行政機關電子憑證推行小組第 29 次委員會議紀錄

一、時間：104 年 10 月 26 日（星期一）下午 2 時 00 分

二、地點：本會寶慶辦公區 B136 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：GRCA 自發憑證(new with old)重新簽發說明

決議：

(一) 原則同意以 SHA256 演算法重新簽發 GRCA 自發憑證(new with old)，憑證總管理中心須確保對用戶不會產生影響，並妥善處理後續公告及憑證散佈等相關事宜。

報告案二： Chrome 瀏覽器停止支援 NPAPI(Netscape Plugin Application Programming Interface)影響說明

決議：

(一) 由於此案造成影響之範圍廣泛，雖非憑證本身所造成之影響，但因使用者並不了解此事之原委，因此於操作產生問題時，難以分辨主因，問題容易被歸類為憑證相關之客訴案件，因此除各憑證管理中心本身相關人員須充分了解此案外，還須針對各憑證相關應用系統之主管機關以及開發廠商等利害關係人進行說明，告知相關事由、短期之配套措施以及長期解決辦法，建議各憑證管理中心針對其憑證相關應用系統進行清查，以確認影響

範圍及相關之利害關係人，並將清單交由國發會統籌，通知相關單位以了解此案內容。

(二) 針對一般民眾之說明內容，請憑證管理中心仔細斟酌，務必站在一般民眾角度思考，說明內容務必淺顯易懂，以降低此案所造成之負面影響。

(三) 憑證管理中心之維運團隊須持續追蹤相關之國際規範及要求，針對未來可能發生之改變及要求，提早進行評估及規劃相關應變措施，並提供相關單位建議做法及時程規畫，以確保政府 PKI 能隨時掌握國際趨勢並且符合相關要求，同時將造成之衝擊及影響範圍降至最低。

審查案整體建議

決議：

(一) 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及章節關連性，經多次修訂後導致文件結構紊亂，部分段落敘述完整性不足，相關專有名詞用法不統一，容易造成閱讀及理解上之困難，建議 GPKI 之憑證政策參照最新國際規範及實務需求予以修訂，並請國發會統籌規劃憑證政策及各憑證管理中心之憑證實務作業基準全面更版作業。

(二) 因各憑證管理中心之憑證實務作業基準進行修訂時，皆各自進行，遵循相同規範之修訂(如：寫入憑證內之電子郵件驗證機制)，書寫內容各自表述，缺乏一致性，建議由國發會統籌針對本次修訂中相同之修定內容統一進行調整，藉此提升政府 PKI 相關文件之品質。

（三）憑證實務作業基準中有關「委託公正之第 3 人」之敘述請各憑證管理中心統一用詞為「委託公正第三方」或「委託公正第三人」。

（四）各憑證管理中心之憑證實務作業基準中關於「私密金鑰之啟動方式」文中宣稱採 m-out-of-n 控管，請評估是否需明確定義 m 及 n 的數字，以及相關人員為那些職位的人。

（五）針對各憑證管理中心新增「寫入憑證內之電子郵件驗證」之章節，因電子郵件寫入憑證並非強制性要求，因此建議於標題旁增加「選擇性」之註記。

審查案一：「內政部憑證管理中心憑證實務作業基準第 1.9 版(草案)」修正案

決議：

(一) 請針對本文中有關出生年月日之敘述，部分段落敘述為「出生年月日六碼」，而部分段落則為「出生年月日」，請統一調整文字敘述為「出生年月日」。

(二) 原則同意「內政部憑證管理中心憑證實務作業基準第 1.9 版(草案)」之修訂，請依審查建議(如附件 1)修定後，依「電子簽章法」規定函送經濟部審查。

審查案二：「工商憑證管理中心憑證實務作業基準第 2.0 版(草案)」修正案

決議：

(一) 原則同意「工商憑證管理中心憑證實務作業基準第 2.0 版(草案)」之修訂，請依審查建議(如附件 2)修定後，依「電子簽章法」規定函送經濟部審查。

審查案三：「政府憑證管理中心憑證實務作業基準第 1.8 版(草案)」修正案

決議：

(一) 原則同意「政府憑證管理中心憑證實務作業基準第 1.8 版(草案)」之修訂，請依審查建議(如附件 3)修定後，依「電子簽章法」規定函送經濟部審查。

審查案四：「組織及團體憑證管理中心憑證實務作業基準第 1.8 版(草案)」修正案

決議：

(一) 原則同意「組織及團體憑證管理中心憑證實務作業基準第 1.8 版(草案)」之修訂，請依審查建議(如附件 4)修定後，依「電子簽章法」規定函送經濟部審查。

審查案五：「醫事憑證管理中心憑證實務作業基準第 1.5 版(草案)」修正案

決議：

(一) 有關配合 GRCA 植入 Mozilla 信賴清單之申請，要求「電子郵件信箱寫入憑證之驗證機制」之修訂，於此版修訂中並無相關敘述，請確認是否符合 Mozilla 規範需求，若有必要請參照各憑證管理中心之修訂進行增修。

(二) 本文中 2.1.2 節敘述，「……使用安全套接層通訊協定 256 位元或其他……」與 6.1.3 節「……安全套接層通訊協定 128 位元…..」敘述不一致，請確認「256 位元」是否為誤植再進行修訂。

(三) 原則同意「醫事憑證管理中心憑證實務作業基準第 1.5 版(草案)」之修訂，請依審查建議(如附件 5)修定後，依「電子簽章法」規定函送經濟部審查。

審查案六：「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 2.0 版(草案)」修正案

決議：

(一) 原則同意「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 2.0 版(草案)」之修訂，請依審查建議(如附件 6)修定後，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。

醫事憑證管理中心申請交互認證儀式

(一) 原則同意醫事憑證管理中心申請交互認證，請政府憑證總管理中心完成交互憑證簽發，依規定辦理後續流程。

七、臨時動議

八、散會：下午 4 時 00 分。

附件 1：內政部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

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
1.2 憑證實務作業基準之識別 本作業基準之名稱為內政部憑證管理中心憑證實務作業基準(Ministry of the Interior Certification Authority Certification Practice Statement)，本版本為第___版，公布日期為___年__月__日。本作業基準的最新版本可在以下網頁取得： http://moica.nat.gov.tw/。	同意原提案之修訂	2	原則同意
1.3.3 註冊窗口 註冊窗口可設於各直轄市、縣（市）戶政事務所、本部移民署各縣（市）服務站，或經由憑證管理中心授權核可的組織來擔任。其設置的地點除了在戶政事務所或是授權核可的組織內，另得視需要設立於臨時的機動地點。	同意原提案之修訂	3	原則同意
2.8.7 個人資料保護 憑證管理中心依照個人資料保護法處理用戶之申請資料，憑證內容記載用戶的中文或英文姓名，以及國民身分證統一編號或居留證號碼的後四碼，所以不會因為公布憑證而洩漏個人的國民身分證統一編號或居留證號碼，而個人電子郵件信箱由用戶自行決定是否要記載於	同意原提案之修訂	20	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
憑證，同時用戶得自行決定是否公布其憑證於憑證管理中心儲存庫，以保障申請民眾之個人資料隱私。			
3.1.2 命名須有意義 憑證管理中心就我國籍用戶的名稱是以本部戶役政系統資料庫所儲存的中文姓名為主，就非我國籍用戶的名稱是以本部移民署之入出國及移民署業務管理系統所儲存的中文或英文姓名為主。	同意原提案之修訂	22	原則同意
3.1.4 命名之獨特性 C=TW，CN=本部戶役政系統資料庫所儲存的中文姓名，或移民署之入出國及移民署業務管理系統所儲存的中文或英文姓名，serialNumber=憑證管理中心自動給定對該用戶的唯一序號。	同意原提案之修訂	22	原則同意
3.1.5 命名爭議之解決程序 憑證管理中心允許用戶的姓名相同，但會以 3.1.4 節中唯一識別名稱中的序號(serialNumber)加以區別，以使用戶的名稱可以保持唯一性。	同意原提案之修訂	23	原則同意
3.1.9 個人身分鑑別之程序 **3.1.9.1 初次申請憑證** 註冊窗口的 RAO 在我國籍憑證申請人本人出示國民身分證正本後，應向本部戶役政資料庫查驗該國民身分證是否為有效，並檢驗此國民身分證所記錄的人員是否確實為該申請者，以確認申請者的身分。	同意原提案之修訂	23-24	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
同時也應檢驗申請者的年齡是否為十八歲以上，設有戶籍之國民，且未受監護宣告者。 註冊窗口的 RAO 在非我國籍憑證申請人本人出示居留證後，應向本部移民署之入出國及移民署業務管理系統，查詢持有該居留證者是否為十八歲以上且尚在合法居留期間內，並檢驗該居留證所記錄的人員是否確實為該申請者，以確認申請者的身分。			
3.1.9.2 寫入憑證內之電子郵件驗證 (1) IC卡類憑證 用戶於取得憑證IC卡後，得申請用戶電子郵件信箱寫入憑證。 用戶以憑證IC卡線上提出申請，憑證管理中心將檢驗憑證之數位簽章以鑑別用戶之身分，並寄送電子郵件驗證信至寫入憑證之電子郵件信箱。 用戶須依照驗證信之內容回覆系統，以確認用戶確實擁有該電子郵件信箱之所有權及控制權。 (2) 非IC卡類憑證 用戶得依照需求於申請非 IC 卡類憑證時，一併申請電子郵件信箱寫入憑證。 憑證管理中心除檢查憑證申請書之資料外，須寄送電子郵件驗證信函至寫入憑證內之電子郵件信箱，	**3.1.9.2 寫入憑證內之電子郵件驗證[選擇性]** ..... 用戶須依照驗證信之內容回覆系統，以確認用戶目前確實擁有該電子郵件信箱之所有權及控制權。	24	原則同意，建議「以確定用戶確實擁有該電子郵件信箱之所有權及控制權」改為「以確定用戶目前確實擁有該電子郵件信箱之所有權及控制權」，此外因電子郵件寫入憑證並非強制性要求，因此建議於標題旁增加「選擇性」之註記。

