植基於 PKI 的立法院資訊安全架構及其實作

陳熙揚 王一琳 高振源 陳幸俐 吳天清
立法院顧問 國立彰化師範大學 立法院資訊處 立法院資訊處 立法院資訊處
兼資訊處處長 商業教育系博士班研究生 科長 管理師 分析師
chensy@ly.gov.tw celily@cc.ncue.edu.tw ly20383@ly.gov.tw ly20646@ly.gov.tw ly30032@ly.gov.tw

中文摘要

建立安全、高可靠度的立法院資訊系統，是立法院資訊建設的首要目標。本文旨在介紹基於 PKI 架構下，結合流程面、管理面與監控面所建立之立法院資訊系統整體架構及其實作。公開金鑰基礎建設（PKI）具備其它非單一技術所能提供之彈性、高度安全的驗證方法、資料加密和數位簽章等功能，實為目前最安全之基礎架構。立法院於 2001 年建立以 PKI 為基礎之立法院憑證管理中心，建構安全的資訊應用環境並結合資訊安全管理系統（ISMS）與自建之資通安全管理中心（SOC），以滿足網際網路環境中重要資訊安全需求，提供完整、容易使用的安全防護機制，故依此基礎建立的立法院資訊系統，深具安全與高可靠度，已達成優質立法院資訊建設目標。

關鍵詞：公開金鑰基礎建設、憑證實務作業基準、資訊安全管理系統、資通安全管理中心、憑證管理中心

英文摘要

The goal of the Congress Information Construction is to establish safe and high reliability systems. This article is for the purpose to introduce the PKI based establishment of Congress MIS Infrastructure in conjunction with the aspects of process, management and monitoring.

PKI is the currently most safe network construction to satisfy the important information security requirements in the Internet environment and provides safety protection mechanism which is complete and easy to use. Certificate Authorization Center based on the PKI was set up since 2001.Through this fundamental establishment of Congress Information System, the goal to possess the safe, high reliability, and good quality information has been achieved.

KEY WORDS：PKI、CPS、ISMS、SOC、CA

1. 前言

近年來立法院積極推動資訊建設，已陸續完成全院寬頻網路、數位電話、大型主機系統等基礎建設及議場多媒體議事公報等六十餘資訊應用系統之規劃、建置與導入，業已建立安全之電子化、科技化資訊環境，達成數位化立法院目標。

有鑑於網路便利化所造成日益增多的資訊安全威脅，資訊安全儼然成為資訊應用上最重要的思考議題，以立法院(以下簡稱本院)環境為例，2008 年 8 月份受中度風險攻擊達 420 萬餘次，高度風險攻擊達 308 萬餘次。故本院資訊系統建設特別重視資訊安全及其架構整合，使用高等級產品、規劃縱深防禦（多層防火牆、企業防護策略、IPS），其中，電腦防毒系統架構共分三層，第一層：NVWE（網路防毒牆）過濾未符合安全性策略的用戶端並阻擋網路病毒或蠕蟲威脅、第二層：由 IWSA（網頁過濾器）提供過濾惡意網頁與釣魚網站威脅

及 IMSS（郵件掃毒伺服器）過濾信件病毒、第三層：OfficeScan（用戶端病毒防護）執行最新病毒碼派送及病毒爆發防範部署。此外，並同時整合相關資訊安全管理機制，在管理面導入 ISO 27001 資訊安全管理系統（Information Security Management System，ISMS），在基礎面建構公開金鑰基礎建設（Public Key Infrastructure，PKI）應用環境，監控面建置資通安全管理中心(Security Operation Center，SOC)，同時秉持服務導向的理念全面導入 ISO 20000 資訊系統服務管理，以建置安全無虞之立法院資訊應用環境。

本院於 2001 年建立「公開金鑰基礎建設」(PKI)，首開國內先河。嗣後持續對全院人員發放 IC 卡識別證（已核發 10,037 張憑證），並結合個人數位憑證，進行人員識別及系統認證，同時訂定「立法院憑證管理中心憑證實務作業基準」（Certification Practice Statement，CPS），俾使本院憑證用戶均能依據該標準進行數位憑證之申請、審核、簽發、公告、廢止與應用等作業，本院所發放之憑證依電子簽章法第 11 條第 1 項之規定，已於 2008 年 9 月經主管機關審查通過核定備查，立法院憑證管理中心相關作業程序已具備法定效力。

公開金鑰基礎建設（PKI）具備其它非單一技術所能提供之彈性、高度安全的驗證方法、資料加密和數位簽章等功能[4]，實為目前最安全之網路安全架構，可以滿足網路環境中重要資訊安全需求，提供完整、容易使用的安全防護機制，故依此基礎建立的立法院資訊系統（含行動資訊系統），深具安全與高可靠度，已達成優質立法院資訊建設目標。

（PKI）架構

PKI 是一組嚴格定義的標準架構（圖 1），用以掌控憑證生命週期的每一狀態。國際 X.509 公開金鑰基礎建設 PKIX 工作小組定義 PKI 為：「在公開金鑰密碼學基礎下，用以產生、管理、儲存、分配及撤銷憑證之一組硬體、軟體、人及過程」。

PKI 包含了一支公開金鑰與一支私密金鑰；前者公諸於大眾，而後者由使用者持有保管[1]。這一對金鑰是具相對應關係的數位密碼，其中一把對訊息進行加密後進行訊息傳輸，使傳輸過程中訊息本身無法輕易由他人解讀；另一支金鑰則作為解密用途，以獲得原始訊息內容。

