出國報告（出國類別：會議）

2007年第八屆共同準則國際研討會（ICCC）

服務機關：國家通訊傳播委員會

姓名職稱：謝進男　委　　員

　　許英明　簡任技正

派赴國家：義大利

出國期間：96 年 9 月 25 日至 9 月 27 日

報告日期：96 年 10 月 30 日

摘要

共同準則國際研討會，每年舉辦一次。會中所發表專題演講內容包括：各國驗證體系介紹、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、共同準則內容及應用之新創見等。我國目前正積極推動資安產品驗證業務。開始受理資安產品驗證。目前有一件數位簽章產生器保護剖繪案通過驗證，另有二件智慧卡在驗證中。本會已向 CCRA 申請入會，目前本案正由 CCRA 的管理委員會審查中。我國若能加入 CCRA 國際組織成為會員國，將可使我國資安產品在國際市場擁有相互認證及行銷的優勢。此次參加研討會除見 CCRA 主席交換意見外，亦實地瞭解我國申請入會的進展狀況及各國驗證機關的作為，供我國推動驗證業務借鏡。

目次

1、 目的---------- 4
2、 過程---------- 5
3、 心得及建議----------21
附件----------24

4、 目的：

(一)主題：2007 年第八屆共同準則國際研討會（ICCC）

共同準則國際研討會（International Common Criteria Conference，簡稱 ICCC），每年由共同準則國際交互承認組織(Common Criteria Recognition Arrangement，簡稱 CCRA)的會員國輪流主辦。該組織目前有 24 個會員國，分成二種身分，一種稱為「接受證書會員國」（Certificate-Consuming Participants，簡稱 CCP）有芬蘭、希臘、以色列、義大利、印度、丹麥、土耳其、瑞典、匈胸牙利、新加坡、奧地利、捷克等 12 個國家。另一種稱為「核發證書會員國」（Certificate-Authorizing Participants，簡稱 CAP）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」指接受核發證書會員國已驗證的資安產品可在其國內市場上行銷，而不必再經其國內驗證機關驗證後，才可在其國內行銷。而「核發證書會員國」是指該國有能力驗證資安產品，並給予驗證證書，使此產品能憑此證書行銷至其他 23 個會員國，而不必再向其輸出國重新申請產品驗證才可上市行銷。

今年研討會由義大利主辦在羅馬舉行，約有 35 個國家 200 多人參加研討會。會期 3 天，自 96 年 9 月 25 日至 9 月 27 日。會中由各個投稿人發表專題演講，共有 69 編，其主要內容包括：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。

(二)緣起：

我國「建立資安產品驗證體系計畫」為四年延續性計畫(*e-Taiwan* 計畫項下)，計畫期程自 92~95 年，其中 92~93 年業由經濟部商業司主辦。惟為因應電信、資訊及傳播科技及產業之匯流，復為有效運用國家資源，並利後續資安工作之推展，行政院科技顧問組遂於 93 年 6 月 1 日函示，將前揭計畫 94~95 年度預算改由交通部電信總局編列並執行。95 年本會依據本會組織法第 3 條第 8 款：資通安全之技術規範及管制，繼續執行此計畫之任務。本會於民國 95 年 7 月在技術管理處成立「技術認證及資訊安全科」積極推動資安產品的驗證業務。目前該團隊有四位成員。現在已經完成的文件草案有：資訊技術安全評估共同準則第二部-安全功能需求技術規範(第 2.2 版)、資訊技術安全評估共同準則第二部-安全功能需求技術規範(第 2.3 版)、資訊技術安全評估共同準則第三部-安全保證需求技術規範(第

2.2 版)、資訊技術安全評估共同準則第三部-安全保證需求技術規範(第 2.3 版)、實驗室管理作業要點、資通安全設備及保護剖繪審驗辦法、規費收費標準等共 7 件。進行中的文件草案有：共同準則第 3.1 版、共同方法論 3.1 版。本會也已採購電腦設備一批，計劃於年底在本會建立一個符合 ISO GUIDE 65 的資安產品驗證專屬的辦公室及文件室。本會於今年 6 月 13 日公布「資通安全產品暨保護剖繪驗證作業要點」，開始受理資安產品的驗證作業。目前已有一件數位簽章產生器保護剖繪已經通驗證，還有二件智慧卡驗證案尚在評估驗證中。

同時、本會也於民國 95 年 10 月向 CCRA 寄出申請文件申請入會，希望成為 CCP，目前本案正由 CCRA 的管理委員會審查中。其間，在 2006 年的 CCRA 主席是荷蘭籍的 Mr.Taal，他未完成我國的入會審核，即交給 2007 年的主席義大利籍 Mr.Palagiano 繼續審核我國入會申請。本會多次向 Mr.Palagiano 連繫探尋狀況，均無回應。甚至，本會劉孔中委員本（96）年三 3 因公出訪西班牙，於回程中去義大利親訪 Mr.Palagiano，亦未獲會見。鑑於我國若能加入 CCRA 國際組織成為會員國，對我國的資安產品在國外市場有相互認證行銷國際的優勢，也更能促進資安產業的發展利基，創造我國巨額外貿營收。本會逐於 8 月決定加派謝進男委員參加今年度的 ICCC 並拜會 Mr.Palagiano。

原定計畫目標：

1. 會見 CCRA 主席義大利籍 M.Palagiano 瞭解我國申請入會的進展狀況。
2. 瞭解各國驗證機關的作為，以供我國推動驗證業務借鏡。

5、 過程：

(一)會見 CCRA 主席 Mr.Palagiano，摘錄重點如下：

1.我國欲加入 CCP 的申請案，以台澎金馬地區名義申請，在遞交文件和程序上均無問題，但需有全體 24 會員的一致同意方能獲准。由於 CCRA 規定「一個國家只能有一個驗證機關代表」，關於此點，審查委員對我國申請入會有意見，本案逐演變成棘手的政治問題。目前尚未有結論。

