行政機關電子憑證推行小組第 25 次委員會議紀錄

一、時間：102 年 12 月 27 日（星期五）上午 9 時 30 分

二、地點：本會 7 樓簡報室

三、主席：趙主任秘書錦蓮　　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「政府機關公開金鑰基礎建設憑證及憑證廢止清冊格式剖繪第 1.8 版(草案)」之修訂(如附件 1)，請針對委員意見修正內容後，公布於政府憑證總管理中心網站並通知政府公開金鑰基礎建設下屬各憑證管理中心。

（二）同意「政府憑證總管理中心憑證實務作業基準第 1.4 版(草案)」之修訂(如附件 2)，請針對委員意見修正內容，並依「電子簽章法」規定函送經濟部審查。

（三）同意「政府憑證管理中心憑證實務作業基準第 1.6 版(草案)」之修訂(如附件 3)，請針對委員意見修正內容，並依「電子簽章法」規定函送經濟部審查。

（四）同意「組織及團體憑證管理中心憑證實務作業基準第 1.6 版(草案)」之修訂(如附件 4)，請針對委員意見修正內容，並依「電子簽章法」規定函送經濟部審查。

（五）同意「醫事憑證管理中心憑證實務作業基準第 1.4 版(草案)」之修訂(如附件 5)，請針對委員意見再修正內容送本會確認後，依「電子簽章法」規定函送經濟部審查。

（六）同意組織及團體憑證管理中心(XCA)、內政部憑證管理中心(MOICA)之交互認證申請案，並請政府憑證總管理中心(GRCA)依照會議決議，於 7 個工作日內完成簽發交互憑證作業，並以公文方式通知憑證管理中心須依 GRCA 憑證實務作業基準之接受憑證程序，完成相關審查與回覆作業。

（七）請各憑證管理中心重新考量憑證實務作業基準等文件「資訊保密範圍」章節內容中有關「機密」一詞用法，政府機關對「機密」文件處理程序須符合國家機密保護法規範。請各憑證管理中心評估資料安全性等級，將「機密」文字調整為「機敏性」、「敏感性」或「保密」等詞彙予以取代，並維持一致性用語。

(八) 有關各憑證管理中心憑證實務作業基準 5.1.7 廢料處理一節，請慎重考量硬碟、光碟等各種儲存媒體銷毀方式，並遵循政府機關資料處理辦法進行銷毀。

(九) 行政院研究發展考核委員會將於103 年 1 月 22 日配合政府組織改造，整併成為國家發展委員會，相關憑證實務作業基準修訂請於 103 年 1 月 22 日後送經濟部商業司審核。

(十) 各憑證管理中心未來產製公開金鑰對時，除說明新金鑰對產製過程中須注意之相關事項外，請同時說明舊金鑰後續處理方式，以昭信公眾。

(十一)請各憑證管理中心針對委員提供之書面審查意見(如附件 6)，修正相關內容。

七、臨時動議：

案由：政府憑證總管理中心、政府憑證管理中心、組織及團體憑證管理中心、工商憑證管理中心、內政部憑證

管理中心、醫事憑證管理中心年度外部稽核(Web Trust CAs)驗證作業，請回歸各主管機關自行辦理。

決議：為落實憑證管理中心權責及管理，自 103 年起，由憑證總管理中心對各憑證管理中心進行外部稽核，各憑證管理中心對所屬憑證管理註冊窗口進行外部稽核，所需經費 103 年度可由研考會協助分攤，104 年起請各憑證管理中心主管機關自行編列預算支應。

八、散會：下午 12 時 30 分。

附件 1:政府機關公開金鑰基礎建設憑證及憑證廢止清冊格式剖繪第 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
封面頁		原則同意
1.1.2 CA 公鑰憑證的設計原則	2	原則同意，請將 Asia PKI Forum 修訂為 Asia PKI Consortium
1.2.1 用戶公鑰憑證的種類	7	原則同意，請將確定文字用法前後之一致性
1.2.2 用戶公鑰憑證的設計原則	10	原則同意，請將 Asia PKI Forum 修訂為 Asia PKI Consortium
1.3.14 TO-Be-Signed 行政法人憑證格式	118	原則同意
2.2 憑證廢止清冊的設計原則	185	原則同意，請將 Asia PKI Forum 修訂為 Asia PKI Consortium

