行政機關電子憑證推行小組第 23 次委員會議紀錄

一、時間：101 年 12 月 3 日（星期一）上午 9 時 30 分

二、地點：本會 7 樓簡報室

三、主席：戴副主任委員豪君　　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「政府憑證管理中心憑證實務作業基準第 1.5 版(草案)」之修訂(如附件 1)，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。

（二）同意「組織及團體憑證管理中心憑證實務作業基準第 1.5 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「工商憑證管理中心憑證實務作業基準第 1.9 版(草案)」之修訂(如附件 3)，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。

（四）同意「自然人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。

（五）同意「醫事憑證管理中心憑證實務作業基準第 1.7 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「政府公開金鑰基礎建設憑證政策第 1.7 版(草案)」之修訂(如附件 6)，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。

（七）同意報告案「政府憑證測試管理中心(GTestCA)移出 GRCA 體系驗證架構」，請依規劃時程辦理 GTestCA 系統移轉作業，並依配套措施進行公告作業，以確保服務不中斷。

（八）各憑證管理中心針對憑證實務作業基準 2.8.1 章節機密之資訊種類一節，建議機密資訊定義應通盤考量各資訊來源，包含契約、職務或營運面等，另保密期限也宜全面考慮是否需涵蓋至終身保密。

（九）各憑證管理中心針對憑證實務作業基準第 5.1.4 水災防範及保護一節，建議水災防範應從各方面考慮，包含管線漏水、天花板漏水，或淹水等事由，非單指防護淹水情形，建議應以提供安全樓層之角度通盤審慎規劃。

（十）各憑證管理中心針對憑證實務作業基準第 5.3.7 聘雇人員之規定一節，建議考量營運中負責之關鍵職務內容是否可由聘僱人員擔任，或採訂定聘僱人員與專任人員之員額比例等方式予以規範。

（十一） 各憑證管理中心針對營運系統之開發品質管控，建議可導入 CMMI 認證方式，以確保各項系統開發品質。

（十二） 自然人憑證管理中心公布個人憑證資訊，其內容包含身分證字號後四碼時，其身分證字號隱碼規則之安全強度是否足夠，請再詳加評估。

（十三） 醫療體系掌握民眾之特種個資，應強化其安全管理，避免遭受未授權之存取，請醫事憑證管理中心再詳加考慮，各項憑證作業與安全是否已完備，另針對內部

稽核活動請至少一年辦理一次以上方式辦理，以落實資訊安全。

（十四） 各憑證管理中心增修憑證實務作業基準時，可借鏡國外憑證機構營運案例，汲取他國憑證實務經驗補強本身憑證實務作業基準內容。

（十五） 建議查明憑證政策第 6.1.5 金鑰長度一節，憑證機構應配合憑證政策改用 SHA256 演算法簽發各類憑證之最晚日期是否有誤繕，經查證行政機關電子憑證推行小組第 20 次委員會議紀錄，已確認日期為民國 105 年 12 月 31 日，與目前憑證政策內容相符合，無須更正。

七、散會：下午 12 時 30 分。

附件 1：政府憑證管理中心憑證實務作業基準第 1.5 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
1.2 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，並可從職務、營業或契約等面向，思考保密的範圍
3.1.4 命名之獨特性		原則同意，請調整伺服器應用軟體憑證之項次為(3)
4.6.2 歸檔之保留期限	43	原則同意
4.6.5 時戳紀錄之要求	44	原則同意
4.7 金鑰更換	44	原則同意
5.1.4 水災防範及保護	48	原則同意，但水災之防護請從全面向考慮，非只考慮淹水因素
5.3.7 聘雇人員之規定	55	原則同意，建議修訂為「除須具備足夠的知識技能與專業倫理，遵守本憑證實務基準相關規定進行，並簽定相關保密協定」，另請再審慎評估營運人員需具備的證照或條件等，或是相關聘僱人員與專任人員之比例。
6.1.1 金鑰對之產製	56	原則同意
6.1.3 公開金鑰安全傳送給政府憑證管理中心	57	原則同意，但建議調整文字順序為本節所指的安全管道為使用專屬通訊協定、資料簽章及加密傳送方式，諸如安全套接層(Security Socket Layer, SSL)通訊協定、憑證管理訊息格式協定(Certificate Management Protocol, CMP)簽章封包、憑證註