2.我方提出在國際貿易組織(WTO)裏，我國也是以台澎金馬獨立關稅領域名義申請獲准入會，但仍無法為 Mr.Palagiano 所接受。

3.Mr.Palagiano 建議我國先行逐一和各國建立資安產品相互承認關

係，到時自然水道渠成，所有會員國均會同意我國加入CCP。

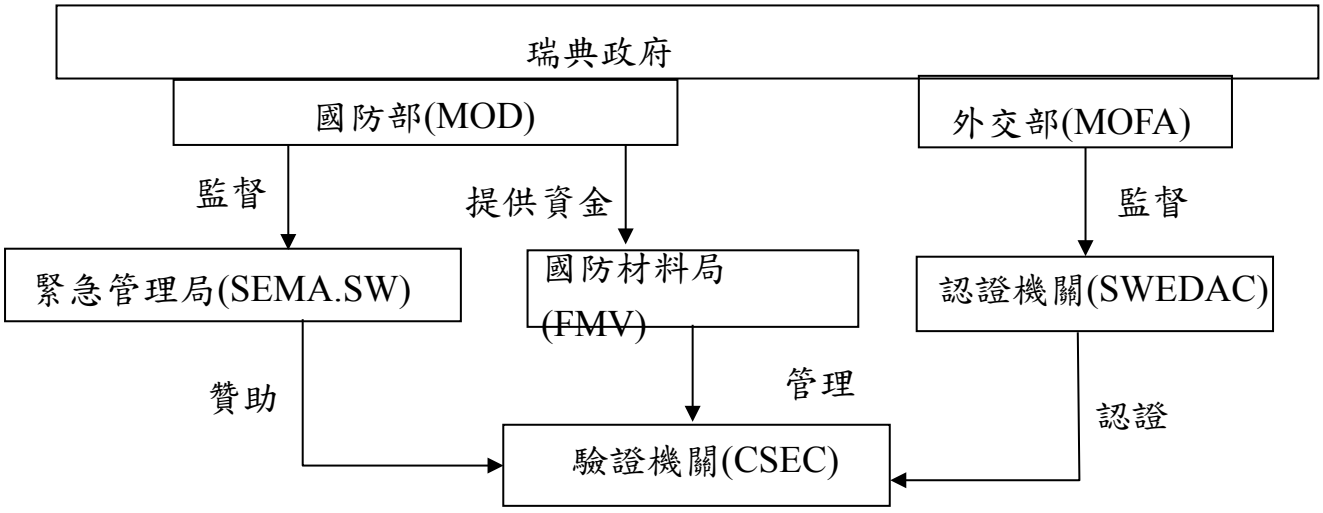
(二)瞭解各國驗證機關的作為：

本次研討會計有6個國家報告其資訊技術安全評估驗證體系，茲摘錄一個接受證書會員國-瑞典，與4個核發證書會員國-韓國、英國、德國、西班牙的驗證運作情形，作為我國發展驗證體系之借鏡。

1.瑞典驗證體系現況

(1)瑞典驗證機關(CSEC)的法源基礎來自於2002年5月瑞典國會通過法案，其內容為：指定瑞典國防材料管理局(FMV)遵照共同準則進行評估和驗證設立和維持制度的工作。評估機構的執照由FMV核發。FMV為驗證機構並核發驗證證書。FMV應從事國際合作，以保證和維持瑞典的驗證證書受到承認。FMV應在評估方法論的持續改善中有國際性的貢獻。經SWEDAC認證的驗證機關是合法的。

(2)驗證機關(CSEC)與政府其他部門之間的關係



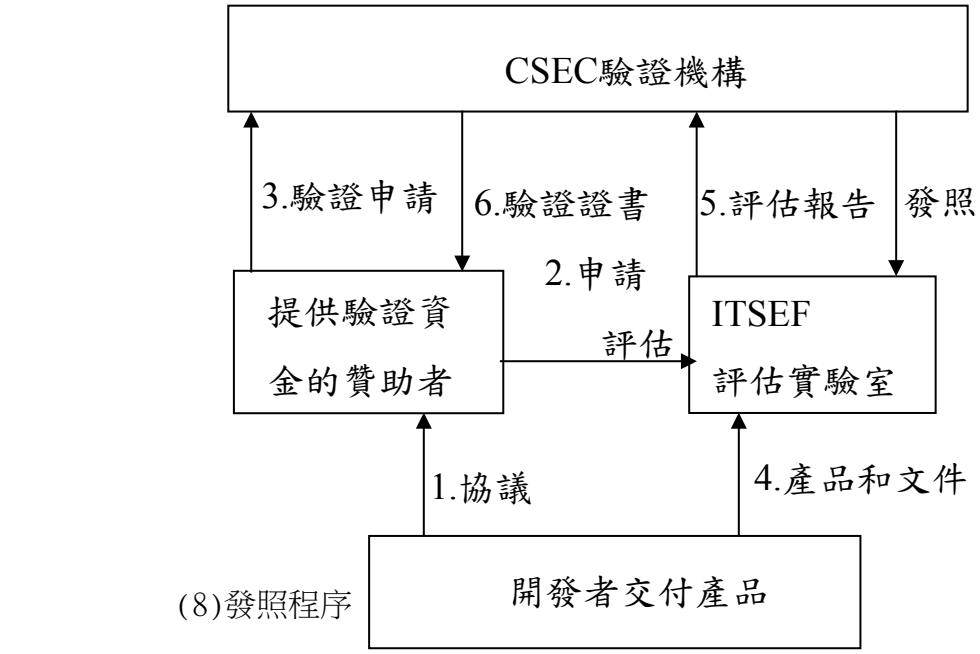
(3)CSEC的主要工作：發照給資訊技術安全評估實驗室(以下簡稱ITSEF)。監督ITSEF的營運。對ITSEF的訓練與支持。監督評估作業。審查評估報告。撰寫驗證報告。頒發驗證證書。公布驗證清單。參與國際合作。推展共同準則。維持並發展驗證體系。執行驗證體系的規範。CSEC的董事會和委員會

(4)FMV董事會：由FMV董事會主席領導，遵照政府的指導制定政策並監督驗證體系的運作。

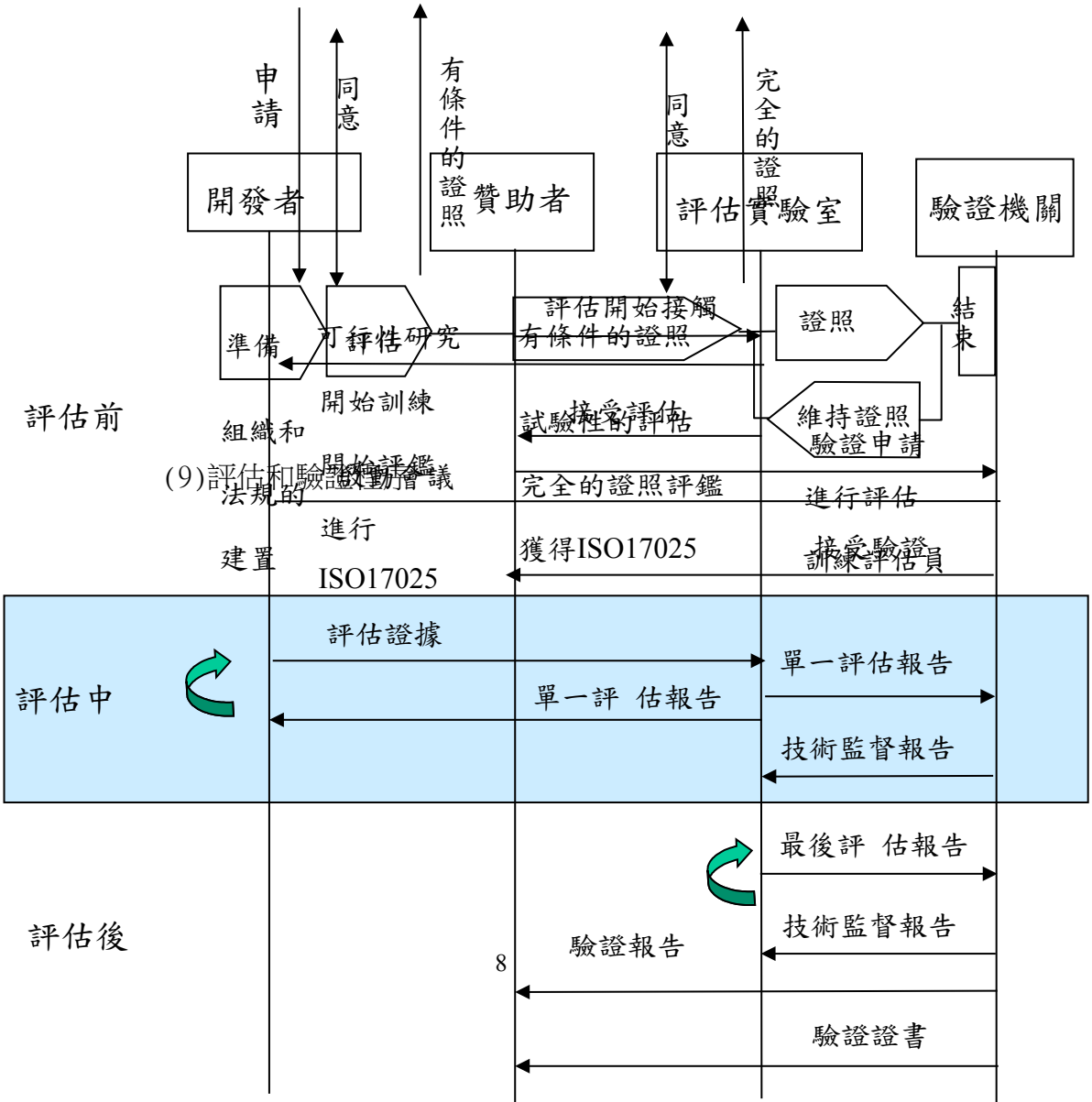
(5)驗證體系諮詢委員會：由CSEC主管領導，參與有關驗證制度的內容和功能性的政策和原則的諮詢。