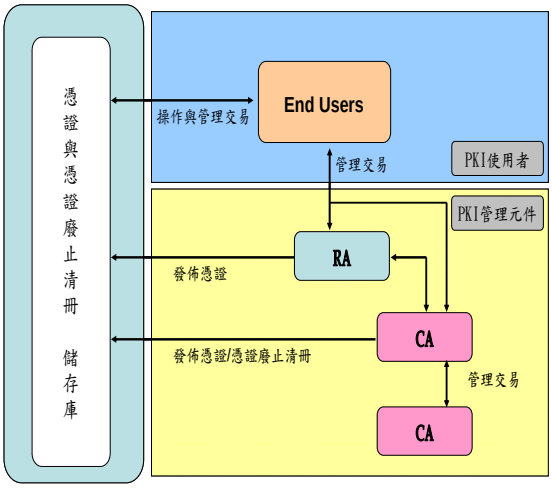

圖 1：PKI 架構模型

X.509 定義公開金鑰憑證應包含下列資訊：

2. 立法院之公開金鑰基礎建設

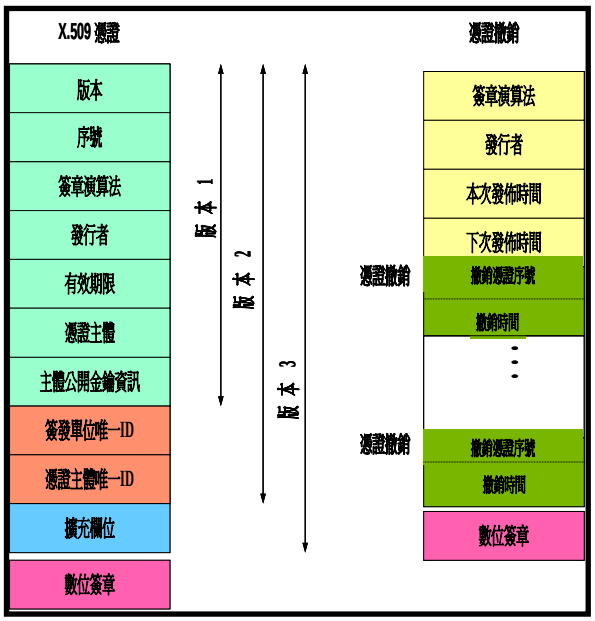

圖 2、X.509 憑證格式

（1）公開金鑰

（2）連結公開金鑰擁有者的資訊

（3）憑證管理中心(CA)的資訊

（4）憑證管理中心(CA)的簽章

其格式請參考圖 2

憑證主要是公開金鑰的儲存體，但它較公開金鑰擁有更多資訊，因此較容易應用於資訊系統中。當憑證管理中心發佈憑證時，由憑證管理中心來簽發此憑證，以確認此憑證的有效性，所有公開金鑰憑證擁有下列資訊[3]：

（1）版本：用以識別憑證所採用 X.509 標準的版本。本院憑證採用 X.509 v3。

（2）序號：當產生一個憑證時，會指定一個序號給此憑證，用以與其他憑證區別。此序號尚有許多用途，例如當某一憑證被廢止，其序號就會被放在憑證廢止清單(CRL)中。

（3）簽章演算法：用來識別 CA 簽發憑證所用的演算法。

（4）發行者：以 CA 的 X.500 名稱用來簽發憑證。當使用者使用此憑證時，意謂信任簽發此憑證之憑證管理中心。

（5）有效期限：有效期限的定義是藉由開始日期及結束日期來訂定，在這段期間內憑證使用者可以信賴此公開金鑰憑證。本院憑證管理中心的憑證有效期限可以是幾秒鐘到一個世紀。

（6）憑證主體：此為可識別的姓名，經由公開金鑰與憑證結合。藉由 X.500 標準所定義的姓名來達到在網路上的獨一無二性。

（7）主體公鑰資訊：包含公開金鑰、演算法及任何相關金鑰的參數。

X.509 的 CRL 經由 CA 簽章加蓋時戳定義廢止憑證。通常 CA 在一定期間公佈 CRL 到儲存庫（Light-weighted Directory Access Protocol，LDAP）及 OCSP 伺服器中。當使用者發現私鑰有洩漏的可能時必須儘快廢止。憑證一經 CA 廢止後會立即公告到本院所指定的 LDAP 與 OCSP 伺服器中。信賴憑證者（LYCA 之信賴憑證者即為信任 LYCA 憑證及 LYCA 所簽發之 CRL，並憑藉此信任基礎進行相關憑證應用者）即可透過應用系統介面取得 CRL 來檢查來源端憑證的有效性。

本院所建構之 PKI 具備下列的功能：

（1）註冊(Registration)：當本院使用者期望擁有憑證時，出示本身資料給 RA 以請求憑證的過程。使用者必須提供姓名、email、及其他個人身分證明，且依循本院

的 CPS 規範（見 ca.ly.gov.tw）。在核發憑證前 RAO 根據 CPS 的規範來檢驗使用者資料是否正確。

（2）憑證發放：藉由 CA 正式發行一個憑證，其中包含使用者公鑰，並將憑證放置於本院 IC 識別證內。

（3）金鑰產生(Key generation)：本院使用者在傳送自身公鑰給 CA 認證之前，會在註冊端產生兩組金鑰對(簽章金鑰對與加密金鑰對)。

（4）金鑰更新：所有的金鑰對，及它們相關的憑證，會在一定的時間更新。

（5）金鑰回復(Key recovery)：本院建構雙憑證環境，每位使用者擁有簽章金鑰對與加密金鑰對，系統在簽發憑證的同時將加密金鑰對存到安全的硬體加密模組(HSM)中(簽章金鑰對絕不允許備份)。亦即當使用者遺失 IC 卡識別證時，原先之加密金鑰對可以回復，允許先前加密的資料可以解密。CA 主要的任務是確保加密金鑰可由使用者回復，但不能由未授權的其他人執行。

（6）廢止(Revocation)：憑證經過 CA 發放之後，直到有效期限期滿前會持續有效。但有下列情況則必須廢止憑證的有效性：

- 使用者改變名字。
- 擁有憑證之使用者離職。
- 金鑰可能發生洩漏。

茲將本院 PKI 架構概述如下：

2.1 立法院憑證管理中心（LYCA）

本院憑證管理中心採用全球 PKI 領導廠商 Baltimore 之 UniCERT 憑證系統，UniCERT 是一個公開金鑰憑證系統（圖 3），提供註冊代理人及遠端使用者線上憑證申請服務。本院即透過 LYCA 之操作員(CA Operator，CAO)來建構本院的 PKI 架構以及定義所有使用者註冊政策。這些政策，和憑證系統中所有運作都依循本院所規範之 CPS。