變更後記載內容	變更後頁數	審查意見
		冊審驗人員簽章等。
6.1.5 金鑰長度	57	原則同意，建議只保留 SHA1 與 SHA256 演算法
6.1.7 金鑰參數品質之檢驗	58	原則同意
6.2.1 密碼模組標準	59	原則同意，建議「IC 卡」更新為「安全 IC 卡」
6.2.5 私密金鑰歸檔	59	原則同意
6.2.6 私密金鑰輸入至密碼模組	60	原則同意
6.2.9 私密金鑰之銷毀方式	60	原則同意
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
6.6.1 系統研發控管措施	63	原則同意，但建議品質管理可嘗試以導入 CMMI 方式進行
6.6.2 安全管理控管措施	63	原則同意
6.6.3 生命週期安全評等	63	原則同意
7.1.3 演算法物件識別碼	65	原則同意
7.1.4 命名形式	66	原則同意
7.1.9 關鍵憑證政策擴充欄位之語意處理	66	原則同意

附件2：組織及團體憑證管理中心憑證實務作業基準第1.5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
1.2 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，並可從職務、營業或契約等面向，思考保密的範圍
4.4.4 憑證廢止申請之處理期間	30	原則同意
4.6.2 歸檔之保留期限	40	原則同意
4.6.5 時戳紀錄之要求	41	原則同意
4.7 金鑰更換	41	原則同意
5.1.4 水災防範及保護	45	原則同意，但水災之防護請從全面向考慮，非只考慮淹水因素
5.3.7 聘雇人員之規定	45	原則同意，建議修訂為「除須具備足夠的知識技能與專業倫理，遵守本憑證實務基準相關規定進行，並簽定相關保密協定」，另請再審慎評估營運人員需具備的證照或條件等，或是相關聘僱人員與專任人員之比例
6.1.1 金鑰對之產製	53	原則同意
6.1.3 公開金鑰安全傳送給組織及團體憑證管理中心	54	原則同意，但建議調整文字順序為本節所指的安全管道為使用專屬通訊協定、資料簽章及加密傳送方式，諸如安全套接層(Security

變更後記載內容	變更後頁數	審查意見
		Socket Layer, SSL)通訊協定、憑證管理訊息格式協定(Certificate Management Protocol, CMP)簽章封包、憑證註冊審驗人員簽章等。
6.1.5 金鑰長度	54	原則同意，建議只保留 SHA1 與 SHA256 演算法
6.1.7 金鑰參數品質之檢驗	55	原則同意
6.2.1 密碼模組標準	55	原則同意，建議「IC 卡」更新為「安全 IC 卡」
6.2.5 私密金鑰歸檔	56	原則同意
6.2.6 私密金鑰輸入至密碼模組	56	原則同意
6.2.9 私密金鑰之銷毀方式	57	原則同意
6.3.2.1 組織及團體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
6.6.1 系統研發控管措施	59	原則同意，但建議品質管理可嘗試以導入 CMMI 方式進行
6.6.2 安全管理控管措施	59	原則同意
6.6.3 生命週期安全評等	60	原則同意
7.1.3 演算法物件識別碼	61	原則同意
7.1.4 命名形式	62	原則同意

變更後記載內容	變更後頁數	審查意見
7.1.9 關鍵憑證政策擴充欄位之語意處理	62	原則同意

附件 3：工商憑證管理中心憑證實務作業基準第 1.9 版(草案)審查意見表

變更後記載內容	變更後頁數	審查意見
1.3.5.2 信賴憑證者	6	原則同意，建議修訂為(1)檢驗電子件的數位簽章之完整性
2.1.3 發卡中心之職責	11	原則同意
2.1.3 發卡中心之職責	18	原則同意，但請再評估遭廢止之用戶是否還可申請退費。
2.8.1 機密之資訊種類	23	原則同意，建議修訂方式可比照 GCA 此節方式。
2.8.8 隱私權保護	24	原則同意，請考慮個資處理一詞是否已包含所有個資使用範圍。
4.2 簽發憑證之程序	33	原則同意
4.4.3 憑證廢止程序	40-41	原則同意
4.6.2 歸檔之保留期限	55	原則同意
4.7 金鑰更換	57	原則同意
5.1.4 水災防範及保護	61	原則同意，但水災之防護請從全面向考慮，非只考慮淹水因素
5.3.7 聘雇人員之規定	69	原則同意，建議修訂為「除須具備足夠的知識技能與專業倫理，遵守本憑證實務基準相關規定進行，並簽定相關保密協定」，另請再審慎評估營運人員需具備的證照或條件等，或是相關聘僱人員與專任人員之比例。
6.1.1 金鑰對之產製	69-70	原則同意

變更後記載內容	變更後頁數	審查意見
1.3.5.2 信賴憑證者	6	原則同意，建議修訂為(1)檢驗電子件的數位簽章之完整性
6.1.3 公開金鑰安全傳送給工商憑證管理中心	71	原則同意，但建議調整文字順序為本節所指的安全管道為使用專屬通訊協定、資料簽章及加密傳送方式，諸如安全套接層(Security Socket Layer, SSL)通訊協定、憑證管理訊息格式協定(Certificate Management Protocol, CMP)簽章封包、憑證註冊審驗人員簽章等。
6.1.5 金鑰長度	71	
6.2.6 私密金鑰輸入至密碼模組	74	原則同意
6.2.9 私密金鑰之銷毀方式	75	原則同意
6.3.2.1 憑證機構公開金鑰及私密金鑰之使用期限	76	原則同意
6.6.3 生命週期安全評等	80	原則同意
7.1.3 演算法物件識別碼	82	原則同意
7.1.4 命名形式	83	原則同意
7.1.9 關鍵憑證政策擴充欄位之語意處理	83	原則同意

