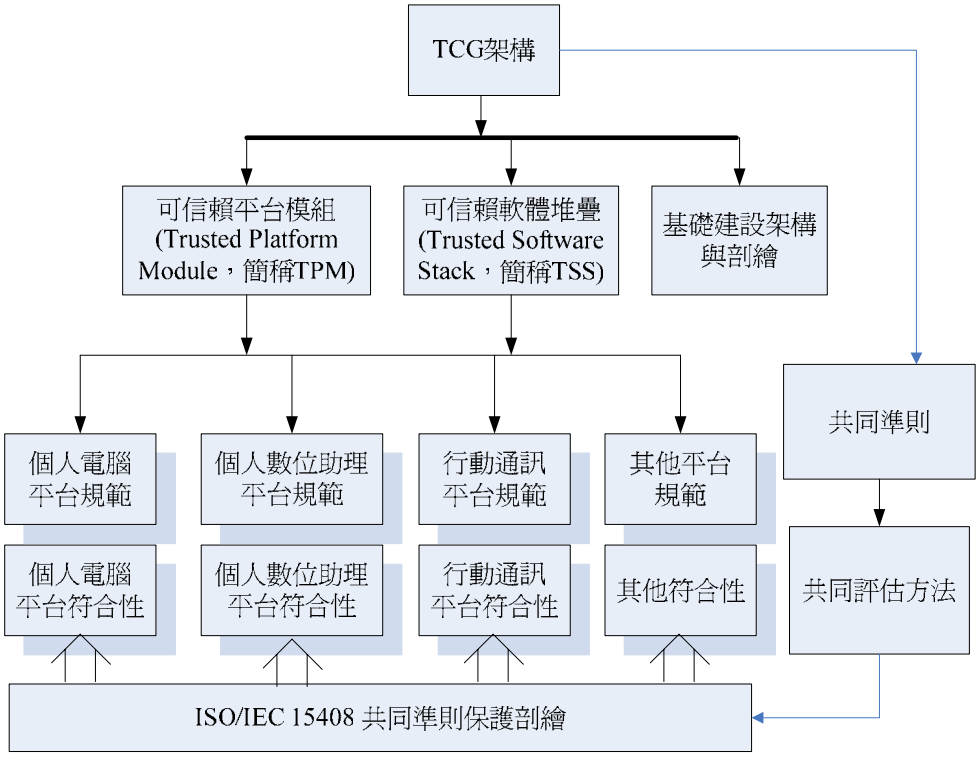


圖 2.5：可信賴計算集團架構

綜上所述，密碼技術已成為圖 2.1 中，多層級之保護層次與方法的礎石。然而，「水能載舟，亦能覆舟」，在 TCP 普及之數位社會，誰掌控了 TPM，誰就掌握了資訊權，更擁有發動資訊戰的利器。鑑於 TCP 與 TPM 之重要性，相關國家均戮力建置自行掌控 TCP 與 TPM 之能量。海峽對岸，在其十五(2001~2005 年)科技攻關之項目中，已於 2004 年 10 月 21 日，宣布完成自行研發之 TCP 及 TPM；並於 2005 年 1 月 19 日正式成立中國全國安全標準化委員會之可信計算工作組，冀期同無線安全般制定中國的 TCP 以及 TPM 國際標準，並宣布未來之 TCP 產品，在中國必須使用中國自製的 TPM【76】。

三、金鑰回復式密碼系統安全規範初探：

3.1、前言：

政府對於人民的秘密應該知道多少？這是一個古今中外永無定論的大問題，然而，在今日資訊化的時代，這個問題已經可以適度的數量化，變成資料加密使用之密碼模組的位元之爭。40 位元、56 位元、128 位元、192 位元還是 256 位元？這場看似「錙銖必較」的爭論，將對未來的個人隱私和群體安全，產生根本與深遠的影響。在虛擬社會中，日常生活各個層面的活動均迅速透明化與數位化，無論從個人隱私、群體安全、身分鑑別、交易安全、授權認證等，密碼模組技術都是最基本的要件之一；甚至在商家鐵捲門與汽車的遙控鎖等均需使用，方能有效保全防止掃瞄解碼行竊集團的毒手。但是，「劍有雙刃，可以自衛，亦可傷人。」，密碼模組技術固然是奠定資訊社會安全的基石，在另一方面，也是犯罪的利器，能輕易妨礙治安單位對犯罪行為的防範、偵測與依法取用。1993 年 2 月 26 日美國紐約的世貿中心爆炸案，因為無法破解的筆記型電腦而大費周章，就是例證。以色情犯罪為例，如果犯罪者使用最簡單的電子信封傳遞色情圖片，治安單位在查扣電腦後，解讀即非易事，將增加定罪的困難性；近年來，恐佈分子與黑道成員等日益猖狂，即使是最重視個人隱私的民權鬥士也不得不承認，某種型態的密碼模組依法取用之技術機制確有必要【29】。在電子化/網路化資訊社會中如何訂定與執行適當的密碼模組技術，先進國家在此問題上的曲折經驗自有值得借鏡之處。資料加密問題因需兼顧個人隱私與群體安全，所有抉擇均得失互見，極難面面俱到；在此一公共政策訂定與執行之後，如何保障國民的秘密通訊自由而又能在必要時，由政府執法或經授權人員能在法律許可範圍內，依法實施監聽或開啟「電子化/網路化社會」中之「電子銀行保險箱」、「安全遙控鎖」等的「金鑰回復式密碼系統（Key Recovery System，簡稱 KRS）」，已是全球各國政府、研究及學術機關與廠商積極研究、實驗或執行的課題【7, 29】。

為因應網際網路的日益普及，密碼技術已成為數位社會安全的基石之一的情境，1997 年 3 月 27 日，OECD 公布了如下之電子資料密碼系統政策八大指導原則【52】：

(1). 信賴原則：為了確保通訊網路系統的安全，各會員國應使用具有一定信賴度的保密系統。

(2). 選擇原則：各會員國網路使用者，於該國法律規定範圍內，應被賦予可選擇使用任何密碼演算法之權。

(3). 市場主導原則：密碼系統之開發及應用應配合個人、企業及政府機關不同之需求及責任範疇進行。

(4). 標準化原則：各會員國應以配合國家整體發展及國際共同趨勢之立場，對於密碼系統的技術標準、技術條件及共同協定之發展及制定以法律加以規範。

(5). 隱私許可原則：各會員國於擬定電子資料密碼系統時，應特別保障個人的隱私權，其中包括秘密通訊及保護資料安全之權利。

(6). 依法取用原則：即使各會員國容許國家依一定之法律程序讀取網路使用人之明文檔案、密碼金鑰或是加密處理過的電子資料，本準則其他事項應受到各會員國最大的尊重。

(7). 責任原則：無論是以契約或立法方式為之，各會員國對於提供密碼系統相關之服務及知悉或保有密碼金鑰之個人或法人，應課予清楚之法律責任。

(8). 國際合作原則：各會員國政府應共同合作以使各國的電子資料密碼政策趨於一致，為達成此目的，各會員國並應排除相關障礙，以避免妨礙國際貿易之進行。

其中「依法取用」原則，是自 1991 年起歐美各國即正式討論如何在資訊時代能兼顧「個人通訊自由與隱私」以及「維護社會安全依法取用」應有之法規與機制的結果，除了正式宣示植基於「金鑰回復(Key Recovery)」能適當保護個人隱私之「依法取用金鑰回復式密碼系統」是 OECD 的指導方針外，同時透過瓦聖那協議(The Wasnaar Arrangement，簡稱 TWA)等國際組織進行控管中【29】；換言之，未來使用密碼模組的機構均須面對「金鑰回復(Key Recovery)」之密碼系統的管理問題。

美國政府在 1993 年 4 月宣佈了一種符合能同時滿足使用者能秘密通訊，政府也能依法取用(Lawful Access)需求的密碼系統，該系統包括：金鑰代管式密碼系統(Key Escrow System，簡稱 KES)和能防止外力讀取(Tamper-proof)資訊的 Clipper 晶片。KES 除了能提供使用者對資料進行適當的加解密外，還可以在必要時，分由兩個具有公信力的公正機構，依法提供執法機關監聽訊息所必須使用的各自擁有之「代管金鑰」的部份資訊。1994 年 2 月美國政府進一步發表有關金鑰代管式密碼系統中使用的「代管加密標準(Escrow Encryption Standard，簡稱 EES)」。該標準主要應用在具敏感性卻非機密性的資料通訊上，包括：電話、傳真和資料傳輸等等。EES 主要目的，是希望在保障民眾的隱私(privacy)外，也可以維護政府的公權力，唯提出之後引起諸多質疑。此外，EES 也提供組織或個人一個使用代管式密碼系統之後，可能發生金鑰損毀或遺失時的解決之道；因此，KES 又稱金鑰回復式密碼系統(Key Recovery System，簡稱 KRS)。在美國 EES 是一個非強制性的國家標準；然而，超過 40 位元的密碼產品從美國銷往台灣時，均須承諾執行 KRS【40】，譬如美國國際商業機器公司(International Business Machines Corporation，簡稱 IBM)的 Lotus Notes 於 1996 年 1 月 18 日宣布執行 KRS。IBM 更發明了商業資料加罩設備(Commercial Data Masking Facility，簡稱 CDMF)技術【38】，使得超過 40 位元金鑰長度之加密設備，在台灣使用時只有 40 位元金鑰長度之加密功能以避開代管金鑰問題，由於使用 CDMF 技術，加密金鑰僅有 1, 099, 511, 627, 776 組有效的加密金鑰，使用窮舉法，美國執法人員能輕易依法破解使用 CDMF 技術之美國加密產品反監聽等功能；同理，不法之徒亦能破解此反監聽功能。換言之，我國若不早日立法禁止 KRS 中之「回復金鑰」不得由外國「依法保管」，則美國相關單位在必要時，可能隨時可以使用 KRS「依法」實行「網路監聽」，表 3.1 是其發展史的簡述。自 1991 年 12 月起，歐盟、北美及紐澳各國政府即開始合作推動資訊社會的「依法取用」工作，目前已進入立法階段，表 3.2 是其執行方案發展史的摘記。為公共安全計，政府有關單位實應早日律定資訊社會「依法取用」的相關法令與 KRS 技術規範，做為在數位社會中，建立如何開拆電子文件信封，電子語音信封等之發奸摘伏，防微杜漸應有「能適當保護個人隱私」的類似「金鑰回復」機制之「金鑰管理基礎建設(Key Management Infrastructure)」的礎石；同時，避免購置具有 128 位元金鑰長度，卻是使用 CDMF 之加密設備而不自知，或是因無法使用 KRS 機制而禁止使用類似 Lotus Notes 產品電子信封功能的狀況發生。

表 3.1：金鑰回復式密碼系統簡史

0	源起：
	0.1 1993 年 4 月 16 日美國聯邦政府公佈的 Clipper 晶片，開啟了第三代密碼系：金鑰代管式密碼系統（Key Escrow System，簡稱 KES）的大門。
	0.2 KES 使用 80 位元的 Skipjack 加密演算法及法律授權存取單位（Law Enforcement，簡稱 LEAF）。
	0.3 委付金鑰管理單位（Escrow Agents），一為美國國家技術標準局，一為美國財政部自動系統局。
1	1995 年 11 月 6 日，美國國家標準與技術研究院（National Standards and

Technology，簡稱 NIST）公布了允許滿足 KES 特性且金鑰長度小於 64 位元（例：DES）的加密產品出口標準草案。

2 1996 年 1 月 18 日，Louts Notes 4.0 與 TIS（Trusted Information System）Gaunlet Firewall 同時宣布已獲得美國聯邦政府同意，出口類似 DES64 位元金鑰的加密產品，TIS 同時宣布了回復金鑰（Recover Key）的技術。

3 1996 年 10 月 1 日，美國高爾副總統首次公佈美國白宮植基於回復金鑰的全球金鑰管理基礎建設（Key Management Infrastructure，簡稱 KMI）計畫，超過 70 家公司組成金鑰回復聯盟（Key Recovery Alliance，簡稱 KRA）正式成立。

4 1996 年 11 月 15 日，美國柯林頓總統發佈了有關非軍事用途加密金鑰出口控制的章程及執行命令，允許金鑰長度小於 64 位元的加密金鑰及其相關產品在 KMI 規範下出口，同時任命 David L. Aaron 先生為代表美國與 OECD(Organization for Economic Cooperation and Development)29 個國家協商 KMI 的大使。

5 1996 年 11 月 25 日，美國國家技術標準局，將其公開金鑰基磐安全服務中之金鑰託管式密碼系統改成可信賴的第三者之回復金鑰管理機制。

6 1996 年 12 月 30 日，美國 BXA(Bureau of Export Administration)發行了一立即有效的加密產品出口管理規則(Export Administration Regulations)，允許承諾執行回復金鑰計畫的廠商，在 1998 年 12 月 31 日出口 64 位元金鑰長度的加密產品。

7 1997 年 7 月 17 日美國參議院商業委員會通過之「公共網路安全法(Secure Public Network Act)」中，明文規定：

7.1 「強制」規定美國境內所有(包括大學在內)隸屬聯邦體系的網路必須使用金鑰回復式密碼系統。

7.2 擴張行政機關的職權，允許只憑一紙行政單位的傳票(Subpoena)而不必事先取得法院的同意，便可逕行要求金鑰回復機構將加密文件予以解密回復，而且不必通知當事人。

7.3 放寬對商業使用的編碼加密產品出口管制，許可長度小於 56 位元的產品出口，但對於參與金鑰回復式密碼系統的加密產品則不受此長度限制。

8 1997 年 8 月 29 日美國眾議院通過之「以編碼加密技術保障安全與自由法(Security And Freedom through Encryption Act)」，簡稱「安全法(S.A.F.E. Act)」中，同意「調查或政府執法部門植基於法律，具備取得加密資訊金鑰的權利。」。

9 1998 年：

9.1 1998 年 7 月 7 日，美國 NIST 公布金鑰回復產品需求草案。

9.2 1998 年 9 月 16 日，美國柯林頓總統宣布除了伊朗、伊拉克、利比亞、蘇丹、敘利亞、北韓以及古巴等支援恐怖活的國家外，美國廠商均可出口 64 位元的金鑰長度的加密產品；此外，除了金融業，美國廠商亦可對醫療、保險業等輸出 128 位元金鑰長度的加密產品。

9.3 1998 年 12 月瓦聖那協議（Wassenaar Arrangement）第 4 次會員大會中，對 KMI/KES 的議題並未達成共識，德國、法國政府相繼將放棄 KES，成為執行 KMI 之重大挫折。

10 2000 年：

10.1 KRA 於聯合國資訊安全刊物發表金鑰回復式密碼系統專案之成果。

10.2 金鑰回復式密碼系統保護剖繪（Protection Profile，簡稱 PP）公布。

11 2001 年 10 月 26 日，美國國會通過明確規範主管機關取得法院許可後可以進行電子郵件、網路瀏覽、線上通訊等網路監視活動之美國愛國者法案(USA PATRIOR Act)。

表 3.2：金鑰回復式密碼系統執行方案發展簡史

1 參考資料：http://www.telepolis.de/tp/english/special/enfo/5382/1.html (1999 年 8 月 3 日)。

2 目的：

2.1 促使業者充分與警察及情治單位合作。

2.2 要求廠商所生產的通訊設備應符合金鑰回復等之規格標準。

2.3 各國實施電信與網路監聽應該有法律依據。

2.4 儘量邀請歐盟以外工業化國家參加。

2.5 加強管制密碼技術。

3 1993 年 11 月 29~30 日，歐盟內政與司法部長會議中，同意美國聯邦調查局的建議，把澳洲、加拿大、香港與紐西蘭納入，同時與其他工業化國家交換電信與網路監聽資訊。

4 1994 年於 3、4、11、12 月的歐盟 K4(專負處理警察、移民、政治庇護與法律合作事務)委員會，討論由荷蘭提出的「合法監聽電信與網路」計畫草案。

5 1994 年 11 月歐盟 K4 委員會決定「先由西方國家實施並統一所有的規格與程序，然後再將產品銷售給其他國家，如此一來，即使不願意參加的國家，在使用標準規格的產品時，仍然可以執行電信與網路的監聽。」之策略。

6 1995 年 1 月 17 日，歐盟通過了其 K4 委員會提出的草案，要點如下：

6.1 為了打擊重大犯罪與保障國家安全，執法機構有權全面監聽電信與網路，同時依法規範業者應有的作業程序與應具備的條件，並且規定監聽的方式與內容不得外洩。

6.2 採行丹麥的制度，各國儘量以修訂刑法的方式來解決人權與隱私權的問題。

7 1995 年 11 月 13 日，歐盟 K4 委員會中的警察工作合作組由西班牙提出 1993 年 7 月發交各會員國填答問卷的總結報告：

7.1 丹麥、德國、奧地利、盧森堡、西班牙、葡萄牙僅需修訂刑法。

7.2 挪威、瑞典、英國、愛爾蘭、荷蘭、比利時、法國、義大利、希臘需另訂新法。

7.3 建議對於可能判處一年刑期以上的「組織犯罪」嫌犯均實施監聽。

8 1995 年 11 月 23 日，歐盟十五個會員國的內政與司法部長簽署備忘錄 (Memorandum of Understanding，簡稱 MOU)。

9 1995 年 12 月，歐盟各會員國的常駐代表，同意致函相關國際標準組織，要求業者遵循其所定的規格及條件。

10 1996 年 11 月 28 日，歐盟內政與司法部長會議，同意致函邀請若干國家參加計畫。

11 1998 年 4 月，荷蘭上議院通過了一個：「若電信通訊公司不能支援政府依法取用 (Lawful Access)的行動，則禁止其提供服務。」的法律修正草案後送荷蘭下議院審議中。

12 1998 年 12 月 6 日，英國倫敦觀察家(Observer)報社，報導 Enfopol 方案要點：

12.1 美國、加拿大與澳洲將參加 Enfopol 方案。

12.2 預定在 1999 年提交歐盟理事會與議會審議並通過。

12.3 各會員國應在 2000 年之前修法或另訂新法以實施電信與網路監聽。

12.4 歐盟會員國的電信公司均需建立監聽介面供依法監聽之用。

13 1998 年 12 月 3 日 33 個瓦聖那協議(Wassenaar Arrangement)國家代表簽署了加強管制密碼技術輸出的報告，並據以執行。

14 1999 年 1 月 19 日，法國總理喬詩班(Lionnel Jospin)宣布全面解除密碼技術的使用限制，在未修法前，先開放 128 位元以下之加密產品。
15 1999 年 3 月 15 日，於比利時布魯塞爾召開的歐盟會議中再次重申並肯定 1995 年 1 月 17 日的歐盟決議案。
16 1999 年 8 月 27 日，美國聯邦通訊委員會宣布通過美國司法部要求之 9 項監聽新標準中的 6 項，2001 年 9 月 30 日是電信服務業者達成司法部要求之最後期限。
17 2000 年 7 月，英國政府通過「規範暨調查權力法案」，准許執法與安全相關機構取閱電子郵件，並可要求個人或公司交出電子信封等金鑰，拒絕交出者最高可處 2 年徒刑。

為因應數位世界資訊安全的要求，世界經濟與發展合作組織(OECD)自 2001 年 9 月 11 日起，由資訊安全及隱私工作委員會(Working Party on Information Security and Privacy，簡稱 WPISP)之專家群(Working Group)經過 4 次 6 天的討論後提出草案，再由 WPISP 經過 3 次 6 天的討論送 OECD 大會(Council)審議，於 2002 年 7 月 25 日公佈「資訊系統與網路安全指導綱要－朝向安全的文化(Guidelines for the Security of Information Systems and Networks：Towards a Culture of Security)」；同時宣佈此指導綱要取代 1992 年 11 月 26 日公佈之「資訊系統安全指導綱要(Guidelines for Security of Information Systems)」【53】。

2002 年 7 月 25 日 OECD 公佈之指導綱要揭示：認知(Awareness)、責任(Responsibility)、回應(Response)、倫理(Ethics)、民主(Democracy)、風險評鑑(Risk Assessment)、安全設計及實作(Security Design and Implementation)、安全管理(Security Management)及重新評鑑(Reassessment)九大原則如后：

(1). 認知：成員應察覺安全對於資訊系統與網路的必要性，以及應如何加強安全性。資訊系統與網路安全的第一道防線，就是覺察風險之所在，以及有哪些防護手段。組織內、外部的風險都會影響資訊系統與網路。成員應該瞭解，安全上的失誤會嚴重損壞他們所控制的系統與網路；同時也應該察覺因為網路互連與相互依存的特性，所可能對其他系統與網路產生的傷害。成員應瞭解所管理系統的設定值與已有的升級程式、該系統在網路中的位置、有哪些良好的作業方式可用來加強安全、以及是否需要其他的成員加入。

(2). 責任：所有的成員都要負責資訊系統與網路的安全性。因所有成員都必須依賴互相連結的本國與世界各地資訊系統及網路，故應該瞭解自己對這些資訊系統與網路所應負的責任。各成員都應按照各自的角色負起應有的責任，成員應定期審核自己的政策、實務、措施、以及工作流程，並評鑑這些項目是否符合這個環境。開發、設計與提供產品及服務的單位應解決系統與網路安全的問題，並即時把適當的資訊發送出去，包括升級程式，讓使用者更能瞭解產品及服務的安全功能，以及自己對安全有什麼樣的責任。

(3). 回應：成員應即時動作，並以合作的方式預防、發現及回應安全事件。所有成員應體認到資訊系統與網路是互相連結的，而且可能在極短時間內造成極大範圍的損失，所以應即時動作，並以合作的方式回應安全事件。成員間應視情況分享有關安全威脅與弱點的資訊，並推動工作流程，以便能迅速、有效進行合作，預防、發現及回應安全事件。如果情況允許，可以與其他組織分享資訊並進行合作。

(4). 倫理：成員應尊重其他單位的法定利益。由於這個社會的資訊系統與網路已經極為普遍，所以成員必須瞭解到，自己的作為與漠然都可能對他人造成傷害。因此道德

行為極為重要，而成員應努力制訂、採用最佳的實務作法，以提倡瞭解安全需求的行為，並尊重其他單位的法定利益。

(5). 民主：資訊系統與網路的安全性應與民主社會的基本價值觀並行不悖。執行安全措施的方式應與民主社會認可的價值觀若合符節，包括交流思想與意見的自由、資訊流通的自由、資訊與通訊的機密性、對個人資訊進行適當保護、開放性與透明性。

(6). 風險評鑑：成員應進行風險評鑑作業。風險評鑑作業可發現威脅與弱點之所在，並且涵蓋範圍應夠廣泛，以便納入主要的內部與外部因素，如技術、實體與人為因素、政策與牽涉安全問題的第三人服務。風險評鑑作業能決定可接受的風險等級，並協助選擇適當的控制措施，以根據所保護的資訊之性質與重要性，管理資訊系統與網路的風險。由於越來越多的資訊系統互相連結，因此風險評鑑作業應該考量到其他系統所導致的潛在傷害，或可能對其他系統產生的傷害。

(7). 安全設計與實作：成員應把安全性當作資訊系統與網路的基本要件。必須謹慎設計、執行、協調系統、網路與政策，才能達到最佳的安全性。這份工作的主要（但非唯一）重點，在於設計並採行適當的防護手段以及解決之道，以避免所發現的安全威脅與弱點，或降低可能的損害程度。防護手段與解決方法必須兼顧技術與非技術層面，而且必須與組織系統及網路上的資訊價值成正比。安全性應該是所有產品、服務、系統與網路的基本要件，而且是系統設計與架構的一部份。為了保護一般使用者，設計與執行安全措施的工作重心，就是為這些人的系統挑選、設定產品與服務。

(8). 安全管理：成員應採用完整的方法來進行安全管理工作。安全管理工作應該根據風險評鑑的結果，而且應該有彈性，能包含所有成員的活動以及各個層面的作業。包括預先反應即將產生的安全威脅，並處理安全事件、系統復原、持續維護、審核與稽核作業的預防、偵測與回應等工作。應協調、整合資訊系統與網路安全政策、實務、措施與工作流程，以便創造協同一致的安全系統。安全管理的要求需視各成員涉入的程度、角色、風險與系統需求而定。

(9). 再評鑑：成員應審核並再評鑑資訊系統與網路的安全性，並對安全政策、實務、措施與流程作適當修改。安全威脅與脆弱性不斷產生、演變。成員應對所有層面的安全性持續進行審核、再評鑑、與修改，以便與這些不斷蛻變的安全風險抗衡。

綜覽 10 年來 OECD 對數位社會安全機制的觀點除了在標題中增列網路安全之重要性外，同時將典範轉移至回應、安全管理以及安全設計與實作等如表 3.3 所示，金鑰回復式密碼系統已是其塑造安全文化之資訊系統安全管理鏈條中的一環。

表 3.3：世界經濟與發展合作組織(OECD)資訊系統安全指導綱要原則比較

	認知	責任	回應	倫理	民主	風險評鑑	安全設計與實作	安全管理	再評鑑	多層面紀律	成正比	整合	適時
OECD: 1992	V	V		V	V				V	V	V	V	V
OECD: 2002	V	V	V	V	V	V	V	V	V				

說明：

1. 10 年來，OECD 將回應、風險評鑑、安全設計與實作、安全管理取代多層面紀律、成正比、整合及適時之原則。
2. 倫理、民主與風險管理已成為 OECD 安全的文化原則之核心。

3.2、公開金鑰基礎建設與金鑰管理基礎建設：

電腦與傳播科技大師 Nicholas Negroponet 先生，在「數位革命」一書中曾說：「從原子潮流演變到位元的潮流已是勢不可當，不可逆轉」。在網路通訊、多媒體技術日趨成熟的今天，我們也確實可以看到如文件資料、音樂、影片等傳統上必須藉助原子型態（紙張、錄音帶、影碟等）送交的物件，正漸漸地轉變成位元的型態，經由高效率的網路，傳送到大眾的眼前。隨著網路的普及與資訊設備性能持續提高而價格卻不斷下滑，已使許多電子文件可以藉由電腦與網路系統進行，網際網路急遽成長已改變了人類許多的行為，也衍生了許多管理上的問題。當人與資料互動的時候，如何在捕捉、分配、儲存及管理資訊流程的過程中，提供適當的防護措施來確保資訊系統面對竄改、竊取、遲滯、冒名傳送、否認已傳送、非法侵入等問題，而建置一個可以信賴的資訊系統作業環境，以奠定資訊社會的基石，已是眾所矚目的焦點。

為了維護資訊在網路上傳遞時的安全，一般均使用密碼技術，對於欲傳輸的資訊，在傳遞前予以加密處理。基於「公開金鑰型密碼系統」具有實現「數位簽章」的特性，與不需事先交換金鑰，即可達「秘密通訊」的優點。目前均使用公開金鑰型密碼系統，對所要傳遞的資訊予以加密或簽章。為了使公開金鑰型密碼系統得以順利運作，必須設法緊密結合並證明某一把公(Public)鑰確實為某人或某機構所擁有。我們利用可信賴的第三者(Trusted Third Party，簡稱 TTP)或機構當作金鑰管理與驗證機構，以簽發電子憑證(Cetrificate)方式證明公鑰的效力；因此，必須建立一個憑證管理系統，來負責簽發、註銷電子憑證。除了憑證管理系統外，所有輔助公開金鑰型密碼系統使用與應用服務的工作均可視為公開金鑰基礎建設(Public Key Infrastructure，簡稱 PKI)運作架構的一部份。在實際應用上，基於效率的考量，一般均以公開金鑰型密碼系統搭配對稱金鑰型密碼系統使用，即使用對稱金鑰型密碼系統加密欲傳送的資訊，再將該把「秘密金鑰」以接收方公開金鑰型密碼系統之「公鑰」加密，組成所謂的「電子信封」，並將此金鑰交予公正第三者保管，然後將此電子信封傳送給接收方。接收方必須先以自己的秘密金鑰(本文簡稱「專(Private)鑰」)將電子信封拆封，以獲得「秘密金鑰」，再以該秘密金鑰解出真正的訊息，兼顧方便與效率。表 3.4 是對稱金鑰型密碼系統與公開金鑰型密碼系統金鑰長度比較參考【60】，表 3.5 是不同之金鑰長度在窮舉攻擊法下被破解所需的平均時間。由此可見，公開金鑰型密碼系統，在通訊安全中扮演重要的角色。

表 3.4：對稱金鑰型密碼系統與公開金鑰型密碼系統金鑰長度比較表

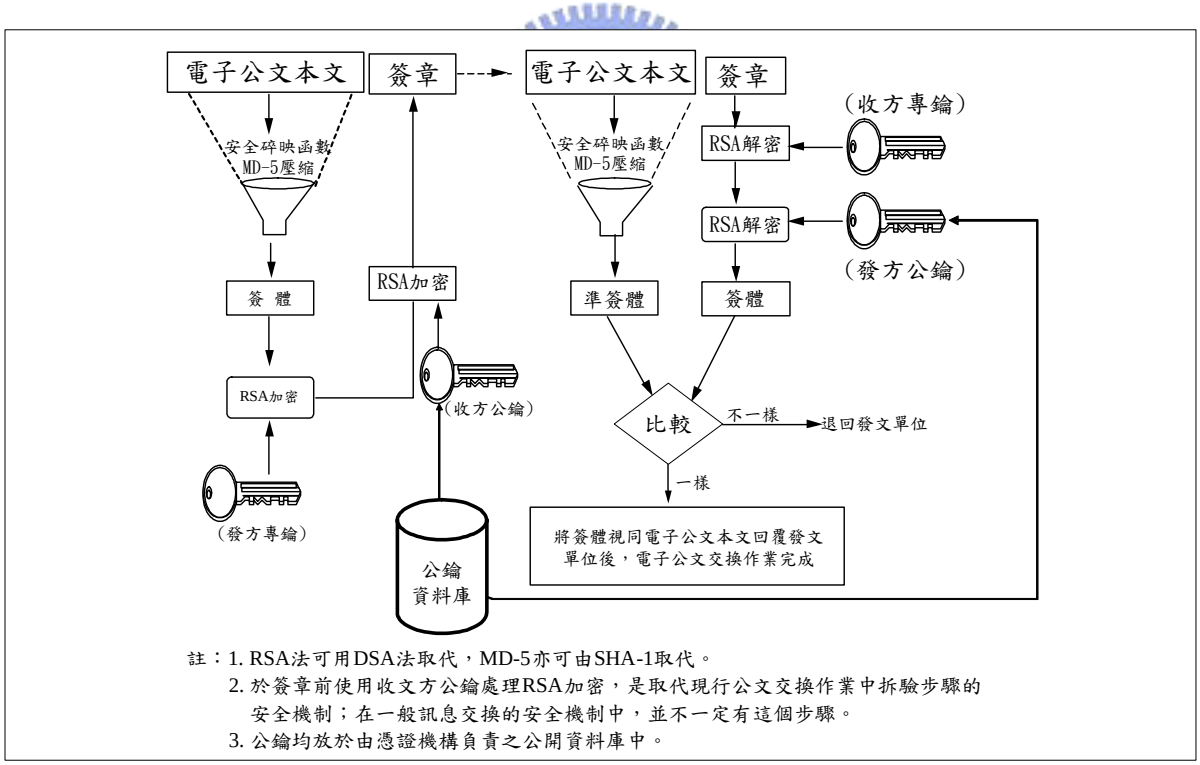
	對稱式加密演算法	雜湊函式	RSA 加密演算法	橢圓曲線
金鑰長度	56 位元	112 位元	512 位元	112 位元
	80 位元	160 位元	1024 位元	160 位元
	112 位元	224 位元	2048 位元	224 位元
	128 位元	256 位元	3072 位元	256 位元
	192 位元	384 位元	7680 位元	384 位元
	256 位元	512 位元	15360 位元	512 位元

表 3.5：在窮舉破解法攻擊下尋找金鑰平均的時間

等價金鑰長度 (位元)	可能的金鑰數	每秒搜尋10^6次 平均破解時間	每秒搜尋10^{12}次 平均破解時間
40	$2^{40} \approx 1.1\times10^{12}$	6.36天	0.55 秒
56	$2^{56} \approx 7.2\times10^{16}$	1142年	10.01小時
128	$2^{128} \approx 3.4\times10^{38}$	5.4×10^{24}年	5.4×10^{18}年
192	$2^{192} \approx 6.2\times10^{57}$	9.95×10^{43}年	9.95×10^{37}年
256	$2^{256} \approx 1.2\times10^{77}$	1.84×10^{63}年	1.84×10^{57}年

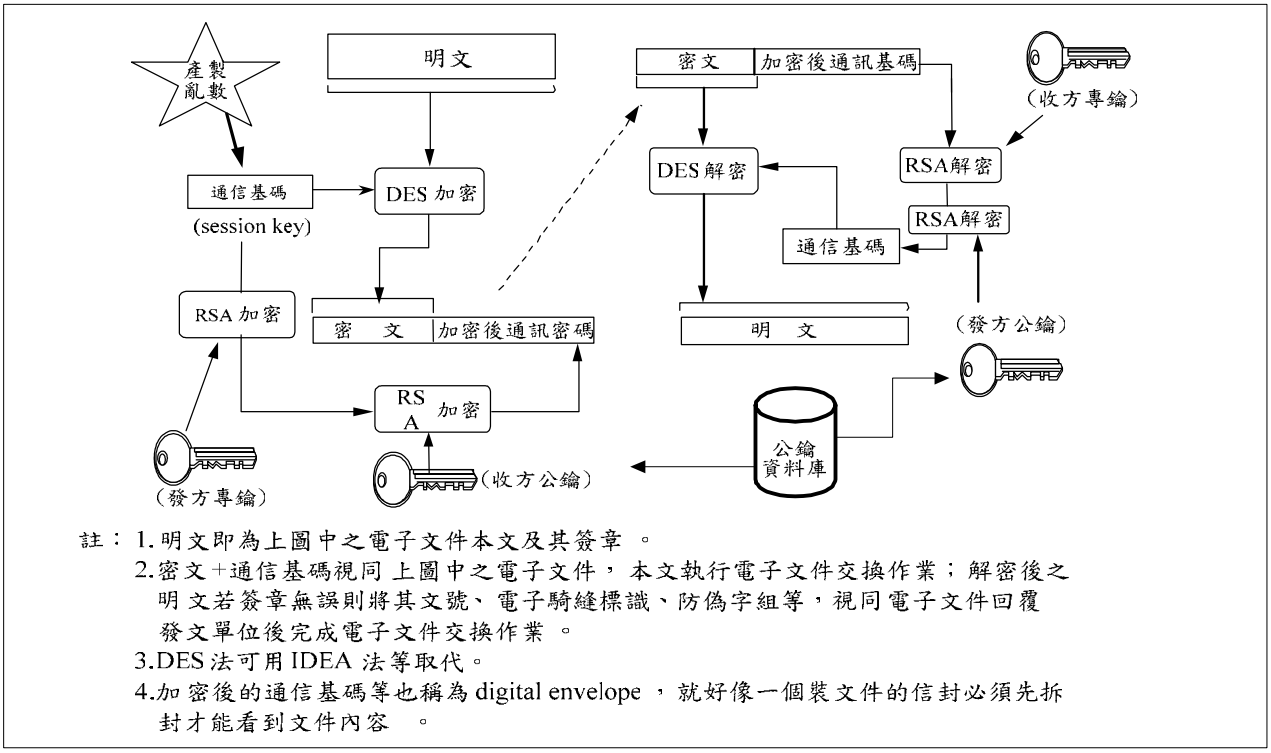
註：在相同安全度的條件下，智慧卡對稱金鑰型密碼系的計算速度約較公開型金鑰密碼系統快10倍【16】。

圖 3.1 是公開金鑰型密碼系統的使用示意，圖 3.2 是公開金鑰型密碼系統與對稱金鑰型密碼系統整合應用示意，圖 3.2 中之通訊基碼即為前述之秘密金鑰。無論是圖 3.1 或圖 3.2 的機制，由於在電腦與網路系統中，傳送的資訊是光電訊號或電磁波、媒體是電纜線、光纖或大氣層並儲存在磁性物質的磁化狀態或半導體物質的電子狀態中，不法人員很容易在公鑰資訊使用的環境中加以竄改、變造、重演或冒名傳送而不留下痕跡；因此，如何在咫尺天涯、素昧平生的電子化/網路化社會中，建置一個能奠定資訊安全的基石之可以信賴的電子文明民主作業環境，已是眾所矚目的焦點。



註：1. RSA法可用DSA法取代，MD-5亦可由SHA-1取代。
2. 於簽章前使用收文方公鑰處理RSA加密，是取代現行公文交換作業中拆驗步驟的安全機制；在一般訊息交換的安全機制中，並不一定有這個步驟。
3. 公鑰均放於由憑證機構負責之公開資料庫中。

圖 3.1：公開金鑰型密碼系統的使用示意



註：1.明文即為上圖中之電子文件本文及其簽章 。
2.密文+通信基碼視同 上圖中之電子文件， 本文執行電子文件交換作業；解密後之明 文若簽章無誤則將其文號、電子騎縫標識、防偽字組等，視同電子文件回覆發文單位後完成電子文件交換作業 。
3.DES 法可用 IDEA 法等取代。
4.加 密後的通信基碼等也稱為 digital envelope ， 就好像一個裝文件的信封必須先拆封才能看到文件內容 。

圖 3.2：公開金鑰型密碼系統與對稱金鑰型密碼系統整合應用示意

美、英、法、澳洲及日本等國均已致力於 PKI 的實現，做為電子化/網路化社會安全的礎石，行政院研究發展考核委員會於 1997 年 11 月公布如圖 3.3 所示之中華民國 PKI 整體架構關係，並於 1998 年 2 月 9 日正式啟用政府憑證管理中心(Government Certification Authority，簡稱 GCA)後，以八十六年度個人綜合所得稅線上申報做為 GCA 啟用後的第一項應用，做為電子化政府中「電子認證機制子計畫」的成果。一般而言，鑑於如智慧卡技術已臻成熟且應用日益普及【8, 17~18】，非常適合做為存放圖 3.1 中之個人身分鑑別用專鑰與啟動電子信封之個人用專鑰的載具；如何確保圖 3.1 與圖 3.2 中之「公鑰資料庫」的安全以及存放與公鑰相對應之專鑰通稱符記卡(Token Card)載具諸如智慧卡等的安全【8, 16~19, 60】，在如圖 3.3 是公開金鑰整體的架構、圖 3.4 之公開金鑰運作機制與圖 3.5 憑證機構服務架構相關作業中，保障消費者之權益，制定相關法律確保 PKI 與 CA 的法效與可信賴性已成為世界趨勢，我國亦於 2001 年 10 月 31 日，立法院三讀通過了已近三年的「電子簽章法」奠定我國 PKI 法律之基礎【25, 81, 88】，並於 90 年 11 月 14 日由總統明令公布，91 年 4 月 1 日起正式施行。此外，為使電子簽章法制更為完備，經濟部依據電子簽章法之授權，分別制訂了「電子簽章法於行細則」、「憑證實務作業基準應載明事項」以及「外國憑證機構許可辦法」，以為電子簽章法施行之相關配套子法。

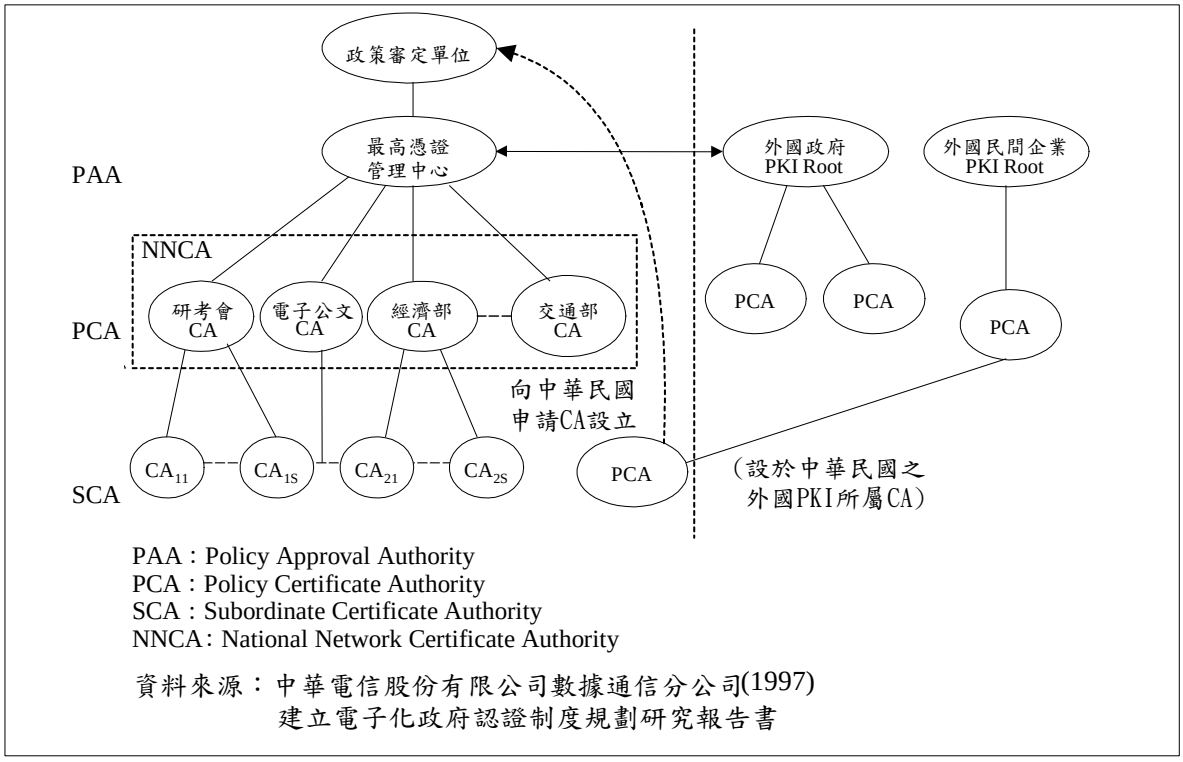
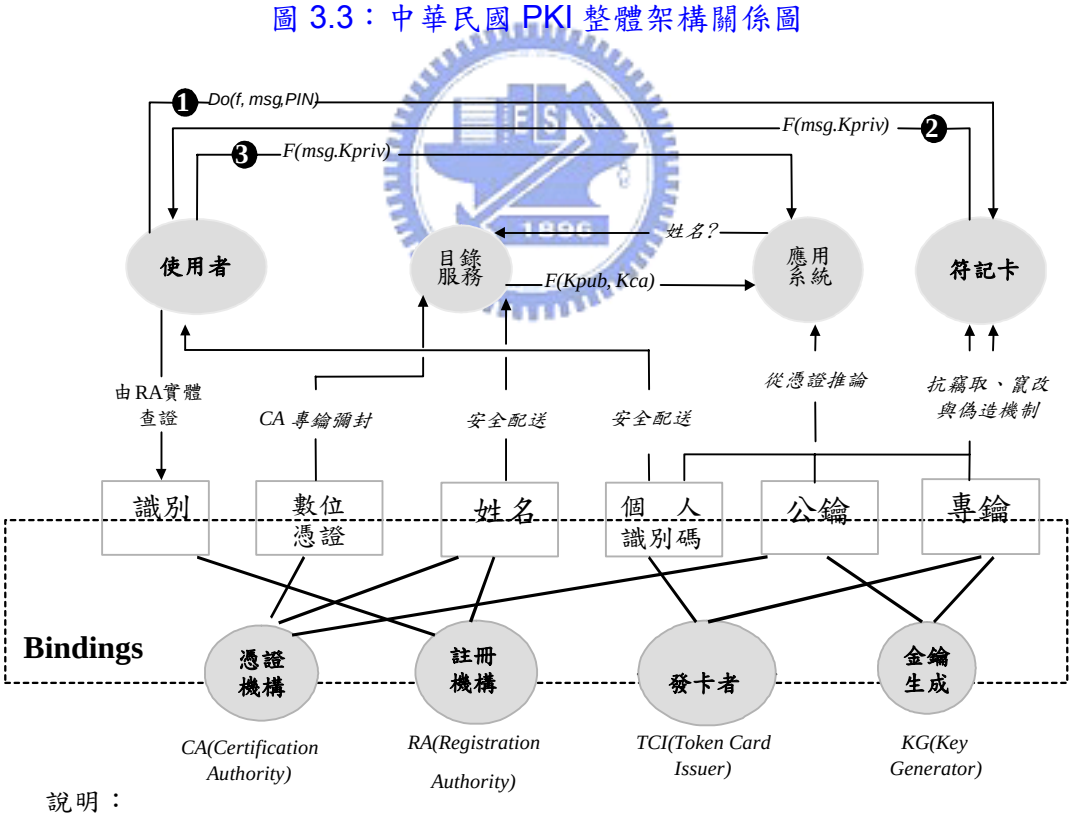


圖 3.3：中華民國 PKI 整體架構關係圖



說明：

Do：執行指令	K_{priv}：使用者專鑰
f：欲執行功能	K_{ca}：CA金鑰憑證簽章專鑰
F：安全函數	msg(message)：訊息
K_{pub}：使用者公鑰	PIN(Personal Identification Numer)：個人識別碼