(6)變革管制委員會：由品質經理領導，管理和控制 CSEC 有關變革管理和違法處理的作業程序

(7)驗證體系架構



(8)發照程序



(10)驗證體制文件：有 SP-001 Certification and Evaluation Scheme – Scheme Overiew。SP-002 Evaluation and certification。SP-003 Certificate Maintenanc。SP-004 Licensing of Evaluation Facilities。SP-005 Mutual Rcobnition and International Liaisn。SP-007 Quality Manual。SP-008 Charges and Fees。SP-010 Certification Application - form。SP-021 ITSEF License Application - form。SP-022 Evaluator Status Change Application - form。SP-024 Evalutor IT Security Competence - form。SP-061 Certification Agreement - form。SP-070 Conditions for the Use of Trademarks。SP-079 Licensing Agreement – form。SP-084 Sponsor’s and Developer’s Guide。SP-089 Complaint Report - form。SP-092 Appeal Report - form。SP-094 Request for Interpretation - form。SP-103 Terms of Reference for the scheme Advisory Committee。SP-136 Legal Dependencies。SP-153 License Agreement。

(11)目前狀況：

A.驗證機關(CSEC)：人員，文件和程序書都已準備妥善。正在進行 4 件產品驗證。申請 EN45011 的認證接近完成。2007 年 9 月初已進行 CCRA 同步檢測。

B.評估實驗室：有二家評估實驗室，即 Combitech 和 atsec。這二家都得到 CSEC 有條件的執照。這二家的認證接近完成。這二家的試驗評估接近完成。在此驗證體系裏約有 10 位評估員。

(12)與 SEMA 的合作事項：有 SEMA 是瑞典緊急管理局部(Swedish

Emergency Management Agent)。提供有關 CC 和 CCRA 的資訊小冊。研究找出 CCRA 能夠合用於瑞典政府單位的保護剖繪。與瑞典政府其他單位合作(認明 IT 產品用於瑞典政府最普遍的威脅。認明由這種 IT 產品所引起最普遍的 IT 事故)。在驗證員監督 PP 和產品評估期間提供指導。

2.韓國驗證體系現況

(1)介紹 ITSCC：

A.ITSCC(IT Security Certification Center，簡稱資訊技術安全驗證中心)，政府部門在採購之前對商用 IT 安全產品評估及驗證以增強 IT 安全目的而設置。為韓國安全驗證的驗證機關。負責韓國的評估和驗證體系之運作。

B.主要角色：

以共同準則驗證 IT 安全產品。協助採購者確認經共同準則驗證過的產品。制定保護剖繪供開發者引用。核准 IT 安全評估實驗室。教育訓練 IT 安全評估員。促進國際合作。

(2)韓國的採購政策：

A.自從 2006 年 1 月 1 日開始，政府部門必採購已經驗證過的 IT 安全產品。促進共同準則在韓國的使用。鼓勵韓國開發者生產健全的安全產品以符合國際準。

B.雖然這個政策在商用 IT 安全產品信賴度的提高有所貢獻，但申請共同準則驗證的產品數量遠超過評估的能力。這樣導致等候評估時間的增加。

(3)新的評估實驗室：

A.核准新的評估實驗室：

擴充評估的容量是必要的，以應付增加的申請量。韓國資訊安全局(Korea Information Security Agency，簡稱 KISA)是韓國法定的唯一評估機關。在 2006 年 12 月，修訂現行的法律和規定，提供法源基礎，發照給 KISA 以外的評估機構。今年年初、韓國測試實驗室(Korea Testing Laboratory，簡稱 KTL)和韓國系統保證(KOrea SYstem ASsurance，簡稱 KOSYAS)申請獲准。KTL 和 KOSYAS 在遵照 ISO17025 認證後，最後分別於 6 月 29 日和 8 月 9 日獲准設立。

B.建立共同準則評估員的證照計劃：

評估機構需要愈來愈多的評估員。產生對系統化教育和評估員管理的需求，以保證評估品質符合國家的水準。

評估員的證照計劃

類別	審核條件	達成工作能力
受訓員	成功完成 10 天的教育訓練並通過考試	在評估員的監督下、有能力參加評估
評估員	參加 1 個以上的 EAL3 評估	有能力評估 EAL3 的產品
高級評估員	參加 2 個以上的 EAL4 評估並當評估員有 3 年以上的工作經驗	有能力評估 EAL4 的產品並且可成為主導評估員

另外，在一流的研究所也開辦共同準則教育課程，由資深的評估員或驗證員來授課。

(4)國內驗證計劃：

實施一種國內驗證計劃以處理產品長期排隊等候評估的問題。此計畫與共同準則相同，除了取樣評估以外不對某些組件全數檢查。此計劃目標在於減少幾星期的評估時間，以減少等候時間。一些可交付的評估需要遵照共同準則的評估。在排隊等候評估有相當長時間的產品，有 50%的產品轉變申請國內驗證。然而大部分最近進入評估排隊的產品申請共同準則的驗證。

(5)提供保護剖繪，供應 IT 安全產品的開發者。指導開發者正確開發產品，大大地減少評估時間，因為它減少可能的觀報告 ITSCC 一年開發 4 件保護剖繪供產品使用。因來自政府各機關的大量需求。和市場成長的高度潛力。

(6) 驗證評估管理系統 (Certification and Evaluation Management System，簡稱 CEMS)

A.自動化評估及驗證處理：

在驗證機關和評估實驗室間進行交付處理時，如：傳送、接收和登記文件，對於評估時不可避免的延遲負有部分的責任。建構一個自動化系統以支持線上交換、交付儲存和線上方案管理的功能會有益的。為以上目的，ITSCC 已經開發 CEMS。

