國外 PKI 現況及未來趨勢簡介

綜觀國外 PKI 推動現況及未來趨勢（詳附錄），在歷經各國政府多年致力於基礎環境發展，並結合多項電子化政府服務之推動，加上網路普及化及電子商務日益成熟，當前各國政府 GPKI 主要推動議題（如下所述），皆可作為國內 GPKI 未來發展之參考依據。

- 擴大深化應用

未來則朝向地方政府擴散，增加一般性地方機關行政業務、便民服務等之 PKI 應用，同時應多方擴大憑證使用者數量。另外，與全體國民之義務與權力相關的部分，如稅務、健康保險等，將朝健康照護或兒童保護等方向發展。

- 加強信賴機制

在歷經多年推動後，由於使用人數增加，網路安全問題亦層出不窮情況下，強化驗證機制、應用生物辨識、建立全國性電子身份認證框架等，為各國以推動或未來將推動的 PKI 信賴環境。

- 掌握行動服務技術及應用發展趨勢

在掌握行動服務技術及應用發展趨勢方面，由於行動通訊技術近年來發展快速，移動模式身份認證、mobile PKI 架構等，其技術已漸成熟至可進入商業化的階段，因此各國政府相繼投入，進行大規模的測試、推廣計畫。

- 參與相關跨國憑證交互認證組織

包括亞洲 PKI 論壇、歐美 EESSI、OASIS、歐盟 eID 計畫等，除持續推動參與成員間成立橋接憑證中心（BCA），進行雙邊或多邊之跨國

憑證交互認證外，國際組織間也開始推動組織對組織間的憑證橋接。跨國憑證相互認證問題的解決，無論由國家與國家間雙邊協商或透過相關國際合作組織之雙邊或多邊協商，或是民間業者依其應用需求自行與國外業者簽訂互通之契約，均應先了解外國憑證機構有無跨國相互認證成功案例，再以之作為規劃我國與外國憑證相互承認的參考。

- 降低憑證管理中心維運成本與提高服務效能

OASIS 調查指出憑證管理中心基礎設施雖已逐漸降低持有成本，但維運管理成本以及導入成本仍需尋求有效的降低成本方案。因此如歐盟整合 eID 計畫與新一代電子護照，就是基於重複使用既有的基礎架構，將更有效率和符合成本效益為考量所推動的方案。

【附錄】下列表格為國外各國 PKI 發展情形，可提供我國 GPKI 發展策略規劃之參考。

國家名稱	說明
加拿大	● 採用 Webtrust for CAs 標準。 ● 美國 PKI Forum 組織會員國之一。 ● 電子憑證應用包含：社會保險服務、移民服務、護照服務、線上申請核發流程追蹤。 ● 提供 Wireless/Mobile PKI 之應用服務。
日本	● 提供跨國憑證互通機制。 ● PKI 屬橋接式架構。 ● 亞洲公鑰基礎建設論壇發起國之一。 ● 提供 Wireless/Mobile PKI 服務。

國家名稱	說明
	● 推動 PKI 過程即考量安全議題與兼顧應用程式間之互通性。 ● 電子憑證應用包含：電子投標系統、線上執照更新、年度稅賦調整等。
韓國	● PKI 屬階層式架構。 ● 亞洲公鑰基礎建設論壇發起國之一。 ● 提供 Wireless/Mobile PKI 服務。 ● 電子憑證應用包含：全民政府系統、電子化採購系統(得獎)、家庭稅務系統、社會保險、資訊分享系統、全國教育資訊系統等。 ● 電子化政府 97 年排名第一。
芬蘭	● PKI 屬階層式架構。 ● 已發行 eID card，且整合健保資料到 ID card。 ● 可透過 Web、SMS、WAP、Voice 通道使用服務，同時針對不同通道提供憑證驗證機制，以支援不同的驗證設備使用。 ● 全世界資訊社會最高度發展的指標國家之一。
荷蘭	● 採用 Webtrust for CAs 標準。 ● 提供 Wireless/Mobile PKI 服務。 ● 已發行 eID card。
新加坡	● 2003 年已完成憑證機構鑑定方針。 ● 推動公共服務卡，作為新加坡政府公務人員在實體政府設施中、政府電腦網路或電子郵件之作為資料

國家名稱	說明
	存取控管。 ● 全世界第一個全國性的無紙化法庭系統，使用電子憑證於電子環境下進行法院審訊。 ● 相關應用包括：網路繳稅、退稅、抽獎、申辦車牌、辦理電子護照、買賣房屋、政府電子商務網、整合性土地資訊系統、電子訴訟系統等。 ● 其島嶼型國家地理環境及語言與台灣相近，可相互比較。
美國	● 採用 Webtrust for CAs 標準。 ● 於 1999 即成立美國 PKI Forum，相當早期即致力於 PKI 研究與發展。 ● 為多個知名 PKI 相關組織或標準制定組織如 OASIS 或 PKI Forum 之發源地。 ● 美國聯邦政府於 1996 年通過 HIPPA 醫療安全條例，對於醫療領域的 PKI 應用已有相當琢磨。 ● 美國政府總服務管理部門於2003年發佈電子驗證政策，目前各州政府及私部門領域的銀行業、汽車業與航太工業等已支援 PKI 技術。 ● 美國國稅局(IRS)從 2007 年起要求資產值超過一千萬美元的公司或免稅機構必須使用 PKI 機制進行網路報稅。 ● 美國聯邦存款保險公司(FDIC) 未來將改採安全性較高的 PKI 認證機制進行網路交易，防止愈來愈多的帳戶被網路入侵。

國家名稱	說明
澳洲	● 採用 Webtrust for CAs 標準。 ● 於 1997 年推動 Gatekeeper 計畫，為實現線上政府服務以及推動資訊經濟的重要推力考量。 ● 澳洲商界推出商務數位簽章憑證，主要概念為提升企業進行線上交易時的安全性。 ● 其全國性的〝文件鑑別服務〞為透過和出生證明、駕照及護照等的交叉比對來降低可能的犯罪行為，並不再支持單一號碼來辨認身分的機制。
德國	● 採用 Webtrust for CAs 標準。 ● 為歐洲地區具代表性發起歐洲橋接式憑證中心計畫之國家。 ● 於 2001 年以現有 PKI 產品互通為目標，發展 PKI Challenge 計畫，與來自世界各國 PKI 產學界代表擬定出各項測試議題的共通性技術評量準則。 ● 德國係全球最大智慧卡製造國，提供各國政府部門 PKI 運用技術，經驗相當豐富。 ● 自 2004 年起，德國政府開始推行身份辨識文件的電子化，包括電子身分證 (ID)、電子護照、以及電子健康保險卡；但對於不同用途的卡片不予以整合，以確保個人資料的獨立性及安全性。 ● 德國公共交通網路經營商(RMV)已用於交通、票證之購買、付款與票證的顯示應用，另外也提供交通運輸時刻查詢，目前已結合信用卡進行應用。
奧地利	● 2007 年除了進行交通票證應用之外，還可進行停車

國家名稱	說明
	場票證、自動販賣機與手機博奕下注等應用。 ● 運用手機結合近距離無線通訊以及 IC 卡的應用。例如在校園應用上，有一百位學生利用 NFC 手機購買學校福利社商品、紅利積點、自動販賣機、活動廣告智慧標籤、P2P 傳輸議程、新聞等應用。 ● 已建置全國性及具有公民卡功能的簽名卡，第一階段使用於電子健康保險。 ● 電子化政府與健康保險卡 e-card 之推動，以社會及健康保險應用為準。