出國報告（出國類別：會議）

參加2008年第9屆
國際共同準則研討會（ICCC）報告

服務機關：國家通訊傳播委員會
姓名職稱：謝進男　委　　員
　　羅金賢　副 處 長
派赴國家：韓國
出國期間：97年9月23日至9月25日
報告日期：97年11月15日

目　　錄

壹、目的

本次出國參加第 9 屆 ICCC (International Common Criteria Conference) 國際共同準則研討會議之主要目的，在於了解各國評估及驗證體系運作、各種資安產品評估及驗證經驗、共同準則面臨問題及建議、未來共同準則發展及趨勢、共同準則內容及其應用創新等議題。

參與本次國際研討會可獲得最新國際資通安全檢測技術資訊、各國資通安全產品檢測及驗證推動現況、共同準則最新版本之制訂內容與進度等相關訊息。有助於本會掌握最新資通安全相關國際技術，俾作為未來修訂相關技術規範參考；亦可了解他國在資通安全產品驗證體系的優缺點，檢測實驗室及驗證機構之專業能力，投入評估驗證之經驗，可作為本會未來強化我國資通安全驗證體系、提升資通安全驗證專業能力及完備評估及驗證作業程序之參考依據。

本次研討會由本會謝委員進男、技術管理處羅副處長金賢、財團法人電信技術中心(TTC)許組長碧姍及林經理家弘共計 4 人參加。TTC 並就目前國際間已普遍使用之電子護照(e-passport)向大會提出該產品檢測的潛在風險研究及建議方案論文，業經大會錄取，並受邀於本屆 ICCC 會議中進行簡報。本會及 TTC 亦利用本研討會期間，與國外驗證主管機關洽談 MRA 合作事宜，並尋求與國外檢測機構洽談產品檢測合作事宜。

貳、研討會簡介

國際共同準則研討會（International Common Criteria Conference，簡稱 ICCC），由共同準則相互承認組織 (Common Criteria Recognition Arrangement，簡稱CCRA)的會員國每年輪流主辦一次。該組織目前共有 24 個會員國，已申請成為「接受證書會員國」（Certificate-Consuming Participants，簡稱CCP），計有芬蘭、希臘、以色列、義大利、印度、丹麥、土耳其、瑞典、匈牙利、新加坡、奧地利、捷克等 12 個國家；已申請成為「核發證書會員國」(Certificate-Authorizing Participants，簡稱CAP），計有美國、加拿大、日本、韓國、澳洲、紐西蘭、德國、英國、法國、荷蘭、西班牙、挪威等 12 個國家。「接受證書會員國」指需接受「核發證書會員國」已驗證的資通產品，不必再經其國內驗證機關核證，即可在其國內市場上行銷。「核發證書會員國」指該國具有驗證資安產品能力，並可核發驗證證書，憑此證書可將產品行銷至其他 23 個會員國，不必再向其輸出國重新申請產品驗證。

本研討會所發表專題演講共計 69 篇，主要內容包括各國驗證機關體系介紹、各種資安產品的評估驗證經驗及問題探討、共同準則問題建議及發展、共同準則內容應用之新創見等。

3、 研討會時間、地點及議程

本屆研討會於韓國濟州島舉行，自 97 年 9 月 23 日至 9 月 25 日共計 3 天，大會議程說明如下：

(一)第一天 (09/23/2008)

Time	Track A	Track B	Track C
09:30-09:50	Opening Plenary IT Security Certification Center National Intelligence Service		
09:50-10:50	Keynote Speech Cross-Border Collaboration in Security & Privacy(Prof. Tai-Myoung Chung, Vice Chair of OECD WPISP, SungKyunKwan University, KR) Security Evaluation of A Moving Target(Prof. Dieter Gollmann, Head of Institute, Technischen Universität Hamburg-Harburg, DE) Enhance Smart Card Business through Common Criteria(Dr. Chilhee Chung, Senior Vice President, Samsung Electronics, KR)		
10:50-11:10	Report from the CC Management Committee Mats Ohlin, MC Chair (FMV, SE)		
11:10-11:30	Coffee Break		
11:30-12:30	Panel Session Common Criteria – Its Value and Future Moderator Mats Ohlin, MC Chair (FMV, SE)		

	Panelists Ms. Audrey Dale, Director of US Scheme (NSA, US) Mr. David Martin, CCDB Chair (CESG, UK) Ms. Irmela Ruhrmann, ES Chair (BSI, DE) Mr. Miguel Banon, CCMB Chair (representing CCN, SP) Mr. Pascal Chour, Head of French Scheme (DCSSI, FR) Mr. Richard Helliwell, Manager of Australian Scheme (DSD, AU)		
12:30-14:00	Luncheon		
14:00-15:30	CCDB report and overview of CC Version 4 work areas David Martin (CCDB Chair)	A new Protection Profile for NFC mobile security C. Loiseaux, R. Presty, JP. Wary, N. Helle, M.Eznack (Trusted Labs, FR)	Practical reading of the CC, success stories in the evaluation of complex products Miguel Banon, Jose Emilio Rico (Epoche, SP)
	CCDB Workgroup - Skills and Interaction David Martin (CCDB Chair)	Enterprise Management Solutions Protection Profiles Eric Winterton (Booz Allen Hamilton, US), Joshua Brickman (CA Inc., US)	Realising benefit and value from CC evaluations Ken Hendrie (Stratsec lab, AU)
	CCDB Workgroup - What Tools do evaluators need? David Martin (CCDB Chair)		
	The assurance	Protection Profile	Setting

	paradigm for lower assurance levels – should there be a greater level of testing? David Martin (CCDB Chair)	for e-voting systems Kwangwoo Lee, Yunho Lee, Woongryul Jeon, Dongho Won, Seungjoo Kim (Sungkyunkwan University, KR)	Expectations for Common Criteria in the Software Development Lifecycle Ray Potter (Apex Assurance Group, US)
15:30-16:00	Coffee Break		
16:00-18:00	Update on Japanese Scheme Yasuhide YAMADA (IPA, JP)	The Next Big Thing: Preparing a Legacy Infrastructure for a Paradigm Shift Jane Medefesser, Vanessa Kong (Sun Microsystems, US), Marilyn Harris (CGI, US)	CCRA – fragmentation or cohesion? Shaun Lee, Petra Manche (Oracle Corporation, UK)
	Update on Spanish Scheme Luis Jimenez (CCN, SP)	Common Criteria Testing in a Common Security Environment – RACF Diana Robinson, William Penny (IBM Corporation, US)	CC and CMMI – An approach to integrate CC with development Wolfgang Peter, Werner Achtert (TUViT, DE)
	Update on Italian Scheme Massimiliano Orazi(OCSI, IT)	Experience with CC 3.1, Class ALC (Life Cycle Support) evaluation Peter van Swieten (Brightsight, NL)	Effective Certification Roadmap Planning for Common Criteria and FIPS – Certification Portfolio

			Approaches Su-Chen Lin, Seyed Safakish (Juniper Networks, US)
	Update on Singporian Scheme Yim Leng WOO (IDA, SG)	Time Flies: Examining Timeliness in ALC_FLR.3 Duncan Harris, Adam O'Brien (Oracle Corporation, UK)	Managing Multiple and Emerging Standards William Penny (IBM Corporation, US)
	Update on Malaysian Schem Norhazimah Abdul Malek, Wan Roshaimi Wan Abdullah (CyberSecurity, MY)		
	Update on Turkish Scheme Merve Hatice KARATAŞ (TSE, TR)		
	CC in China Liu Zhuohui (CNCA, CH)		

(二)第二天 (09/24/2008)

Time	Track A	Track B	Track C
09:00-10:30	CCDB Workgroup – Evidence-based Approach Steve LaFountain (NIAP, US)	AVA_VAN.2 – Performing Vulnerability Analysis under CC v3.1 Eve Pierre, James L. Arnold Jr. (SAIC, US)	Scoping the TOE Nithya Rachamadugu (CygnaCom, US)
	CCDB Workgroup – Predictive Assurance Irmela Ruhrmann (BSI, DE)	Circular Reasoning: Venn Will We Agree on a Common SoF Analysis Method? Nathan Lee, Amy Nicewick (Corsec Security, US)	Developer Documentation – A Who to Guide Erin Connor (EWA, CA)
	CCDB Working Group – Writing a More Meaningful Certification/Validation Report Robert Harland (CSE, CA)	Attack Potential: Using it Properly and Evolving it for the Future Tony Boswell (SiVenture, UK)	An analysis of the coverage of some cryptographic aspects in the Common Criteria Massimiliano Orazi, Vittorio Bagini, Renato Menicocci, Franco Guida (Fondazione Ugo Bordoni, IT)
10:30-11:00	Coffee Break		
11:00-12:30	Challenging the concept of one Evaluation Assurance Level per evaluation Miriam Serowy (BSI, DE), Nils Tekampe (TÜViT, DE)	About the World-first CC smart card Certificate using Formal Assurances Boutheina Chetali (Gemalto, FR)	Should and How CC be used to Evaluate RFID based Passports or Banknotes? Chia Hung Lin (Telecom Technology

			Center, TW)
	EAL1: resuscitate or euthanize? The low assurance problem Julian Straw (BT, UK)	Smartcard security development using formal method tool SPIN Naohisa ICHIHARA (NTTDATA, JP)	Security Domain Separation as a Prerequisite for Business Flexibility Igor Furgel (T-Systems, DE)
	Proposal for a COTS Software Assurance Package Wesley H. Higaki (Symantec Corporation, US)	Towards Modelling and Evaluating SPM for XML Access Control Il-gon Kim, Hee-Jun Yoo, Won-Tae Sim, Byung-kyu Noh (KISA, KR)	Integration of Architectural Requirements into the CC Structure Helmut Kurth (atsec, US), Susanne Pingel (BSI, DE)
12:30-14:00	Luncheon		
14:00-15:30	CC V4 – Proposed Approaches Anthony J. Apted, James L. Arnold Jr. (SAIC, US)	Consistency Verification Method Between TSFI and SPM on High Level Evaluation Hee-Jun Yoo, Il-Gon Kim, Gyu-Min Cho, Byung-Gue Noh (KISA, KR)	IT security starts here: At the building structure and its mission critical infrastructure Joachim Faulhaber, Wolfgang Peter (TÜViT, DE)
	Common Criteria from a Commercial Perspective – and options for improvement with version 4.0 Simon Milford (SiVenture, UK)	Designing the Trusted Service Bus for EAL5 David Ochel (atsec, US), Brian Vetter (BlueSpace Software, US)	Secure System Integration Methodology Satoshi HARUYAMA, Toshiya YOSHIMURA, Naohisa ICHIHARA

			(NTTDATA, JP)
	Multi-Level Certifications – Using lower EALs as project milestones Bertolt KrÜger (SRC Security Research & Consulting, DE), Christian Tabias (Utimaco Safeware AG, DE)	High Assurance Evaluations – Challenges in Formal Security Policy Modeling and Covert Channel Analysis Sai Pulugurtha (CygnaCom, US)	Measuring the effectiveness of a security development process Michael Grimm (Microsoft, US), Helmut Kurth (atsec, US)
15:30-16:00	Coffee Break		
16:00-18:00	Introducing Usability to the Common Criteria Matthew Nicolas Kreeger, Marcus Streets (nCipher, UK)	High Assurance Product Development and the Common Criteria: Rethinking EAL7 Rance DeLong, John Rushby (LynuxWorks, US)	Site Certification – another step to improve the CC process and to reduce costs Hans-Gerd Albersten (NXP Semiconductors, DE), Juergen Noller (Infineon Technologies AG, DE)
	Introducing Assurance Measures for Security Target Yi Mao (atsec, US)	Biometrics in Common Criteria 2008: The big picture Nils Tekampe (TÜViT, DE)	Site evaluation according to the Site Certification Process Thomas Schroder (T-Systems, DE)
	Common Criteria and Source Code Analysis	New Challenges on Biometric	The Centrality of Common