附件2：政府憑證總管理中心憑證實務作業基準第1.4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	viii	原則同意
1.1 概要	2	原則同意
1.2 憑證實務作業基準之識別	2	原則同意
2.8.1 機密之資訊種類	18	原則同意，建議將「機密」修訂為「機敏性」或「敏感性」
2.8.2 非機密之資訊種類	19	原則同意，建議將「機密」修訂為「機敏性」或「敏感性」
3.1.8 組織身份鑑別之程序	23	原則同意
3.1.9 個人身份鑑別之程序	24	原則同意
4.1 申請憑證之程序	26	原則同意，請確定本段文字前後用法一致性
5.1.7 廢料處理	47	原則同意，儲存媒體的銷毀方式請依照政府機關訂定之標準程序辦理
7.1.4 命名形式	69	原則同意

附件 3：政府憑證管理中心憑證實務作業基準第 1.6 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	viii	原則同意
1.1 概要	1	原則同意
1.2 憑證實務作業基準之識別	2	原則同意
2.8.1 機密之資訊種類	17	原則同意，建議將「機密」修訂為「機敏性」或「敏感性」
2.8.2 非機密之資訊種類	18	原則同意，建議將「機密」修訂為「機敏性」或「敏感性」
5.1.7 廢料處理	49	原則同意，儲存媒體的銷毀方式請依照政府機關訂定之標準程序辦理
6.3.2.1 政府憑證管理中心公開金鑰及私密金鑰之使用期限	63	原則同意

附件4：組織及團體憑證管理中心憑證實務作業基準第1.6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	viii	原則同意
1.1 概要	2	原則同意
1.2 憑證實務作業基準之識別	2	原則同意
2.8.1 機密之資訊種類	17	原則同意，建議將「機密」修訂為「機敏性」或「敏感性」
2.8.2 非機密之資訊種類	18	原則同意，建議將「機密」修訂為「機敏性」或「敏感性」
5.1.7 廢料處理	45	原則同意，儲存媒體的銷毀方式請依照政府機關訂定之標準程序辦理
6.3.2.1 政府憑證管理中心公開金鑰及私密金鑰之使用期限	58	原則同意

附件 5：醫事憑證管理中心憑證實務作業基準第 1.4 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	ix	原則同意
1.1 概要	2	原則同意
1.3.6.1 用戶	5	原則同意
1.3.7 以委外方式提供認證服務	6	原則同意
1.4.1 憑證實務作業基準之制訂及管理機關	8	原則同意
1.4.2 聯絡資料	9	原則同意
2.1.2 註冊中心之職責	10	原則同意
2.3 財務責任	18	原則同意
2.4.1 適用法律	18	原則同意
2.5 費用	19	原則同意
2.5.1 憑證簽發費用	19	原則同意
2.5.4 憑證更新費用	20	原則同意
2.5.5 其他服務之費用	20	原則同意
2.6.2 公布頻率	21	原則同意
2.9 智慧財產權	25	原則同意

變更後記載內容	變更後頁數	審查意見
3.1.2 命名須有意義	27	原則同意
3.1.4 命名之獨特性	28	原則同意
3.1.5 命名爭議之解決程序	30	原則同意
3.1.8.1 醫事機構憑證	32	原則同意
3.1.9.1 初次申請憑證	33	原則同意
3.1.10 硬體裝置或伺服軟體鑑別之程序	34	原則同意
6.1.1 金鑰對之產製	69	原則同意
6.2.2 金鑰分持之多人控管	72	原則同意
6.5.2 電腦安全評等	75	原則同意
6.6.1 系統研發控管措施	76	原則同意

附件 6：委員書審意見表

政府機關公開金鑰基礎建設憑證及憑證廢止清冊格式剖繪第 1.8 版(草案)	
項次	意見
1	Page2:"符合 IETF PKIX Certificate and CRL Profile (RFC 3280) 之憑證規格"，目前此標準在 IETF 已被廢棄，最新標準為 RFC 5280，建議考慮採用最新標準。(後續相關引用也請一併考量)
2	Page2："符合 IETF PKIX Qualified Certificates Profile (RFC 3039) 之憑證規格"，目前此標準在 IETF 已被廢棄，最新標準為 RFC 3739，建議考慮採用最新標準。(後續相關引用也請一併考量)。
3	Page9：OCSP 協定之說明，目前 RFC 舊規範 2560 及 6277 皆已廢棄，最新標準為 RFC 6960，請詳細說明本規範採用那一個 RFC 規範。
4	To-Be-Signed 憑證格式的說明，針對 serialNumber 建議強調為不可重複。
5	學校憑證中 Subject 一欄是否需要定義何謂地區性學校(中小學？)私立學校是否需要使用 L=縣市名稱 L=鄉鎮市區名稱)。
6	學校憑證中 Subject 針對學校分校的狀況，是否需要特別考量？
7	自然人憑證 subject 建議針對新移民及原住民等特殊狀況，增加欄位，保留原始的姓名。
8	伺服器的憑證格式，建議針對雲端的應用狀況(如新增 VM 增加 AP)其 subject 中的 serialNumber=伺服器應用軟體的識別代號，是否足以識別做考量。
9	Page193、201、208:aACompromise 一列中"當懷疑 AA 簽發 Attribute Certificate 用之私密金鑰，此 CRLReason 遭竊或被破解時使用此 CRLReason"文字不是很通順，請修正。