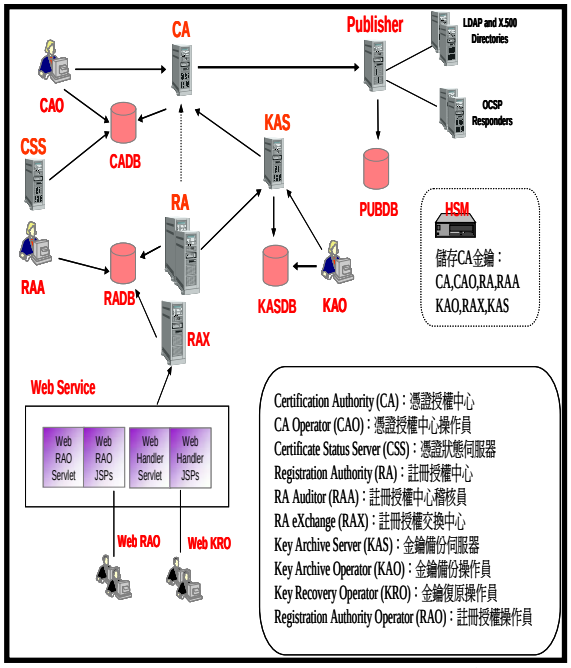

圖 3、立法院憑證管理中心 UniCERT 系統架構圖

本院憑證管理中心採用兩種政策型態：

（1）運作的政策：此政策主導所有 PKI 的政策，同時也定義每天 CA 執行的合法細節，例如使用者如何挽救他們的憑證及 CRL 產生的頻率。在建構 PKI 架構時即依據本院實際需求將相關

參數規劃到不同的各個元件中，目前本院即依據此定義的操作政策運作中。

（2）客戶註冊政策：本院為不同的使用者定義不同的憑證註冊政策，使用者必須依據不同的憑証政策提供必要的資訊給註冊管理員，例如，email 位址或是組織等，且這些資訊會進入使用者公開金鑰憑證中。

本院憑證管理中心包含下列模組：

（1）憑證授權中心（Certification Authority，CA）

CA 在本院的 PKI 架構中是一個最高階層的元件。它主要服務項目是簽發及公佈數位憑證，此數位憑證提供安全電子訊息交換的工具。本院憑證管理中心後端搭配符合 FIPS 140-1 Level 4 的硬體加密模組來保護憑證管理中心所有元件的金鑰，並透過安全機制將金鑰以 m of n 的方式由本院秘書長、資訊處、會計處、總務處、人事處等一級單位主管各自分持。

（2）憑證授權中心操作員（CA Operator，CAO）

CAO 是與 CA 之間的管理介面。整個 PKI 架構都是透過 CAO 關聯到 CA 來控制所有元件。在啟動 CA 之後不需要直接接觸 CA 來開啟其服務，所有的動作都透過 CAO，經由 CAO 的定義及設定可以用到 PKI 系統中其他元件。

（3）註冊授權中心（Registration Authority，RA）

RA 主要任務是轉換與 CA 之間的訊息，接受透過 RAO 的臨櫃憑證請求，然後利用 PKIX 透過 TCP/IP 將請求送給 CA，並利用 PKIX 通訊協定在 RA 及 CA 間通訊確保傳送資料之完整性。一旦 CA 為使用者產生憑證後就將它送回給 RA，再適當的經由 Gateway 傳給請求的 RAO。RA 也將所有事件保留到它的資料庫中，以方便 RAO 存取的需求。

（4）註冊授權操作員（Registration Authority Operator，RAO）

RAO 是憑證請求接受過程中的介面。請求可經由 email、www 或臨櫃方式向本院 RA 申請(本院僅接受臨櫃方式申請憑證)。RAO 處理請求並完成任何認為必要的步驟來確保請求者提出的訊息及憑據是有效的。一旦完整的建立有效性，RAO 就可以接受這個請求，並將其紀錄到 RA 資料庫中，然後 RA 會傳送這有效的請求到 CA 去核發憑證。在申請的同時，RAO 會為使用者在本院 IC 識別證中產生金鑰。

（5）金鑰備份伺服器（Key Archive Server，KAS）

KAS 主要的任務是將使用者的加密金鑰備份至安全的儲存設備中；也就是若使用者加密金鑰對遺失或損壞時可以加以回復。

（6）WebRAO

WebRAO 提供一個以 Web 為主的 RAO 應用程式。就如同 RAO，WebRAO 允許註冊授權操作員處理使用者臨櫃及遠端的憑證申請。

國內於 1998 年建置第一個憑證管理中心 GCA，從 2001 年至 2004 年陸續建置 eCA、TaiCA、Hitrust 等商業應用憑證中心，因此 PKI 互運機制（interoperability）已成為重要議題。互運機制的方式有階層式（hierarchy）與橋接式（bridge）憑證授權（certificate authority）兩種，我國互運機制則採用後者[2][5]，本院憑證管理中心亦遵循此機制與其他憑證管理中心互運。

2.2 線上憑證狀態協定（Online Certificate Status Protocol，OCSP）

OCSP 可以取代或是補充 CRL 的檢查。主要是解決 CRL 在發布上的限制。OCSP 採用請求-回應的訊息語法，主要提供應用程式驗證使用者所擁有憑證的憑證註銷狀態資訊。OCSP 伺服器較 CRL 提供更多的狀態資訊。本院 OCSP 伺服器具有下列優點：

（1）OCSP 的請求-回應訊息可以取代傳統 CRL，給有需要的使用者，同時解決 CRL 發布上的限制。

（2）OCSP 請求-回應訊息支援 client-server 模式，允許 OCSP 支援更大量的使用者。主要是因為 OCSP 所回應的訊息較完整的 CRL 為短。

（3）OCSP 訊息透過 TCP/IP 網路，利用應用層協定 HTTP 來傳遞，如此可以通過大多數的網路防火牆。

（4）OCSP 訊息可以回應單一被請求驗證憑證註銷狀態的資訊，不像 CRL 必須被完整的公告，透過 CRL 模式驗證註銷狀態時，請求者詢問特定憑證的狀態資訊會取得完整 CRL，而不是簡單的得到"bad"憑證清單。