	Tools: Competitors or Complements Adam O' Brien (Security Assurance Group, UK)	Vulnerability Analysis on Fingerprint Devices Marino Tapiador (CCN, SP)	Criteria in a World of Advanced Technologies Lior Carmi (SII, IL)
	Software design complexity assurance using automated tools Tim Huntley (Juniper Networks, US)	Evaluation Methodology Based on CEM for Testing Environmental Influence in Biometric Devices Belen Fernandez-Saavedra, Raul Sanchez-Reillo, Raul Alonso-Moreno (University Carlos III of Madrid, SP)	Maximising the Benefits of Assurance Continuity David MacFarlane (Research In Motion, CA)

(三)第三天(09/25/2008)

Time	Track A	Track B	Track C
09:00-11:00	FMEA for Improving Vulnerability Prevention Byeonggak Ko (KTL, KR)	Common Criteria works! (How the smartcard industry uses the CC) Tyrone Stodart (ISCI, UK)	Guidelines for Evaluation Reports according to CC 3.1 Christian Krause (BSI, DE)
	Tool for Supporting a Common Criteria Evaluation Maria Soraya (CESTI, SP)	Experience of smart card evaluation under Japanese scheme Masashi Tanaka, Kazuo Morimura, Yasuhiro Hosoda, Takahiro Yamamoto (NTT, JP)	How to write Protection Profiles and Security Targets - ISO/IEC TR 15446, The PP/ST Guide Michael Nash (Gamma Secure Systems Ltd, UK)
	Tools and Techniques for Evidence Production Supporting tools for CC evaluation Ismael Kane (LGAI-APPLUS, SP)	The complete(d) CC v3.1 experience on a smart card IC with cryptolibrary Wouter Slegers (Brightsight, NL)	Lessons learnt in writing PP/ST Wolfgang Killmann (T-Systems, DE)
	EPM (Enterprise Project Management) construction for evaluating progress management Nam-kyun Baik, Won-Tae Sim, Byung-kyu Noh (KISA, KR)	The Functional Verification of AES RTL Design Using H/W Assisted Co-Emulation Jae-Deok Ji, Byung-Kwon Lee, Byung-kyu Noh (KISA, KR)	Further streamlining of PPs and STs Dirk-Jan Out (Brightsight, NL)
11:00-11:30	Coffee Break		

11:30-12:00	Closing Remark Mats Ohlin, MC Chair
12:00-12:10	Closing Address IT Security Certification Center
12:10-12:30	Announcement of 10th ICCC
12:30-14:00	Luncheon

肆、研討會過程摘述

1、驗證體系部分

(一)中國大陸驗證體系現況：

1.中國大陸自 1997 年開始翻譯共同準則 CC 1.0 英文版，當 1999 年 11 月發布 ISO/IEC 15408 後，中國大陸亦開始翻譯共同準則 CC 2.1 英文版。

2.中國大陸官方於 2001 年發布 GB/T 18336(CC2.1)(Information technology - Security techniques - Evalution criteria for IT security: Part 1-3)，等同 ISO/IEC 15408:1999(CC 2.1)標準。

3.中國大陸代表除第 5 次 ICCC 研討會，因簽證問題未派員參加外，均參加歷年 ICCC 的研討會。中國大陸資訊安全驗證機關亦曾派代表拜訪歐盟資訊安全驗證機關，如 Atsec、Tuvit、DCSSI、Syntegra 等。中國大陸也從其他國家的驗證機構邀請專家進行專業的技術訓練。

4.2008 年 7 月以前，由 CNITSEC 依共同準則(CC)標準，負責辦理自願性的資安產品驗證業務。目前則由中國大陸信息安全認證中心(China Information Security Certification Center, ISCCC)負責辦理自願性及強制性的資安產品驗證業務。

5.中國大陸指派 ISCCC 負責強制性資安產品驗證工作。ISCCC 為公正及獨立第三方的驗證機關，ISCCC 執行驗證活動，並依國際、國內標準及相關審驗規定提供驗證服務。其他驗證活動包括資訊安全管理系統(ISMS)及資訊安全(IS)服務等。ISCCC 並負責制訂及公布國家資安產品驗證及認證系統法規：No.[2004]57。

6.國家認證認可監督管理委員會(CNCA)負責國家資安產品驗證及認證系統之管理、監督及協調。由 8 個政府機關部門共同參與，包括中共國務院公安部(Ministry of Public Security, MPS)、中共國務院國安部

(Ministry of State Security, MSS)、國務院信息化辦公室(State Council Informatization Office)、信息產業部(Ministry of Information Industry)、狀態密碼管理局(State Cryptography Administration)、國家機密保護全國管理(National Administration for the Protection of State Secrets)、AQSIQ、CNCA。

7.國家資訊安全產品驗證管理及執行委員會(National Information Security Products Certification Administration and the Executive Committees)由政府相關部門、製造商、使用者、研發商及標準開發者所共同組成，負責制訂下列相關法規：

（1） 發布Protection Profile(PP)安全規範標準如下：

GB/T 18019-1999 (for packet filter firewall)、

GB/T 18020-1999 (for application level firewall)、

GB/T 20276-2006 (for smartcard embedded software)、

GB/Z 20283-2006 (Guide for the Protection of Protection Profile and Security Targets)

（2） 完成ISO/IEC 18405:2005(Methodology for It security evaluation, CEM)中文化翻譯工作，成為國家標準GB/T 18336。

8.資安產品之驗證

（1） 2001年發布GB/T 18336後，共有56件資安產品依CC標準完成驗證。自2002年中國資安產品有8 %係經過CC驗證。56件資安產品驗證等級說明如下：

EAVL1:2件、EAL2: 7件、EAL3: 22件(主要為防火牆及IDS)

EAL4 :25件(主要為行動通信之智慧卡，如SIM卡、UIM卡、相關嵌入軟體(COS))。

（2） 資安產品之技術規範及測試評估方法標準包括：

a.GB/T 20275-2006(Intrusion Detection System技術規範及測試評估方法)。

b.GB/T 20278-2006(Network Vulnerability Scanners技術規範)。

c.GB/T 20280-2006(Network Vulnerability Scanners測試評估方法)。

d.GB/T 20945-2007(Information System Security Audit Products技術規範及測試評估方法)。

e.GB/T 20281-2006(Firewall Products技術規範及測試評估方法)。

9.共同準則之保證需求(Assurance requirements)是相當抽象的，不容易閱讀，許多中國廠商認為很難了解這些保證需求。一位評估人員需要2到3年才能了解CC及實際利用它；當新的技術出現，可能沒有適合的PP，也沒有查核表，所以很難執行技術分析和決定安全功能強度，也很難保證從不同的實驗室能得到一致的評估結果。實施共同準則的經驗如下：

(1)評估人員需要更多的訓練。

(2)需翻譯更多的保護剖繪(PP)。

(3)對新的安全標的(TOE)，需發展更多的PP。

(4)將考慮加入CCRA。

(二)西班牙驗證體系現況：

1.國家密碼中心(National Cryptologic Centre, CCN)職掌

(1)協調行政單位使用及管理密碼產品及裝置。

(2)保證公務行政部門的資訊技術安全。

(3)協調密碼裝置的採購。

(4)訓練行政幕僚熟悉此專業的領域。

(5)資訊技術安全驗證及認可密碼產品及裝置。

2.CCN 法規架構

(1)ACT 11-2002 年 5 月 6 日：管制單位為國家情報中心(National Intelligence Centre, CNI)包括 CCN。

(2)Royal Decree 421-2004 年 3 月 12 日：規範及定義 CCN 範圍及功能。

(3)Order PRE/2740-2007 年 9 月 19 日：定義國家 IT 安全評估及驗證體系辦法。

3.CCN 評估及驗證活動

(1)密碼驗證

(2)TEMPEST 驗證

(3)功能驗證 ISO 15408 (CC)