B.CEMS 的主要特性：

CEMS 是一套以網路為基礎的客戶-伺服器系統，在 Windows

IIS 和 MS-SQL 的伺服器上執行。它包括二個次系統，即：CMS 和 EMS：CMS 不可接取外部的驗證機關。EMS 能夠從評估實驗室經由被鑑別的客戶進行存取。因此、評估員能夠上載或下載資料。它能夠線上文件管理和管理。即時監督工作進度。文件樣本的管理。CEMS 使用者管理和稽核功能。備份和其他系統的維護。

4.英國驗證體系現況：

(1)英國驗證體系：

英國於 1991 年建置一個使系統和產品能夠評估的驗證體系。在國際上其驗證證書已受承認。因為開發者需要他們的產品安全特性聲明，有一張正式在國際上被承認的證明。由獨立的測試實驗室(CommerciaL Evaluation Facilities – 簡稱 CLEF)實施評估。驗證機關(Certification Body，簡稱 CB)，以 CESG 為主，監督和驗證英國所有系統和產品的評估。已成功地完成一件評估，一個正式保證等級和頒發一張驗證證書；其結果被公布在 CESG 網站的驗證報告裏和 CC 網站上。CB 提供英國驗證體系的基礎建設：包括評估準則，方法論，程序和規則(UKSPs)，解釋文等。其驗證體系規則包括：品質和管理、安全/機密性、評估員訓練和能力、指派工作和 CLEFs 的認證。評估相關參與者有開發者、贊助者、評估員、驗證員、認證員。驗證業務以成本為考量。由商用實驗室進行評估。已驗證的 EAL1-EAL5 的產品總共有 68 件，其報告公布 CESG 網站上。經 ISO 17025：2005 認證的 CLEF 有 4 家：包括 LogicaCMG、EDS、BT、SiVenture。

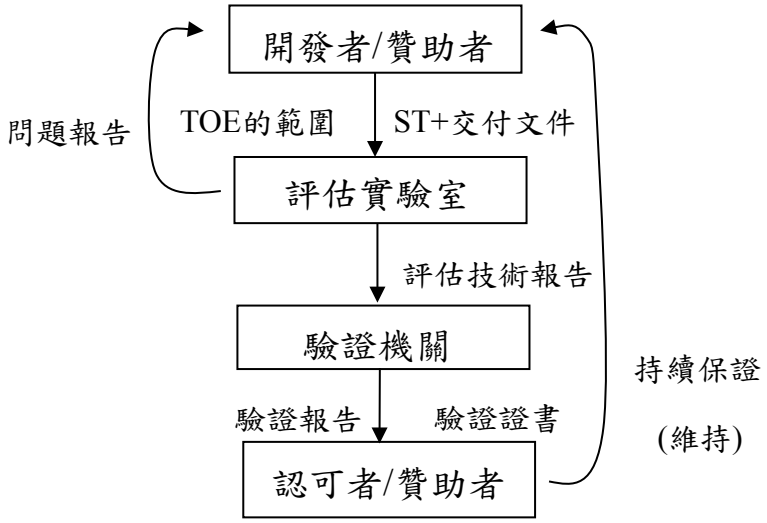
(2)驗證業務發展趨勢：

今年在英國共同準則驗證和評估的需求有相當大的增加。通常評估所需的時間要 6 個月，但視後述情況而定：由贊助者和 CESG 所排定的評估優先秩序、資源的可用性、評估產品的大小，範圍和複雜度、適時和正確的文件交付問題。

(3)英國驗證體系的做法：

在 2005 年更新評估和驗證程序，著重於技術監督。TOE 的範圍要與我們所期望的終端使用者群所使用的產品一致。在開始正式評估之前，安全標的(Security Target，簡稱 ST)須經 CB 同意。脆弱性分析(Vulnerability Analysis，簡稱 VLA)的重點著重於識別潛在的脆弱性。

(4)英國 IT 安全評估和驗證程序：



(5)目前業務：

目前有 11 件產品正在評估中。其類型包括：通信、安全消除資料、資料庫、防火牆、網路系統、作業系統、PC 存取制、保護剖繪和軍用系統的雜項產品。

驗證產品統計

	美國	西班牙	英國	芬蘭	以色列	日本	計
已驗證產品	25	1	38	0	1	3	68
評估中產品	1	0	9	1	0	0	11

(6)其他由 CESG 所提供的業務：

CESG 裁減保證業務（簡稱 CTAS），為了能取代 SYSn 和 Track、IA 顧問(機關、團體、公司內部)、CESG 顧問徵募方案，經由產業合夥關係提供顧問服務、CESG 援助產品方案、評估和符合性測試。TEMPEST 評鑑和驗證。IT 安全健康檢查和 CHECK，滲透測試。CESG 入侵偵測業務。

(7)CESG 裁減保證業務（CTAS）：

CTAS 於 2007 年 6 月開始。以一種單項業務取代 SYSn 評估和 Fast Track 評鑑、取二家之長、全面性符合 HMG Infosec 一號標準（IS1）的需求等同於 EAL2-EAL4。其改善評估方法為保證尋找脆弱性更會徹底。其改善對顧客的服務為提供保證活動項目裁減至驗證者的需求。目前已選出 3 家 CTAS 評估公司：即 KPMGLLP、NCC Group plc 和 NGS Software Ltd。

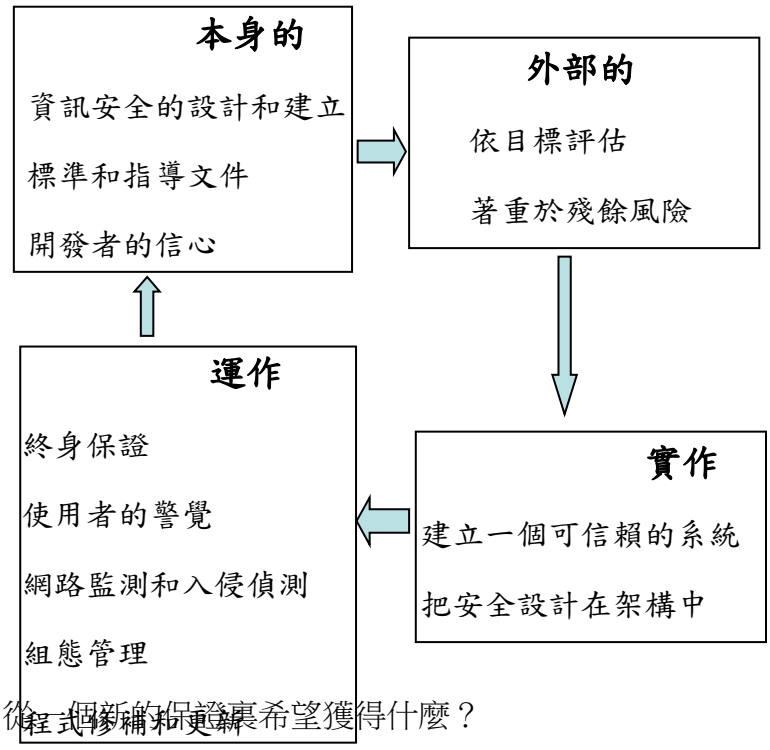
(8)CTAS 保證活動項目：

A.低等級（EAL2-EAL3）的活動項目有：開發程序評論、產品功能和設計評鑑、安全功能（和滲透）測試、系統架構和設計評論、安裝和操作程序評、保證維持評論。

B.高等級（EAL4）的活動項目有：除以上之外另加、原始碼分析、脆弱性分析和測試。

(9)CTAS 的特點：對特定的需求，用清礎、簡潔的英文說明其安全標的、評估工作計劃說明保證活動項目和裁減的項目、評估員要會寫安全標的、評論工作從檢查範圍、安全架構和保證策略開始加強評估員瞭解產品或系統並且開發安全（功能和滲透）測試。一有重大問題產生，應立即透過觀察報告解決。評估報告在安全使用上提供指引，著重在安全問題和殘餘的風險。CESG 的聲明只是確認評估技術的適當性，而不授予正式 的保證等級。保證維持在確保其持續性。

