行政機關電子憑證推行小組第 28 次委員會議紀錄

一、時間：104 年 4 月 23 日（星期四）下午 2 時 00 分

二、地點：本會寶慶辦公區 513 會議室

三、主席：高副主任委員仙桂

四、出列席單位及人員：(如簽到表)　　記錄：黃柏盛

五、主席致詞：(略)

六、決議：

報告案一：國際稽核要求與憑證中心因應說明

(一) 簡報中用語務求精確，例「SHA-1 憑證」正確用語應為以 SHA-1 演算法簽發之憑證，另第二代雜湊演算法「SHA-2」則有四種演算法，請釐清憑證管理簽發之憑證係採何種雜湊演算法，並更正相關文字。

(二) 有關國際規範之要求及各瀏覽器提出之相關規範，請國發會提供風險及衝擊評估、時程規劃及建議做法，以利各憑證管理中心配合辦理。

(三) 有關 SHA-1 演算法之退場機制及時間表，目前除醫事憑證管理中心(HCA)外，其他各憑證管理中心皆已完成升級 SHA256 演算法，請 HCA 依政府總憑證管理中心規劃時程完成升級作業。

(四) 請持續追蹤各瀏覽器提出之相關規範以及國際趨勢並提早因應，以確保政府 PKI 能符合相關要求。

審查案一：「內政部憑證管理中心憑證實務作業基準第 1.8 版(草案)」修正案

(一) 本次草案取消載具型態限制(不限於 IC 卡型態)，作業基準內容中有關「 IC 卡」之用語改為「符記」，惟部分內容仍有「IC 卡」文字，請檢視是否一致，並再檢查草

案內容中文字用語或敘述不通順部分請內政部一併修改。

(二)原則同意「內政部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1)，請內政部依「電子簽章法」規定函送經濟部審查。

(三)鑒於目前憑證實務作業基準之修訂皆以前一版本為基礎進行修訂，修訂多為內容之增刪，並未考慮整體文件結構，日積月累下導致文件結構紊亂，專有名詞用法不統一等，請內政部憑證管理中心評估該憑證實務作業基準於後續重大更版時一併調整文件結構，並補充相關專有名詞解釋。

七、臨時動議

八、散會：下午3時30分。

附件1：內政部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

原提案修訂內容	依委員建議後修訂內容	變更後頁數	審查意見
摘要 1、主管機關核定文號：經商字第_____號[待定]	同意原提案之修訂	Viii	原則同意
摘要 2、簽發之憑證： …(略) (3) 適用範圍：僅適用於開放網路中的身分識別與資料保護。用戶及信賴憑證者應謹慎使用憑證管理中心所簽發之憑證，並應注意本作業基準使用範圍之限制且不得使用於本作業基準所禁止之範圍。	**摘要** 2、簽發之憑證： …(略) 適用範圍：僅適用於~~開放~~網路中的身分識別與資料保護。用戶及信賴憑證者應謹慎使用憑證管理中心所簽發之憑證，並應注意本作業基準使用範圍之限制且不得使用於本作業基準所禁止之範圍。	Viii	原則同意，並將”開放網路中”改成”網路中”。
摘要 3、認證服務的第三方稽核： 憑證管理中心每年接受二項的第三方稽核：其一為整體認證服務通過國家發展委員會的GPKI憑證機構年度外部稽核；其二為資訊安全管理系統通過ISO27001:2013評鑑。最新的第三方稽核結果請見http://moica.nat.gov.tw/網站。	**摘要** 3、認證服務的第三方稽核： 憑證管理中心每年接受二項的第三方稽核：其一為整體認證服務通過國家發展委員會的 GPKI 憑證機構年度外部稽核；其二為資訊安全管理系統通過 ISO27001: 2013 評鑑。最新的第三方稽核結果請見 http://(請填寫實際網址)網站。	Viii	原則同意，但經查詢該網站並無明確的資料可確認此稽核報告，請修訂實際連結網址。
摘要 4、法律責任重要事項： (2) 用戶或信賴憑證者因使用憑證而發生損害賠償事件時，若可歸責於憑證管理中心或其所屬人員未依本作業基準或相	同意原提案之修訂	ix	原則同意

原提案修訂內容	依委員建議後修訂內容	變更後頁數	審查意見
關規定辦理用戶註冊、憑證簽發或停用、廢止作業，憑證管理中心依 2.2.1.4 所訂賠償範圍內，賠償用戶或信賴憑證者因憑證作業致受有直接損害為限，但不包括間接損害，例如用戶或信賴憑證者因憑證作業致其依通常情形或依已定計劃，預期可取得利益之喪失。			
摘要 4、法律責任重要事項： (6) 用戶之憑證如須暫停使用、恢復使用或廢止，應依照本作業基準相關規定辦理。	同意原提案之修訂	ix	原則同意
摘要 5、其他重要事項： …(略) (4) 憑證管理中心如因故無法正常運作時，用戶及信賴憑證者應儘速尋求其他途徑完成與他人應為之法律行為，不得以憑證管理中心無法正常運作，作為抗辯他人之事由，如因此致第三人對憑證管理中心為任何主張或請求時，均由用戶及信賴憑證者負責，並對造成憑證管理中心的所有損害負賠償責任。	同意原提案之修訂	x	原則同意