(4)ITSEC

(5)其他 IT 安全驗證

4.CCN 推動 CC 歷程

(1)西班牙於 2000 年由公共事務管理部(Ministry of Public Administration)簽署參加 CCRA。

(2)西班牙國防部 2000 年基於 ITSEC 及 ITSEM 建立評估驗證體系。

(3)2002 年 5 月 6 日 ACT 11 規範 CNI 設置 CCN。

(4)2004 年 3 月 12 日公佈 Royal Decree 421-規範及定義 CCN 範圍及功能，作為國家資訊技術安全評估及驗證之驗證機關。

(5)2004 年 7 月 CCN 開始運作成為 CC 之驗證機關(CB)。

(6)2006 年 9 月 CCN 任命參與 CCRA。

(7)2007 年 9 月 19 日公佈 Order PRE/2740-定義國家 IT 安全評估及驗證體系辦法。

5. 2007 年及 2008 年有兩家民間檢測實驗室成立:APPLUS 及 EPOCHE

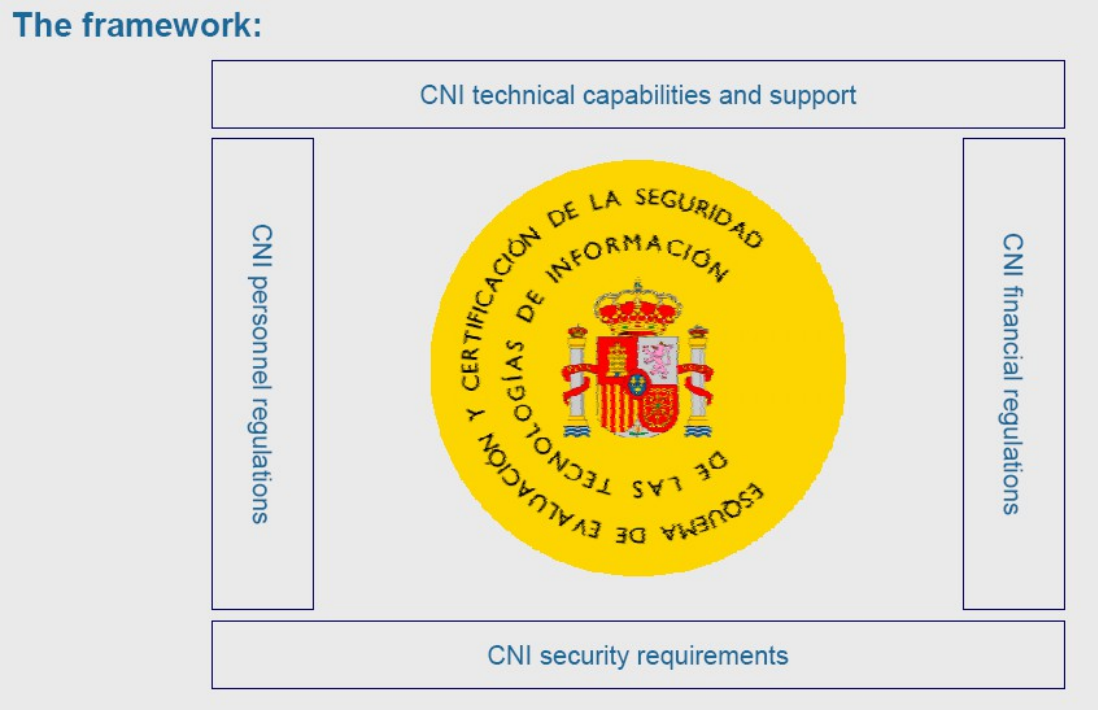


圖 1：西班牙國家情報中心(CNI)架構圖

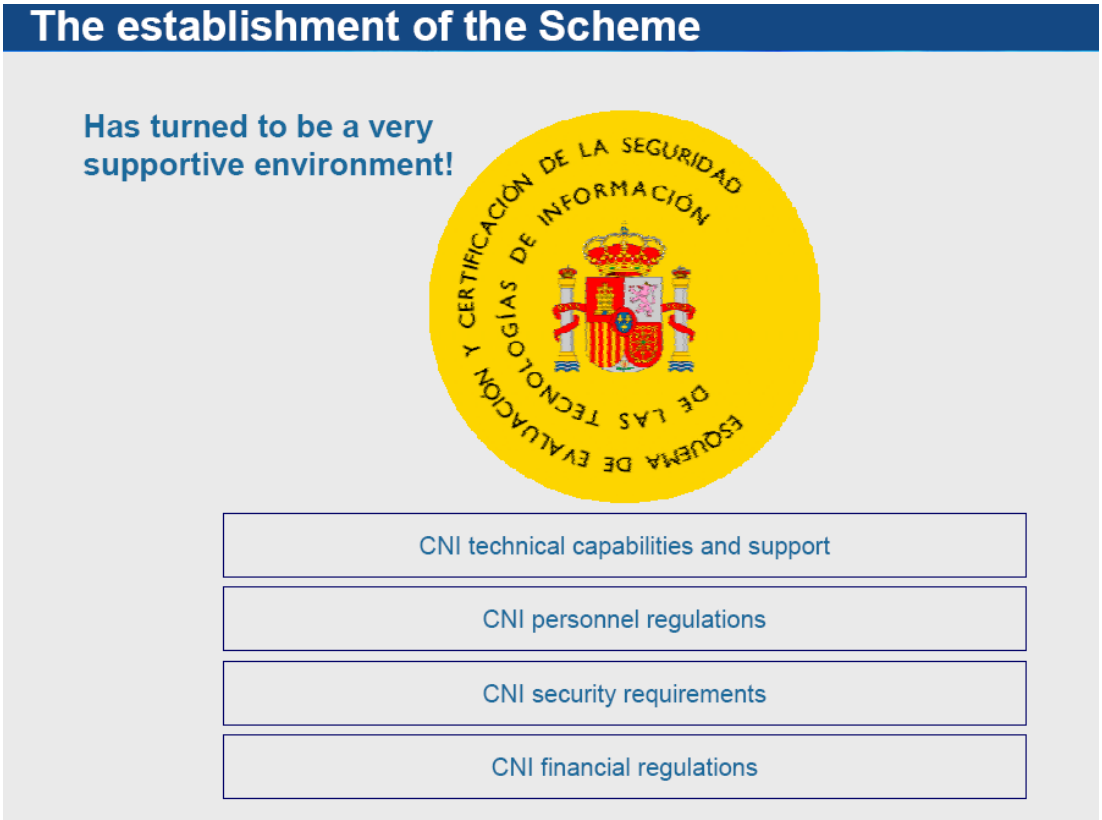


圖 2：國家情報中心(CNI)體系建立

6.體系驗證件數統計(2005-2008)

(1)已發證案件：10 件 CC 驗證(EAL2-EAL4+TOEs)、4 件 ITSEC 驗證(系統)。

(2)評估中案件：25 件主要為 CC 也有 ITSEC。

(3)保護剖繪(PP)案件：4 件進行中，等級為 EAL 1 －EAL3。

7.趨勢及願景

(1)西班牙正在急起直追數位簽章領域的安全驗證，並有初步成果，特別有關電子身分辨識，將增加產品受驗的應用程式 CCN 亦正在採取措施，以改善檢測實驗室的效率，並規劃強化其本身的能力，以因應未來所增加的業務需求。

(2)西班牙將要求 IT 產品須驗證安全，如相關國際電子 ID 卡的數位簽章，未來驗證申請的需求將增加；另適用於西班牙行政部門新的保護剖繪(PP)亦在持續發展中；在國家安全體系下， E 政府新的法規將被規範，包括明確的 IT 安全驗證需求；CCN 觀察到未來 CC 評估將有連續線性的成長，CCN 為妥善處理，將對檢測實驗室亦提出改善效率計畫。

(三)日本驗證體系現況：

1. 日本資訊安全產品檢測與驗證體系(JISEC)概要

(1)日本資訊安全產品檢測與驗證體系（Japan Information Security Evaluation and Certification Scheme,JISEC）」是指基於國際共同準則標準 ISO/IEC15408，由第三方之檢測實驗室對 IT 相關產品進行安全功能的適當性、確實性評估，並由驗證機關認可評估的結果。該體系之驗證機關為情報處理推進機構(Information-Technology Promotion Agency,IPA)。

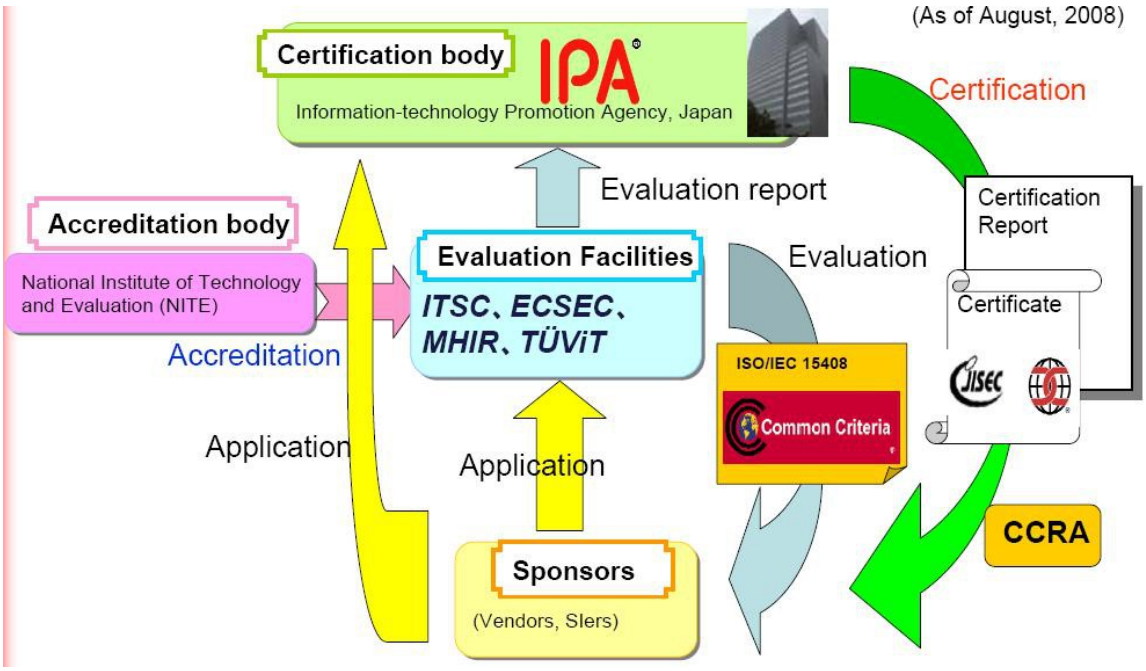


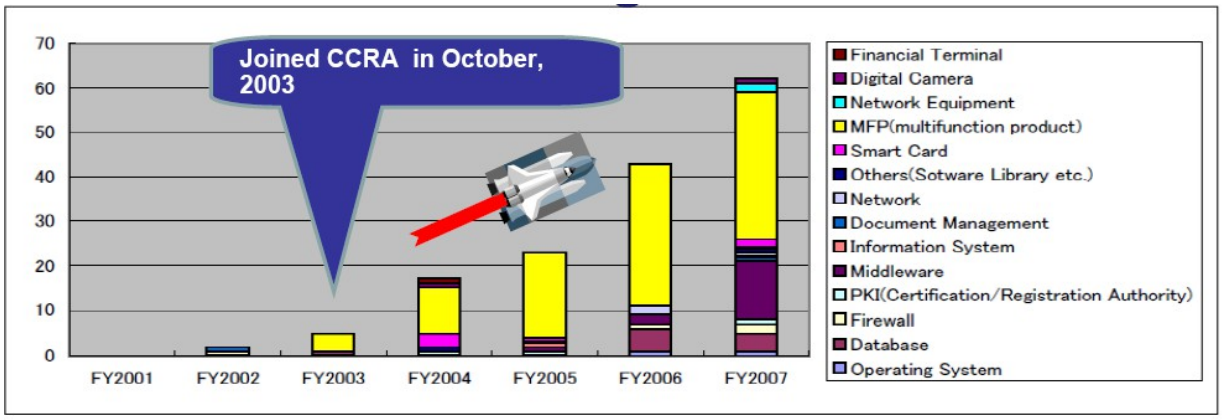
圖 3：日本情報處理推進機構(IPA)驗證體系

表 1：截至 2007 年日本資安產品驗證件數統計

MFP	98	64%
Middleware	16	11%
Database	10	7%
Smartcard	6	4%
Firewall	4	3%
PKI	3	2%
Network	3	2%
OS	2	1%
Document Management	2	1%
Software Library	2	1%
Network Equipment	2	1%
Digital Camera	2	1%
Information System	1	1%
Financial System	1	1%
TOTAL	152	

MFP（Multi Function Product/Printer/ Peripheral）has been a single main engine !

（2）JISEC 自 2001 年起開始建置，至今已有 8 年的時間。於 2001 年自 2007 年期間，共計有 MFP(Multi Function Product/Printer/Peripheral)、Middleware、Smartcard...等 14 類型的資安產品通過驗證機關 IPA 的審驗，並取得驗證證書，核發證書的總數量累計達 152 張。其中又以多功能事務機佔所有驗證產品(佔 IPA 核發證書中的 64%)為大宗，EAL3 等級的產品佔大多數(約佔 40%)。2001 年至 2007 年資安產品依評估標的(TOE) 驗證件數成長趨勢如下圖。



TOE Type	FY2001	FY2002	FY2003	FY2004	FY2005	FY2006	FY2007	Total
Operating System	0	0	0	0	0	1	1	2
Database	0	0	1	0	0	5	4	10
Firewall	0	1	0	0	0	1	2	4
PKI(Certification/Registration Authority)	0	0	0	1	1	0	1	3
Middleware	0	0	0	0	1	2	13	16
Information System	0	0	0	0	1	0	0	1
Document Management	0	1	0	0	0	0	1	2
Network	0	0	0	0	0	2	1	3
Others(Sotware Library etc.)	0	0	0	1	0	0	1	2
Smart Card	0	0	0	3	1	0	2	6
MFP(multifunction product)	0	0	4	10	19	32	33	98
Network Equipment	0	0	0	0	0	0	2	2
Digital Camera	0	0	0	1	0	0	1	2
Financial Terminal	0	0	0	1	0	0	0	1
Total	0	2	5	17	23	43	62	152

圖 4．日本 CC 產品證書核發統計

(3)日本於 2003 年成為 CCRA 會員國，在短短 5 年內所累積的驗證證書數量，已成為授與證書會員國當中，證書核發數量之第 3 名(僅次於德國與美國)。目前境內共有 4 家經認證機構(National Institute of Technology and Evaluation)認可之共同準則檢測實驗室，分別為 ITSC(IT Security Center)、ECSEC(Electronic Commerce Security Technology Laboratory)、MHIR(Mizuho Infomration & Research Institute)及 TÜViT(TÜV Informationstechnik GmbH Evaluation Body for IT-Security)。各國 CC 產品證書件數統計比較如下表。

表 2: 各國 CC 產品證書件數統計比較表

1.How has the JISEC grown ?