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
用戶須依照驗證信之內容回覆系統，以確認用戶確實擁有該電子郵件信箱之所有權及控制權。			
3.1.9.3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) 線上暫時停用憑證 以4.1.1節中用註冊窗口自行選定的用戶代碼來做為身分鑑別的依據。 (2) 緊急暫時停用憑證 以傳真相關身分證明的文件做為身分鑑別的依據。詳細的身分證明文件如4.4.7節所述。 (3) 線上恢復使用憑證 以4.1.1節中用註冊窗口自行選定的用戶代碼來做為身分鑑別的依據。 (4) 線上申請展期憑證 我國籍憑證用戶得以其現行有效的憑證，並輔以其身分證字號及出生年月日六碼資訊，經電子簽章來做為身分鑑別的依據。 (5) 線上申請屆期憑證換發 我國籍憑證用戶得以其現行有效的憑證，並輔以其身分證字號及個人生日六碼等資訊，經電子簽章來做為	同意原提案之修訂	25-26	原則同意，但本文中部分段落敘述為「出生年月日六碼」，而部分段落則為「出生年月日」，請統一調整敘述方式為「出生年月日」。

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
身分鑑別之依據。 (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等資訊，經電子簽章來做為身分鑑別之依據。 (7) 線上申請電子郵件寫入憑證 用戶以現行有效的憑證，並輔以其身分證字號或居留證號碼及出生年月日等資訊，經電子簽章來做為身分鑑別之依據。			
3.1.9.4 各憑證管理事項委託代辦 我國籍憑證用戶就各項憑證管理作業，除憑證申請及憑證廢止外，其他各項目均得委託他人至各註冊窗口代為辦理，委託人及受委託人應先行填妥並確認自然人憑證代辦事項委託書之內容正確性並親筆簽名或用印，並由受委託人攜帶該委託書及雙方之國民身分證正本至各註冊窗口辦理。	同意原提案之修訂	26	原則同意
3.2.2 憑證展期 憑證展期係指簽發一張與原憑證具有相同憑證主體名稱、金鑰及相關資訊的新憑證，新憑證只對有效期限(notAfter)予以展延一段時間，給予一個新的憑證序號。 我國籍憑證用戶申請憑證展期如以臨櫃方式辦理或	同意原提案之修訂	27	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
委託他人代為辦理時，用戶身分識別及鑑別程序與3.1節規定相同；憑證展期如以線上方式辦理時，用戶身分識別及鑑別程序以現行未廢止及未停用私密金鑰經本管理中心認定可信賴之個人身分鑑別做簽章方式進行之。			
3.5 憑證內容變更 我國籍憑證用戶就憑證內容變更之申請，用戶臨櫃或委託他人代辦之鑑別程序與3.1節規定相同。	同意原提案之修訂	28	原則同意
3.6 憑證暫時停用與恢復使用 我國籍憑證用戶就憑證暫時停用與恢復使用之申請，用戶臨櫃或委託他人代辦之鑑別程序與3.1 節規定相同。	同意原提案之修訂	28	原則同意
4.1.1 憑證申請 1.臨櫃申請憑證時 臨櫃申請憑證時，我國籍憑證申請人應提供本人之國民身分證正本，以供RAO當面確認是否為本人申請。註冊窗口在收到憑證申請資料後，將依本作業基準3.1.9節規定，進行身分鑑別程序，以作為判定是否同意憑證申請之依據。 非我國籍憑證申請人應提供本人之居留證正本，以供RAO當面確認是否為本人申請，註冊窗口在收到憑證申請資料後，將依本作業基準3.1.9節規定，進行身分鑑	同意原提案之修訂	29-30	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
別程序，以作為判定是否同意憑證申請之依據。 2.集體申請憑證時 另由RAO視業務需要機動到各組織內臨櫃受理憑證申請時，我國籍憑證申請人應填具憑證申請書，及提供本人之國民身分證正本，以供RAO當面確認是否為本人申請。RAO再將已確認身分的憑證申請書依本作業基準3.1.9節規定，進行身分鑑別程序，以作為判定是否同意憑證申請之依據。 3.線上申請憑證時 憑證申請人持有效之憑證，可依3.1.9.3節規定進行身分識別程序，並依照流程辦理線上申請憑證作業。 申請者應選定其個人的用戶代碼及電子郵件信箱，以供RAO輸入到註冊窗口系統中。 申請者如欲將電子郵件信箱寫入憑證內，應依照第3.1.9.2節要求辦理。			
4.1.2憑證內容變更時之憑證申請 用戶如有變更個人的姓名或國民身分證統一編號、居留證號碼等身分資料時，則原憑證由憑證管理中心逕行廢止，用戶如再申請有效的憑證，則須以變更後的姓名或國民身分證統一編號、居留證號碼進行憑證的重新申請。申請憑證時，依4.1.1	同意原提案之修訂	30	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
節規定的程序進行辦理。 用戶可視應用的需要變更憑證中所記載的電子郵件信箱，則原憑證由憑證管理中心逕行廢止用戶以更改的電子郵件信箱重新申請憑證時，依4.1.1節規定的程序進行辦理。 上述的憑證內容變更時，憑證管理中心只對用戶最新且有效的二張憑證做內容的變更。			
4.1.4 憑證到期之展期憑證申請 憑證管理中心在 6.3.2.2 節所訂的憑證金鑰對原則使用期限到期後，可以由我國籍憑證用戶自行決定選擇進行金鑰更換或是憑證展期。 當我國籍憑證用戶想要申請展期憑證時，則以原憑證效期為參考，憑證展期申請方式如下：	同意原提案之修訂	31	原則同意
4.1.5憑證屆期線上換發 我國籍憑證用戶就憑證屆期之重新申請，除依照4.1.1之規定臨櫃進行申請外，另外可於憑證到期前六十天內，在網路上進行線上換發申請，憑證申請人應持本人持有且尚未過期之憑證，使用憑證線上換發功能進行換發申請。線上換發之身分鑑別將以本人之電子簽章並輔以其身分證字號及出	同意原提案之修訂	31-32	原則同意，但本文中部分段落敘述為「出生年月日六碼」，而部分段落則為「出生年月日」，請統一調整敘述方式為「出生年月日」。

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
生年月日六碼資訊，以作為判定是否同意憑證申請之依據。			
4.2.1 申請憑證時 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申請人之符記中。 若申請者申請將電子郵件信箱寫入憑證內，應依照第3.1.9.2節要求辦理。	同意原提案之修訂	32-33	原則同意
4.2.2 線上申請屆期憑證換發時 就我國籍憑證用戶，由以下的步驟完成憑證的簽發：	同意原提案之修訂	33	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
4.2.3 臨櫃申請憑證內容變更時 由以下的步驟完成憑證的簽發： (1) RAO確認憑證申請人之身分後，由註冊窗口系統呈現該申請人憑證內容變更的相關訊息。若我國籍憑證申請人委託他人代辦時，其身分鑑別程序與3.1.9.3節規定相同。 (2) RAO核可憑證內容變更的申請後，對憑證內容變更申請資料加簽數位簽章。 (3) 其餘的步驟如4.2.1節的步驟(3)，(4)，(5)。	**4.2.3 臨櫃申請憑證內容變更時** 由以下的步驟完成憑證的簽發： (1) RAO確認憑證申請人之身分後，由註冊窗口系統呈現該申請人憑證內容變更的相關訊息。若我國籍憑證申請人委託他人代辦時，其身分鑑別程序與3.1.9.3節規定相同。 (2) RAO核可憑證內容變更的申請後，對憑證內容變更申請資料加簽數位簽章。 (3) 其餘的步驟如4.2.1節的「臨櫃簽發憑證」步驟(3)，(4)，(5)。	34	原則同意，此段步驟(3)之敘述，參照之章節編號外，請補充章節標題。
4.2.5 線上申請展期憑證時 就我國籍憑證用戶，由以下的步驟完成憑證的簽發： (1) 用戶於內政部憑證管理中心下載線上憑證展期軟體，由系統確認用戶之身分及使用期間。 (2) 將憑證展期申請資料進行簽章後，再透過安全加密管道上傳至註冊中心。 (3) 註冊中心檢驗用戶的簽章，並確認用戶身分及未受監護宣告無誤後，待憑證管理中心完成憑證簽發後，用戶再透過	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
安全加密管道下載憑證並寫入原用戶之符記中。			
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。若我國籍憑證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。	同意原提案之修訂	35-36	原則同意
4.4.1 廢止憑證之事由 1.用戶在以下情形時，必須向註冊窗口提出廢止憑證申請： (1) 懷疑或證實私密金鑰遭到破解。 (2) 憑證所記載之資訊重大改變，足以影響其信賴度。例如用戶的姓名、	同意原提案之修訂	37-39	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
身分證字號或居留證號碼已變更。 (3) 憑證不再需要使用。 (4) 憑證毀損或遭到竊取。 2.憑證管理中心得就下列情形逕行廢止我國籍憑證用戶原有的憑證，毋須事先經過用戶同意，並於廢止後告知用戶廢止原因及相關事項： (1) 確認憑證記載之內容不實。 (2) 確認用戶之私密金鑰遭冒用、偽造或破解。 (3) 確認憑證管理中心之私密金鑰或系統遭冒用、偽造或破解，足以影響憑證之信賴度。 (4) 確認用戶之憑證未依本作業基準規定之程序簽發。 (5) 確認用戶違反本作業基準或相關法令規定。 (6) 依據司法機關正式公文之通知。 (7) 用戶死亡或經死亡宣告者。 (8) 用戶喪失中華民國國籍者。 (9) 用戶做姓名變更者。 (10) 用戶國民身分證統一編號變更者。 (11) 用戶申請憑證內容變更			