原提案修訂內容	依委員建議後修訂內容	變更後頁數	審查意見
1.2 憑證實務作業基準之識別 …(略)本作業基準的最新版本可在以下網頁取得：http://moica.nat.gov.tw/。	**1.2 憑證實務作業基準之識別** …(略)本作業基準的最新版本可在以下網頁取得：http://(請填寫實際網址)	2	原則同意，提供網址連結的部分請修訂為實際連結網址。
1.3.4 卡管中心 用戶憑證金鑰對之符記(Token)須符合6.2.1節規範[新增]，憑證管理中心將委託可信賴的卡管中心進行符記產製及管理作業。符記產製及管理作業包括符記內部產製金鑰對、以亂數設定符記之初始個人識別碼(以下簡稱PIN碼)及符記之配送管理。	同意原提案之修訂	4	原則同意
1.3.7.1 憑證之適用範圍 憑證管理中心所簽發及管理的憑證類別為自然人憑證，且包含簽章用及加密用憑證。 憑證管理中心所簽發的憑證符合憑證政策保證等級第三級之規定，本憑證適用於開放網路中的身分識別及資料保護。	同意原提案之修訂	5	原則同意
2.1.4 卡管中心之職責 (1) 依照 6.1.1.1 節規定，驅動符記使之在內部安全產製用戶之金鑰對。 (2) 以初始碼設定符記初始 PIN 碼。 (3) 統一初始化符記。 (4) 提供符記開卡資料管理作業。 (5) 提供符記鎖卡管理作業。	同意原提案之修訂	9	原則同意

原提案修訂內容	依委員建議後修訂內容	變更後頁數	審查意見
(6) 執行符記配送管理作業。			
2.1.5 用戶之義務 (1) … (略) (2) 在憑證管理中心核定憑證申請並簽發憑證後，用戶應依照 4.3 節規定領取憑證與接受憑證。 (3) … (略) (4) 應妥善保管及使用憑證。 (5) … (略) (6) … (略) (7) 在應用憑證時如因故無法正常運作時，用戶應儘速尋求其他途徑完成與他人應為之法律行為，不得以無法正常運作，作為抗辯他人之事由，如因此致第三人對憑證管理中心為任何主張或請求時，均由用戶及信賴憑證者負責，並對造成憑證管理中心的所有損害負賠償責任。	同意原提案之修訂	9-10	原則同意
2.1.6 信賴憑證者之義務 (1) … (略) (2) 在使用憑證管理中心簽發之憑證時，應先評估與檢驗憑證之保證等級符合其應用系統安全等級需求，同時應對用戶憑證進行驗證，並自行承擔可能產生之相關風險。 (3) … (略) (4) … (略) (5) … (略) (6) 應慎選安全的電腦環境及可信賴的應用系統，	同意原提案之修訂	10-11	原則同意，並增加說明，請信賴憑證者須針對其用戶訂定相關使用者規範

原提案修訂內容	依委員建議後修訂內容	變更後頁數	審查意見
如因電腦環境或應用系統本身因素導致信賴憑證者或其系統用戶權益受損時，應自行承擔責任。 (7) 憑證管理中心如因故無法正常運作時，信賴憑證者應儘速尋求其他途徑完成與他人應為之法律行為，不得以憑證管理中心無法正常運作，作為抗辯他人之事由，如因此致第三人對憑證管理中心為任何主張或請求時，均由用戶及信賴憑證者負責，並對造成憑證管理中心的所有損害負賠償責任。 (8) … (略)			
2.2.1.4 賠償責任 憑證管理中心提供用戶於開放網路中的身分識別及資料保護之服務過程，致用戶受有損害，且可歸責於憑證管理中心或其所屬人員未依本作業基準或相關規定辦理用戶註冊、憑證簽發或停用、廢止作業時，負賠償責任。但憑證管理中心業依本作業基準與相關規定執行作業時，不在此限。 憑證管理中心依前項約定，對於用戶或信賴憑證者所負賠償責任之範圍，均以賠償因憑證作業致受有直接損害為限，但不包括間接損害，例如用戶或信賴憑證者因憑證作業致其依通常情形或依已定計劃，預期可取得利益之喪失之情況，不在賠	同意原提案之修訂	12-13	原則同意