	USA	UK	Canada	France	German	Australia	Japan	Netherland	Norway	Korea	Spain	
1997	0	0	1	0	0	0	0					1
1998	1	6	0	0	1	0	0					8
1999	1	5	2	4	1	0	0					13
2000	2	7	2	11	0	1	0					23
2001	4	4	2	16	1	1	0					28
2002	26	7	2	12	8	2	2					59
2003	18	13	7	5	13	5	5					66
2004	31	6	6	22	49	3	17					134
2005	62	6	7	23	46	2	23					169
2006	39	4	4	21	44	1	43	1	2	53	4	216
2007	45	10	18	22	32	5	43	0	0	13	4	192
2008	7	1	2	0	14	-1	19	0	1	2	1	46
合計	236	69	53	136	209	19	152	1	3	68	9	955

↑ Australia includes NZ (March 28, 2008)

(4)情報處理推進機構(Information-Technology Promotion Agency, IPA)為日本資安產品之驗證機構，負責資安驗證體系之運作，共有 10 位驗證人員，具備 IT 產品 10 年以上經驗，每一位驗證人員每年處理 5 至 6 件評估工作，驗證人員任務是確認檢測實驗室之評估員的評估技術報告(ETR)、提出驗證報告(CR)、對產品開發者進行 CC 訓練、發展 CC 相關指導文件。

(5)日本目前評估實驗室共有四家：ITSC、ECSEC、MHIR、TUVIT 評估工作需 3 個月至 1 年時間，依 EAL、TOE 範圍、發展計畫延遲等不同因素，評估工作時間會受影響。

(6)評估保證等級統計件數如下圖。

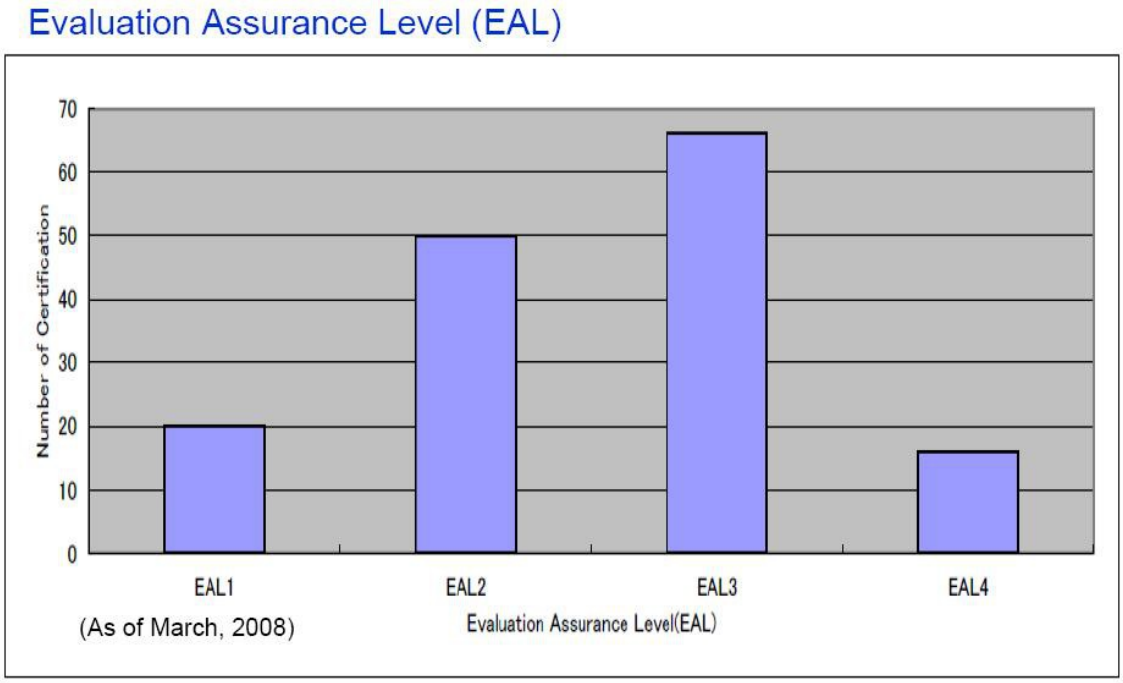


圖 5: 日本評估保證等級統計件數

2.日本政府採購政策

(1)2005 年 12 月日本發布改善 E 政府安全之標準:(Standard for Information Security Measures for the Central Government Computer Systems)

(2)強制規範重要之 E 政府資訊系統及軟體發展，要求安全標的(ST)確認，包括安全標的評估(ASE) 及發展功能規格(ADV_FSP)，以 CCV3.0 版為準。

(3)強力要求採購時，考慮採用經 CC 驗證之資通產品。

3.對日本廠商及使用者進行調查

(1)68%的 IT 使用者不知道 CC，不利於廠商，因為主要獲取 CC 證明的動力是來自使用者。

(2)CC 評估花費時間太長，不符合廠商產品的生命週期，例如他們在產品推出市場時，還不能拿到 CC 證明。

(3)CC 評估費用太高，廠商及使用者不確定 CC 評估有很好的成本效益。

4.日本成立共同準則專案小組(CCTF)

(1)於 2007 年 12 月成立 CCTF。

(2)組成：IPA、評估實驗室、廠商、NITE、METI..等。

(3)決定日本體系方向。

(4)3 個協調工作小組： 市場面工作小組、技術面工作小組、制度面工作小組。

(5)解譯 CC 3.1 版。

(四)新加坡驗證體系現況：

1.體系目標

(1)2005 年國家資通安全委員會資通安全第一期主要計畫，係對商業 IT 產品賡續備妥發展安全能力及相關配套措施，並申請加入 CCRA。

(2)新加坡共同準則評估及驗證體系：

2005 年 5 月指派新加坡資通訊發展局(Infocomm Development Authority of Singapore,IDA)為驗證機關，負責核發驗證證明。

(3)2008 年 4 月資通安全第二期主要計畫：

強化 IT 安全及增強其安全地位、倡議資通安全能力、結合資通安全專業、提供國家資安講學金、建立網路安保聯盟、強化資通安全規範(共通方法論、正確及充分對策、共同準則訓練及維持)、強化國家資通架構及服務、增加國際合作、參與 CCRA 活動及交換最佳實務範例。