2.3 時戳伺服器（Time Stamp Server，TSS）

本院 TSS 主要用於建立電子文件中關聯到日期及時間的加密。時戳可以用來驗證一特定時間點所發生的事件確實存在。本院 TSS 可以對需要在時間上用時戳來信任訊息被發行或是憑證有效性的功能提供不可否認服務。

TSS 可以看作是一個被信任的第三者所提供的時戳服務。TSS 功能以可信任的第三者來驗證憑證註銷前的數位簽章確實用在訊息上，以再次確認註銷的公開金鑰憑證在註銷前所建立的簽章。

TSS 是非常重要的，電子文件上如無時戳，則任何人不可信任簽署的文件，也無法解決簽章者偽造簽章的狀況。時戳明顯提高對電子文件信任的等級，同時確保簽章金鑰在註銷前所簽署的文件仍是可被信賴的。本院 PKI 系統與應用完整架構如圖 4 所示

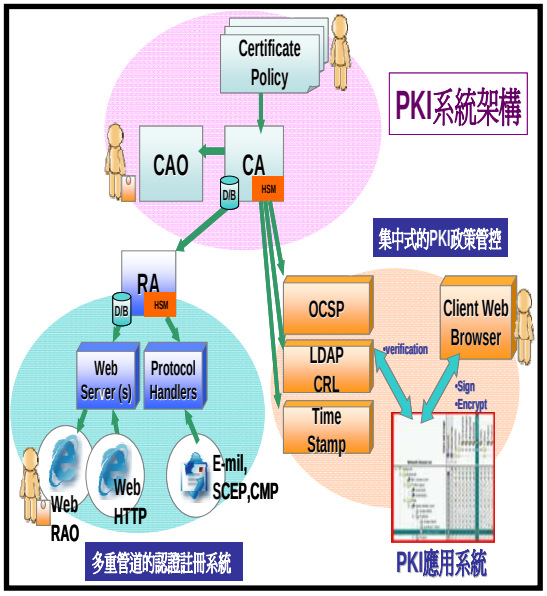

圖 4、PKI 系統與應用架構圖

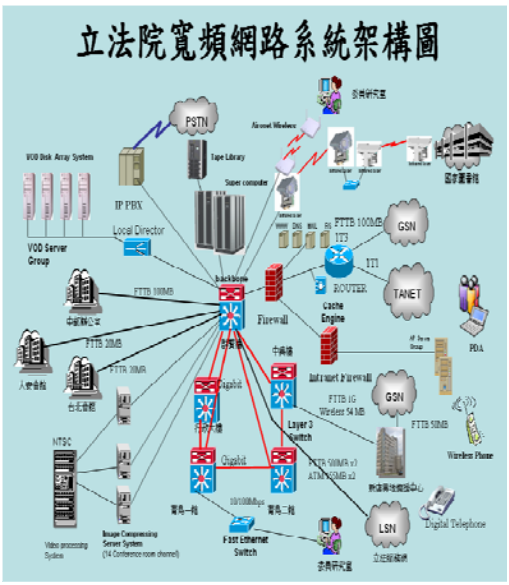

圖 6、立法院寬頻網路系統

3. 立法院 PKI 之實作

立法院資訊系統整體架構（圖 5），旨在符合相關法規、技術及標準之規範，與遵循政策及業務需求下，提供兼具整合、服務、創新、安全的資訊服務。近年來本院已建置優質立法院寬頻網路系統（圖 6），結合 SOC、ITIL 與 ISMS 相關規範實作 PKI，如整合數位簽章、檔案加密、單一簽入權限控管、郵件加密等技術及無線網路認證，完成創新的立法院資訊服務系統、行政支援系統、業務支援系統及決策支援系統。植基於 PKI 的應用系統建置里程碑詳見表 1。

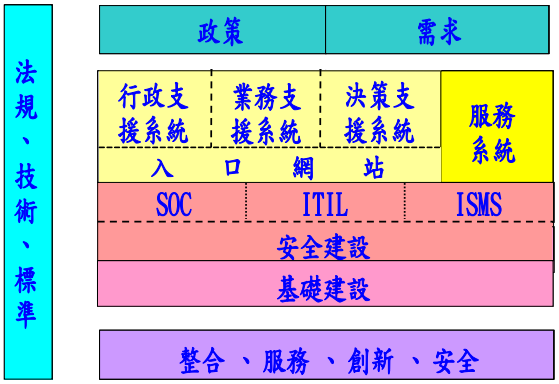

圖 5、立法院資訊系統整體架構

表 1、植基於 PKI 的立法院資訊應用建置里程碑

時程	PKI 相關應用內容
2001 年	建置立法院憑證管理中心
2002 年	建置多媒體隨選視訊系統
2002 年	建置立法服務網
2003 年	建立存取控制與單一簽入機制
2003 年	電子郵件簽章服務
2004 年	建置異地備援中心
2005 年	網路（有線/無線）存取控制和授權整合服務
2006 年	建置立法服務網 Service Desk
2007 年	SOC 正式營運

植基於PKI之應用系統係依圖7之原理運作，茲將各系統架構分述如下：

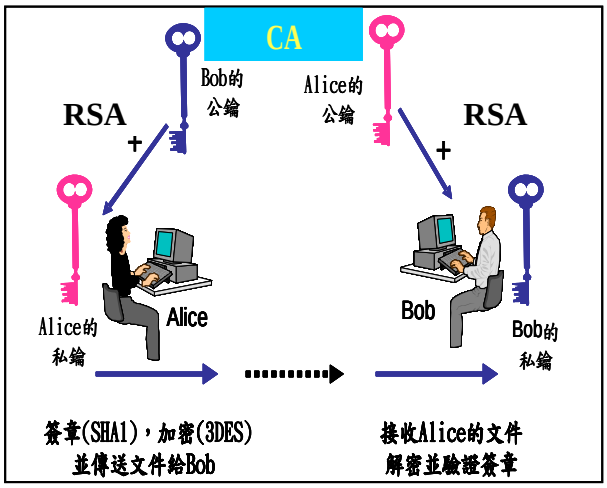

圖 7、PKI 架構(認證採用 RSA 1024bits，簽章採用 SHA1，加密則採用 3DES)

