行政院及所屬各機關出國報告
(出國類別：其他)

赴美國參加 CMVP2002 會議報告

服務機關：中華電信研究所
出國人　職　　稱：助理研究員
姓　　名：鄭玉玲

出國地區：美國
出國期間：91**年**3**月** 25**日至**91**年**3**月**29**日**
報告日期：91**年** 5**月** 25**日**

赴美國參加 CMVP2002 會議報告

內容摘要

CMVP(Cryptographic Module Validation Program Conference) 密碼模組驗證程序會議，主要是對於密碼模組檢測新標準 FIPS 140-2 做介紹。會議中之主題除了對此標準之介紹，亦包括其與其前身 FIPS 140-1 間之差異、演算法的測試、資訊產品安全標準'共通規範'的議題等。為提昇中華電信產製之硬體密碼模組的公信力及市場競爭力，本組正積極進行產品送驗程序，參加此次會議對於新標準檢驗的流程及方法可進一步了解，對與爾後的產品送驗進行有很大的幫助。

本報告將首先說明本次出國行程概要以及密碼模組驗證程序會議概況，其次彙整本次會議之重點摘要，最後則提出參加本次會議之感想與建議。

赴美國參加 CMVP2002 會議報告

目錄 (Contents) **頁次(Page)**

1. 前言

CMVP(Cryptographic Module Validation Program Conference) 密碼模組驗證程序會議，主要是對於密碼模組檢測新標準 FIPS 140-2 做介紹。會議中之主題除了對此標準之介紹，亦包括其與其前身 FIPS 140-1 間之差異、演算法的測試、資訊產品安全標準'共通規範'的議題等。為提昇中華電信產製之硬體密碼模組的公信力及市場競爭力，本組正積極進行產品送驗程序，參加此次會議對於新標準檢驗的流程及方法可進一步了解，對與爾後的產品送驗進行有很大的幫助。

2. 行程概要

1.1 3月 24日：晚上 18:20 搭乘長榮班機，至紐華克國際機場。

1.2 3月 25日：7:00 搭乘大陸航空至華盛頓 DC。

1.3 3月 26日：CMVP2002 第一天。

1.4 3月 27日：CMVP2002 第二天。

1.5 3月 28日：下午 19:30 搭乘大陸航空班機至紐華克國際機場轉長榮班機 ， 於 3/30 下午 13:30 返抵桃園中正國際機場。

3. 會議議程

Tuesday, March 26

7:00-8:30am

Registration and Check-in - Ballroom Foyer

Continental Breakfast

8:30-10:00am

Welcome

Randall J. Easter, NIST

Dr. Susan F. Zevin,

Deputy Director of ITL, NIST

Keynote Speaker

Dave Simpson,

Communications-Electronics Security Group (CESG)

UK Government

Update of Standards

Ed Roback,

Computer Security Division Chief, NIST

10:00-10:30am

Coffee Break

10:30-11:30am

CMVP Status

FIPS 140-2 Tutorial

FIPS 140-1 and 140-2 Differences

Annabelle Lee, Director, CMVP, NIST

CMVP Team, NIST

11:30am-1:00pm

Luncheon Buffet / Exhibits

1:00-2:30pm

Testing to FIPS 140-2 Derived Test Requirements

Randall J. Easter, NIST

Algorithm Testing

Larry Bassham, NIST

2:30-3:00pm

Coffee Break

3:00-3:45pm

National Voluntary Laboratory Accreditation Program

Jeffery Horlick, NIST

3:45-4:30pm

CMT Laboratory Accreditation under the Standards Council of Canada

Jean Campbell, Director, CMVP, CSE

Questions and Answers

4:30pm-7:00pm

Exhibit Hall and Reception

Hors d'oeuvres, Beverages

Wednesday, March 27

7:30-9:00am

Continental Breakfast

9:00-10:30am

Agency Panel

Kim Mitchel, SSA]

Fred Stillwagen, NASA

Jean Campbell, Director, CMVP, CSE

10:30-11:00am

Coffee Break

11:00-11:30am

ANSI / ISO Update

Annabelle Lee, Director, CMVP, NIST

11:30am-12:00noon

CSE / ITS Product Pre-qualification Program

Ghislain Lagacé, CMVP Program Manager, CSE

12noon-1:30pm

Luncheon Buffet/Exhibits

1:30-2:30pm

Common Criteria and CMVP

Annabelle Lee, Director, CMVP, NIST

Dr. Ronald S. Ross, Director, NIAP, NIST

Pamela Grannum, CSE

2:30-3:00pm

Coffee Break

3:00-4:30pm

Laboratory Panel

Atlan Laboratories

Ed Morris, Lab Director

CEAL: A CygnaCom Solutions Laboratory

Miles Smid. Lab Director

COACT Inc. CAFE Laboratory

Bill Hebler, Lab Director

DOMUS IT Security Laboratory

Greg Scorsone, Program Manager

EWA - Canada LTD. IT Security Evaluation Facility

Erin Connor, Lab Manager

InfoGard Laboratories, Inc.