(10)CESG 的保證模型：



(11)從一個新的保證裏希望獲得什麼？

一個更全面性的保證觀點，使所有觀點被認為可增益資訊安全信心、更豐富的資訊集，幫助認證者和風險管理者、決定保證的努力應該被放在何處以產生最大的利益和那個元件會有最大的風險、加速保證處理並且減少成本、鼓勵終身持續朝向 IA 努力、幫助指導 CESG 保證業務的發展、成為文化變革的觸

媒，它包括加重責任以確保開發者/廠商，國家技術局，和顧客/使用者、在交付的制度下，增廣其專業地位。

(12)重要訊息有：對所有保證活動有一個更廣更全面性的看法、持續和生命週期的保證、風險的識別，降低和管理、共享所有並保證負責。

4.德國驗證體系現況

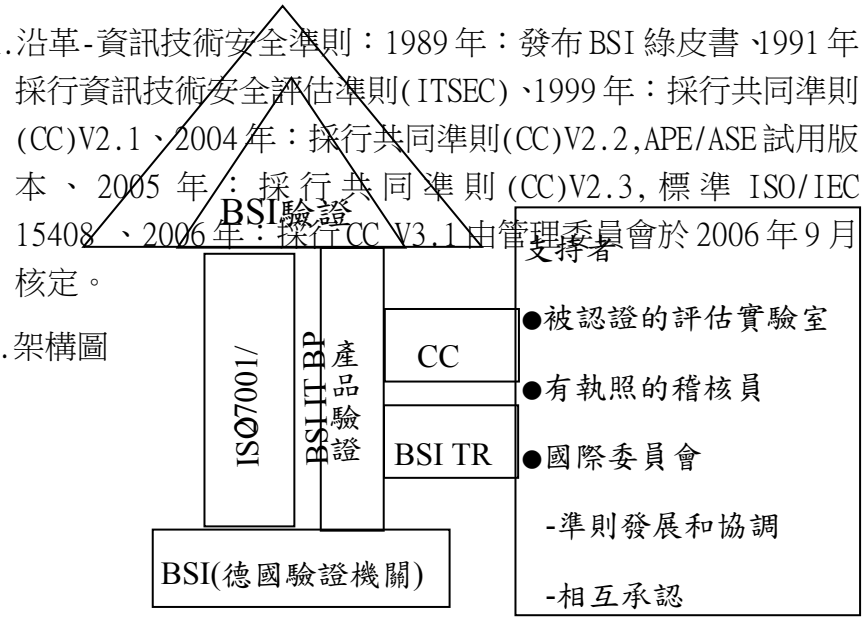
(1)BSI 驗證機關：

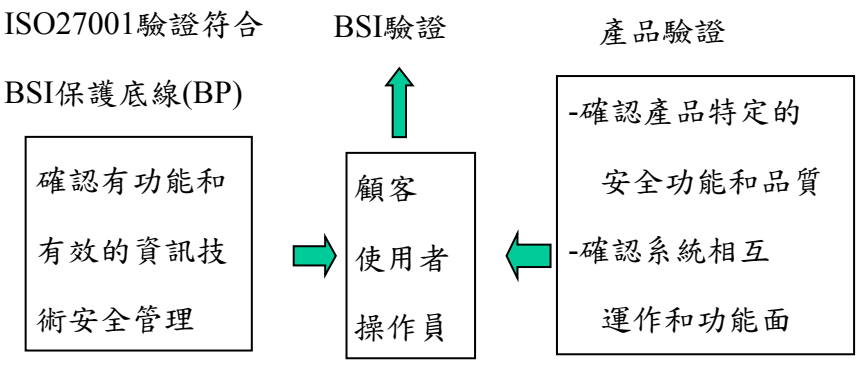
德國驗證機關(The Federal Office for Information Security，簡稱 BSI)由德國國會於 1911 年同意創立。1990 年 12 月 17 日公布的 BSI 組織法第 3 條定義 BSI 的職掌。BSI 組織法第 3 條定義 BSI 的職掌有：研究安全風險、準則的發展、測試和評估資訊技術系統或組件的安全並且頒發驗證證書。相關法規有：BSI 組織法、BSI 驗證法、聯邦內政部法、費用明細表。

(2)德國驗證體系：

A.沿革-資訊技術安全準則：1989 年：發布 BSI 綠皮書、1991 年：採行資訊技術安全評估準則(ITSEC)、1999 年：採行共同準則(CC)V2.1、2004 年：採行共同準則(CC)V2.2,APE/ASE 試用版本、2005 年：採行共同準則(CC)V2.3,標準 ISO/IEC 15408、2006 年：採行CC V3.1 由管理委員會於 2006 年 9 月核定。

B.架構圖

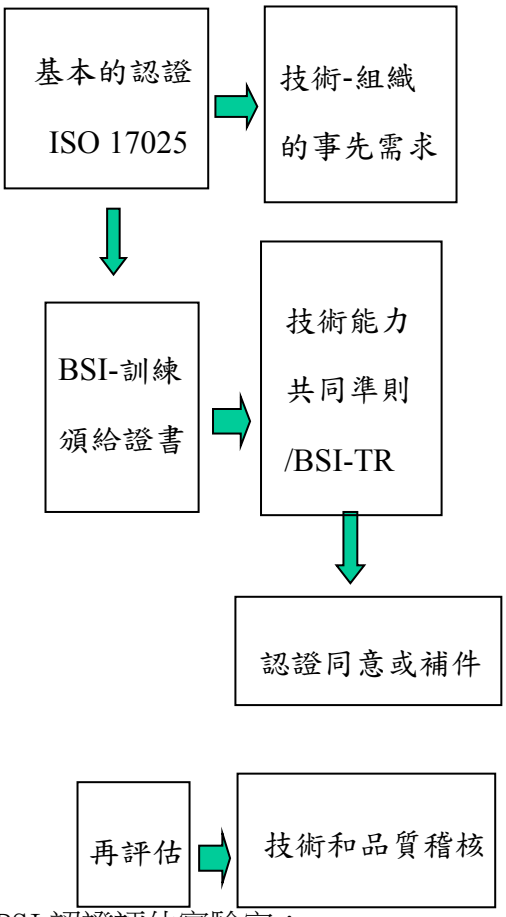




在BSI驗證體系裏，ISO27001與BSI底線保護相符而打算補充產品驗證

C.製造商的動機：有廠外組織進行產品獨立評估。有關產品安全功能的品質改善。設計有被文件證明，評估有被文件證明。商用評估實驗室能力好(為CC認可並取得證照)。由獨立驗證機關監督評估。國家驗證機關保證中立且驗證證書受到國際承認。受承認的驗證證書具有行銷的優勢。