3.1 無線網路系統架構

本院無線網路支援 IEEE802.11b 及 IEEE802.11g 通訊協定，採用 WEP 加密方式(加強型對稱金鑰協定)，應用公開金鑰基礎建設(Public Key Infrastructure，PKI)，結合個人電子數位憑證(Digital certificate)，並搭配本院無線網路單一認證機制，使用者須先向本院資訊處註冊及設定金鑰後才能連接無線網路系統（圖 8)。

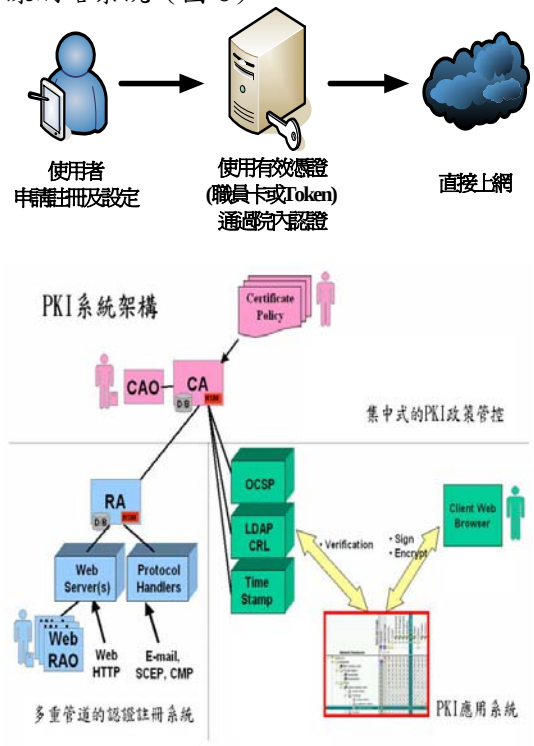

圖 8、本院無線網路申請流程

3.2 資通安全管理中心（Security Operation Center，SOC）系統架構

本院 SOC 以整合本院所有區域之資通安全管理平台，包含院區本部、青島會館一、二、三館、大安會館、台北會館，立法服務網、院外委員辦公室及異地備援中心等為實體範圍，其建置目標見圖 9：

圖 9、SOC 建置目標

為了完成 SOC 的建置，必須具備最佳之 SOC 政策、作業及程序（PPP)，以管理 SOC 所有資產的安全。

SOC 整體解決方案之實體架構（圖 10)，包含五大系統：資安系統、環控系統、主機系統、網路系統及應用系統，此等系統之意外事件都會傳送到本院大型主機系統之服務台。SOC 監控人員將各種不同的意外事件通報給相關承辦人員，承辦人員依據不同的資安事件，進行各種問題的排除。所有安全事件及資訊傳送均透過加密機制保護。

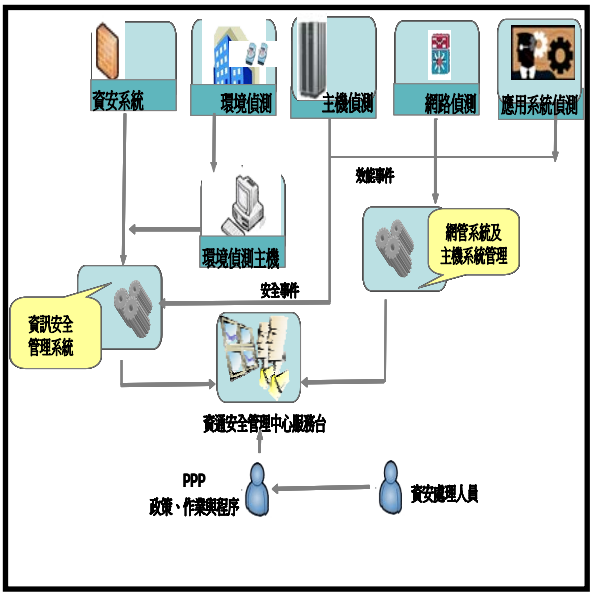

圖 10、SOC 實體架構

本院自實施資安事件通報以來，SOC 已偵測許多過去被忽略的警訊，其中重大資訊安全事件，如：攻擊事件、中毒事件等實施監控而被提早發現，立即處理。本院 2008 年 SOC 監控服務績效見表 2，其通報紀錄請參閱附件 1。本院更進一步配合防毒系統相關人員實際至現場採樣，2007 年共偵測到 710 隻新型病毒，2008 共偵測到 858 隻新型病毒，寄送專業防毒廠商研究中心解毒，有助於整體資安的提升。

表 2、SOC 監控服務績效表

日期 / 項目	2008年1月	2008年2月	2008年3月	2008年4月	2008年5月	2008年6月	2008年7月	2008年8月	2008年9月	2008年10月	2008年11月	2008年12月
主機效能	25	14	29	21	29	25	51	20	11	33	13	31
應用系統	16	1	5	20	6	9	10	5	2	19	7	9
環控系統	12	2	8	5	5	2	0	4	6	4	4	3
網路系統	21	7	8	9	20	10	4	3	2	3	3	14
資訊安全	4	0	1	4	5	2	6	10	14	31	27	35
其他	0	0	0	0	0	0	0	1	0	1	1	0
總計	78	24	51	59	65	48	71	43	35	91	55	92

本院 SOC 與國家資通安全防護管理中心（National Security Operation Center，NSOC）間，建置有效的資安事故訊息互通模式，藉由彼此資源的整合，對國家之整體資通安全環境狀態、網路威脅狀態等有一個全盤性的分析及預警能力，並朝向建立可以互助之聯防體系邁進。

3.3 ISMS（Information Security Management System）

本院 ISMS 驗證範圍包括：立法院網路暨資訊機房基礎建設、大型主機系統、PKI 機制運作、資訊應用系統等，及其所牽涉之相關作業程序、實體作業環境、人員等。本院推動 ISMS 重要里程碑如表 3。