圖 3.4：公開金鑰基礎建設(Public Key Infrastructure)運作機制示意

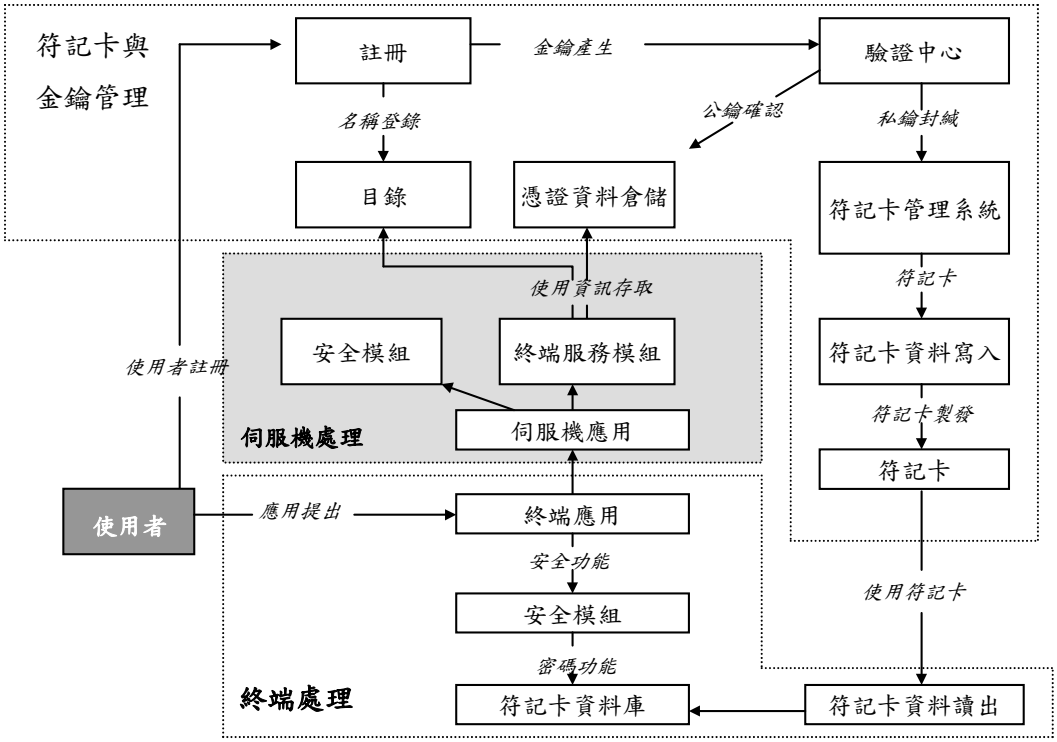


圖 3.5：憑證機構服務架構示意

在 PKI 之標準中，非常重視安全的要求，舉例而言，表 3.6 與表 3.7 分別是 CA 等之憑證表達 ISO/IEC 9594(CNS 13915)及其安全需求的示意說明；圖 3.6 是 CA 等之金鑰管理標準 ISO 11568(CNS 14380)的金鑰管理生命週期示意，其說明分如表 3.8 與表 3.9 所示，圖 3.7 是 PKI 相關標準之安全塑模示意說明。

表 3.6：ISO/IEC 9594-8 簡介

1. ISO/IEC 9594-8 與 X.509 幾乎相同。
2. X.509 的最初版本發表於 1988 年，1993 年發表第二版；主要針對（安全）碎映(Hash)函數的部分從新改寫，1995 年再度修訂，主要是針對建置規範提出 37 頁的修正說明(AMENDMENT 1: Certificate Extensions)；1997 年發表第三版，除訂正一些錯誤外，金鑰種類由第二版的七個增加為九個；2001 年的第四版，增訂授權管理基礎建設(Privilege Management Infrastructure，簡稱 PMI)建置規範。
3. ISO/IEC 9594-8 提供金鑰管理及鑑別簽證服務的協議標準。
4. ISO/IEC 9594-8 採用公開金鑰及數位簽章的技術。
5. ISO/IEC 9594-8 中的數位簽章需要碎映函數與其配合使用。

表 3.7：ISO/IEC 9594-8 中的防護要項

1. 使用者的密鑰被破解。
2. 驗證中心的密鑰被破解。
3. 驗證中心製作不正確的簽證(Certificate)。
4. 驗證中心與使用者共謀舞弊。
5. 偽造的簽證。
6. 偽造的符記(Token)。
7. 密碼攻擊。

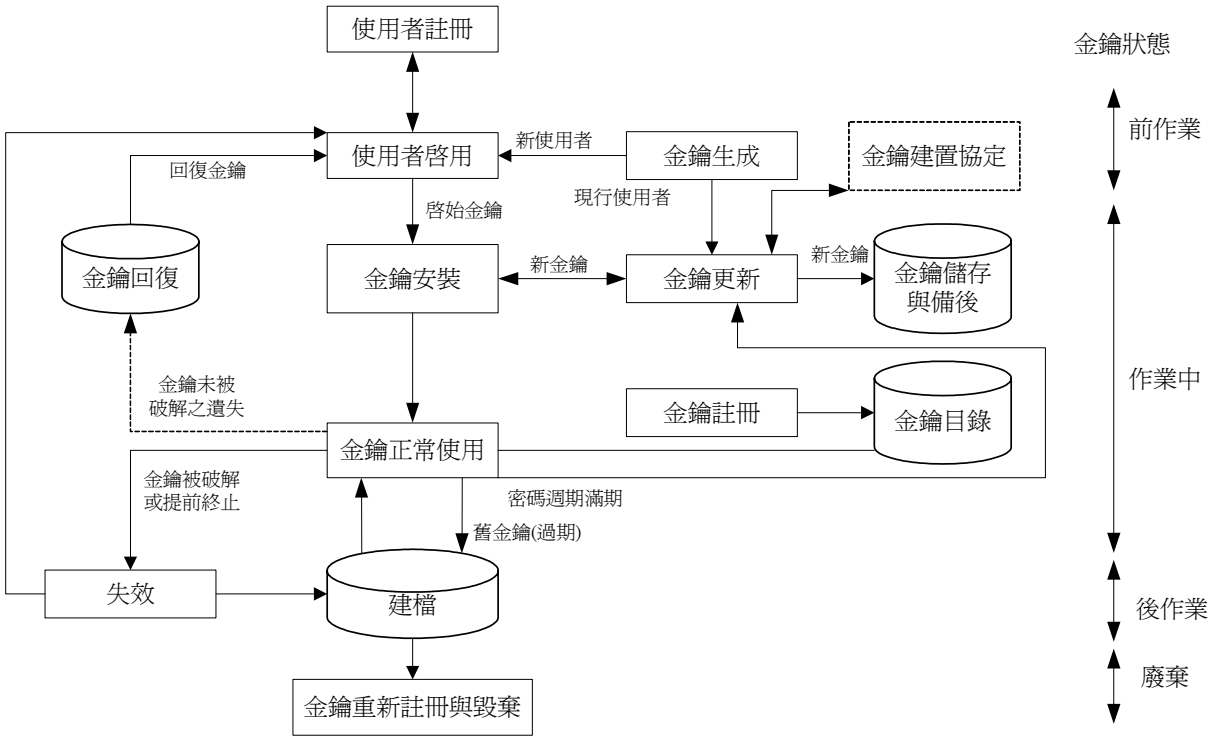


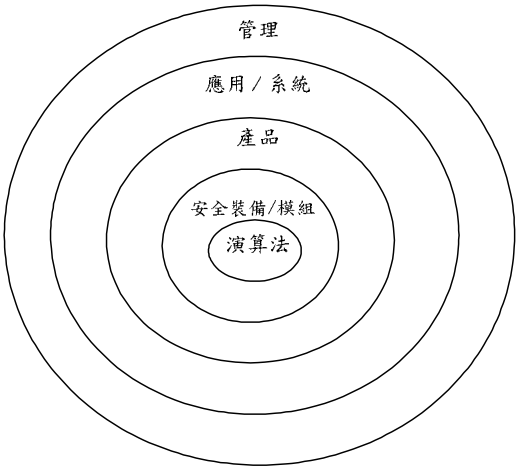
圖 3.6：金鑰管理生命週期示意

表 3.8：金鑰管理之目的

1. 在使用者執行密碼運算時提供所需之金鑰。 2. 控制金鑰之使用。 3. 在金鑰的整個生命週期中提供適當的保護。

表 3.9：金鑰管理之原則

1. 金鑰應只以ISO 11568所允許的形式存在。 2. 沒有人能接觸到未加密的金鑰。 3. 系統需保障曾使用的金鑰之安全。 4. 系統應能偵測金鑰是否已遭攻擊。 5. 系統應能預防/偵測金鑰之不當使用。 6. 產生金鑰的方式應為不可預測的。 7. 系統應能偵測出不當使用金鑰的企圖。 8. 金鑰須定期更新。 9. 在字典攻擊法奏效前須更新金鑰。 10. 得知或懷疑金鑰已被瓦解時，必須立即停用。 11. 不同金鑰之安全性不得互相影響。 12. 已遭瓦解的金鑰不得用於更新作業。 13. 在使用金鑰(load)前，密碼模組設備須證明其安全性。



層次 (Level)	例 (Example)	規範 (Specification)
管理 (Management)	安全控管	ISO/IEC 13335 ISO TR 13569 ISO/IEC 15416 ISO 15782 ISO/IEC 17799
應用 (Application)/ 系統 (System)	電信基礎建設 (Telecommunication Infrastructure)	ISO/IEC TR 19791 ISO/IEC 15504
產品 (Product)	憑證簽發與管理組件 (CIMC)	ISO/IEC 15408 CIMC PP
安全裝備/模組 (Security Device/Module	密碼裝備/模組 (Crypto Device/Module)	ISO 13491 ISO/IEC 19790 ISO/IEC 15408
演算法 (Algorithm)	DES MOVS	ISO/IEC 18033

CIMC ： Certificate Issuing and Management Components.
MOVS ： Mode Operation Validation System.
PP ：Protection Profile.

圖 3.7：PKI 安全模型及其標準舉例說明示意

隨著電子簽章的使用日益普及，「不論這場實驗是好戲還是歹戲，已經開場，開場之後或許我們會猛然發現；在數位社會中，誰與爭鋒，難以確定，誰有權威，同樣未必盡然。」安全的目的是為塑造使用環境的可信賴性，如何恰如其分仍是尚待琢磨的領域，SET 與 SSL(Secure Socket Layer)在電子商務應用上之興衰即為明證(註：由 VISA 與 Master Card 共同經營之「電子交易規格公司(SET Co.)」，已宣布更改 SET 的名稱為 3D-SET 或「Three Domain Model」，可接受 SSL 等 non-SET 規格；VISA 組織已表示 SET 現有之形式並不適合全球電子交易運作，已使用 3D-SET 的作業規格。)惟無論是 3D-SET、SET、SSL 均遵循 PKI 標準對安全之要求。

當使用者因忘記起動圖 3.5 中之符記卡時，如何在「堅若磐石、使用便捷，依法取用，遺失不懼」的使用環境中，經由圖 3.6 之金鑰回復模組(Key Recovery)暨其機制繼續正常使用 PKI。滿足數位社會資訊安全要求的完整之金鑰回復機制，就是 PMI；至 2006 年 5 月 5 日之前，我國的 PMI 僅止於討論，並未建立，惟 PGP 等 OSC 均已提供金鑰回復之模組【92】。

3.3、金鑰回復式密碼系統相關規範：

美國國家標準與技術研究院（NIST）聯邦資訊處理標準（Federal Information Processing Standards，簡稱 FIPS）出版品系列，是在 1996 年資訊科技管理改善條例（Public Law 104-106）第 5131 節以及 1987 年電腦安全條例（Public Law 100-235）所提供下，有關採用並公布標準與指導原則之官方出版品。在這些訓令下，商務部長（Secretary of Commerce）公布適合於聯邦電腦系統效率、安全與隱私的標準與指導原則。美國國家標準與技術研究院透過它的資訊科技研究室，其使命在於為聯邦電腦系統發展標準、指導原則與相關方法及技巧，並對產業與政府在標準實施上提供技術的協助。

NIST 的技術諮詢委員會（Technical Advisory Committee）針對聯邦金鑰管理基礎架構所發展一個聯邦資訊處理標準(FIPS)，在 1998 年 11 月提出一份金鑰回復式密碼系統產品之需求規劃報告（以下簡稱本標準）【44】，這個標準指出聯邦政府機構所使用的金鑰回復式密碼系統產品所需符合的必要條件。這類商品提供了使用於適當授權以取用保管或通訊的資料時，解密資料的金鑰回復機制，同時成為 1996 年 10 月成立之金鑰回復聯盟（Key Recovery Alliance，簡稱 KRA）超過 70 家公司建置金鑰回復式密碼系統的規範【44, 65】。

由於聯邦機構有權利及義務去保護在資訊科技系統間所包含、處理與傳送之資訊與資料。資訊的擁有權通常由個人、公司與機構所共享，因此通常也要求政府為其本身或共有者之利益而保護此資訊。這種保護必須符合或超越聯邦政府與那些共有者的標準。

「加密」是保護通訊或保管的資料之私密性的一個重要工具，當運用合宜的「強加密」演算法並以適當的保證實施時，「加密」可以預防通訊或保管的資料洩漏給未授權的關係人；但是，「無法取用」、「遺失」或「毀壞」解密資料需用的金鑰會可能防礙對獲得授權之關係人的依法取用其資訊。為便於獲授權者取用加密資料時可能遭遇到這種失誤，NIST 因此提出需求規劃報告，以藉此標準建立金鑰回復式密碼系統產品的必要條件。

本標準既未要求也未推薦任一用於金鑰回復式密碼系統的特定技術。本標準致力於與技術無關，是以不至於不當地阻礙此新領域的創新。然而，並非每一個想的到的金鑰回復技術都一定可以經本標準成功的評估，例如，本質上就不安全的「金鑰回復式密碼系統」技術或許是無法評估的。

標準中提出一個「金鑰回復式密碼系統」的通用模式。此模式確認任一「金鑰回復式密碼系統」的固有功能：「金鑰回復資訊」（Key Recovery Information；簡稱 KRI）的產生、「金鑰回復資訊」的管理、要求金鑰回復，以及以一個或多個金鑰回復代理（Key Recovery Agents，簡稱 KRAs）來滿足要求金鑰回復的需求。本標準建立個別「金鑰回復式密碼系統」功能施行時在功能、安全、安全保證、及互通的需求。

本標準並未要求供評估的產品要包含所有訂定之功能，附屬產品可能無法構成一個完整的「金鑰回復式密碼系統」。本標準也未要求從單一廠商提供的單一產品或整套商品要包含一個完整的「金鑰回復式密碼系統」所需要的所有功能。因此，本標準允許根據由一個或多個來源的產品組合所模組化製作之「金鑰回復式密碼系統」。因為運用金鑰回復的機制需要一個具備完整功能的「金鑰回復式密碼系統」，其他文件應提供額外的指示以協助評估以符合本標準評估之數個產品（從一個或數個廠商）組合的系統之安全性。

「金鑰回復式密碼系統」的安全依賴不同安全領域，包括電腦、通訊、程序上的、實體的、與個人安全的領域混合。本標準僅陳述「金鑰回復式密碼系統」安全中

關於電腦與通訊的方面。其他「金鑰回復式密碼系統」運作的重要層面不在本標準之範圍內。例如本標準並未陳述這類考量：「如果金鑰回復式密碼系統必須確保經授權可取用加密資料，此系統必須立即可用並可長存。」等之需求，又如，許多金鑰回復方法利用公開金鑰技術與相關的公開金鑰基礎建設（Public Key Infrastructure，簡稱 PKI）。但是，公開金鑰基礎架構安全的許多層面並不在本標準範圍內。因此，遵循本標準代表一套對所有「金鑰回復式密碼系統」安全與實用的必要但非充分之條件；NIST 將金鑰回復系統之安全分成低安全性之 Level 0，中等安全之 Level 1 與高安全性之 Level 2 的 3 個等級。

如果「金鑰回復式密碼系統」作為機構所提供之服務，此機構可以運用符合本標準的產品（例如 KRA）。但是，附屬產品的使用並不保證全體「金鑰回復式密碼系統」的安全，也不保證如上述的立即可用並可長存之「金鑰回復式密碼系統」功能；因此，「金鑰回復式密碼系統」提供之服務不能說是遵循本標準。

3.3.1、金鑰回復模式：

「金鑰回復式密碼系統」讓得到授權者在解密金鑰無法以其他方式取得時，可以將加密的資料回復為普通本文，金鑰回復是一個應用於許多不同金鑰回復技巧的廣義詞彙。各個技巧都導致金鑰—這裡稱為「標的金鑰」（Target Key）—的回復。「標的金鑰」可能是：

(1). 用於解密資料的資料加密金鑰（Data Encryption Key，簡稱 DEK），或是
(2). 一把直接或間接用以將「資料加密金鑰」解密的金鑰。

回復一特定之「標的金鑰」所必要的資訊對不同的技巧而言，可能是相異的。「金鑰回復資訊」一詞指以金鑰回復技巧回復「標的金鑰」所需的匯總資訊，「金鑰回復資訊」可以用不同的方式管理，或許只存在電子傳輸時的短短時間，或者可存放一段相當長的時間。「金鑰回復資訊」可能分佈於不同的處所（例如，在一個或多個「金鑰回復代理」處），與某訊息、檔案結合或附屬於某訊息、檔案，在終端用戶處，在第三者的系統處，在某憑證機構（Certification Authority；簡稱 CA），在某個憑證中，或者在某個申請設備中。

標準中描述兩種形式的金鑰回復技巧：「金鑰封裝(Key Encapsulation)」與「金鑰託管(Key Escrow)」，「金鑰封裝」技巧以允許「金鑰回復代理」回復「資料加密金鑰」的方式，結合金鑰回復資訊與加密資料，「金鑰託管」技巧直接讓「金鑰回復代理」取得密碼終端系統金鑰，通常是長期的金鑰例如公開金鑰/私密金鑰對等。

顯示金鑰回復式密碼系統的一般模式如圖 3.8 所示，包含產生「金鑰回復資訊」，「金鑰回復資訊」管理以及金鑰回復。這個模式顯示為了「標的金鑰」的回復要產生「金鑰回復資訊」，「金鑰回復資訊」的管理和由此「金鑰回復資訊」回復「標的金鑰」。

產生「金鑰回復資訊」由一個或多個「金鑰回復資訊」產生功能所執行，「金鑰回復資訊」管理是由「金鑰回復資訊」傳遞功能以及一個額外的「金鑰回復資訊」確認功能所執行，金鑰回復則由「金鑰回復申請功能」及一個或數個「金鑰回復代理」功能所執行，這些功能如圖 3.9 所示。

金鑰回復模式呈現多個金鑰回復技巧並支援廣泛的資料應用，包括：

(1). 即時通訊（Real-time Communication Sessions）；
(2). 分段遞送通訊（Staged Delivery Communications）；以及
(3). 資料儲存（Data Storage）。

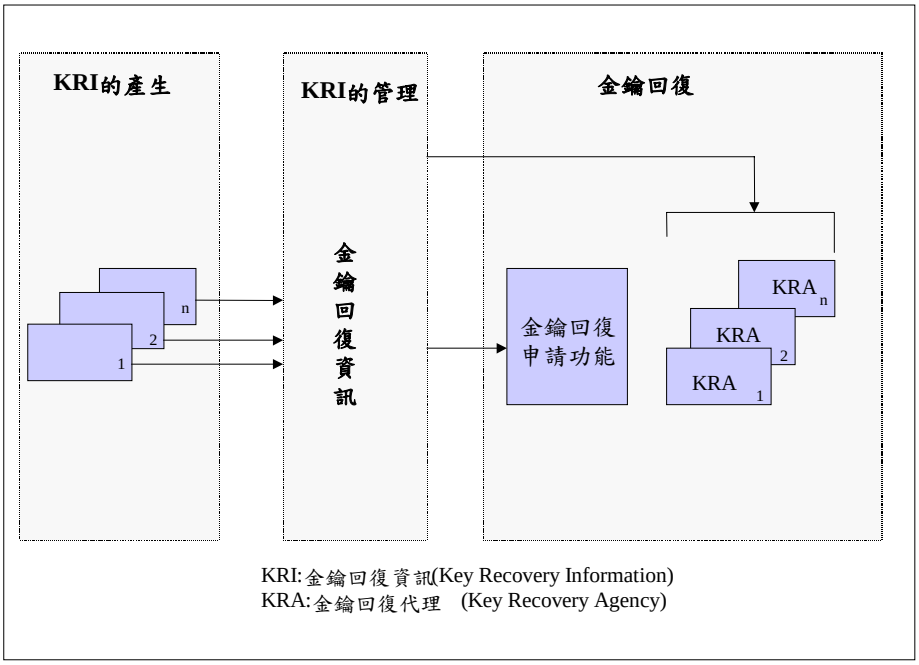
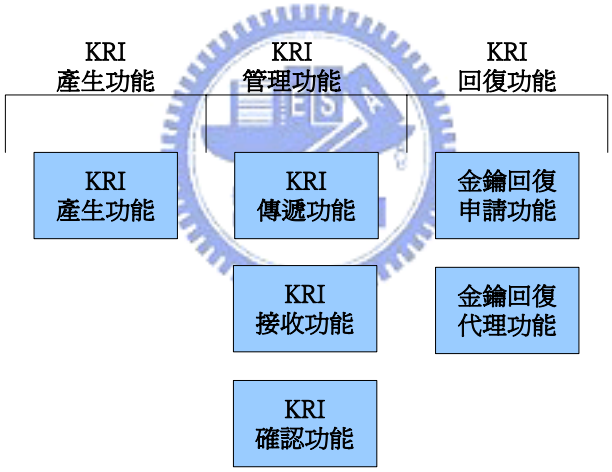


圖 3.8：金鑰回復式密碼系統框架



KRI：金鑰回復資訊（Key Recovery Information）

圖 3.9：金鑰回復式密碼系統的功能

「金鑰回復式密碼系統」可能存在於許多"處所"（例如，密碼終端系統、金鑰回復代理系統、申請系統以及儲存或傳送媒介），應用程式使用的正常金鑰交換機制不一定要被金鑰回復機制所影響；但是，金鑰交換機制會被用來支援金鑰回復資訊的產生及分佈（例如，不排除將金鑰回復資訊整合於現存的金鑰交換機制）。未來，金鑰交換協定設計者或許會發現將金鑰回復整合於協定的基本設計會很有用。

本標準所述之金鑰回復模式之功能必須在與金鑰回復政策及程序合用或形成金鑰回復式密碼系統的產品中實施，金鑰回復政策指出在其政策下，必須產生金鑰回復資訊之情形與可以釋放金鑰回復資訊的狀況，金鑰回復政策指明授權的金鑰申請以及各申請授權以取得資料的情形。金鑰回復政策也指示獲准之金鑰回復代理，如何維護金鑰回復資訊或在何處維護金鑰回復資訊，以及在沒有金鑰回復資訊時，所收到的加

密資訊是否要處理。金鑰回復政策必須是"固定的"（例如，實行的方式不得允許跳過金鑰回復），可由使用者選擇的，或者以政策管理表格或模組實施。

接著，在本節中我們簡述設計與本標準一致之金鑰回復式密碼系統產品的功能性與互通性的必要條件，我們以(Req. No.)條列必要條件如後：

(1) 產品的金鑰回復功能與金鑰回復模式的功能應有清晰的對應。廠商應提供描述完整金鑰回復式密碼系統方法的文件，敘述其產品如何運作於金鑰回復式密碼系統。必須能夠測試所述，介於其產品與用來提供完整金鑰回復式密碼系統方法所需的功能間的介面。

(2) 廠商委託評估產品應交付一份附屬文件，描繪其產品如何合乎本標準所有適用的條件。

(3) 產品應該可以設定組合（Configurable），並且要能夠與某些（無論是否是已有的）產品互通，以形成一個僅由附屬金鑰回復式密碼系統功能組合成的完整的金鑰回復式密碼系統。在沒有任何其他非產品附屬金鑰回復式密碼系統功能下，產品中的附屬金鑰回復式密碼系統功能要能夠獨立運作。

（一）金鑰回復資訊產生功能：

(1) 產品中的某功能如果在有附件或無附件模式下都可以運作，此功能要能夠設定組合，提供使用者可以明確的決定是否引用有附件或無附件模式。

(2) 各個金鑰回復資訊產生功能階段應產生所有金鑰回復資訊或部分金鑰回復資訊。所有金鑰回復資訊產生功能的組合應產生足以回復金鑰的金鑰回復資訊。

(3) 金鑰回復資訊產生功能單一階段組合並形成全部或部分金鑰回復資訊，以提供其他金鑰回復功能使用。

(4) 金鑰回復資訊產生功能負責確保其輸出之有效性。

(5) 金鑰回復資訊產生功能應提供所產生之金鑰回復資訊予金鑰回復資訊遞送功能。

(6) 第二階的產品不可提供使金鑰回復資訊產生無效的設置。

（二）金鑰回復資訊傳遞功能：

(1) 當金鑰回復資訊與標準的通訊協定一起傳遞時，傳輸的格式要由協定標準決定。

(2) 金鑰回復資訊傳遞功能應儲存金鑰回復資訊，此存放之持續性與可用性應相當於所保管的加密本文。

(3) 金鑰回復資訊傳遞功能應讓金鑰回復申請功能、或金鑰回復代理功能或此兩者可以獲取金鑰回復資訊。

(4) 金鑰回復資訊傳遞功能應讓金鑰回復資訊接收功能可以獲取金鑰回復資訊。

(5) 金鑰回復資訊傳遞功能應讓金鑰回復資訊確認功能可以獲取金鑰回復資訊。

（三）金鑰回復資訊確認功能（KRI Validation Function）：

(1) 金鑰回復資訊確認功能應該可以被啟動或被解除。

（四）金鑰回復申請功能（KRR Function）：

(1) 給定某金鑰回復資訊，金鑰回復申請功能應該可以藉由與一個或多個金鑰回復代理功能互動以回復標的金鑰。

(2) 由金鑰回復申請功能傳輸的加密資料除如圖 3.10 所示之標的金鑰資訊外，應該是可以回復的。

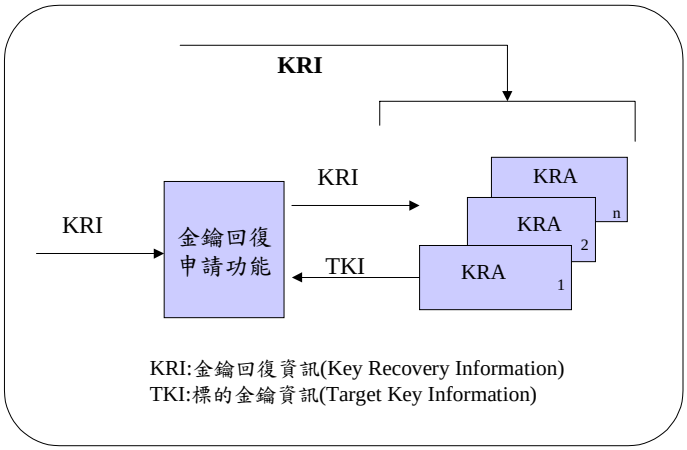


圖 3.10：金鑰回復申請功能框架

（五）金鑰回復代理功能（KRA Function）：

(1) 金鑰回復代理功能應儲存金鑰、金鑰組件（Key Components）或任何其他欲滿足「標的金鑰」回復必要之資訊。

(2) 所有需用來運作金鑰回復代理功能的資料以及所有金鑰回復代理功能使用之密碼模組，必須可以安全的複製，以支援可用性。

(3) 金鑰回復代理功能應有能力處理金鑰回復申請提供的金鑰回復資訊。金鑰回復代理功能的處理應產生用以解密申請者取得的資料，部分或全部之必要資訊。

(4) 金鑰回復代理功能所傳輸的加密資料應是可以回復的。

（六）密碼終端系統（Cryptographic End Systems）：

(1) 廠商委託評估本標準下之產品如果它利用標的金鑰並結合一金鑰回復資訊產生、金鑰回復資訊傳遞或金鑰回復資訊確認功能，對應用資料加密或解密（除金鑰回復之目的外），應聲明此產品為一密碼終端系統。

（七）互通性（Interoperability）：

(1) 密碼終端系統必須可以設定組合，以在跟相容的密碼終端系統通訊時，無論其是否引用金鑰回復，保有互通性。

(2) 利用標準通訊加密協定的「密碼終端系統」廠商，必須提供文件示範其產品傳送金鑰回復資訊與其開發規格一致，並且其協定要由已知之標準團體所採用。

3.3.2、金鑰回復式密碼系統產品安全要求：

以下描述金鑰回復式密碼系統模式中所定的所有功能之安全需求。此安全需求已訂為允許很多不同的產品架構。包括例如（不限於這些例子）：不可載入未評估之軟體或韌體的產品、無其他軟體或韌體可載入的產品及為了某一般性作業系統（像是 UNIX、Windows 2000 等）所建立的產品。

金鑰回復式密碼系統功能的要求定義為促進廣泛地、各種可能的產品架構之評估。如果在產品架構中符合要求可能會減輕某些威脅，產品架構可能會暗示性（Implicitly）地滿足本標準的部分要求。例如，若產品是無其他軟體或韌體可載入的單一商品，則不必適用於領域分離（Domain Separation）、信任路徑（Trusted Path）以及參考確認機制（Reference Validation Mechanism）要求，因為不會有未信

任軟體威脅（Untrusted Software Threat）。這種情形下，此產品是符合標準中這些要求的。

某些要求可以藉由所用的一般用途（General Purpose）系統軟體來滿足，像是作業系統，以及/或者資料庫管理系統。例如，所用的一般用途系統可以滿足識別、鑑別與稽核的要求。

以下要求金鑰回復式密碼系統功能必須實施於，使用並遵循如表 3.10 所示之 FIPS 140-2（註：原為 FIPS 140-1，但自 2001 年 5 月 25 日起，FIPS 140-2 已取代 FIPS 140-1）Level 1、2，或 3 的密碼模組產品之中【45】，表 3.11 是 FIPS 140-1 與 140-2 之差異分析比較：

（一） 金鑰回復資訊產生功能：

1 Level 1 中等安全金鑰回復資訊產生器：

1.1 密碼功能：

所有密碼模組應該符合 FIPS 140-2 Level 1 或更高的標準。

1.2 密碼演算法：

金鑰回復資訊產生功能應能設定組合，（在適用處）只使用 FIPS 核准的演算法。

1.3 機密性：

任何作為部分金鑰回復資訊傳送的標的金鑰，必須經加密保護。用以保護標的金鑰的演算法強度至少必須是加密以及用於資料加密引用的金鑰管理演算法強度，或者是所回復金鑰的產生強度。

1.4 完整性（Integrity）：

(1) 產品應運用資料完整性服務於預定為金鑰回復代理功能的所有對外交易。用於完整性的演算法強度至少必須是加密以及用於資料加密引用的金鑰管理演算法強度，或者是所回復金鑰的產生強度。

(2) 產品所產生的傳送給金鑰回復代理功能的交易，應包含足夠的資訊以明確的連結各回應與相對的申請。

1.5 識別與鑑別（Identification and Authentication）：

(1) 所有密碼模組應實施基於角色的鑑別。

(2) 密碼模組應包含一個密碼管理員角色（Crypto officer role）。

1.6 存取控制（Access Control）：

(1) 金鑰回復資訊產生功能只應允許一位密碼管理員設定此功能。

(2) 最少，設定要包含啟動與解除此功能。

1.7 鑑別收到的交易（與金鑰回復代理有關）：

(1) 產品要確認交易的來源，資料來源鑑別機制的強度至少必須是加密以及用於用戶通訊加密引用的金鑰管理演算法強度，或者是所回復金鑰的產生強度。

(2) 產品要確認所收到的交易的完整性，完整性機制的強度至少必須是加密以及用於用戶通訊加密引用的金鑰管理演算法強度，或者是所回復金鑰的產生強度。

(3) 產品要明確的連結各收到的回應與相對的申請。

2 Level 2 高度安全金鑰回復資訊產生器：

2.1 密碼功能：

所有密碼模組應該符合 FIPS 140-2 Level 2 或更高的標準。

2.2 密碼演算法：同 Level 1。

表 3.10：密碼模組安全等級需求 NIST FIPS 140-2 驗證標準說明

等級 / 領域	安全等級 1	安全等級 2	安全等級 3	安全等級 4
密碼模組規範	密碼模組、密碼邊界規格，已核准演算法，已核准操作模式。密碼模組規格描述包括所有硬體、軟體、韌體(Firmware)等組件。必須陳述模組安全策略(Module Security Policy)。			
密碼模組介面	必須及備選介面。必須要有所有介面與所有輸出/入資料路徑(Data Path)規格。		重要安全參數之資料埠(Data Ports)應該在實體上與其他資料埠分開。	
角色，服務，與鑑別	必須及備選角色與服務應在邏輯上分開。	角色基(Role_Based)操作者鑑別(Authentication)	本體基(Identity_Based)操作者鑑別。	
有限狀態機	有限狀態機模型規格。必須狀態與備選狀態。狀態轉移圖(State Transition Diagram)與狀態轉移規格。			
實體安全	製造等級(Production Grade)設備。單使用者。	上鎖或篡改證據記錄。	篡改偵測與開蓋及開門反應(Response For Covers And Doors)。	篡改偵測與開封反應(Response Envelope)。 實體安全之環境失敗保護/測試
作業環境	可執行碼。已核准完整性技術。	符合 EAL2 評估要求的 DAC(Discreti-Onary Access Control)與稽核之 PP_S。	符合 EAL3 加可信賴的路徑加安全政策塑模評估要求之 PP_S。	符合 EAL4 評估要求加可信賴的路徑之 PP_S。
密碼金鑰管理	金鑰管理機制：隨機數和金鑰生成，金鑰建置、金鑰配送，金鑰進出、金鑰儲存、金鑰歸零(Zeroization)。			
	使用工作手冊(Manual)方法建置秘密(Secret)和私密(Private)金鑰可能以原文(Plaintext)形式進出。		以加密形式使用手冊方法建置秘密和私密金鑰之進出或以分開知識程序(Split Knowledge Procedures)進/出。	
EMI/EMC	47 CFR FCC Part 15,Subpart B, Class A(商業用)。可用之 FCC 需求(剖繪)。		47 CFR FCC Part 15,Subpart B,Class B(家庭用)。	
自我測試	開機測試(Power-up Tests)：密碼演算法測試，軟/韌體完整性(Integrity)測試，關鍵功能測試，條件測試。		依要求執行 RNG/PRNG 統計測試。	開機時執行 RNG/PRNG 統計測試。
設計保證	組態管理(Configuration Management, 簡稱 CM)。安全設置與生成。設計與政策相關。導引文件。	CM 系統。安全配送。功能規範。	高階語言建置。	正規模型(Formal Model)。詳細解釋(非正規證明 Informal Proof)。事前條件與事後條件。
其他攻擊的降低	目前尚未提供降低其他攻擊之測試需求規範			

註：

1. EAL：評估保證等級(Evaluation Assurance Level)。
2. PP：保護剖繪(Protection Profile)。
3. FCC：美國聯邦通訊傳播委員會(Federal Communications Commission)
4. RNG：亂數生成器(Random Number Generator)。
5. PRNG：似亂數生成器(Pseudo Random Number Generator)。

表 3.11：彙整 FIPS 140-1 與 FIPS 140-2 的差異分析比較表

章節	**FIPS 140-1 的內容**	**FIPS 140-2 的內容**
1.	緒論	緒論
2.	定義與縮寫字	定義與縮寫字*
3.	安全功能的需求	安全功能的需求
4.	安全需求	安全需求
4.1	密碼模組	密碼模組規格*
4.2	密碼模組介面	密碼模組埠及介面
4.3	角色與服務	角色、服務與鑑別*
4.4	有限狀態機模型	有限狀態模型
4.5	實體安全	實體安全*
4.6	軟體安全	作業安全*
4.7	作業系統安全	密碼金鑰管理
4.8	密碼金鑰管理	電磁干擾與電磁相容(EMI/EMC)
4.9	密碼演算法	自我測試*
4.10	電磁干擾與電磁相容(EMI/EMC)	設計保證*
4.11	自我測試	減緩其他類型的攻擊*
附錄 A	文件需求總結	文件需求總結
附錄 B	軟體發展實務的建議	軟體發展實務的建議*
附錄 C	精選的參考資料	密碼模組安全政策*
附錄 D		精選的參考資料*

說明：“*”表示此章節內容有新增或重大之修改。

1. Level 1 指明密碼模組的基本安全要求。模組中，除生產級（production-grade）的設備需求外，不需要任何實體安全機制。軟體密碼功能可以用一般的個人電腦來執行。
2. Level 2 藉由(a)要求證明無竄改的外裝、封印或防拆解的鎖(b)要求基於角色（role-based）的鑑別以及(c)與 C2 (EAL2)或同級的作業系統合用時，在多用戶分時系統中，允許軟體密碼方法，來改善 Level 1 密碼模組的實體安全。
3. Level 3 藉由(a) 要求竄改偵測機制(b)要求基底識別（identity-based）之鑑別 (c)對於輸入與輸出關鍵安全參數，指定較強的要求與(d) 與 B1(EAL4)或同級的可信作業系統合用時，有可信的路徑以輸入與輸出關鍵安全參數時，在多用戶分時系統中，允許軟體密碼方法，來改善 Level 1 與 Level 2 密碼模組的安全。

2.3 機密性：同 Level 1。

2.4 完整性（Integrity）：所有 Level 1 的要求以及

當預定為某密碼終端系統產生金鑰回復資訊時，金鑰回復資訊產生功能應產生金鑰回復資訊，此金鑰回復資訊可以讓金鑰回復資訊驗證功能驗證此資訊可成功地用於回復標的金鑰。

2.5 識別與鑑別（Identification and Authentication）：無額外要求。

2.6 存取控制（Access Control）：所有 Level 1 的要求以及

金鑰回復資訊產生功能必須可以在兩個以上的金鑰回復代理間區分標的金鑰資訊。

2.7 鑑別收到的交易（與金鑰回復代理有關）：同 Level 1。

（二）金鑰回復資訊遞送功能：無安全要求。

（三）金鑰回復資訊確認功能：

1 Level 1 中等安全金鑰回復資訊確認功能：Level 1 產品無需評估此功能。

2 Level 2 高等安全金鑰回復資訊確認功能：

2.1 密碼功能：

所有密碼模組應該符合 FIPS 140-2 Level 2 或更高的標準。

2.2 密碼演算法：

金鑰回復資訊確認功能應能設定組合，（在適用處）只使用 FIPS 核准的密碼演算法。

2.3 完整性：

除了下列情形，當金鑰回復資訊確認功能啟動時，金鑰回復資訊驗證功能應符合一個或多個如下之要求：

- 金鑰回復資訊確認功能應確保所收到的金鑰回復資訊確認功能是準確的。也就是，此資訊可以成功地用來執行金鑰回復。
- 在接收的密碼終端系統的金鑰回復資訊產生功能必須為收到的加密資料，產生準確的金鑰回復資訊。
- 如果所收到的金鑰回復資訊不完整時，接收的密碼終端系統不應該可以取得正確的資料解密金鑰。
- 若產品執行上述工作而確認失敗，則此產品可以藉由驗證金鑰回復資訊之完整性以及藉由確認金鑰回復資訊與（加密的）資料，（額外地）滿足驗證。

2.4 存取控制（Access Control）：

金鑰回復資訊確認功能應該只能允許一位密碼官員啟動或解除此功能。

（四）金鑰回復申請功能（KRR Function）：

1 Level 0 低安全性：

1.1 密碼功能：

所有密碼模組應該符合 FIPS 140-2 Level 1 或更高的標準。

1.2 密碼演算法：

金鑰回復申請功能應能設定組合，（在適用處）只使用 FIPS 核准的演算法。

1.3 機密性：

金鑰回復申請功能應保護接收及保管的標的金鑰資訊，避免洩漏於未授權者。

1.4 完整性：

(1) 產品應運用資料來源鑑別於所有申請，用於鑑別的演算法強度至少必須是加密以及用於資料加密引用的金鑰管理演算法強度，或者是所回復金鑰的產生強度。
(2) 產品應運用完整性服務於所有申請，用於完整性的演算法強度至少必須是加密以及用於資料加密引用的金鑰管理演算法強度，或者是所回復金鑰的產生強度。
(3) 對於產生的交易，產品要包含足夠的資訊，以明確的連結各回應與申請。

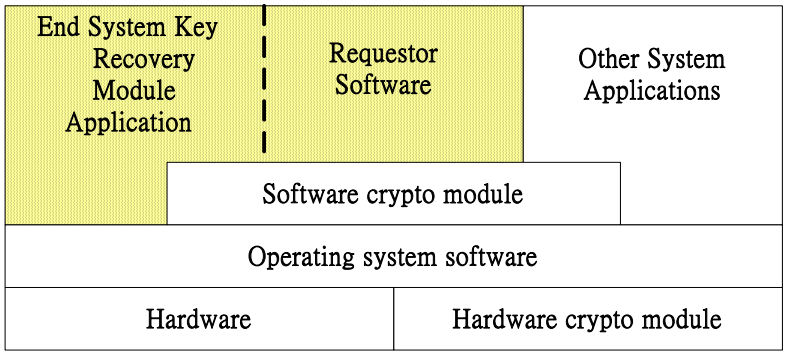
在金鑰回復代理功能要求（Key Recovery Agent Function Requirements）中，本FIPS 標準同樣分別訂定 Level 1 – 中等安全性，以及列出 Level 2 – 高安全性的需求。這些要求列於(1) 密碼功能 (2) 密碼演算法 (3)機密性 (4)完整性 (5) 稽核 (6) 識別與鑑別 (7) 存取控制 (8) 收受交易之鑑別 (9) 不可否認性 (10) 可信任的安全功能保護等小節的要求項目中；詳細的內容不一一列舉，有興趣之讀者可以直接參照其細節說明【44】。在另一方面，國際標準組織（International Organization for Standardization，簡稱 ISO）已根基於 FIPS 140-2 據以制定 ISO/IEC 19790 中【9】，其內容是建置 KRS 時宜注意之規範。

3.3.3、金鑰回復保護剖繪：

根基於 NIST 提出之金鑰回復產品需求與金鑰回復聯盟的實作經驗，想定於對抗有組織之犯罪團體，能適宜保護非機密性（Unclassified）KRS 的框架；於 2000 年 1~2 月間，美國國家安全局（National Security Agency，簡稱 NSA）公佈了分如圖 3.11 及圖 3.12 所示之 KRS 架構以及 KRS 組件示意說明的 3 份保護剖繪（Protection Profiel，簡稱 PP），做為測試、驗證 KRS 之遵循規範【39, 47~50】。

遵循 KRS 之 PP，實作能兼顧個人隱私與依法取用之作業需求的金鑰回復式密碼系統，於應用時，尚需考慮如表 3.12 所示之不同等級之需求。

隨著密碼技術使用之普及，KRS 的建置已是事實【33, 39, 50】，一個安全性不足之 KRS 將是一項高風險的資訊資產，上述 3 份 PP【47~49】宜做為 KRS 實作時遵循之標準。



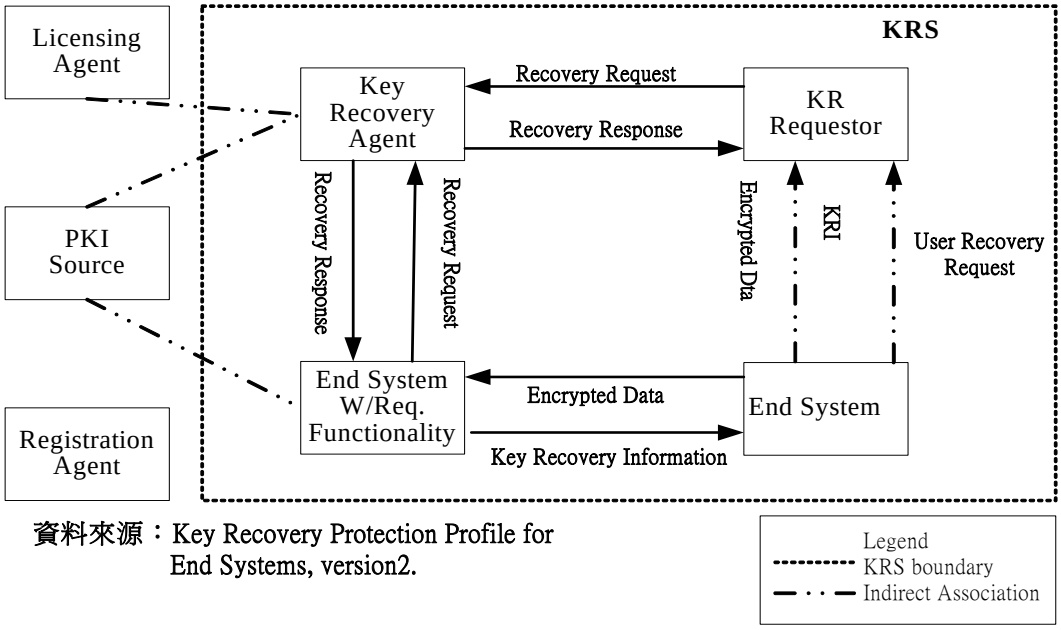
資料來源：NSA(2000)Key Recovery Protection Profile for End Systems,Version 2.

= TOE

=Functional boundary between software and hardware

= Functional boundary within integrated software

圖 3.11：金鑰回復式密碼系統（Key Recovery System，簡稱 KRS）架構示意



資料來源：Key Recovery Protection Profile for End Systems, version2.