原提案修訂內容	依委員建議後修訂內容	變更後頁數	審查意見
償範圍內。			
2.2.3 卡管中心之責任 卡管中心遵守本作業基準規定之程序，負責驅動符記以產製用戶的金鑰對及相關發卡作業，卡管中心因執行符記管理作業所引發之法律責任由憑證管理中心負責。	同意原提案之修訂	14	原則同意
2.9 智慧財產權 憑證管理中心的金鑰對及金鑰分持為憑證管理中心之智慧財產。用戶使用之符記須符合6.2.1節規範，由憑證管理中心信賴的卡管中心驅動符記，而由符記自行產製金鑰對，該金鑰對屬於該用戶。	同意原提案之修訂	21	原則同意
3.1.7 證明擁有私密金鑰之方式 由憑證管理中心所信賴的卡管中心驅動符記，在符記內部自行產製金鑰對，簽發憑證時由註冊窗口透過安全管道將用戶之公開金鑰傳送至憑證管理中心，因此用戶在申請憑證時不必證明持有私密金鑰。	同意原提案之修訂	23	原則同意
3.1.9.2 各項線上辦理的憑證管理 憑證管理中心有六項憑證管理以線上方式辦理，這些線上辦理作業的身分鑑別方式分別規範如下： (1) … (略) (2) … (略) (3) … (略) (4) … (略)	同意原提案之修訂	24	原則同意

原提案修訂內容	依委員建議後修訂內容	變更後頁數	審查意見
(5) … (略) (6) 線上申請憑證 用戶以現行有效的憑證，並輔以其身分證字號及出生年月日六碼等資訊，經電子簽章來作為身分鑑別之依據。			
4.1.1 憑證申請 1.臨櫃申請憑證時 … (略) 2.集體申請憑證時 … (略) 3.線上申請憑證時 憑證申請人持有效之憑證，依3.1.9.2節規定進行身分鑑別程序，並依照流程辦理線上申請憑證作業。 … (略)	同意原提案之修訂	28-29	原則同意
4.1.3 憑證遺失時之憑證申請 若用戶曾持有憑證，但是因為遺失或損毀而無法使用，可申請新的憑證。在申請之前，必須依4.4.3節的規定先將遺失或損毀之憑證做廢止，然後再依4.1.1節的規定申請新的憑證。	同意原提案之修訂	29	原則同意
4.2.1 申請憑證時 由以下的步驟完成憑證的簽發： 1.臨櫃簽發憑證 (1) … (略) (2) RAO 確認輸入資料正確無誤後，以其 IC 卡對憑證申請資料加簽數位簽章，進行符記產製。 (3) … (略) (4) … (略) (5) 憑證管理中心回傳所簽	同意原提案之修訂	31-32	原則同意

原提案修訂內容	依委員建議後修訂內容	變更後頁數	審查意見
發之憑證，再由註冊窗口系統將簽發的憑證寫入申請人之符記中。 2.線上簽發憑證 (1) 依 3.1.9 節由 RAO 臨櫃或透過線上確認憑證申請人之身分後，將用戶申請資料上傳至註冊中心，並產生一組驗證碼提供給申請者。 (2) 申請者登入線上申請系統並輸入驗證碼進行憑證簽發流程 (3) 註冊中心檢驗申請者輸入之驗證碼無誤後，就以完整的憑證申請訊息向憑證管理中心申請憑證。 (4) 憑證管理中心回傳所簽發之憑證，再由註冊中心將簽發的憑證寫入符記中。			
4.3.1 申請憑證與憑證內容變更時 當完成憑證簽發後，申請者必須親自領取憑證，申請者可視需要使用以下二種方式之一進行接受憑證的作業：一為臨櫃，另一種為線上方式。 臨櫃進行接受憑證時，註冊窗口系統會列印憑證接受確認書給申請者，申請者應檢視憑證接受確認書所列印有關憑證的內容，如確認憑證內容無誤，就應接受所簽發的憑證，在憑證接受確	同意原提案之修訂	34-35	原則同意