表 3、本院推動 ISMS 重要里程碑

時程	內　　容
2003 年	制訂立法院資訊安全管理要點
2004 年	通過 BS 7799 PART 2:2002 (Specification for Information Security Management Systems 資訊安全管理系統要求)驗證
2006 年	通過 ISO 27001 驗證

在「立法院資訊安全管理要點」規範下，已制定「資訊安全組織作業原則」、「資訊安全風險評鑑與管理作業原則」、「災害復原管理作業原則」等共 26 種資訊安全作業原則及相關作業稽核文件、表單，做為全院 ISMS 遵行依據（圖 11）。

本院 ISMS 在各級長官的推動下榮獲 ISO 27001 暨 CNS 27001 資訊安全管理系統雙驗證，至今每半年接受一次外部複評，並通過 4 次續評，充分落實 ISMS 相關規定，重要具體成效有：

（1）整合人事服務系統資料，落實人事資料之一致性與正確性。本院資源入口網站結合本院 PKI 數位憑證，整合資訊應用系統之單一簽入與權限集中控管機制，落實系統權限控管。

（2）整合電腦維修、應用系統服務、資安監控，落實資訊服務之一致性與管理有效性。本院「單一資訊服務窗口」值班人員執行工作，依據 ISMS 規定量化應用系統安全指標，其工作內容皆紀錄於「服務案件明細」，提供落實各系統契約規定之 SLA 水準之平台，依據各系統契約 SLA 規定產生稽催管制。

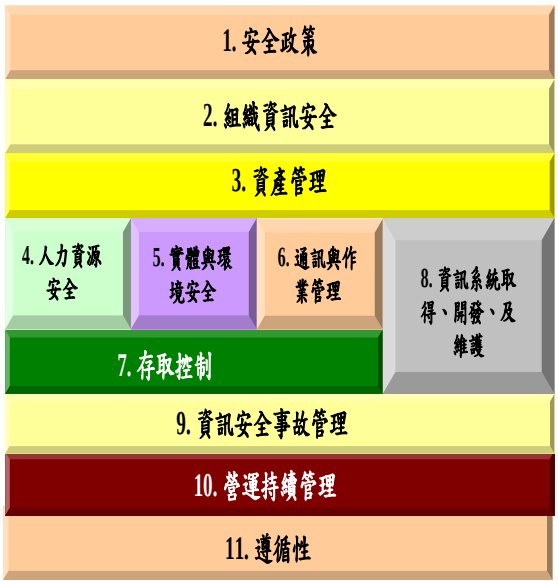

圖 11、ISMS 資訊安全管理系統架構圖

3.4 ITSM（Information Technology Service Management）

本院對於院區使用者之電腦叫修及各種應用系統故障排除叫修，已於 2000 年提供「電腦維修系統」供院內委職員工使用；對於分佈全國的立法委員服務處亦於 2004 年建置「立法服務網」提供電腦叫修及各種應用系統使用故障排除服務。

本院近幾年為整合使用者之問政及業務需求，陸續建置多項資訊基礎建設進而發展各式應用系統。為建立標準化之維修服務程序與統計管理機制，並配合本院資訊安全管理系統基礎建設之推動與有效評估各類量化安全指標之績效，有效達成資訊系統管理之透明化，於 2006 年規劃建置「ITSM 資訊服務管理系統」，提供單一資訊服務窗口，以使服務對象之各項資訊服務申請能在短時間獲得有效解決，並隨時監控各系統服務狀況，提高服務績效。另為提高本院資安監控效益，故結合「資通安全管理中心系統（SOC）」，可將 SOC 即時監控所發現之事件於第一時間通知相關人員處理，以避免資安事件發生或擴大。

本院 ITSM 旨在提供使用者單一資訊服務窗口，重視使用者資訊服務需求及滿意度，主動發現問題、啟動並追蹤服務案件處理流程，以強化各系統維護服務的橫向溝通與稽催功能，其架構如圖 12，服務管理中心架構如圖 13。

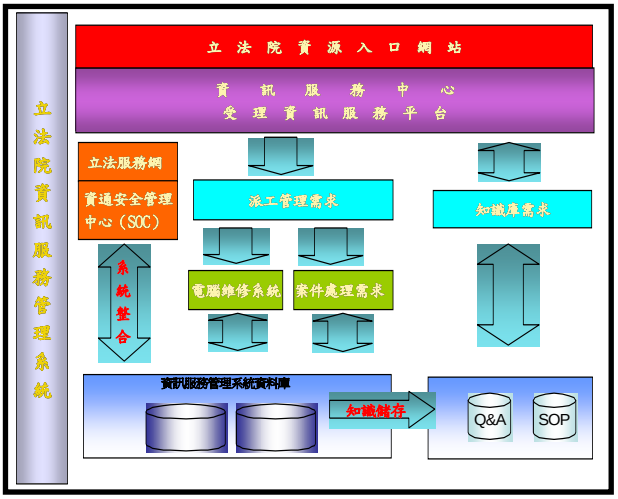

圖 12、ITSM 系統架構圖

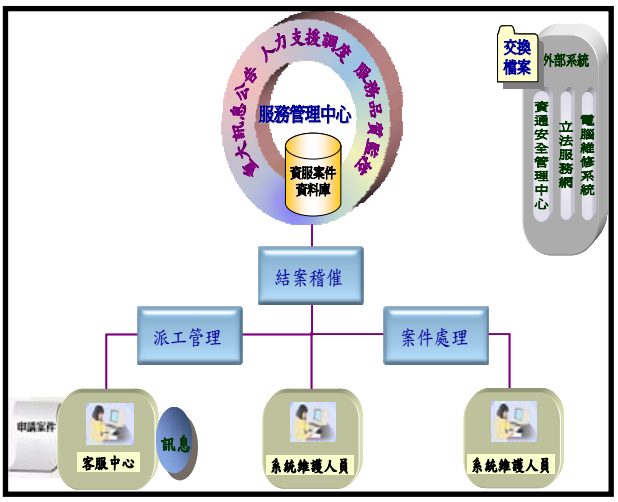

圖 13、服務管理中心架構

本院推動 ITSM 之具體績效有：

（1）利用事件控制和災害復原政策減少處理回應時間。

（2）結合本院「資通安全管理中心系統（SOC）」，提升本院資安監控效益。

（3）提供叫修服務、系統中斷、功能錯誤、資料錯誤、程式異動及資安事件等六類資訊服務案件統計報表，據以衡量本院 ISMS 資安指標。

4.結合 PKI 之立法院資訊應用

4.1、IC 識別證結合悠遊卡應用

立法院 IC 識別證提供悠遊卡功能（圖 14），惟其悠遊卡儲值內容並不含押金，可用金額為零元，同仁需自行加值後才可搭乘相對交通運輸工具。悠遊卡之其他使用相關細則，均依公告之「台北 IC 卡票證發售及使用須知」辦理，並參照交通業者所公告之規定施行。

