行政機關電子憑證推行小組第 21 次委員會議紀錄

一、時間：101 年 5 月 25 日（星期五）下午 2 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：蔡分析師淑瑋

四、出列席單位及人員：（如簽到冊）

五、主席致詞：（略）

六、決議：

（一）同意「醫事憑證管理中心憑證實務作業基準第 1.2 版(草案)」之修訂(如附件 1)，請針對委員意見修正內容後送本會依「電子簽章法」規定函送經濟部審查。

（二）同意「工商憑證管理中心憑證實務作業基準第 1.8 版（草案)」之修訂(如附件 2)，請針對委員意見修正內容後送本會依「電子簽章法」規定函送經濟部審查。

（三）原則同意政府憑證管理中心及組織與團體憑證管理中心酌收用戶 IC 卡工本費；請針對各憑證管理中心之 IC 卡工本費收費方式(包含價格、繳費對象、服務水準規範、行政作業等議題)提出一致性建議作法並報經行政機關電子憑證推行小組同意後再行實施。

（四）請各憑證管理中心重新檢視及確保各項維運活動流程(包含憑證申請、核發及註銷等各階段流程活動)之安全性，以維政府公開金鑰基礎建設整體資訊安全。

七、散會：下午 4 時 30 分。

附件 1：醫事憑證管理中心憑證實務作業基準第 1.2 版(草案)審查意見表

變更後記載內容	變更後頁數	審查意見
摘要	x	原則同意。
1.2 憑證實務作業基準之識別	2	原則同意。
1.4.2 聯絡資料	8	原則同意。
1.4.3 憑證實務作業基準之審定	9	原則同意
3.1.4 命名之獨特性	28-30	原則同意
4.4.3 憑證廢止之程序	44	原則同意
6.1.1 金鑰對之產製	69	原則同意
6.1.8 金鑰經軟體或硬體產製	71	建議修改文字說明"用戶使用通過 NIST 所訂定之 CNS 15135、ISO 19790、FIPS 140-2 Level [刪除]~~3~~ [新增] 2 或安全強度相當之 IC 卡"
6.2.1 密碼模組標準	71	建議修改文字說明"本管理中心使用[刪除]~~安全等級 3~~[新增] 通過 FIPS140-2 Level3 認證安全等級的硬體密碼模組[新增] 產制亂數及用戶金鑰對....."
6.5.2 電腦安全評等	75	原則同意

附件 2：工商憑證管理中心憑證實務作業基準第 1.8 版(草案)審查意見表

變更後記載內容	變更後頁數	審查意見
2.5 費用	17	原則同意。
3.1.4 命名之獨特性	27	原則同意
3.1.6 商標之辨識、鑑別及角色	27-28	原則同意。
3.2.2 憑證展期	30-31	原則同意。
4.1.2 申請展期憑證之程序	33-34	原則同意。
4.2.3 展期憑證之簽發審核程序	37	原則同意。
6.1.1 金鑰對之產製	71	原則同意。
6.2.4 私密金鑰備份	74	原則同意，另建議刪除 SafeBox 字樣
6.3.2.1 憑證機構公開金鑰及私密金鑰之使用期限	77	原則同意。
6.1 金鑰對之產製及安裝 ~6.4 啟動資料之保護	70-79	建議將內文中所出現 FIPS 140-1 部分，依照現況調整為 FIPS 140-2
6.2.5 私密金鑰歸檔	73	建議修改文字說明"本管理中心亦不對[新增]用戶簽章用[新增]之私密金鑰進行歸檔"。
6.5.2 電腦安全評等	79	建議電腦安全性強度說明採與 HCA 相同之敘述。