附件4：自然人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
1.2 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，並可從職務、營業或契約等面向，思考保密的範圍
2.8.7 隱私權保護	19	原則同意，請考慮個資處理一詞是否已包含所有個資使用範圍。
3.1.9.3 各憑證管理事項委託代辦	23	原則同意
3.2.2 憑證展期	24	原則同意
3.5 憑證內容變更	25	原則同意
3.6 憑證暫時停用與恢復使用	25	原則同意
4.1.4 憑證到期之展期憑證申請	28	原則同意
4.2.2 臨櫃申請憑證內容變更時	29	原則同意
4.2.3 臨櫃申請展期憑證時	29	原則同意
4.3.1 初次申請憑證與憑證內容變更時	30	原則同意
4.4.7 暫時停用憑證之程序	34	原則同意
4.4.9 恢復使用憑證之程序	36	原則同意
4.5.8 弱點評估	43	針對文內中”憑證管理系統”並

變更後記載內容	變更後頁數	審查意見
		無明確定義。建議可將”憑證管理系統”修改為”憑證管理中心所有系統”，藉以涵蓋全部系統範圍
4.6.2 歸檔之保留期限	44	原則同意
4.6.4 歸檔備份程序	44	原則同意
4.6.5 時戳紀錄之要求	45	原則同意
4.7 金鑰更換	46	原則同意
5.1.4 水災防範及保護	50	原則同意，但水災之防護請從全面向考慮，非只考慮淹水因素
6.1.1 金鑰對之產製	58	原則同意
6.1.3 公開金鑰安全傳送給內政部憑證管理中心	58	原則同意，但建議調整文字順序為本節所指的安全管道為使用專屬通訊協定、資料簽章及加密傳送方式，諸如安全套接層(Security Socket Layer, SSL)通訊協定、憑證管理訊息格式協定(Certificate Management Protocol, CMP)簽章封包、憑證註冊審驗人員簽章等。
6.1.5 金鑰長度	59	原則同意，建議只保留 SHA1 與 SHA256 演算法
6.1.7 金鑰參數品質之檢驗	59	
6.2.1 密碼模組標準	60	原則同意，建議「IC 卡」更新為「安全 IC 卡」
6.2.5 私密金鑰歸檔	61	原則同意

變更後記載內容	變更後頁數	審查意見
6.2.6 私密金鑰輸入至密碼模組	61	原則同意
6.2.9 私密金鑰之銷毀方式	62	原則同意
6.3.2.1 內政部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
6.5.2 電腦安全評等	65	原則同意
6.6.3 生命週期安全評等	65	原則同意
7.1.3 演算法物件識別碼	67	原則同意
7.1.4 命名形式	67	原則同意
7.1.9 關鍵憑證政策擴充欄位之語意處理	68	原則同意

附件 5：醫事憑證管理中心憑證實務作業基準第 1.7 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
1.2 憑證實務作業基準之識別	2	原則同意
1.3.8.1 憑證之適用範圍	7	原則同意，SSL 的中文翻譯方式請參照標檢局
1.4.1 憑證實務作業基準之制定及管理機關	8	原則同意
2.6.4 儲存庫	22	原則同意，請考慮將日曆天改為工作天
2.7.1 稽核之頻率	22	原則同意，請將不定期稽核改正為至少一年一次
3.2.1 憑證之金鑰更換	34	原則同意
4.4.7 暫時停用憑證之程序	45	原則同意，HCA 掌握各民眾特種個資，請再評估註冊窗口上傳資料註冊系統時，是否無須加數位簽章，確認其安全性
4.4.9 恢復使用憑證之程序	47	原則同意，HCA 掌握各民眾特種個資，請再評估註冊窗口上傳資料註冊系統時，是否無須加數位簽章，確認其安全性
6.2.4 私密金鑰備份	72	原則同意，並經「清除」改為「刪除」
6.7 網路安全控管措施	76-77	原則同意

附件 6：政府公開金鑰基礎建設憑證政策第 1.7 版(草案)審查意見表

變更後記載內容	變更後頁數	審查意見
1.2 憑證政策之識別	4	原則同意
2.7.2 稽核人員之身分及資格	20	原則同意
3.8.1 憑證之適用範圍	27	原則同意，建議訂正「條例」用法