圖 3.12：金鑰回復式密碼系統(Key Recovery System，簡稱 KRS)組件示意

表 3.12：金鑰回復式密碼系統不同等級需求

1. 金鑰回復式密碼系統（Key Recovery System，簡稱 KRS）知道所有使用者之秘密金鑰（Secret Key）。 2. 金鑰回復式密碼系統可以偽造一份不合法的使用資料。 3. 金鑰回復式密碼系統無法使用資訊技術偽造一份不合法的使用資料。

3.4、金鑰管理與金鑰回復式密碼系統及其鑑測：

我國在 1999 年 7 月 14 日公布全文 34 條條文之「通訊保障及監察法」13 條規定：「監察通訊以截收、監聽、錄音、錄影、攝影、開拆、檢查、影印或其他類似之必要方法為之。但不得於私人住宅裝置竊聽器、錄影設備或其他監察器材。」如同 1995 年美國法院授權許可「網際網路通訊監察之阿迪他事件」，我國於 2003 年亦首度引用前述之通訊保障及監察法，執行如表 3.13 所示之「共諜嫌犯網路通訊監察蒐證作業」。

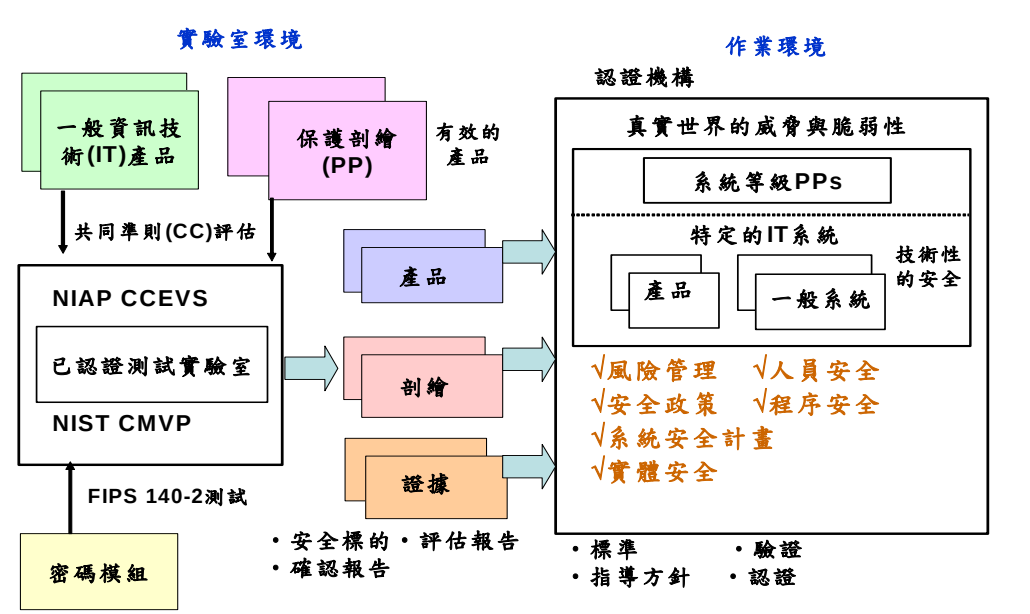
表 3.13：網際網路通訊監察例

1. 資料來源 1.1 2003 年 8 月 6 日，聯合報 A1，記者呂開瑞、宋伯東、牟玉珮／連線報導。 1.2 2003 年 8 月 7 日，聯合報 A2，記者宋伯東／台北報導。 2. 桃園艾君喜科技公司負責人葉裕鎮涉嫌為中共刺蒐我國軍事情報，透過國防部中山科學院技術員陳士良及美籍華人許希哲等人，分別在台、美兩地蒐集我國發展 TMD 戰區飛彈防禦系統機密及台美軍事合作機密。台灣高檢署 2003 年 8 月 5 日指揮調查局基隆海員調查處 6 路同步搜索、拘捕及約談葉裕鎮等 8 人到案。 3. 檢調偵辦葉裕鎮集團涉嫌替中共蒐集台美合作軍機案，首度使用監看嫌犯電子郵件的蒐證技術。檢調派出多名電腦專家，克服過去無法攔截嫌犯寄送電子郵件給共犯之蒐證障礙，成功截到葉裕鎮寄出的電子郵件，掌握葉裕鎮等人不法取得軍事機密之具體事證。

網際網路上的通訊，經常使用密碼學技術，本文介紹之「金鑰回復式密碼系統（KRS）」與按鍵側錄系統（KLS）機制，是美、英等國執行「通訊保障及監察法」第 13 條中「開拆」電子信封之必要方法之一。隨著資訊技術的一日千里，「運籌於虛擬實境之外，決勝在網頁方寸之中」的數位犯罪日益嚴重；KRS 已成為在應尊重個人隱私，維護人性尊嚴的前題下，追求國家安全與社會安定之議題。

國際標準組織（International Organization for Standardization，簡稱 ISO）公佈之金融界的金鑰管理標準，如圖 3.6 所示之金鑰管理生命週期中，由於金鑰管理系統必須在整個生命週期中提供適當的保護，過期金鑰因法律效期等因素，仍應建檔，並安全存放【13, 62, 98】。此時，由於使用者非常容易遺忘金鑰，一個能適當保護個人隱私之金鑰回復式密碼系統與數位社會加密檔案鑑偵工具的按鍵側錄系統將能在數位社會中為人類創造安全性。

金鑰回復式密碼系統如圖 2.1 所示，是美國數位空間資訊安全中金鑰管理基礎建設之礎石，為保證其安全性，遵循美國聯邦資訊安全管理法案的要求，NIST 已提出如圖 3.13 之安全鑑測作業並施行中【43, 58, 94】。



資料來源：Katzke, S., Protecting Federal Information Systems and Networks, In Presentation of the 4th International Common Criteria Conference, Sept. 7~9, 2003, Stockholm, Sweden.

圖 3.13：資訊系統安全保證之全面性鑑測方法----結合關鍵評鑑行動

四、密碼技術及其應用之鑑測初探：

4.1、前言：

隨著資訊科技的一日千里，電腦與網路之結合已在 20 世紀末期，發生令人眩目之光芒，數位生活已成為全球性的發展趨勢。政府做為國家組成及資訊流之中心節點，在社會資訊化之進程中位居樞紐而又無可替代的作用。一般而言，電子化政府(Electronic Government)之建設，包括：

(1). 政府機關成員上網獲取機構內部與外部之工作所需要的資訊。
(2). 政府機關資訊上網，供社會大眾瞭解與使用。
(3). 政府機關事務，機關內、機關間、機關與公眾等事務經由網路處理。

由於「電子化政府」涉及機密性與敏感性(簡稱機敏性)資料之處理，其資訊系統如何確保機敏性資料不受未經授權之存取、使用、揭露、破解、修改與毀壞，以提供機密性、完整性和可用性的電子化政府相關資訊系統之應用，已是宜正視的問題。

今日有關資訊安全可信賴性的策略，都是在不完整的資訊內容下做決定的，標準可以減輕因不完整資訊所引發的困難，因為標準可以減少選擇的範圍而簡化可信賴性供給與需求決策制定的過程。標準的發展與改革會仔細研討以減少現有設計的缺點並且因而提昇可信賴性。同時，標準的存在會提昇關於一個評估脆弱性存在與否的基礎。

自關稅暨貿易總協定(General Agreement on Tariff and Trade，簡稱 GATT)體系之技術性貿易障礙協定(Agreement on Technical Barrier to Trade，簡稱 TBT)中要求各國為安全、衛生、環保或保護消費者等因素，而訂定之技術法規或標準，以及證明相關產品符合這些技術法規或標準之符合性評鑑程序(Conformity Assessment Procedure，簡稱 CAP)，不應對國際貿易造成沒有必要的障礙後，鑑於沒有真確性(Integrity)等安全可靠性質的資訊，電子商務與電子化／網路化政府等均將遙不可及，虛擬世界仍將跳不出文娛和廣告的格局；1999 年 12 月 1 日，自 1990 年開始制定之全球資訊技術安全評估共同準則(Common Criteria for Information Technology Security Evaluation，簡稱 CC) CC 2.1 版正式成為 ISO/IEC 15408 號標準【34】，圖 4.1 是其發展簡史。換言之，在電子化／網路化的社會中，資訊技術的產品、系統及服務之安全測試標準將有調和一致的國際規範，開放源碼(Open Source Code，簡稱 OSS)之產品亦宜通過共同準則的驗證提供安全性保證。根基於此，在本節中我們簡述共同準則與應用密碼技術在角色基存取控制之架構。

4.2、共同準則簡介【34】：

CC 是結合 TCSEC、ITSEC 與 CTCPEC 的優點，做為經由保護剖繪(Protection Profile，簡稱 PP)與安全標的(Security Target，簡稱 ST)讓資訊系統發展者與評估者遵循一致規範之描述資訊產品或系統安全性的共通結構與語言。在 CC 中，PP 包含許多和實作上無關的安全需求，可為資訊技術安全需求的詞典；ST 則是進行資訊安全評估主體之評估標的(Target of Evaluation，簡稱 TOE)所需的許多安全需求與規格所形成的集合，是評估資訊產品或系統的基石。在 CC 中，功能組件(Component)是表示 PP 與 ST 中的各種安全需求；CC 同時包含評估其未列出之功能組件的安全評估保證需求的規範，在使用 CC 未列出之功能組件時，事先須經評估機關核准。為落實 CC 之認證、驗證與檢測機制，自 1997 年 10 月 7 日起，美國就公告了其相關工作計畫，並於

1999 年 5 月 14 日起正式實施，其使用示意請參見表 4.1，表 4.2 是其保證評核等級檢測項目示意說明。

表 4.2 中定義之七級評估保證等級(Evaluation Assurance Level，簡稱 EAL)之七級，其內含簡述如后：

(1).EAL1：功能測試，適用於要求正確操作而安全威脅認為並不嚴重的情況，它對要求獨立安全保障來支持應有的內容保護是很有價值的，適用於個人(家庭)資訊使用環境的保護。

(2).EAL2：結構測試，在交付設計文件和測試結果時，EAL2 需要研發者的合作，但不應超越與良好商業運作的一致性而要求研發方付出更多的努力。這樣，就不需要增加過多的費用或時間的投入。EAL2 適用於在缺乏現成可用的研發記錄時，需要一種低或中等級別的獨立保證的安全性。在保護傳統系統的安全或者限制對研發者的訪問時，會有這樣的情況。

(3).EAL3：系統地測試和檢查，可使一個盡責的研發者，在設計階段能從有效的安全工程中獲得最大限度的保證，而不需要對現有的合理的研發實踐作大規模的改變。EAL3 適用於需要一個中等級別的獨立保證的安全性之使用環境。

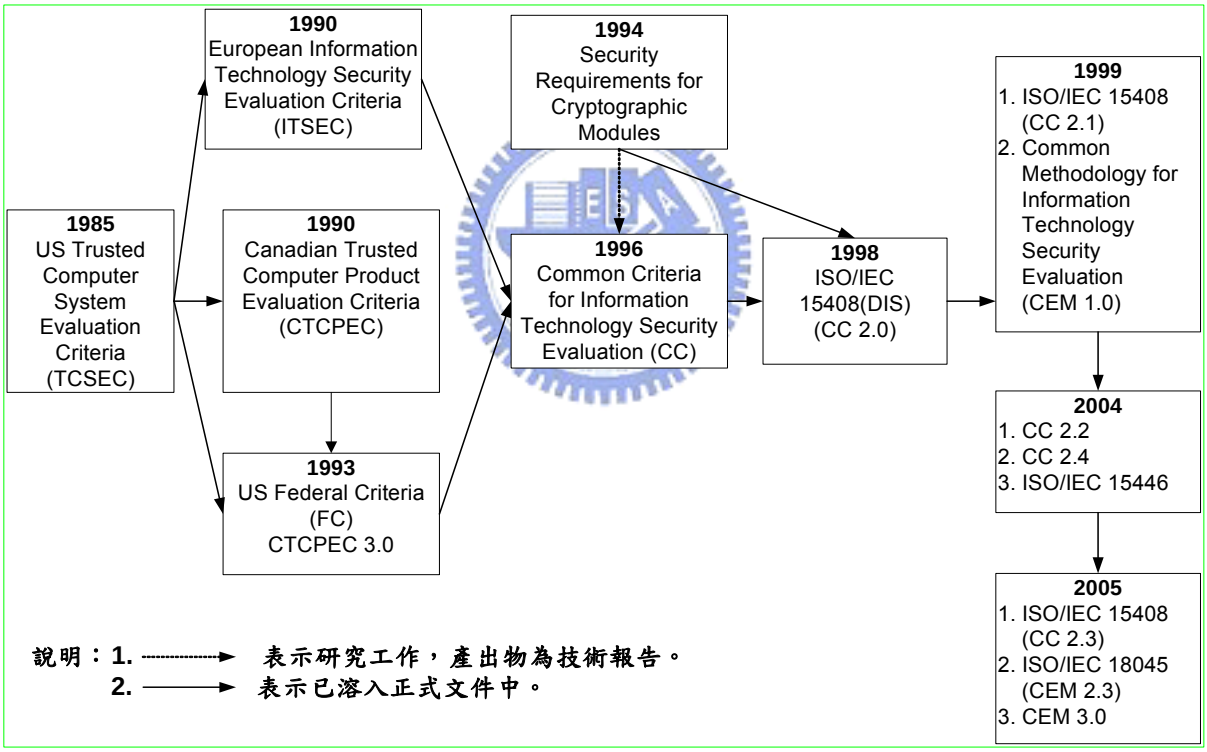


圖 4.1：可信賴通資訊系統安全評估準則簡史

表 4. 1：資訊技術安全評估共同準則使用示意

共同準則典範(Paradigm)	系統取得典範(註：ISO/IEC 15408 亦即 CC)
保護剖繪(Protection Profile)	徵求建議書文件(Request for Proposals)
安全標的(Security Target)	建議書(Proposals)
評估標的(Target of Evaluation)	交付(Delivered)系統
系統評估結果	系統驗收與否依據

說明：共同準則－資訊技術安全評估共同準則(Common Criteria for Information Technology Security Evaluation，簡稱 CC)。

表 4.2：資訊技術安全評估保證等級摘要

保證類別 (Class)	保證屬別 (Family)	保證組件(Component)						
		評估保證等級						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
組態管理	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
交付和運行	ADO_DEL		1	1	2	2	3	3
	ADO_IGS	1	1	1	1	1	1	1
開發	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
指導性文檔	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
生命週期支援	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
測試	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
脆弱性評鑑	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

說明：ACM、AUT 等之定義請參考 ISO/IEC 15408 號標準。

(4).EAL4：系統地設計、測試和複查，可使研發者從有效的安全工程中獲得最大限度的保證，這種安全工程基於良好的商業研發實踐，這種實踐雖然很嚴格但並不需要大量專業知識、技巧和其他資源。在經濟合理的條件下，對一個已經存在的生產線進行翻新時，EAL4 是所能達到的最高等級。EAL4 適用於對常規產品需要一個中等到高等級別的獨立保證的安全性之使用環境，還適用於研發者或用戶準備負擔額外的安全專用工程費用的情況。

(5).EAL5：半正規化設計和測試，可使一個研發者從系統安全工程中獲得最大限度的保證，這種安全工程基於嚴格的商業研發實踐，是靠適度應用專業安全工程技術來支持的。EAL5 適用於在有規劃的研發中需要高級別的獨立保證的安全性之使用環境，此時還需要有嚴格的研發方法。

(6).EAL6：半正規化查證的設計和測試，可使研發者通過把安全工程技術應用於嚴格的研發環境，而獲得高度的保證，以便保護高價值的資訊資產，對抗重大風險，EAL6 適用於高風險之使用環境。

(7).EAL7：正規化查證的設計和測試，適用於在風險非常高的地方和/或有高價值資訊資產進而值得更高級之研究的地方。EAL7 的實際上只局限於那些非常關注能經受廣泛的正規化分析並修正安全功能的產品。

評估保證等級即是資訊技術安全驗證(Certification)機制中如圖 4.2 所示之符合性申明，至於圖 4.2 中之資訊安全目標等之關聯，請參見圖 4.3。在圖 4.2 中，我們可以清楚的瞭解保護剖繪的重要性。一般而言，機敏性檔案存取控制之保護剖繪之評估保證等級宜高於或等於 EAL4【15】。

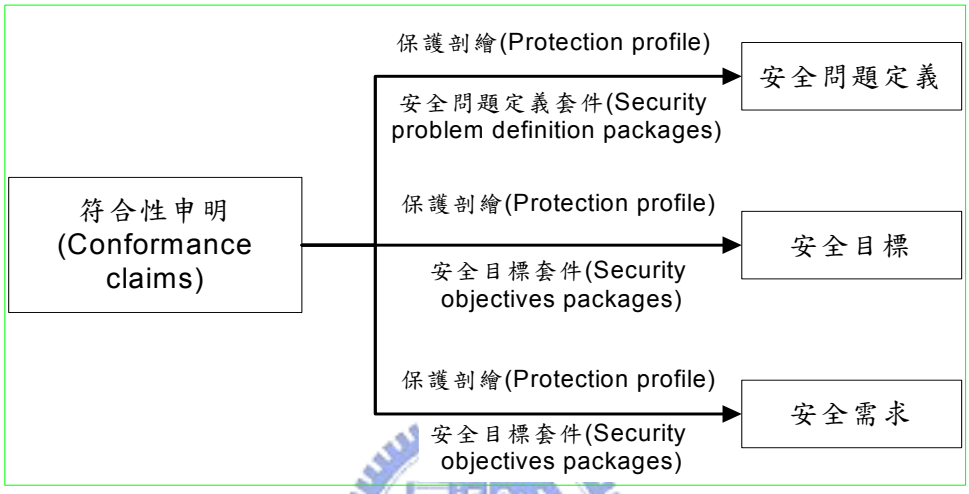


圖 4.2：符合性申明示意說明

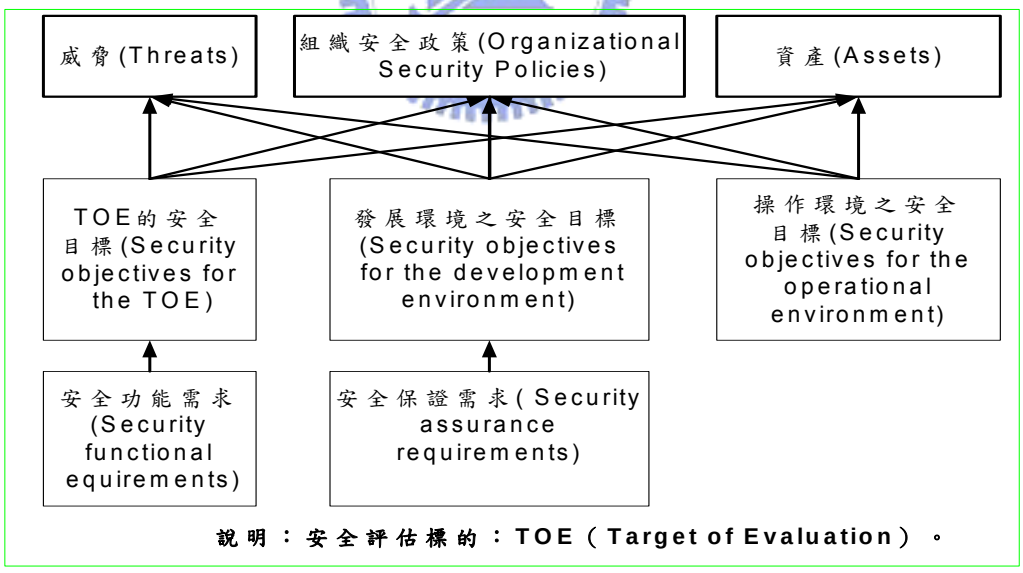


圖 4.3：資訊安全目標及需求關係示意

共同準則之標的在進行資訊技術的安全評估，以提供信賴基礎之保障。共同準則要求加大以往資訊技術安全評估的廣度、深度與強度，來測試資訊技術產品或系統安全之有效性。保護剖繪(PP)及其安全標的(ST)提供使用者一個參考特定安全需求集合的方法；如圖 4.3 與圖 4.4 所示，PP 及其 ST 律定之安全規格，期能讓使用者對這些要求進行驗證工作時，更容易進行評估工作，表 4.3 是已確認之 EAL4 作業系統舉隅。

以 Linux 為例，SuSE Linux 已於 2004 年 1 月 14 日獲得共同準則受控存取保剖繪(Controlled Access Protection Profile，簡稱 CAPP)EAL3 之驗證合格證書【46】，SuSE Linux 之評估標的(Target of Evaluation，簡稱 TOE)分為 TOE 安全功能(TOE Security Function，簡稱 TSF)與非 TOE 安全功能(non TSF)兩類，如圖 4.5 及圖 4.6 所示【14】。

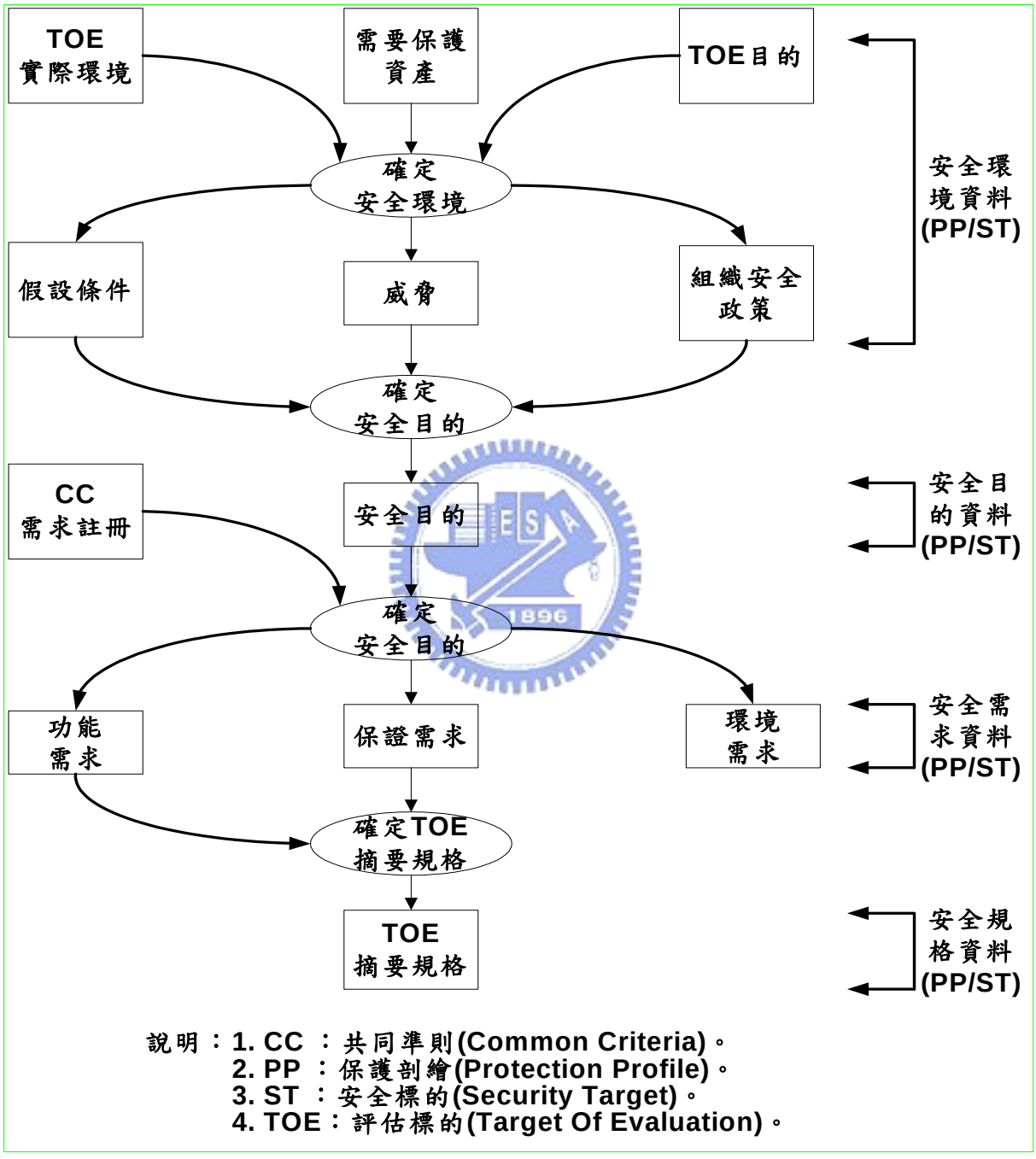


圖 4.4：共同準則之需求和規格推導

表 4. 3：共同準則已確認(Validated)之 EAL4 作業系統舉隅

產品名稱	符合性宣告	確認日期	共同準則發證國家
AIX 5L for Power V5.2, Program Number 5765-E62	EAL4	2004 年 4 月	德國
Hewlettt-Packard HP-UX(lli) Version 11.11	EAL4	2001 年 9 月	英國
Solaris 8 2/02	EAL4	2003 年 4 月	英國
SUN Solaris Version 8 with Admin Suite v3.0.1	EAL4	2000 年 11 月	英國
SUN Trusted Solaris, v8 4/01 Maintenance release Dec. 2003	EAL4	2002 年 6 月	英國
Windows 2000 Professional Server and Advanced Server with SP3 and Q326886	EAL4 Augmented ALC_FLR.3	2002 年 10 月	美國
Windows XP Professional, Windows Server 2003 (Standard, Enterprise and Data Center Edition)	EAL4+: ALC_FLR.3	2005 年 11 月	美國
XTS-400/STOP 6.0E	EAL4 Augmented ALC_FLR.3	2004 年 3 月	美國
說明：1. EAL：Evaluation Assurance Level。 2. ALC_FLR.3：Assurance Life cycle support-Systematic Flaw Remediation。			

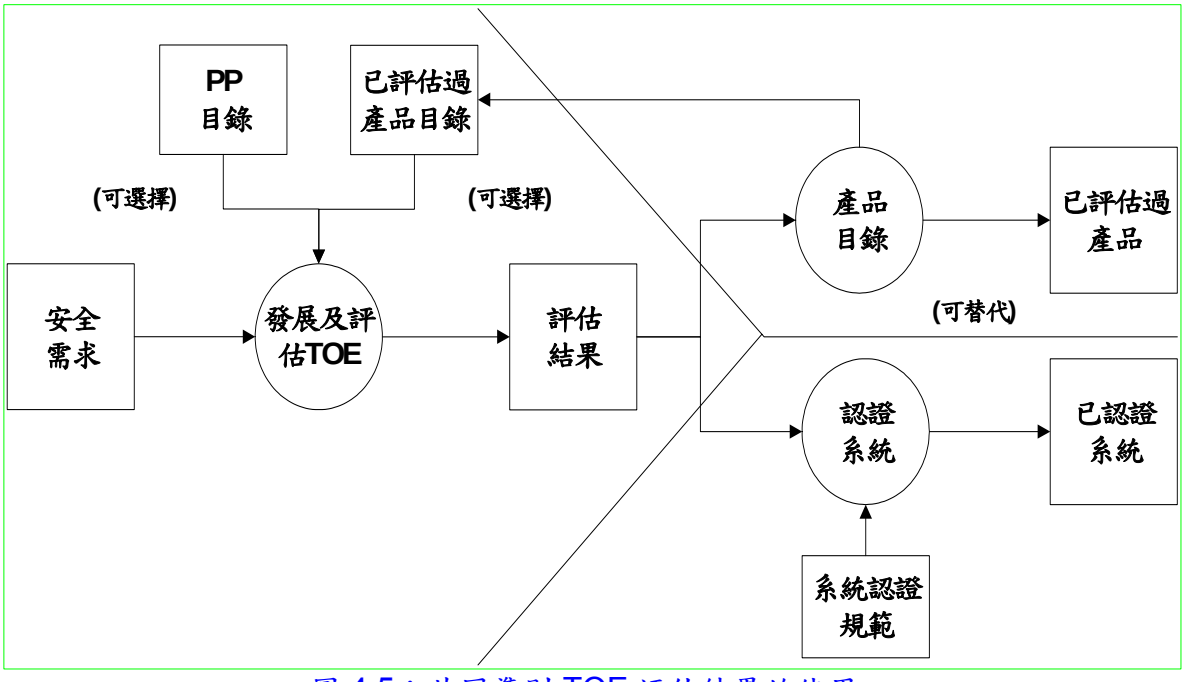


圖 4.5：共同準則 TOE 評估結果的使用

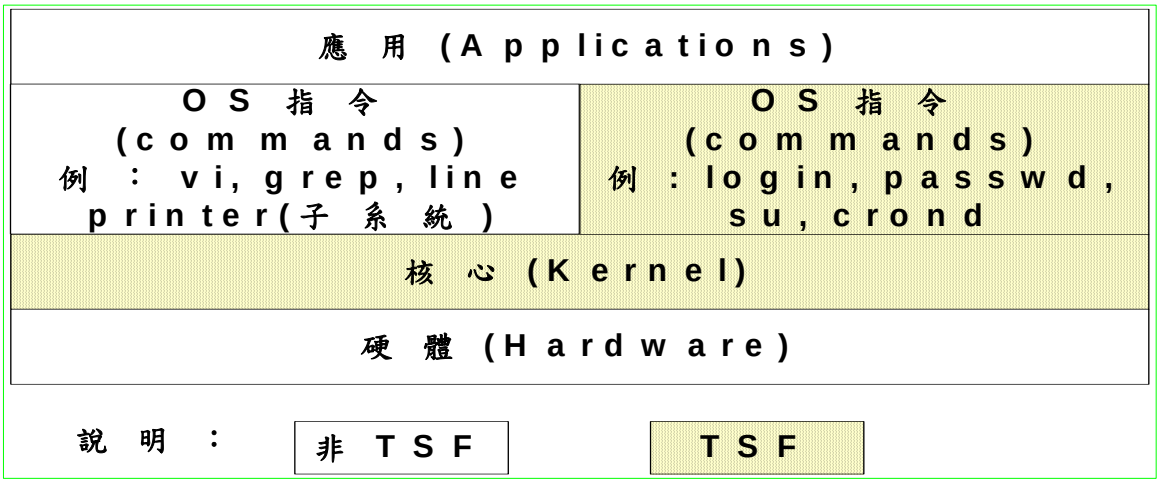


圖 4.6：SuSE Linux TSF 與非 TSF 軟體示意

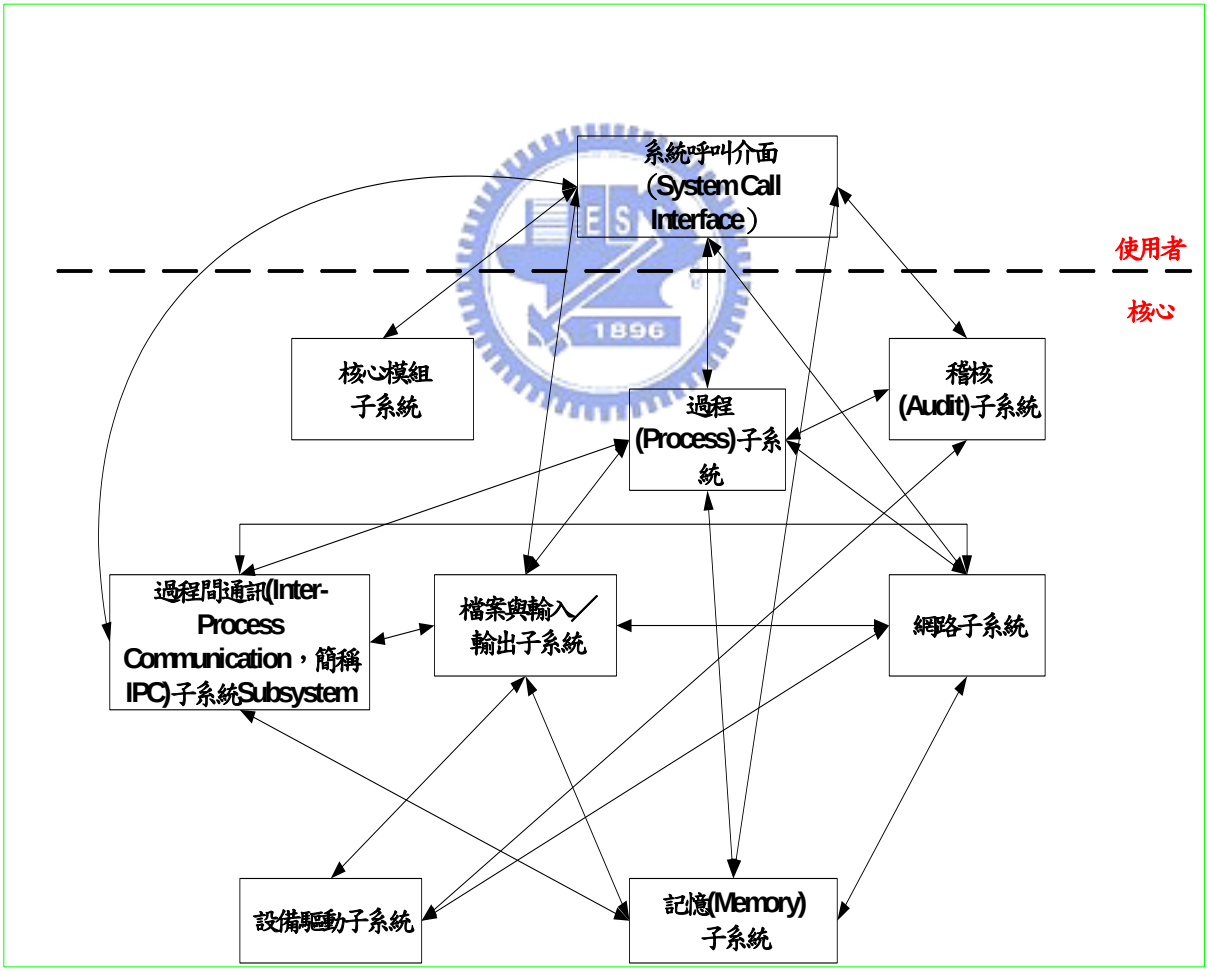


圖 4.7：SuSE Linux 核心子系統及其交互工作示意

4.3、Linux 與角色基存取控制：

一般而言，Linux 核心之安全根基於過程與能力(Process and Capability)、檔案系統與封包控制之安全性，其中檔案系統及封包控制和一般常見之方法類似，過程與能力方面，簡述於后【78】：

Linux 中的使用者行為都是藉由過程(Process)來完成，一個過程通常具有以下幾個屬性：

(1).RUID，RGID：真正用來執行過程的 UID 及 GID。
(2).EUID，EGUID：用來做權限檢查。
(3).SUID，SGID：用來做權限轉換。
(4).umask：存取控制的設定。
(5).limits：資源使用的限制。
(6).FSUID，FSGID：用來做檔案系統存取權限的檢查，通常都會等於 EUID、EGID。
(7).capabilities：POSIX capability 資訊。

基於安全的考量，Linux 給予一般使用者盡可能低的權限，而把全部的系統權限賦予一個單一的帳戶－root。Root 用來管理系統、安裝軟體、管理帳戶、執行某些服務等。但一般使用者很多的執行動作也需要 root 權限，此時可透過 setuid 來達到目的。但這種依賴單一帳戶執行權限的運作方式，卻增加了系統面臨的安全威脅。因為某些程式需要 root 權限可能只是為一個很簡單的執行目的而已，例如：bind 到特定 port、打開一個只有 root 權限可以開啟的檔案等。但這些程式可能存在安全漏洞，若該程式不是以 root 的權限執行時，其存在的漏洞對系統造成的安全威脅就會降低。

Linux 從 2.1 版開始，核心開發人員在 Linux 核心中加入了能力(Capability)的概念，其目的就是降低過程在執行某些動作時對 root 帳戶的依賴。從 2.2 版本的核心開始後，就可以用一些能力的基本功能。傳統 UNIX 的信任模型非常簡單，就是「root 對一般使用者」模型。在這種模型中，一個過程不是什麼都能做，就是幾乎什麼也不能做，這取決於過程的 UID。很顯然這樣對系統安全存在很大的威脅，UNIX 系統中常見之的 SUID 的安全問題就是由這種信任狀模型造成的。

過程與能力之設定可以降低類似 SUID 等的安全風險，系統管理員為了系統的安全可以刪減 root 的能力，這樣即使是 root 也無法進行某些執行動作。而這個過程又是不可逆的，也就是說如果一種能力被刪除，除非重新啟動系統，否則即使 root 也無法重新加入被刪除的能力。

能力是一種規範，它定義了能夠對某個目標進行之所有操作行為，以及允許在這個目標上進行的操作行為。能力的操作動作包括：複製某個能力、程序間某個能力之遷移、修改某個能力以及取消某個能力等。目前為止，各種作業系統對能力(Capability)的應用程度並不相同。

舉例來說，File Descriptor 就是一種能力，當使用者利用開啟(Open)這個系統呼叫(System call)來獲得檔案的讀或寫權限，如果 Open 執行成功，系統的核心就會建立一個 File Descriptor。如果收到讀或寫的請求，核心就使用這個 File Descriptor 作為一個資料結構的索引，檢查相關的操作是否已被允許。

基於單一 root 之脆弱性的風險；因此，訂定資訊安全政策時，通常會建議管理者使用 Linux 核心定義的這些能力，依系統需求分割 root 的權限，避免因系統中 root 的權限過大所造成的安全風險【42】，表 4.4 是 Linux 中之能力表列【42, 77~78】。

表 4. 4：Linux 之能力表列

能力名稱(Capability Name)	代號	說明
CAP_CHOWN	0	允許改變檔案的所有權
CAP_DAC_OVERRIDE	1	忽略所有 DAC 的存取
CAP_DAC_READ_SEARCH	2	忽略所有對讀、搜索操作的限制
CAP_FOWNER	3	如果檔案屬於過程的 UID，就取消對檔案的限制
CAP_FSETID	4	允許設置 setuid
CAP_FS_MASK	0x1f	用來決定 fall back 到 suers()或 fsuers
CAP_KIL	5	忽略過程間傳送 signal 時檢查 uid 的限制
CAP_SETGID	6	允許改變群組 ID
CAP_SETUID	7	允許改變使用者 ID
CAP_SETPCAP	8	允許向其它過程轉移能力及刪除能力
CAP_LINUX_IMMUTABLE	9	允許修改檔案的 IMMUTABLE 和 APPEND-ONLY 屬性
CAP_NET_BIND_SERVICE	10	允許應用程式 bind 小於 1024 的 port
CAP_NET_BROADCAST	11	允許網路 Broadcast 和 Multicast
CAP_NET_ADMIN	12	允許執行網路管理任務：socket、防火牆等
CAP_NET_RAW	13	允許使用 raw socket
CAP_IPC_LOCK	14	允許鎖定 IPC
CAP_IPC_OWNER	15	忽略 IPC 所有權檢查
CAP_SYS_MODULE	16	插入和刪除核心模組
CAP_SYS_RAWIO	17	允許對 ioperm/iopl 的存取
CAP_SYS_CHROOT	18	允許使用 chroot() system call
CAP_SYS_PTRACE	19	允許 trace 任何程序
CAP_SYS_PACCT	20	允許設定過程 accounting
CAP_SYS_ADMIN	21	允許執行系統管理任務，如：檔案系統控制、quota、設定網域名稱等
CAP_SYS_BOOT	22	允許重新啟動系統
CAP_SYS_NICE	23	允許提升 nice 值
CAP_SYS_RESOURCE	24	忽略資源限制
CAP_SYS_TIME	25	允許改變系統時間
CAP_SYS_TTY_CONFIG	26	允許設定 TTY Device
CAP_SYS_MEM DUMP	27	允許傾印任何記體體區塊
CAP_SYS_EERPOM	28	允許存取 EEPROM
CAP_SYS_PSDUMP	29	允許列出所有執行過程
CAP_SYS_SIGTRIP	30	允許執行 trace trap
CAP_MKNOD	31	允許使用 mknod() system call
CAP_LEASE	32	Allow taking of leases on files

現有之 Linux 作業系統以傳統 Bell-LaPadula【42, 77~78】安全機制為主流，其對資料的完整性等安全需求有所不足的，因此美國國家安全局(National Security Agency，簡稱 NSA)在 2001 年的 Linux 核心高峰會上，以 Linux 為架構，提出研究發展近 10 年之安全增強 Linux 機制：SE Linux【27】，使用較具有彈性的 flask【77】

框架，將 Linux 安全等級提升至 EAL4，同時具有資料標記及強制的存取控制【51】，號稱是最安全的 Linux 作業系統。SE Linux 可以被用來規範最小特權，保護過程與資料的完整性、機密性及可歸責性宜有之職責區隔機制等。

SE Linux 系統之安全體系結構如圖 4.8 所示，封裝於安全服務中之政策(Policy)與具體執行實施(Enforcement)的對象管理器兩部分組成；首先以政策語言(Policy Language)提供系統管理者來制定安全政策(Security Policy)，並由核心層存取控制檢查。SE Linux 同時提供了範例政策(Example Policy)，並允許使用者利用型態強化(Type Enforce，簡稱 TE)與角色基存控制(Role-Based Access Control，簡稱 RBAC)及可選之多級別安全性(Optional Multilevel Security)方式來客製化系統。

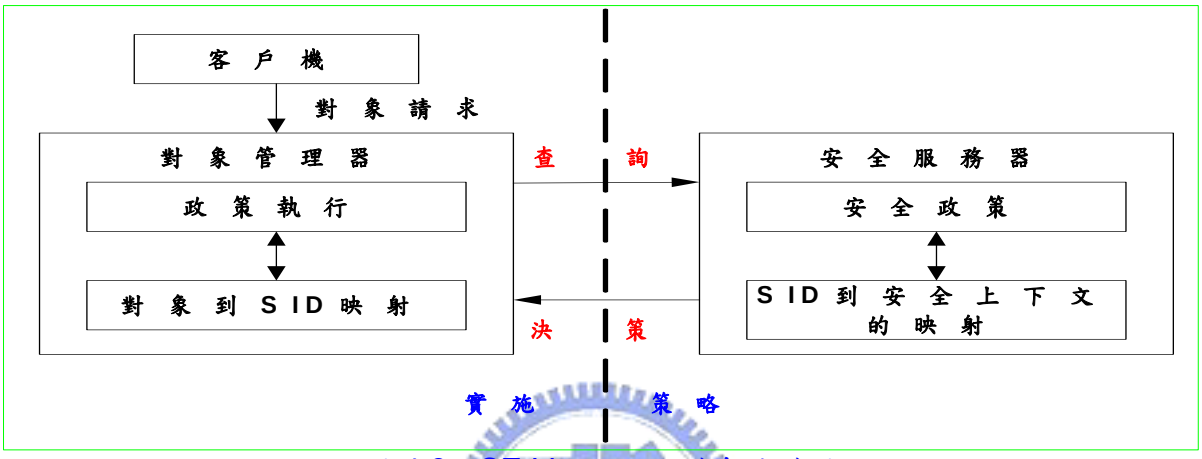


圖 4.8：SE Linux 安全體系結構圖

SE Linux 系統中關於安全的請求和決策有三種情況【27, 51, 77】：

(1).標示決策(Labeling Decision)：確定一個新的主體或受體採用什麼安全標示(如創建受體時)；

(2).存取決策(Access Decision)：確定主體是否能存取受體的某種服務(如文件讀寫)；

(3).多模態決策(Polyinstantiation Decision)：確定一個過程在訪問某個 polyinstantiation 受體時，可不可以轉為另一個過程(如從 login_t 轉到 netscape_t)。

SE Linux 設計精神主要由根據特定目的定義類別(Domain Type)，限制其存取物件類別之 TE 與如圖 4.9 所示 RBAC 以及可選的多級別安全性(Optional Multilevel Security)混合制定而成。

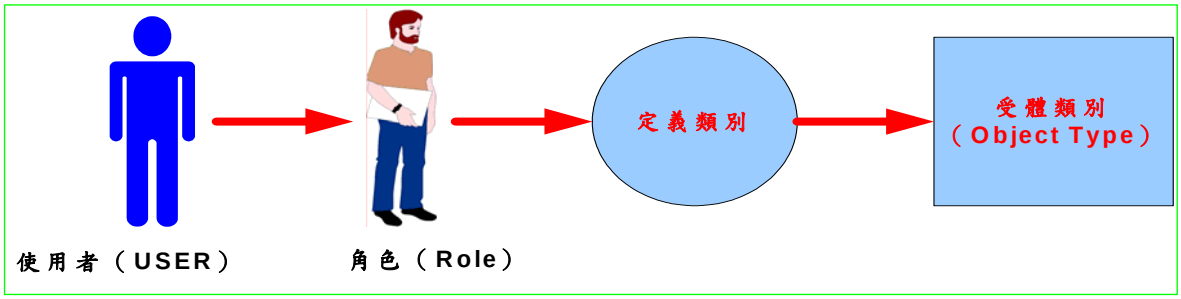


圖 4.9：SE Linux 為以角色為基底的存取控制

SE Linux 複雜的安全政策固然提供管理者很大的安全制訂彈性，但因 SE Linux 語法複雜且龐大，例如由 SE Linux 所提供的政策範例(Example Policy)中，至少包含 3 個角色，29 個 object class，22 個 attribute，115 個 permission，253 個 type，及上萬行的語法，因此在使用 SE Linux 時所面臨設定及管理安全政策上的複雜及困難，也衍生出許多相關研究，例如所設定的規則是否符合使用者所要求的目標等；如欲善用 SE Linux，宜先了解 RBAC。

4.3.1、RBAC 簡介：

組織中，每位工作人員所擁有的職權與職責是基於其所擔任的角色而定，而非工作人員本身。在過去我們採用「隨意性存取控制」(Discretional Access Control，簡稱 DAC)與「強制性的存取控制」(Mandatory Access Control，簡稱 MAC)做存取控制的控管，然而這兩種存取控制控管模式隨著組織結構的日益複雜化和安全需求的提高已不足以適用。因此，多位學者提出了"以角色為基礎"的想法，透過角色本身所擁有的職權與責任、職位與工作等角色之間的互動關係與組織管理政策的結合，提出了「以角色為基礎的存取控制管制」(Role- Based Access Control，簡稱 RBAC)的參考模式【59】。

角色本身代表了職權與責任等的組合，例如組織定義了「人事部經理」這個角色，規範出它應負的責任，即公司人事及薪資的管理，同時也授與它相對的權力，如人事任用決定權。在更完整的職務模式(Role Model)中包含了角色之間的關聯性，以及其限制條件【11】。在 1996 年提出並形成共識之 RBAC96 模式【59】依照應用的層面分為 $RBAC_0$、$RBAC_1$、$RBAC_2$、和 $RBAC_3$，其關聯性如圖 4.10 所示。

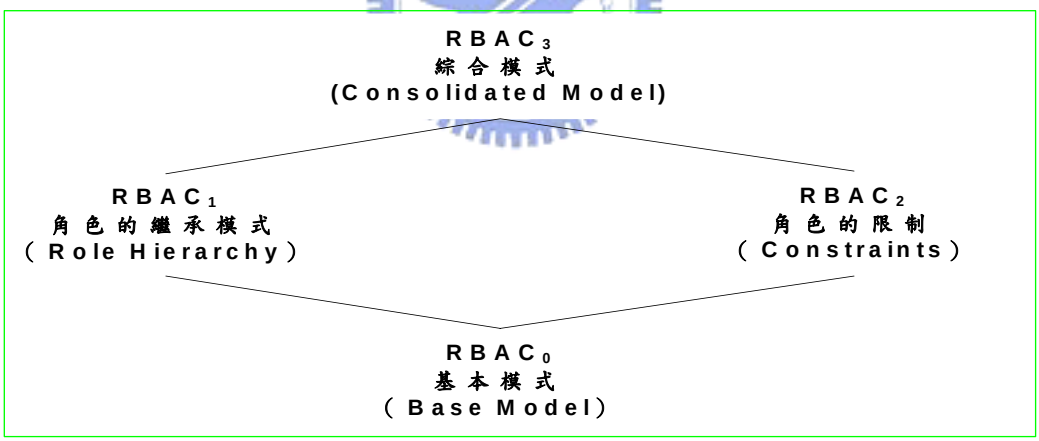


圖 4.10：以角色為基礎的存取控制模式

RBAC 中之基本模式定義了使用者(User)、角色(Role)及權限(Permission)三者之間的關聯。在角色的繼承模式中包含了基本模式，另外加入角色繼承的觀念，在角色的限制方面，RBAC96 認為在此可加入組織內部的控制方法，如權責區分、情境限制等，以符合大部份組織長久以來所規範的管理原則。在綜合模式中，將以上三者做整合，提供完整的角色存取控制方案。