Tom Caddy, Lab Director

Questions and Answers

Closing Remarks

Kenneth Donaldson,

Head - Cryptographic Security Section, CSE

4. FIPS 140-2 介紹

美國商務部國家標準與技術研究院（ＮＩＳＴ）九十年六月二十八日於聯邦公報公告通過美聯邦密碼模組安全標準 FIPS 140-2（Federal Information Processing Standard ），該標準於九十年十一月二十五日生效，美聯邦政府機構將依照該標準保護其機密性資料之安全。

FIPS 140-2 為美ＮＩＳＴ所制定替代 FIPS 140-1 密碼模組之安全標準，目的在於規範售與美國政府部門之密碼模組產品所必須遵守的安全需求，同時建立一套產品認證的機制。此套認證機制的流程如圖 4-1, 密碼模組製造廠商將其產品送至檢測實驗室測試, 檢測實驗室負責測試此產品是否符合 FIPS 140-2 ，並撰寫報告送至 NIST/CSE , NIST/CSE 負責審核報告並發給證書，同時將其產品加入通過驗證的名單中公佈於網站上。

而檢測實驗室是由NVLAP(National Voluntary Laboratory Accreditation Program)依據NIST Handbook 150-17(Cryptographic Module Testing)、 ISO17025 、ISO9002、來鑑定資格。NVLAP 會每年定期檢查檢測實驗室，每兩年實地評估檢測實驗室。

