行政機關電子憑證推行小組第 8 次委員會議紀錄

壹、時間：94 年 8 月 4 日（星期四）上午 9 時 30 分

貳、地點：本會簡報室（台北市濟南路 1 段 2 之 2 號 7 樓）

參、主席：何處長全德　　記錄：吳啟文

肆、出列席人員（如簽到冊）

伍、主席致詞（略）

陸、報告事項（略）

一、宣讀上次會議紀錄。

決定：(一)第7次委員會議紀錄確定備查。

(二)GPKI策略會議紀錄一(一)，決議1除自然人憑證外，請增加工商憑證，另增加決議3”對於民間應用使用GPKI所簽發憑證，採不主動、不拒絕、不推廣策略”。

柒、討論事項

一、 審查工商憑證管理中心憑證實務作業基準修正事宜。

決議：(一)1.3.7.2節不做修正。

(二)1.3.7.3節(5)修正為”法令公告禁止適用之範圍”。

(三)3.1.8節”…(與事業主體登記時所使用之印鑑章同款)…”修正為”…(與事業主體登記時所使用之印鑑章相符)…”。

(四)3.5節修正為”申請人連線至儲存庫提出憑證暫時停用或恢復使用申請時，註冊中心系統將以用戶輸入之用戶代碼鑑別其身分”。

(五)授權由承辦單位（研考會資管處）確認本文件（修正本）是否通過。

二、 審查組織及團體憑證管理中心（XCA）憑證實務作業基準修正事宜。

決議：(一)1.3.7.2節不做修正。

(二)1.3.7.3節(5)修正為”法令公告禁止適用之範圍”。

(三)3.5節修正為”申請人連線至儲存庫提出憑證暫時停用或恢復使用申請時，註冊中心系統將以用戶輸入之用戶代碼鑑別其身分”。

(四)授權由承辦單位（研考會資管處）確認本文件（修正本）是否通過。

三、審查政府機關公開金鑰基礎建設（GPKI）技術規範修正事宜。

決議：(一)請補充與ISO標準對應之CNS標準，並將其列於ISO標準之前。

(二)請統一SHA-1、SHA-256等演算法之表示法，並註明其出處。

(三)2.4節部分：

1、請註明3-Key之Key Length為112 bits或168 bits，並考量是否只接受CBC Mode。

2、請考量是否採用比RC-2還新之RC-4。

(四)請統一有關NIST FIPS PUBS或PUB之寫法，另2.6節(4)雜湊函數OID誤植為id-SHA384，請修正。

(五)標準或規範部分，請將”（含）以上”修正為”或其最新版”。

(六)行政機關電子憑證推行小組請加上引號，以資區別。

(七)授權由承辦單位(研考會資管處)確認本文件(修正本）是否通過。

捌、臨時動議

一、 因應科技快速發展及政府應用推廣，請規劃每季召開本小

組委員會議，並定期檢討GPKI憑證政策、技術規範等相關規定。

二、 請研究XCA委託公正第三者設立統一RA窗口之可行性。

玖、散會：上午 11 時 55 分