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
者。 (12) 用戶申請金鑰更換者。 (13) 受監護宣告者。 (14) 憑證管理中心系統遭破壞(如火災、地震等災害)以致無法復原時。 3.憑證管理中心得就下列情形逕行廢止非我國籍憑證用戶原有的憑證，毋須事先經過用戶同意，並於廢止後告知用戶廢止原因及相關事項： (1) 確認憑證記載之內容不實。 (2) 確認用戶之私密金鑰遭冒用、偽造或破解。 (3) 確認憑證管理中心之私密金鑰或系統遭冒用、偽造或破解，足以影響憑證之信賴度。 (4) 確認用戶之憑證未依本作業基準規定之程序簽發。 (5) 確認用戶違反本作業基準或相關法令規定。 (6) 依據司法機關正式公文之通知。 (7) 用戶死亡或經死亡宣告者。 (8) 用戶回復或取得中華民國國籍。 (9) 用戶做姓名變更者。			

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
(10) 用戶居留證號碼變更者。 (11) 用戶申請憑證內容變更者。 (12) 用戶申請金鑰更換者。 (13) 受監護宣告者或居留期限屆滿。 (14) 憑證管理中心系統遭破壞(如火災、地震等災害)以致無法復原時。 (15) 發生其他經本部移民署撤銷或廢止其居留許可，並註銷其居留證之事由。			
4.4.2 憑證廢止之申請者 憑證管理中心所認可的憑證廢止之申請者可為以下三者： (1) 廢止憑證之用戶。 (2) 依正式公文辦理的司法機關。 (3) 本部移民署。	同意原提案之修訂	39	原則同意
4.4.3 憑證廢止之程序 廢止憑證之用戶須臨櫃辦理，應提供本人之國民身分證或居留證正本，註冊窗口在收到憑證申請資料後，將依本作業基準第三章規定，進行身分鑑別程序，以作為判定是否同意廢止憑證之依據，憑證廢止申請審核通過後，用戶可連線至儲存庫查詢憑證廢止情形。	同意原提案之修訂	39-40	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
若司法機關依正式公文通知廢止特定的憑證，則憑證管理中心將於確認公文後，廢止該憑證。 如本部移民署以系統通知居留證註銷資料，則憑證管理中心將於確認通知內容後，廢止該憑證。			
4.4.7暫時停用憑證之程序 暫時停用憑證之我國籍憑證用戶若臨櫃辦理時，應提供本人之國民身分證正本，註冊窗口在收到憑證暫時停用申請後，將依本作業基準3.1.9節規定，確認用戶身分，以作為判定是否同意暫時停用憑證之依據。用戶也可填寫自然人憑證代辦事項委託書並委託他人臨櫃代辦憑證暫時停用，其身分鑑別程序與3.1.9.3節規定相同。 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與其相對的用戶代碼，以做為身分鑑別依據。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	同意原提案之修訂	41	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
暫時停用憑證程序辦理。用戶須以傳真方式辦理緊急暫時停用憑證，檢附含有可鑑別身分之書面資料，例如：身分證、居留證正反面影本或警察機關報案三聯單，並署名緊急聯絡電話與本人簽名。憑證管理中心收到傳真申請單後會以電話聯絡申請者，洽詢相關問題進行身分鑑別，以作為判定是否同意緊急暫時停用憑證之依據。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。			
4.4.9 恢復使用憑證之程序 用戶在暫時停用憑證後，如需要恢復憑證的使用，得以下列的臨櫃或線上程序完成。 臨櫃申請恢復使用憑證時，申請人應提供本人之國民身分證或居留證正本，註冊窗口在收到申請資料後，比照本作業基準3.1.9節規定，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。用戶也可填寫自然人憑證代辦事項委託書並委託他人臨櫃代辦憑證恢復使用，其身分鑑別程序與3.1.9.3節規定相同。 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	同意原提案之修訂	42	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
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。 如以上之恢復使用憑證申請審核不通過時，憑證管理中心將拒絕恢復使用憑證。			
6.3.2.2用戶公開金鑰及私密金鑰之使用期限 用戶之公開金鑰及私密金鑰之金鑰長度為RSA 1024位元及RSA 2048位元，公開金鑰憑證之使用期限為五年，私密金鑰之使用期限為五年，於效期到期時得展期一次，且為期三年，而使公開金鑰及私密金鑰的使用期限最長為八年。	**6.3.2.2用戶公開金鑰及私密金鑰之使用期限** 用戶之公開金鑰及私密金鑰之金鑰長度為RSA 1024位元或RSA 2048位元，公開金鑰憑證之使用期限為五年，私密金鑰之使用期限為五年，於效期到期時得展期一次，且為期三年，而使公開金鑰及私密金鑰的使用期限最長為八年。	69	原則同意，建議修訂為 1024 位元【或】RSA 2048 位元

附件 2：工商憑證管理中心憑證實務作業基準第 2.0 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 … 2. 簽發之憑證 (1) 種類： 我國登記設立之公司、分公司、商業及有限合夥等事業主體(以下統稱事業主體)憑證(包括簽章用及加解密用的兩種憑證)。 … 3. 法律責任重要事項 … (6) 用戶之憑證如須暫時停用、恢復使用、廢止或重發，應依照本作業基準相關規定辦理，如發生私密金鑰資料外洩或遺失等情形，必須廢止憑證時，應立即通知本管理中心，但用戶仍應承擔異動前所有使用該憑證之法律責任。 … 4. 其他重要事項 … (8) 本管理中心由電子化政府主管機關依政府採購法，委外辦理政府機關公開金鑰基礎建設憑證機構之外部稽核作業，並委託公正之第 3 人，就本管理中心的運作進行稽核。	4. 其他重要事項 … (8) 本管理中心由電子化政府主管機關依政府採購法，委外辦理政府機關公開金鑰基礎建設憑證機構之外部稽核作業，並委託公正之第三方，就本管理中心的運作進行稽核。	viii-xi	原則同意，摘要第 XI 頁:委託公正之第 3 人，宜修正為公正之第【三】人;或是修正為「公正之第三【方】」以利與各憑證管理中心用法一致。