(4)推動 CCRA 策略：

對公務部門 IT 產品買者，計畫推動 CCRA 共同準則認知方案，並對投標者提出優先 CC 驗證產品之建議程序。

2.IDA 組織圖

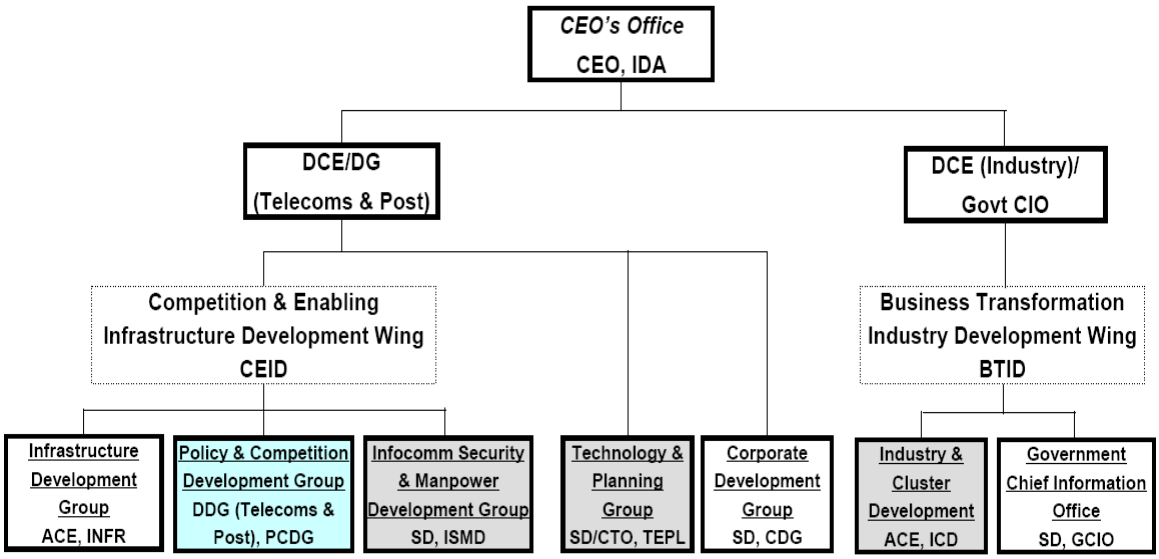


圖 6: 新加坡 IDA 組織架構

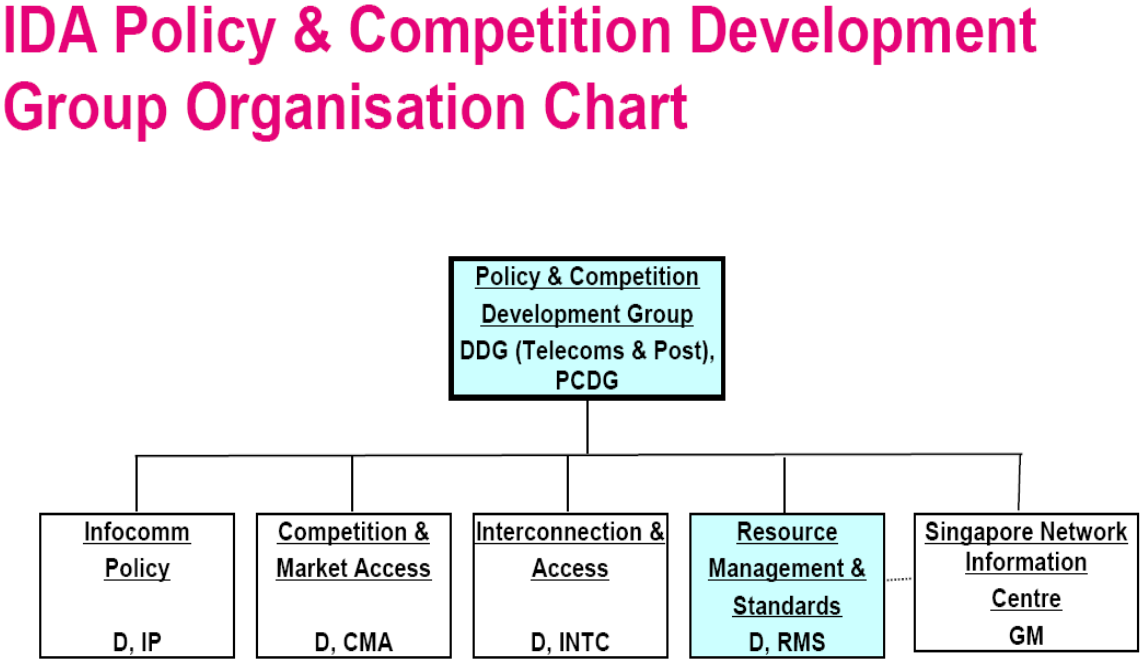


圖 7:新加坡 IDA 政策及競爭發展組織架構

3.驗證機構架構與運作

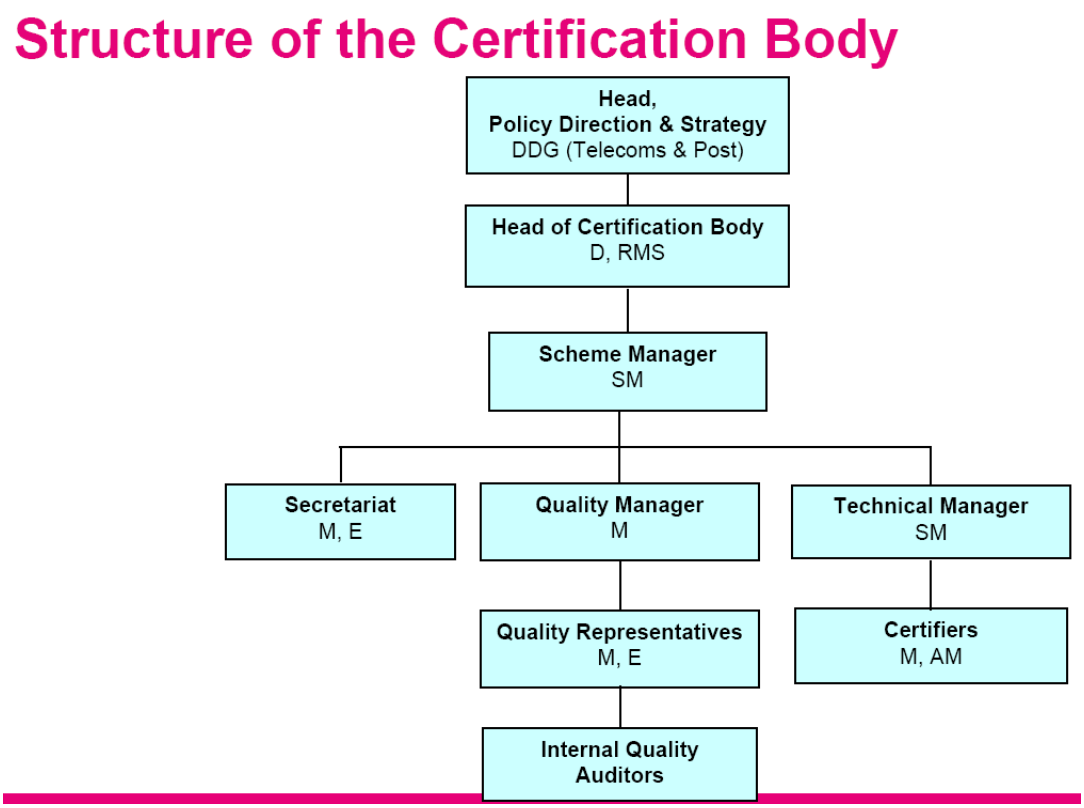


圖 8:新加坡驗證機構架構

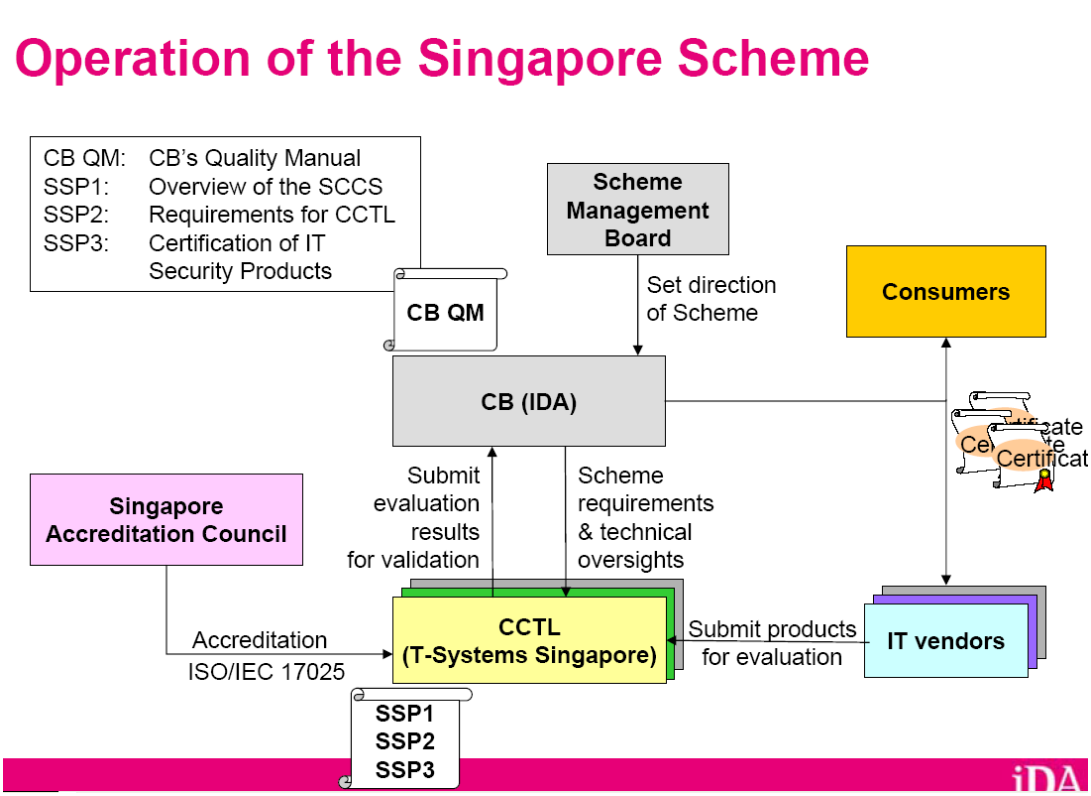


圖 9:新加坡驗證體系運作圖

4.政府體系架構

Governance Structure of the Singapore Scheme

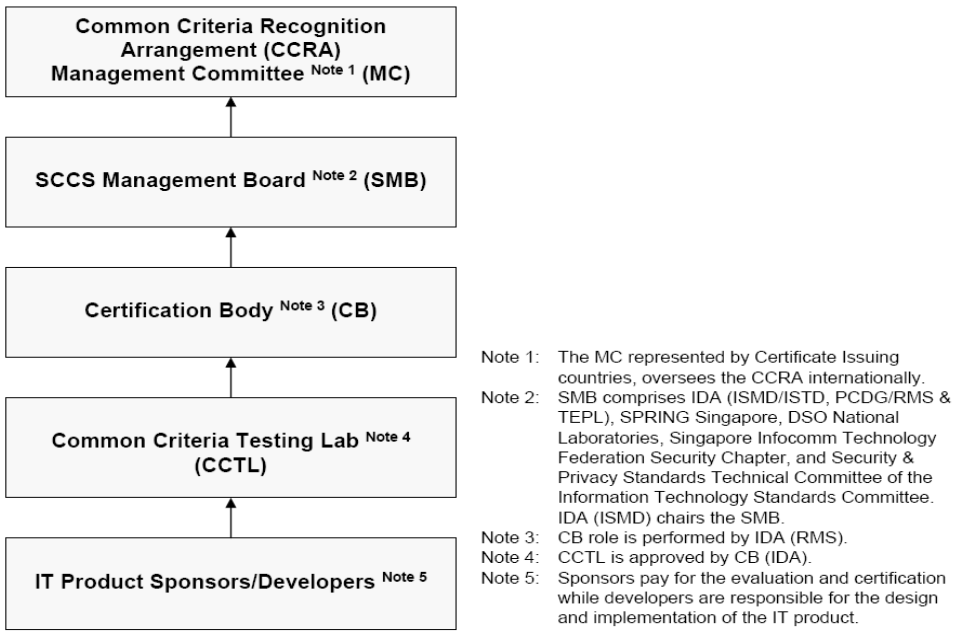


圖 10:新加坡政府體系架構

5.新加坡認證協會(Singapore Accreditation Council)自 1997 年起，已與國際知名的認證機構進行多邊 MRA 簽署，被認可的認證機構如下：。

(1)Asia Pacific Laboratory Accreditation Cooperation for Testing, Calibration and Inspection。(APLAC)

(2)European Accreditation Cooperation for Testing and Calibration International Accreditation Cooperation for Testing and Calibration。(EA)

(3)International Accreditation Cooperation for Testing and Calibration。(ILAC)

(4)International Accreditation Forum for Quality Management System。(IAF)

(5)Pacific Accreditation Cooperation for Quality Management System。(PAC)

(五)馬來西亞驗證體系現況：

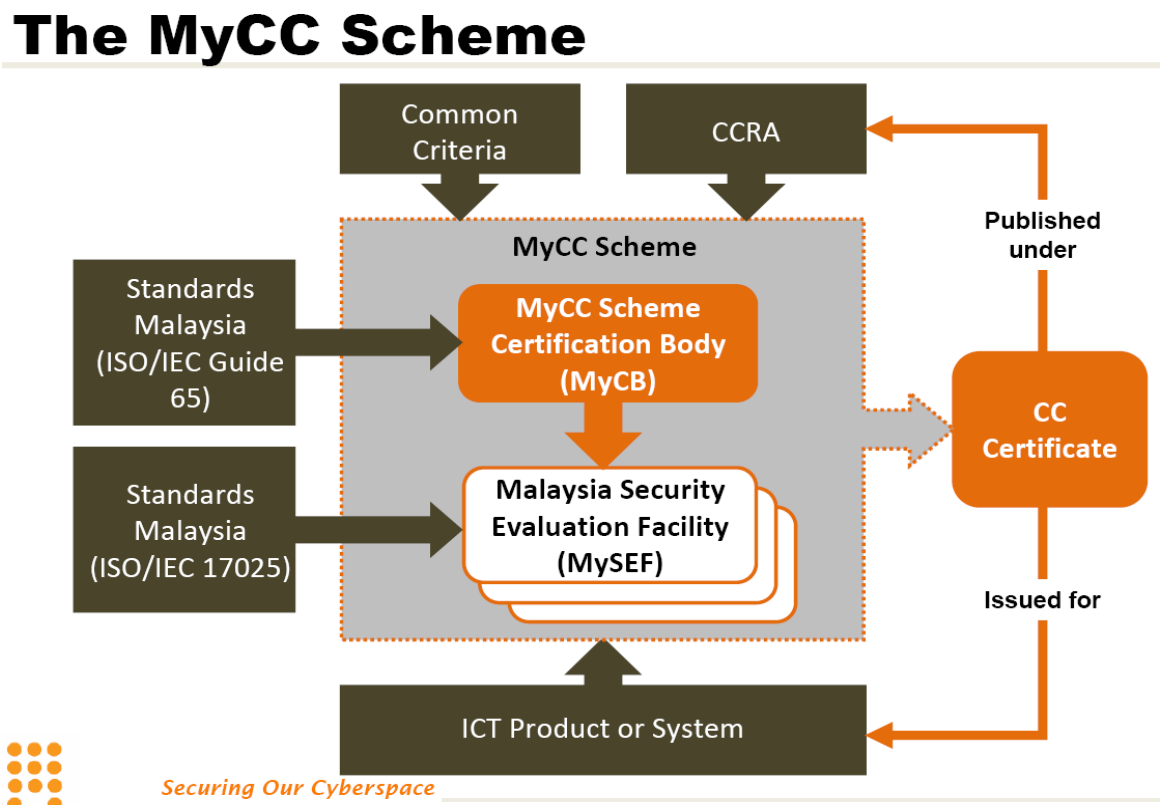


圖 11：馬來西亞驗證體系

1．MYCC 體系之背景

（1） 2006 年建立體系執行計畫。

（2） 2007 年 3 月接受驗證證書。

（3） 2008 年 9 月 MYCC 開始運作。

（4） 依 EAL3/EAL4 執行第一件評估案件。

2.MYCC 體系之任務

增加馬國競爭力、確保資安品質保證、植基於 CC 標準、建立消費者對馬國資安產品的信心。

3.MYCC 體系之服務

(1)ICT 產品及系統、PP 之安全評估及驗證：

依 CC(ISO/IEC 15408) V3.1 版執行評估及驗證，其結果將公布於馬國經驗證合格之產品清單上。

(2)依 CCRA 規定，對經驗證合格之 IT 產品及系統，須負責維持資安保證。

(3)如須特殊目的之認可證明，則由 MYCC 體系政策決定。

4.MYCC 體系之效益

(1)增進 ICT 產品在全球市場的競爭力。

(2)強化馬國在全球 ICT 安全保證服務信譽。

(3)使馬國 ICT 產品得以近接國際市場。

(4)強化馬國資安體系架構。

(5)增強 ICT 產品安全。

5.MYCC 體系之利害關係人

(1)開發者：發展 TOE 評估標的及提出相關資安佐證。

(2)贊助者：大多案例屬開發者，與 MYCC 簽訂合約，提供評估佐證資料。

(3)安全評估之檢測實驗室：評估證據，並提出評估技術報告。

(4)CC 驗證機關：驗證評估結果，產出驗證報告及審驗證明。

6.MYCC 之核心服務

(1)安全評估及驗證 ICT 產品及系統。

(2)安全評估及驗證 CC 之 PP。

(3)維持經驗證之 ICT 產品及系統等級。

(4)為特別目的，認可 CCRA 證明。

(5)其他支援服務：解譯管理、參與 CCRA 訓練及發展、出版管理、證明文件管理。

7.馬國安全檢測實驗室(MYSEF)