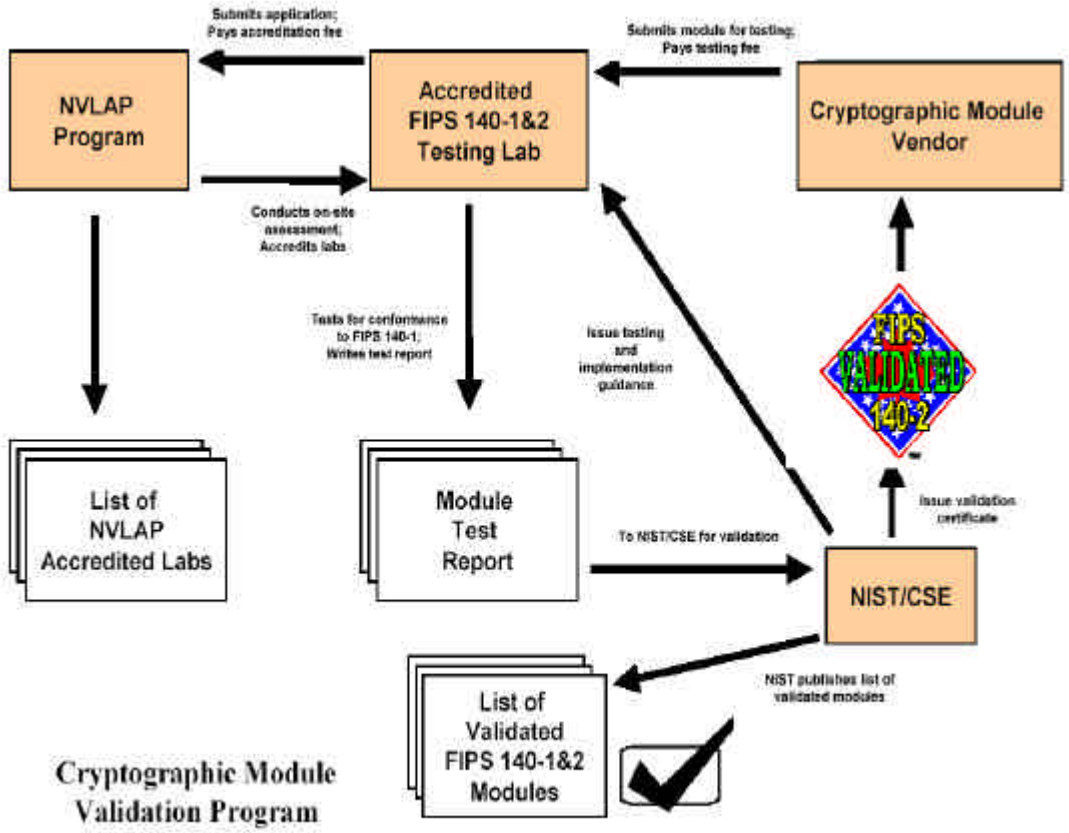

圖 4-1 FIPS 140-2 **檢測流程**

FIPS 140-2 **對於密碼模組安全等級需求分成四個等級, 等級越高安全性越強。如圖** 4-2 **所示**

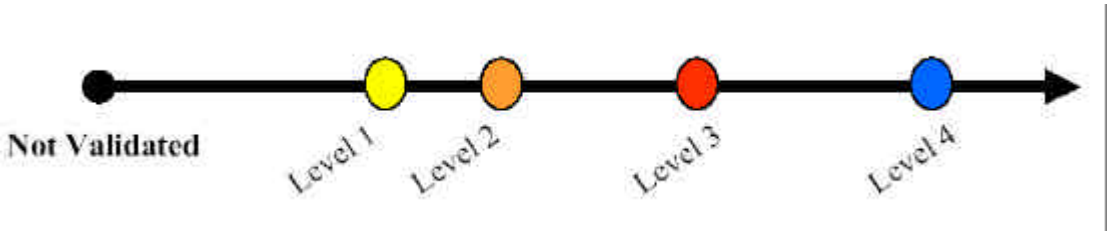

圖 4-2 **密碼模組安全等級**

- **安全等級一**(Level 1)**提供最低等級的安全，此為密碼模組的基本安全需求(至少使用一個認可的密碼演算法或安全功能)，無需實體防護。例如個人電腦即可視為安全等級一。**

- **安全等級二**(Level 2)**加強安全等級一的實體防護，須有侵入的證據。密碼模組的實體防護包括塗料密封或上鎖。當有非法入侵會有證據留下。另外安全等級二**(Level 2)**還須要以角色為身份鑑別的基礎**(role-based)**。安全等級二**(Level 2)**允許軟體或韌體在一般電腦上執行運算，但其操作系統必須在** Common Criteria (CC) EAL2 **以上。**
- **安全等級三**(Level 3) **密碼模組的實體防護除了安全等級二**(Level 2) **須有侵入的證據外，還須有篡改偵測與開蓋及開門反應** (response for covers and doors) **，以本體基**(identity_based)**操作者鑑別為基礎來加強安全等級二**(Level 2)**還須要以角色為身份鑑別的基礎**(role-based) **，以加密形式進/出金鑰或以分開知識程序** (split knowledge)**直接進/出。安全等級三**(Level 3)**允許軟體或韌體在一般電腦上執行運算，但其操作系統必須在** Common Criteria (CC) EAL3 **以上。**
- **安全等級四**(Level 4) **提供最高等級的安全，此安全等級密碼模組的實體防護為完全的保護。從任何方向侵入都會被偵測到，並會立刻將明文的金鑰和安全參數歸零，所以對於沒有安全保護的環境非常有用。另外若環境的溫度或電壓不在正常的操作範圍內，密碼模組也會被安全的保護。安全等級四**(Level 4)**允許軟體或韌**