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 序論 工商憑證管理中心憑證實務作業基準...如何遵照憑證政策保證等級第 3 級之規定，進行我國登記設立之公司、分公司、商業及有限合夥等事業主體（以下統稱事業主體）的公鑰憑證(以下簡稱憑證)之簽發及管理作業。	同意原提案之修訂	1	原則同意
1.3.3 發卡中心 本管理中心用戶使用之符記（Token）為 IC 卡時，本管理中心將委託可信賴的發卡中心進行 IC 發卡作業；...。發卡中心並負責將 IC 卡郵寄至事業主體之登記地址給用戶或發放到經授權之單位，由事業主體負責人或其受託人領取。	同意原提案之修訂	4-5	原則同意
1.3.5.1 用戶 本管理中心之用戶，係指記載於本管理中心所簽發憑證的憑證主體名稱(Certificate Subject Name)的個體，以本管理中心負責簽發公司、分公司、商業及有限合夥等事業主體憑證而言，用戶就是公司、分公司商業及有限合夥等事業主體。	同意原提案之修訂	5	原則同意
1.3.6 以委外方式提供認證服務 中華電信股份有限公司接受本部委託，負責本管理中心之建置及系統維運作業。	同意原提案之修訂	7	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
1.3.7.3 憑證之禁止使用情形 (1) 犯罪。 (2) 軍令戰情及核生化武器管制。 (3) 核能運轉設備。 (4) 航空飛行及管制系統。 (5) 法令公告禁止適用之範圍。	同意原提案之修訂	8	原則同意
2.1.4 用戶之義務 … (6) 如須暫時停用、恢復使用、廢止或重發憑證，應依照第 4 章規定辦理，如發生私密金鑰資料外洩或遺失等情形，必須廢止憑證時，應立即通知本管理中心，但用戶仍應承擔異動前所有使用該憑證之法律責任。	同意原提案之修訂	11-12	原則同意
2.2.2.3 責任上限 如因註冊中心審驗錯誤，導致用戶或信賴憑證者遭受損害時，註冊中心與本管理中心之損害賠償責任以民法及電子簽章法所訂之責任範圍為限。	同意原提案之修訂	16	原則同意
2.2.3 發卡中心之責任 發卡中心遵守本作業基準規定之程序，負責產製用戶的金鑰對及相關發卡作業，因可歸責於發卡中心之事由所生損害，由本管理中心負責處理。	同意原提案之修訂	16	原則同意
2.5.4 請求退費之規定 憑證申辦人如依 4.1 節規定申請憑證，如因故無法辦理，	同意原提案之修訂	18	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
所預繳交予本管理中心之費用，得於送交憑證申請書至憑證註冊窗口辦理前提出退費申請。相關規定請至網站查詢： http://moeaca.nat.gov.tw/。			
2.6.1 工商憑證管理中心之資訊公布 … (3) 本管理中心本身之憑證(公布至與該憑證之公開金鑰相對應之私密金鑰所簽發的所有憑證效期到期為止)。 … (8) 憑證政策。	同意原提案之修訂	18-19	原則同意
2.8 資訊保密之範圍 本節說明憑證認證服務過程中，可能取得用戶個人資料之保護機敏性資訊之種類及公開資訊的範圍。	同意原提案之修訂	22	原則同意
2.8.1 機敏性之資訊種類 以下由本管理中心產生、接收或保管之資料，均視為機敏性資訊： … (7) 列為機敏性資訊的營運相關文件。 現職或曾任職於本管理中心之人員，對於因營運、職務所接觸之機敏性資訊或契約規範不得外洩之內容均應負保密責任；現職或曾任職之外部稽核人員亦同。	同意原提案之修訂	22-23	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
2.8.2 非機敏性之資訊種類 (1) 本管理中心儲存庫公布之憑證、已廢止憑證及憑證廢止清冊不視為機敏性資訊。 (2) 識別資訊或記載於憑證的資訊，除特別約定外，不視為機敏性資訊。	同意原提案之修訂	23	原則同意
2.8.4 應司法人員要求釋出資訊 司法機關、監察機關或治安機關如因調查或蒐集證據需要，必須查詢 2.8.1 節機敏性資訊，依法定程序辦理，不對用戶另作通知；惟本管理中心保留向申請查詢之機關收取合理費用之權利。	同意原提案之修訂	23	原則同意
2.8.5 應民事訴訟要求釋出資訊 司法機關如因調查或蒐集證據需要，必須查詢 2.8.1 節機敏性資訊，依法定程序辦理，不對用戶另作通知；惟本管理中心保留向申請查詢之機關收取合理費用之權利。	同意原提案之修訂	23	原則同意
3.1.2 命名須有意義 事業主體憑證之憑證主體名稱必須符合公司法、商業登記法及有限合夥法等對事業主體命名之相關法令規定。	同意原提案之修訂	26	原則同意
3.1.4 命名之獨特性 本管理中心的 X.500 唯一識別名稱為： …	同意原提案之修訂	26-27	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
3. 商業憑證 C=TW L=縣市名稱 O=商業的正式登記名稱 serialNumber=憑證管理中心自動給定對該用戶的唯一序號 4. 有限合夥 C=TW O=有限合夥的正式登記名稱 5. 有限合夥分支機構 C=TW O=有限合夥的正式登記名稱 OU=有限合夥分支機構的正式登記名稱 本管理中心所採用的事業主體正式登記名稱係來自於經濟部公司、商業及有限合夥登記資料。			
3.1.5 命名爭議之解決程序 如發生用戶名稱所有權爭議時，將依照公司法、商業登記法及有限合夥法等相關法令規定處理，並以 3.1.4 節中的唯一序號(serialNumber)加以區別，以使用戶名稱可以保持唯一性。 但是當自動給定的序號發生重複時，本管理中心得以人工給定的方式，而保持序號的唯一，以解決命名爭議的問題。	同意原提案之修訂	27-28	原則同意
3.1.6 商標之辨識、鑑別及角色 依 3.1.4 節規定，本管理中心	同意原提案之修訂	28	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
所採用的事業主體正式登記名稱，係來自於經濟部公司、商業及有限合夥登記資料，商標之辨識及鑑別非本管理中心管轄範圍，如名稱有爭議，用戶應透過相關法令規定之救濟機制處理。			
3.1.8 組織身分鑑別之程序 … 本管理中心逕行發證時，用戶於收受發卡中心寄發之憑證 IC 卡後，應使用線上註冊申請作業，… 用戶 IC 卡正卡憑證使用期限屆滿應予換發時，用戶得於該憑證到期前 2 個月內利用線上申請方式申請換發憑證，註冊中心將驗證 IC 卡正卡之數位簽章來鑑別事業主體之身分。	同意原提案之修訂	29	原則同意
3.1.9 個人身分鑑別之程序 …。如逕行發證需至註冊窗口領取，將以事業主體負責人個人身分證正本以及受託人身分證正本作為事業主體領取憑證之身分鑑別依據。	同意原提案之修訂	30	原則同意
3.1.11 寫入憑證內之電子郵件信箱驗證 因用戶申請符記不同分成以下 2 種驗證方式： (1) 用戶申請符記為 IC 卡 用戶取得 IC 卡後，得於本管理中心網站(http://moeaca.nat.gov.tw)以 IC 卡提出將電子郵件信箱寫入	參考 MOICA、GCA 及 XCA 修訂之敘述	30-31	原則同意，其書寫方式與 MOICA、GCA 及 XCA 不一致，建議是否宜改為一致。

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
憑證之申請，本管理中心檢驗 IC 卡之數位簽章，完成鑑別身分程序後，將寄送電子郵件驗證信至待寫入憑證之電子郵件信箱。用戶依電子郵件驗證信之內容回覆系統後，始完成用戶擁有該電子郵件信箱之所有權及控制權確認。 (2) 用戶申請符記為非 IC 卡 用戶申請非 IC 卡類憑證時，若需將電子郵件信箱寫入憑證中，應於依 4.1.1.1 節辦理申請時於本管理中心網站(http://moeaca.nat.gov.tw)填寫該電子郵件信箱。本管理中心將寄送電子郵件驗證信函至該電子郵件信箱，待用戶依電子郵件驗證信之內容回覆系統後，始完成用戶擁有該電子郵件信箱之所有權及控制權確認。			
3.2.1 憑證之金鑰更換 … 當用戶之私密金鑰使用期限屆滿必須更換金鑰時，應向本管理中心辦理換發憑證作業，得於該憑證到期前 2 個月內辦理申請。其中，正卡憑證得於該憑證到期前以私密金鑰於線上辦理申請。註冊中心將依照 3.1 節規定，對於申請換發憑證之用戶進行識別及鑑別。	同意原提案之修訂	31	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
4.1.1 憑證之申請程序 **4.1.1.1 申請發證程序** … **4.1.1.2 逕行發證程序** … **4.1.1.3 申請憑證 IC 附卡或換發 IC 卡正卡程序** … 若用戶欲將電子郵件信箱寫入憑證中，應依 3.1.11 節規定辦理。	同意原提案之修訂	34	原則同意
4.1.1.1 申請發證程序 … (2) 完成費用繳納後列印憑證申請書，並於憑證申請書上蓋用事業主體之印鑑及代表該事業主體負責人之印鑑，印鑑必須與該事業主體登記設立所使用的印鑑章相符。	同意原提案之修訂	33	原則同意
4.1.1.2 逕行發證程序 本管理中心為因應政策而主動簽發之憑證，於用戶完成 4.3.2 節更改用戶代碼及設定 PIN 碼時，視為完成申請作業。	同意原提案之修訂	33	原則同意
4.1.1.3 申請憑證 IC 附卡或換發 IC 卡正卡程序 用戶申請憑證 IC 卡附卡或依 3.2.1 節規定線上辦理之 IC 卡正卡申請換發程序如下： …	同意原提案之修訂	33-34	原則同意
4.2 簽發憑證之程序 本管理中心或註冊中心在收到憑證申請資料後，應依本	同意原提案之修訂	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
作業基準第 3 章規定，進行以下審核程序，以作為判定是否同意簽發憑證之依據。憑證申請人可逕至本管理中心查詢憑證申請結果與簽發情形，而註冊窗口亦需以公文書方式通知用戶審核結果。若用戶申請將電子郵件信箱寫入憑證，其驗證方式則依第 3.1.11 節方式辦理。			
4.2.1 IC 卡正卡憑證及非 IC 卡類憑證簽發程序 依 3.2.1 節規定線上辦理申請之 IC 卡正卡憑證簽發程序將依照 4.2.2 節規定辦理。	同意原提案之修訂	35	原則同意
4.2.1.1 申請發證審核程序 … (4) 因用戶使用之符記不同分成以下兩種簽發程序： A. 如用戶使用符記為 IC 卡： 經憑證註冊審驗人員檢查通過之憑證申請資料將交由本管理中心所信賴的發卡中心進行發卡作業，發卡作業包括 IC 卡內部產製金鑰對、以亂數設定 IC 卡之初始 PIN 碼、…發卡中心並負責將 IC 卡郵寄至該事業主體之登記地址給用戶。	同意原提案之修訂	35-36	原則同意
4.2.1.2 逕行發證審核程序 … (1) 由註冊窗口發送 IC 卡時，應由事業主體負責人或其受託人攜帶領取通知書（包	同意原提案之修訂	37	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
含事業主體正式登記名稱、統一編號及聯絡人資料等）於領取單上蓋用事業主體暨負責人之印鑑章（與事業主體登記時所使用之印鑑章相符）並攜帶負責人身分證正本以及受託人身分證正本向註冊窗口領取 IC 卡。			
4.2.2 IC 卡附卡簽發程序 採用線上申請方式，使用正卡之數位簽章進行憑證申請，由註冊中心驗證正卡之數位簽章的方式進行，後續簽發程序比照 4.2.1.1 節符記為 IC 卡之簽發步驟。	同意原提案之修訂	37-38	原則同意
4.3.1 申請發證 … (2)如用戶使用非 IC 卡類憑證時，接受憑證之程序如下： A.申請憑證之用戶在收到憑證接受通知電子郵件後，應檢查電子郵件中所列憑證內容是否正確，並連線至本管理中心網站（http://moeaca.nat.gov.tw）進行憑證接受作業。	同意原提案之修訂	38	原則同意
4.3.2 逕行發證 … (1)用戶連線至本管理中心網站 …以供本管理中心作為通知之用。如用戶發現憑證內容不正確，則應停止憑證接受作業。	同意原提案之修訂	39	原則同意
4.4.1 廢止憑證之事由	同意原提案之修訂	40-41	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
… 另外，本管理中心得就下列情形逕行廢止憑證，毋須事先經過用戶同意： … (4) 確認公司或有限合夥已被宣告破產、辦理解散、合併解散、撤銷或廢止登記；分公司或有限合夥分支機構撤銷或廢止；外國公司撤回、撤銷或廢止認許；商業歇業、撤銷。 (5) 確認用戶已變更名稱或統一編號。惟商業憑證用戶名稱所冠縣市名因縣市改制而改變者，不在此限。 … (9) 依用戶登記設立機關或是目的事業主管機關之通知。			
4.4.2 憑證廢止之申請者 (1) 將廢止憑證之用戶。 (2) 事業主體登記設立機關或是目的事業主管機關。	同意原提案之修訂	41	原則同意
4.4.3 憑證廢止之程序 … 事業主體登記設立機關或是目的事業主管機關提出憑證廢止申請時，其程序如下： … (3) 經憑證註冊審驗人員檢查通過之憑證廢止申請資料，將由本管理中心進行憑證廢止，該用戶所有未過期憑證全部廢止。	同意原提案之修訂	42	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
4.4.5 暫時停用憑證之事由 … 另外，本管理中心得就以下情形逕行暫時停用憑證，毋須事先經過用戶同意： (1) 事業主體用戶遭停業時。 (2) 依用戶登記設立機關或是目的事業主管機關之通知。	同意原提案之修訂	43	原則同意
4.4.6 暫時停用憑證之申請者 以下兩者可做為暫時停用憑證之申請者： (1) 將暫時停用憑證之用戶。 (2) 用戶登記設立機關或是目的事業主管機關。	同意原提案之修訂	44	原則同意
4.4.7 暫時停用憑證之程序 … 事業主體登記設立機關或是目的事業主管機關提出暫時停用憑證申請時，其程序如下： (1) 憑證註冊窗口之憑證註冊審驗人員查詢事業主體相關登記資料，確認事業主體已停業登記之狀況。	同意原提案之修訂	45	原則同意
4.4.9 恢復使用憑證之程序 … 事業主體登記設立機關或是目的事業主管機關提出恢復使用憑證申請時，其程序如下： (1) 憑證註冊窗口之憑證註冊審驗人員查詢事業主體相	同意原提案之修訂	47	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
關登記資料，確認事業主體先前暫時停用之事由已消滅。			
4.5.1 被記錄事件種類 (1) 安全稽核 A.任何重要稽核參數之改變，如稽核頻率、稽核事件型態、新舊參數的內容。 B.任何嘗試刪除或修改稽核紀錄檔。 (2) 識別與鑑別 A.嘗試新角色的設定不論成功或失敗。 B.身分鑑別嘗試的最高容忍次數改變。 C.使用者登入系統時身分鑑別嘗試的失敗次數之最大值。 D.如管理者將已被鎖住的帳號解鎖，而且該帳號是因為多次失敗的身分鑑別嘗試而被鎖住的。 E.管理者改變系統的身分鑑別機制，例如從通行密碼改為生物特徵值。 (3) 金鑰產製 本管理中心產製金鑰時（不包括只用在單次或只限1次使用的金鑰產製）。 (4) 私密金鑰之載入和儲存 A.載入私密金鑰到系統元件中。 B.所有為進行金鑰回復的工作，對保存在本管理中心之私密金鑰所做的存取。	同意原提案之修訂	49-53	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) 可信賴公開金鑰的新增、刪除及儲存。 可信賴公開金鑰之改變，包括新增、刪除與儲存。 (6) 私密金鑰之輸出 私密金鑰之輸出 （不包括只使用在單次或只限 1 次使用之金鑰）。 (7) 憑證之註冊 憑證之註冊申請過程。 (8) 廢止憑證 憑證之廢止申請過程。 (9) 憑證狀態改變之核可 核可或拒絕憑證狀態改變之申請。 (10)本管理中心組態設定 本管理中心安全相關之組態設定改變。 (11)帳號之管理 A.加入或刪除角色和使用者。 B.使用者帳號或角色之存取權限修改。 (12)憑證格式剖繪之管理 憑證格式剖繪之改變。 (13)憑證廢止清冊格式剖繪之管理 憑證廢止清冊格式剖繪之改變。 (14)其他 A.安裝作業系統。 B.安裝本管理中心系統。 C.安裝硬體密碼模組。 D.移除硬體密碼模組。 E.銷毀硬體密碼模組。			