在 $RBAC_0$ 中定義了三個主要的個體(Entity)，分別為使用者(User)、角色(Role)、以及權限(Permission)三者。另外也納入連線(Session)的觀念，其關係如圖 4.11 所示：

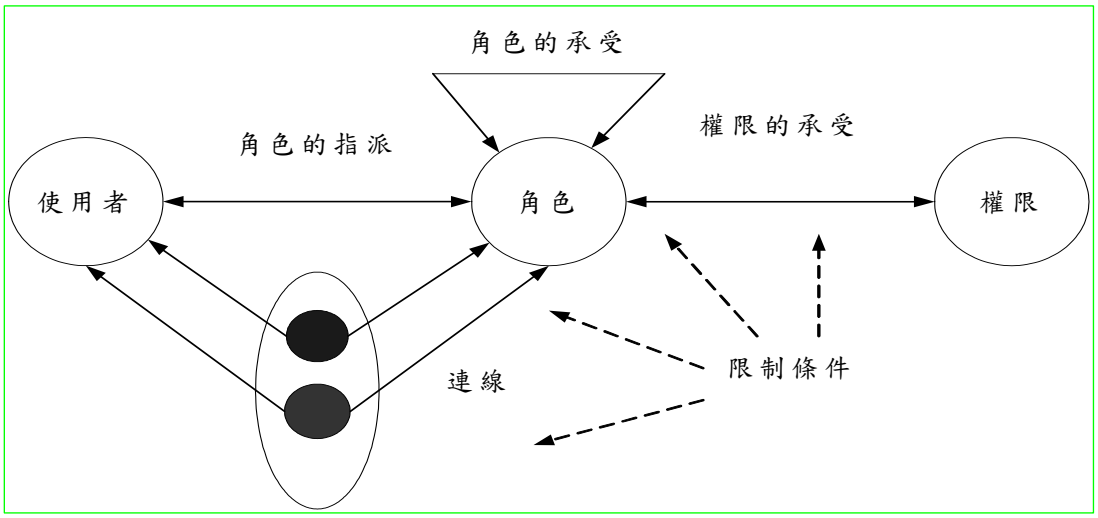


圖 4.11：以角色為基礎的存取控制管制基礎架構

使用者可透過角色的指派取得其所擔任的職位應有的職權與責任，例如吳茲仁先生為採購部主管，那麼他便可以經由角色的指派取得採購部主管的權力。而每一個角色可以執行的作業程序則在權限的指派來做設定；例如採購部主管的權限為核准採購單，因此我們便可以將“核准採購單”這個作業程序指定給“採購部主管”這樣的角色。另外連線(Session)也是一種使用者與角色之間的關聯性，不同的是它是在動態執行時所產生，代表了使用者目前在執行中的角色集合。

在 $RBAC_1$ 中除了 $RBAC_0$ 對角色的基本定義外，納入了組織內角色承受的概念；也就是在組織中職位高的員工可以繼承職位低的員工的工作。舉例來說，在電腦軟體部門裡，主管除了可以執行相關的管理工作外，也可以做程式撰寫的工作(此為程式設計師的工作內容)，如圖 4.12 所示。

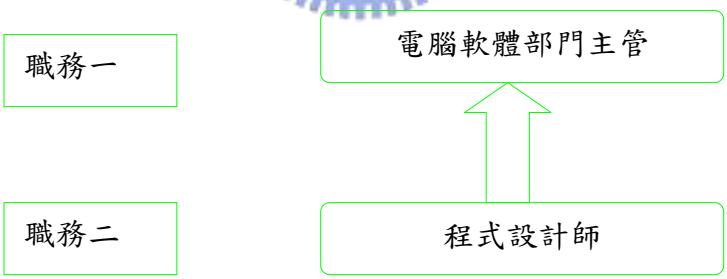


圖 4.12：RBAC 中角色之繼承概念

在 $RBAC_2$ 中納入了許多角色實行時的限制條件，這些限制條件在組織的運作上組成了重要的控制點，用以實現傳統企業的內部控制原則。其中包括權責區分(Seperation of Duties)、組織取得的必備條件限制(Prerequisite Condition)、指派組織的數量限制(Cardinality Constraint)、被啟動的組織限制(Session Limited)等。

在 RBAC 理論中，由於考慮到組織的實際需求，因此相較於傳統的存取控制理論(如 DAC 或 MAC)，具有以下的優點【1, 11, 59】：

(1).對於屬於同一個角色的數個員工，其工作權限只需定義一次。

(2).當員工轉換個職位時(如升遷或離職)，角色的工作權限不需要更動，只需將此員工指派至新角色即可。

(3).許多內部控制的原則，如權責區分及角色代理，皆可在角色本身或角色與角色間加入限制條件(Constraint)來達成；在另一方面，角色基存取控制還可以與身分鑑別機制整合，提昇資訊系統整體之安全性與可用性，目前已成為 Web Service 之工業標準【1】。

4.3.2、以角色為基礎的存取控制標準簡析：

Ferraiolo, D. F.、R. Sandhu、S. Gavrila 三位學者，在 2001 年發表了"A Proposed Standard for Role-Based Access Control"【11】一文，整理出過去學術界以及美國國家標準與技術研究院(National Institute of Standards and Technology，簡稱 NIST)在 RBAC 領域的研究成果，根基於 RBAC96【59】提出美國聯邦政府使用之標準建議的 RBAC 之定義與理論模型，將 RBAC 模型分成幾個部分，包括核心 RBAC、階層式 RBAC、限制式 RBAC；限制式 RBAC 又可以分為靜態權責區分(Static Separation_of_Duty Relations)與動態權責區分(Dynamic Separation_of_Duty Relations)兩種方式；其區別在於在存取控制的過程中，為了避免發生濫用職權的情形，而加諸之不同的管制與限制方法；分述於后：

(1).核心 RBAC(Core RBAC)：RBAC 核心概念就是將角色指派給使用者，而每個角色則給予不同的權限。一個使用者可以被指派多個角色，而一個角色可以指派給多個使用者。另一個核心的概念是使用者期間(User Session)，當使用者選擇啟動一角色職位，就是一個使用者期間的開始，於期間中，使用者可以選擇性地啟動或終止角色職權的行使。相較於 $RBAC_0$ 並沒有使用者期間的觀念，核心 RBAC 則是將圖 4.10 中之 $RBAC_2$ 模組中的期間(Session)加入其中，圖 4.13 是其示意說明。

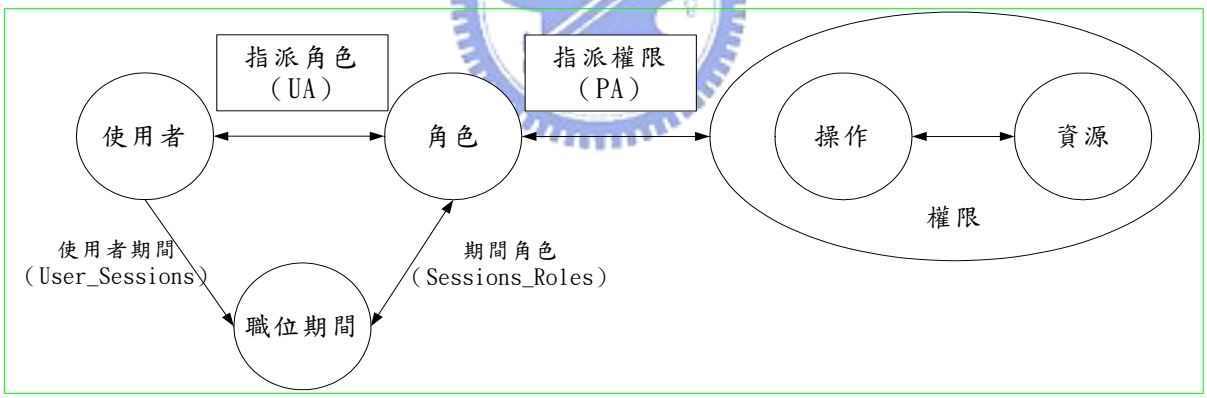


圖 4.13：核心 RBAC 示意圖【11】

(2).階層式 RBAC(Hierarchical RBAC)：主要的觀念就是角色之間的層級關係與繼承關係。舉例來說，當角色甲具有角色乙所有的權限，則可以說角色甲與角色乙有繼承的關係；將一些共同的基本權限規劃於層級較低的角色，利用繼承的關係，免去每個角色都必須重複指派共同權限的動作，減輕管理的負擔。階層式 RBAC 又可以再分為兩種：

(2.1). 一般職位階層模式(General Hierarchical RBAC)：上層的角色可以繼承下層所有的權限，而沒有任何限制條件。

(2.2). 限制職位階層模式(Limited Hierarchical RBAC)：一般而言，在組織運作實務中，職位階層模式常常無法滿足管理的需求；因此，限制式的職位階層模組，強化繼承上的管理限制；上層角色所能繼承的權限範圍，應根據管理政策加以限制。

(3).靜態權責區分(Static Separation_of_Duty Relations)：權責區分的主要用意在於避免利益衝突(Conflict of Interests)的情形。具有利益上衝突的兩個角色，應將此二角色設定為強互斥(Mutually Exclusive)，也就是說不能由同一人同時擔任這兩個角色。靜態權責區分的限制根基於角色層級的定義與使用者指派角色的情境上。

(4).動態權責區分(Dynamic Separation_of_Duty Relations)：依據最小權限原則，某些角色可以指派給同一人，但是不可以同時啟動這些角色，這些角色間的關係稱為弱互斥(Weak Exclusion)。動態權責區分的目的，在於提供組織實務運作上更大的彈性與效率，只要兩個角色在單獨啟動時不會有利益衝突的顧慮，則允許將這兩個角色指派給同一使用者。

圖 4.14 是上述不同 RBAC 之示意說明。

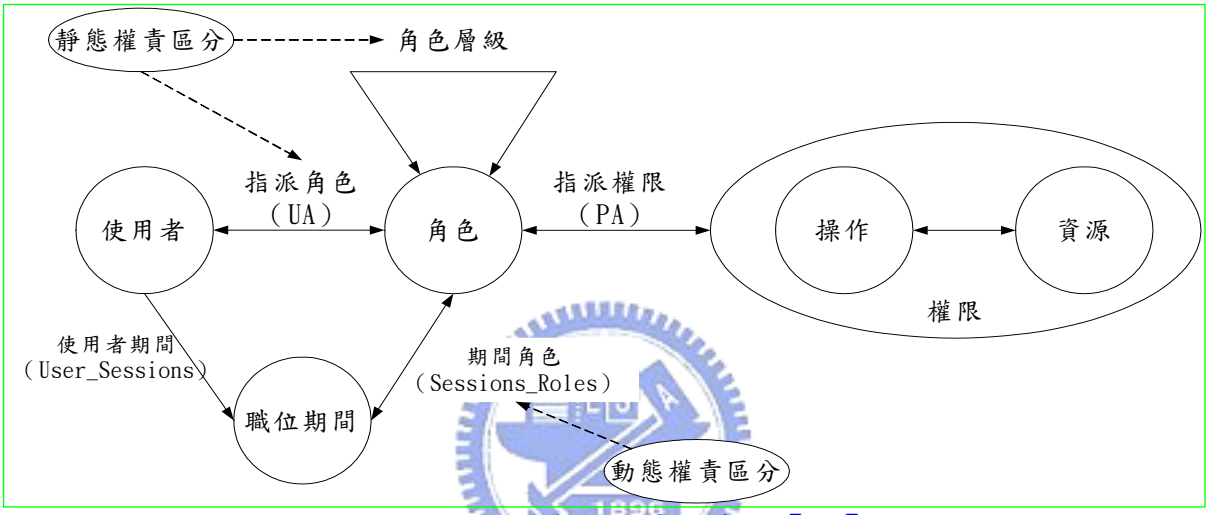


圖 4.14：限制式 RBAC 示意圖【11】

一般而言，RBAC 具有下列 3 個優點：

(1).容易理解與管理：使用者的權限已經融入角色之中，管理者針對單一使用者不必考慮要給予哪些權限，而是指派哪些角色給他。角色職權的設定不會因為員工離職、調職而有所變更，僅需變更該員工的設定即可，在管理上是比較方便的。

(2).擴充性高：在一個使用者眾多的系統之中，角色的數量一定是小於所有使用者的數量。以電子商務為例，角色可能包含買家、賣家、管理人員，但是實際的使用者數量可能是超過幾千、幾萬人。與傳統的存取控制比起來，RBAC 在應用於大量使用者的環境，更具有擴充性。

(3).具有最小權限、權責區分、權限繼承的概念：綜合以上對於 RBAC 的介紹，強調 RBAC 於資源存取控制上，基於最小權限原則，授與使用者完成任務所需的最小權限；基於避免利益衝突的原則，可以設定角色之間的關係為靜態的強互斥，或是動態的弱互斥；在角色層級的設定上，具有繼承權限的觀念，減少被指派權限的管理工作，而在繼承權限時，也可以指定繼承部分的權限，提供一個可以代理角色的機制。

根基於 RBAC 之塑模，其實作系統架構，可以區分為以下兩種【1, 3, 11, 55, 59】：

(1).以使用者端為主的架構(User-Pull Architecture)：當使用者要存取資源時，必須由

使用者端主動獲取角色資訊，提供給網頁伺服器，作為判斷是否有權限存取的依據。

(2). 以伺服器為主的架構(Server-Pull Architecture)：本架構將角色資訊儲存於伺服器端的目錄伺服器中，當使用者要求存取資源時，網頁伺服器必須向目錄伺服器取得角色資訊，加上原本就儲存在伺服器端的角色層級資訊、權限資訊，判斷該使用者是否具備存取某資源的權限。

上述兩種架構分如圖 4.15 與圖 4.16 所示【6】，其包括：使用者端使用上的便利性、整體系統的效能、可重複使用性、角色資訊更新的難易度與發生單點錯誤的影響等之比較如表 4.5 所示，說明如后：

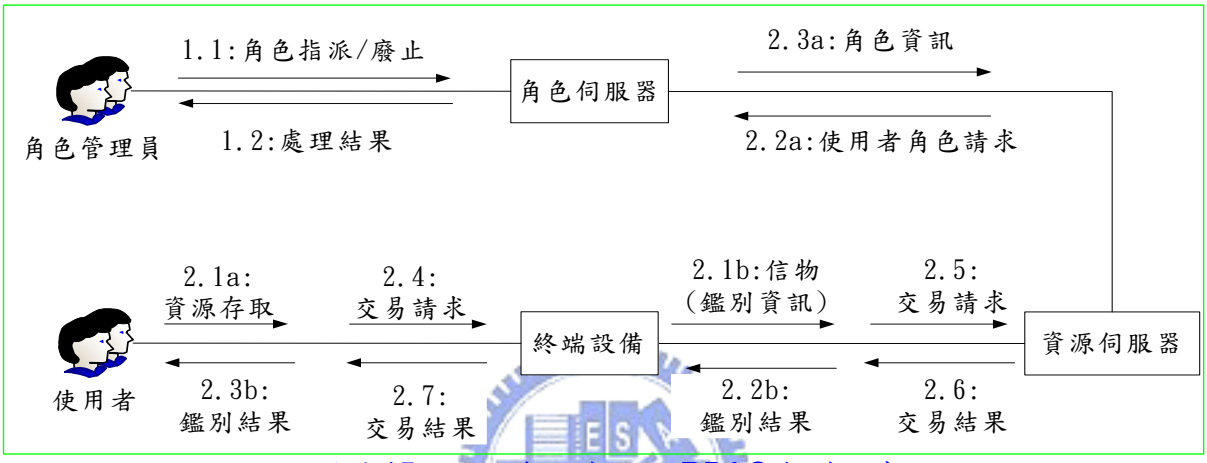


圖 4.15：使用者端為主之 RBAC 架構示意

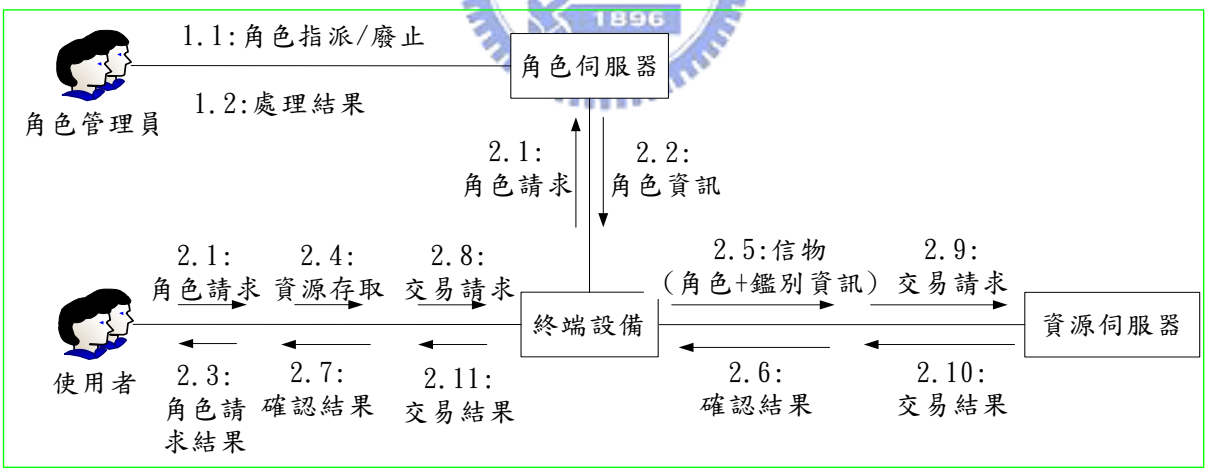


圖 4.16：伺服器端為主之 RBAC 架構示意

表 4.5：RBAC 系統架構的比較

項目	User-Pull 架構	Server-Pull 架構
使用者便利性	低	高
整體系統效能	高	低
可重複使用性	高	低
角色資訊更新速度	低	高
發生單點錯誤的影響	低	高

(1). 使用者便利性：以使用者為主的架構來說，必須在使用者的平台上加裝軟體，對於使用者而言無異是一項負擔。在使用上，必須由使用者端主動提出角色資訊，造成使用者端於效能上的減低。
(2). 整體系統效能：因為伺服器為主的架構，將所有處理角色資訊的工作，完全置於伺服器端來完成，所以造成伺服器端必須分配額外的資源加以處理，間接影響到處理網頁服務的能力，整體系統的效能也跟著降低。
(3). 可重複使用性：使用者端取出角色資訊之後，這一份角色資訊理應存放於伺服器上，等待使用者端下一次要求連線時使用。這是屬於一般快取的機制，增加了資訊的可重複使用的特性，也減少了網路傳輸的負擔。
(4). 角色資訊更新速度：因為角色資訊統一存放於伺服器端，等待使用者端要求連線始取出使用，一旦角色資訊有需要更新的情形，僅需要更新中央資料庫即可。相較之下，以使用者端為主的架構，必須更新使用者端的角色資訊，還要判斷目前是否有使用中的角色資訊，必須要一併更新，增加工作之負荷。
(5). 發生單點錯誤的影響：以使用者端為主的架構，如果錯誤發生於單一使用者端，其影響的範圍僅限於該端點。如果錯誤發生於伺服器為主的架構下，影響的範圍可能擴散至整個系統。

由於 SE Linux 已獲得世界性的公認為 Linux 的安全性加強工具，同時 SE Linux 本身安全政策語法繁雜，淺述於后。SE Linux 是否有權存取是針對受體(Object)及主題(Subject)的安全上下文(Security Context)來決定，而安全上下文主要是以 user: role: type 來表示。此外 SE Linux 主要以 TE 及 RBAC 方式制定安全政策。

SE Linux 政策語言主要包含四種表達方式：宣告(Declarations)，規則(Rules)，限制(Constraints)與主張(Assertions)；根基於此，建置 EAL4 之 RBAC 系統將有事半功倍的效果【10, 87】。

在可信賴計算平台之規範下，前述的 TE 與 RBAC 之實作均將使用可信賴平台模組【56, 95】。

4.4、密碼技術應用之驗證與認證初探：

4.4.1、前言：

2001 年 2 月 5 日，行政院函送「建立我國通資訊基礎建設安全機制計畫」至各所屬機關並要求切實配合辦理，正式開啟了我國資訊安全發展的新頁。近年來世界各國(如：美、英等國)皆全力投入推動資訊安全基礎建設，再加上「七二九全台大停電」及「九二一大地震」對台灣社會所造成莫大的衝擊，根基於此，有關單位於 1999 年春季起意識到通資訊基礎建設安全對國家的重要性，隨即著手規劃「我國通資訊基礎建設安全機制」；但由於我國現有之通資訊安全措施均侷限於局部性，並無整體防護、識別及回復能力等，為爭取時效，行政院國家資訊通信基本建設(National Information Infrastructure，簡稱 NII)專案推動小組研討相關規劃作業；經審慎研擬，於 2001 年 1 月 31 日召開「國家資通安全會報」第一次會議，期以 4 年的時間，以圖 4.17 與圖 4.18 之架構完成「建立我國通資訊基礎建設安全機制計畫」。

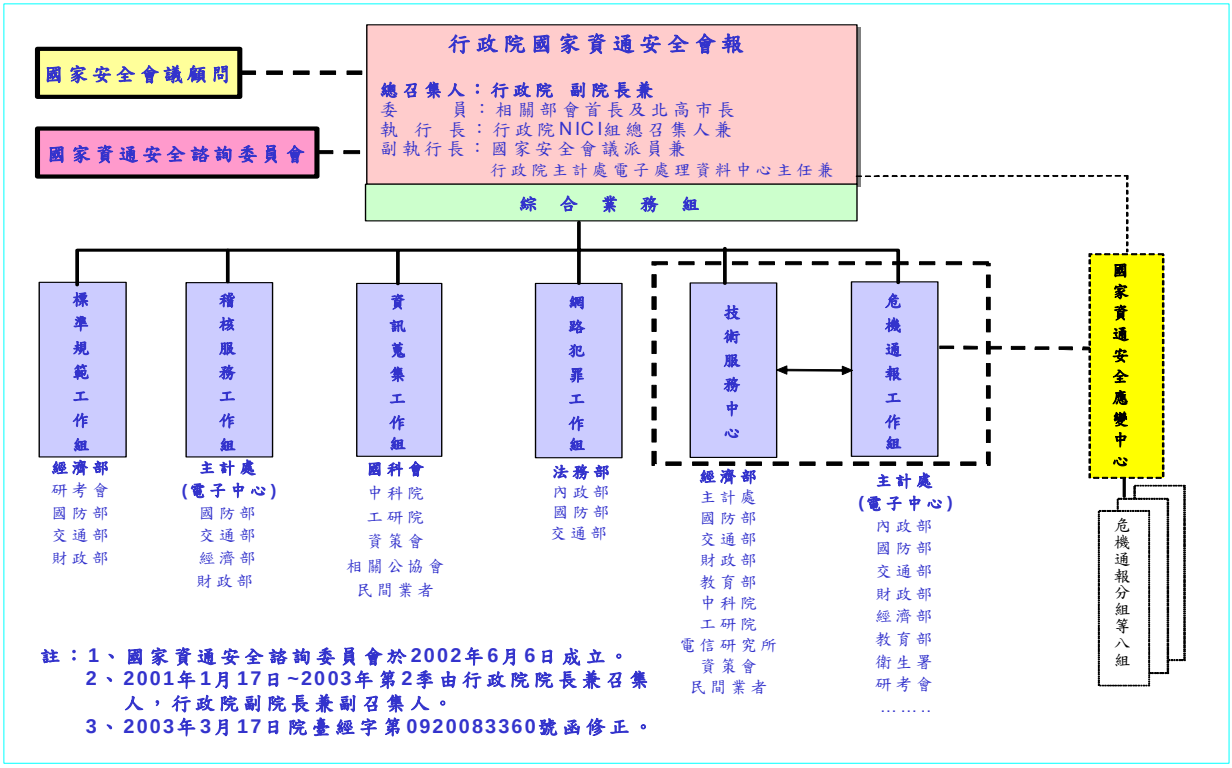


圖 4.17：我國資通安全之組織架構(2001 年 1 月 17 日~2004 年 10 月 20 日)

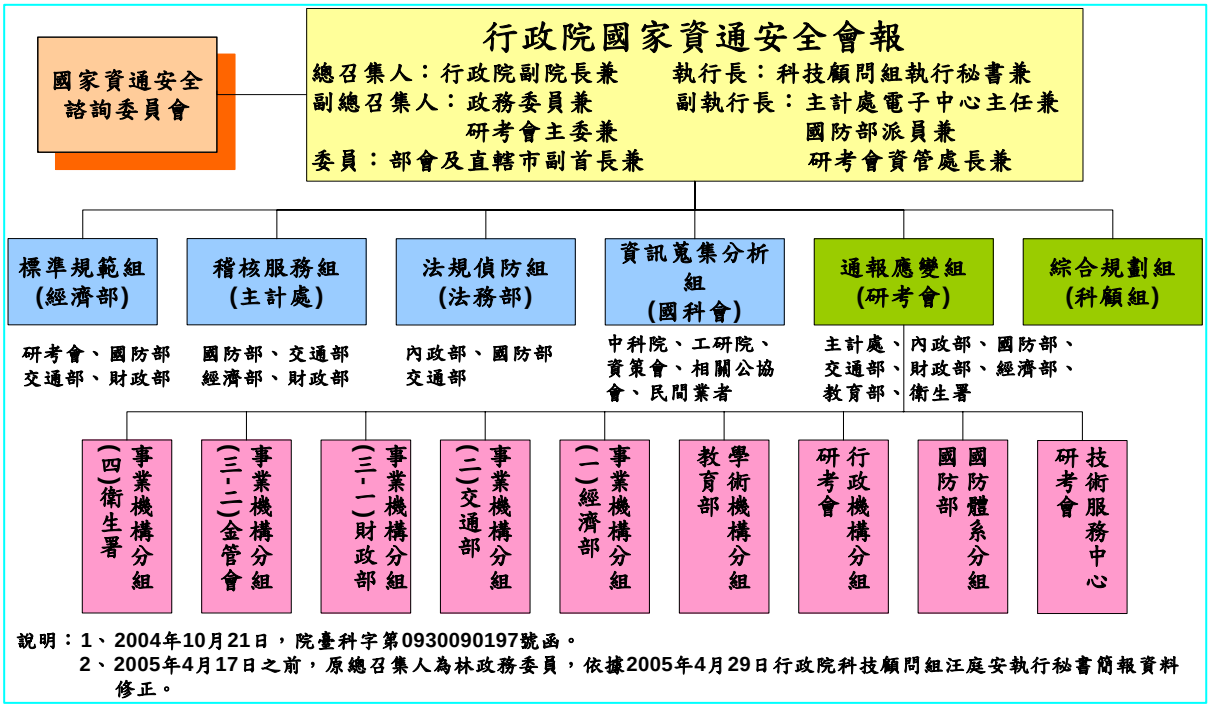


圖 4.18：我國資通安全之組織架構(2004 年 10 月 21 日~迄今)

前述計畫在行政院正式成案之前，動員人數之多、牽涉層面之廣、民間互動之深等各方面，於我國資訊安全領域均屬空前，未來對資訊安全方面之科技專案研發方向，可能亦將產生深遠的影響。國家通資安全會報成立時，是由行政院院長與副院長分別擔任正、副召集人，並由行政院資訊通信發展推動小組(National Information and Communication Initiative Committee，簡稱 NICI)的總召集人擔任執行長，會報下設立綜合業務工作組、危機通報工作組、技術服務中心、網路犯罪工作組、資料蒐集工作組、稽核服務工作組與標準規範工作組等七個組，負責推動國家通資訊安全基礎建設之各項工作，其中標準規範工作組是由經濟部為主要負責單位，而研考會、國防部、交通部、財政部則配合協辦，主要職掌陳述如下：

(1).訂定資通安全技術標準。
(2).訂定各機關辦理資通安全有關作業規範。
(3).規劃建置資通安全驗證方法。
(4).規劃建置資通安全認證程序。

為達成前述計畫之工作計畫目標，經濟部標準檢驗局已根基於 1994 年公布之世界貿易組織烏拉圭回合多邊貿易談判協定(The Results of The URUGUAY Round of Multilateral Trade Negotiations)技術性貿易障礙協定(Agreement on Technical Barriers to Trade，簡稱 TBT)附件 1~3(Annex 1~3)之規範，分以下述 4 項為工作方向推動相關工作中：

(1).資訊技術安全評估共同準則(ISO/IEC 15408)系列、資訊安全管理(ISO/IEC 17799)、軟體處理評估(ISO/IEC TR 15504)系列等標準之制定。
(2).ISO/IEC 15408 系列標準中針對不同產品(例：存取控制、密碼模組、金鑰憑證發行及管理)之保護剖繪(Protection Profile，簡稱 PP)與其之共同性檢測技術之建置。

(3).將 BS 7799-2(Information Security Management Systems Part 2: Specification for Information Security Management Systems)轉定為國家標準，建置我國通資訊安全之管理系統驗證作業體系(備考：此項工作於 2005 年將使用 ISO/IEC 27001:2005(E)轉定為國家標準取代)。
(4).符合 ISO/IEC Guide 62、ISO/IEC Guide 65 與 ISO/IEC 17025 之要求，分別建置通資訊安全管理系統認證、產品驗證認證以及實驗室認證之認證程序。

4.4.2、密碼技術應用產品之檢驗與測試【96】：

我國自 1997 年起，於密碼模組測試實驗室之定位一直在規劃作業中，至今已有之共識為：『遵照美國 NIST FIPS 140 之標準，其中「作業環境」的測試項目應遵循共同準則的規範；所以要通過密碼模組安全需求測試的產品，在作業環境之測試項目必須先取得共同準則的證書。』，共同準則原先規劃共有 6 個部分，除已公布之 ISO/IEC 15408 系列標準的 3 部分外，尚有下述之評估準則：

(1). 第 4 部分：預先定義之保護剖繪(Predefined Protection Profile，簡稱 PPP)：
  (1.1).針對 FC 之商用安全(Commercial Security，簡稱 CS)，與 TCSEC C2 安全等級之諸如作業系統、資料庫管理系統及其他敏感性使用環境的應用，使用共同準則定義「基礎受控存取保護(Basic Controlled Access Protection)」之 PP。
  (1.2).針對 FC 之 CS3 安全等級之諸如作業系統、資料庫管理系統與其他敏感性使用環境的應用，使用共同準則定義「角色基底存取保護(Role-Based Access Protection)」之 PP。
  (1.3).「網路/傳輸封包過濾防火牆(Network/Transport Packet Filter Firewall)」之 PP。
(2). 第 5 部分：PP 之登錄與維護程序。
(3). 第 6 部分：就密碼學(Cryptography)定義
  (3.1).機密資訊(Classified Information)。
  (3.2).非機密但會衝擊(Impact)國家安全(National Security)之敏感性(Sensitive)資訊。
  (3.3).敏感但與國家安全無關之資訊。
  等 3 種不同層級的密碼學支援(Support)需求 PP 與安全標的(Security Target，簡稱 ST)，以提供：
  (3.4).密碼模組(Cryptographic Module，簡稱 CM)實作。
  (3.5).密碼政策作業方針(A Cryptographic Policy Operational Doctrine，簡稱 CPOD)。
  (3.6).評估標的(Target of Evaluation，簡稱 TOE)遵行 CPOD 使用 CM 時之驗證。

共同準則於 1996 年 1 月 31 日公布 CC1.0 版時僅包含第 1~4 部分，於同年 3 月 30 日公布第 6 部分之技術報告 0.99b 版；1998 年 5 月公布之 CC 2.0 版已將原規劃之共同準則第 6 部分溶入。換言之，共同準則之範疇已包含美國 NIST FIPS 140 且擴及機密資訊與國家安全相關資訊；在另一方面，除密碼模組外，亦擴及使用密碼模組之評估標的。美國聯邦政府等自 1919 年起有系統的應用密碼學，1994 年 6 月 30 日正式生效，處理敏感但非機密性資訊之美國 NIST FIPS PUB 140-1 正式開啟密碼模組之驗證機制，其 2001 年 5 月 25 日公布之 NIST FIPS PUB 140-2，在作業環境中明文要求

遵循共同準則之保護剖繪，其檢測技術關連示意如圖 4.19 所示，其中除 TEMPEST(包含 EMI/EMC)屬於驗證體系中之檢驗(Inspection)工作，其他均屬測試(Testing)之範疇。

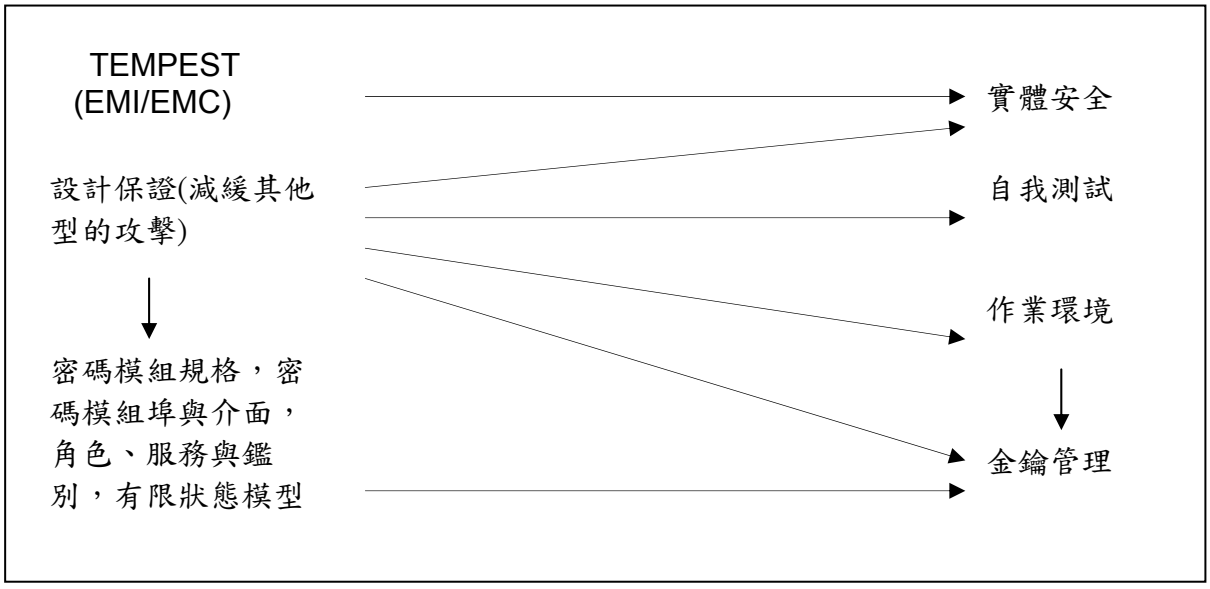


圖 4.19：密碼模組檢測技術關聯示意

表 4.6 為 NIST FIST PUB 140-2 中除 EMI/EMC 安全需求項目外與共同準則中安全功能、保護剖繪等之對應關係，在 NIST FIPS PUB 140-2 中之作業環境安全需求項目最高要求僅至 EAL4+，且於減緩其他類型的攻擊中，僅要求提出說明並未有任何實質要求。根基於圖 4.19 與表 4.6，我們應能確認共同準則測試實驗室除 EMI/EMC 外，應可執行 NIST FIPS 140-2 之密碼模組安全需求測試工作，尚可考慮擴充至：

(1). 安全等級 5：處理非機密但會衝擊國家安全之敏感性資訊之密碼模組。

(2). 安全等級 6：處理機密性使用之密碼模組。

表 4. 6：美國聯邦政府密碼模組安全需求(FIPS 140-2:2001)與共同準則[ISO/IEC 15408:1999(E)]對應關係示意說明

	FIPS 140-2:2001	共同準則[ISO/IEC 15408:1999(E)]
安全需求項目	密碼模組規格	安全功能中之密碼支援類別
	密碼模組埠與介面	安全功能中之密碼支援類別與安全保證中之發展類別
	角色、服務與鑑別	安全功能中之使用者資料保護、識別與鑑別以及安全管理類別
	有限狀態模型	安全保證中之發展類別
	實體安全	安全功能中之安全稽核類別
	作業環境	保護剖繪：受控存取，作業系統
	密碼金鑰管理	安全功能中之密碼支援類別
	自我測試	安全功能中之密碼支援與 TOE 安全功能保護類別
	設計保證	安全保證：組態管理類別，發展類別
	減緩其他類型的攻擊	安全保證中之脆弱性評鑑類別

備考：FIPS 140-2 列舉之安全需求中電磁干擾與電磁相容(EMI/EMC)項目，於我國自 1995 年 9 月 27 日起已開始檢驗並已建置具備相當規模之檢驗實驗室。

其驗證標準以作業環境為例：
(1).安全等級 5：符合 EAL4+ 評估要求之保護剖繪。
(2).安全等級 6：符合 EAL5+ 評估要求之保護剖繪。
其他密碼支援等部份，可以分別參照共同準則相關資訊等加以制定。

除前述之安全等級不足以滿足建置我國通資訊基礎建設安全機制中諸如已知 VISA 晶片卡等之需求外，如表 4.6 與圖 4.20 所示，於優先秩序上欲建置完成 NIST FIPS PUB 140-2 驗證標準之資訊安全測試實驗室，必須先建置完成具備測試作業環境能力之共同準則資訊安全測試實驗室，表 4.7 是 NIST FIPS PUB 140-2 與共同準則驗證作業之比較。

表 4.7：密碼模組安全需求與共同準則驗證作業比較表

	密碼模組安全需求(FIPS 140)	共同準則(ISO/IEC 15408)
評估範圍	評估密碼模組(內含密碼演算法)在實體上及邏輯上的安全性。	對任何形式之包含密碼功能在內的資訊技術產品、系統或服務作安全評估。
安全需求	特定的功能。	以符合遵循共同準則之保護剖繪要求的功能與保證需求。
遵循標準	2001 年 5 月 25 日美國聯邦政府使用之 NIST FIPS 140-2	1999 年 12 月 1 日國際標準組織頒布之 ISO/IEC 15408 系列規範
源起	1994 年 1 月 4 日之美國 NIST FIPS 140-1	1985 年之美國 Trusted Computer System Evaluation Criteria
安全等級	四個	1.於安全功能與安全保證均有等級之分，使用者可依產品或系統的保護剖繪與安全等級決定其所需要的產品或系統。 2.共同準則在產品或系統設計上針對不同產品或系統經由保護剖繪提出符合安全需求之反制安全威脅應有的特定功能。 3.將脆弱性評鑑中之抵抗潛在入侵能力區分為基礎(Basic)、適度(Moderate)與高(High)三個等級。
對象	密碼模組	資訊技術產品、系統與服務，於保護剖繪登錄上，目前分為存取控制(Access control)、通訊(Communication)、資料庫(Database)、作業系統(Operation systems)、網路(Networking)、智慧卡(Smart card)及其他(Miscellaneous)七個領域。
至 2005 年 11 月 30 日止經認可之實驗室數目	美國：7；加拿大：2；英國：2；德國：1	美國：10；加拿大：3；英國：5；法國：5；德國：13；澳洲及紐西蘭：2；荷蘭：1；日本：3
進行中之計畫	2006 年 3 月 1 日公布 ISO/IEC 19790 之密碼模組安全需求，2005 年 1 月 12 日，ISO 公布制定 FIPS 140-3。	2005 年 10 月 1 日公布 ISO/IEC 18045 :2005 之資訊技術安全評估方法，並進行預定在 2007 年使用之共同準則與共同評估方法 3.0 版。

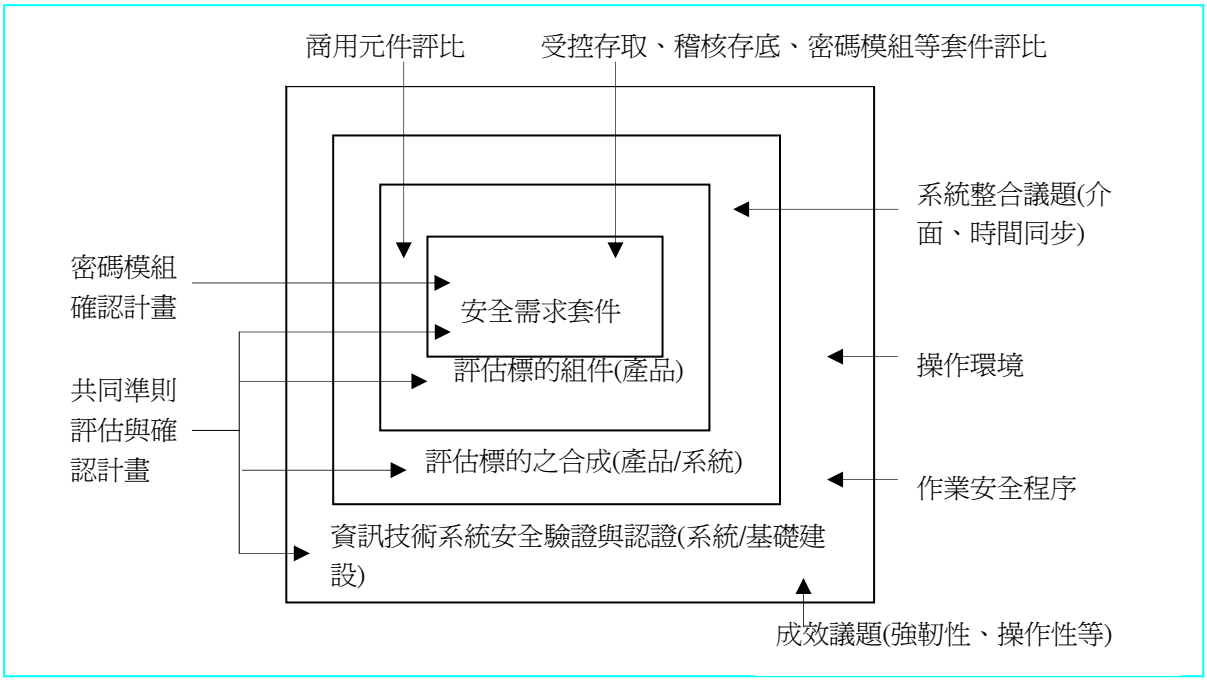


圖 4.20：美國聯邦政府資訊技術安全評估示意說明

保護資訊資產的安全，已成為當今文明國家之共識，亦為民主法制國家、社會與人民必備的素養。資訊安全認、驗證體系是達成資訊安全保證之礎石，以美國為例，由國家通信與資訊系統安全委員會(National Security Telecommunications and Information Systems Security Committee，簡稱 NSTISSC)制定行政方針，NSTISSC 已於 2000 年 7 月頒布明確之訓令，要求相關機構實施資訊安全認、驗證作業中。前述之共同準則與密碼模組等驗證作業在資訊技術安全評估中之關連與角色如圖 4.19 所示；換言之，FIPS140-2 僅是共同準則中一個重要的資訊技術安全需求套件。以公開金鑰基礎建設(Public Key Infrastructure，簡稱 PKI)為例，已公布之保護剖繪等如表 4.8 所示，其中受控存取保護剖繪(Controlled Access Protection Profile，簡稱 CAPP)是套件，憑證簽發與管理組件保護剖繪(Certificate Issuing and Management Components Protection Profile，簡稱 CIMCPP)是組件，金鑰回復系統(Key Recovery System，簡稱 KRS)是表 4.8 中之 6、8 與 9 三個 PP 之評估標的之合成，高保證環境的遠端存取保護剖繪是系統的型樣(註：表 4.8 中之 13)，資訊技術系統安全驗證與認證則包含關鍵資訊基礎建設(Critical Information Infrastructure)在內，表 4.8 中之 PKI 相關保護剖繪等之關連示意如圖 4.21 所示，其中 RBAC 之實作，如圖 4.15 與圖 4.16 所示，幾均使用密碼技術【95】。

根基於表 4.6，我們可以提出如表 4.9 中擴充度列所示之安全保證套件(Security Assurance Package，簡稱 SAP)做為圖 4.15 與圖 4.16 中，處理 4.4.2 節中述及之機密資訊以及會衝擊國家安全之敏感性資訊的密碼模組及 PKI 安全核心保護剖繪中之保證需求，以為「建立我國通資訊安全機制基礎建設」密碼應用技術產品檢驗、測試實驗室的參考。

表 4. 8：以公開金鑰基礎建設為例，已公布之保護剖繪表列

1. Certificate Issuing and Management Components Protection Profile。
2. Controlled Access Protection Profile。
3. Directory for US Department of Defense Class4 PKI (Public Key Infrastructure) Protection Profile (Strawman Draft VERSION 0.2)。
4. Guidance for COTS (Commercial off the Shelf) Security Protection Profile。
5. Intrusion Detection System (IDS) System Protection Profile。
6. Key Recovery Protection Profile for End Systems。
7. Labeled Security Protection Profile。
8. Protection Profile for Key Recovery Agent Systems。
9. Protection Profile for Key Recovery Third Party Request。
10. Protection Profile for Single-Level Operating Systems in Environments Requiring Medium Robustness。
11. Protection Profile for Multi-Level Operating Systems in Environments Requiring Medium Robustness。
12. Public Key Infrastructure and Key Management Infrastructure Token Protection Profile (Medium Robustness)。
13. Public Key Infrastructure (PKI) Secure Kernel Protection Profile (PSKPP)。
14. (U.S. DoD) Remote Access Protection Profile for High Assurance Environments。
15. Role-Based Access Control Protection Profile。
16. Security Requirements for Cryptographic Modules (ISO/IEC 19790)。
17. Smart Card Security User Group Smart Card Protection Profile。
18. Virtual Private Network (VPN) for confidentiality ─ VPN Protection Profile。

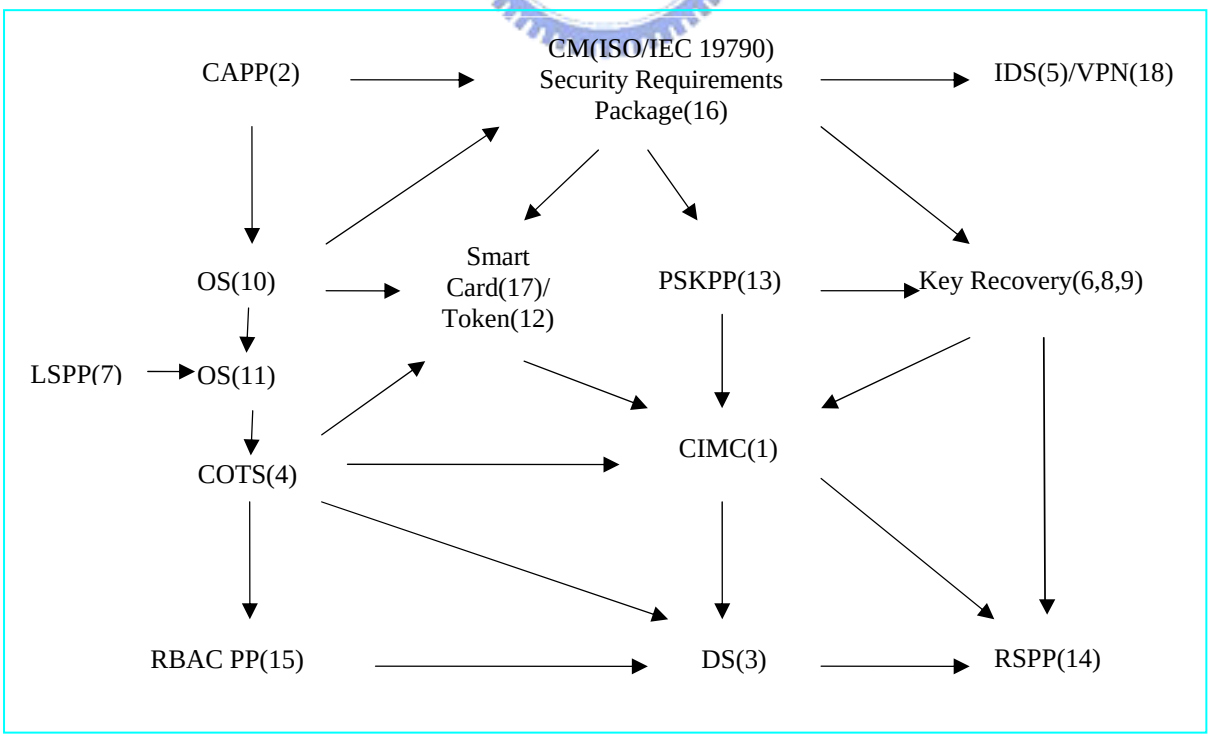


圖 4.21：PKI 相關保護剖繪關連示意

表 4. 9：處理機密性與會衝擊國家安全之敏感性資訊的密碼模組及 PSK PP 安全保證需求(PSK Security Assurance Requirements)擴充

組件(Component)	評估保證等級(EAL)	擴充度(Augmentation Degree)
ACM_AUT.2	EAL4+	EAL6
ACM_CAP.4	EAL4	EAL4
ACM_SCP.3	EAL4+	EAL5
ADO_DEL.2	EAL4	EAL4
ADO_IGS.1	EAL4	EAL4
ADV_FSP.3	EAL4+	EAL5
ADV_HLD.3	EAL4+	EAL5
ADV_IMP.3	EAL4+	EAL6
ADV_INT.3	EAL4+	EAL7
ADV_LLD.I	EAL4	EAL4
ADV_RCR.2	EAL4+	EAL5
ADV_SPM.2	EAL4+	EAL4+
AGD_ADM.1	EAL4	EAL4
AGD_USR.I	EAL4	EAL4
ALC_DVS.2	EAL4+	EAL6
ALC_FLR.3	EAL4+	EAL4+
ALC_LCD.3	EAL4+	EAL7
ALC_TAT.2	EAL4+	EAL5
ATE_COV.2	EAL4	EAL4
ATE_DPT.3	EAL4+	EAL7
ATE_FUN.2	EAL4+	EAL6
ATE_IND.2	EAL4	EAL4
AVA_CCA.I	EAL4+	EAL5
AVA_MSU.2	EAL4	EAL4
AVA_SOF.I	EAL4	EAL4
AVA_VLA.2	EAL4	EAL4

說明：

1. EAL：評估保證等級(Evaluation Assurance Level)。
2. PSK：PKI Secure Kernel。
3. ＋：已增加(Augmented)。

資料來源：The PSK Protection Profile, Version 1.1, April4, 2002, pp.114.