體在一般電腦上執行運算，但其操作系統必須在 Common Criteria (CC) EAL4 **以上。**

FIPS 140-2 **對於密碼模組的安全需求項目共有** 11 **項**

1**、密碼模組規格（**Cryptographic Module Specification**）**

2**、密碼模組進出埠與存取介面（**Cryptographic Module Ports and Interfaces**）**

3**、角色、服務、與身分鑑別（**Roles, Services, and Authentication**）**

4**、有限模組狀態定義（**Finite State Model**）**

5**、實體安全（**Physical Security**）**

6**、操作環境（**Operational Environment**）**

7**、金鑰管理（**Cryptographic Key Management**）**

8**、電磁檢驗（**EMI/EMC**）**

9**、自我檢測功能（**Self-Tests**）**

10**、設計發展擔保（**Design Assurance**）**

11**、降低其他攻擊方式之設計概述（**Mitigation of Other Attacks**）**

表 4-1 ~ 4-2 **為各項目對各安全等級需求的摘要。**

表 4-1：**密碼模組安全等級需求** NIST FIPS 140-2 **驗證標準說明之一**

等級 領域	安全等級 1	安全等級 2	安全等級 3	安全等級 4
密碼模組規格	密碼模組與邊界規格。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)・			
密碼模組進出埠與存取介面	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阜(data ports)應該在邏輯上與其他資料阜分開。	
角色、服務、與身分鑑別	必須及備選角色與服務應在邏輯上分開。	角色為身份鑑別的基礎(role-based authentication)	本體基(identity_based)操作者鑑別。	
有限模組狀態定義	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。	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)。 實體安全失效保護/測試之環境
操作環境	可執行碼鑑別機制。單機、單使用者。	符合EAL2評估要求之PP。	符合EAL3評估要求之PP加可信賴的通訊路徑再加安全政策塑模。	符合EAL4評估要求之PP加安全政策塑模，隱密通道分析，與模組化。
金鑰管理	經通過之產生/分配技術。		以加密形式進/出金鑰或以分開知識程序(split knowledge)直接進/出。	
電磁檢驗	FCC Part 15,Subpart B, Class A(商業用)。可用之FCC需求(voice用)。		FCC Part 15,Subpart B,Class B(家庭用)。	

註：1. EAL：**信保評核等級**(Evaluation Assurance Level)。
2. PP：**保護外觀**(Protection Profile)。

表 4-2: 密碼模組安全等級需求 NIST FIPS 140-2 驗證標準說明之二

等級 領域	安全等級 1	安全等級 2	安全等級 3	安全等級 4
自我檢測功能	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。
設計發展擔保	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。功能測試。	高階語言建置。測試涵蓋性分析。	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。
降低其他攻擊方式之設計概述	提供降低其他攻擊之測試需求規範			

註：1. RNG：亂數生成器(Random Number Generator)。
2. PRNG：擬亂數生成器(Pseudo Random Number Generator)。

5. 會議內容摘要

在此次會議中介紹與 FIPS 140-2 相關的標準，對稱金鑰演算法有 DES (FIPS 46-3,FIPS 81)，3DES (FIPS 46-3 ,FIPS 81,X9.52)，AES (FIPS 197) ，HMAC (FIPS 198) ，非對稱金鑰演算法有數位簽章 DSA (FIPS 186-2, X9.30) ，RSA(FIPS 186-2, X9.31) ，ECDSA (FIPS 186-2, X9.62) ，金鑰建立設計 Diffie-Hellman (X9.42) ，RSA (X9.44) ，

