電子憑證應用程式介面（API）配合2048位元改版說明會

行政院研究發展考核委員會
資訊管理處二科
林輝誼科長
97年10月22日

大綱

- 電子憑證應用程式介面（API）配合2048位元改版緣由
- 本日議程介紹
- 電子憑證應用程式介面（API）轉換建議
- 順便解決現有API之技術支援問題

電子憑證應用程式介面（API）配合2048位元改版緣由

- 依據國際密碼學發展趨勢之分析
  - 參考世界各主要國家的非對稱金鑰最小安全長度的建議，以中期程的安全防護所需，將RSA 1024提升為RSA 2048是一個合理的決定
- 依據行政機關電子憑證推行小組委員會議及96年9月至97年6月歷次GPKI工作月會決議辦理
- 世界各大IC卡廠產品世代交替趨勢
  - 主流IC卡產品都已經是2048位元卡片了
  - 1024位元RSA卡片已經屬於是前一世代的產品了，在不久的將來有停產的可能
  - 目前2048位元RSA卡片的價格及效能已經相當於1024位元RSA卡片，且記憶容量大於1024位元卡片

本日議程介紹

時間	活動內容	負責人
9:00-:9:30 (13:30-14:00)	報到	中華電信數據通信分公司
9:30-9:45 (14:00-14:15)	長官致詞	行政院研究發展考核委員會資訊管理處二科 林輝誼科長
9:45-10:30 (14:15-15:00)	CSP 及PKCS11改版說明	中華電信研究所資通安全研究室 徐美惠小姐
10:30～11:10 (15:00-15:40)	HiSecure API改版說明	中華電信研究所資通安全研究室 游菀瑄小姐
11:10～12:00 (15:40-16:30)	1. 有獎徵答10題 2. 問題討論(前5名發問者提供小禮品)	行政院研究發展考核委員會資訊管理處二科 林輝誼科長/中華電信研究所資通安全研究室王文正博士

參加訓練之公務人員可登記公務人員學習護照3小時

電子憑證應用程式介面（API）轉換建議

- GCA/XCA預計於98年5月換2048 bits IC卡
- 由97年10月下旬至98年5月GCA/XCA開始提供2048 bits RSA卡，應用系統有半年多的緩衝時間來轉換到新版API
- 除於今天說明會「問題討論」表達意見外，可於學員訓後滿意度調查問卷填寫意見
- 本會另將於會後發文各GCA/XCA應用主管機關改版期程，請於11月20日前回覆配合改版時程
  - GPKI其他CA之辦理情形
    - 經濟部MOEACA已於97年8月28日辦竣”工商憑證應用安全保密函式庫改版說明會”，並定出98年3月1日開始在MOEACA核發RSA 2048 bits的憑證IC卡，並請各機關與PKI應用系統開發廠商配合改版。

順便解決現有API之技術支援問題

- GCA/XCA現有1024 bits卡之PKCS#11及CSP為國外原廠提供，在技術支援上面臨以下問題：
  - 國外原廠所提供的API版本在我國流通的版本有1.0.8版、1.0.9版、2.3版共三個版本，但三個版本的函式呼叫方式差異頗大，且沒有向下相容，導致用戶如果安裝了新版的API則可能原先使用較舊版API撰寫之應用系統就變成無法正常使用了
  - 由於國外原廠之API版本沒有向下相容，所以GCA/XCA官方正式對外提供之API版本只能維持在1.0.8版，但是1.0.8版的API無法支援Windows 2003及Vista作業系統，也無法支援Linux作業系統。
  - 1.0.8版之CSP在IC卡連續簽章達30次後，會開始發生錯誤而無法再繼續產生簽章，但國外原廠基於1.0.8版之產品生命周期已經結束，並不願意針對1.0.8版修正此問題
  - 如果藉著換卡的機會，讓各應用系統逐漸Migrate到國內自行研發的新版API，則可順便解決以上技術支援問題

報告完畢

敬請指教!