D.認證-德國評估實驗室的資格



E.BSI認證評估實驗室：

採用共同準則和/或ITSEC ITSEF有13家：Atos Origin GmbH。atsec information security GmbH。brightsight by (former TNO-ITSEF BV)。CSC Deutschland Solutions GmbH。datenschutz nord GmbH。DFKI(German Research Institution for Artificial Intelligence)GmbH。media transfer AG。Secunet SwissIT AG。SRC Security Reserch & Consulting GmbH。Tele-Consulting security

｜networking｜training GmbH(TC)、T-System GEI GmbH、TUV Informationstechnik (TUVIT) GmbH。Industrieanlagen-Betriebsgesellschaft GmbH (IABG)(only ITSEC)。

ITSEF 是針對 BSI-TR(BSI 技術指導方針)進行評估。BSI TR 034104(電子通行產品資料獲取，品質檢查和資料傳輸)。BSI TR 03105(電子護照符合性測試)。

F.國際間資訊技術產品驗證證書相互承認：

國際間協議(在 2000 年)/共同準則/評估到 EAL4 等級全世界有 24 國。歐洲協議(在 1998 年)/共同準則+ITSEC/包括所有評估等級/有 12 個歐洲國家。接受證書會員國：芬蘭、希腊、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。核發證書會員國：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。

G.正在驗證中的產品類別：軟體產品有：作業系統(主架構、中等規模)、PC 安全產品(安全保護層、整體保護)、資料通信產品、防火牆、生物量測安全產品(語音辨識)、簽章應用程式。硬體產品有：智慧卡讀卡機、智慧下控制器、自動記錄速度計組件(動作感測器、車輛控制單元、智慧卡)。智慧卡有作業系統和應用程式。

H.CC 已驗證產品的市場發展情形：

BSI-驗證證書(張)

	2000	2001	2002	2003	2004	2005	2006	2007(預測)
CC	0	1	14	15	34	37	88	100
ITSEC	7	6	5	2	3	7	8	4

驗證產品(件)

	智慧卡應用程式	記速器組件	作業系統	簽章應用程式	其他	智慧卡控制器	防火牆
2003	0	1	6	0	3	4	1
2004	0	3	9	7	2	15	1
2005	1	6	8	3	7	19	1
2006	13	5	5	10	17	42	2

I.驗證程序的型式有：與產品開發並行驗證。對完成的產品驗證

保證持續性(再評估、維持)(大部分是硬體/智慧卡，有幾個是軟體，一個保護剖繪)

J.最近驗證案件

NO	公司	驗證產品
1	Infineon	智慧卡控制器(SLE66CL180PE，SLE66CL180PEM，SLE66CL180PES，SLE66CL81PE，SL66CL81PEM，SLE66CL80PE，SLE66CL80PEM，SLE66CL80PES，SLE66CL41PE)
2	Renesas	智慧卡控制器(AE55C1(HD65255C1))
3	SuSE LINUX Products	作業系統(SUSE Linux Enterprise Server V8，with Service Pack 3)
4	Microsoft	交換伺服器，資料庫伺服器(微軟 sql 伺服器的資料庫引擎)，防火牆(ISA 伺服器)，目錄伺服器
5	IBM	作業系統(z/OS)，AIX，PR/SM，目錄伺服器，Tivoli 存取管理器
6	GeNUA	防火牆(GeNUScreen 1.0)
7	NXP Semiconductors Germany	智慧卡控制器(P5CD080V0B，P5CN080V0B 和 P5CC080V0B)
8	Sharp	智慧卡控制器(SM4148)
9	Oce Technologies	印表機控制器(Oce SRA 控制器 V.3 8.02 卷)
10	OPENLiMiT Sign Cubes AG	簽章應用程式軟體(SignCubes 基組件 2.1)
11	Siemes VDO	記速器(數位記數器 DTCO 1381，公開版 1.2a)

K.最近驗證維持案件

公司/檔案	產品名	產品類別
NXP Semiconductors Germany GmbH	NXP 安全智慧卡控制器 P5CC0737V0B 有特定的	智慧卡平

(BSI-DSZ-CC-0410-2007-MA-01)	IC 專屬軟體	台
IBM Deutschland Entwicklung GmbH (BSI-DSZ-CC-0426-2007-MA-01)	NXP PS21G072V0P(JCOP 21 v2.3.1)，NXP PS31G072V0P(JCOP 31 v2.3.1)和 NXP PS21G072V0Q(JCOP 31 v2.3.1)	智慧卡平台
OPENLiMiT Sign Cubes AG (BSI-DSZ-CC-0432-2007-MA-01)	OPENLiMiT Sign Cubes 基本組件 2.1 V2.1.6.2	簽章應用軟體
Infineon Technologies AG (BSI-DSZ-CC-0338-2007-MA-03)	Infineon 智慧卡 IC(安全控制器) SLE66CLX640P/m1522-a15 和 SLE66CLX641P/m1522-a15 二者有 RSA2048 V1.3 和特定的 IC 專屬軟體。	智慧卡控制器

L.重要的驗證計劃有：電子護照[新的電子通行證包括生物測定遵照最近非接觸式的智慧卡(ISO 14443)和 IT-安全技術。評估標的：RFID-控制器(硬體)，內建軟體(作業系統)，MRTD(ICAO)應用程式。生命週期：開發。製造。個人化。運用。資訊技術安全驗證遵照共同準則保護剖繪和按照技術指導手冊的符合性測試。技術指導手冊：BSI-TR 03105「電子護照符合性測試」(TR-ePass)。保護剖繪：機械可讀的旅行文件有「JACO 應用程式」延伸存取控制，V1.1]。國民健保卡[被驗證的重要安全組件有：eGK-電子健康卡供 8 千萬市民更換健保卡(KVK)。HPC-健康專業卡提供給 50 萬以上健康專業人員。SMC-安全模組卡，由一個健康專家所控制的一個協會使用。B4HC-位元 4 健康連結器，提供存取中央遠程通信連繫基礎建設。以上依照已驗證的保護剖繪實施]。數位記速器[按照 EU 指令的驗證需求：依照「一般安全標的」所規定。與共同準則保護剖繪觀念相符合。ITSEC，E3 高等級。共同準則(CC)，EAL4+]。技術組[動作感應器。車輛控制單元。記速計卡(工廠/服務，警察，司機)]。

M.其他最近所開發的保護剖繪有：個人視訊資料保護軟體-閉路電視(CCT)保護剖繪。電子投票保護剖繪(CC V2.3/CC V3.1)。供隨身碟資料儲存器保護剖繪。行動同步服務保護剖繪。安全IC平台保護剖繪(CC V3.1)。

N.在BSI驗證體系裏的重要計劃有：ISO 9001-按照產業規範的驗證，驗證機關的品質管系統已經被驗證。工作場地驗證：在2007年第4季會引入德國驗證體系。開發者的指導手冊文件。對CC V3.1體系解釋文件的更新持續進行中。

(3)展望：經由驗證改善資訊技術安全和資訊技術產品品質。增加驗證證書和保護剖繪的數量使其遍及全世界。成功因素有：把共同準則當成一個國際標準、制定規範和採購政策以促進產品驗證。公部門和私部門對驗證的需求。驗證政策是德國對資訊基礎建設保護的國家計劃之一部份。資訊技術市場領導者完整的產品平台獲得驗證。新的CC版本和計劃執行促使驗證更簡單。驗證機關內部過程發揮最大效用以提升效率。在保護剖繪的開發再努力。