Elliptic curve (X9.63)，安全的雜？函數 SHA-1 (FIPS 180-1) ，如圖 5-1 所示，圖中紅色部分表示標準還在擬定中。

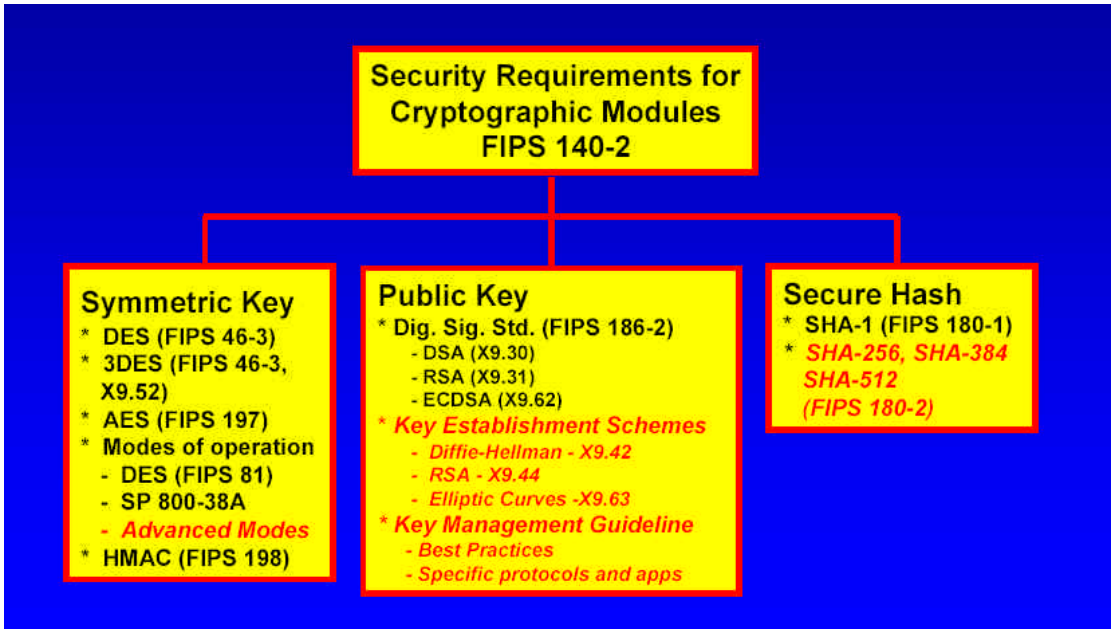

圖 5-1 FIPS 140-2 相關標準

而密碼演算法強度的金鑰長度比較如圖 5-2 ，黑底部分表示已經不安全，白底部分表示為 FIPS 認可，黃底部分表示目前為草案或推薦長度。NIST 密碼標準的狀況如 圖 5-3，同樣地，黑底部分表示已經不安全，白底部分表示為 FIPS 認可，黃底部分表示目前為草案，紅底部分表示目前還在草案擬定中，灰底部分表示開始推薦公佈中。在此次會議中還談到 FIPS 140-1 與 FIPS 140-2 的差異，表 5-1 就是將其各項目比較的摘要。