4.4.3、密碼裝置與管理【93】：

任何一個基於密碼學的安全機制，其在應用上的安全與否，均仰賴其安全密碼裝置（Secure Cryptographic Device，簡稱 SCD）管理的良莠，宛如一個防護措施完善的銀行金庫，一旦鑰匙被入侵者破解；那麼這座銀行金庫對抗入侵者之威脅是非常困難的工作。安全密碼裝置管理是銀行安全控制措施中非常重要的一環，絕對的安全在實務上是無法冀求的，銀行安全密碼裝置的安全是根基於 SCD 之生命週期中每個階段的適當管理程序與密碼學特性之互補組合而定，這些管理程序提供預防的措施以降低威脅密碼裝置安全之機會。若密碼裝置之特性不能預防或偵測安全破解的威脅，將由管理程序提供偵測出任何對敏感性或機密性資料非經授權存取之高可能性。

零售式電子銀行業的安全性大部份依賴這些密碼裝置的安全。安全需求以電腦檔案可被存取及調改，通訊系統可"被竊聽" 而已獲授權的資料或控制輸入至系統裝置可由未經授權的輸入來置換為前題。然而特定的密碼裝置 (例如：主機安全模組) 位於相當高度的安全處理中心，大多數使用在零售式銀行業中的密碼裝置 (例如：客戶個人識別碼輸入器，自動提款機，等等) 現在都處於不安全的環境中。因此當客戶個人識別碼（Personal Identification Number，簡稱 PIN），訊息鑑別碼（Message Authentication Code，簡稱 MACs），密碼金鑰及其它的敏感資料在這些裝置運作時，就有裝置可能被竄改或破解以揭露或修改此資料的風險。

經由適當地使用具有恰當的實體和邏輯安全特性及被恰當地管理的密碼裝置，金融損失的風險必須確保被降低。為確保安全密碼裝置擁有恰當的實體及邏輯安全，它們需要評估與稽核。

需要適當的裝置特性以確保該裝置具有恰當的運作能力及對其所包含的資料提供適度的保護。需要適當的裝置管理以確保該裝置是合法的，及它並沒有以未授權的方式被修改，(例如：經由 "竊錄")，且任何位於該裝置中的敏感資料 (例如：密碼金鑰) 沒有遭受揭露或更改。

絕對的安全在實務上是達不到的。密碼安全取決於安全密碼裝置的生命週期的每一個階段以及適當的裝置管理程序和安全密碼特性的結合。這些管理程序執行 預防措施以降低密碼裝置安全破壞的機會。這些措施能夠偵測裝置特性無法預防或偵測安全破解的事件中任何對敏感的或機密的資料的違法的存取。

適當的裝置特性對確保裝置有正確的運作能力，以及提供裝置內資料適當的保護是必要的。而適當的裝置管理對確保裝置合乎公認標準是必要的，即其未受到未授權的方式修改（例如藉由“竊錄（bugging）方式”），以及置於裝置內的敏感資料（例如密碼金鑰（Cryptographic Key））尚未受到揭露或變更之威脅亦是必要的。根基於此，國際標準組織（International Organization for Standardization，簡稱 ISO）針對銀行業零售式（Retail）的安全密碼裝置(例：自動櫃員機)之安全性於 1998 年 6 月 15 日頒布標準，規範其管理的需求【93】。

零售式銀行業利用密碼裝置之幫助以確保：

(1). 敏感資料的完整性，例如交易明細。
(2). 秘密資訊的機密性（Confidentiality），例如客戶個人識別碼（Personal Identification Number，PIN）。
(3). 達成這些目標之密碼金鑰的機密性。

為了確保上述目標，必須防止下列的威脅：

(1). 儲存在或登錄至裝置之敏感資訊的揭露。
(2). 敏感資訊的修改。

(3). 裝置的未授權使用。
(4). 未授權存取服務。

因為絕對的安全在實務上是達不到的，所以描述一個 SCD 為“防破壞（Tamper Proof）”或“實體保全（Physically Secure）”是不切實際的。事實上，只要有足夠的成本、努力及技術，任何安全方案皆可被破解。再者，即使以前深信免於可能的攻擊之安全方案，隨著科技的進展，有可能發展出新的技術來攻擊它。所以，更實際的是依安全裝置具有的抗破壞程度加以分類，而可接受的程度是在裝置的運作生命期間內安全裝置被視為足以阻止任何想像中可能的攻擊，並考量發動一個成功之攻擊需要的設備、技巧及其它成本，以及從此攻擊中能夠獲得的財務利益。

零售式系統的安全考量裝置安全、運作環境的安全及裝置的管理之實體及邏輯觀點，結合這些因素建立裝置及裝置所使用的應用程式安全，安全需求則由應用程式之風險評鑑衍生而出。

所要求的安全特性將視規劃的應用程式、運作環境及必須考量的攻擊型式而定，應該將風險評鑑做為選擇最適當的裝置安全評估方法之輔助，然後，評鑑其結果，以決定某一應用程式及環境接受該裝置。接著我們分別從攻擊場景，防禦措施與風險評鑑三個構面探討安全密碼裝置之管理觀念。

(1). 攻擊場景：此處所敘述的攻擊場景不試圖做為一個包含一切攻擊的表列，僅列出有關的主要範圍。SCD 易受到下列五個主要型式的攻擊。
(i.) 滲透（Penetration）。
(ii.) 監視（Monitoring）。
(iii.) 調處（Manipulation）。
(iv.) 修改（Modification）。
(v.) 替代（Substitution）。

這些攻擊如下：

(1.1). 滲透：

滲透是一種主動的攻擊，它包括實體洞穿或未授權的開啟裝置以探查裝置內之敏感資料，例如金鑰密碼，所以滲透是對裝置的實體特性之攻擊。

(1.2). 監視：

監視是一種被動的攻擊，可能包括為了發覺裝置內之敏感資訊，而監視電磁輻射（Electromagnetic Radiation），或視覺上、聽覺上或電子監視登錄至裝置的秘密資料，所以監視是對裝置的實體特性之攻擊。

(1.3). 調處：

調處是未授權的送出一連串的輸入值到裝置，以便導致敏感資訊的揭露，或以未授權的方式獲得服務，例如，為了能夠揭露敏感資訊或調處裝置的完整性，而使裝置入“測試模式(Test)”。調處是對裝置的邏輯特性之攻擊。

(1.4). 修改：

修改是對裝置之邏輯或實體特性的未授權之修改或更改，例如，在 PIN 的登錄點與 PIN 的加密(Encryption)點之間，於 PIN 輸入器(PIN Pad)插入一個 PIN 竊錄器。必須注意的是修改可能包括滲透，但此滲透之目的與其說是揭露裝置內的資訊，不如說是修改裝置。未授權的取代在裝置內之密碼金鑰也屬於修改的一種型式，修改不是對裝置的實體特性就是對裝置的邏輯特性之一種攻擊。

(1.5). 替代：

替代是未授權的以另一裝置取代原有裝置，所取代的裝置可能看起來是相似的“偽造品（Counterfeit）”，或是模仿具有全部或某些正確之邏輯特性及某些未授權功能（例如，PIN 竊取器）的裝置，而且可能是一時合法的裝置，其易受到未授權的修改及另一合法裝置的替代。移除是替代的一種型式，有可能是為了更適合執行滲透或修改攻擊的環境而實行移除，或者移除是替代攻擊的第一個步驟，有可能是從運作環境中將裝置移除。替代能夠視為修改的特例，在修改過程中，對手並非實際修改標的裝置，而是以修改之後的替代品取代標的裝置。替代是裝置的實體及邏輯特性之一種攻擊。

(2). 防禦措施：為了防禦上的攻擊計畫，結合下列三個因素以提供所需要的安全：

(i.) 裝置特性。

(ii.) 裝置管理。

(iii.) 環境。

正常的情況下，必須具備所有因素才能達到預期結果，然而在某些情況下單一因素（例如裝置特性）可能具支配性。

(2.1). 裝置特性：

將密碼裝置設計及實作成具邏輯及實體安全，以阻止上節敘述的攻擊場景，如經由對應用與環境所作之風險評鑑.

實體安全裝置特性的主要目的是防禦滲透攻擊，可將此特性細分成三種類型：

(i.) 破壞存跡特性。

(i). 抗破壞特性。

(ii). 破壞回應特性。

破壞存跡的目的是提供一個曾嘗試攻擊之證據，以及它可能已經導致或尚未導致敏感資訊的未授權揭露、使用或修改。一個曾嘗試的攻擊能夠以實體證據（例如包裝的破壞）之型式揭露，此外，裝置已不在預期的位置也能夠做為證據。

抗破壞的目的是封鎖攻擊，運用被動的障礙物保護資訊使其免遭受到未授權揭露、使用或修改。防禦或障礙物通常是單一的用途，將它們設計成阻止特定的威脅。抗破壞設計的實作是非常依賴設計者對特定實作之已知攻擊方法的知識與經驗。因此緣故，針對抗破壞實作的攻擊通常是對準發覺實作者疏於處理之已知威脅。攻擊者也嘗試發覺新的攻擊方法，而這些攻擊方法可能是實作者所不知道的。評估正常僅能證明設計成功地阻止已知的攻擊，但無法或不能評估抵抗未知的攻擊，所以抗破壞設計的評估是困難的且無定論。

破壞回應的目的是運用主動的障礙物以阻止針對保護的資訊之未授權揭露、使用或修改的攻擊方法。主動的障礙物設法將保護的資訊修改為無法使用的型式。透過某些預先設定之條件或發現對資訊之攻擊，來啟動破壞回應的部署。

實體實作通常是三種類型特性的組合。其它的實體安全特性可能是防禦監視所需要的，也可能有助於防禦修改或替代。

(2.2). 裝置管理：

裝置管理意指在裝置的生命週期期間及其環境所設之外部控制。這些控制包括外部金鑰管理方法、安全實務及運作程序。在裝置的生命週期期間，可以變更安全等級。裝置等管理的主要目標是確保在裝置的生命期間裝置特性不受到未授權的修改。

(2.3). 環境：

環境安全之目標是控制 SCD 的存取及 SCD 的服務，因此要防止或至少偵測出對 SCD 的攻擊。在這個 SCD 的生命週期，SCD 將處在一個多變的環境，這些環境可從高度控制到最低控制。一個高度控制環境包括由可信賴的個體時常監視，而一個最低控制環境可能不包括任何特別的環境安全補強。如果 SCD 的安全視控制某些功能而定，則必須令人滿意地證明該控制環境實際提供此功能。

(3). 風險評鑑：

因為絕對安全在實務上是達不到的，所以評鑑處理考慮到整個裝置生命週期中可能的攻擊場景、可用的裝置保護及預期的運作環境。其它因素包括業務需求、技術需求及整體系統安全也併入評鑑處理。

不僅是取決於風險評鑑，也經常包括價值裁定。風險評鑑是一個反覆考量下列情形的處理：

(i.) 攻擊的威脅。

(ii.) 攻擊成功的損壞或漏失。

(iii.) 這些可能的攻擊發生之機率。

就所有型式的攻擊而言，風險是與各個攻擊有關之機率與漏失的函數，它是否能接受特定攻擊之風險或是否採取保護動作的政策與商業決策。攻擊的複雜性視所需要的工具、設備、技巧及資源（時間與材料）而定。

能夠使用各種不同的方法進行風險評鑑，但是這些議題不在本標準的範圍內。

一個密碼裝置達到安全是經由它本身的特性及該裝置所在的環境的特性。當完成這些稽核核對表列，該裝置所在的環境必須被考量。舉例來說，一個在公共地點所用的裝置比在受控環境中相同的裝置需要更多的本身安全性。一般而言，稽核不需去調查被評估的裝置所在的特定環境，因此一個稽核可能被要求去評估在特殊的環境下特定的裝置的運作狀況。然後這種裝置可被運用在特定的設施中，只要該設施本身已被稽核以確保它提供已得到保證的環境。上述工作，均應在風險評鑑報告中提供量化之證據，供稽核使用。

密碼裝置的安全不僅取決於裝置特性，也取決於放置的環境特性，所以裝置管理可視為裝置的環境需求。裝置應該符合適當的稽核與控制，這些稽核與控制適用於裝置生命週期的每一階段，如果不這麼做，則裝置在生命週期的某個階段可能易受到先前所識別的攻擊場景。這種攻擊會在裝置正式運作使用時危害其安全。

不論是否足以偵測破解或是否必須預防破解，以及能夠用於實作預防或偵測的方法端視裝置在生命週期的那個階段而定。

(1). 生命週期階段：

裝置的生命週期階段是裝置隨環境及/或狀態的改變結果，不同的密碼裝置會有不同的生命週期。表 4.10 呈現一般化的裝置生命週期，顯示密碼裝置生命之可能的階段及導致從一個階段變遷至下個階段的事件。因為裝置的保護需求與提供保護的方法可能使裝置從某個生命週期階段移至另一個，所以辨別這些階段是重要的。

ISO 定義下列的生命週期階段：

(1.1). 製造：裝置的設計、建構、修復、升級及測試，以結合該裝置預期的功能及實體特性。

(1.2). 製造後：製造後階段包括裝置的傳送、儲存及起始金鑰載入。

(1.3). 使用前：在裝置生命週期的此階段中，裝置含有一把尚未安裝供運作使用的金鑰。

表 4. 10：裝置生命週期階段

生命週期階段	變遷事件（進入下一階段）
製造	完成
製造後	起始金鑰載入
使用前	安裝
使用	移除
使用後	重新安裝 修復、升級 破壞

(1.4).使用：當裝置為了預定的目的，已經安裝於預定的位置時，該裝置可視為在運作使用狀態。

(1.5).使用後：在裝置生命中將裝置移除而不再提供服務的階段，此移除可能是暫時的，例如，將裝置移到其它的運作位置或修復裝置；也可以是永久的，例如，移除裝置並且以後不打算再使用它。

(2). 生命週期保護需求：

在裝置生命週期的大部分階段，通常不需要預防安全破解，只需要偵測安全破解，這是因為裝置並未包括任何密碼金鑰或其它被使用中或曾使用的敏感材料，因此如果在裝置正式使用之前被破解且該破解被偵測出來，則可以捨棄或修復該裝置以移除破解的效應。

裝置的安全不應該僅取決於設計細節的秘密性，無論如何，在此保密提供裝置安全的同時，整個所有生命週期階段仍須要求預防破解。當不要求對設計特性保密時，每一個階段的一般需求如下：

(2.1).製造與製造後：

在製造與製造後階段期間，裝置內沒有密碼金鑰，直到已經載入一把起始金鑰之前，必須偵測裝置是否被破解，但不需要預防它。如果偵測出破解，只需在所有破解的效應排除之前，確保裝置還未提供服務。

在起始金鑰載入之前，由裝置本身特性所提供的保護僅是開啟裝置的實體困難度，或取得替代裝置之偽造品的實體困難度。在起始金鑰載入之後，裝置如果提供金鑰抹除（key-erasure）機制，則能夠提供堅固的額外保護。

(2.2).使用前：

在使用前階段期間，裝置至少包含一把起始金鑰，如果有下列情形，應要求預防裝置被破解：

(i.) 湊巧其它設備可能或已經使用起始金鑰對秘密資料加密。

(ii.) 在破解金鑰之後，並在第一次未授權的使用金鑰之前，無法在所有能與破解的裝置通訊之密碼裝置上封鎖已被破解的金鑰。

除了上述之外，應該要求有高的機率能偵測出裝置的被破解機制。

一般而言，當在使用之前，密碼裝置僅要求破解偵測時，裝置內起始金鑰的存在能夠做為偵測的有效方法，倘若裝置一旦被破壞時，裝置具有引發自動且立即清除金鑰的特性。當裝置付諸服務時，如果缺少一把正確的起始金鑰，就會在第一次嘗試使用裝置時突顯出來，該裝置會立刻停止服務並視為是可疑的。所以，這樣的裝置在起始金鑰載入之後，所要求的裝置管理較不如在起始金鑰載入之前所要求的裝置管理嚴格。

(2.3).使用：

當運作使用時，如果有下列情形，密碼裝置應要求預防破解：

(i.) 裝置包含它或其它裝置已經使用的任何金鑰，或包含能獲得此金鑰的資訊。

(iii). 在裝置能夠重新安裝之前，無法偵測裝置的破解。

除了上述之外，應該要求所有高的機率能偵測裝置的破解。

一般而言，為了最小化預防破解的需求，裝置應該實作"每次交易唯一金鑰"之技術，使得裝置內包含的所有資料即使被揭露也不會提供任何能夠揭露該裝置已經使用之任何金鑰的任何資訊。

裝置管理應該預防或偵測裝置之未授權功能的更改，例如，裝置軟體的未授權的修改。因此當可以使用下載的方式時，應該包括一個鑑別軟體及／或資料的特定技術，此技術將保證僅有預定的下載的方式時，下載項目及已經由控制者及／或其代理鑑別且／或加密的項目才能夠被載入及安裝在裝置內。

對於某些型式的密碼裝置，其裝置管理可能要求預防誤用（例如調處）裝置，例如，如果裝置執行驗證個人識別碼（Personal Identification Number，簡稱PIN），其裝置管理可能要求預防未授權的裝置呼叫，避免藉由窮舉的試誤（Trail-and-error）確定 PIN。

(2.4). 使用後：

在使用後階段期間，如果密碼金鑰或其它敏感資料仍儲存在密碼裝置內，而且該裝置在使用週期要求預防破解，則密碼裝置應該要求預防破解。

(3). 生命週期保護方法：

生命週期的五個階段每一個皆有其獨具的特性。

(3.1). 製造：

在製造處理期間，製造者應該實作稽核與控制程序，使製造的裝置僅有預期之實體及功能的特性。應該有高的機率預防或偵測任何裝置實體保護機制的未授權的更改或任何裝置功能的增加或刪除，也應該有高的機率預防或偵測以偽造替代品取代裝置，例如藉由裝置的雙重控制。

(3.2). 製造後：

在此階段期間，稽核與控制程序應該實作成有高的機率預防或偵測裝置的未授權更改或以偽造替代品取代裝置。

載入一把或多把密鑰至專門使用對稱加密器的裝置，而這些密鑰係由外部產生再傳至裝置。使用非對稱加密器的裝置本身可以產生及保留密鑰，並且只揭露相對應的公鑰（為了金鑰載入處理）。無論金鑰產生的方法為何，應該以任何人都不能確定密鑰的方式來執行金鑰載入。

在起始金鑰載入之前，應確保裝置尚未受到未授權修改或替代，這可藉由下列方法達成：

(i.) 裝置的測試及／或檢驗。

(iv). 從製造或最近一次的裝置測試及／或檢驗之後，謹慎地稽核與控制裝置。

(v). 確認製造者為了確認裝置合法性的單一目的，而安裝的一把裝置唯一的秘密金鑰或資料的確存在裝置之內。

裝置管理應提供對偷竊或未授權移除裝置的偵測，一般而言，應在安全設施內進行起始金鑰載入。

(3.3). 使用前：

應將稽核與控制實作成偵測及預防任何可能揭露裝置之敏感金鑰的破壞，或任何裝置的未授權修改。就這些具有自動金鑰清除機制的裝置而言，此機制本身可能提供偵測的方法。任何為了確定金鑰或未授權修改的目的，而獲得存取裝

置的企圖應該導致清除金鑰，在初次企圖運作使用時，就應偵測其影響。一般而言，除非裝置金鑰最先被破解，否則正常的話是不可能以偽造替代品取代裝置。此外，替代的裝置不會包含正確的金鑰，當裝置初次代換運作使用時，將會偵測出此事實。

即使裝置有金鑰抹除機制，仍然會要求某種程度的稽核與外部控制，這是必須確保在足夠長的時間內對手無法利用該裝置，所謂足夠長的時間是指對手可能成功破解這些機制及確定金鑰，或者是略過這些機制、未授權修改裝置，然後裝回該裝置。

如果特定的密碼裝置易受到詐欺時，則在允許運作使用之前，裝置可以要求一個"解鎖碼（Unlocking Code）"的登錄，其中詐欺可能發生的原因是裝置安裝在未授權位置、由未授權人員安裝裝置或裝置長時間是無防備的。

裝置管理應該提供對偷竊或未授權移除裝置的偵測。

(3.4).使用：

裝置特性與裝置管理的組合應有高的機率預防對裝置的成功攻擊。

如果密碼裝置是在最低控制環境中運作，裝置的安全主要取決於裝置特性，裝置管理只是次要的。

適當設計的裝置未從裝置的運作位置被移除時，應不可能被破解，裝置管理應該藉由下列的方法提供偷竊或未授權移除的偵測：

(i.) 報告程序，使得裝置使用者依裝置控制者或其代理者的規定，及時報告遺失裝置。

(vi). 電子詰問（Electronic Interrogation）程序，主電腦（Host Computer）系統藉由該程序定期地詰問裝置，並由裝置送回的密碼鑑別回應（Cryptographically-Authenticated Response）確認此系統中裝置的運作狀態。

(vii). 稽核及控制程序，用以確認所有指定的裝置都在其預期的運作位置。

裝置的故障在任何時間都會發生，此事件可能要求裝置從服務進入裝置生命週期的"使用後"階後。如果有裝置撤離服務之後，並清除失效裝置的金鑰，則直到能夠確保裝置的實體或功能特性未被更改之前，置換金鑰（Replacement Key）不應該安裝在修復的裝置。如果密碼裝置輸出警告，指出已經發生故障且可能使裝置安全瀕於危險，則裝置應該立即撤離服務。

(3.5).使用後：

如果裝置進入使用後階段，並且打算在相同的組織再使用該裝置，則只要賦予該裝置使用時相同的保護型式（預防破解或破解偵測），就可以保留並仍然存在金鑰再次使用。

任何預期可能再使用的裝置在使用後階段至少要求破解偵測。

如果裝置為了修復而進入使用後階段，並且如果在修復期間無法預防或偵測金鑰破解，則應該清除所有金鑰。應該特別注意以確保修復處理不會導致裝置的未授權實體或功能修改。

為了修復及／或再使用而儲存之前，若清除裝置的金鑰，則只有當裝置已經免於未授權實體或功能修改時，新的金鑰才可以載入至裝置。一般而言，均要求在安全設施進行金鑰置換。

當裝置撤離服務，而且組織內並無意恢復裝置的服務時，直到清除或毀壞裝置金鑰以前，裝置該具有運作使用期間需求相同的保護型式。這時能將裝置轉送給其它組織，並且進入生命週期中的使用前階段；或是裝置必須是實體損壞，使得裝置無法恢復服務。如果在其它方面無法保證意外或蓄意都將無法載入金

鑰至裝置並且恢復服務，或裝置被當成一個偽造替代品，則應該選擇此技術。然後，能以任何方法處理該裝置。

如果無法清除或毀壞裝置的金鑰，則應該實體毀壞裝置，使得不可能破解金鑰或其它敏感資料。

(4). 可歸責性（Accountability）：

在裝置生命週期的每個階段，個體（一個人或一群人）應該對裝置負責，針對適當的生命週期階段，可歸責的個體應該了解及實作相關標準的需求。一般而言，對實體裝置的管理及裝置邏輯安全管理的可歸責性，可歸責到不同組織中不同的人。

負責整體安全的組織應該以書面方式明確規定參與裝置管理的每個個體之責任。應該準備一個稽核核對表列，使得能夠評估是否遵循這些需求。

獨立的稽核員可以是組織內部或外部的人員，稽核員應該定期地使用稽核核對表列確定所有的裝置管理需求正能符合組織的需求，並且確定負責的人適當地履行他們的職責。

對每個生命週期階段，應該維護可歸責性記錄以顯示每個裝置的位置及狀態。這些記錄應該可識別歸責的個人。當將裝置轉送給其它組織時，其他人變成該裝置可歸責的人。所以起始及接收兩端組織的記錄應該識別裝置，並且指示轉送日期、從那個組織轉送到那個組織、轉移的方法及轉移過程中所使用的保護方法（例如，安全轉送者(Secure Courier)、破壞存跡防偽包裝(Counterfeit-Resistant Tamper-Evident Packaging）。應該有某些方法確認接收的組織已經同意可歸責性，而且在轉送的組織之紀錄中應該包括目前被轉送裝置之可歸責的人名。

(5). 稽核與控制的密碼裝置管理原則：

稽核與控制是密碼裝置管理非常重要的部分，表 4.11 彙總一些關於稽核與控管程序的一般原則，並指示稽核與控管程序在裝置生命週期之每個階段的適用性。

根基於表 4.11，ISO 制定規範性（Normative）之安全密碼裝置符合性查檢表如表 4.12~表 4.19 所示；同時提供表 4.20 的參考性（Informative）之安全密碼裝置符合性查檢表供使用者參考。

表 4. 11：稽核與控制原則

程序		生命週期階段				
		製造	製造後	使用前	使用	使用後
1	負責裝置的一個人或一群人	M	M	M	M	M
2	小心查核或控制對最低控制環境中之裝置作存取的人員	M	M	M	M	M/R
3	小心查核或控制對控制環境中之裝置作存取的人員	M	M	R	NA	M/R
4	控制製造處理以確保裝置（僅）包括合法之實體及功能的特性	M	NA	NA	NA	NA
5	以破壞存跡防偽包裝之裝置的控制機制或彌封（seal）來預防未偵測出的裝置存取	NA	M	R	NA	R
6	稽核與核對表列的準備與使用	M	M	M	M	M
7	由合格的人員適時地驗證是否正確填寫稽核核對表列	R	R	R	R	R
8	依適當的國際標準規定實作金鑰管理程序	NA	M	M	M	M
9	利用電腦化或人工書面記錄正確追蹤每一個裝置	M	M	M	M	M
10	以書面程序預防裝置的偷竊或未授權存取，當裝置運作使用時要求預防破解	NA	NA	M	M	M
11	裝置文件分送的控制	R	R	R	R	R
12	運作裝置的定期電子詰問，以密碼方式確認裝置依然在運作位置	NA	NA	NA	R	NA
13	以書面報告程序適時偵測出裝置從儲存器或運作位置遭未授權移除，或偵測出裝置於轉移時不知去向	R	M	M	M	M
14	以書面報告程序預防金鑰在運作使用之後存留在遺失的或永不服務的裝置內，例如中央控制金鑰	NA	NA	M	M	M
15	如果為了修復而將裝置搬離其運作位置且修復期間不能預防或偵測金鑰破解，則清除金鑰	NA	NA	NA	NA	M
16	如果裝置永久撤離服務，且裝置內含已經使用在加密仍屬秘密的資料之金鑰（即裝置要求預防破解），則清除金鑰	NA	NA	NA	NA	M
17	如果裝置永久撤離服務，且其內含不是在所有能與裝置密碼通訊之設施都無效的金鑰，則清除金鑰	NA	NA	NA	NA	M
18	為了在運作使用中裝置要求預防破解，除非已經清除金鑰，否則在裝置撤離服務之後，控制該裝置的預防破解	NA	NA	NA	NA	M
19	為了維護裝置的機密性，要求控制維護處理	NA	NA	NA	NA	M/R
20	控制修復處理或修復之後的檢驗／測試以確保裝置已經不易受到未授權修改	M	NA	NA	NA	M

M：必備　　R：建議
NA：不適用　　M/R：當要求預防破解時必備，否則為建議

表 4. 12：安全密碼裝置共同特性符合性查檢項目

分類		查檢項目
一般	一般安全特性	5
	破壞存跡特性	1
	抗破壞性特性	2
	破壞回應特性	6
邏輯安全特性	邏輯安全特性	17
裝置管理	一般考量	6
	製造者的裝置保護	2
	製造者和使用前的裝置保護	4
	使用前及安裝前的裝置保護	1
	安裝後的裝置保護	5
	停止服務後的裝置保護	3
備考：所有安全密碼裝置均須查檢共同特性之符合性查檢項目。		

表 4. 13：具備 PIN 登錄功能之安全密碼裝置符合性查檢項目

分類		查檢項目
裝置特性	實體安全特性	7
	邏輯安全特性	12
裝置管理	起始金鑰載入期間 PIN 登錄的裝置保護	2
	安裝後的 PIN 登錄裝置保護	2

表 4. 14：具備 PIN 管理功能之安全密碼裝置符合性查檢項目

分類		查檢項目
裝置特性	實體安全特性	1
	邏輯安全特性	11
裝置管理	裝置管理	8

表 4. 15：具備訊息鑑別功能之安全密碼裝置符合性查檢項目

分類		查檢項目
邏輯安全裝置特性	邏輯安全裝置特性	6

表 4. 16：具備金鑰產生功能之安全密碼裝置符合性查檢項目

分類		查檢項目
裝置特性	實體安全特性	1
	邏輯安全特性	9
裝置管理	裝置管理	8

表 4. 17：具備金鑰轉送與下載功能之安全密碼裝置符合性查檢項目

分類		查檢項目
裝置特性	實體安全特性	1
	邏輯安全特性	7
裝置管理	裝置管理	14

表 4. 18：具備數位簽章功能之安全密碼裝置符合性查檢項目

分類		查檢項目
一般考量	一般考量	1
裝置管理	裝置管理	1
備考：「除共同特性」外，表 4.16「具備金鑰產生功能」之安全密碼裝置符合性查檢項目亦為必須查檢項目。		

表 4. 19：環境面之安全密碼裝置的參考用符合性查檢項目

分類	查檢項目
最低限度之受控環境	3
受控環境	5
安全環境	9

一個密碼系統的安全等級是環境安全等級與密碼裝置安全等級的結合，圖 4.22 是此安全等級之示意說明，其中水平軸是密碼裝置的安全等級，垂直軸是環境的安全等級，白色的區域表示可接受的密碼系統安全，灰色三角形的區域表示無法接受的安全，灰色的邊緣表示最低可接受的界限，說明如后：

(1). 點 A 表示裝置安全超過其運作環境所需的最低需求之密碼裝置。
(2). 點 B 表示裝置安全符合其運作環境所需的最低需求之密碼裝置。
(3). 點 C 表示裝置安全是不適當的且未符合其運作環境所需的最低需求之密碼裝置，虛線表示將裝置移至安全較高的環境，在此環境內裝置安全是適當的。
(4). 交點 X 表示裝置安全適足以使裝置在未具安全的環境下運作。
(5). 交點 Y 表示環境安全足以供未具安全的裝置運作。

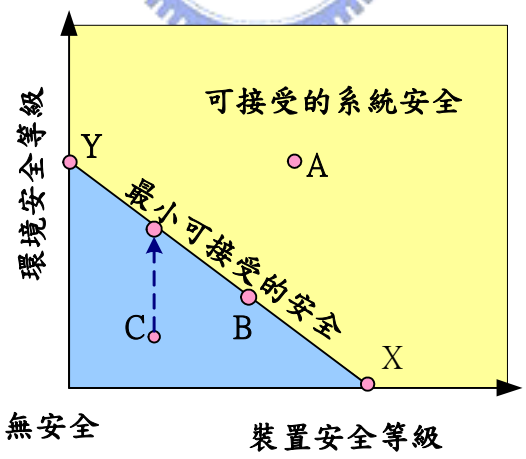


圖 4.22：密碼系統安全等級示意說明

代表密碼裝置安全等級的水平軸實際是由裝置的邏輯與實體安全特性組成，可以進一步將實體安全特性分成如圖 4.23 與圖 4.24 所示之 3 類實體安全之間的 3 維關係（Three Dimensional Relationship）。

(1). 破壞存跡特性。
(2). 抗破特性。
(3). 破壞回應特性。

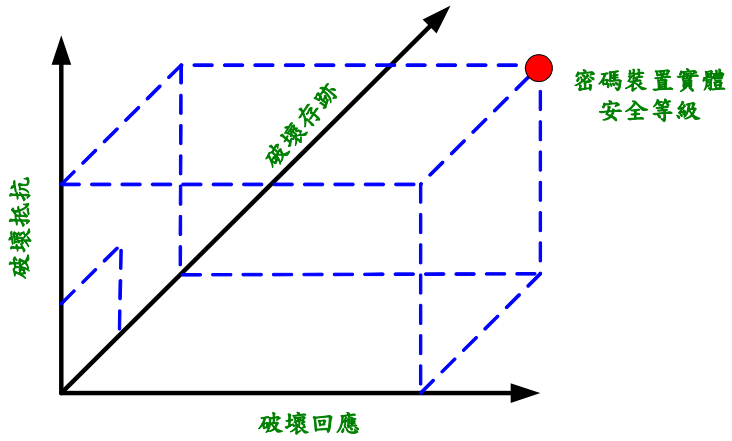


圖 4.23：密碼裝置實體安全等級示意說明之一

情況 I：顯示具抗破壞與回應特性但無破壞存跡特性的裝置之 2 維最低可接受的安全界限。

情況 II：顯示抗破壞與存跡特性但無破壞回應特性的裝置之 2 維最低可接受的安全界限。

情況 III：顯示抗破壞存跡與回應特性但無抗破壞回應特性的裝置之 2 維度的最低可接受的安全界限。

情況 IV：顯示兼具 3 類實體安全特性的裝置之 3 維最低可接受的安全界限。

將三類實體安全特性併入一個單一軸成為實體安全特性，並相對繪製裝置的邏輯安全特性。圖 4.25 顯示結合後之實體安全特性與邏輯安全特性之間的關係。

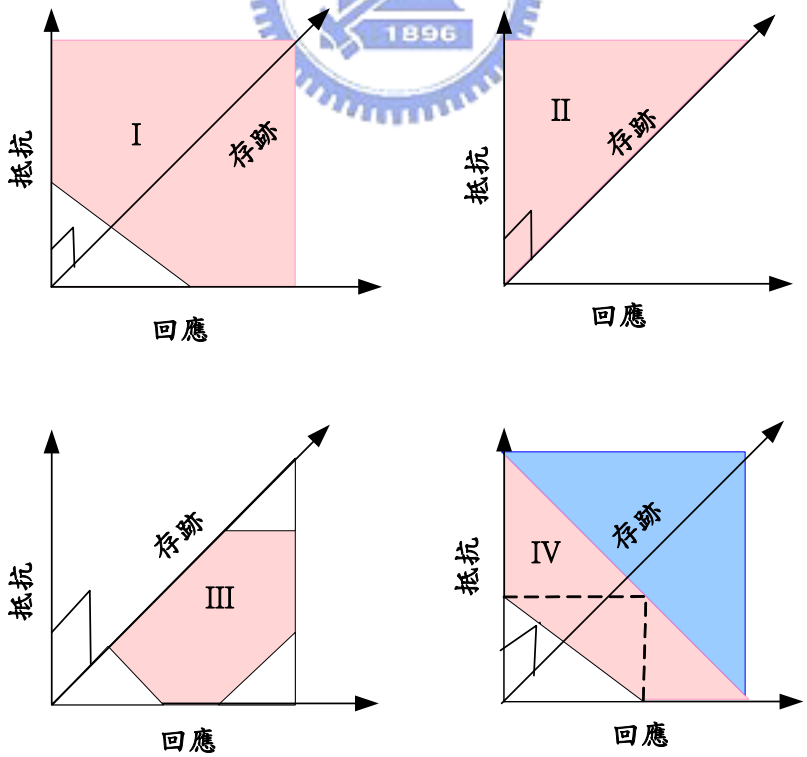


圖 4.24：密碼裝置實體安全等級示意說明之二

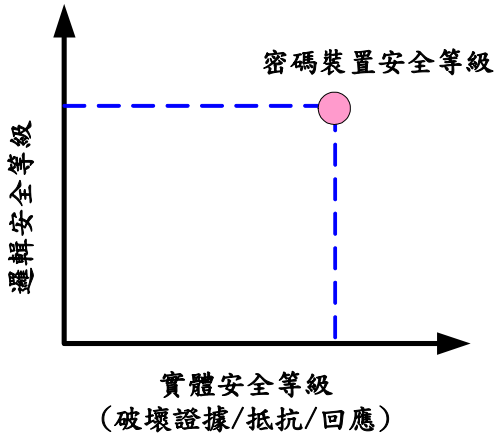
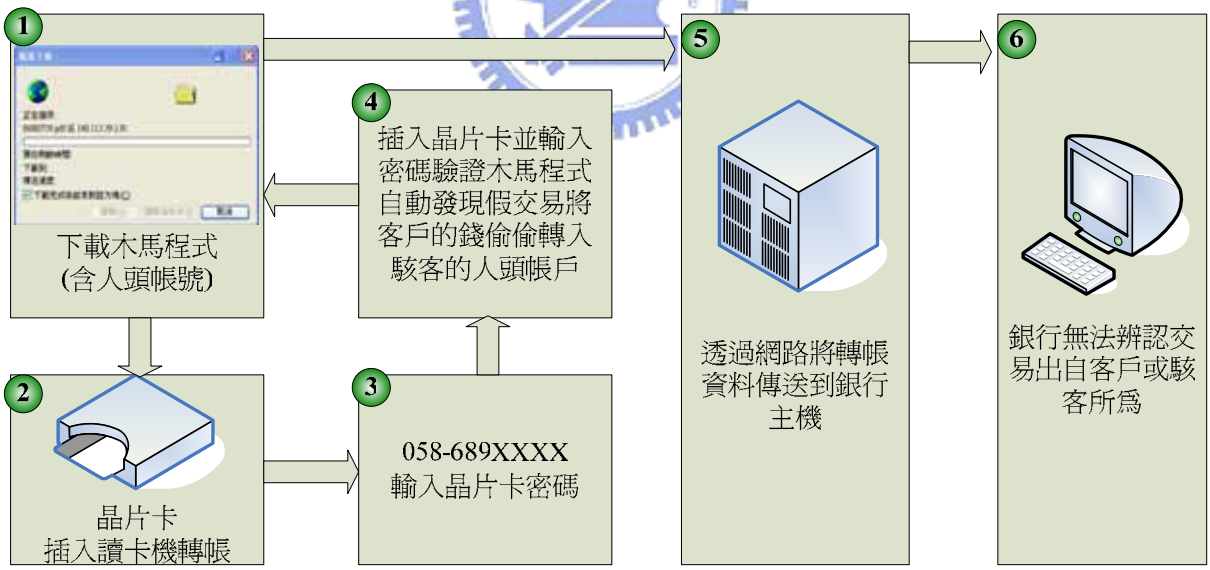


圖 4.25：密碼裝置安全等級示意說明

邏輯安全特性與 3 類實體安全特性併入一個單一軸成為裝置安全等級，如圖 4.25 所示，裝置安全等級與對應的環境安全等級決定整體安全是否將在可接受的系統安全內，在最低可接受的安全界限或系統安全是否不適當。2005 年 10 月 17 日，報載我國 2003 年 9 月至 2004 年 6 月方啟用之晶片金融卡密碼裝置，如圖 4.26 所示，疑已遭破解，其原因即為不遵循 ISO/IEC 13491 的要求，允許使用者直接經由個人電腦等終端設備鍵入 PIN 而遭破解。換言之，我國晶片金融卡的密碼裝置因讀卡機之脆弱性，其安全等級並不適當；「一葉知秋」，如何善用並遵循已有的「密碼技術及其應用規範」已是我國宜嚴肅面對之課題。



說明：

1. 資料來源：2005 年 10 月 17 日，聯合報 A10，記者陳一雄、吳雯雯/台北報導。
2. 消費者於網路銀行自動櫃員機(Automatic Teller Machine，簡稱 ATM)，使用第一代晶片金融卡讀卡機時，並無防護「電子商務木馬屠城」之假交易轉帳的安全功能。
3. 上述晶片金融卡讀卡機之脆弱性，於第二代晶片金融卡讀卡機已加強安全功能。

圖 4.26：網路銀行自動櫃員機(Automatic Teller Machine，簡稱 ATM)之木馬屠城計示意圖

根基於表 4.12~表 4.19，安全密碼裝置之查檢項目不在此一一列舉，僅針對破壞存跡特性、抗破壞特性與破壞回應特性的安全密碼裝置之安全符合性表列總結格式整理如表 4.20~表 4.22 所示，其中稽核員必須明確表示是（T）、否（F）或是不適用（N/A）。一個「否」的答案不必然是不可接受之實作，僅是表示受稽單位必須書面解釋；「不適用」的聲明，受稽單位亦必須提出書面解釋。

表 4. 20：安全密碼裝置破壞存跡特性之稽核安全符合性表列

編號	安全符合性聲明	T	F	N/A
1	該裝置被設計和建構以致不可能滲透該裝置為了： -- 對該裝置的硬體或軟體增加，替代，或修改 (例如：竊錄器的安裝)；或 -- 決定或修改任何敏感資訊 (例如：個人識別碼，存取密碼(Access Code)，及密碼金鑰) 然後再重新安裝該裝置，無需取得專門技巧和一般無法取得的設備，且： 1) 沒有造成被高度偵測到的裝置損壞，或 2) 造成該裝置從原來位置消失的時間太長以致於它的消失或再現被偵測到。			

表 4. 21：安全密碼裝置抗破壞特性之稽核安全符合性表列

編號	安全符合性聲明	T	F	N/A
1	藉由實體保護的程度該裝置被保護以避免滲透。			
2	在獲得對該裝置不受限的，不被阻擾的存取，發現該標的裝置中之機密資訊是不可能的。			