(1)MYSEF 符合 ISO/IEC 17025 檢測實驗室之標準，為 MYCC 所認可。

(2)核心服務：

a.安全評估 ICT 產品及系統。

b.安全評估 CC 之 PP。

c.提交評估技術報告至驗證機關(MYCB)進行驗證。

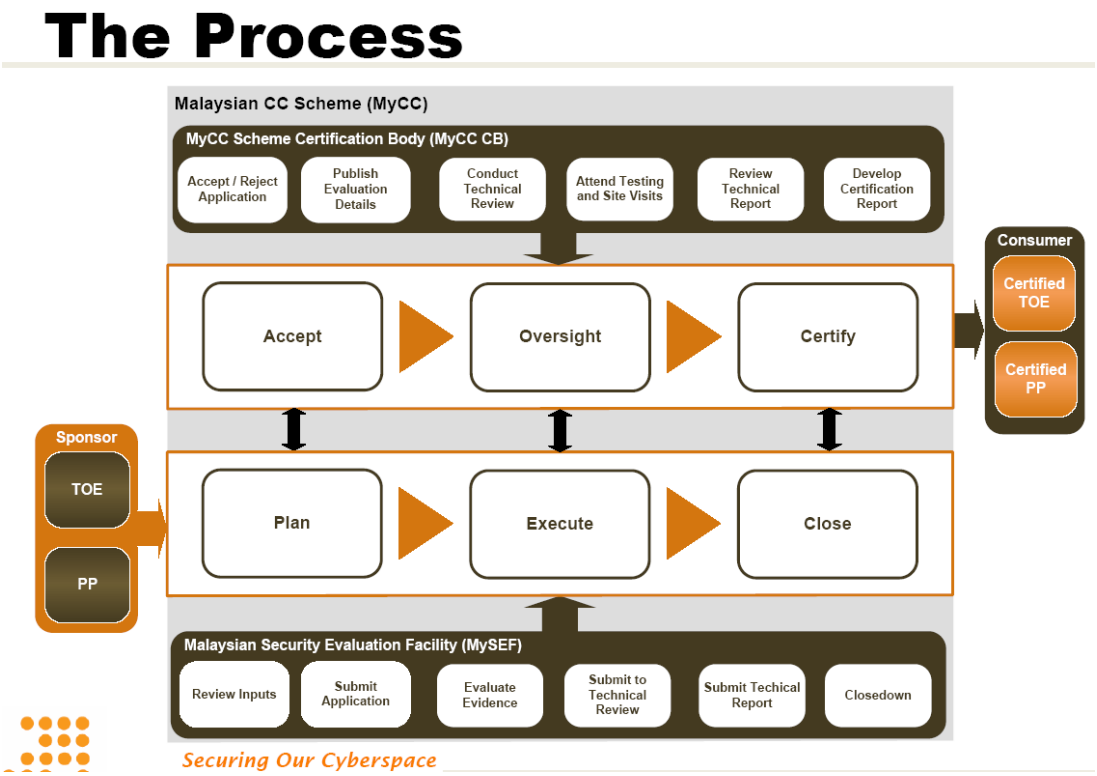


圖 12：馬來西亞驗證處理流程圖

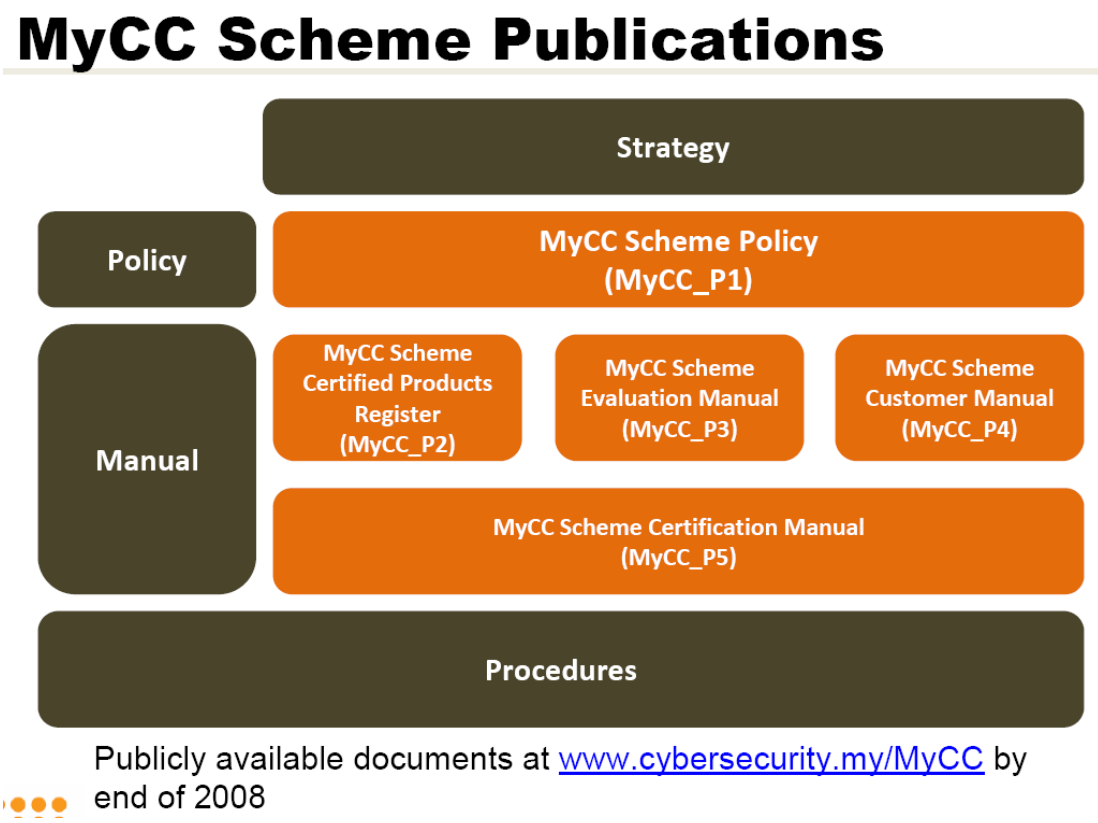


圖 13：馬來西亞驗證文件

Milestone	Date
MyCC Scheme Strategy and Implementation Plan	October 2007
MyCC Scheme and Certification Body Established	August 2008
Accredited Evaluation Facility Established	March 2009
Issue First Certificates (2 products EAL3 or EAL4) using MyCC Scheme	April – June 2009
Application to become CCRA Certificate Producer Member	March 2009
Voluntary Periodic Assessment	June-August 2009

圖 14：馬來西亞驗證體系發展時程

(六)義大利驗證體系現況：

義大利體系於 2003 年 10 月 30 日立法，並於 2004 年 4 月 27 日由首相頒布，其驗證機關為 OCSI。

1.體系文件

(1)LGP1：體系介紹

(2)LGP2：檢測實驗室(LVD)

(3)LGP3：評估及驗證程序

(4)LGP4：評估方法(CEM)

(5)LGP5：評估工作計畫

(6)LGP6：PP 及安全標的(ST)

(7)LGP7：專有名詞。

2.檢測實驗室之資格

實驗室認可有效期限為 3 年，須符合 ISO/IEC 17025 規定，須熟悉國家驗證體系，須具備熟悉 ITSEC 及 CC、IT 安全能力，須嚴格遵守驗證規定。認證機構評鑑檢測實驗室時，須至現場檢查，要求進行 5 天評估技術測試能力，並模擬評估活動，第一次產品評估時，將一步一步監視評估活動；業經認可之證明，若發現不符合認證規定，亦可能被取消。

3.檢測實驗室家數

7 家檢測實驗室具有評估能力：Consorzio RES、IMQ/LPS、ProgeSec、Eutelia s.p.a.、Technis S.C.R.L.、FINSA Tech、GFI Security Lab。

4.2007 年至 2008 年活動

(1)2007 年 9 月參加義大利羅馬舉辦之第 8 屆 ICCC 研討會。

(2)參與 CCDB 工作小組活動並於本屆 ICCC 研討會發表論文。

(3)2007 年開始進行評估案件，已完成 2 件 EAL3 評估，包括 ID 卡產生器 、Authentication and Access control)。

(4)2008 年 7 月 14 日核發上述評估案件之驗證證明，檢測實驗室為 Consorzio RES；另有 1 件 Smart card 進行 EAL4 評估中，檢測實驗室為 Eutelia。

(七)土耳其驗證體系現況：

1.土耳其共同準則評估及驗證體系於 2001 年開始建置。

2.體系相關機構

土耳其標準局(Turkish Standards Institude, TSE)、科技研究委員會(The Scientific and Technological Research Council of Turkey)(TUBITAK)、國家電子及密碼研究院(Natioanal Research Institute of Electronics and Cryptology)(UEKAE)、Turkish General Staff(TGF)、不同開發者、消費者。

3.共同準則驗證系統(CCCS)為土國之驗證機構，係依 CCRA、EN 45011、CCMB 程序及其國家相關法規所成立。

4.CC 進度報告

(1)2001 年

TGF 開始對土耳其國防部(Turkish Armed Forces,TAF)實施 CC 計畫，目標是建立 CC 體系，對 TAF 發展的軟硬體產品或 TAF 採購的資安產品，須依據該計畫辦理。在科技研究委員會(TUBITAK)下之國家電子及密碼研究院(UEKAE)設立 OKTEM 檢測實驗室。

(2)2003 年

a.OKTEM 為土國的共同準則檢測實驗室，係設立於 TUBITAK 之 UEKAE 下。

b.Turkish 標準局(Turkish Standards Institude,TSE)被指派為商業產品之驗證機關。

c.已與 CCRA 簽署為驗證消費國家。

(3)2005 年

a.土耳其立法 TSE 為驗證機關

b.軍事體系由 TGS 經營，商業體系由 TSE 經營，TSE 為土耳其為唯一在共通準則體系的驗證機關。

c.TGS 為唯一對驗證產品的認可機關。

(4)2007 年

TSE、TGS、TUBITAK 下之 UEKAE 開始 CC 體系的運作。

5.組織發展及進度

(1)OKTEM 為檢測實驗室具 CC 評估經驗能力，經 TURKAK 認證機構認證符合 EN17025，並取得 CCCS 核發之檢測實驗室執照，該實驗室目前有 6 個評估員，2 件評估將完成。