5.西班牙驗證體系現況

(1)2006-2007的事實和形像

主辦2006年第七屆國際共同準則研討會，表達西班牙那時正好被核可承認成為共同準則協議組織的一個授與證書會員國的一份敬意。

通過EN45011稽核，被ENAC認可為一個符合其標準的需求驗證機關，補充其適合EN 45011驗證機關的角色和來自法律架構的責任。這樣特別在數位簽章的國家規範之下會使得工作更適合。

已經發出第二張評估實驗室執照，並且已經接受第三家評估實驗室的申請。三家實驗室為：#CESTI/INTA評估實驗室[安全等級：CLASIFICADO、評估標準和等級：ITSEC，E4 、共同準則/共同評估方法論，EAL4+]。#LGAI Technological Center S.A[安全等級：NO CLASIFICADO、評估標準和等級：共同準則/共同評估方法論，EAL4+]。#Epoche and Esori S.L.U.[(申請中) 、安全等級：CLASIFICADO、評估標準和等級：ITSEC，E3、共同準則/共同評估方法論v3.1，EAL4+]。

已驗過9項產品的安全，目前有14項在評估中。其中有些是用ITSEC/ITSEM標準驗證。

(2)繼續支持 CC/CEM：

西班牙一直都以提供資源來維持 CC 和 ISO 標準持續支持共同準則。西班牙的支持將被維持至 2008 以後。最近三年、西班牙一直贊助 www.commoncriteriaportal.org。這將會被維持下去，但西班牙計劃按照 ISO/IEC 15292-資訊技術-安全技術-保護剖繪登記程序在 ISO/IEC PP 登記。

(3)趨勢和展望：

西班牙在需要資訊技術有被驗證安全的文化上正在急起直追，在數位簽章的領域裏有些初步成果，特別有關國家電子身分證即將增加其受驗的應用程式和產品的需求。

CCN 正在採取措施以改善發照給實驗室效率和規劃其本身能力以應付未來所增加的需求。

6、 心得與建議

(一)心得

1. 推展資訊技術安全產品驗證業務是國際趨勢。加入 CCRA 對我國資安產品進軍國際市場扮演關鍵角色。然鑑於我國在國際舞台上非為聯合國會員之一，每每在國際組織社會裏，因為國籍身分遭受排拒。此種外交困境，常須借重外交單位來協助。

2. 各國驗證體系都遵循共同準則也都大致相同。然各國在資安產品驗證業務上的推動卻略有差異，各具特色，如下表所述：

國家	共同點	特　色
瑞典	驗證機關為 CSEC。有 2 家評估實驗室。驗證產品有：4 件。	建立 21 種驗證體制文件。與政府其他單位互動機制健全。驗證體系規劃完善。
韓國	驗證機關為 ITSCC。有 3 家評估實驗室。驗證產品有：26 件	建立評估員證照制度。每年開發 4 個保護剖繪供產品引用。要求政府部門必採購已經驗證過的 IT 安全產品。實施國內驗證計劃以處理產品長期排隊等候評估的問題。建立驗證評估管理系統提升驗證作業效率。
英國	驗證機關為 CESG。有 4 家評估實驗室。驗證	CB 提供英國驗證體系的基礎建設。已驗證 EAL1-EAL5 的產品總共有 68 件。

	產品類型有：通信、安全消除資料、資料庫、防火牆、網路系統作業系統、PC 存取制、保護剖繪和軍用系統的雜項產品。	評估和驗證程序，著重於技術監督。脆弱性分析的重點著重於識別潛在的脆弱性。
德國	驗證機關為 BI。有 13 家評估實驗室。驗證產品類型有：智慧卡應用程式、記速器組件、作業系統、簽章應用程式、智慧卡控制器、防火牆等。	驗證產品以智慧卡應用程式和控制器為大宗。已驗證產品有 250 件以上經驗豐富。動要的驗證計劃有：電子護照、國民健保卡、數位記速器、技術組件。最近開發 4 種保護剖繪。將把工作場地驗證引入驗證體系。將編撰開發者的指導手冊文冊。把共同準則當成一個國際標準。制定規範和採購政策以促進產品驗證。
西班牙	驗證機關為 CCN。有 3 家評估實驗室。驗證產品有：9 件。	以提供資源來維持 CC 和 ISO 標準持續支持共同準則。在數位簽章的領域裏有些初步成果。即將增加國家電子身分證受驗的應用程式和產品的需求。

(二)建議：

1.在申請加入 CCRA 方面：

經由外交途徑，向各國在共同準則管理委員(Common Criteria Management Board，簡稱 CCMB)代表的上級實權單位主管進行遊說。促使他們的代表能在審查我國入會問題上支持我國，並能替我們說明台灣與中國是兩不同政治實體，支持我國能以加入世貿易組織(WTO)成功的模式加入，即以台澎金馬關稅獨立領域的身分加入。

2.在推動我國資訊技術安全產品驗證體系方面：

(1)效法各國政府在採購政策上的支持作法。即要求政府單位應優先採購經驗證機關驗證合格的資安產品。

(2)政府可採經費補助獎勵措施，對評估費用予適當補助，俾提高廠商產品送驗之意願。

(3)在初階段的驗證業務推動中，可先選定一至二件具我國資訊技術產品特色為主要業務，發展出其獨特的評估驗證經驗，如智慧卡

產品。

(4)積極開發保護剖繪，供開發者憑以開發產品。

(5)建立評估員和驗證員證照制度，積極儲備人才，維護評估及驗證的國家水準。

＜附件＞研討會議程

研討會　　第一天議程

09:30-10:15	**Opening Session**	Speaker	
	Opening Plenary	General Chair Maurizio Decina, President of Fondazione Ugo Bordoni	
	Welcome address	Paolo Gentiloni, Italian Minister of Communications* Marcello Fiori, OCSI-ISCOM Director, Head of the General Secretariat of the Italian Ministry of Communications	
10:15-10:30	**Keynote speech**	G. Caggiano, ENISA Management Board Member	
10:30-10:45	**Keynote speech**	C. Manganelli, Member of the Management Board of the Italian Centre for IT in the Government (CNIPA)	
10:45-11:00	**Keynote speech**	C. Comella, Head of the Technological Department of the Italian Privacy Authority (Garante per la protezione dei dati personali)	
11:00-11:30	*Coffee break*		
11:30-12:30	**Panel session**	chaired by Franco Guida, Fondazione Ugo Bordoni, OCSI.	
12:30-13:00	**Report from the CC Management Committee**	MC chair Gen. L. Palagiano, Presidency of the Council of Ministers, National Security Authority (ANS), Central Security Office	
13:00-14:00	*Lunch*		
	Aula Minor	*Aula 11*	*Aula 7*
14:00-14.30	**Assurance continuity: what and how** Rachamadugu Nithya, CygnaCom Solutions	**Activity report covering the work of the CCDB, the CCMB and the vendor's group** David Martin CCDB	**Evaluating Modern Address Space Integrity protections within the CC** Fox Ashley, CSC