表 4. 22：安全密碼裝置破壞回應特性之稽核安全符合性表列

編號	安全符合性聲明	T	F	N/A
1	該裝置被保護以避免滲透藉由包括可偵測任何企圖破壞該裝置的特徵且在偵測到時造成所有密碼金鑰和敏感資料立即消除。			
2	無論授權或未授權移除該裝置內部組件、機殼或通道的任何存取登錄會造成該裝置中所存的密碼金鑰自動且立即消失。			
3	當該單位永遠無法運作時有一個明確的方法以確保被使用於加密機密資料的機密資料或任何密碼金鑰會被從該單位除去。有一個明確的方法以確保，當該單位永遠無法運作時，任何該單位中未來可能被用的密碼金鑰不是從該單位移除就是在所有該單位能執行密碼保護通訊的設施中無效。			
4	即使沒有應用電源的狀況任何破壞偵測/金鑰抹除的機制仍會運作。			
5	如果該裝置沒有移動的安全偵測機制，那麼就不可能擊敗破壞偵測機制，或發現目標裝置中的機密資訊，即便被從操作環境中移除。該裝置的損害應需要目前無法取得之設備和技巧。 備考：例如，這些資訊的發現需要一定的時間，如一個月的準備 – 也許包括其它裝置的分析 – 及在獲得對該裝置不受限的，不被阻擾的存取後需至少一週的努力去損害該裝置。			
6	如果該裝置有移動的安全偵測機制，那麼就不可能擊敗破壞偵測機制，或發現目標裝置中的機密資訊。該裝置的損害應需要目前無法取得之設備和技巧；和在裝置地無法取得也無法輕易傳送到裝置地點之設備。 備考：例如，這些資訊的發現需要一定的時間，如一個月的準備 – 也許包括其它裝置的分析—和至少十二小時對該裝置不受限的，不被阻擾的存取。			

綜上所述，密碼模組因應用之不同，一個資訊系統使用的「安全密碼裝置」其查檢項亦不相同，以銀行業之零售式安全密碼裝置為例，如表 4.12~表 4.19 所示，諸如表 4.20~表 4.22 等均宜具備相當之深層知識，方能克盡職責。

五、密碼技術及其應用之管制現況：

5.1、前言：

新新聞周報於 604 期報導：「1998 年 9 月 22 日海基會秘書長許惠祐先生在啟程訪問大陸三天的行程中，某位官員在出入重要場合時都會攜帶一個外型與一般公事包無異的手提箱，據說這是防止外界竊聽專用的高科技裝備。國家安全局局長殷宗文上將曾在一項茶會中向記者透露，其實那是一種能對傳真或電話訊息重新「製碼(Encoding)」的儀器，以防止外界竊聽或截收傳真機以及電話之內容，即使截收到了，也是一堆無法讀取的亂碼，只有透過另一台同型的裝備，才能對訊息解碼；另一方面，殷局長也不諱言，為了切實執行「機關保防」工作，國安局已經為所有政務次長以上官員，加裝電話加(解)密器，使外界無法透過監聽得知官員們的通話」，自無線通信問市以來，由於大氣層是其儲存媒體之一，如何確保通信安全就是關鍵技術研發要項中之一環，1993 年 4 月 29 日在美國眾議院電信與財經委員會主席麻塞諸塞州眾議員愛德華馬基(Edward J. Markey)先生主持的聽證會中，下村勤(Tsutomu Shimomura)先生使用剛從超商買來的全新且未被拆封的行動電話，在兩分鐘內改裝成行動電話監聽器的示範更是震驚了美國的立法者。時至今日，通信設備內嵌密碼模組已日益普及，在公元 2000 年實施之第三代行動電話之國際行動通信(International Mobile Telecommunications 2000，簡稱 IMT 2000)於安全管理需求中，已明文要求下列七項安全功能事項均須處理：

(1).鑑別(Authentication)
(2).隱私與匿名(Privacy and Anonymity)
(3).機密性(Confidentiality)
(4).完整性(Integrity)
(5).授權與存取控制(Authorization and Access control)
(6).事件的管制(Event limitation：denial of access to particyular services)
(7).事件的報告(Event reporting)

Source：ITU-R Rec. E. 168：Security Principles for Futher Public Land Mobile Telecommunication Systems

一般而言，產業界均使用密碼模組設計完成滿足 IMT2000 安全管理需求的第三代行動電話通信系統中【57】；其實密碼學的應用可以上溯至中世紀，並且攸關國家安全，目前更是數位時代資訊社會安全的礎石【89】。世界各國基於國家安全與外交政策等原因，大多實施科技管制措施，限制具有潛在軍事用途的產品之移轉與再移轉。我國貿易法第十三條明文規定：「戰略性高科技貨品由主管機關會商有關訂定辦法管理。」一般而言，為確保國家安全，履行國際合作與協定，大多數的國家均會加強戰略性高科技貨品之輸出入與流向，國際間科技管制如圖 5.1 所示，主要是以傳統武器與大規模毀滅武器來區分【26, 30, 82~83, 100】，密碼學及其應用技術屬於傳統武器。

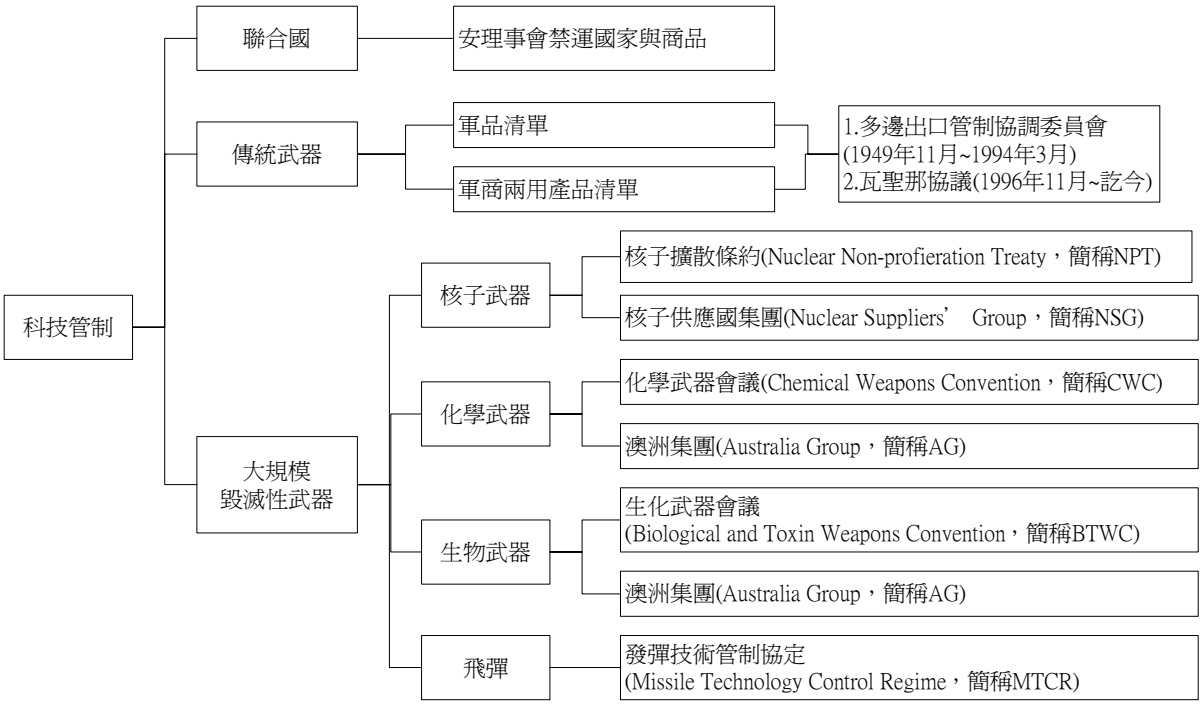


圖 5.1：國際科技管制組織框架

5.2、聯合國安全理事會與國際高科管制：

安全理事會（以下簡稱安理會）是聯合國六大機構之一，根據聯合國憲章，安理會的主要任務是維護國際和平與安全。安理會由十五國理事組成，包括（英、法、美、俄、中國）五個常任理事國與十個由大會選出、任期兩年的理事國。

根據聯合國憲章，安理會之主要職能為：

(1). 依照聯合國之宗旨與原則來維護國際和平及安全；
(2). 調查可能引起國際摩擦的任何爭端或局勢；
(3). 建議調解這些爭端的方法或解決條件；
(4). 制定計劃以處理對和平之威脅或侵略行為，並建議應採取的行動；
(5). 促請各國會員實施經濟制裁和除使用武力以外的其他措施以防止或制止侵略；
(6). 對侵略者採取軍事行動；
(7). 就接納新會員國以及各國加入＜國際法院規約＞的條件提出建議；
(8). 在「戰略地區」行使聯合國的托管職能；
(9). 就秘書長的任命向大會提出會議，並與大會共同選舉國際法院的法官。

為維持國際和平防止侵略，安理會對具有威脅或侵略行為之國家實施不同程度之武器禁運與經濟制裁，這些國家包括：南非、伊拉克、利比亞、索馬利亞、海地、安哥拉、盧安達、賴比瑞亞、蘇丹、獅子山國、前南斯拉夫、南斯拉夫共和國（含科索伏）、阿富汗、伊索匹亞【82~83, 100】。

聯合國安理會在 2001 年 9 月 28 日晚間快馬加鞭，十五個理事國一致通過美國提案，決議要求全球各國切斷支持恐怖份子的財源及其他後勤支援。據悉美國新任大使 9 月 27 日才向安理會提出此一決議案，結果在不到 24 小時後即在安理會獲得一致通過，距離美國受 911 恐怖攻擊還不到 3 星期，這在安理會史上是罕見的例子。決議文並引用聯合國憲章第七章，因此對所有 189 個會員國具有強制約束力。該章規定，凡不遵守聯合國安理會決定的國家，將受到經濟及外交制裁，甚至武力對付。安理會譴

責此次恐怖攻擊行動，認為是「對國際和平與安全的威脅」。在安理會通過的決議案下，聯合國所有會員國均有法律義務「防止及取締資助恐怖份子的行為。」決議文中要求各國必須遵守的義務包括：為恐怖活動籌募資金，無論直接或間接，都列為犯罪行為；立即凍結恐怖份子與恐怖組織資產及經濟來源；禁止主動或被動對恐怖份子提供任何形式的支持；禁止本國國民或在其境人的任何人向恐怖份子提供經費或服務；不得給予資助、策劃、支持或從事恐怖活動者安全庇護，亦不得庇護窩藏這些人的人；有效管制邊界，做好護照及身分證明文件的管理；盡最大努力合作調查恐怖活動，盡力將恐怖份子交付法律制裁等【26, 82】，密碼學及其應用技術亦在其範疇內。

5.3、多邊出口管制協調委員會：

密碼方法的出口長久以來一直是有限制的。很明顯的，政府想要避免有力的密碼方法落入外國政權之手，因為如此一來將妨害其情報工作之能力。密碼方法一直被視為是一種武器，佔軍用品出口表單中的重要地位。在出口控制的主要國際協議於美蘇兩大集團冷戰時是多邊出口管制協調委員會（Coordinating Committee for Multilateral Export Control；簡稱 COCOM）的條約。

二次世界大戰後，蘇聯大力扶植東歐各國成立共產政權，威脅西方盟國之安全。美國與西歐諸國於 1949 年 4 月 4 日成立北大西洋公約組織（North Atlantic Treaty Organization，簡稱 NATO），以防禦蘇聯、東歐等共產集團國家。美國為防止以其為首之自由世界國家將具有戰略價值之科技產品與技術輸出或轉運至以蘇聯為首之共產集團國家，於 1949 年 11 月 22 日，邀集北大西洋公約組織之美國、荷蘭、比利時、盧森堡、英國、法國與義大利等七國，成立多邊出口管制協調委員會（Coordination Committee for Multilateral Export Control，簡稱 COCOM）。從 1950 年 1 月開始運作，COCOM 將密碼學及其應用技術視為軍商兩用（Dual-Use）科技，並加以管制。

COCOM 成立之目的是彌補 NATO 之不足，故其防衛對象亦與 NATO 相同－蘇聯、東歐共產集團、北韓、越共、中華人民共和國等。COCOM 會員國從最初成立的 7 國，主要會員為 NATO 國家（冰島除外），加上日本；經過數次擴增，結束時已有：澳大利亞、比利時、加拿大、丹麥、法國、德國、希臘、義大利、日本、盧森堡、荷蘭、挪威、葡萄牙、西班牙、土耳其、英國、美國 17 個會員國。

COCOM 之「出口管制」並非禁止出口，而是藉由各國之行政力量來管制某些產品之最終流向及用途的管制責任；即由出口國移轉給進口國，若有再出口或轉出口的情形，則管制責任再由原進口國移轉給下一個進口國。因此，科技產品的出口管制乃是透過國際間管制責任的傳承，對於某些特定產品的最終流向和用途加以限制，以達到維護國際政治、社會及經濟的安全與繁榮。

COCOM 過去是一個為戰略性產品與技術資料，由國家會員出口至禁制目的地相互控制的國際組織。其法規之主要目的是預防武器與軍需品被出口到「危險」的國家—通常是與恐怖組織維持友善關係的國家，像利比亞、伊拉克、伊朗和北韓。COCOM 管制之科技產品，雖然通常需要有授權許可，一般是可以出口至其他國家的。COCOM 保有國際產業表（International Industrial List）與國際軍需表列（Internation Muitions List）及其他表列。

雖說過去各種密碼方法均受管制（Regulated），唯在 1989 年時，COCOM 解除了通行碼（Password）與純鑑別（Authentication-only）之密碼學及其應用技術的管制。1989 年時，COCOM 決定容許大眾市場（Mass-market）密碼軟體（包括公開領域軟體(Public-domain software)的出口。COCOM 的多數會員國遵循其規定，但有些，像德國與美國，仍維持個別管制。

COCOM 於 1994 年 3 月解散，在新條約未簽訂前，多數 COCOM 會員原則上同意維持現狀，且密碼學及其應用技術方法仍在出口管制名單中。1995 年，有 28 個國家決定建立 COCOM 的後繼者，就是對傳統武器及軍商兩用用途產品與技術之出口管制的瓦聖納協議。條約的協商在 1996 年 7 月完成，並由 31 個國家簽署。瓦聖納協議管制武器及可以作為軍事與一般用途的軍商兩用產品之出口，密碼學及其應用技術方法即為此類軍商兩用產品。我國自 1993 年起，遵循 COCOM，實施高科技貨品出口管制。

5.4、瓦聖納協議（Wassenaar Arrangement，簡稱 WA）：

在冷戰結束之後，1949 年 11 月 22 日由北大西洋公約組織發起之多邊出口管制協調委員會(Coordinating Committee for Multilateral Export Control，稱稱 COCOM)出口管制組織的會員國認為東西方對峙的觀點已不適合做為出口管制的基礎，有必要成立新的協定來處理國際和區域安全與穩定相關的武器和軍商兩用產品與技術之出口管制。1993 年 11 月在海牙舉行的第 16 屆高峰會議（High Level Meeting，簡稱 HLM）中，17 個 COCOM 會員國的代表同意結束 COCOM，成立新的多邊協定，暫時取名為「新論壇（New Forum）」。1994 年 3 月 29-30 日在荷蘭海牙附近的瓦聖那（Wassenaar）召開的 HLM 高峰會（Further HLM）確認上述決策，COCOM 在 1994 年 3 月 31 日正式結束，參加國（Participating States）也同意繼續採用 COCOM 的管制清單做為各國出口管制的基礎。同時，以前 COCOM 的合作國（Cooperating countries），澳地利、芬蘭、愛爾蘭、紐西蘭、瑞典、瑞士，將成為「新論壇」的參加國。為儘速成立新的協定，HLM 成立了 3 個工作小組（Work Groups），第一個工作小組負責研擬新協定的目標、規則與程序，第 2 個工作小組的任務是研擬應納入管制的產品和技術清單，第 3 個工作小組則負責處理行政事務。

在 1995 年 9 月 11-12 日的 HLM 中蘇聯、捷克、匈牙利、波蘭和斯洛伐克也加入成為會員國。在 1995 年 12 月 19 日在瓦聖那的 HLM 中，決議成立「瓦聖那協議」（The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies，簡稱 Wassenaar Arrangement, WA）。同時決議在維也納成立秘書處（Secretariat），並組成籌備委員會（Preparatory Committee of the Whole）籌備第一次的會員大會（Plenary meeting）。

1996 年 4 月 2-3 日在維也納召開瓦聖那協議籌備會議，南韓和羅馬尼亞也加入成為創始會員國。然而因有多項議題無法達成共識，大會決定暫緩召開，以爭取時間解決若干重要議題之歧異問題。

1997 年 7 月 11-12 日高峰會議再度召開，保加利亞和烏克蘭加入，總計有 33 個創始會員國，會中達成共識，通過「創會要點」（Initial Elements），並建立新的管制清單和資訊交換機制，自 1996 年 11 月 1 日開始實施，在 1996 年 12 月 12-13 日在維也納召開瓦聖那協議第一次會員大會，此後固定在每年 12 月召開大會，檢討管制與審核管制清單，我國自 1995 年 7 月開始遵循 WA，實施高科技貨品出口管制。

WA 是由工業化國家團體所決議的協議，目前有 35 個會員國，這是為了限制傳統武器與“軍商兩用”技術出口至被認為是危害世界和平之國家或地區以及一特定的其他國家。

瓦聖那協議採無歧視之開放原則，凡符合入會資格之國家均得申請入會，其參加國審核入會資格係以下列因素做為該國對協議成立宗旨之貢獻：

(1). 是否為武器或工業設備之生產國或出口國；

(2). 是否將反擴散政策（Non-Proliferation Nolicies）各管制項目納入國家政策各相關法規中。
(3). 奉行完整有效的出口管制。
申請入會國經全體參加國同意，始成為參加國，表 5.1 是 2004 年 8 月 25 日之 WA 參加國表列【30】。

表 5. 1：瓦聖那協議之參加國

阿根廷	Argentina	冰島	Iceland	羅馬尼亞	Romania
澳大利亞	Australia	愛爾蘭	Ireland	俄羅斯	Russian Federation
奧地利	Austria	義大利	Italy	斯洛伐克	Slovak Republic
比利時	Belgium	日本	Japan	南非	South Africa
巴西	Brazil	韓國	Republic of Korea	西班牙	Spain
保加利亞	Bulgaria	拉脫維亞	Latvia	瑞典	Sweden
加拿大	Canada	盧森堡	Luxembourg	瑞士	Switzerland
捷克	Czech Republic	荷蘭	Netherlands	土耳其	Turkey
丹麥	Denmark	紐西蘭	New Zealand	烏克蘭	Ukraine
芬蘭	Finland	挪威	Norway	英國	The United Kingdom
法國	France	波蘭	Poland	美國	The United States
匈牙利	Hungary	葡萄牙	Portugal		

瓦聖那協議之成立是為了促進區域和國際之安全與穩定，提倡以透明化和更高的責任來管制傳統武器和軍商兩用產品與技術之移轉，以避免不當之使用。參加國將尋求透過其國家政策來確保上述項目之移轉，不會助長有損安全與穩定之軍事力量，也不支持該軍事力量的擴張。瓦聖那協議將補充並強化，但不重覆，現有大規模毀滅性武器及推進系統之管制組織，及其他國際認可的評量，以促進管制之透明化與責任的加強，針對足以威脅區域和平與安全之武器與精密軍商兩用產品與技術的移轉。瓦聖那協議也將加強合作，以避免武器和精密軍商兩用產品項目被購買做為軍事用途，如果此情況發生在某地區，或某國家有此行為發生，將受到其他參加國之嚴重關切。瓦聖那協議要求：
(1). 參加國必須針對如表 5.2 所示之軍商兩用貨品清單與表 5.3 所示的軍用貨品清單之所有產品項目進行管制【82】，以避免未經許可之移轉或再移轉。
(2). 軍商兩用產品與技術清單（tier1）有兩個敏感項目附件（tier2）和若干非常敏感項目（sub-set tier2）。
(3). 管制清單定期審核，以反映科技發展和參加國之經驗，以及軍商兩用產品與技術之固有軍事能力。

密碼學及其應用技術屬於瓦聖那協議軍商兩用貨品第五類之第二部分與軍品清單之第 21 項（ML21）【82】，1999 年 12 月 1~3 日 WA 第 5 次會員大會討論同時兼顧安全、科技發展與子商務之現代化加密技術管制之議題，WA 參加國同意針對清單上所列的「軟體（Software）」與「技術（Technology）」，同時包含無形移轉（Intangible Transfers）之管理加以廣泛控制是重要的。在另一方面，參加國也同意以政治／機構層次等進行採購活動（Acquisition Activities）、出口政策（Export Policy）、相關計畫（Projects of Concerns）等資訊交換，以避免重複；同時經由平行或合作方案，以促進調和一致【30】。

WA 對於遵從出口管制準則的其他國家是全球開放的。要被協議接納的國家必須：（1）生產及（或）出口武器或雙重用途工業設備者（2）維護防止擴散政策即適當的國家政策，包括遵循國際防止擴散制度與條約（3）維護完整有效的出口管制。雖然協議並未提供觀察員身分，但有規劃一個外延的政策以通知非會員國有關 WA 之目的與活動，並鼓勵這種非會員在於傳統武器與雙重用途技術，包括密碼學及其應用技術方法的出口上，採納符合 WA 的國家政策。

表 5. 2：WA 之軍商兩用貨品清單表列

第一類：尖端材料	Category 1 － Advanced Materials (http://www.wassenaar.org/list/Cat1-99.pdf)
第二類：材料加工程序	Category 2 － Materials Processing (http://www.wassenaar.org/list/Cat2-9.pdf)
第三類：電子	Category 3 － Electronics (http://www.wassenaar.org/list/Cat3-99.pdf)
第四類：電腦	Category 4 － Computers (http://www.wassenaar.org/list/Cat4-99.pdf)
第五類：電信及資訊安全	Category 5 － Part1-Telecommunications (http://www.wassenaar.org/list/Cat5P1-99.pdf) Category 5 － Part2- Information Security (http://www.wassenaar.org/list/Cat5P2-99.pdf)
第六類：感測器及雷射	Category 6 － Sensors & Lasers (http://www.wassenaar.org/list/Cat6.99pdf)
第七類：導航及航空電子	Category 7 － Navigation & Avionics (http://www.wassenaar.org/list/Cat7.99pdf)
第八類：海洋技術	Category 8 － Marine (http://www.wassenaar.org/list/Cat8.99pdf)
第九類：推進系統	Category 9 － Propulsion (http://www.wassenaar.org/list/Cat9.99pdf)
附件一	Annex1
附件二	Annex2

表 5. 3：WA 之軍品清單表列

ML1：小型武器	ML11：電子裝備
ML2：大口徑兵器或武器	ML12：動能武器系統
ML3：彈藥	ML13：裝甲裝備及結構
ML4：炸彈、魚雷、火箭及飛彈	ML14：軍事訓練及裝備
ML5：射控設備	ML15：影像及反制裝備
ML6：車輛	ML16：鍛造、鑄造及未經加工產品
ML7：毒劑、崔激瓦斯彈等	ML17：雜項設備、材料及圖書資料
ML8：軍用火炸藥	ML18：設備及技術
ML9：戰艦	ML19：聚能武器系統
ML10：戰機	ML20：低溫及超導設備
	ML21：軟體
	ML22：技術

在 1998 年 12 月 3 日，瓦聖納協議的秘書處宣布已將世界經濟合作發展組織（Organization for Economic Cooperation and Development，簡稱 OECD）於 1997 年 3 月 27 日公布之密碼指導原則加到協議中。瓦聖納軍商兩用管制清單現行將加密軟硬體密碼產品擴張至 56 bit 以上，包括全球資訊網瀏覽器、電子郵件應用、電子商務伺服器、以及防電話竊聽設備。其他超過 64 bits 的強勢大眾市場產品，例如個人電腦作業系統、文書處理、與資料庫程式只受兩年的管制。這些管制必須重新被更新且一致同意，否則他們將被取消。雖然對於清單中 56 bits 與 64 bits 加密間的差異仍然還是覺得混淆，但這卻指明參與國有責任對使用超過 64 bits 長金鑰的"大眾市場"加密軟體建立新的出口管制。除非正式出口許可被相關國家政府所發行，他們也必須限制其他使用超過 56 bits 長金鑰的對稱性加密軟硬體。

簽署瓦聖納協議國家也同意管制其他 56 bits 層級的軟體，例如是用於某些特定領域，包括銀行、保險與保健。至於依法取用（Lawful Access）方面，並未接受美國之提議僅支持由民間機構自己統理的金鑰回復（Key Recovery）之管制措施，根據德國經濟部所發表的新聞說，「已開始要求對金鑰託管（Key Escrow）產品有特殊處置的某些國家已經不成功了，這可以在美國與英國見得到。因此，加密技術的管制將依舊是不將金鑰存放在政府機構。」這些管制不應用至保護智慧財產權的加密產品，例如數位浮水印。這個免除權可以被看做是對娛樂產業的專屬權。

更重要的是，WA 管制極難應用至無形的密碼學及其應用技術之散佈（包括從網際網路上下載），這就構成了一個重要的漏洞。對於加密產品流通的實際效果會如何仍待觀察。像加拿大與德國的這些國家已經指示他們不計畫對大眾市場軟體提出新的嚴格出口管制，瑞士政府亦指出瓦聖納協議在 1998 年 12 月份的改變將不會改變自由的瑞士密碼管理政策。

5.5、中華民國戰略性高科技貨品輸出管理制度：

鑑於 80 年代我國積極推動自由貿易政策，為引進先進國家高科技產品，以帶動產業升級、促進科技發展，並履行 1990 年「中美保護戰略性貨品及技術資料貿易瞭解備忘錄」，爰遵循國際規範、維護國際安全，美方承諾協助我國建立一套與 COCOM 組織規範相容之「國際進口證明書與抵達證明書制度」，以管制高科技貨品輸出入流向及用途，如能有效執行，美方亦將對輸往我國之高科技貨品給予輸出許可之優惠；自 1992 年 11 月起我國已建立高科技產品輸出管制制度，推動此制度沿革之摘要說明請參見表 5.4。電信及資訊安全產品屬於 1995 年 12 月取代 COCOM 之 WA 軍商兩用貨品清單中的第 5 類之第 2 部份，自 1995 年 6 月起至 2000 年 9 月止，我國於 WA 中之軍商兩用貨品(共 9 類)與軍品(共 22 類)清單中，申請鑑定案件共 204 件，電信及資訊安全類為 91 件；1998 年 7 月 1 日起，依據經濟部高科技貨品鑑定及稽查小組設置要點第 5 條，實施之高科技貨品鑑定作業程序，請參閱圖 5.2、5.3 與 5.4。於圖 5.4 中，技術專家填製之鑑定結果表中的鑑定結果僅係作為申請機構之參考文件。

表 5. 4：中華民國資訊安全產品輸出入管理簡述

1	1990 年簽訂中美保護戰略性貨品及技術資料貿易瞭解備忘錄，雙方承諾由美國協助我國建立一套與 COCOM 組織規範相容之管制高科技貨品輸出入流向及用途之執行制度；1992 年 11 月起，先於新竹科學園區試辦。
2	1993 年 2 月 5 日公布貿易法，植基於該法第 13 條，經濟部國際貿易局，於相關機構、學者及業界代表召開第 13 次會議後，在 1994 年 3 月 31 日訂定我國：「高科技貨品輸出入管理辦法」，報院核備實施；1994 年 7 月，全面實施。

3	目前遵循「瓦聖那協議清單」，於軍商兩用貨品清單由經濟部工業局彙整訂定，軍品清單由國防部審定。
4	密碼學及其應用技術屬於「瓦聖那協議清單」中，軍商兩用貨品清單第五類第二部份產品。
5	2000 年 7 月 19 日，「高科技貨品輸出入管理辦法」改名為「戰略性高科技貨品輸出入管理辦法」，同時將過境、轉運或進儲保稅倉庫納入管理。

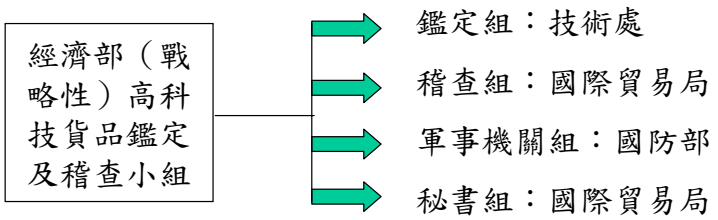


圖 5.2：戰略性高科技貨品鑑定作業程序之 1─工作依據

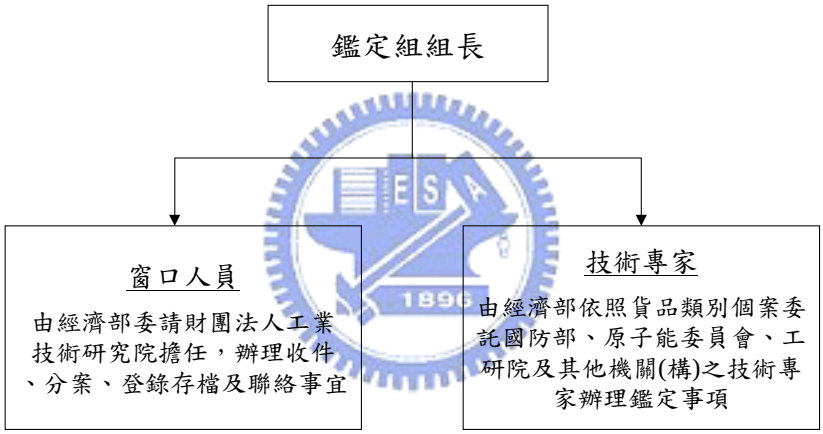


圖 5.3：戰略性高科技貨品鑑定作業程序之 2─人員組織

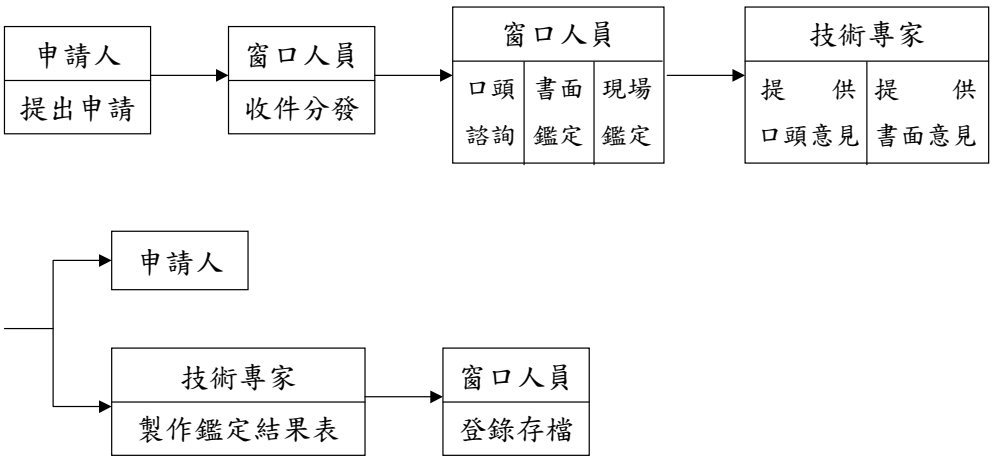


圖 5.4：戰略性高科技貨品鑑定作業程序之 3─鑑定作業流程

美國喬治亞大學之國際貿易暨安全中心（The Center for International Trade and Security）發展了一套十項要素 72 項指標的系統來評估一個國家出口管制之質與量，有效出口管制系統之十項要素為【82】：

(1). 審批系統／法律架構（Licensing system/legal framework）：管制戰略性物資出口應有法源依據，並有專責機構負責出口許可之審批。
(2). 管制清單（Interagency Process）：須有管制清單詳列應納入管制之貨品、服務和技術，包括飛彈、核子、化學、生物、領域和傳統武器。
(3). 機構合作（Interagency Process）：由於出口管制許可與出口管制政策之執行通常由不同部門負責，因此專家認為為平衡政策和執行之競爭利益，多部門的決策是很重要的。
(4). 海關權限（Customs Authority）：專責監督國境活動與船運之單位。
(5). 參與國際協議（Regime Adherence）：係是否參與多邊管制組織，包括瓦聖那協議(WA)、飛彈技術管制協定(NTCR)、澳洲集團(AG)和核子供應國集團(NSG)。
(6). 滴水不漏條款（Cathch-all Clause）：由於管制清單無法盡列，因此法律依據必須載明企業不得出口或轉口「有理由相信」會被用來製造大規模毀滅性武器之貨品，即使該貨品未及列入管制清單中。
(7). 資訊分享與蒐集（Information Sharing/Gathering）：應蒐集並分享有關違反出口和敏感的最終使用者的資訊。政府必須告知出口商相關法令要求和配合措施。
(8). 查證（Verification）：包括法源、機構和程序三方面，以確保核發許可之貨品為最終使用者（政府部門或是企業）在認可之地點使用，且是為許可之目的而使用。涉及審批前之查核、進口許可證明、運送許可和裝船檢查。
(9). 訓練（Training）：有足夠之政治與技術之訓練，使政府相關人員有能力評估技術和武器出口所可能產生之風險。
(10). 罰則（Penalties）：對於違反出口管制應該負有民事、刑事責任。

由表 5.5 之各國出口管制系統比較表可知日本以 97.92 分排名第一，其次是美國和英國，台灣則以 88.51 分排名第四，中華人民共和國以 65.56 居於第十三。相較於前三名，台灣表現較差的項目是國際協議、訓練、海關、罰則、資訊與蒐集等 5 項，其中國際協議與資訊分享與蒐集互為因果，由於台灣之國際地位使得政府無法積極參與相關國際組織，連帶影響到對國際組織之資訊分享與蒐集也較為被動；從表 5.5 可知，台灣於密碼學及其應用技術的出口管制方面屬於較嚴格之國家；惟於其他方面較諸美國、中華人民共和國等已立法管制之狀況【2, 40, 69, 90~91】則有明顯差距。

表 5.5：國際出口管制評估比較彙整

國家(Country)	審批 (License)	表列 (Lists)	國際協議 (Intl. Regimes)	滴水不漏 (Catch All)	訓練 (Training)	機構合作 (Agency Process)	海關 (Customs)	查證 (Verif.)	罰則 (Penalty)	資訊分享與蒐集 (Info.S/G)	總分 (Total Score)
日本(Japan)	17.86	15.16	7.65	2.87	9.25	6.22	15.78	8.78	4.30	10.04	97.92
美國(United States)	14.82	15.16	7.65	2.87	9.25	8.30	15.78	8.78	4.30	10.04	96.96
英國(United Kingdom)	17.86	15.16	7.65	1.43	9.25	5.56	15.78	5.88	4.30	8.73	91.60
台灣(Taiwan)	17.86	15.16	5.41	2.87	7.70	7.60	13.14	8.78	3.58	6.68	88.51
烏克蘭(Ukraine)	17.86	15.16	7.65	1.43	4.62	8.30	13.09	5.79	3.56	8.33	85.79
阿根廷(Argentina)	17.86	12.58	7.65	2.87	4.62	8.30	10.41	8.78	3.56	9.13	85.76
捷克共和國(Czech Republic)	17.86	15.16	7.34	2.87	4.62	7.88	7.89	7.28	3.56	10.04	84.53
以色列(Israel)	17.86	15.16	4.82	0.46	6.66	4.65	15.78	4.92	3.57	5.02	79.00
蘇俄(Russia)	14.82	15.16	7.33	1.43	6.10	6.88	10.41	6.76	2.83	4.51	76.29
南韓(South Korea)	16.37	15.16	7.33	0.00	3.08	5.99	10.52	6.38	2.87	4.18	72.33
印度(India)	14.82	12.58	0.00	0.00	6.10	8.30	13.09	5.79	2.83	7.03	70.54
古巴(Cuba)	13.39	10.00	1.91	0.00	8.14	6.22	15.78	5.79	2.83	6.25	70.31
中國(China)	14.82	12.63	3.19	0.00	3.08	6.88	10.52	4.88	2.87	6.69	65.56
哈薩克(Kazakhstan)	13.39	12.58	1.91	0.00	5.14	6.22	10.41	2.45	2.15	5.02	59.26
喬治亞(Georgia)	5.89	10.15	0.00	1.92	5.18	4.15	10.57	1.49	1.41	1.25	42.01
烏茲別克(Uzbekistan)	14.82	2.58	0.00	0.00	0.00	1.40	14.50	0.00	0.00	0.00	33.28
吉爾吉斯(Kyrgyzstan)	8.93	10.00	0.00	0.00	0.00	0.99	10.57	0.00	0.00	0.00	30.42
塔吉克(Tajikistan)	0.00	0.00	0.00	0.00	0.00	0.00	7.89	0.00	0.00	0.00	7.89

資料來源： http://www.uga.edu/cits/documents/html/nat_eval_nec_table.htm (12-Oct-2004)

5.6、美國之密碼學及其應用技術管制政策：

美國聯邦政府自 1919 年起，如表 5.6 所示有系統的應用密碼學技術，在第一次與第二次世界大戰均獲取重大之利益，長久以來，密碼學及其應用技術均視同傳統武器加以管制遵循 1976 年之武器出口管制法案（Arms Export Control Act of 1976）的出口管理制度與程序。近年來，為回應瓦聖那協議之重視經濟利益、反應科技進步與促進電子商務發展等議題，其管制政策具體的改變為高性能電腦及加密軟體管制之放寬。然在實施之際，適逢 911 恐怖攻擊事件的發生，讓美國國家安全局與聯邦調查局長久以來反對密碼學及其應用技術出口之立場，因恐將使美國無法解讀外國政府及恐怖組織的秘密通訊，致可能危及國家安全而更加堅持，密碼學及其應用技術管制放寬之腳步趨緩。

表 5. 6：美國政府使用密碼學及其應用技術簡史

1919 年 5 月 20 日，由 Herbert O. Yardley 先生擔任主管，專責密碼學實際應用，美國國務院支持的「美國黑房（America's Black Chamber）」正式成立。
1921 年 11 月 28 日，美國黑房破解於同年 11 月 14 日 5 強限武會議中，日本政府通知日本代表佳藤海軍大將之：「美國、英國、日本海軍噸數的可接受最低比例為 10:10:6」的底牌。
1924 年 1 月，美國海軍部於代號 OP-20-G 之安全單位負責類似美國黑房之工作。
1929 年 10 月 31 日，美國國務卿 Henry L. Stimson 先生堅持：「君子非禮勿視」，下令解散美國黑房。
1930 年 4 月 24 日，美國陸軍部支持之訊號情報處（Signal Intelligence Service, SIS）正式成立，專責秘密通訊攻防實際應用，由 William F. Friedman 先生擔任主管。
1931 年 6 月 1 日，Herbert O. Yardley 先生著之「美國黑房（The American Chamber）」一書問世，其第 2 本著作「日本的外交秘密：1921~1922（Japanese Diplomatic Secrets：1921~1922）」原稿被美國司法部沒收；1933 年 4 月 3 日，美國眾議院通過「保護政府檔案」法，同年 5 月 10 日在參議院稍事修改後也通過了，同年 6 月 10 日由美國總統簽署成為法律。
1942 年 1 月 19 日，美國國防部長 Henry L. Stimson 先生下令整頓各單位紛紛成立之類似美國黑房的組織。
1942 年 3 月，美國國防部在其軍事情報處（Military Intelligence Service）中設立一個特別分部（Special Branch）專責密碼學實際應用工作。
1942 年 6 月，美國國防部軍事情報處特別分部，破解了日本「紫色（Purple）」密碼，得知日本海軍攻擊阿留申（Aleutian Islands）群島是聲東擊西的序幕，真正的目標是中途島（Midway Island）；同一時期，英國也破解了德國的「奇謎（Eigma）」密碼。
1943 年 5 月 17 日，美、英兩國正式簽署英美協定（Britain United States Agreement），兩國於美國黑房的工作互相全面合作；1944 年 3 月，加拿大和澳洲加入前述協定；1947 年，UKUSA 協定正式簽定，美、英 2 國是第 1 當事國，加拿大、澳洲和紐西蘭 3 國是第 2 當事國；後來，日本、南韓和北約各國等均陸續成為 UKUSA 的第 3 當事國。
1946 年，美國成立了美國通訊委員會（United States Communications Intelligence Board, USCIB），整會國務院、陸軍部、海軍部、空軍部、聯邦調查局、中央情報局之類似美國黑房的組織。

1949 年 5 月，美國總統下令，整合陸軍部、海軍部、空軍部的類似美國黑房的組織，成立武裝部隊安全局（Armed Forces Security Agency, AFSA）。

1952 年 11 月 4 日，基於由 1951 年 12 月 13 日美國總統下令國務卿與國防部長共同成立之調查委員會，在 1952 年 6 月 13 日提出之 239 頁的報告，國家安全局（National Security Agency, NSA）正式成立，成為類似美國黑房組織的最高主管機構。

NSA 成立後，幾壟斷美國密碼學的研究，直到為研究密碼學已三度轉換工作的 Horst Feistel 在 1970 年代初期，研發出「魔王（Lucifer）」的密碼產品方告一段落。

1975 年，英國政府通訊總部（Government Communications Headqurarters, GCHQ）之通訊電子安全組（Communications Electronics Security Group, CESG）部門研究已近 10 年的公開金鑰密碼學（例：RSA 等）系統已建立完整的基礎，此項成果直到 1997 年 12 月 18 日方由 GCHQ 同意對外公開，守密近 30 年，James Ellis（註：已於 1997 年 11 月 25 日去世，享年 73 歲。）、Clifford Cocks、Malcolm Williamson 終於能公佈他們的貢獻，唯 1969 年 James Ellis 有關此方面研究（已證明公開金鑰密碼學之金鑰管理的可行性等）的文件仍列為最高機密。

把加密金鑰限定在 10^{17} 左右的 NSA 要求之條件下，美國國家標準局在 1976 年 11 月 23 日正式採用 56 位元版本的「魔王」，改名後稱之為資料加密標準（Data Encryption Standard, DES）。

1981 年 1 月，美國以國家通訊安全和電磁安全條例的形式頒布了暴風雨（Tempest）標準：「Electromagnetic Compromising Emanations Laboratory Test Standard」。

1982 年 4 月 14 日，植基於 DES（Data Encryption Standard）使用者的需求，美國國家標準與技術研究院（National Institute of Standard and Technology, NIST）公佈了密碼模組安全需求評估準則 FIPS(Federal Information Processing Standards)140；也就是美國 1982 年公佈的聯邦標準（Federal Standard, FS）1027：「使用 DES 設備的一般安全需求（General Security Requirements for Equipment Using the DES）」。

1988 年 FS1027 的驗證工作轉由 NIST 負責，NIST 為因應資訊技術的變遷，就 FIPS140 廣徵意見，並於 1989 年正式成立 FIPS140 修訂委員會。

1991 年 NIST 公佈 FIPS140-1 草案，並廣徵產、官、學、研各方面意見。

1991 年 8 月 30 日，NIST 公佈數位簽章標準（Digital Signature Standard, DSS）

1993 年 5 月 11 日，NIST 公佈安全碎映標準（Secure Hash Standard, SHS）。

1994 年 2 月 9 日，NIST 公佈代管加密標準（Escrowed Encryption Standard, EES）。

1994 年 1 月 11 日，NIST 公佈 FIPS140-1，將處理敏感但非機密性資訊之密碼模組產品的安全等級分成 4 級，並宣佈於 1994 年 6 月 30 日正式生效，同時公佈（Cryptographic Module Validation, CMV）計畫。

1996 年 1 月，共同準則（Common Criteria, CC）1.0 版公佈。

1997 年 6 月 30 日以後，美國聯邦政府祇准購買通過 FIPS140-1 CMV 測試的密碼模組產品，分成一～四級。

植基於 FIPS 140-1 等，CC(Common Criteria for Information Technology Security Evaluation)著手訂定密碼學評估準則（Evaluation Criteria for Cryptography）中，

1996 年 3 月 30 日公佈之版本 0.99b 中，將處理機密性資訊之密碼模組等均納入。
1998 年 5 月 12 日，NIST 於 FIPS 140-1 研討會中討論 FIPS 140-2，FIPS 140-2 將與 ANSI（American National Standards Institute）X9.66 調和一致。
1998 年 5 月，包含前述處理機密性資訊密碼模組等密碼學評估準則之 CC2.0 版公佈。
1999 年 11 月 18 日，NIST 公佈 FIPS 140-2 草案。1999 年 12 月 1 日，CC2.1 版正式公佈成為國際標準組織（International Organization for Standardization, ISO）之 ISO/IEC 15408。
2000 年 8 月 30 日，NIST 公告 FIPS 140-2 將以符合 CC 之規範撰寫，並冀期成為 CC 密碼模組保護剖繪（Protection Profile）。
2001 年 5 月 25 日，NIST 公佈使用 CC 之 FIPS 140-2。
2001 年 11 月 26 日，NIST 公布 FIPS197 之先進加密標準（Aduanced Encryption Standard, AES，同年 12 月 4 日，美國商務部正式批准 AES。）
2002 年 4 月 4 日，共同準則之公開金鑰基礎建設安全核心保護剖繪（Public Key Infrastructure Secure Kernel Protection Profile, PSKPP）1.1 版公布。
2002 年 7 月 1 日，美國國家安全之電信與資訊系統安全(National Security Telecommunications and Information Systems(Security) Committee, NSTISS)委員會頒佈之 NSTISS 政策第 11 號，要求美國總統決策令第 63 號(Presidential Decision Directive No.63, PDD63)中之範疇，均遵循 CC 與 NIST 之確認計畫。
2002 年 10 月，英國之 Logica CMG 成為北美之外第 1 個 CMV 計畫承認之第 7 個密碼模組測試實驗室（美國 4 個、加拿大 2 個）。
2003 年 6 月 30 日，國際標準組織（International Organization for Standardization，簡稱 ISO）公布根基於 FIPS 140-2 制定之密碼模組安全需求 ISO/IEC 19790 第 1 版（1st）工作草案（Working Draft，簡稱 WD）。
2004 年 6 月 30 日，ISO 公布 FIPS 140-2 與 CC 之資訊技術安全保證比較分析資料，於惡意程式碼攻擊之對抗性方面，FIPS 140-2 有相當改善空間。
2005 年 1 月 12 日，ISO 公布制定 FIPS 140-3。
2006 年 3 月 1 日，ISO 公布增加脆弱性分析要求之 ISO/IEC 19790 標準。

