

## 行政機關電子憑證推行小組第 14 次委員會議紀錄

一、時間：97 年 6 月 26 日（星期四）上午 9 時 30 分

二、地點：本會 7 樓簡報室

三、主席：宋副主任委員餘俠

記錄：戴慧明

四、出席單位及人員：（如簽到冊）

五、主席致詞：（略）

六、決議：

- (一) 同意醫事憑證管理中心(簡稱 HCA)加入政府機關電子憑證公開基礎建設(簡稱 GPKI)機制，以及衛生署完成 HCA 實務作業基準 (CPS) V1.0 審查意見與建議(詳如附件 1)之各項修訂，請衛生署針對委員之意見（詳如附件 2）修正後送本會核備，同時送請經濟部進行後續審查作業。
- (二) 有關規劃推動國內電子憑證所需之密碼模組、簽章格式、加密演算法及雜湊函數演算法等國家政策與標準，請先提報行政院國家資訊通信發展推動小組確認作法，可委託公/協會或學者專家進行先期研究及請國家通訊傳播委員會就技術監理面及實務面需求初審，通過後交由經濟部標準檢驗局確認及訂頒，分三階段進行。鑒於檔案管理局目前正制訂歸檔文件之標準格式，請邀檔案管理局共同研議。
- (三) 為配合環境保護及提升行政效率，GCA、XCA 之電子憑證申請、廢止等作業，一律改採公文電子交換方式，隨函檢送憑證申請書電子檔至本會，並請修正 GCA、XCA CPS 相關內容。
- (四) 原則同意「GPKI 用戶憑證到期換卡行動方案-以 GCA、XCA 為行動標的」乙案，由公文電子交換系統優先試辦。有關 1024 bits 卡之私密金鑰載具介面 (PKCS#11) 及卡片

介面服務軟體 (Cryptographic Service Provider, CSP), 請維運團隊以使用者與開發者之需求考量, 自行研究 API 使用軟體之可行性, 並考量作業系統升級和應用程式界面 (API) 相容性之問題。

(五) 請儘速規劃自然人憑證結合公務識別證聯名卡應用, 以配合線上簽核、節省用紙及節能減碳等政策目標推動; 並請各機關配合優先編列經費辦理。

七、散會：中午 12 時