		chair	Australia
14:30-15:00	**Assurance continuity/assurance maintenance (AC/AM): experiences, strategies, further improvements** Gauvreau Mark, EWA-Canada	**Update on Swedish Scheme** Stroman Dug	**Operating System Evaluations - What security functionality is expected** Helmut Kurth, Atsec
15:00-15:30	**Composite evaluation for smart card and similar devices** Furgel Igor, T-Systems	**Update on US scheme** Audrey Dale **Update on UK scheme** Nigel Jones	**Assurance Considerations for a Highly robust TOE** Nguyen Thuy D., Naval Postgraduate School, Department of Computer Science
15:30-16:00	**Compositional Security Evaluation: the MILS approach** Rushby John, SRI International	**Update on German scheme** Rurhmann Irmela, BSI	**XML-based Security Targets for tool-supported evaluations** Ochel David, Atsec
16:00-16:30	*Coffee Break*		
16:30-17:00	**A common criteria authoring environment supporting composition** DeLong Rance, SRI International	**Update on Korean scheme** Cho Sung	**Economical Use of Formal Methods** Yi Mao, Atsec
17:00-17:30	**Challenging the concept of one evaluation assurance level per evaluation** Tekampe Nils, Tuvit	**Update on Spanish scheme** Luis Jimenez	**An empirical study on effort-ratio among EALs and product types for estimation of evaluation duration**

			and cost Gang Soo Lee, Han Nam University
17:30-18:00	**Common Criteria: Optional Security requireme nts and functions** Arnold Jr James L, SAIC Accredited Testing & Evaluation Laboratories	**Issues for CC v4.0** Straw Julian, BT	**Software Security Reviews Static and dynamic analysis** Ahlbin Magnus, Combitech AB

研討會　　第二天議程

	Aula Minor	*Aula 11*	*Aula 7*
09:00-09:30	**Graduated CC protection profiles for cryptographic modules** Gereon Killian, BSI	**Vendor Strategies for Schedule Reduction through improved Evidence Delivery Processes** Medefesser Jane, Sun Microsystems	**POS/ATM Protection Profile for a Common European Banking Industry Approval Scheme** Amendola Sandro, SRC
09:30-10:00	**Common Criteria vulnerability analysis of cryptographic security mechanism** Trinh Quang M., SAIC Accredited Testing & Evaluation Laboratories	**Formal Methods in practice: when the standard meets the experience** Gimenez Eduardo, Trusted Labs S.A.S	**Protection Profile of telecommunication device for telebiometrics system mechanism (TSM)** Shin Yong Nyuo, Korea Information Security Agency
10:00-10:30	**Formal security policy modelling and covered channel analysis: an experience with**	**How to Eat a Mammoth** Krummeck Gerald, Atsec	**Apply CC to the biometric system** Chih-Cheng Liu, Telecom Technology Center

	evaluation methodologies Katikaneni Swapna, CygnaCom Solutions		
10:30-11:00	*Coffee Break*		
11:00-11:30	**High efficient evaluations: vertical assurance packages, certified sites and new software development tools and techniques requirements** Josè Emilio Rico, CCN	**Effective smartcard evaluations process: CEST-LETI and Gemalto experience** Martine Chiocca, Gemalto	**Application of the U(sim) card as secure device for eletronic signature** Fuertes Pedro, Consultant
11:30-12:00	**Technical guidance for CC evaluation** Killmann Wolfgang, T-Systems	**Onom@topic+, Methodology for High Level certification of the ICAO e-passport** Chetali Boutheina, Gemalto	**Synergies of the Common Criteria with other standard** Gauvreau Mark, EWA-Canada
12:00-12:30	**Has the Common Criteria Delivered?** Apted Anthony J., SAIC Accredited Testing & Evaluation Laboratories	**Secure Software Download a Maintenance process?** Hanke Lars, T-Systems	**Design and Development of a Knowledge-based tool based on multiples international standards** Ramirez Caceres Guillermo Horacio, Graduate School of Engineering, Soka University
12:30-13:00	**How vendor involvement can improve Common**	**An innovative approach to manage evaluation evidences**	**Secure System Design** Pattinson Fiona,

	Criteria Higaki H. Wesley, Symantec Corporation	**by a software tool** Di Iorio Paolo, ST Incard SRL	Atsec
13:00-14:30	*Lunch*		
14.30-15.00	**Updating information assurance in the 21st century** David Martin, CESG UK	**Migrating Developer Evidence from CC v2 to CC v 3** Serowy Miriam, BSI	**Simple use of UML for assisting in the creation of CC evaluation inputs** Sheh Karen, CSC Australia
15:00-15:30	**Life-cycle evaluation methodology** Naaman Nir, Metatron Ltd.	**CCv3.1 Vulnerability Assessment: What is new?** Furgel Igor,T-Systems	**A technical approach to an integration model of IT security evaluation methodologies** Tapiador Marino, CCN
15:30-16:00	**Evaluation of an e-voting device based on CC PP** Vogt Roland, DFKI	**CC v3.1 release 2, what has changed?** Banon Miguel, Epoche and Espri	**Omissions and errors in the CC? - Who got it right?** Cater Denise, IconSecurity Ltd
16:00-16:30	*Coffee Break*		
16:30-17:00	**The 7th year Itch: time to commit or time to move on?** Shaun Lee, Oracle	**Should & How RFID System be evaluated against CC v3.1** Yao-Chang Yu, Telecom Technology Center	**Common Criteria in the Real World** Pattinson Fiona, Atsec
17:00-17:30	**Guideline for Developer Documentation** Krause Christian, BSI	**Practical experience of CC3.1 applied on smartcard hardware** Slegers Wouter, Brightsight	**TSP formal modelling and verification - case of e-passport IC** Ichihara Naohisa, NTTDATA Corporation
19:30-23:00	*Gala Dinner*		

研討會　　第三天議程

	Aula Minor	*Aula 11*	*Aula 7*
09:00-09:30	**Developer Documentation - A Who to guide** Connor Erin, EWA-Canada	**CC V3 application to smart Cards and similar devices** Forge Francoise, Gemalto	**A Study on the Cryptographic Module validation in the cc evaluation from vendor's point of view** Tagashira Nobuhiro, Canon Inc. PF Technology Development
09:30-10:00	**BSI activities in developing PPs an the BSI-PP/ST- guide** Grefrath Frank, BSI	**Smart security devices: new technologies evaluation challenge** Forge Francoise, Gemalto	**Semiformal framework for ICT Security development** Bialas Andrzej, INSI
10:00-10:30	**Security Target Level of Detail** Arnold Jr James L., SAIC Accredited Testing & Evaluation Laboratories	**Evaluation of basic technology for business solutions as example for the evaluation of complex systems** Cordes Christoph, Atos Origin GmbH	**Towards a smooth migration to CCV3: update of protection profiles, first experience on Security IC Protection Profile** Gibert Catherine, Eurosmart PSSWG
10.30-11.00	**Threats, Policies, and Assumptions in the CC** Diaz Terrie L., SAIC Accredited Testing & Evaluation Laboratories	**Current practice in covering some aspects of cryptographic mechanisms in the CC context** Menicocci Renato,	**IEEE P2600: Breaking new ground in protection profile structure** Smithson Brian, Ricoh Americas Corporation

		FUB	
11:00-11:30	*Coffee Break*		
11:30-12:00	Closing Panel "Roundup of events at the 8thICCC"		
12:00-12:30	Closing Plenary		
12:30-13:45	Announcement of 9th ICCC from the Korean		
13:45-14:45	*Lunch*		