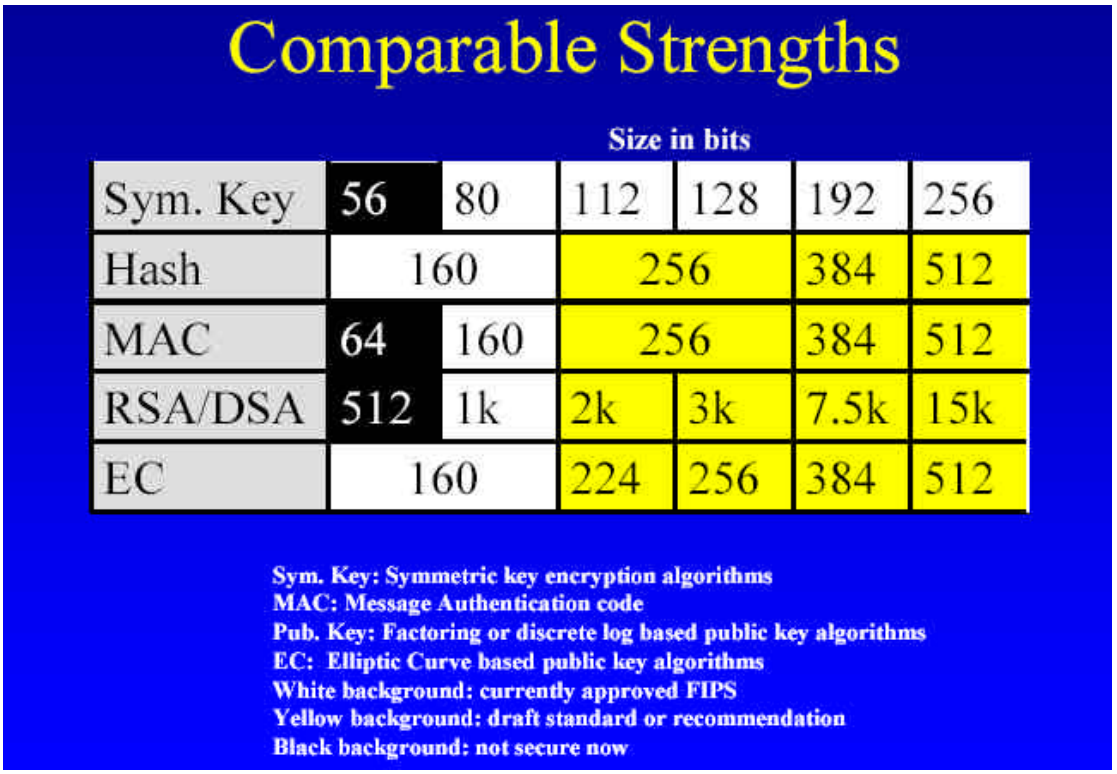

圖 5-2 FIPS 140-2 **相關標準**

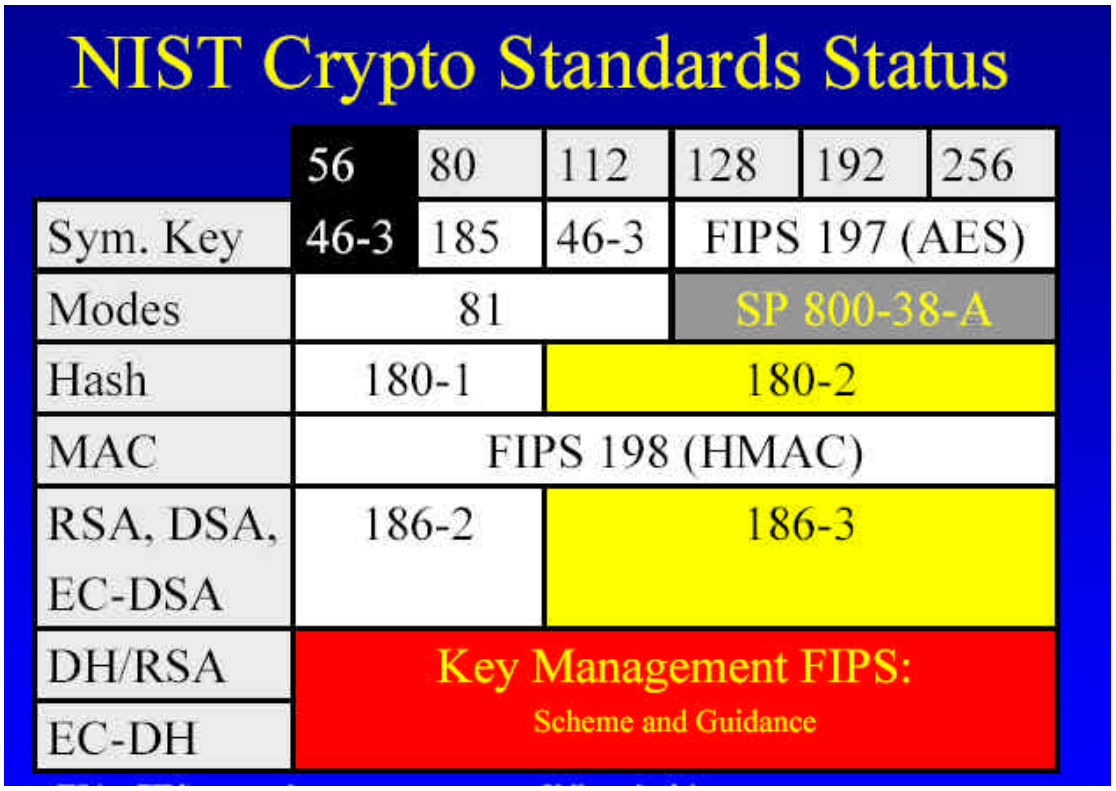

圖 5-3 **密碼標準的狀況**

表 5-1 FIPS 140-1 **與** FIPS 140-2 **比較**

Tables of Content	
FIPS 140-1	*FIPS 140-2*
1. Overview	1. Overview
2. Glossary of Terms and Acronyms	2. Glossary of Terms and Acronyms*
3. Functional Security Requirements	3. Functional Security Requirements
4. Security Requirements	4. Security Requirements
4.1 Cryptographic Modules	4.1 Cryptographic Module Specification*
4.2 Cryptographic Module Interfaces	4.2 Cryptographic Module Ports and Interfaces
4.3 Roles and Services	4.3 Roles, Services, and Authentication*
4.4 Finite State Machine Model	4.4 Finite State Model
4.5 Physical Security	4.5 Physical Security*
4.6 Software Security	4.6 Operational Environment*
4.7 Operating System Security	4.7 Cryptographic Key Management
4.8 Cryptographic Key Management	4.8 EMI/EMC
4.9 Cryptographic Algorithms	4.9 Self-Tests*
4.10 EMI/EMC	4.10 Design Assurance*
4.11 Self-Tests	4.11 Mitigation of Other Attacks*
Appendixes	*Appendixes*
A: Summary of Documentation Requirements	A: Summary of Documentation Requirements
B: Recommended Software Development Practices	B: Recommended Software Development Practices*
C: Selected References	C: Cryptographic Module Security Policy*
	D: Selected Bibliography*

* Section added or significantly revised.