(2)TSG 驗證機關決定推動兩種符合 EAL3 以上評估等級的產品。

(3)目前有 3 件正式申請，2 件(EAL4+及 EAL3+)開始評估，6 件以上的產品申請案，尚在協商中。

(4)預定 2009 年第一季於 CCRA 更新體系的最新進展。

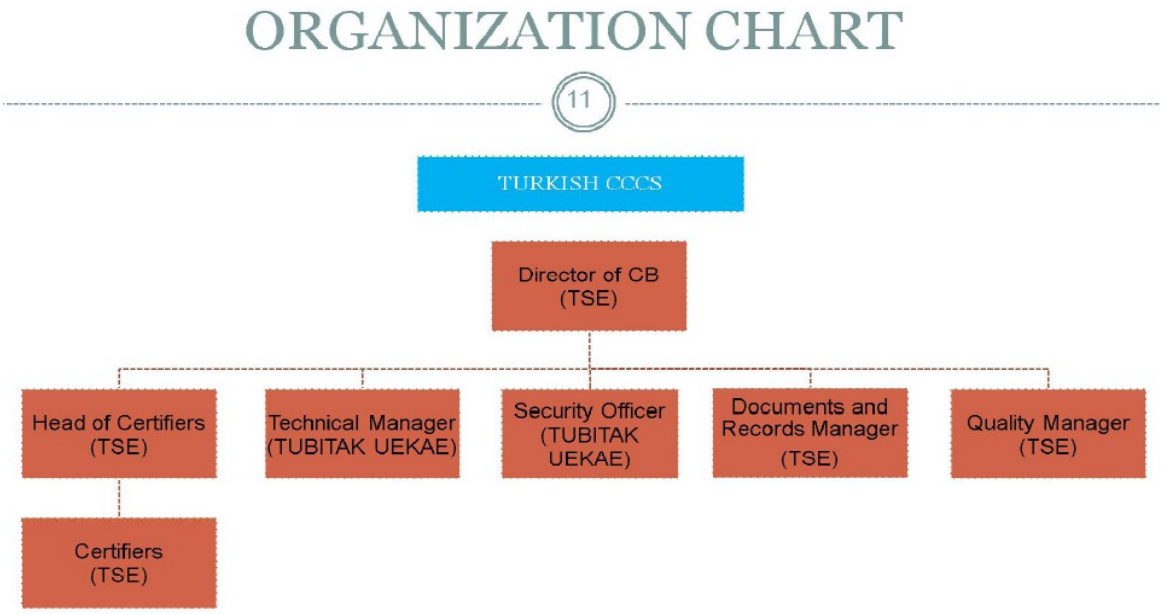


圖 15：土耳其驗證體系組織架構

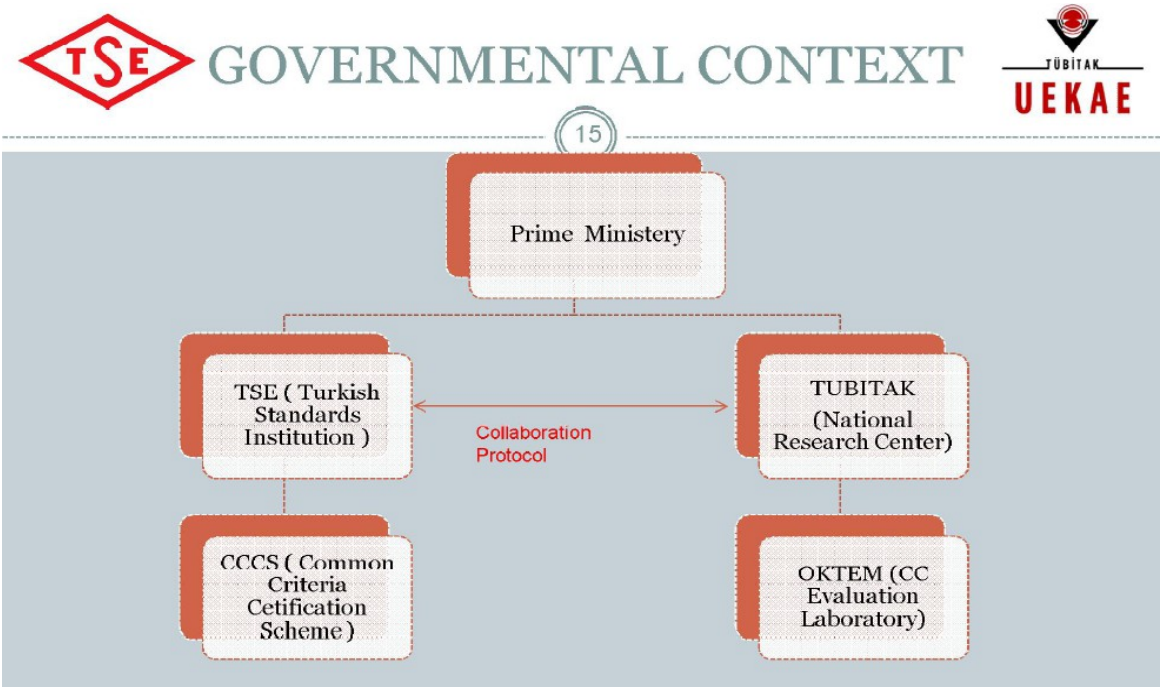


圖 16：土耳其驗證體系政府脈絡

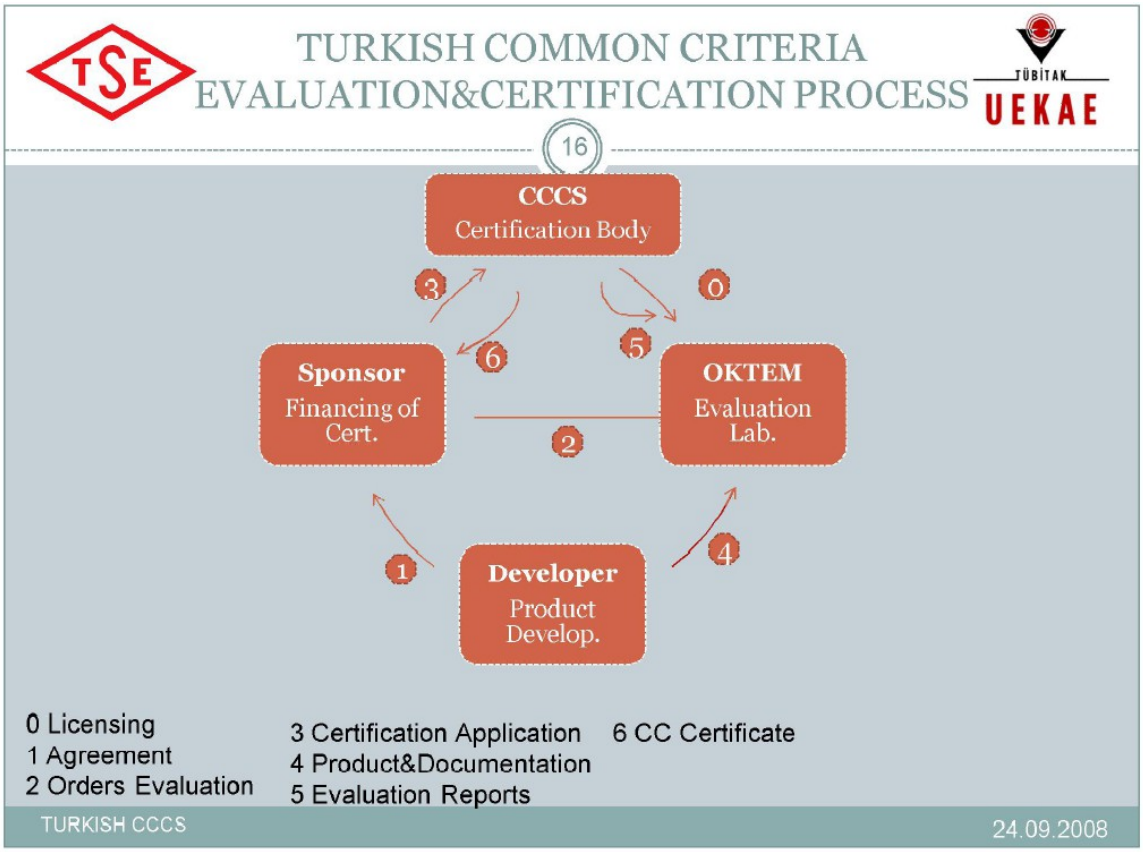


圖 17: 土耳其共同準則評估驗證程序

6.驗證案件

(1)第 1 件 TOE 係 EAL4+安全閘道器，依 CCV2.3 評估，將於 2009 年 2 月完成。

(2)第 2 件 TOE EAL3+公鑰基礎 CA，依 CCV3.1 評估將於 2009 年 1 月完成。

7.CC 經驗

(1)一些評估的步驟，需要較多時間完成，更須投入較多的費用。

(2)土國檢測實驗室具備專業能力及充分經驗，在完整開放的體系組織下，能受理新的評估產品申請案件。

2、檢測機構部分

我國 TTC 於大會簡報 Should and How CC be used to evaluate RFID based Passports/ Chia-Hung Lin, TTC，茲摘述說明如下：

(一)本篇係由 TTC 顧問鄭博仁博士、許碧姍組長及林家弘經理所共同研擬投稿的題目，主要針對目前國際間使用的電子護照所隱藏的安全風險進行研究，並依據共同準則的觀點提出建議事項。

(二)電子護照(e-passport)主要是將護照持有者的生物特徵，以安全存放的模式存於電子護照中的安全晶片，並透過 RFID 的方式進行資料傳輸。就持有者的生物特徵(如：指紋或數位化照片)存放於晶片中這個階段，在 ICAO Doc9303, Part1 Vol.2 規範中已有明確的規定；但在資料傳輸過程部分，也有相關的文獻證明透過 RFID 的方式傳遞資料，確實有存在攔截並竄改資料的風險存在。

(三)電子護照在歐美及部分亞洲國家(共計有 36 個國家)已逐漸普遍使用，雖然所使用的晶片及操作介面有相關的驗證證明，但目前並未有任何完整的電子護照取得共同準則標準上的驗證證書。分析其原因在於共同準則無法針對大型及複雜的產品做一完整性的驗證，更無法確保其使用的安全性。在這樣的使用介面下，必須尋求確保晶片的資料存放、讀取及傳送均能有一定程度的防護機制。

(四)我們發現目前共同準則產品驗證清單中，並未有任何 RFID 相關的 PP 或 ST 經過驗證。因此我們提出可以參考美國政府所制訂的 FIPS 140-2 標準，並運用它在角色、服務與驗證、實體安全及設計保證上的安全分類，對這類型的產品進行驗證，以保護重要的機敏資料能被妥善的保存，以對抗外來的入侵攻擊行為。同時搭配共同準則標準中 FPT 與 FTA 的安全要求，強化電子護照使用上的安全強度。

3、資安廠商部分

因參與研討會之場次問題，僅以德國代表簡報 Biometric in Common Criteria 2008: The big picture/ Nil Tekampe 之內容，摘述分析如下：

(一)簡報者為德國 TÜViT 的評估員，對於生物辨識類的產品檢測已有多年的檢測經驗，在他的簡報中主要是強調生物辨識的技術已越來越成熟，並已普遍的運用在產品上(如：運用在電子護照中)。但是根據統計發現，取得 CC 證書的生物辨識產品，大多在基本的安全防護等級(如:EAL1 及 EAL2)而已，未見較高等級的生物辨識類別產品取得驗證證明。就共同準則的觀點分析其原因，發現生物辨識這類型產品似乎缺乏較為合適且相對應的安全項目進行評估。主要是因為它有別於一般的資安產品，且部分的生物辨識產品常有系統更新的狀況，以及光依賴 CEM 並無法有效的進行評估工作。