美國商務部出口管理局 1999 年 12 月 17 日公佈了最近的密碼產品管制政策，於 2000 年 1 月 14 日起施行此暫行規範，並於 2000 年 5 月 15 日前接受大眾提出各種修正建議，此新措施已於 2000 年 10 月 19 日正式生效實施。整個管制規範的修正重點，包括了：

(1). 任何加密產品（包括軟體），除了出口至國外政府所有之網路或電信服務事業之零售加密產品，以及古巴、北韓、伊朗、伊拉克、利比亞、蘇丹等地區仍須事先核准外，其餘僅須通過技術審驗後，均採行事後申報即可。
(2). 已公諸大眾之加密原始碼，出口無須事先核准，也不須經技術審驗。
(3). 在美國境內從事相關工作之外國公民，不須取得核准。
(4). 任意長度之加密產品，無須經技術審驗即可出口至國外之美國子公司。
(5). 除了供人消費的零售或金融用途之加密產品外，出口特定的 64 位元以上加密產品到非隸屬美國之主體，必須於事後申報。

整個出口管理條例（Export Administration Regulations，簡稱 EAR）之修正要點，說明如下：

(1). 重要的出口管理條例項目與準則：不限制之加密原始碼、商業加密原始碼，以及零售產品，均已由網際網路下載過濾需求中免除。另加入一修訂過的、對於其他出口

至政府終端用戶的加密產品之過濾機制。值得注意的是，EAR 也對相關的加密原始碼及目的碼軟體出口的定義加以規範。

(2). 未限制的技術與軟體：修正案的變更是回應瓦聖那協議，特別是，加密軟體不再適用於通用軟體註解（General Software Note）中大眾市場的處理方式。加密的大眾產品及軟體現在適用於瓦聖那協議軍商兩用貨品第五類第二部分含技術註解之大眾市場處理方式。這份註解對大眾市場加密大眾產品及軟體解除管制至 64 位元。這種產品在 BXA 檢視與分類後，歸類於出口大眾產品管制號（Export Commodity Control Numbers，簡稱 ECCNs）5A992 或 5D992 下，因此解除"加密項目"（Encryption Item，簡稱 EI）與"國家安全"（National Security，簡稱 NS）的管制，並使其適用於對所有目的地之出口及再出口（EAR 之§742.15 節）。當大眾市場加密產品與大眾產品由"EI"中解除管制，它們即可適用於一般的處理方式。

(3). 同時在考慮「開放源碼」方式對軟體的發展，不隸屬於授權費支付的特殊協議、產品版稅或以原始碼開發的任一產品銷售之未限制加密原始碼，可以不經審查，解除"EI"控管並在不受限之技術與軟體（Technology and Software Unrestricted，簡稱 TSU）之例外許可下出口與再出口。智慧財產保護（例如：著作權、專利或商標）本身不得解釋為對於授權費支付、產品版稅或以原始碼開發的任一產品銷售之的特殊協議。欲符合資格，出口商必須通知出口管理局（Bureau of Export Administration，簡稱 BXA）其網際網路位置（例如萬用資源網址（Universal Resource Locator，簡稱 URL）或網際網路位址）或在出口時提供開放源碼的副本。只有在首次出口時需要這些通知，對於終端用戶後續使用開放源碼則無須通知。通知可以採行傳送電子郵件的方式將郵件傳至 crypt@bxa.doc.gov。

對於使用此開放源碼的外國製產品則不需檢視與分類。此外，不限制的加密開放源碼之出口不限制其對於使用此開放源碼之外人提供技術支援。而且，開放源碼的出口商不隸屬網際網路下載過濾需求。張貼開放源碼於任何人均可下載的網際網路（例如 FTP 或 WWW）不會形成禁止出口與再出口的（EAR 所定義的）「知識」。這種張貼不會觸發「紅旗」（Red flag），而有不得不查詢部分補充之"瞭解顧客"指引的必要責任。否則，遵循 EAR 需求以禁止出口與再出口仍然適用。

(4).「加密大眾產品與軟體」之例外許可授權（Exception Commodities and Software，簡稱 ENC），加上實施管理新政策之免申請出口 ENC 之例外許可授權修訂如下：

(4.1). ECCNs 5A002、5D002 或 5E002 下的加密項目可以出口或再出口至美國的國外分公司，包括不必經技術檢視與分類的移轉加密技術給在美國的外國雇員。由美國公司開發的任何銷售或再移轉至美國境外公司的項目必須由 BXA 所檢視與分類，外國公司及其美國分公司可以申請加密授權協議（Encryption Licensing Arrangements，簡稱 ELAs）以獲取等同於美國母公司之外國分支所延伸的待遇。

(4.2). 增加「加密大眾產品與軟體」之授權範疇：經 BXA 之 ECCNs5A002、5D002 所檢視與分類後，可以出口或再出口任何加密大眾產品與軟體給個人、商業公司或其他非政府終端用戶。

(4.3). 增加「零售加密大眾產品與軟體」。經 BXA 之 ECCNs5A002、5D002 所檢視與分類為零售後的任何加密大眾產品與軟體，可以出口或再出口給終端用戶。

(4.4). 增加「網際網路與電訊服務提供者」之授權範疇：任一網際網路與電訊服務提供者可在 ENC 之例外許可下獲得零售產品，並用於提供服務與任一個體。

網際網路與電訊服服務提供者可在 ENC 之例外許可下獲得並使用供內部使用的加密產品，以提供各種服務。

(4.5). 增加「商業加密原始碼與一般用途工具」之授權範疇：加密原始碼會視為公開可取，而且隸屬於授權費支付的特殊協議、產品版稅或以原始碼開發的任一產品，出口時有傳送文字通知 BXA 網際網路位址或原始碼副本，則可以不經審查與分類，在 ENC 之例外許可下出口與再出口給任一終端用戶。不得意出口或再出口原始碼或以此原始碼開發的產品至古巴、伊朗、伊拉克、利比亞、北韓、蘇丹或敘利亞。張貼原始碼於任何人均可下載的網際網路所有（例如 FTP 或 WWW）不會形成禁止出口與再出口的（EAR 所定義的）「知識」。這種張貼不會觸發「紅旗」（red flag），而有不得不查詢部分補充之"瞭解顧客"指引的必要責任。

(4.6). 追溯（Grandfathering）與增加金鑰長度。

(4.7). 檢視與分類作業之簡化：可以藉由傳送分類需求予 BXA，起始加大眾產品與軟體的檢視與分類作業。除非特別通知，接到 BXA 分類需求收據 30 天後，即可出口與再出口任一加密產品予任一非政府終端用戶。

(4.8). 非屬必要，均免除報告需求。

(5). 金鑰管理基礎建設（Key Management Infrastructure，簡稱 KMI）：增加 ATTN 之地址。

(6). 不受限之技術與軟體（Technology and software unrestricted）

本之例外許可授權操作技術與軟體、銷售技術與軟體、軟體更新、隸屬於一般軟體註解（General Software Note）的大眾市場軟體、以及未限制的加密原始碼之出口與再出口，唯宜注意加密軟體並不隸屬於一般軟體註解（General Software Note）之範疇。

(7). 未限制的加密開放源碼：

(7.1). 加密開放源碼在 5D002 下控管會視為公開可取，而且如果在出口時，有傳送文字知 BXA 網際網路位址或開放源碼副本，則不隸屬於授權費支付的特殊協議、產品版稅或以開放源碼開發的任一產品銷售之未限制加密開放源碼，可以不經審查，

(7.2). 不得蓄意出口或再出口開放源碼或以此開放源碼開發的產品至古巴、伊朗、伊拉克、利比亞、北韓、蘇丹或敘利亞。

(7.3). 張貼原始碼於任何人均可下載的網際網路（例如 FTP 或 WWW）不會形成禁止出口與再出口的（ERA 所定義的）「知識」。這種張貼不會觸發「紅旗」（Red flag），而不得不查詢部分補充之"瞭解顧客"指引的必要責任。

(8). 加密大眾產品與軟體（Encryption commodities and software，簡稱 ENC）

(8.1). 某些加密大眾產品與軟體的出口與再出口：

可以在例外許可下，出口及再出口加密大眾產品與軟體與元件(ERA 772 部分所定義)時，除非出口至美國公司的分支機構，不得使用 ENC 之例外許可。

(i). 供美國分支機構使用的加密大眾產品、軟體與技術：不必經技術檢視與分類，可以出口或再出口 ECCNs5A002、5D002 或 5E002 下的加密項目或任意長度金鑰至美國的國外分公司（772 部分所定義），包括公司內部使用的開放源碼與技術，例如開發新產品。美國公司也可以在 ENC 之例外許可下，移轉加密技術（5E002）給在古巴、伊朗、伊拉克、利比亞、北韓、蘇丹或敘利亞除外之美國的外國雇員供公司內部使用，包括新產品的開發。由美國公司生產或開發的、以本節所述之加密大眾產

品、軟體與技術的出口隸屬於 EAR，任何銷售或再移轉至美國境外公司前必須由 BXA 所檢視與分類。

(ii). 增加「加密大眾產品與軟體」授權之範疇：經 BXA 之 ECCNs 5A002、5D002 所檢視與分類後，可以出口或再出口任何加密大眾產品與軟體給個人、商業公司或其他非政府終端用戶之之前對於公司內私人使用的限制出口或再出口已經免除。

零售加密大眾產品與軟體：經 BXA 之 ECCNs 5A002、5D002 所檢視與分類為零售後的任何加密大眾產品與軟體，可以出口或再出口給終端用戶。零售加密大眾產品、軟體與元件為：

(8.1.1). 以下列方法可以公開取得者：

(i.) 獨立於製造商之零售外賣店、以實體形式銷售。

(ii.) 特別設計供個別客戶使用並透過實體或非實體方式銷售或移轉。

(iii.) 無限制地大量販賣，透過郵購交易、電子交易、或電話交易。

(8.1.2). 符合所有下列：

(i). 加密功能不會輕易由使用者更改。

(ii). 安裝及使用不需大量支援。

(iii). 加密功能未經修改或客制化為顧客規格。

(iv). 不是提供大量通訊使用路由器（Router）或交換器（switch）等之網路基礎建設產品。

(8.1.3). 零售加產品包括（不限於）一般用途作業系統及其相關使用者介面軟體、嵌入式的網路與伺服器功能之一般用途作業系統、不可程式化的加密晶片、限制設計供零售的加密晶片、低階路由器、供小型辦公室或家庭用之防火牆及纜線設備、可程式化的資料管理系統與相關應用伺服器、直接提供使用者介面的低階伺服器與特定應用伺服器（包括主從架構之應用如基於 SSL（Secure Socket Layer）的應用）、以及免費或透過自由匿名下載散佈的加密產品。

(8.1.4). 加密產品與基於網路、提供等於分類為零售的其他加密產品功能的應用。

(8.1.5). 出口與再出口可以提供服務給任一個體之諸如智慧卡(Smart Card)等產品。

(8.1.6). 財務特定使用之加密大眾產品與各種金鑰長度（因設計限制）之軟體（如極度因場合而定、有驗證程序以及不易移轉於其他終端用戶者，諸如自動櫃員機等）並用於保護財務通訊如電子商務者，被視為零售加密產品。

(8.1.7). 有 512 到 1024 位元的金鑰交換機制之 56 位元產品或不歸類為大眾市場的同等產品，視為零售。

網際網路與電訊服務提供者：某些限制適於網際網路與電訊服務提供者。任一網際網路與電訊服務提供者可在 ENC 之例外許可下獲得零售產品，並用於提供服務與任一個體。網際網路與電訊服務提供者可在 ENC 之例外許可下獲得並使用供內部使用的加密產品，以提供各種服務。但未歸類為零售產品的任一產品、以提供政府終端用戶特定使用（如廣域網路、區域網路、虛擬私有網路、語音與固定連結服務、特定應用與電子商務服務、僅供政府終端用戶特定之公開金鑰基礎建設的加密服務），必須有許可。

商業加密開放源碼與一般用途工具：隸屬餘下列提供者，可以出口與再出口未解除的開放源碼與一般用途工具－

(i). 加密原始碼會視為公開可取，而且隸屬於授權費支付的特殊協議、產品版稅或以原始碼開發的任一產品，出口時有傳送文字通知 BXA 網際網路位址或原始碼副本，則可以不經審查與分類，在 ENC 之例外許可下出口與再出口給任一終端用戶。不得蓄意出口或再出口原始碼或以此原始碼開發的產品至古巴、伊朗、伊拉克、利比亞、北韓、蘇丹或敘利亞。

(ii). 不被認為公開可得的加密開放源碼、也不包括編譯時提供開放密碼介面者，經 BXA 檢視分類後，可以在 ENC 之例外許可下出口與再出口給任一非政府終端用戶。

(iii). 一般用途加密工具可以經 BXA 檢視分類後，出口與再出口給任一非政府終端用戶。

(iv). 使用加密原始碼開發、供商業銷售的任一國外產品，或在本出口的一般用途工具均必須依據報告需求，以綁售(Bundling)或編譯原始碼開發的國外產品不屬於此。

(8.2). 不適用的目的地：

無任何加密項目可在 ENC 之例外許可下，出口或在出口至古巴、伊朗、伊拉克、利比亞、北韓、蘇丹或敘利亞。

(8.3). 移轉：

移轉所列之項目予政府端用戶或在同一國家內的終端使用是禁止的，除非有許可授權或 ENC 之例外許可外。

(8.4). 結合美國加密原始碼、元件或工具的外國產品出口與再出口：

仍隸屬於 EAR，但不需由 BXA 檢視與分類，可以在不必進一步授權下出口與再出口。

(8.5). ENC 之例外許可適用性：

(8.5.1). 檢視與分類：可以藉由傳送分類需求予 BXA，起始加密大眾產品與軟體的檢視與分類。除非特別通知，接到 BXA 分類需求收據 30 天後，即可出口與再出口任一加密產品予任一非政府終端用戶。此項下不允許出口予政府終端用戶。當分類暫緩時，BXA 保留暫緩出口適用性的權力。

(8.5.2). 追溯(Grandfathering)：BXA 過去檢視與分類的，財務特定使用以及 56 位元之加密產品，無須再檢視可出口與再出口任一終端用戶。其他過去核可的加密大眾產品與軟體或元件，無須再檢視可出口與再出口予任一終端用戶。除非 BXA 之分類為零售，否則出口至政府終端用戶需要許可。

(8.5.3). 增加金鑰長度：出口商可以增加過去分類產品金鑰長度，不需逐一檢視持續出口，唯不允許改變加密功能：

(i). 過去分類為 5A002 或 5D002 者，可以升級隱私用的金鑰長度或金鑰交換演算法，在 ENC 之例外許可下出口與再出口至非政府終端用戶，均不需額外的檢視。需另一分類已決定是否適於零售。

(ii). 出口商要由公司正式出具信函向 BXA 保證，只有隱私用的金鑰長度或金鑰交換演算法改變，沒有其他加密功能改變。BXA 要在認可升級產品出口前取得此保證書，保證書的副本要送給 ENC 加密請求之協調人。

(8.6). 公開加密介面：除原始碼外，ENC 之例外許可不適用於加密產品提供公開介面者。

(8.7). 報告需求：美國分公司之加密產品，財務特定產品。小於 64 位元的加密大眾產品等，均無報告需求。

(8.8). 配銷商與零售商：符合規範之配銷商與零售商，可以使用 ENC 之例外許可。

美國為了維持情報與執法機構之電子檢查能力，曾採取軟硬兼施的方法來鼓勵民間配合政府之管制政策。在數位社會的環境需求及各界之輿論壓力下，一再修正其密碼學及其應用技術的管制政策已如前述。一般而言，於出口後之最終使用者並非美國公司的密碼產品與加密技術均需通過技術審查，並取得許可證，方可銷售。

5.7、中華人民共和國之商用密碼管理政策：

中華人民共和國之密碼學及其應用技術由保密局負責，在中國大陸的公司必須先通過審批、取得執照，方能進出口密碼學及其應用技術之相關產品，審批由保密局等相關機構主責，執照的申請與核發由外貿部（Ministry of Foreign Trade）或各省之外貿局負責，相關機構有一份禁止及限制進出口產品的名單。根據各種相關報導顯示，在中國大陸境內取得使用加密產品之許可並不容易；此外在中國大陸境內使用加密產品或裝置之外國機構與個人，均須提出申請及接受審批。由於相關資料取得之限制，在此，僅探討中國大陸之商用密碼管理政策。

1999 年 10 月 7 日，中華人民共和國國務院令第 273 號發布：「商用密碼管理條例（以下簡稱條例）」規定凡是對不涉及國家秘密內容之資訊進行加密或安全驗證所使用之密碼學及其應用技術與產品均屬「國家秘密」及「商用密碼」，由「國家密碼管理委員會」負責管理，未經指定（許可）任何單位或個人不得生產（銷售）商用密碼產品【69】。

條例分成 7 章共 27 條，其中第 6 章是罰則，第 7 章是附則，分別律定商用密碼產品由國家密碼管理機構執行，未遵循商用密碼管理規定之生產與銷售的罰則，以及相關管理規定由國家密碼管理委員會制定。第 1 章、……、第 5 章內容依序簡介於后。

在第一章總則中，條例說明其目的是加強商用密碼管理，保護信息安全，保護公民和組織之合法權益，維護國家的安全與利益。國家密碼管理委員會及其辦公室（簡稱密碼管理機構）主管全國之商用密碼管理工作。自治區、直轄市負責密碼管理的機構受國家密碼管理機構的委託，承擔商用密碼的有關管理工作。

條例指出：商用密碼技術屬於國家秘密，國家對商用密碼產品之科研、生產、銷售和使用實行專控管理。

在第二章科研、生產管理中規定：商用密碼之科研任務由國家密碼管理機構指定的單位承擔。商用密碼指定科研單位必須具有相應之技術力量和設備，能夠採用先進的編碼理論和技術，編制的商用密碼算法具有較高之保密強度和抗攻擊能力。商用密碼的科研成果，由國家密碼管理機構組織專家按照商用密碼技術標準及技術規範審查、鑑定。商用密碼產品由國家密碼管理機構指定之單位生產。未經指定，任何單位或者個人不得生產商用密碼產品，商用密碼產品指定生產機構必須具有與生產商用密碼產品相適應之技術力量及確保商用密碼產品質量的設備、生產工藝和質量保證體系。商用密碼產品指定生產單位生產的商用密碼產品的品種和型號，必須經國家密碼管理機構批准，並不得超過批准範圍生產商用密碼產品。商用碼產品必須經國家密碼管理機構指定的產品質量檢測機構檢測合格，表 5.7 是中國大陸商用密碼產品及其相關產品與人員之測評認證機制表列。

表 5.7：中國信息安全測評認證機制現況示意表

1 信息安全技術及產品的測試與驗證：

1.1 主責單位：中國信息安全產品測評認證中心。
1.2 遵循規範：共同準則(Common Criteria)。

2 信息系統安全評估與驗證：
2.1 主責單位：中國信息安全產品測評認證中心。
2.2 遵循規範：共同準則(Common Criteria)。

3 信息安全服務機構評估與認證：
3.1 主責單位：中國信息安全產品測評認證中心。
3.2 遵循規範：SSECMM(System Security Engineering Capability Maturity Model)。

4 信息安全人員評估與認證：
4.1 主責單位：中國信息安全產品測評認證中心。
4.2 遵循規範：CISSP(Certified Information Systems Security Professional)。

5 涉密信息系統：
5.1 主責單位：國家保密局涉密信息系統安全保密測評中心。
5.2 遵循規範：共同準則(Common Criteria)。

6 TEMPEST 的檢測：
6.1 主責單位：國家保密局電磁洩漏發射防護產品檢測中心(註：依附於國家保密局 1991 年成立之國家保密技術研究所。)。
6.2 遵循規範：BMB1-1994、BMB2-1998、BMB3-1999、GGBB1-1999、GGBB2-1999、BMB4-2000、BMB5-2000、BMB6-2001、BMB7-2001、BMB7.1-2001。

7 信息安全之一般管理：
7.1 主責單位：公安部計算機系統安全產品質量監督檢驗中心(註：依附於公安部 1978 年成立之第 3 研究所。)。
7.2 遵循規範：共同準則(Common Criteria)。

8 軍用信息安全產品：
8.1 主責單位：中國人民解放軍信息安全測評認證中心。
8.2 遵循規範：共同準則(Common Criteria)與 6.2 中之遵循規範。

9 商用密碼產品：
9.1 主責單位：國家密碼管理局商用密碼檢驗中心。
9.2 遵循規範：共同準則。

10 信息安全認證：
10.1 主責單位：中國信息安全產品測評認證中心吳世忠主任於 7 月 2 日上午 11 時 20 分左右口頭表示預定在 2003 年完成。
10.2 遵循規範：ISO(International Organization for Standardization) /CASCO (Committee on Conformity Assessment)相關規範。

11 信息安全檢測單位(註：僅為作者已知部分)：
11.1 信息產業部太級聯合實驗室(註：1995 年，信息產業部電子 15 所聯合 10 餘家計算機廠商，共同成立。)。
11.2 國家計算機病毒應急處理中心(註：2000 年 8 月成立，前身是天津市公安局與天津市技術監督局在 1996 年建立之「計算機病毒防治產品檢驗中心」。)。

在第三章銷售管理中規定：商用密碼產品由國家密碼管理機構許可之單位銷售。未經許可，任何單位或者個人不得銷售商用密碼產品。銷售商用密碼產品，應當向國家密碼管理機構提出申請，並應當具備下列條件：有熟悉商用密碼產品知識和承擔售後服務人員；有完善之銷售服務和安全管理規章制度；有獨立的法人資格。經審查合格之單位，由國家密碼管理機構發給＜商用密碼產品銷售許可證＞。銷售商用密碼產品，必須如實登記直接使用商用密碼產品之用戶的名稱（姓名）、地址（住址）、組織機構代碼（居民身份證號碼）以及每台商用密碼產品的用途，並將登記情況報國家密碼管理機構備案。進口密碼產品以及含有每台商用密碼技術之設備或者出口商用密碼產品，必須經國家密碼管理機構批准。任何單位或者個人，不得銷售境外的密碼產品。

在第四章使用管理中規定：任何單位或者個人只能使用經國家密碼管理機構認可之商用密碼產品，不得使用自行研制的或者境外生產的密碼產品。境外組織或者個人在中國境內使用密碼產品或者含有密碼技術的設備，必須報經國家密碼管理機構批准；但是，外國駐華外交代表機構與領事機構除外。商用密碼產品的用戶不得轉讓其使用之商用密碼產品。商用密碼產品發生故障，必須由國家密碼管理機構指定的單位維修。報廢、銷售商用密碼產品，應當向國家密碼管理機構備案。

在第五章安全、保密管理中規定：商用密碼產品之科研、生產，應當在符合安全、保密要求的環境中進行。銷售、傳輸、保管商用密碼產品，應當採取相應的安全措施。從事商用密碼產品的科研、生產和銷售以及使用商用密碼產品之單位和人員，必須對接觸與掌握的商用密碼技術承擔保義務。宣傳、公開展覽商用密碼產品，必須事先報請國家密碼管理機構批准。任何單位及個人不得非法攻擊商用密碼，不得利用商用碼危害國家的安全以及利益，危害社會治安或者進行其他違法犯罪活動。

中國大陸如表 5.7 所示，於 1997 年初開始建設商用密碼產品相關之產品質量檢測機構，在 1998 年 7 月 28 日正式掛牌營運之後【90】，1999 年 10 月 7 日方公布「商用密碼管理條例」，「工欲善其事，必先利其器」，其建設與管理之軌跡，值得參考。

明末清初中國商人依據唐代「飛錢」之遺意創造發明了匯(會)票，康熙、雍正、乾隆三朝，無論是見票兌付的匯票，還是按約定時間兌付的期票，均已成為當時中國商業市場流通的信用工具。匯票與期票所以無假，敢於實行「認票不認人」的兌付制度，在於它有一套防偽的方法，除了使用中國書法中每個人的風格筆力不同的特性以辨別真偽外；同時，運用漢字編製防偽密碼，用以代表簽發月日與銀兩的暗碼，寫在匯票與期票的背面做為分別本尊或分身的依據。舉例而言，清道光 27 年 11 月 5 日山西日昇昌平遙總號開立萬和全商號匯往廣州 14,300 兩紋銀的匯票時；當時日昇昌山西平遙總號使用「謹防假票冒取，勿忘細視書章。」代表 1 年 12 個月，用「堪笑世情薄，天道最公平，昧心圖有利，陰謀害他人，善惡終有報，到頭必分明。」三十個字代表一個月的三十天，用「生客多察看，斟酌而後行。」10 個字代表「1、2、3、4、5、6、7、8、9、10」十個數字，用「國寶流通」4 個字代表「萬、仟、百、十」的單位字；因此，前述的匯票背面，就由日昇昌山西平遙總號的開票人寫下「書薄」和「生國察寶多流」8 個字的暗碼，這就是中國銀行界「押碼」制度的由來。

自摩斯(Morse)先生發明之電報(1830~1839 年)，貝爾(Bell)先生於 1876 年發明之電話，均在十九世紀末期逐漸普及後，由於「千里傳音，彈指收訖。」的效率，在國防、外交、商業等方面均使用漸廣。中國亦不例外，自有線電報在中國架設使用以來，因中國文字異於歐、美各國使用的由字母合成的拼音文字，且同音字又甚多，早於清朝光緒五年(西元 1879 年)由丹麥大北電報公司 Piniu 先生協同我國黃孝餘先生，

從「康熙字典」中挑選 7,750 個常用單子，用四個數字組成「明碼」，代表一個中文單字；並用「部首檢字法」順排分為 214 個部首，編成現在仍在使用中的電報「明碼本」。在電報發送中必須保持其內容機密時，一般均利用「明碼本」使用「加碼」、「移位」或改編「明碼本」頁、行次密碼方法【74】；在這樣的密碼機制下，清朝光緒十年編纂的「電報新書」中亦訂有「.....今另設一金匙開鎖變法，.....以便高價寄信秘密之用。.....」；僅使用「加碼」、「移位」加解密方法的安全度自然無法抵擋專業之破密分析，1884 年 6 月 23 日在當時日本外相陸奧宗光伯爵主導下，日本外務省電信課長佐藤愛麿先生宣布破解了清朝官方使用的「金匙」，在 1884 年 7 月 25 日豐島海戰首開甲午戰爭戰端，至 1885 年 4 月 17 日在日本下關春帆樓簽下馬關條約，把台灣、澎湖割讓給日本的過程中，立下了第一功【79】。

1922 年 9 月間服務於天津電報局的蔣宗標先生破解直系首領曹錕電令江蘇督軍齊燮元等，並用 1,350 萬元賄選的密電加解密方法，並將相關資料經鄭洪平先生與葉恭綽先生轉知奉系首領張作霖，於 1922 年 10 月 5 日曹錕以 480 票當選大總統後通電全國反對非法賄選，登諸報章，全部事實確鑿，舉國嘩然。此後蔣宗標先生採用「抄本加聯句」，改進奉系加解密方法；所謂「抄本」就是將「明碼本」重新編排，「聯句」即為將常用「術語」整句編碼，除提高安全度外，尚能節省時間與成本。

1928 年 10 月，任職交通部國際電訊局局長的哈佛大學物理學博士溫毓慶先生，因對股票也偶爾參與買賣並炒作，研究用「金匙」加解密之密電破解方法，對破密分析甚有心得，由關務署署長張福運先生轉知宋子文先生後，立即撥發經費，由溫毓慶先生主持加、解密分析的研究。1930 年 10 月，溫毓慶先生任職交通部電政司司長後，開始研究破解日本外交密電的方法，並於 1935 年正式成立「密電檢電檢譯所」，由原廣西大學數學系教授楊肆先生出任研究負責人，正式開始我國密碼學的研究工作。1939 年 6 月由軍統局代局長戴笠先生呈報軍事委員會蔣介石委員長，奉准統一中國各單位之加、解密研究機構，合併成立「技術研究室」由溫毓慶先生兼任同中將主任，軍事委員會機要室主任毛慶祥先生與軍事委員會第四處處長兼軍令部第四處處長兼任副主任；「技術研究室」於 1940 年 4 月 1 日正式成立，共分六組，各組組長與首席秘書均為少將軍階，奠定我國密碼研究機制的基礎。1993 年 12 月 30 日，總統令公布「國家安全局組織法」明定由國家安全局統籌全國密碼管制政策及研發等有關事項，並分由第五處與第六處掌理電訊安全工作與密碼及其裝備之管制、研製之有關事項；1994 年 5 月 21 日中華民國資訊安全學會在台北市正式成立【99】，更使我國之密碼學的研究日漸普及。

密碼學及其應用技術，如表 5.8 所示，除牽涉到國家安全之使用環境，我國無論是在政府或民間，除瓦聖那協議之要求外，於使用管制、驗證管理與依法取用方面，幾均無主責機構，建請考慮早日建立通資訊安全產品認、驗證體系與檢測實驗室，提供類似電信法第六條第 2 項：「電信事業應採適當並必要之措施，以保障其處理通信之秘密。」所需之「安全品質」服務。換言之，我國之通資訊安全產品「使用管制」政策應可以「保障通資訊安全及維護使用者權益」為基礎來律定相關規範，再依據 2005 年 11 月 9 日正式公布之「國家通訊傳播委員會組織法」第三條法定其掌理之「資訊安全之技術規範及管制。」建制其運作機制。1995 年 4 月 27 日使用廣泛的個人電腦硬碟介面 ATA(Advance Technology Attackment)第 3 代，ATA-3 第 1 版，已規劃如表 5.9、圖 5.5 與圖 5.6 所示之依法取用機制【92】，在我國之使用者幾無人知道其使用之筆記型電腦中之「主密碼」之現況，於我國密碼技術應用的情形，可見一斑。自 ATA 使用密碼技術增進安全起，內嵌如圖 2.2 與圖 2.4 所示之可信賴平台模組(Trusted Platform Module, TPM)的可信賴計算平台(Trusted Computing Platform, TPC)

電腦(例：HP、聯想、宏碁等)均已產製中【92】；配合密碼技術之大量使用的資料儲存密碼技術之工業標準亦在製定中【21~22】。如何防止如表 5.10 所示之 Crypto AG 事件的發生，宜是我國通資訊安全產品管制應面對的之議題。

表 5. 8：美國、中華人民共和國與台灣之密碼技術管制政策比較

	出品管制		使用管制				安全驗證			
	產品	法規	產品		演算法		產品		演算法	
			機密	一般	國家機密	其他	政府	民間	政府	民間
美國	有	有	有	有	有	有	強制	自願	強制	自願
中華人民共和國	有	有	有	有	有	有	強制	強制	強制	強制
台灣	有	有	有	未知	有	未知	未知	未知	未知	未知

表 5. 9：ATA-3 磁碟機安全機制分類示意

	高安全 (High Security)	最大安全 (Maximum Security)
主密碼 (Master Password)	當終端使用者密碼遺失時，解除硬碟機的閉鎖狀態。	當終端使用者密碼遺失時，必須清除硬碟機內的所有資料。
終端使用者密碼 (End User Password)	必須用來啟動安全模式，解除硬碟機的閉鎖狀態以進行資料存取	必須用來啟動安全模式，解除硬碟機的閉鎖狀態以進行資料存取

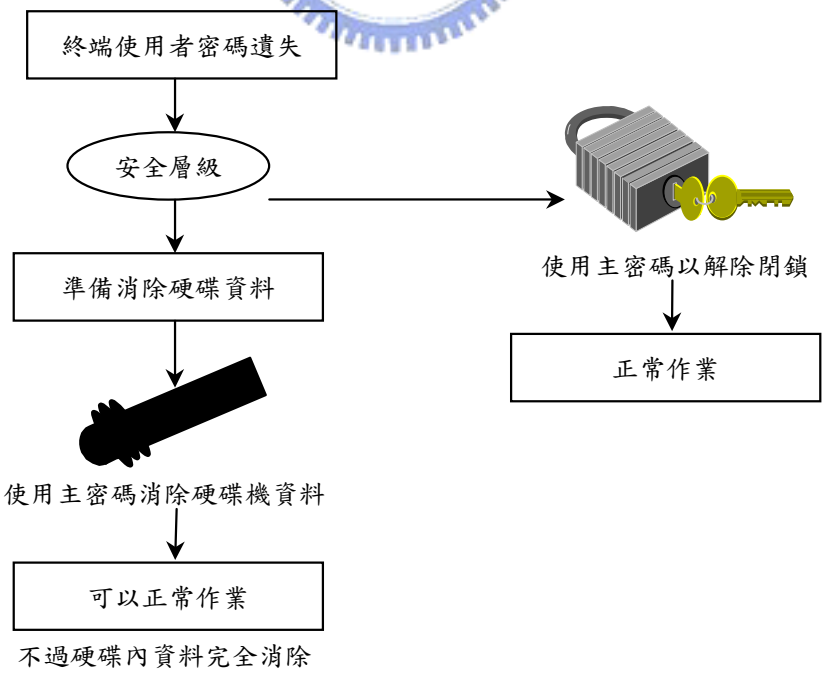


圖 5.5：ATA-3 磁碟機安全機制作業示意之一

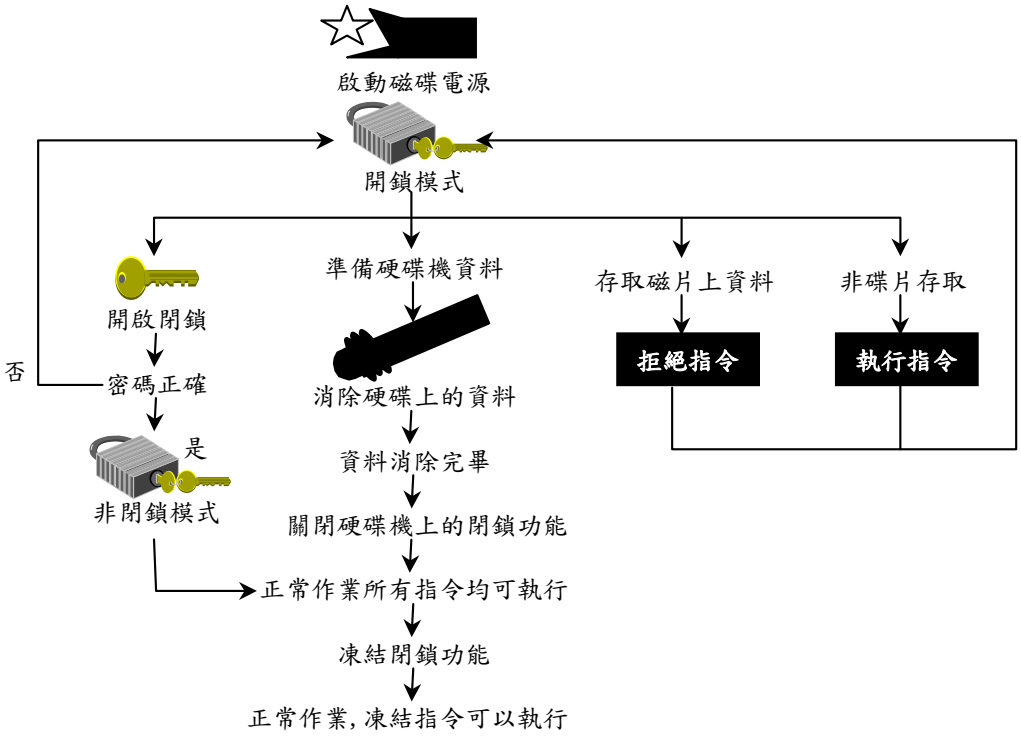


圖 5.6：ATA-3 磁碟機安全機制作業示意之二

表 5. 10：Crypto AG 與 Hans Beuhler 先生的故事

1. 1992 年，Crypto AG 一名業務員 Hans Beuhler 先生被伊朗警方逮補，並且控告他是美國和德國的間諜。9 個月以後，Crypto AG 以 U.S.$1,000,000 換取 Hans Beuhler 先生的自由，但在 Hans Beuhler 先生回到瑞士後將其解僱。
2. Hans Beuhler 於傷心困惑之餘，與同事討論他的遭遇時，「Crypto AG 的創辦人 Boris Hagelin 先生於 1957 年接受美國國家安全局密碼專家 William Friedman 先生在 Crypto AG 所產生的每一部密碼機中留一道後門的建議；從此之後，Crypto AG 幾壟斷密碼機市場。1970 年與德國情報機構有密切淵源的西門子公司（Siemens AG）取得 Crypto AG 的控制權；所以，美國與德國均知曉 Crypto AG 密碼機的演算系統及其細節。」的傳言成為媒體炒作的新聞，Crypto AG 的商譽受到嚴重的打擊。
3. Crypto AG 於 1994 年上法院控告 Hans Beuhler 先生，但當來愈來愈多的 Crypto AG 離職員工被傳為證人後，這個案子不久就在庭外達成和解。

六、數位社會密碼政策初探（代結論）：

在今日資訊化的時代，密碼模組的應用範疇，已是無遠弗屆，幾達網站架設之地，即有運用密碼之處。「劍有雙刃，可以自衛，亦可傷人。」，密碼技術固然是奠定資訊社會安全之基石，在另一方面，也是犯罪的利器，能輕易妨礙治安單位對犯罪行為的防範、偵測與依法取用。在電子化/網路化資訊社會中如何訂定與執行適當之密碼政策，先進國家在此問題上的曲折經驗自有值得借鏡之處。密碼模組內嵌於作業系統底層的技術，具備「使用便捷」之性質，在 TCP 逐漸普及後，除增進資訊社會的安全性，更涉及資訊權自主之國家安全議題。在另一方面，資料加密問題因需兼顧個人隱私與群體安全，所有抉擇均得失互見，極難面面俱到；在此一公共政策訂定與執行之後，如何保障國家安全與國民「遺失不懼」的秘密通訊自由而又能在必要時，由政府執法人員能在法律許可範圍內，依法實施監聽或開啟「電子化/網路化社會」中之「電子銀行保險箱」、「加密之電子信封」等的「金鑰回復式密碼系統（Key Recovery System，簡稱 KRS）」，已是全球各國政府、研究及學術機關積極研究、實驗或執行的課題。

一個能適當保護個人隱私的金鑰回復式密碼系統（Key Recovery System，簡稱 KRS），依法取用(Lawful Access)時，技術上必須使執法人員在取得使用者數位信封(Digital Envelope)等金鑰之後，無法擴張其依法取用的權利；也就是說應具備能確保同一家族中未被「依法取用」之其他使用者「回復金鑰」的安全度及執法人員取得之「回復金鑰」在「依法取用」結束後自動失效，的兩項功能【13, 62, 98】。聯合報於 1999 年 6 月 13 日以社論：「交出大門鑰匙：密碼模組豈可向政府報備？」表達對「電信法 22 條修正案」中「依法取用」運作的觀點，正是社會大眾對非法監聽恐懼的寫照。唯有在政府業務主管部門於製訂「通訊安全密碼模組安全需求」時，清楚規範「回復金鑰」在「依法取用」過程中，「能適當保護個人隱私」之應有安全機制，方能釋疑。

2003 年 9 月 26 日公布之「國家機密保護法施行細則」第 21 條第 4 項：「以電子通信工具傳遞國家機密者，應以加裝政府權責主管機關核發或認可之通信、資訊保密裝備或加密技術傳遞。」已規範我國通信、資訊保密裝備或加密技術應用於傳遞國家機密之電子通信工具，應由政府權責主管機關核發或認可。2005 年 5 月 27 日發布之「政府機關密碼統合辦法」共 24 條，規範國家安全統合政府機關密碼暨其裝備之研發、鑑測、密碼作業與保密業務的框架。綜前所述，無論是 TPM 還是金鑰回復式密碼系統之研發與鑑測工作均需 3~5 年方見成效。

依據國家安全局組織法第十八條，我國已成立「中央密碼管制協調會報」，由國家安全局局長擔任主席，審查密碼管制政策、指導推動政府機關密碼管制工作，分政務、外交、軍事、情報 4 體系，逐級推動密碼管制業務。

研究「政策」是需要「同情」與「推理」能力，「同情」是制定「政策」的人有相同之情，那樣體驗的「政策」自然是立體、多元的。「同情」加上「推理」，則「政策」是活的，每一分「政策」之頒布是因或是果，是一個趨勢的契機或是成績。「政策」是無數偶然形成，但是亦絕非偶然，「政策」從長遠的角度來看，便可以體察出是有一股流勢，勢不可當，有無法阻擋的推移之力。掌握先機，盱衡各國密碼政策之現況，綜整前述可信賴平台模組、回復式金鑰密碼系統與密碼技術應用鑑測的發展方向，審時度勢，擬案如下：

6.1、遵循國際標準發展趨勢，根基於「資訊安全保證」，分從「需求、安全服務、指導綱要」、「安全技術與機制」及「安全評估準則」3 個構面，制定密碼技術及其應用宜遵循之規範：

國際間資訊安全標準因密碼學研究之成果逐漸在政府大量使用，於 1977 年 1 月 5 日，美國頒布聯邦資訊處理標準(Federal Information Processing Standards，簡稱 FIPS)出版品(Publication)第 46 號之資料加密標準(Data Encryption Standard，簡稱 DES)起，隨著金融交易的需求，至 1987 年 6 月 1 日國際標準組織(International Organization for Standardization，簡稱 ISO)負責：「銀行、安全與其他金融服務(Banking, Securities and Financial Services)」之第 68 技術委員會(Technical Committee，簡稱 TC68)根基於 DES，頒布了 ISO 8731，成為第 1 份 ISO 之資訊安全的國際系列標準【31~32】。

為制定密碼技術之標準，負責訂頒資訊處理(Information Rocessing)標準之 ISO TC 97 於 1981 年 1 月召開第 1 次之第 1 工作會(Working Part 1，簡稱 WP1)，自 1983 年起，TC 97 WP1 將此項工作轉交由德國標準機構支援的「資料密碼學技術(Data Cryptographic Techniques)」的 20 分組(Subcommittee，簡稱 SC20)，SC20 下轄秘密金鑰演算法與應用(Secret Key Algorithms and Applications)之第 1 工作小組(Working Group，簡稱 WG1)、公開金鑰密碼系統與模式的使用(Public Key Crypto - Systems and Modes of Use)之 WG2 與在通訊架構中使用加密技術(Use of Decipherment Techniques In Communication Architectures)的 WG3，正式展開資訊安全國際標準的制定工作。1986 年上半年，美國書面建議 TC97 修正 SC20 之工作範疇，不要再發展加密演算法之標準；TC97 在 1986 年 5 月召開會員大會(Plenary Meeting)，將此數個會員國關切的政治上敏感之議題提交 ISO 會議(Council)，ISO 會議決定不頒布加密演算法之 ISO 8227，同時調整 TC SC20 的工作方向【6, 64】。

1989 年，由 ISO 與國際電工協會(International Electro-technical Commission，簡稱 IEC)，在根基於共同與一般之安全測量標準已取代僅根基於密碼學應用之特定範圍標準的制定工作，成立如圖 6.1 所示之 ISO/IEC 第 1 聯合技術委員會(Joint Technical Committee，簡稱 JTC1)的資訊技術(Information Technology，簡稱 IT)安全技術(Security Techniques，簡稱 ST)之第 27 分組委員會(Sub-Committee，簡稱 SC27)。ISO/IEC JTC1/SC27 下轄 3 個工作組(Working Group，簡稱 WG)分別就資訊安全之「需求、安全服務與指導綱要(WG1)」、「安全技術與機制(WG2)」及「安全評估準則(WG3)」，負責研擬 ISO/IEC JTC1/SC27 計畫制定之標準草案等工作。

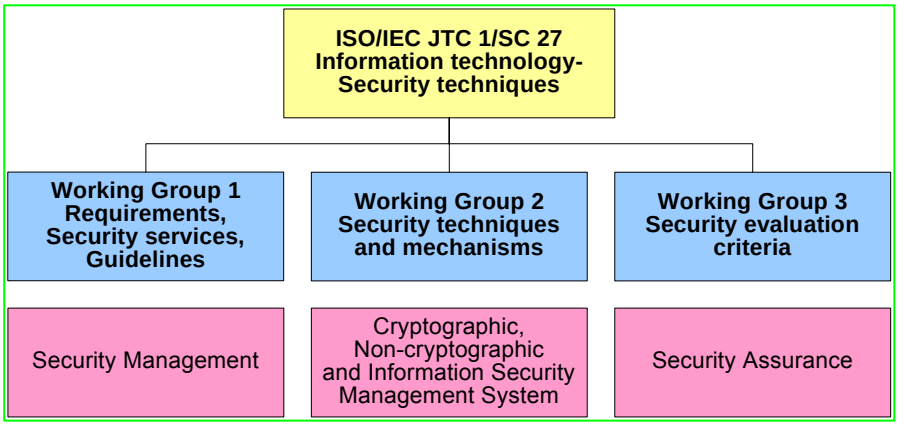


圖 6.1：ISO/IEC JTC1/SC27 組織架構

ISO/IEC JTC1/SC27 下轄 3 個工作小組遵循如下之步驟制定國際標準：

(1). 研究階段(Study Period)：就一標準之需求非正式的交由委員會加以研究，將其結果就此需求刪除或提交新工作項目建議書(New work item Proposal，簡稱 NP)進行票決。

(2). 新工作項目建議書(NP)階段：完成提交 JTC1 秘書處之建議書。

(3). 工作草案(Working Draft，簡稱 WD)階段：分項委員會(SC)或工作小組(WG)內部文件集。

(4). 委員會草案(Committee Draft，簡稱 CD)或技術報告草案建議(Proposed Draft Technical Report，簡稱 PDTR)階段：當 WD 考量其穩健性已足夠充分後，由分項委員會向 ISO/IEC 之資訊技術工作組(Information Technology Task Force，簡稱 ITTF)登錄成為 CD，由 SC 國家會員代表在 3 個月內投票並提出評論，相關文件由 JTC1 派送。

(5). 國際標準草案(Draft International Standard，簡稱 DIS)或技術報告草案(Draft Technical Report，簡稱 DTR)階段：當 CD 或 PDTR 已充分討論，無技術面被期待之修改，SC 向 ITTF 提出票決成為 DIS 或 DTR，由 JTC1 國家會員代表 4 個月內投票並提出評論。

(6). 國際標準(International Standard，簡稱 IS)或技術報告(Technical Report，簡稱 TR)階段：遵循 IS 或 TR 出版之程序，就各個國家會員代表發現技術錯誤的瑕疵報告(Defect Report)，SC 決定此 IS 或 DTR 修正、取消或頒布 IS 或 TR。

