行政院國家科學委員會專題研究計畫　成果報告

PMI 與 PKI 整合之前瞻研究

計畫類別：個別型計畫
計畫編號：NSC93-2623-7-009-004-
執行期間：93 年 01 月 01 日至 93 年 12 月 31 日
執行單位：國立交通大學資訊工程學系(所)

計畫主持人：陳昌居

報告類型：完整報告

處理方式：本計畫可公開查詢

中　華　民　國 94 年 3 月 2 日

國防科技學術合作計畫研發成果資料表

日期：94 年 1 月 11 日

<table>
<tr><td colspan="3">計畫名稱：PMI 與 PKI 整合之前瞻研究
計畫主持人：陳昌居教授、謝續平教授
計畫編號：NSC 93-2623-7-009-004</td></tr>
<tr><td rowspan="2">論文</td><td>期刊</td><td></td></tr>
<tr><td>研討會</td><td></td></tr>
<tr><td colspan="2">技術報告</td><td>PMI 與 PKI 整合前瞻研究報告</td></tr>
<tr><td rowspan="3">專利</td><td>申請</td><td></td></tr>
<tr><td>獲得</td><td></td></tr>
<tr><td>應用</td><td></td></tr>
<tr><td colspan="2">與軍方研發機構互動之具體研發成果</td><td>本計劃研究出一個整合 PKI 與 PMI 兩大基礎建設之架構，針對 PKI 憑證系統及 PMI 憑證系統之特性分析，以現有的 PKI 架構再加入 PMI 的屬性憑證應用，以強化整個憑證系統之適用範圍，讓憑證系統不僅止於做身分認證，更進一步可以做到權限控制的功能。

PKI 可以解決許多網路安全問題，並初步形成了一套完整的解決方案，它是基於公開金鑰理論和技術建立起來的安全體系，是提供資訊安全服務的具有普適性的安全基礎設施。該體系在統一的安全認證標準和規範基礎上提供線上身份認證，是 CA 認證、數位證書、數位簽章以及相關安全應用元件模組的集合。作為一種技術體系，PKI 可以作為支援認證、完整性、機密性和不可否認性的技術基礎，從技術上解決網路身份認證、資訊完整性和不可否認性等安全問題，為網路應用提供可靠的安全保障。但 PKI 絕不僅僅涉及到技術層面的問題，還涉及到電子政務、電子商務以及國家資訊化的整體發展戰略等多層面問題。PKI 作為國家資訊化的基礎設施，</td></tr>
</table>

	是相關技術、應用、組織、規範和法律法規的總和。PKI 的核心是要解決網路上的信任問題，確定資訊網路中各種經濟、軍事和管理行為主體（包括組織和個人）身份的惟一性、真實性和合法性，保護資訊網路空間中各種主體的安全利益。 授權管理基礎建設 PMI (Privilege Management Infrastructure)，目的是向用戶和應用程式之間提供授權管理服務，提供用戶身份到應用授權的對映功能，簡化應用系統的開發與維護。授權管理基礎建設 PMI 是一個由屬性憑證及屬性授權機構所構成的系統，用來實現權限和憑證的產生、管理、儲存、分發及撤銷等功能。PMI 使用屬性憑證表示和存放權限資訊，通過管理憑證的生命週期實行對權限有效期限的管理。屬性憑證的申請，簽發，註銷，驗證流程對應著權限的申請，發放，撤消，使用和驗證的過程。而且，使用屬性憑證進行權限管理使得權限的管理不必依賴某個具體的管理系統，而且利於權限的安全分佈式應用。 總括本研究計劃，包含了以下研究成果： 1. 對 ITU X.509v4 標準作深入詳細的研究，以其作為實作整合系統之基礎，使其合乎國際標準 2. 研究國內外相關領域之研究工作，吸取相關系統之開發經驗以利本計劃之系統實作 3. 研究 PKI 及 PMI 之關聯性及整合方法，並提出整合模型 4. 實作 PKI 與 PMI 整合之原始模型，成為此一領域之先驅
可推廣於民間產業之技術或可開發之產品	PKI 目前已經廣泛地被運用在各種領域中，包括像是我國政府電子公文系統、網路報稅、線上領標投標系統、證券交易、電子商務等，但是目前僅止於身份認證之用。

	面對現今各式各樣新式應用系統的需求，除了身份認證之外的功能也逐漸受到重視。整合 PMI 系統的運用可以很廣泛也可以僅止於單一的使用，例如： 1. IC 晶片卡權限管理系統 2. 保全控管系統 3. 電子商務身份互信及權限控制
可推廣之產業別（如無限通訊 微機電等）或可能技轉之廠商	本計劃主要研究網路上身份認證及權限控制之整合方案，本計劃之研究結果可廣泛地運用在許多產業上，例如： 1. 無線通訊 2. 網路安全 3. 電子商務、政務系統 4. 保全系統 5. 企業資源控管

本表若不敷使用，請自行影印使用。