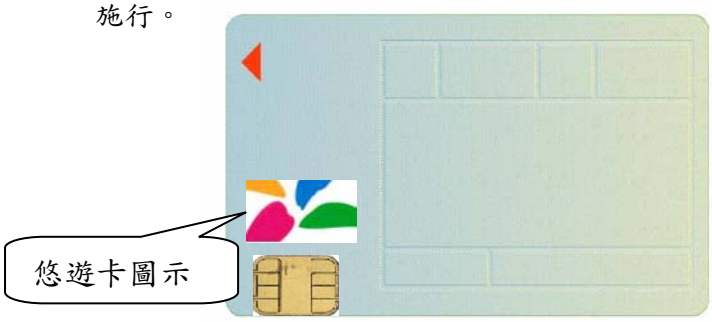

圖 14、IC 識別證結合悠遊卡功能

4.2、IC 識別證員工餐廳等消費應用

本院小額付款方案，由員工消費合作社統籌辦理員工院內消費使用識別證付款之營運，採預付型繳款機制，必須先完成加值動作方可消費，建立儲值、扣款及清算系統，茲述之如下：

（1）員工持識別證到院內合作社進行儲值、退費、結清。

（2）員工持識別證至員工餐廳進行刷卡扣款消費。

（3）透過管理系統，依日期、員工、儲值、消費等不同種類列印報表。

（4）員工已刷卡即視同消費確認，進行扣款，不予退費。

（5）員工如需退費，或查詢交易記錄，可前往儲值地點進行辦理。

（6）系統架構見圖 15，說明如下：

- 儲值地點與餐廳地點及儲值交易資料庫地點透過內部網路連線。
- 系統需具本院識別證儲值、扣款及身份辯識之前台作業功能與設備。
- 後台作業系統需具儲值退費、結清、清算及交易記錄資料庫等功能與設備。
- 系統需具本院識別證儲值卡作廢、停用之機制。
- 交易程序採離線式(off-line)交易，所有交易皆直接針對卡片進行，交易紀錄可以離線批次上傳至後台帳務管理系統。
- 刷卡晶片為非接觸式。

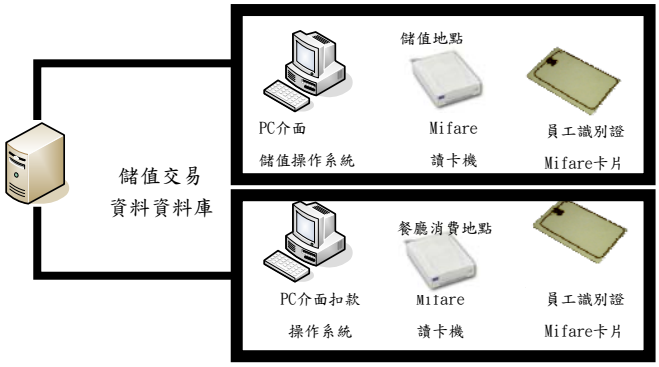

圖 15、IC 識別證消費系統架構圖

4.3、教育訓練刷卡簽到(退)管理系統

系統整合本院「教育訓練行政系統」，解決以往教育訓練學員報到時無法即時獲得應（實）到人數與出席率等相關資訊，同時增益本院 IC 識別證加值應用，利用 Mifare 機制，作為設計本案整體架構依據（圖 16），將教育訓練簽到自動化，以減少紙張利用及資料登錄人力，提高行政效率。

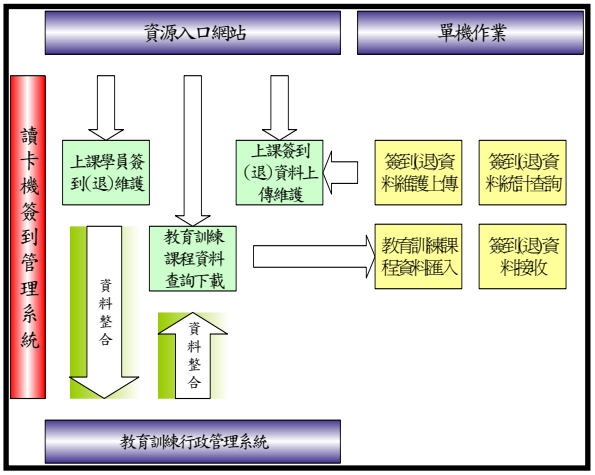

圖 16、教育訓練刷卡簽到（退）管理系統構圖

5. 結論與未來展望

立法院是中華民國最高立法機關，其立法品質與行政效率之良窳直接影響政府施政效能，故須善用資訊科技，提昇服務品質，俾能充分掌握民意脈動，增進立法時效。綜上所述，結合 PKI 的立法院資訊應用獲致下列具體效益：

（1）統一控管人員基本資料與各系統使用者帳號、密碼，透過集中認證、授權方式提供各類應用系統權限控管服務，有效降低各系統之維護成本與人力，保障本院資訊系統之安全存取與資訊安全地傳遞。

（2）確保院內資訊系統整體作業環境之安全與系統服務品質，配合政府資訊安全政策之推動，完成異地備援系統之設置，符合 ISMS 資訊安全管理系統企業永續經營之要求與目標。