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
F.啟動系統。 G.嘗試登入本管理中心的憑證管理作業。 H.硬體及軟體之接收。 I.嘗試設定通行密碼。 J.嘗試修改通行密碼。 K.本管理中心之內部資料備份。 L.本管理中心之內部資料回復。 M.檔案操作（例如產生、重新命名及移動等）。 N.傳送任何資訊到儲存庫公布。 O.存取本管理中心之內部資料庫。 P.任何憑證被破解之申告。 Q.憑證載入符記。 R.符記之傳遞。 S.符記之零值化。 T.本管理中心之金鑰更換。 (15)本管理中心之伺服器設定改變 A.硬體。 B.軟體。 C.作業系統。 D.修補程式（Patches）。 E.安全格式剖繪。 (16)實體存取及場所之安全 A.人員進入本管理中心之機房。 B.存取本管理中心之伺服器。 C.得知或懷疑違反實體安全規定。			

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
(17)異常 A.軟體錯誤。 B.軟體檢查完整性失敗。 C.接收不合適訊息。 D.非正常路由之訊息。 E.網路攻擊(懷疑或是確定)。 F.設備失效。 G.電力不當。 H.不斷電系統（UPS）失敗。 I.明顯及重大網路服務或存取失敗。 J.憑證政策之違反。 K.本作業基準之違反。 L.重設系統時鐘。			
4.5.2 紀錄檔處理頻率 本管理中心每 2 個月檢視 1 次稽核紀錄，追蹤調查重大事件。檢視工作包括驗證稽核紀錄是否被竄改、檢視所有的紀錄項目及檢查任何警示或異常等。檢視稽核紀錄之結果以文件記錄。	同意原提案之修訂	53	原則同意
4.5.3 稽核紀錄檔保留期限 稽核資料現場(on site)保留 2 個月，並依照 4.5.4 節、4.5.5 節、4.5.6 節及 4.6 節紀錄保留管理機制等相關規定辦理。	同意原提案之修訂	54	原則同意
4.7 金鑰更換 本管理中心之私密金鑰依照 6.3.2 節規定定期更換。本管理中心於私密金鑰執行簽發憑證用途之使用期限到期前 2 個月內，更換其用來簽發憑證的金鑰對，並取得政府憑證總管理中心核發之交互憑	同意原提案之修訂	58	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
證。			
4.9 工商憑證管理中心之終止服務 … (2) 本管理中心終止服務時必須： A.廢止所有未廢止或未過期之憑證，並依電子簽章法相關規定進行檔案紀錄之保管及移交。 B.針對憑證未過期而遭廢止之用戶，依比例合理退還其所繳費用，最高以其所繳費用（不含 IC 卡等其他工本費）80%為上限。	同意原提案之修訂	60	原則同意
5.1.1 實體所在及結構 本管理中心機房位於中華電信股份有限公司數據通信分公司，符合儲存高重要性及敏感性資訊的機房設施水準，並具備門禁、保全、入侵偵測及監視錄影等實體安全機制，以防止未經授權存取本管理中心之相關設備。	同意原提案之修訂	61	原則同意
5.1.7 廢料處理 2.8.1 節所述之本管理中心機敏性資訊，文件資料部分在不需使用時，將經碎紙機處理；磁帶、硬碟、磁碟、磁光碟(MO)及其他形式的記憶體，在報廢前，將經格式化程序清除儲存的資料，光碟將被實體銷毀。	同意原提案之修訂	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
5.2.1 信賴角色 … (1) 管理員負責： A.安裝、設定和維護本管理中心系統。 B.建立和維護本管理中心系統之使用者帳號。 C.設定稽核參數。 D.產製和備份本管理中心之金鑰。 (2) 簽發員負責： A.啟動/停止憑證簽發服務。 B.啟動/停止憑證廢止服務。 (3) 稽核員負責： A.對稽核紀錄的查驗、維護和歸檔。 B.執行或監督內部的稽核，以確認本管理中心運作是否遵照本作業基準的規定。 (4) 維運員負責： A.系統設備的日常運作維護。 B.系統的備援及復原作業。 C.儲存媒體的更新。 D.除本管理中心憑證管理系統外之軟硬體更新。 E.網路及網站的維護：建置系統安全與病毒防護機制及網路安全事件的偵測與通報等。 (5) 實體安全控管員負責： 系統的實體安全控管（如機房的門禁管理、防火、防水及空調系統等）。	同意原提案之修訂	64-65	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
5.3.1 身家背景、資格、經驗及安全需求 (1) 人員甄選及進用之安全評估 A.個人性格之評估。 B.申請者經歷之評估。 C.學術、專業能力及資格之評估。 D.人員身分之確認。 E.人員操守之評估。 … (3)人員之任免及遷調管理 如人員之進用、約聘僱條件或契約有所變更，特別是人員離職或約聘僱契約終止時，將遵守維護保密責任之約定。 (4)維護保密責任之約定 本管理中心之相關人員均負維護保密之責任，並簽署保密切結書，不得以口頭、影印、借閱、交付、文章發表或其他方法洩漏機敏性資訊。	同意原提案之修訂	67-68	原則同意
5.3.7 聘雇人員之規定 本管理中心任職之聘雇人員須具備足夠的知識技能與道德規範，遵守本作業基準相關規定，並依循本作業基準相關規定及簽定之相關保密協定進行作業。	同意原提案之修訂	70	原則同意
6.1.1.1 用戶金鑰對的產製 用戶所使用之符記為 IC 卡，其金鑰對由本管理中心所信賴的發卡中心代為產製。…	同意原提案之修訂	71	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
6.2.4 私密金鑰備份 本管理中心私密金鑰以 Triple-DES 或 AES 演算法加密後由硬體密碼模組輸出儲存於硬碟，此加密儲存之私密金鑰將會被複製 1 份至本管理中心備援主機與異地備援機房進行線上備援及離線備援，同時亦以光碟燒錄方式備份，存放至異地安全保險櫃中。	同意原提案之修訂	75	原則同意
6.2.7 私密金鑰之啟動方式 … 用戶使用其他密碼模組時，私密金鑰之啟動方式，可使用之認證鑑別方式包含(但不限於)通行詞組(Pass-Phrase)、個人符記、PIN 碼或生物識別。但輸入的啟動資料必須避免被洩露。	同意原提案之修訂	76	原則同意
6.4.2 啟動資料之保護 …IC 卡移交時新的保管人員必須重新設定 PIN 碼。	同意原提案之修訂	79	原則同意
	1.4.2 聯絡資料 對本作業基準有任何建議，或用戶報告遺失符記等事件，請與本管理中心聯絡，本管理中心之聯絡電話：(02)412-1166，郵遞地址：10048 台北市信義路 1 段 21 號，電子郵件信箱：moeaca@moeaca.nat.gov.tw，請參閱 http://moeaca.nat.gov.tw/。	9	建議修訂本文第 1.4.2 節聯絡資料敘述中「...或用戶報告遺失金鑰等事件...」，針對儲存金鑰之符記修改用詞，聯絡電話的部分請增加區碼，郵遞區號建議以 5 碼更新