(7). 審核(Review)階段：每份 IS 或 TR 在 5 年內應重新審核，由 SC 負責提出 IS 或 TR 宜修正、作廢或維持之確認報告後，由 JTC1 決定。

表 6.1 是 ISO/IEC JTC1/SC27 WG3 已頒布和正制定中之國際標準，密碼模組之測試與角色基存取控制均已進入 NP 階段，表 6.2 是 ISO 之國際標準制定、發行等流程的示意說明。

ISO TC68 密碼演算法標準繼續 TC97 SC20 的類似工作，差別僅在銀行(Banking)還是資訊技術(Information Technology)而已。1996 年 10 月 ISO 與國際電工協會(International Electro-technical Commission，簡稱 IEC)轄下之第 1 聯合技術委員會(Joint Technical Committee 1，簡稱 JTC1)之 SC27 的會員大會中，於已取得 ISO 會員國之共識，建議恢復 SC20 的工作範疇，1996 年 12 月之 JTC1 會員大會中，全體一致同意 ISO/IEC JTC1/SC27 包含制定密碼演算法國際標準在內之新工作方向。

2003 年 9 月，美國國家標準與技術研究院(National Institute of Standards and Technology，簡稱 NIST)負責制定資訊安全管理聯邦標準成員之一的 Katzke, S.博士，正式向 ISO/IEC JTC1/SC27 提出如圖 3.7 之框架與支持制定資訊系統安全管理相關標準的說明，已成為 ISO 現階段安全保證鑑測機制之參考框架【39, 63】。

「他山之石，可以攻錯」，ISO 歷經「資料加密」、「資訊安全」、「資訊安全保證」3 個階段之成果，如圖 6.2 所示之圖 3.7 中使用的 FIPS 140-2 與共同準則的比較分析【35】等，均可做為現階段我國制定「密碼技術及其應用」相關規範之參考。

表 6. 1：ISO/IEC JTC1/SC27 WG3 (Security Evaluation) 已完成與進行中計畫

1. 資料來源：ISO/IEC JTC1/SC27 WG3 召集人 Ohin, M., 2005 年 9 月 28 日之報告與本研究自行蒐集所得。
2. SC27 目前有 31 個有投票權的成員，11 個無投票權的觀察員。
3. SC27 已完成與進行中之計畫：
   - 3.1 ISO/IEC 15292 (2001-12-15)：Protection Profile Registration Procedures。
   - 3.2 ISO/IEC 15408 (1999-12-1)：Evaluation Criteria for IT Security。
   - 3.3 ISO/IEC FDIS 15408 (CC 2.3) (2005-1-1)：Evaluation Criteria for IT Security。
   - 3.4 ISO/IEC WD 15408 (CC 3.0) (2005-4-1)：Evaluation Criteria for IT Security。
   - 3.5 ISO/IEC TR 15443-1 (2005-2-1)：A Framework for IT Security Assurance (註：ISO/IEC TR 15443-2 已進入出版階段，ISO/IEC 15443-3 目前停滯於 5th WD 中)。
   - 3.6 ISO/IEC TR 15446 (2004-7-1)：Guide on the Production of Protection Profiles and Security Targets (PPST Guide)。
   - 3.7 ISO/IEC FDIS 18045 (CC 2.3)(2005-1-1)：Methodology for IT Security Evaluation (CEM)。
   - 3.8 ISO/IEC WD 18045 (CC 3.0)(2005-4-1)：Methodology for IT Security Evaluation (CEM)。
   - 3.9 ISO/IEC FCD IS 19790 (2005-05)：Security Requirements for Cryptographic Modules。
   - 3.10 ISO/IEC DTR 19791 (2005-06-30)：Security Assessment of Operational Systems。
   - 3.11 ISO/IEC 3rd WD 19792 (2005-1-17)：A Framework for Security Evaluation and Testing of Biometric Technology (SETBIT) 。
   - 3.12 ISO/IEC 21827 (2002-10-1)：Systems Security Engineering - Capability Maturity Model (SSE-CMM)。

表 6. 2：ISO 之國際標準制定、發行等流程

階段	子階段						
	00	20	60	90 決議			
	註冊	主要活動的開始	主要活動的完成	92 重複之前的階段	93 重複現在的階段	98 中止	99 繼續進行
00 預備階段	00.00 NP 已收到	00.20 NP 等待審核	00.60 審核摘要被傳遞			00.98 NP 被中止	00.99 NP 被批准被投票
10 提案階段	10.00 NP 被註冊	10.20 NP 投票開始	10.60 投票摘要被傳遞	10.92 提案被退回提交者再做定義		10.98 NP 被拒絕	10.99 NP 被批准
20 籌備階段	20.00 NP 被註冊為 TC/SC 工作計畫	20.20 WD 研究啟始	20.60 評論摘要被傳遞			20.98 計畫被刪除	20.99 WD 被批准登錄成為 CD
30 委員會階段	30.00 CD 被註冊	30.20 CD 研究/投票開始	30.60 評論/投票摘要被傳遞	30.92 CD 被交付退回給 WG		30.98 計畫被刪除	30.99 CD 被批准登錄成為 DIS
40 詢問階段	40.00 DIS 被註冊	40.20 DIS 投票啟始：*5 個月*	40.60 投票摘要被派送	40.92 全部報告被傳遞：DIS 被交付退回給 TC/SC	40.93 全部報告被傳遞：決議為新 DIS 投票	40.98 計畫被刪除	40.99 全部報告被傳遞：DIS 被批准登錄成為 FDIS
50 批准階段	50.00 FDIS 被註冊為正式批准	50.20 FDIS 投票啟始:*2 個月* 論證被送到秘書處	50.60 投票摘要被派送 論證被秘書處退回	50.92 FDIS 被交付退回給 TC/SC		50.98 計畫被刪除	50.99 FDIS 被批准出版
60 出版階段	60.00 IS 等待出版		60.60 IS 被出版				
90 審核階段		90.20 IS 等待定期的審核	90.60 審核摘要被派送	90.92 IS 被修正	90.93 IS 被確認		90.99 撤銷的 IS (由 TC/SC 所起草)
95 撤銷階段		95.20 撤銷投票啟始	95.60 投票摘要被派送	95.92 決議不撤銷 IS			95.99 撤銷的 IS

說明：

1. 資料來源：http://www.iso.org/iso/en/widepages/stagetable.html。
2. WG：工作小組(Working Group)。
3. TC：技術委員會(Technical Committee)。
4. SC：分組(Sub-committee)。
5. NP：新工作項目建議書(Proposal for New Project)。
6. WD：工作草案(Working Draft)。
7. CD：委員會草案(Committee Draft)。
8. DIS：國際標準草案(Draft International Standard)。
9. FDIS：最終國際標準草案(Final Draft International Standard)。
10. IS：國際標準(International Standard)。
11. TR：技術報告(Technical Report)。

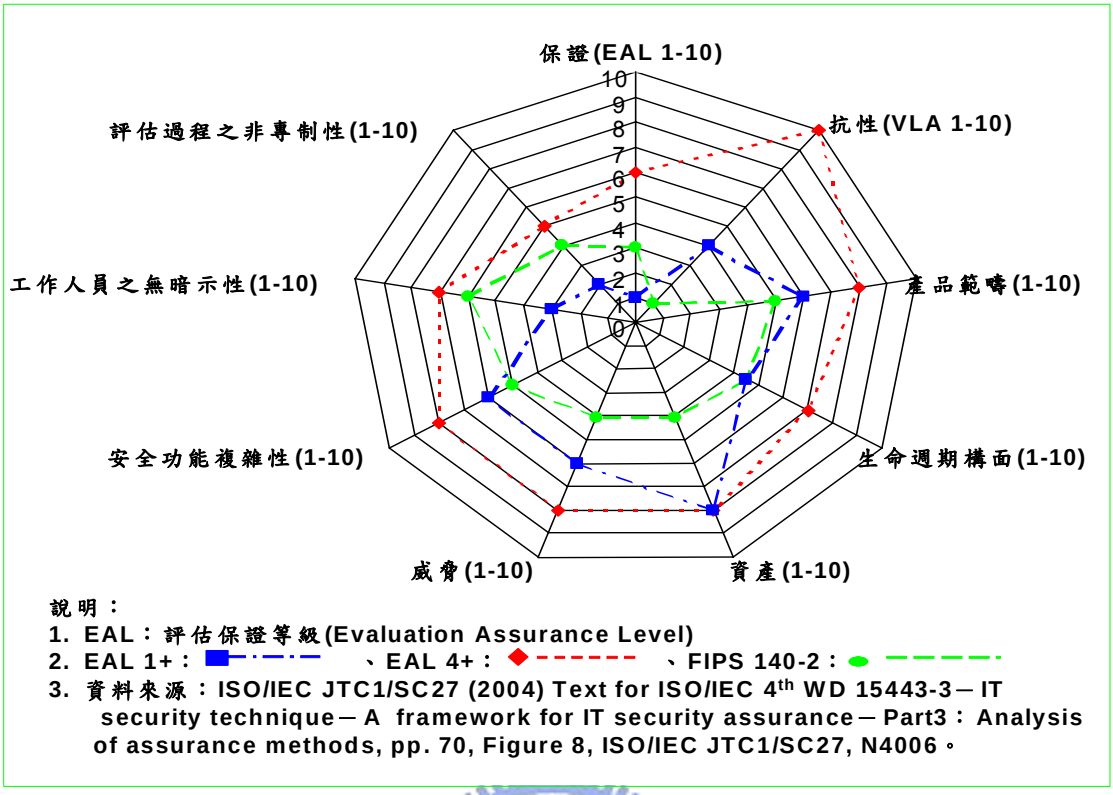


圖 6.2：NIST FIPS 140-2 與 ISO/IEC 15408: 1999(E) EAL: 之蛛網比較圖

6.2、建立能提供海峽對岸網軍攻擊之「密碼技術及其應用」的資訊安全保證之研發能量：

「密碼技術及其應用」之複雜度已至空前的等級，增加組織建立暨使用資訊安全之挑戰。這些挑戰存在於整個系統生命週期中，及其結構細節等級中，它們的產生來自許多源池：

(1).所建立之「密碼技術及其應用」的硬體、軟體與使用者之間固有的差異。

(2).「密碼技術及其應用」涉及之專業領域缺乏調合與整合，其深層知識包括科學、工程與管理。

(3).幾乎每個資訊安全系統均植基於密碼技術及其塑模之支援，而其技術尚在發展中。

因此，「密碼技術及其應用」之資訊安全保證宜建立包括「密碼技術及其應用」可信賴資訊使用環境生命週期所涵蓋範疇的共同框架，以已獲得 10 張以上 FIPS 140-2 與 3 張以上共同準則驗證合格證書之微軟公司為例，圖 6.3 是其可信賴資訊使用環境生命週期示意說明。舉例而言，如圖 6.2 所示，FIPS 140-2 於「資料保密」的資訊使用環境或許可以信賴，其在銀行作業「資訊安全」完整性非常重要之資訊使用環境中，無法滿足表 4.11 的密碼裝置符合性檢查項目【36】；隨著「密碼技術及其應用」之日益普及，法國已正式提出於「密碼模組安全需求」之國際標準中，宜加入「共同準則(ISO/IEC 15408)」的考量，其中尤其是脆弱性評鑑部分應考慮如表 6.3 與 6.4 所示之測量【41】，美國 NIST 已承諾在預定於 2007 年 5 月出版之 FIPS 140-3 中納入；整合 FIPS 140-2 與共同準則方能有效鑑測出諸如「網路 ATM(Automatic Teller Machine)遇駭，3 秒盜走 10 萬」的風險【68】。

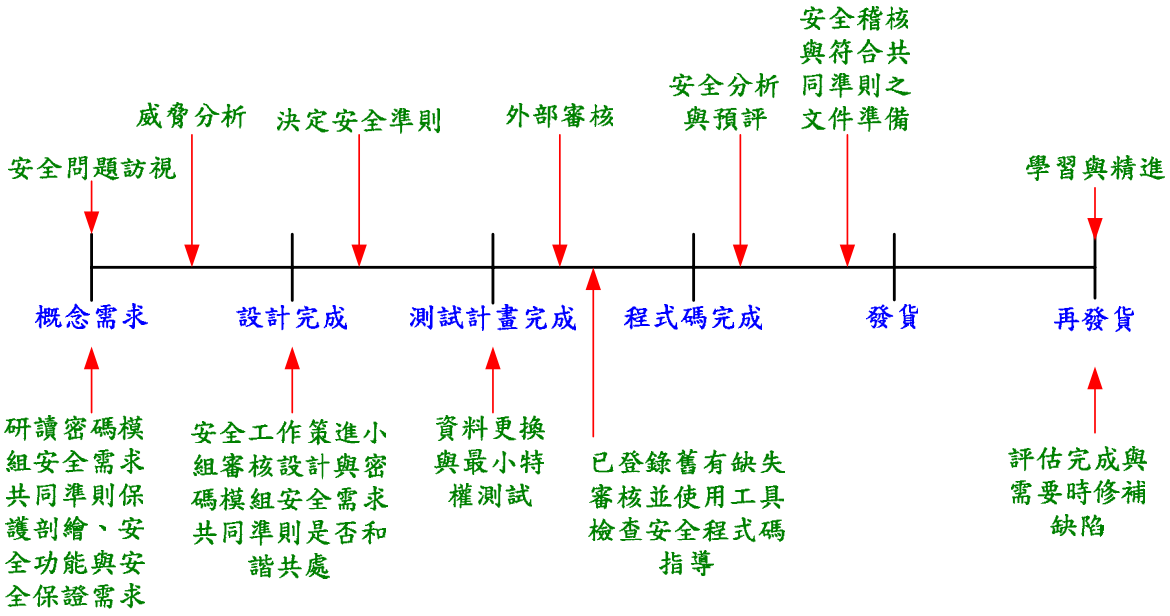


圖 6.3：微軟公司之可信賴資訊使用環境生命週期

表 6. 3：潛在入侵(Attack Potential)計算對照表 (* 代表超越高度困難之潛在入侵，**代表幾不存在可開採之潛在入侵路徑)

因素	範圍	鑑別參考值
開採花費時間	小於一天	0
	小於一週	1
	小於一個月	4
	小於三個月	13
	大於三個月	26
	一切實際	*
專業技術層次	門外漢	0
	熟練者	2
	專家	5
需具有之評估標的相關知識	公開	0
	內部資訊	1
	敏感資訊	4
	關鍵資訊	10
機會之窗	不需要/存取不受限制	0
	容易	1
	適度	4
	困難	12
	無	**

所需之相關設備	標準的	0
	特殊的	3
	特製的	7

1. 說明：潛在脆弱性開採類別(Attempted Exploitation of Potential Vulnerabilities，簡稱 PAV)之屬別(Families)與組件(Components)：
   1.1. 開採花費時間(Time taken to identity and exploit，簡稱 PAV_TTE)：6 組件。
   1.2. 專業技能需求(Specialist technical expertise required，簡稱 PAV_STE)：3 組件。
   1.3. 評估標的設計與操作之知識(Knowledge of the TOE design and operation，簡稱 PAV_KNO)：4 組件。
   1.4. 機會之窗(Window of opportunity，簡稱 PAV_WOP)：5 組件。
   1.5. 開採所需之資訊技術硬體與軟體或其他設備(IT hardware/software or other equipment required for exploitation，簡稱 PAV_HSW)：3 組件。
2. 資料來源：ISO/IEC JTC 1/SC 27 WG 3 (2005) ISO/IEC WD 18045：2005(E) p.293。

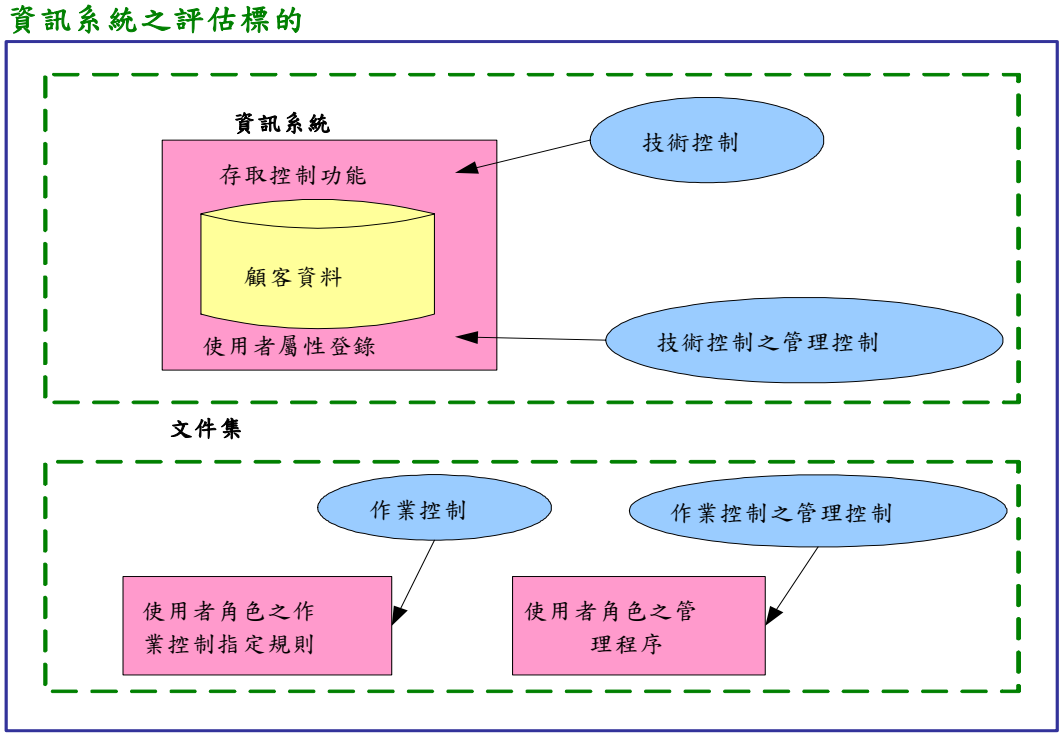
表 6. 4：脆弱性評比(Rating of Vulnerabilities)

評估值範圍	0~2	3~5	6~9	10~14	15~26	*
抵抗攻擊者潛在入侵成功之能力級別	不評比(no rating)	基礎(Basic)	基礎延伸(Extended—Basic)	適度(Moderate)	高(High)	超越高級別(Beyond High)

資料來源：ISO/IEC JTC 1/SC27 WG 3 (2005) ISO/IEC WD 18045：2005(E), p294。

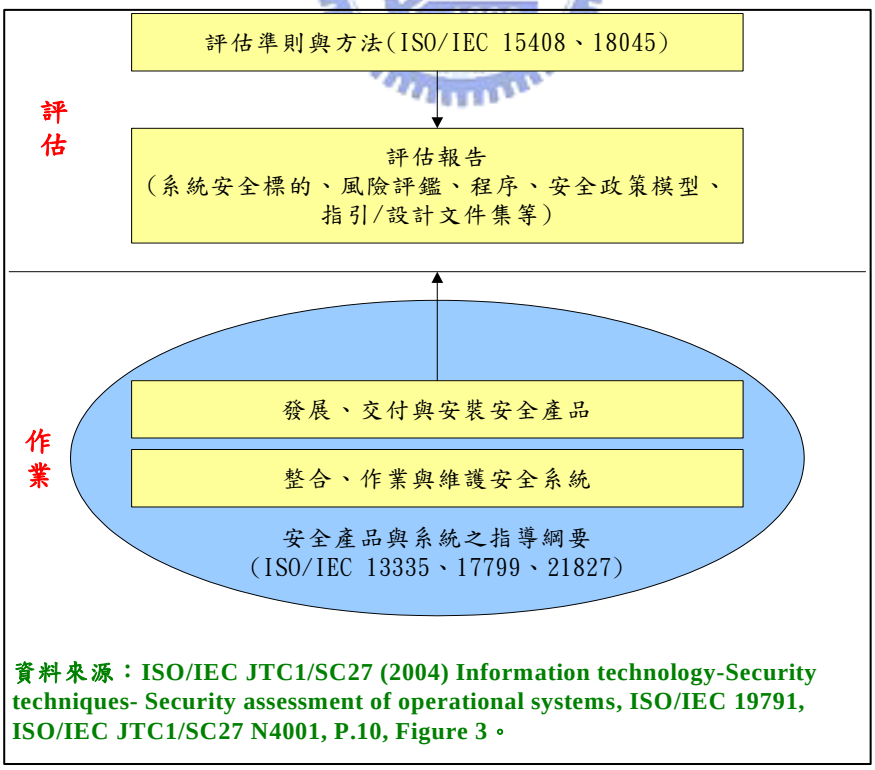
2002 年 9 月 1 日，英國泰晤士報報導，中國政府已在國務院信息產業部旗下成立秘密部門，統轄一支稱為「網路戰士」的精英小組，對美國等國際強權從事 21 世紀數位戰爭之準備【67】。要求匿名的一位中國「網路戰士」描述中國持續尋找愛國情操與才能兼備的人才，希望促使中國資訊安全策略更上一層樓，比美在 1941 年，藉助破解「奇謎(Enigma)」的優勢，實力較弱的英國扭轉歐洲第 2 次世界大戰局勢之柏雷屈里園(Bletchely Park)工作小組【89】。

綜觀前述報導，中國「網路戰士」的工作於操控網路監督網友活動、破解密碼、潛入銀行帳戶等工作，屬於資訊技術安全評估工作中之攻擊樹方法(Attack Tree Methodology，簡稱 ATM) 滲透測試方法；其冀求標的之破解奇謎的工作則屬瑕疵假設方法(Flaw-Hythesis Methodology，簡稱 FHM)，ATM 與 FHM 是滲透測試(Penetration Testing，簡稱 PT)中之兩大分支。在資訊技術安全保證(Information Technology Security Assurance)方法中，PT 已是樞紐方法之一，我國僅密碼模組安全保證作之規劃自 1998 年 10 月 15 日正式開始，成本已逾千萬，訖今尚未論及相關之滲透測試工作。一般而言，滲透測試工作是培育「網路戰士」的搖籃，亦為「網路戰士」實兵演習之合法訓練中心，於 ISO 頒佈之如圖 6.4 與圖 6.5 所示資訊系統安全評估方法，PT 亦為基石之一【37】；換言之，PT 是保證我國使用「密碼技術及其應用」的資訊系統防止大陸駭客入侵政府網站等事件的資訊安全保證之源池之一，美國聯邦政府將資訊系統安全依將面對之攻擊者等的能量分成如表 6.5 所示之低、中、高 3 級【12】，表 6.6 是表 6.5 中低攻擊能量示意，表 6.7 是表 6.5 中的中級攻擊能量示意，前述「柏雷屈里圖工作小組」是表 6.5 中之高級攻擊能量示意，中國「網路戰士」應已具備表 6.5 中的高級攻擊能量【24, 65, 73, 80, 97】。



資料來源：ISO/IEC JTC1/SC27 (2005) Information technology - Security techniques - Security assessment of operational systems, ISO/IEC DTR 19791, page 17, Figure 5。

圖 6.4：資訊安全管理系統之控制類別關連示意



資料來源：ISO/IEC JTC1/SC27 (2004) Information technology-Security techniques- Security assessment of operational systems, ISO/IEC 19791, ISO/IEC JTC1/SC27 N4001, P.10, Figure 3。

圖 6.5：資訊系統作業環境與評估準則之關連示意

表 6. 5：美國 C&A 過程計畫之安全控制選擇與實作的攻擊者等資源分類示意

	低	中	高
攻擊者	個體戶	有組織的團體	涉及國家之組織與團體（例：網軍）
預算	≦U.S. $1,000,000	≦U.S. $10,000,000	＞U.S. $10,000,000
技能	自學	有計畫之訓練	有計畫與控制之訓練

表 6. 6：1998 年 5 月印度巴琵原子研究中心事件

1. 1998 年 5 月綽號「t3k.9」的 15 歲美國少年，因在電視上看到了印度與中國、巴基斯坦進行核武競賽的新聞，基於「人道」還是「第三世界的普羅大眾的貧窮」等未知原因而氣憤不已。
2. t3k.9 撥入 Infoseed 的搜尋引擎，接通「in atomic」，出現了印度巴琵原子研究中心(Bhabha Atomic Research Center，簡稱 BARC)，點選 BARC 使用(John Ripper DES Encryption Cracker)進行攻擊，45 秒後，t3k.9 發現已成為 BARC 的合法用者。
3. 幾天後，t3k.9 將整個 BARC 的通行碼檔案(約 800 個合法使用者)公佈在駭客頻道，BARC 遭到上百次之駭客攻擊。

表 6. 7：抵抗中度(Moderate)潛在入侵之滲透測試例─神鬼尖兵(Sneaker)真實版例

1 Source：Behar, R. (1997) Who's reading your e-mail?, FORTURE, Feb. 1997, pp.36~46.

2 WheelGroup Corp. 總裁在 1996 年 10 月宣稱面對：
2.1 擁有大型網路的公司(例：財星 500 大)，我們一個下午即可以侵入。
2.2 小型公司，僅需 2 個小時就可以侵入。

3 財星雜誌徵得排名 500 大之內的 XYZ 跨國企業參加測試，並由著名的 Coopers &Lybrand 會計師事務所(全球六大會計師事務所之一，首創電腦稽核業務)協防。

4 WheelGroup Corp. 五人小組於 D 日凌晨 1:10 開始作業。

5 經過 16 個小時，於 1500 次的撥號測試後過濾出 55 個可能有機會的數據機專用號碼。

6 D 日晚上 21:13，使用字典攻擊法，WheelGroup Corp 五人小組獲得賓果大獎。

7 D + 1 日凌晨 0:01，WheelGroup Corp 五人小組再度以字典攻擊法成功的控制了 XYZ 公司稅務(Tax)部門的資訊系統。

8 D + 1 日凌晨 2:02，WheelGroup Corp 五人小組再一次以字典攻擊法成功的控制了 XYZ 公司技術 (Technology)部門的資訊系統。

9 WheelGroup Corp 五人小組使用偽造的 XYZ 公司員工帳號發出一封致批准此次實驗計畫的主管，請求核准獎勵參加此次「財星試驗 (FORTUNE's experiment) 計畫」的員工 5,000 元美金聖誕節獎金的電子郵件。

10 XYZ 批准此次實驗計畫的主管立刻裁示：「Okey, fine」，實驗結束。

11 結論：
11.1 因資訊安全系統役於人，所以符記卡(例: IC 卡)於資訊安全系統的使用上非常重要。
11.2 使用者的行為必須配合安全控管的要求，方能確保資訊系統的安全。

在 ISO 之主導下，資訊安全保證分成發展保證(Development Assurance，簡稱 DA)、整合保證(Integration Assurance，簡稱 IA)與作業保證(Operation Assurance，簡稱 OA)3 個構面，無論是 DA、IA 還是 OA，我國均少有人涉獵；舉例而言，「密碼技術及其應用」中，對抗網軍攻擊應執行的「正規分析」與「密碼協定安全性分析」於我國密碼學研發領域中仍屬罕見，即可見一斑【4, 68, 75】。

沒有人會懷疑中國大陸具有犯台的決心、企圖與準備，「人無遠慮，必有近憂」，鑑於「不分平時、戰時，任何用來影響對方資訊與通資訊系統，同時防護我方資訊與通資訊系統的行動。」均屬資訊戰，及其首戰即是決戰的特性。在我國通資訊基礎建設對「密碼技術及其應用」的依賴性逐漸昇高之時，如何因應資訊與通信、財務與金融、重要民生服務、實體配送以及能源等之通資訊基礎建設的安全保護工作亦日益重要。我國在邁向數位化生活之時，應慎密、深沈的考慮面對台灣之機會與威脅，建立能提供海峽對岸網軍攻擊的「密碼技術及其應用」資訊安全保證之研發能量的策略與執行計畫，實為當務之急。

「密碼技術及其應用」之工作，非常講究基本功，一定要經過長期的努力經營，方能有實實在在之成果；除前述營建與厚植我國「密碼技術及其應用」能量的策略面建議外，考量國內外之環境與海峽對岸的威脅，在密碼督導機關之組織架構下，於立即可操作的面向，提案如下：

(1). 參照美國之要求與 ISO 的標準(含 NP、WD、CD、PDTR、DIS 及 DTR)，規劃分成管理(Manage)、籌獲(Acquire)、設計與發展(Design and Development)、實作與作業(Implementation and Operation)、審核與評估(Review and Evaluation)之「密碼技術及其應用」的基礎(Beginning)、中級(Intermediate)及進階(Advanced)課程。

(2). 就我國已有基礎之公開金鑰基礎建設(Public Key Infrastructure，簡稱 PKI)，檢討其資訊安全保證的符合性及其改進方案。

(3). 建置我國如圖 3.6 所示之電子化政府的金鑰管理基礎建設(Key Management Infrastructure，簡稱 KMI)。

(4). 建立我國如圖 6.6「密碼技術及其應用」之資訊安全保證鑑測機制。

(5). 研發能對抗網軍攻擊之可信賴平台模組。

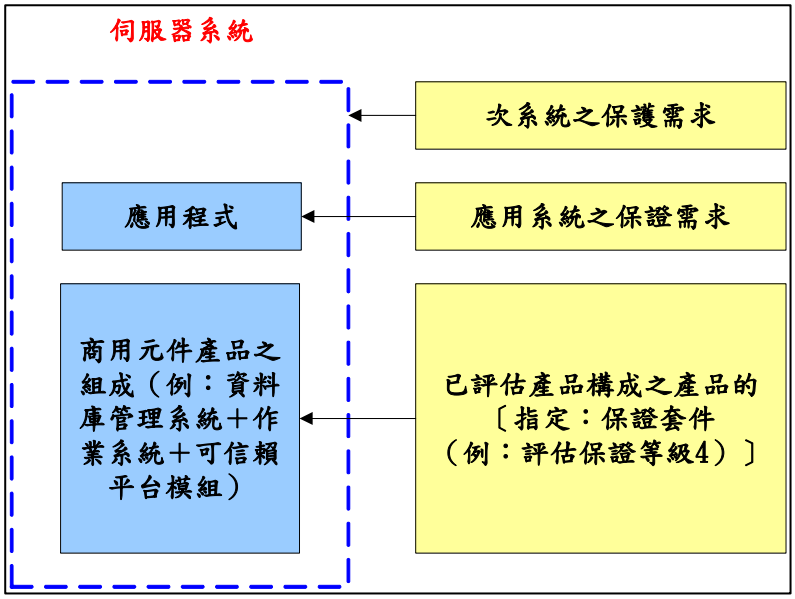


圖 6.6：密碼技術及其應用鑑測之組成(Composition)示意

6.3、實作機制：

2005 年 11 月 9 日，總統正式公布 2005 年 10 月 25 日立法院第六屆第二會期第七次會議通過之「國家通訊傳播委員會組織法」，其中第三條律定「國家通訊傳播委員會」掌理「資通安全技術規範及管制」；換言之，本文提出的「密碼技術及其應用宜遵循之規範」應由「國家通訊傳播委員會」主責，執行 2005~2008 年度「建立我國通資訊基礎建設安全機制計畫」要求的「設立資通安全軟、硬體產品驗證機構及建立認證／驗證程序」之重要措施，實作「推廣民間機構落實資通安全產品驗證規範」與「建立資通安全產品驗證體系」兩項行動方案【71】。

「建立能提供海峽對岸網軍攻擊之密碼技術及應用的資訊安全保證之研發能量」，建議由經濟部主責，先行納入 2005~2008 年度「建立我國通資訊基礎建設安全機制計畫」要求之「研發資通安全技術，推廣研發成果，移轉民間應用發展」行動方案中實作；為求完備，宜比照「密碼技術及其應用宜遵循之規範」將其層級提昇至 2005~2008 年度「建立我國通資訊基礎建設安全機制計畫」要求之重要措施，就提案的全景強化諸如：程式安全(Writing Secure Code)、強化 PKI 資訊安全保證能量【84】、KMI 之建置等項目納入國科會、教育部等已在進行中的行動方案【71】。

安全就像空氣，原本毫無價值，失去時才會痛苦覺察其存在。乙酉歲末，回顧已見成果之「密碼技術及其應用」的現今；展望未來，面對「密碼技術及其應用」普及於電子化政府中之事實，宜正視的資訊安全保證議題仍所在多有；除提出「制定密碼技術及其應用宜遵循之規範」與「建立能提供海峽對岸網軍攻擊之密碼技術及其應用的資訊安全保證之研發能量」二項政策，並在可操作的前提下，提出「密碼技術及其應用」之「認知、訓練與教育」、「PKI 與資訊安全保證」、「電子化政府之 KMI」、「資訊安全保證之密碼技術及其應用之鑑測」及「研發 TPM」等 5 項議題，若能落實，對達成使用「密碼技術」時，「使用便捷、遺失不懼」的可信賴資訊應用環境之願景，應有正面的助益。

參考文獻：

【1】 Bacon, J., K. Moody and W. Yao, (2002) A Model of OASIS Role-Based Access Control and its Support for Active Security, ACM Transactions on Information and Systems Security, Vol.5, No.4, pp492~540.

【2】 Baker, S. A. and P. H. Hurst (1998), The Limits of Trust, Klawer Law International.

【3】 Bartion, E., B. Catania, E. Ferrari, and P. Perlasca, (2003) A Logical Framework for Reasoning about Access Control Models, ACM Transactions on Information and System Security, Vol.6, No.1, PP.71~127.

【4】 Boute, R. (2005) Formal Reasoning About Systems, Software and Hardware Using Functionals, Predicates and Relations, in Information Security edited by Reis, R., pp. 85~115, Kluwer Academic Press.

【5】 Burr, W. E. Etal. (2004) Electronic Authentication Guideline, NIST SP 800-63, NIST.

【6】 Calkin, A., (1995) Nine years of an ISO/IEC Secretariat on IT security, Computer Standards and Interface, Vol. 17, pp. 139~143.

【7】 Dam, W. K. and H. S. Lin, eds (1996) Cryptography's Role in Securing the Information Society, National Academy Press.

【8】 Domingo- Ferrer,J. etal eds. (2000) Smart Card Research and Advanced Applications, Kluwer Academic Publishers.

【9】 Easter, R.J. etal. (2003) Text for ISO/IEC 2nd WD 19790, Information technology-Security techniques-Security requirements for cryptographic modules, ISO/IEC JTC1/SC 27/WG3 N637.

【10】Ferraiolo, D.F., D.R. Kuhn and R. Chandramouli, (2003) Role-Based Access Control , Artech House.

【11】Ferraiolo, D.F., S. Sandhu, D. Gavrila, D.R. Kuhn, and R. Chandramouli, (2001) A Proposed Standard for Role-Based Access Control, ACM Transactions on Information and Systems Security, Vol.4 , No.3 , pp224~274.

【12】Frederick, Cynthia, etal. (2002), Information Assurance Technical Framework 3.1, National Security Agency (http://www.iatf.net).

【13】Gennaro, R. etal. (1997) Two-Phase Cryptographic Key Recovery System, Computer and Security, Vol. 16, No. 6, pp. 481~506.

【14】GmbH and IBM, (November 26, 2003) SuSE Linux Enterprise Server V8 with Service Pack 3, Security Target for CAPP Compliance.

【15】Hamilton, B.A., (2002) Depart of Defense Public Key Infrastructure and Key Management Infrastructure Token Protection Profile (Medium Robustness), NSA (National Security Agency).

【16】Handschuh, H. and P. Paillier (1998) Smart Card Crypto-Coprocessors for Public-Key Cryptography, CRYPTOBYTES, Vo1.4, No, 1, pp.6~11.

【17】Hassler, V. etal. (2002) Java Card for E-Payment Applications, Artech House.

【18】Hendry, M. (2001) Smart Card Security and Applications, 2nd ed., Artech House.

【19】Housley, R. and T. Polk (2001) Planning, for PKI, Wiley.

【20】Howard, M. and D. LeBlanc (2003) Writung Secure Code, 2nd ed. Microsoft Press.

【21】http://grouper.ieee.org/groups/1667/ (2005-11-11)

【22】http://issaa.org (2005-11-11)

【23】http://siswg.org (2005-11-11)

【24】http://tech.sina.com.cn/i/2005-04-01/1103568515.shtml (2005-10-29)

【25】http://www.esign.org.tw
【26】http://www.liberttimes.com.tw/2001/new/sep/30/today-t2.htm (2001-9-30)
【27】http://www.nsa.gov/SE Linux (2004/7/29)
【28】http://www.trustedcomputinggroup.org (2005-10-09)
【29】http://www.telepolis.de/tp/english/special/enfo/6382/1.html (1999/8/3)
【30】http://www.wassenaar.org/docs/ (2004-8-25)
【31】ISO (1987), Banking - Approved algorisms for message authentication - Part 1: DEA, ISO 8731-1:1987(E), ISO, 1987.
【32】ISO (1987), Banking – Approved algorithms for message authentication - Part 2: Message authenticator algorithm, ISO 8731-2: 1987(E), ISO, 1987.
【33】ISO (1994), Banking-Key management (retail) (all parts), ISO 11568, ISO.
【34】ISO (1999), Information technology- Security techniques- Evaluation criteria for IT security (all parts), ISO/IEC 15408.
【35】ISO/IEC, (2004), Information technology - Security techniques – A framework for IT security assurance – Part 3: Analysis of assurance methods, ISO/IEC 4th WD 15443-3 (SC27 N4006), 2004-10-22.
【36】ISO/IEC 13491-2 (2005), Banking—Secure Cryptographic Devices (retail)—Part 2: Security Compliance Checklists for Devices Used in Financial Transactions.
【37】ISO/IEC JTC1/SC27 (2004), Information technology-Security techniques-Security assessment of operation system, ISO/IEC 19791, ISO/IEC JTC1/SC27 N4001.
【38】Johnson, D. B. et al. (1994), The Commercial Data Masking Facility (CDMF) Data Privacy Algorithm, IBM J. Res. Develop. Vol.38, No.2, pp.217~226.
【39】Katzke, S. (2003), Protecting Federal Information Systems and Networks, in Presentation of the 4th International Common Criteria Conference, Stockholm Sweden, 7~9, Sept. 2003.
【40】Koops, Bert-Jaap (1998) The Crypto Controversy, Kluwer Law International.
【41】Krimn, J.-P. (2005) A FIPS 140-2 evaluation could anthorize CC-like tests, in Presentation of the 6th International Common Criteria Conference, Sept. 28~29, Tokyo, Japan.
【42】Mann, S. and E.L. Mitchell (2000), Linux System Security, Prentice Hall.
【43】NIST (2005), Minimum Security Requirements for Federal Information and Information Systems (Initial Public Draft), FIPS PUB 200, NIST.
【44】NIST (1998), Requirements for Key Recovery Products, November 1988, NIST.
【45】NIST (2001), Security Requirements for Cryptographic Modules, NIST FIPS PUB (Publication) 140-2, NIST.
【46】NSA (National Security Agency) (1999), Controlled Access Protection Profile (CAPP), Version 1.d, October 8, 1999.
【47】NSA (National Security Agency) (2000), Key Recovery Agent System, V1.1, January 14, 2000, NSA.
【48】NSA (2000), Key Recovery End System, V2, January 14, 2000, NSA.
【49】NSA (2000), Key Recovery Third Party Requestor, V1.0, February 21, 2000, NSA.
【50】NSA (2000), Information Assurance Technical Framework, Version 3.0, September, 2002, NSA.
【51】NSA (1999), Labeled Security Protection Profile, Version 1.b, October 8, 1999.
【52】OECD (1998), Cryptography Policy, The Guidelines and the Issues, OECD.

【53】OECD (2002), Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security, OECD.
【54】Oppliger, R. and R. Rytz (2005) Does Trusted Computing Remedy Computer Security Problems? IEEE Security & Privacy, Vol. 3, No. 2, pp. 16~19.
【55】Park, J.S., G.-J, Ahn and R. Sandhu, Role-Based Access Control on the WEB using LDAP, Database and Application Security XV, eds by Oliver, M.S. and D.L. Spooner, Kluwer Academic Publishers, pp. 19~30, 2002.
【56】Ren, J. et al. (2005) Design and Implementation of TPM SUP320, in Security and Privacy in the Age of Ubiquitous Computing, pp. 143~154, eds by Sasaki, R. et al. Springer.
【57】Rhee, Man Young (1998) CDMA Celluar Mobile Communications and Network Security, Prentice-Hall.
【58】Ross, R. etal. (2004) Guide for the Security Certification and Accreditation of Federal Information Systems, NIST Special Publication 800-37, NIST.
【59】Sandhu, R.S., E.J. Coyne, H.L. Feinstein and C.E.Youman (1996), IEEE Computer, Vol.29, No.2, pp38~47.
【60】Schneier, B. (1996) Applied Cryptography, 2nd ed. Wiley.
【61】Science Applications International Corporation, Windows 2000 Security Target ST Version 2.0, October 18, 2002.
【62】Song, C.-H., Farn, K.-J. and Y.-S. Yeh (2000) A Scheme for Public-Key Based Key Recovery System with Limited Time Span, in Proceeding of IFIP/SEC 2000: Information Security for Global Information Infrastructures eds. by Sihan Qing and J. H. P. Eloff, pp.199~204, International Academic Press.
【63】Tanabe, T. (2005) challenge to the business value-up through objective evaluation for IT Security, & Japan's IT Security policy, in Presentation of the 6th International Common Criteria Conference, 28~29, Sept. 2005, Tokyo, Japan.
【64】Vedder, K., (1998), International Standardization of IT Security, in State of the Art in Applied Cryptography, eds. By Preneel, B. & V. Rijmen, Lecture Nates in Computer Science, No. 1528, pp. 353~366, Springer – Verlag.
【65】Wang Xiaoyun, Y. Lisa and H. Yu (2005-02-07) Collision Search Attacks on SHA-1 (http://theory. Csail.mit.edu/~yiqun/shanote.pdf).
【66】Williams, C. etal. (2000) Key Recovery Alliznce (KRA) Technology Papers, Special Issue, Computers & Security, Vol.19, No.1 pp.18~104.
【67】2002 年 9 月 2 日，自由時報 11 版，編譯陳宜君／綜合報導。
【68】2005 年 10 月 17 日，聯合報 A10，記者陳一雄、吳雯雯台北報導。
【69】中國信息安全產品測評認證中心（2003），信息安全標準與法律法規，人民郵電出版社。
【70】朱秋南（2000），ATA 硬碟之來龍去脈，微電腦傳真雜誌，第 19 卷，第 3 期，頁 267~278。
【71】行政院國家資通安全會報(2004)，建立我國通資訊基礎建設安全機制計畫(九十四年至九十七年)。
【72】行政院國家資通安全會報(2005)，政府機關(構)資訊安全責任等級分級作業施行計畫。
【73】李英明等（2001），中共發展「信息戰」及對我國建立資訊安全制度影響之研究，行政院研究發展考核委員會。

【74】胡志奎（1993），中華密碼學之南北開山－蔣宗標與溫毓慶，傳記文學，第63卷，第5期，頁87~93。
【75】范紅與馮登國(2003)，安全協議與方法，科學出版社。
【76】卿斯漢(2005)，可信計算，2005年8月20日，中國信息安全協會銀川會議。
【77】卿斯漢等，操作系統安全導論，科學出版社，台北，2003。
【78】陳奕明主編(2003)，Linux 系統安全分析，行政院國家科學委員會技術資料中心，台北。
【79】陳鵬仁譯（1994），中日世紀甲午戰爭，原名「蹇蹇錄」，日本伊藤博文內閣外相陸奧宗光口述回憶錄，開今文化事業有限公司。
【80】黑客防線（2004），總第37期（攻冊與防冊）～總第42期（攻冊與防冊）。
【81】經濟部(2000)，建立電子簽章法制，加速電子商務發展，經濟部。
【82】經濟部工業局（2003），瓦聖那協定傳統武器及軍商兩用貨品及技術輸出管制：軍商兩用貨品技術清單。
【83】經濟部國際貿易局（2000），戰略性高科技貨品輸出管理制度說明會（會議資料）。
【84】經濟部商業司(2006)，2005台灣PKI年鑑，經濟部商業司。
【85】葉義雄等(2005)，密碼與標準，財團法人國家實驗研究院科技政策研究與資訊中心。
【86】資策會電子商務研究所(2004)，主要國家電子化政策分析研究報告，經濟部技術處。
【87】鈺松國際資訊股份有限公司(2004)，網路服務效能式防火牆之開發(期末報告)。
【88】蔡冠婷(2001)，電子化的法制基礎－電子簽章法，資訊與電腦，257 期，頁3~5。
【89】劉燕芬譯（2000），碼書：編碼與解碼的戰爭，商務印書館。
【90】樊國楨（2001），中國國家信息安全測評認證中心簡介，資訊安全通訊，第七卷第三期，頁19~25。
【91】樊國楨（2000），美國最新密碼產品管制政策淺述，戰略性高科技貨品出口管理制度研究季刊，第5期，頁9~12。
【92】樊國楨、王美靜與林樹國(2005)，數位社會資訊安全與密碼政策初探技術報告，中華資訊安全管理協會。
【93】樊國楨、林樹國與陳彥學(2005)，密碼模組管理初探，第111期，頁68~79。
【94】樊國楨、林樹國與鄭東昇(2005)，美國聯邦資訊安全管理法案實作初探，電腦稽核，第13期，頁115~130。
【95】樊國楨、林樹國與盧公瑜(2006)，開放源碼機敏性檔案存取控制安全技術評估初探，檔案季刊，第五卷，第一期，頁115~147。
【96】樊國楨、林樹國與羅濟群(2004)，建立我國資安產品驗證與認證體系之研究，資訊安全通訊，第10卷，第1期，頁8~23。
【97】樊國楨等（2004），中華人民共和國資訊安全認證與驗證機制初探，中華資訊安全管理協會。
【98】樊國楨與趙承宗(1999)，能適當保護個人隱私的金鑰代管方法，CCL Technology Forum, 1999年7月1日，頁8~10。
【99】賴溪松、韓亮與張真誠（1995），近代密碼學及其應用，松崗電腦圖書資訊股份有限公司。
【100】謝寶煖(2002)，產業科技管制措施，90-EC-2A-17-0118-07，工業技術研究。