政府憑證總管理中心憑證實務作業基準第 1.4 版(草案)審查意見	
項次	意見
1	Page22 ：一般 CA 的翻譯為 certificate authority，總管理中心的自簽憑證的名稱為 C=TW，O=Government Root Certification Authority，與一般翻譯不一樣，請確認。
2	Page49:信賴角色定義 5 個角色，而其工作未明確包含金鑰分持管理，建議補充此部分。

3	Page58:總管理中心使用 4096 位元的 RSA 金鑰及 SHA-1 或 SHA-2 雜湊函數演算法簽發憑證，與"政府機關公開金鑰基礎建設憑證及憑證廢止清冊格式剖繪"所示為 Sha1 及 Sha256 有差異，內容建議同步。

政府憑證管理中心憑證實務作業基準第 1.6 版(草案)審查意見	
項次	意見
1	Page 1：一般 CA 的翻譯為 certificate authority，政府憑證管理中心英譯為 Government Certification Authority，與一般翻譯不一樣，請確認。
2	Page 1：一般 CA 的翻譯為 certificate authority，政府憑證管理中心英譯為 Government Certification Authority，與一般翻譯不一樣，請確認。
3	Page 8：政府憑證管理中心之職責:建議強化對於 OCSP 的功能的描述。
4	Page 10 信賴憑證者之義務:建議強化對於 OCSP 的功能描述。
5	Page 11 儲存庫服務之義務:建議強化對於 OCSP 的功能描述。
6	Page 50：信賴角色:未提及金鑰分持之功能由誰負責，建議強化此部分描述。

組織及團體憑證管理中心憑證實務作業基準第 1.6 版(草案)審查意見	
項次	意見
1	Page1：一般 CA 的翻譯為 certificate authority，組織及團體憑證管理中心名稱為 miXed organization Certification Authority, XCA，與一般翻譯不一樣，請確認。
2	Page 46:信賴角色定義 5 個角色，而其工作未明確包含金鑰分持管理，建議補充此部分。
3	Page 4:有關 1.3.4 儲存庫，建議強化對於 OCSP 應用之說明。
4	Page 10 信賴憑證者之義務:建議強化對於 OCSP 的功能描述。
5	Page 10 儲存庫服務之義務:建議強化對於 OCSP 的功能描述。

醫事憑證管理中心憑證實務作業基準第 1.4 版(草案)審查意見	
項次	意見
1	Page1：一般 CA 的翻譯為 certificate authority，醫事憑證管理中心英譯為 Healthcare Certification Authority，與一

	般翻譯不一樣，請確認。
2	Page10:；"安全管道為使用安全插座層[刪除]安全套接層[新增]通通訊協定"多一個"通"字。
3	Page11:註冊窗口之職責一節，未明確描述"應用於醫事專門用途的伺服器應用軟體"的申請權責。
4	Page14:信賴憑證者之義務:建議強化對於 OCSP 的功能描述
5	Page5:有關 1.3.4 儲存庫，建議強化對於 OCSP 應用之說明
6	Page30:伺服器應用軟體憑證建議針對雲端的應用狀況(如新增 VM，增加 AP)serialNumber=伺服器應用軟體的識別代號，是否足以識別做考量。
7	Page 30:伺服器應用軟體憑證:"醫事機構的 X.500 Name"，是否應為"O=醫事機構的 X.500 Name"或是其他狀況，請確認。另外，就命名之獨特性，若不加區域資訊，是否可以明確確認(如有分院的狀況)?
8	Page 69:"本節所指的安全管道為使用安全插座層通訊協定 128 位元或其他相同或更高等級之資料加密傳送方式"與 P10"將申請資料及用戶公開金鑰透過安全管道 (安全管道為使用安全套接層 通通訊協定 256 或其他相同或更高等級之資料加密傳送方式)傳送給本管理中心"，文字(安全插座層 vs 安全套接層)及位元數(128 vs 256)有差異，請確認。
9	Page 70:金鑰長度一節，建議至少參照 GRCA 可支援 SHA256。