(二)本簡報提出目前共同準則的標準已無法對生物辨識這種類別的產品，提供合適的產品檢測依據。應考慮參考過去 CC V2.1 版當中已定義的 BEM（Biometric Evaluation Methodology)，對生物辨識類型產品進行評估，並搭配目前仍在修訂中的 ISO/IEC 19792 標準，方可確保生物辨識類別產品中的：假設與定義、生物辨識科技的安全評估觀念錯誤率、脆弱性評估及隱私性。

(三)特別針對目前修訂中的 ISO/IEC 19792 標準提出說明，並表示未來如成為正式版本後，會包含下列符合生物辨識類型產品特性之要求：產品開發者應提供與安全相關的錯誤率證明、產品開發者應測試生物辨識系統，並提供符合標準的證據，由第三方再針對產品發展者所提出的檢測項目及結果再次進行審驗，將可大幅提昇產品檢測的安全性與可信賴度。

伍、與國外相關單位交流情形

一、研討會期間，本會與 TTC 拜會德國及日本驗證機關代表，並與對方洽談雙方簽訂 MRA 事宜。TTC 亦與德國、日本及美國等國外知名檢測機構進行洽談，以尋求最佳合作模式。另針對中國大陸目前的發展現況，亦與中國信息安全認證中心人員進行討論，對於目前中國大陸的進展亦有進一步的了解。會議期間所拜會之單位與人員詳見表 3 說明。

表 3. 拜會單位一覽表

拜會單位	拜會人員
德國驗證主管機關(BSI)代表	Miss Irmela Ruhrmann
日本驗證主管機關(IPA)代表	Mr. Yasuhide Yamada (山田安秀)
德國 TÜViT 實驗室高階主管	Mr. Antonius Sommer
日本 ECSEC 實驗室高階主管	Mr. Yasuyoshi Uemura (植村泰佳)
日本 IT Security Center 主管	Mr. Naoki Ugamura (宇賀村直紀)
美國 CygnaCom 實驗室高階主管	Miss Nithya Rachamadugu
中國信息安全認證中心副主任	陳曉樺女士

二、與國外驗證機關及檢測機構代表交流情形，茲說明如下：

(一)德國驗證主管機關(BSI)代表表示，無法與非 CCRA 會員國簽訂任何形式的

MRA。

(二)日本驗證主管機關(IPA)代表表示，對於我國目前尚未加入CCRA國際組織感到相當遺憾，因為CC檢測只是單純的技術議題。在瞭解我國申請的現況後，日本代表同時提出以下建議：

1.願意協助我國向其他會員國(如：美國NIAP)詢問，以瞭解各會員國對我國申請案之支持狀況。

2.如我國仍尚未申請成為CCRA會員國之前提下，TTC可考慮是否以依循日本CB的規範，向日本政府提出CC檢測實驗室的申請。

(三)德國TÜViT實驗室高階主管表示，對於我國尚未申請入會案感到遺憾，但TÜViT可以以實驗室的角色從旁協助安排NCC與其他會員國之CB代表洽談簽訂MRA事宜。

(四)日本ECSEC實驗室高階主管表示，未來TTC如有檢測訓練的需求，ECSEC將可協助提供。如有廠商欲申請日本CB所核發的證書，亦可由TTC負責執行前端的顧問諮詢服務，由ECSEC負責執行後端的產品檢測業務。

(五)美國CygnaCom實驗室高階主管表示，美國政府已明確規定欲申請美國CB(NIAP)所核發的驗證證書之送檢廠商，需先訂出未來將銷售的政府單位及聯繫窗口，並填妥意向書(Letter Of Intent，LOI)，實驗室始得受理檢測案件。未來國內如有廠商欲申請美國CB所核發的證書，可由TTC負責提供顧問諮詢服務，CygnaCom負責執行產品檢測，並送交美國CB進行審驗。

(六)中國大陸目前發展現況

1.已參與8次的ICCC年會，於本次會議中首次發表論文-「CC in China」一篇。

2.由信息安全認證中心(Information Security Certification Center)擔任主管機關。

3.已將CC V2.1版翻譯成為中文版，並已制訂相關文件(如：firewall的PP、smartcard embedded software的PP及Guide for PP and ST)，目前正進行CEM(2005版)中文版之翻譯工作。

4.截至目前為止已發行56張CC驗證證書(佔全部證書約8%，EAL1 x 2 、EAL2 x 7、EAL3 x 22、EAL4 x 25)，及639張非CC驗證證書。

5.對於是否承認國外已審驗通過並取得證書之資安產品，中國大陸的代表表示，因中國目前尚非CCRA會員國，所以無法承認國際上已檢測通過的產品證書。

6.未來是否提出CCRA會員國申請，中國代表則表示這部分目前仍在評估中。

陸、心得及建議

一、各國驗證體系具專責單位及專業技能

(1) 以日本為例，日本設置 IPA(Information Security Certification Office)負責審核檢測機構之共同準則評估技術報告，並制定日本資通產品之驗證規範、提供資通產品之審驗服務、核發符合共同準則之產品驗證證書。目前共有 10 位審驗員，且具有超過 10 年之產品研發經驗，平均每位審驗員，每年負責約 5 至 6 件產品審驗案件。

(2) 本會為我國資通安全產品審驗之主管機關，雖然目前本會推動資通安全產品審驗業務尚屬初步階段，然就資通審驗人員的編制及審驗專業技能的培育，日本的經驗及其他新進國家的編制及人力頗值得本會參考。

二、各國驗證體系要求政府機關採購經驗證之資安產品

(1) 自 2005 年起，日本政府對中央政府機關之電腦系統制訂規範，用以改善電子化政府之安全性；並強制要求重要政府機關之資訊系統及軟體開發，應符合 CC V3 中 ASE 及 ADV_FSP 的安全要求，同時更進階要求政府機關於採購 IT 產品時，應優先考量通過 CC 驗證之產品。其他國家如中國大陸亦指派 ISCCC 驗證機關負責強制性資通安全產品驗證工作。如日本亦強力要求採購時，考慮採用經 CC 驗證之資通產品。

(2) 本會於我國資通訊基礎建設第三期機制計畫中，亦將規劃推動政府機關優先採購經本會審驗通過之資通安全產品，此與世界先進國家推動政府機關率先採用資安產品須經認證的方向是一致的。

三、各國皆以加入 CCRA 組織為其國際化之目標（以新加坡為例）

(一)新加坡 IDA (Infocomm Development Authority)為其驗證機關，依據新加坡資通安全發展藍圖規劃，持續發展新加坡 IT 發展能力，於 2005 年 2 月起開始投入參加 CCRA，並於 2007 年 3 月開始制訂 CC 產品驗證體系及推動相關活動，期望與國際接軌。同時依據資通安全發展藍圖規劃之延續，於 2008 年 4 月起加強 IT Security 的執行績效，特別針對：如何增加新加坡之資通安全能量、擴大國家資通安全基礎建設與服務及增加國際合作等方向努力。

(二)雖然新加坡於共同準則領域的規劃與建置起步並不甚早（2005 年起），但目前已是 CCRA 接受證書會員國之一，且對於國際間已核發之 CC 驗證證書，已採相互承認的模式。新加坡的運作模式與各國並無特別不同之處：由認證機關 SAC（Singapore Accreditation Council）負責核發實驗室認證證書，而共同準則之規範是由 IDA 下之規範管理委員會所制訂；目前新加坡境內僅有一家檢測實驗室(T-Systems)。

(三)新加坡的共同準則驗證體系的建立比我國晚，但卻比我國更早成為 CCRA 接受證書會員國，他們在與國際接軌及建置共同準則規範上的努力，值得我國借鏡。特別是他們目前並未有自己的檢測實驗室，僅一家 T-Systems 係德商在新加坡所設立的檢測機構，但主管機關已具備符合國際驗證機關的技術能力。截至目前為止，我國亦僅有一家檢測實驗室 TTC，但完全是由國家經費投入所建置，對照之下，我國資通安全驗證體系已建構出檢測實驗室(TTC)、驗證機關(NCC)及認證機構(TAF)三者關係，並已完整具備驗證體系應有組織架構。

四、我國檢測實驗室之能量分析

(一)觀察本次研討會部分國家所介紹的資通安全產品檢測實驗室建置情況，

了解有的國家尚在起步階段；與國外檢測試驗能力比較，目前我國資安檢測實驗室 TTC 受理案件雖然不多，但環觀 TTC 自初期資通安全環境規劃及建置、檢測設備採購，乃至人員培訓等各階段，已投入相當大的成本及人力。透過培訓單位(德國 TÜViT 實驗室)的能力比對，證明實驗室的評估人員具備與國外相近不遠的檢測能量。截至目前為止，實驗室所累積的檢測技術足以獨立進行 EAL1-EAL4 的產品檢測工作。未來如能參考國外實驗室的營運模式，透過多元化的產品檢測及穩定的檢測數量，來培育評估人員的技術能力，並持續累積檢測經驗，相信對於縮短本國檢測實驗室與國外實驗室間的差距，將會有顯著的成效。

(二)目前我國已提出申請加入 CCRA 會員國，雖本會所核發之驗證證書無法具備國際效力，可能造成檢測實驗室檢測業務拓展的困難，但由於 TTC 實驗室已陸續投入大量的人力與物力，如何在短時間內發揮目前已累積的檢測能量，TTC 應尋求並爭取更多的檢測案及顧問案，使 TTC 檢測能量發揮其極大的效益。

(三)就目前 TTC 檢測能量分析，檢測實驗室已可獨立進行產品檢測業務並提供客戶足夠的顧問諮詢服務。但對於有意願申請檢測的國內廠商而言，並無法滿足國際相互承認的需求。對此，建議 TTC 宜持續與國外檢測機構進行交流，以累積檢測技術，並建立良好合作關係。同時評估是否擔任國外檢測機構之委外實驗室，提供產品檢測初期的顧問諮詢、產品測試及撰寫測試報告等服務給國內申請的廠商，並擔任廠商與國外檢測機構之聯繫窗口，協助廠商取得國外檢測證書。透過 TTC 檢測實驗室提供國內客戶顧問諮詢服務，再由國外實驗室進行後半段的產品檢測，預估可節省廠商直接送檢國外之成本及有效掌握專案執行時程。

(四)未來 TTC 仍需透過與國外檢測機構已建立的合作關係，持續協助 NCC 與國外檢測機構及驗證機構建立聯繫管道，並適時協助 NCC 與國外單位進行交流，進一步與各會員國驗證機關洽談簽訂雙邊 MRA 合作事宜，以爭取簽訂雙邊 MRA 機會，使我國資訊安全產品認驗證業務能順利推向國際舞台。

五、持續參加下屆研討會，並爭取介紹我國驗證體系現況的機會

持續參加下屆研討會，並爭取投稿機會，於會議中介紹我國驗證體系及推動共同準則情形，以增加國際間了解我國在此領域所投入的努力及具體成果的機會。就目前國際現況及本次會議中所獲得的訊息看來，我國欲順利申請成為 CCRA 會員國目標，尚須爭取各會員國的支持，爭取在 ICCC 國際研討會中介紹我國驗證體系機會，使各國了解我國推動國際共同準則情形，應是本會下一屆參加 ICCC 研討會的首要目標。

柒、附件：研討會會場


9th ICCC
9th International Common Criteria Conference
23 - 25 September 2008, Shilla Jeju Hotel, Jeju, Korea
Organized by nis
CCRA Overview
CCRA = Arrangement document signed by all members to recognise CC certificates
Members
Governmental Bodies representing 25 nations
Goals
Enable Mutual Recognition


9th ICCC
9th International Common Criteria Conference
23 - 25 September 2008, Shilla Jeju Hotel, Jeju, Korea
Organized by nis