附件 3：政府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。	同意原提案之修訂	viii	原則同意
1.1 概要 依據憑證政策的規定，本管理中心是政府機關公開金鑰基礎建設(Government Public Key Infrastructure, GPKI，以下簡稱本基礎建設)的第 1 層下屬憑證機構(Level 1 Subordinate CA)，在本基礎建設中負責簽發及管理政府機關(構)、單位及其所屬的伺服器應用軟體等 3 種憑證(包括簽章用及加解密用的憑證)。 在本作業基準中，將說明本管理中心的憑證作業實務，以確保本管理中心的憑證簽發及管理作業符合憑證政策所訂定之保證等級第 3 級之規定。本作業基準所載明之實務作業規範僅適用於與本管理中心相關之個體，如本管理中心、註冊中心(Registration Authority)、用戶(Subscribers)、信賴憑證者(Relying Parties)及儲存庫(Repository)等。 本管理中心之 SSL 類憑證簽發管理，同意遵循憑證機構與瀏覽器論壇(CA/Browser Forum: http://www.cabforum.org)所發行的 Baseline Requirements the Issuance and Management of Publicly-Trusted Certificates	同意原提案之修訂	1-2	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
正式版本，若本作業基準在SSL類憑證簽發管理上與該論壇規範有牴觸情形，將優先遵循CA/Browser Forum所頒布之條款。 …(略)			
1.2 憑證實務作業基準之識別 本作業基準之名稱為政府憑證管理中心憑證實務作業基準(Government Certification Authority Certification Practice Statement)，本版本為第1.8版，公布日期為___年__月__日。最新版本的本作業基準可在以下網頁取得：http://gca.nat.gov.tw/download/GCA_CPS_v1.8.pdf。	同意原提案之修訂	2	原則同意
1.3.4 儲存庫 儲存庫負責公告由本管理中心所簽發之憑證、憑證廢止清冊(Certificate Revocation List, CRL)及其他憑證相關資訊。 儲存庫提供24小時全天的服務，網址為：http://gca.nat.gov.tw/。	同意原提案之修訂	4	原則同意
3.1.11 寫入憑證內之電子郵件驗證 (1) IC卡類憑證 用戶於取得憑證IC卡後，得申請用戶電子郵件信箱寫入憑證。 用戶以憑證IC卡線上提出申請，憑證管理中心將檢驗憑證之數位簽章以鑑別用戶之身分，並寄送電子郵件驗證信至寫入憑證之電子郵	**3.1.11 寫入憑證內之電子郵件驗證[選擇性]** ..... 用戶須依照驗證信之內容回覆系統，以確認用戶目前確實擁有該電子郵件信箱之所有權及控制權，並確認該電子郵件信箱可代表該機關。	24	原則同意，建議「以確定用戶確實擁有該電子郵件信箱之所有權及控制權」改為「以確定用戶目前確實擁有該電子郵件信箱之所有權及控制權」，並新增針對證明此電子信箱代表此機關有

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
件信箱。 用戶須依照驗證信之內容回覆系統，以確認用戶確實擁有該電子郵件信箱之所有權及控制權。 (2) 非 IC 卡類憑證 用戶得依照需求於申請非IC卡類憑證時，一併申請電子郵件信箱寫入憑證。 憑證管理中心除檢查憑證申請書之資料外，須寄送電子郵件驗證信函至寫入憑證內之電子郵件信箱， 用戶須依照驗證信之內容回覆系統，以確認用戶確實擁有該電子郵件信箱之所有權及控制權。			所之描述。此外因電子郵件寫入憑證並非強制性要求，因此建議於標題旁增加「選擇性」之註記。
3.1.12 網域名稱擁有者識別程序 用戶申請伺服器應用軟體憑證(SSL Certificate)時，憑證管理中心須依照第 3.1.8 節之「一般申請」程序，鑑別該組織真確性；另得使用以下方式查詢該申請之主機網域名稱確實存在且屬該申請者所註冊擁有： ■ 政府 WHOIS 主機-政府中英文網域名稱註冊系統(https://rs.gsn.gov.tw) ■ TWNIC Whois Database (http://whois.twnic.net.tw)	同意原提案之修訂	25	原則同意
4.1 申請憑證之程序 (1) ……(略) (2) ……(略) (3) ……(略) (4) ……(略) 申請憑證時，憑證申請	同意原提案之修訂	27-29	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
人應提供正確資料。為確保政府機關(構)及單位網站之可信賴性，申請SSL類伺服器應用軟體憑證之政府機關(構)及單位，必須確實擁有向政府網際服務網(Government Service Network)之政府中英文網域名稱註冊系統註冊登記之政府網域，始得向本管理中心申請SSL類伺服器應用軟體憑證。 政府機關(構)及單位如欲將電子郵件信箱寫入憑證內，應依照第3.1.11節要求辦理。 為確保電子化政府相關時戳服務的互通性及可信賴性，政府機關所設立的時戳服務機構（Time Stamp Authority，TSA）得向本管理中心申請時戳類伺服器應用軟體憑證。用戶之憑證申請資料，本管理中心及註冊中心將依本作業基準之規定妥善保管。			

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
4.2.1 政府機關(構)、單位憑證之正卡、非 IC 卡類憑證 政府機關(構)、單位憑證之正卡之簽發審核程序如下： (1)註冊窗口之憑證註冊審驗人員檢查憑證申請公文的真偽及申請機關(構)、單位之資格(已遭裁撤或合併之機關(構)、單位不能申請)。 (2)憑證註冊審驗人員檢查憑證申請書之資料，若用戶申請將電子郵件信箱寫入憑證內，應依照第3.1.11節要求辦理。如資料正確無誤，將使用憑證註冊審驗人員之IC卡對憑證申請資料加簽數位簽章後，將相關資料上傳至註冊中心。 (3)..... (4).....	同意原提案之修訂	29-30	原則同意
4.2.3 政府機關伺服器應用軟體憑證 政府機關(構)伺服器應用軟體憑證之簽發審核程序如下： (1) 憑證註冊審驗人員檢查憑證申請公文的真偽及申請機關(構)、單位之資格。 (2) 申請SSL類憑證者，憑證註冊審驗人員須依照第3.1.8節及第3.1.12節完成機關(構)身分鑑別及網域名稱擁有者鑑別程序。 經憑證註冊審驗人員檢查通過之憑證申請資料將由本管理中心簽發憑證，並將憑證以電子郵件方式傳送給用戶。	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
	3.1.4 命名之獨特性 本管理中心的X.500唯一識別名稱為： C=TW，O=行政院，OU=政府憑證管理中心 為使本管理中心所簽發憑證的憑證主體名稱具備獨特性，本管理中心採用以下名稱格式： (1)政府機關(構)憑證 …… (2)政府單位憑證 …… (3)伺服器應用軟體憑證 ……	21	請修訂P.21: A.伺服器應用軟體憑證，宜修正為(3)伺服器應用軟體憑證。

附件 4：組織及團體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：第__號。	同意原提案之修訂	VIII	原則同意
1.2 憑證實務作業基準之識別 本作業基準之名稱為組織及團體憑證管理中心憑證實務作業基準(miXed organization Certification Authority Certification Practice Statement)，本版本為第1.8版，公布日期為___年__月__日最新版本的本作業基準可在以下網頁取得：http://xca.nat.gov.tw/data/XCA_CPS_v1.8.pdf 。	同意原提案之修訂	2	原則同意
1.3.4 儲存庫 儲存庫負責公告由本管理中心所簽發之憑證、憑證廢止清冊(Certificate Revocation List, CRL)及其他憑證相關資訊。 儲存庫提供24小時全天的服務，網址為：http://xca.nat.gov.tw/。	同意原提案之修訂	4	原則同意
3.1.9 寫入憑證內之電子郵件驗證 (3) IC 卡類憑證 用戶於取得憑證IC卡後，得申請用戶電子郵件信箱寫入憑證。 用戶以憑證IC卡線上提出申請，憑證管理中心將檢驗憑證之數位簽章以鑑別用戶之身分，並寄送電子郵件驗證信至寫入憑證之電子郵件信箱。	**3.1.9 寫入憑證內之電子郵件驗證[選擇性]** ..... 用戶須依照驗證信之內容回覆系統，以確認用戶目前確實擁有該電子郵件信箱之所有權及控制權。	23-24	原則同意，建議「以確定用戶確實擁有該電子郵件信箱之所有權及控制權」改為「以確定用戶目前確實擁有該電子郵件信箱之所有權及控制權」，此外因電子郵件寫入憑證並非強制性要