（3）利用 IC 識別證作為儲值卡之用，員工可自行掌握個人消費儲值情形並有效控管費用支出。

（4）充分利用 Mifare 機制，加值應用本院 IC 識別證資訊應用範圍。

而結合 SOC、ITIL/ITSM 及 ISMS 之 PKI 安全架構更獲得下述效益：

- 自建本院 SOC

（1）依此 PKI 基礎建立的立法院資訊系統（含行動資訊系統），深具安全與高可靠度，已達成優質立法院資訊建設目標，而自建 SOC 從國家整體角度制定防護策略（聯網、垂直、水平整合），提供標準的安全管理架構，持續遵行國家資訊安全政策，鞏固資訊安全管理。

（2）使用容易延伸的安全設備模組合作架構(framework)取代單一台主機架構(stand-alone)；透過集中及標準的架構，提供更大的經濟成本效益。

- SOC 與 ISMS 結合

（1）依據 ISMS 規範每半年針對風險評鑑結果風險較高系統，規劃有效因應的安全控管措施，以降低系統風險至可接受程度。

（2）透過資通安全管理中心(SOC)維運模式，提升本院同仁監控、研判、歸納與追蹤處理資安事件技術能力，與隨時汲取專業廠商經驗，充實本院資安監控處理機制，持續降低資安風險繼而充份掌握整體的資安狀態，發揮資安監控防護的具體成效。

（3）基於 PKI 架構，結合流程面、管理面與監控面實作之 SOC，自 2007 年元月開始建置時，統計事件發生次數從每 30 秒 18,000 筆，降至目前每 30 秒 400 筆，而人員每 15 分鐘可判斷 20 筆資安事件；統計通報次數從 2007 年的每月約 150 筆降至 2008 年的每月平均 60 筆左右，此次數的降低代表通報之事件合理性及準確性已大幅提高。

作者認為基於 PKI 的立法院資訊安全架構未來應從下列方向持續精進：

（1）強化 SOC 運作功能，作為未來資安工作的重點。

（2）提供高附加價值服務，提升民眾對立法院優質形象。

（3)永續提供與 SLA 管理標準一致的 MIS 服務。

（4）降低因災害發生造成資產損失機率。

（5）提供持續、彈性服務平台與資訊服務，滿足業務需求，提高整體立法效率。

（6）持續加值 IC 識別證應用範圍，提高本院 IC 識別證重要性。

（7）朝 IS20000 驗証目標邁進，以提供更優質資訊服務。

（8）資訊應用系統以通過 CMMI-ACQ 評鑑為目標，確保資訊委外服務品質。

致謝

作者誠摯感謝立法院 PKI 系統之承包商－異術科技股份有限公司黃總經理元中，在研究過程中提供本院 CA 架構精闢的見解。

參考文獻

[1] C.Adams and S.Lloyd , **“Understanding PKI: Concepts , Standards, and Deployment Considerations,”** 2nd ed,Addison-Wesley,2002.

[2] Gwo-Chin Tai and Chung-Ming Ou **“The development of PKI interoperability in Taiwan,”** Security Technology, 2003.

Proceedings. IEEE 37th Annual 2003 International Carnahan Conference 14-16 Oct.2003,pp.405-409.

[3] J.Dankers，T.Garefalakis，R.Schaffelhofer and T.Wright,**"Public key infrastructure in mobile systems,"**Electronics & Communication Engineering Journal vol.14,issue 5,pp.180-190,Oct.2002.

[4] R.Guida，R.Stahl，T.Bunt，G.Secrest and J.Moorcones; **"Deploying and using public key technology: lessons learned in real life,"**Security & Privacy, IEEE vol.2,issue 4,pp.67-71,Jul-Aug 2004.

[5] Zheng Guo，T.Okuyama and M.R.Finley"**A New Trust Model for PKI Interoperability**," Autonomic and Autonomous Systems and International Conference on Networking and Services, 2005. ICAS-ICNS 2005. Joint International Conference 23-28 Oct.2005, pp.37-37.

附件一、立法院 SOC 通報紀錄

項次	發生時間	通報時間	回復時間	事件摘要描述	嚴重程度	事件原由	受影響的資產設備系統(Nodes)	事件類別	SOC監控人員	電話通報對象	簡訊通報對象	Email通報對象
1	2008/10/1 16:25	2008/10/1 16:26	2008/10/1 17:46	2008/10/01 16:25 發現 xxx.xxx.xxx.xxx 持續對多數 IP 連線，目的 port 25。	嚴重		xxx.xxx.xxx.xxx	資訊安全	鍾○○	吳○○、陳○○		吳○○
2	2008/10/1 17:01	2008/10/1 17:06	2008/10/2 1:04	2008/10/01 17:01 xxx.xxx.xxx.xxx & 6 網段對 xxx.xxx.xxx.xxx 5 持續連線 113 Port。	嚴重		xxx.xxx.xxx.xxx	資訊安全	鍾○○	吳○○		吳○○
3	2008/10/1 23:54	2008/10/2 0:23	2008/10/1 23:55	2008/10/01 23:54 外部 IP:xxx.xxx.xxx.xxx 對外部 IP:xxx.xxx.xxx.xxx 網段進行掃描被 Deny，連線 Port:8080。	嚴重			資訊安全	王○○			吳○○
4	2008/10/2 23:40	2008/10/3 1:14		xxx.xxx.xxx.xxx 持續出現使用 P2P 軟體(驢子)之連線紀錄，且不停嘗試連線外部 DNS 伺服器，此主機在 2008/10/03 晚間流量一直是第一名，約每小時留出 420MB，xxx.xxx.xxx.xxx 之前曾中毒過，煩請吳先生查詢。	嚴重			資訊安全	王○○			吳○○
5	2008/10/2 23:42	2008/10/3 1:14	2008/10/2 23:43	2008/10/02 23:42 外部 IP:xxx.xxx.xxx.xxx 對內部 IP:xxx.xxx.xxx.xxx 連線，來源目的，疑似被植入後門程式，煩請吳先生查詢。	嚴重	有安裝 P2P 軟體		資訊安全	王○○			吳○○
6	2008/10/3 1:09	2008/10/3 1:14	2008/10/3 9:28	時間：2008/10/03 01:09 說明：檔案系統使用率超過 85%持續 15 分鐘 影響主機： LYXXX 檔案系統：/backup/rman_backup 目前使用率：86.13%	一般		Lyxxxx	系統效能	王○○			葉○○