原提案修訂內容	依委員建議後修訂內容	變更後頁數	審查意見
認書簽名表示已接受所簽發的憑證，再由RAO以該申請者的憑證簽發憑證接受訊息，完成憑證接受的程序。若申請人委託他人代辦憑證內容變更時，則由受委託人確認憑證內容之正確性，並於憑證接受確認書簽名。 以線上方式進行接受憑證時，註冊窗口系統會呈現憑證接受確認訊息給申請者，申請者應檢視憑證接受確認訊息中有關憑證的內容，如確認憑證內容無誤，就應於註冊窗口系統上點選確認接受所簽發的憑證。			
4.4.7 暫時停用憑證之程序 …(略) 用戶亦可連線至儲存庫申請暫時停用憑證，但須填寫憑證IC卡的卡號或身分識別資料[新增]與其相對的用戶代碼，以作為身分鑑別依據。用戶如忘記用戶代碼，得臨櫃辦理暫時停用憑證，在RAO確認用戶身分後，由RAO代為向憑證管理中心提出暫時停用憑證申請，得併同辦理重設用戶代碼。 用戶如遺失憑證，也忘記用戶代碼，因時空限制，而無法利用上述程序之一辦理憑證暫時停用時，則得以緊急暫時停用憑證程序辦理。……(略)傳真號碼請見本作業基準1.4.2節之客戶服務聯絡資料，相關細部程序與表單公布於http://moica.nat.gov.tw。	**4.4.7 暫時停用憑證之程序** ……(略)傳真號碼請見本作業基準 1.4.2 節之客戶服務聯絡資料，相關細部程序與表單公布於 http://(請提供正確連結)。	38-39	原則同意，提供網址連結的部分請修訂為實際連結網址。另文中傳真號碼於 1.4.2 節並無提供，於網站中也無法直接取得，請確認此敘述是否正確。

原提案修訂內容	依委員建議後修訂內容	變更後頁數	審查意見
4.4.9 恢復使用憑證之程序 …(略) 線上申請恢復使用憑證時，用戶可連線至儲存庫申請恢復使用憑證，須填寫憑證IC卡的卡號或身分識別資料與其相對的用戶代碼，進行身分鑑別程序，以作為判定是否同意恢復使用憑證之依據。 …(略)	同意原提案之修訂	39	原則同意
6.1.1 金鑰對之產製 …(略) 用戶使用之符記須符合6.2.1節規範，其金鑰對是在卡管中心以安全控管機制驅動符記後，在符記內部自行產製，且金鑰對產製完畢後，其私密金鑰將無法由符記中匯出。	同意原提案之修訂	61	原則同意
6.1.2 私密金鑰安全傳送給用戶 憑證管理中心簽發憑證後，由RAO將存有私密金鑰的符記使用權交給用戶。	同意原提案之修訂	61	原則同意
6.1.8 金鑰經軟體或硬體產製 …(略) 卡管中心依照6.2.1節規定，使用符合規範之密碼模組產製用戶之金鑰對。	**6.1.8 金鑰經軟體或硬體產製** …(略) 卡管中心依照6.2.1節規定，使用符合規範之符記產製用戶之金鑰對。	63	原則同意
6.2.1 密碼模組標準 …(略)，用戶是使用通過FIPS140-2安全等級第二級認證的密碼模組。 憑證管理中心所使用的獨立硬體密碼模組是有安全性佐證資料，用戶所使用的符記是有可資公信佐證資料。	**6.2.1 密碼模組標準** …(略)，用戶是使用通過FIPS140-2安全等級第二級認證的符記。 憑證管理中心所使用的獨立硬體密碼模組是有安全性佐證資料，用戶所使用的符記是有可資公信佐證資料。	63	原則同意

原提案修訂內容	依委員建議後修訂內容	變更後頁數	審查意見
6.3 用戶金鑰對管理之其他規定 用戶必須自行管理金鑰對，憑證管理中心不負責保管用戶的私密金鑰。 用戶憑證金鑰對之符記可為不同形式但須符合6.2.1節規範，其中包含簽章用及加密用二種均為有效的憑證。 …(略)	同意原提案之修訂	65	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 憑證管理中心公開金鑰及私密金鑰之金鑰長度為RSA 2048位元，使用期限至多為二十年，以私密金鑰執行簽發憑證用途之使用期限至多為十年，簽發憑證廢止清冊與線上憑證狀態查詢(OCSP)伺服器憑證則不在此限。…(略)	同意原提案之修訂	66	原則同意
			委員於會議中提出，修訂載具後，卡管中心、持卡人等用詞是否須調整，若須修訂請全文一併修訂。 並請確認全文中IC卡相關用詞全數完成修訂。
			委員於會議中提出CPS提及之相關網址均以:http://monica.nat.gov.tw/ 代表，

原提案修訂內容	依委員建議後修訂內容	變更後頁數	審查意見
			不易搜尋相關資料，請列實際網址避免民眾查詢困擾。
	sha-1WithRSAEncryption: {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha1-with-RSA-Signature(5)} sha256WithRSAEncryption: {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256-with-RSA-Signature(11)} sha384WithRSAEncryption: {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha384-with-RSA-Signature(12)} sha512WithRSAEncryption: {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha512-with-RSA-Signature(13)}	70	委員於會議中提出P.70格式剖繪中，為利與oid編碼容易對應，目前sha1 with RSA Encryption之描述{iso(1)…pkcs-1(1)5}建議調整為{iso(1)…PKCS-1(1)sha1-with-RSA-Signature(5)};其他sha256 with RSA Encryption, sha384 with RSA Encryption, sha512 with RSA Encryption建議一併調整。