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
用戶須依照驗證信之內容回覆系統，以確認用戶確實擁有該電子郵件信箱之所有權及控制權。 (4) 非 IC 卡類憑證 用戶得依照需求於申請非IC卡類憑證時，一併申請電子郵件信箱寫入憑證。 憑證管理中心除檢查憑證申請書之資料外，須寄送電子郵件驗證信函至寫入憑證內之電子郵件信箱。 用戶須依照驗證信之內容回覆系統，以確認用戶確實擁有該電子郵件信箱之所有權及控制權。			求，因此建議於標題旁增加「選擇性」之註記。
4.1 申請憑證之程序 (1)……(略) (2)……(略) (3)……(略) 用戶如欲將電子郵件信箱寫入憑證內，應依照第3.1.11節要求辦理。 用戶應提供正確之憑證申請資料，本管理中心及註冊中心將依本作業基準之規定妥善保管用戶相關資料。	同意原提案之修訂	26-27	原則同意
4.2.1 憑證正卡 (1)註冊窗口依照3.1.8節的規定，對申請憑證之組織或團體之身分進行識別與鑑別，審查其資格及申請書(已遭撤銷登記、註銷登記或解散之組織或團體不能申請)。 (2)若用戶申請將電子郵件信箱寫入憑證內，應依照第3.1.11節要求辦理，如申請資料正確無誤，憑證註冊審	同意原提案之修訂	27-28	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
驗人員將對憑證申請資料加簽數位簽章後，將相關資料上傳至註冊中心。 (3).....(略) (4).....(略)			
		45 63	建議 5.非技術性安全控管換頁(P45)，7.格式剖繪自本頁頂端開始(P63)

附件 5：醫事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

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：中華民國___年__月__日經商字第_____號	同意原提案之修訂	ix	原則同意
摘要 4、其他重要事項： (3)用戶及信賴憑證者應慎選安全的電腦環境及可信賴的應用系統，如因電腦環境或應用系統本身因素導致用戶及信賴憑證者權益受損時，應自行承擔責任。 (4)本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，不得以本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	xi- xii	原則同意
1 序論 醫事憑證管理中心憑證實務作業基準(Healthcare Certification Authority Certification Practice Statement，以下簡稱本作業	同意原提案之修訂	1	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
基準)係依據政府機關公開金鑰基礎建設憑證政策(Certificate Policy for Government Public Key Infrastructure，以下簡稱憑證政策)訂定，並遵循電子簽章法及其子法「憑證實務作業基準應載明事項準則」、符合 CA/Browser Forum 組織要求等相關規定，說明醫事憑證管理中心(Healthcare Certification Authority, HCA，以下簡稱本管理中心)如何遵照憑證政策保證等級第 3 級之規定，進行醫事領域專業醫事人員、醫事機構及其所屬應用於醫事專門用途的伺服器應用軟體之終端用戶憑證簽發及管理作業。			
1.2 憑證實務作業基準之識別 本作業基準之名稱為醫事憑證管理中心憑證實務作業基準(Healthcare Certification Authority Certification Practice Statement)，本版本為第___版，公佈日期為___年__月__日。本作業基準的最新版本可在以下網頁取得(http://hca.nat.gov.tw/Release.aspx)。	同意原提案之修訂	2	原則同意，(http://hca.nat.gov.tw/Release.aspx)此連結無法直接下載 CPS，請提供可直接下載 CPS 之網址連結。

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
1.3.6.1 用戶 本管理中心認定之憑證實體用戶包括： (1)本部醫事管理系統登記核准之醫事人員。 (2)本部醫事管理系統登記核准之醫事機構。 (3)具有應用於醫事專門用途的伺服器應用軟體(醫事用途由部認定之)所有權的醫事機構。 第(1)項醫事人員用戶使用之符記主要採為IC卡，但用戶也可使用自備之其他安全行動裝置為符記，惟用戶須確保其符記之安全，本管理中心對於用戶不當保管與使用自備符記所造成的損害，亦不負擔任何責任。每個符記可同時儲存簽章用及加解密用兩種憑證。每張卡片存有兩對金鑰對，一為簽章用金鑰對，另一為加解密用金鑰對；行動裝置符記存有一對金鑰對，為簽章用金鑰對。	同意原提案之修訂	5	原則同意
2.1.5 用戶之義務 憑證用戶應負擔以下義務： (1) 詳閱本管理中心公布之本作業基準文件，並應遵守其中所列之相關規定。 (2)保證提供本管理中心註冊中心正確之用戶之註冊資料，並授權依本作業基準所載之規定之範圍內使用該資料。	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
(3)瞭解並遵守本管理中心核發憑證時對金鑰用途之限制，並同意不在設定之用途外不當使用本金鑰。 (4)本管理中心採用高安全度之 RSA 憑證做為私密金鑰儲存設備，用戶應妥善保管及使用私密金鑰並設定安全之個人密碼以確認使用權。 (5)若非由本管理中心代為產製金鑰對之憑證用戶，用戶應自行負責安全產製其金鑰對。 (6)對本管理中心所簽發之伺服器應用軟體憑證，應有保管人對私密金鑰之使用進行瞭解與監控。伺服器應用軟體應採用安全之金鑰管理機制，防止該金鑰遭不正當之複製導致金鑰非法使 (7)本管理中心所簽發之伺服器應用軟體憑證中所指之憑證主體(Certificate Subject)為各該伺服器應用軟體，並以其所有權人或經授權使用之人為用戶。如各該伺服器應用軟體之所有權或使用權發生移轉時，用戶應廢止原憑證並重新申請憑證。 (8) …… (9) …… (10)…… (11) …… (12) 本管理中心如因故無法正常運作時，用戶應儘速尋			

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
求其他途徑完成與他人應為之法律行為，不得以本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。			
2.1.6 信賴憑證者之義務 (1) 在使用本管理中心所簽發之憑證或查詢儲存庫時，必須遵守本作業基準之相關規定。 (2) …… (3) …… (4) …… (5) …… (6) …… (7) 應慎選安全的電腦環境及可信賴的應用系統，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。 (8) 本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，不得以本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	同意原提案之修訂	14	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
損害負賠償責任。			
2.9 智慧財產權 本管理中心的金鑰對與金鑰分持之財產權屬於本部。醫事機構、醫事人員憑證用戶使用之符記(Token)須符合6.2.1節規範，由本管理中心代為產製金鑰對，該金鑰對之財產權屬於該醫事人員、醫事機構。伺服器應用軟體憑證及非以IC卡為符記之醫事人員及醫事機構憑證之金鑰對由憑證用戶自行產製，該金鑰對之財產權屬於該憑證申請單位。	同意原提案之修訂	25	原則同意
3.1.7 證明擁有私密金鑰之方式 (1) 醫事人員、醫事機構IC卡類憑證 由本管理中心之卡管中心驅動 IC 卡，在IC卡內部自行產製金鑰對，簽發憑證時由卡管中心透過安全管道將用戶之公開金鑰傳送至本管理中心，因此用戶在申請憑證時不必證明持有私密金鑰。 (2) 伺服器應用軟體憑證及非IC卡符記之醫事人員及醫事機構憑證由用戶自行產製金鑰對，然後使用金鑰對產生PKCS#10 憑證申請檔並加以簽章，並於申請憑	同意原提案之修訂	31	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
證時將該憑證申請檔交給註冊中心，註冊中心將使用該用戶的公開金鑰驗證該憑證申請檔的簽章，以證明用戶擁有相對應的私密金鑰。			
3.1.9.2 各項醫事人員憑證線上辦理之管理 本管理中心醫事人員憑證線上辦理作業，其作業的身分鑑別方式分別規範如下： (1) 線上暫時停用憑證 以用戶所自行選定的用戶代碼來做為身分鑑別的依據。 (2) 緊急暫時停用憑證 以傳真相關身分證明的文件或線上核對資料做為身分鑑別的依據。 (3) 線上恢復使用憑證 以用戶所自行選定的用戶代碼來做為身分鑑別的依據。 (4) 行動裝置申請憑證 授權醫事機構單位之行動化裝置，以用戶之正卡做為身分鑑別的依據。	同意原提案之修訂	33-34	原則同意
4.1.1 憑證申請 (1)..... (2).....	同意原提案之修訂	37-38	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
(3)..... (4) 伺服器應用軟體憑證及非 IC 卡符記之醫事人員與醫事機構憑證申請 A.由申請之醫事機構之所有人或經授權之使用人，代表申請憑證。 B.由憑證申請人自行產製金鑰對，然後使用金鑰對產生 PKCS#10 憑證申請檔並加以簽章。 C.憑證申請人連線至本管理中心網站(http://hca.nat.gov.tw/)，閱讀 醫事憑證用戶同意書，如同意條款內容則填寫憑證申請書及設定用戶代碼，並將 PKCS#10 憑證申請檔上傳。 D.將憑證申請書以公文書方式函送註冊中心辦理。 E. 採用線上申請方式，連線至本管理中心網站(http://hca.nat.gov.tw/)，在同意條款內容，使用伺服器軟體憑證或非 IC 卡符記醫事人員及醫事機構憑證申請資料加簽數位簽章後，將相關資料上傳至註冊中心。 用戶應提供正確之憑證申請資料，本管理中心及註			