以下就其改變部分說明

1. **密碼模組規格**:

主要修改 : 包含了認可的演算法及安全函數

2. **密碼模組進出埠與存取介面**

主要修改 : 輸出入明文金鑰要由實體分開埠或是邏輯分開但可信賴的路徑。

3. **角色、服務、與身分鑑別**

主要修改 : 增加了身分鑑別機制的強度

4. **有限模組狀態定義**

主要修改: **參考有限模組狀態定義對硬體、軟體和韌體有較好的表現方式。**

5. **實體安全**

主要修改: **重新組織部分章節使其更清楚更一致。**

6. **操作環境**

主要修改: **將** TCSEC **的需求改為**CC **的需求。**

7. **金鑰管理**

主要修改: **增加無線電**Over-The-Air-Rekeying (OTAR) ,**及增加金鑰建立機制的強度。**

8. **電磁檢驗**(EMI/EMC)

主要修改: **反映** FCC **需求的修改**

9. **自我檢測功能**

主要修改: **增加亂數產生器統計特性測試的強度，對於旁路模式有較好的說明。**

10. **設計發展擔保**

主要修改 : **對於設計發展擔保採組態管理，安全配送，並有導引文件。**

11. **降低其他攻擊方式之設計概述**

新章節 ：**對於新型態的密碼模組攻擊提供資訊及建議**

12. **附錄**

A、 Summary of Documentation Requirements : **更新**

B、 Recommended Software Development Practices: **更新**

C、 Security Policy: **對於安全政策內容及架構的授權管理修改**

D、 Selected Bibliography: **更新**

Annex A: Approved Security Functions

Annex B: Approved Protection Profiles

Annex C: Approved Random Number

Annex D: Approved Key Establishment

6. 檢討與建議

密碼模組僅是資訊社會安全重要環節之一，電子化政府中之識別證卡事實上，台閩地區金融卡使用之自動提款設備中之密碼模組，幾均未具備 FIPS 140-1 **之證明，如何積極推動並訂定國內資訊安全(含密碼**

模組)的相關安全需求標準與認證體系等，實是當務之急，更是電子化/網路化政府資訊安全稽核子計畫應正視的問題。

在高度資訊化的社會中，由於企業或政府體系在現今網際網路的作業環境下，往往對資訊系統的安全性有很大的隱憂及顧慮，而無法將組織體系的運作完全依靠於資訊系統，藉以提昇組織的競爭力和效率，尤其對於目前正蓬勃發展的電子商務交易環境更是一大阻礙。追根究底可知資訊系統的安全因素顧慮為其原因之一，雖然系統開發廠商皆聲稱其資訊系統安全性很高，但對於資訊系統的安全性很難有一個客觀的標準，形成各說各話情況而讓系統使用者無所依據及參考。

因應現今市場對網路安全之需求，本公司有提供 PKI 服務(公開金鑰基礎建設)在網路的環境中做身分認證及其他相關業務，然而此種服務之品質及公信力，必須由系統元件(如密碼模組軟硬體)之安全及可信度開始建立，因而系統中元件的安全檢驗極為重要。

為了要有效率的對生產者所提供的各式密碼模組產品做合理的評估，以判斷這些產品所宣稱的安全功能是否真正提供使用者適當及所需的保障，就需要有審驗的標準以做評定。而由於考量資訊產品市場的全球化，此種安全評定也漸趨朝向一個全球一致的標準。美國的 FIPS140-2 標準正是對密碼模組安全性做此種評定的一種標準。此標

準也同時為加拿大政府所接受，NIST 與加拿大的 CSE 並於 1995 年簽署協議，共同承認由經過 NIST 或 CSE 核可之檢測實驗室所檢測之結果。由於美加安全科技在世界上具領導地位，且其檢測架構及流程定義嚴密，故經其檢測認證之結果在國際上極具公信力。

FIPS140-2 標準中的安全等級共分四級，此標準是根據早先已使用數十年的美國國家標準 FIPS140-1 做更進一步的修訂與添加而成。NIST 已於今年（2002 年）五月 25 日停止受理 FIPS 140-1 之審驗業務。

近年來由於本國積極推動電子化政府，通資訊基礎建設之安全機制受到廣泛的重視。許多政府相關之標案皆要求承標廠商之產品需符合一定的安全標準。若是本所所研發之硬體保密器通過 FIPS140-2 之審驗及認證，不但可以提升使用者對此產品的信心、增加企業網路本身的安全度、同時更可以增加中華電信在網路安全上的公信力。