行政機關電子憑證推行小組第 12 次委員會議紀錄

一、時間：97 年 1 月 17 日（星期四）下午 14 時整

二、地點：本會 7 樓簡報室

三、主席：陳副主任委員俊麟　　記錄：戴慧明

四、出列席單位及人員：（如簽到冊）

五、主席致詞：(略)

七、決議：

(一) 修訂政府機關公開金鑰基礎建設(CP)相關條文詳附件 1。

(二) 修訂內政部憑證管理中心憑證實務作業基準（CPS）相關條文詳附件 2。

(三) 有關密碼模組、簽章格式、加密演算法及雜湊函數演算法，請發文國家通訊傳播委員會訂頒國家政策與標準，除考量電子化政府應用需求研究適用之標準及演算法轉換時機，並避免技術來源單一性，及考量分散風險。

(四) 各憑證主管機關送審憑證實務作業基準（CPS）前，請先洽法規單位檢視文句修訂意見。

八、散會：下午 15 時 50 分

附件 1：

NO	修正後條文	原條文	章節
1.	私密金鑰無立即被破解之虞	私密金鑰無立即被破解的危險	3.2.2
2.	若金鑰為 RSA 1024 位元，則私密金鑰使用期限至多為 5 年。另憑證機構得經評估適法性、便民性、安全性、成本效益之需要，而將 RSA 1024 位元金鑰之展期不得超過 3 年。但展期後的使用期限至多到民國 102 年 12 月 31 日為止。	若金鑰為與 RSA 1024 位元安全強度相當，則私密金鑰使用期限~~原則上~~至多為 5 年。另憑證機構得經評估適法性、便民性、安全性、成本效益之需要，而將 RSA 1024 位元金鑰之使用期限至多展延 8 年，但展延後的使用期限至多到民國 102 年 12 月 31 日~~(含)~~為止。	6.3.2.2
3.	基於金鑰安全強度的需求，憑證機構最晚必須在民國 99 年 12 月 31 日停止簽發 RSA 1024 位元的憑證，但在此之前簽發的憑證，仍可使用到效期到期日為止。	基於金鑰安全強度的需求，憑證機構最晚必須在民國 99 年 12 月 31 日~~(含)~~停止簽發與 RSA 1024 位元安全強度相當的憑證，但在此之前簽發的憑證，仍可使用到~~這些憑證~~效期到期日為止。	6.3.2.2

附件 2：

NO	修正後條文或文字	原條文或文字	章節/頁次/修訂原則
1.	展期	展延、延展	
2.		~~原則為~~	贅詞刪除
3.	配合行政院秘書處文書處理手冊公文書橫式書寫數字使用原則，修訂文件中數字表示方式。		
4.	通過 ISO 27001:2005 評鑑	通過 BS-7799:2002 評鑑	Viii
5.	4.2.2-4.2.4 展期步驟描述過於詳細，請改以原則性陳述重點。		
6.	在憑證到期前的 60 天開始至到期期間內，且憑證有效下（指已完成接受憑證、未停用且未廢止），用戶可自行使用憑證展期軟體辦理線上展期，或至各地憑證註冊窗口辦理臨櫃展期。	在憑證到期前的 60 天開始至到期的期間內，且憑證目前仍有效（指已完成接受憑證，未停用，且未廢止）下，用戶可自行使用憑證展期軟體辦理線上展期，或至各地憑證註冊窗口辦理臨櫃展期。	4.1.4
7.		註冊中心檢驗用戶的簽章無誤後，就以完整的憑證申請訊息向憑證管理中心申請簽發憑證。待憑證管理中心完成憑證簽發後，用戶再透過	4.2.4 請簡化說明

NO	修正後條文或文字	原條文或文字	章節/頁次/修訂原則
		安全加密管道下載憑證並寫入原用戶之 IC 卡中	
8.		作展期、進行展期	請統一用詞
9.	憑證展期時只展期其效期與變更其憑證序號，其餘內容與原憑證相同。	因憑證展期是對原先已經接受過的憑證作展期，此展期憑證的內容和原憑證的差別，只在於約定的效期展延與憑證序號不同。	4.3.2
10.	無論採用臨櫃或線上方式申請憑證停用，均可從臨櫃或線上任一方式恢復。		4.4.9 請兼顧用戶方便與系統之安全，可從線上及臨櫃任一種方式恢復憑證使用。
11.	如以上恢復憑證使用申請審核不通過時，本管理中心將拒絕恢復憑證使用。	如以上之恢復憑使用申請審核不通過時，本管理中心將拒絕恢復憑證使用。	4.4.9 缺漏字
12.		最後、欲暫時停用憑證之用戶、用戶如遺失憑證 IC 卡，也忘記了用戶代碼等	4.3 P32、 4.4.7 P36 修改文件中之語句或連接詞為法

NO	修正後條文或文字	原條文或文字	章節/頁次/修訂原則
			律或一般正式文件之用語
13.	4.4.5 請簡化有關電子式紀錄所用時間之描述。		