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
冊中心將依本作業基準之規定妥善保管用戶相關資料。			
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	38	原則同意
4.2.1 醫事人員憑證 由以下的步驟完成憑證的簽發： 1. 用戶使用之符記為 IC 卡: (1) 註冊窗口確認憑證申請人之身分資料後，便將憑證申請書的資料(含用戶代碼)輸入/轉入註冊窗口系統中。 (2) 註冊窗口系統將相關憑證申請資料透過安全管道傳送至註冊中心。 (3) 註冊中心進行申辦資料覆核後，透過安全管道傳送至本管理中心簽發憑證。 (4) 本管理中心簽發憑證並同時傳送請求檔至卡管中心進行製卡作業，製卡作業包括 IC 卡內部產製金鑰對、以亂碼設定 IC 卡之初始 PIN 碼、將憑證寫入 IC 卡中及印卡等工作。	2. 用戶使用其他符記: (1).....	39-40	原則同意，第 4.2.1 醫事人員憑證本節內容”2.用戶使用其他符記[新增]”，請將“[新增]”移除。

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) 製卡完成後，卡管中心將 IC 卡郵寄給用戶。 2. 用戶使用其他符記:[新增] (1) 線上申請軟體憑證，使用機構憑證與人員憑證之數位簽章進行申請者，則由註冊中心以線上驗證之數位簽章方式辦理。 (2)經註冊中心複核或驗證通過之憑證申請資料將透過安全管道傳送給本管理中心，本管理中心在簽發憑證後，將以超文件傳輸協定或電子郵件方式傳送給用戶。			
4.3 接受憑證及公布憑證之程序 憑證用戶取得憑證與簽發結果通知後，應查驗下列事項： (1)..... (2)..... (3)..... (4) ..... (5) ..... (6)憑證應於簽發後 90 個日曆天內，完成接受憑證。 未能於憑證簽發後90個日曆天內，完成接受憑證且無主動告知憑證中心事由，則視為拒絕接受憑證，該憑證將自動被廢止，不另行公布。	同意原提案之修訂	42	原則同意
5.1.1 實體所在及結構 本管理中心機房位於衛生福利部 3 樓機房，符合儲存高重要性及敏感性資訊	同意原提案之修訂	62	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
的機房設施水準，並具備門禁、保全、入侵偵測及監視錄影等實體安全機制，以防止未經授權存取本管理中心之相關設備。			
5.1.2 實體存取 本管理中心以保證等級第 3 級的實體控管規定運作。機房共有 4 層門禁，第 1 層和第 2 層分別為衛生福利部全年無休的大門及大樓警衛，第 3 層為機房管理人員執行進出管制，第 4 層為機房人員辨認與門禁密碼磁卡進出系統。 除門禁系統可限制不相干人員接近機房外，機房之監控系統可監控機房之開啟，以防止未經授權存取硬體、軟體和硬體密碼模組等相關設備。	同意原提案之修訂	62	原則同意
5.1.3 電力及空調 本管理中心機房的電力系統，除市電外，另設有發電機(滿載油料可連續運轉 4 小時以上，當實際發生市電中斷供應後，指定人員會視情況即時請供應商補充原料，以達持續運作)及不中斷電源系統(UPS)可提供至少 30 分鐘以上備用電力，並具有市電及發電機的電源自動切換功能，供儲存庫備援資料。 本管理中心機房設有恆溫空調系統，以控制環境的溫度	同意原提案之修訂	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
及濕度，使機房保持最佳運作環境。			
6.1.7 金鑰參數品質之檢驗 本管理中心採用 ANSI X9.31 演算法產生 RSA 演算法所需的質數，該法可保證該質數為強質數(Strong Prime)。 用戶金鑰可於符記內部產生 RSA 演算法中所需的質數，但不保證該質數為強質數。	同意原提案之修訂	72	原則同意

附件3：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1.9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
一　因應有限合夥法立法通過，新增第1.2.1節用戶公鑰憑證的種類中有關有限合夥憑證與有限合夥分支機構憑證之相關說明、第1.3.9 節To-Be-Signed有限合夥憑證格式以及第1.3.10節To-Be-Signed有限合夥分支機構憑證格式。	同意原提案之修訂	7-8 79-87 87-96	原則同意
二　因應內政部憑證中心可提供外來人口自然人憑證之簽發，新增第1.2.1節用戶公鑰憑證的種類中有關外來人口自然人憑證之相關說明及第1.3.19節To-Be-Signed 外來人口自然人憑證格式。	同意原提案之修訂	7-9 165-174	原則同意
三　因應內政部憑證中心可提供外來人口自然人憑證之簽發，修訂第1.3.18節To-Be-Signed自然人憑證格式中有關subjectDirectoryAttributes欄位的欄位說明，將其tailOfCitizenID屬性重新命名為tailOfPersonalID，並修改該屬性相關說明，使之適用於記載憑證Subject為自然人或外來人口自然人之身分識別證號尾碼。	同意原提案之修訂	162-163	原則同意
四　因應內政部憑證中心可提供自然人憑證附卡之簽發，修訂第1.3.18節To-Be-Signed自然人憑證格式中有關subjectDirectoryAttributes欄位的欄位說明，新增cardHolderRank屬性，以區分此憑證Subject之卡片持有人為正卡或附卡持有人。	同意原提案之修訂	162	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
五 因原分公司憑證Subject類別之OID名稱無法正確表達分公司之意，修訂第1.3.7節To-Be-Signed分公司憑證格式中之subjectDirectoryAttributes欄位，修改subjectType屬性內容之OID名稱。	同意原提案之修訂	67	原則同意
六 組織團體憑證原於憑證主體名稱中增加統一編號(serialNumber=統一編號)，藉以區別同一縣(市)出現同名組織團體之現象，但因目前統一編號非必填欄位，且組織團體可自行持憑證正卡進行更改，難以確保其正確性；同時，目前XDS中約有2800多筆組織團體(約8%)未填寫統一編號，因此，建議改以OID識別碼替代統一編號進行區別同一縣(市)之同名組織團體(serialNumber=OID識別碼)，故修訂第1.3.15節To-Be-Signed自由職業事務所憑證格式及第1.3.17節To-Be-Signed其他組織或團體憑證格式中之Subject欄位，修改serialNumber屬性內容為該憑證Subject之OID識別碼。	同意原提案之修訂	132 149	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
七　因應GRCA新增支援OCSP功能的欄位說明，同時，補充修訂GCA/XCA/MOICA/MOEACA/HCA支援OCSP功能之欄位說明，修訂下述19個憑證格式之authorityInfoAccess欄位，新增OCSP功能的AccessDescription屬性說明。 ● 1.3.2 To-Be-Signed 自發憑證格式 ● 1.3.3 To-Be-Signed 交互憑證格式 ● 1.3.4 To-Be-Signed 政府機關憑證格式 ● 1.3.5 To-Be-Signed 政府單位憑證格式 ● 1.3.6 To-Be-Signed 公司憑證格式 ● 1.3.7 To-Be-Signed 分公司憑證格式 ● 1.3.8 To-Be-Signed 商號憑證格式 ● 1.3.11 To-Be-Signed 社團法人憑證格式 ● 1.3.12 To-Be-Signed 財團法人憑證格式 ● 1.3.13 To-Be-Signed 學校憑證格式 ● 1.3.14 To-Be-Signed 醫事機構憑證格式 ● 1.3.15 To-Be-Signed 自由職業事務所憑證格式 ● 1.3.16 To-Be-Signed 行政法人憑證格式 ● 1.3.17 To-Be-Signed 其他組織或團體憑證格式	同意原提案之修訂	25-27 34-36 43-44 52-53 60-61 69-70 77-78 103-104 112-113 121-122 129-130 138-139 146-148 155-156 164-165 181-182 191-192 200-202 210-211	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
● 1.3.18 To-Be-Signed 自然人憑證格式 ● 1.3.20 To-Be-Signed 醫事人員憑證格式 ● 1.3.21.1 To-Be-Signed SSL 類伺服應用軟體憑證格式 ● 1.3.21.2 To-Be-Signed 專屬類伺服應用軟體憑證格式 ● 1.3.21.3 To-Be-Signed 時戳伺服應用軟體憑證格式			
八　因文字誤植的緣故，故修訂下述11個憑證格式之subjectDirectoryAttrubutes欄位，修改SubjectDirectoryAttrubutes屬性的說明，將原本誤植為「政府機關」的文字修正為符合該憑證主體之說明。 ● 1.3.5 To-Be-Signed 政府單位憑證格式 ● 1.3.6 To-Be-Signed 公司憑證格式 ● 1.3.7 To-Be-Signed 分公司憑證格式 ● 1.3.8 To-Be-Signed 商號憑證格式 ● 1.3.13 To-Be-Signed 學校憑證格式 ● 1.3.14 To-Be-Signed 醫事機構憑證格式 ● 1.3.18 To-Be-Signed 自然人憑證格式 ● 1.3.20 To-Be-Signed 醫事人	同意原提案之修訂	50 58 67 75 119 127 162 179 189 199 208	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
員憑證格式 ● 1.3.21.1 To-Be-Signed SSL類伺服應用軟體憑證格式 ● 1.3.21.2 To-Be-Signed 專屬類伺服應用軟體憑證格式 ● 1.3.21.3 To-Be-Signed 時戳伺服應用軟體憑證格式			
九　修訂第1.2.1節用戶公鑰憑證的種類之內容說明，補充「醫事機構」與「醫事人員」等兩種GPKI用戶公鑰憑證種類。	同意原提案之修訂	7	原則同意
十　修訂第1.2.1節用戶公鑰憑證的種類之公司憑證的敘述。	同意原提案之修訂	7	原則同意