行政機關電子憑證推行小組第30次委員會議紀錄

一、時間：105年12月1日（星期四）上午9時30分

二、地點：本會寶慶辦公區513會議室

三、主席：曾副主任委員旭正

四、出列席單位及人員：（如簽到表）　　記錄：黃亦弘

五、主席致詞：（略）

六、決議：

報告案一：GCA/XCA憑證IC卡使用者付費機制規劃

(一) 有關GCA/XCA憑證IC卡收費規劃，請國發會參考政府GPKI規模相近之憑證中心憑證成本結構，請於下次會議針對收費方式提出詳細之規劃及說明，以利委員進行評估。

(二) 考量GCA憑證收費係由各機關編列公務預算，如有緊急需要，其購買行政流程較為繁複，且均由政府預算支應，請國發會評估GCA憑證維持現行由國發會統一購置之可行性。

報告案二：政府網站導入HTTPS安全連線規劃

有關政府網站全部導入HTTPS安全連線規劃，建議由國發會評估導入時程後向各機關說明並提供相關技術諮詢。

報告案三：行動自然人憑證推動說明

(一) 行動自然人憑證應用服務立意良好，惟報告中對於適法性、整體安全管理機制、適用範圍及效力等未進行說明，請內政部憑證管理中心整理資料後於下次會議提出討論。

(二) 行動自然人憑證暫維持目前試行範圍，建議內政部將此議題提至國發會「公共政策網路參與平台眾開講」，徵求民眾意見。

整體建議

(一) 有關各憑證管理中心之憑證實務作業基準中「私密金鑰之啟動方式」m-out-of-n之敘述，如不定義m及n，建議以分持秘密方式說明，或敘明可信任人員為何，並於後續RFC 3647文件架構改版中，一併調整m-out-of-n之敘述方式。

(二) 鑑於國內GPKI體系已發展一段時間，請國發會針對目前憑證之管理、稽核制度、委外管理以及使用者回饋機制提出通盤性之檢視，以精進國內GPKI之發展。

(三) 建議憑證管理中心針對有保存個資之憑證管理中心進行評估，除資安防護外，是否另需針對個資保護通過相關個資保護之驗證(eg:TPIPAS、BS 10012等)(鄭委員仁傑書面意見)。

(四) 建議評估量子電腦進程，及對於PKI架構可能產生之影響(鄭委員仁傑書面意見)。

審查案一：「工商憑證管理中心憑證實務作業基準第2.1版(草案)」修正案

(一) 有關3.1.8、3.1.9、4.2.1三節中「註冊中心須驗證事業主體負責人自然人憑證之數位簽章」之敘述，建議將「數位簽章」之用詞統一改為「電子簽章」。

(二) 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，請依審查建議修訂後，依「電子簽章法」規定函送經濟部審查。

審查案二：「政府機關公開金鑰基礎建設憑證政策第 1.8 版（草案）」修正案

(一) 文中第 4.4 節中要求「稽核紀錄檔至少每月應備份一次」，而第 5.1.8 節中要求「全部資料備份必須 1 星期至少執行一次」，請確認「全部資料之備份」是否包含稽核資料，並於後續 RFC 3647 文件架構改版中統一調整。

(二) 因 CMM 為較舊版本，且於 2000 年已修正為 CMMI(Capability Maturity Model Integration)，目前已發展至 CMMI ver1.3，請將文中提及關於 CMM 之敘述，調整為 CMMI(Capability Maturity Model Integration)。

(三) 原則同意「政府機關公開金鑰基礎建設憑證政策第 1.8 版(草案)」之修訂，請依審查建議修訂後，依「電子簽章法」規定函送經濟部審查。

審查案三：「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 2.1 版(草案)」修正案

(一) 文件中有關工商憑證「商號」之用詞，統一改為「商業」，其他相關文件也請一併修改。

(二) 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，請依審查建議修訂後，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。

(三) 同意重新簽發第二代 GCA 憑證，及重新啟用第一代 GRCA 之金鑰重新簽發 GRCA 自發憑證，並確保對用戶不會產生影響及妥善處理後續公告、憑證散佈等事宜。

七、臨時動議

八、散會：上午 11 時 25 分。

附件1：工商憑證管理中心憑證實務作業基準第2.1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
3.1.4 命名之獨特性 本管理中心的X.500唯一識別名稱為： … 1.公司憑證 C=TW O=公司的正式登記名稱 serialNumber=憑證管理中心自動給定用戶之唯一序號 2.分公司憑證 C=TW L=縣市名稱 O=公司的正式登記名稱 OU=分公司的正式登記名稱 serialNumber=憑證管理中心自動給定用戶之唯一序號 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用戶之唯一序號	同意原提案之修訂	26-28	
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，公司、分公司及商業之命名爭議將以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	同意原提案之修訂	28	原則同意
3.1.8 組織身分鑑別之程序	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
用戶申請憑證時，必須將憑證申請書（包含事業主體正式登記名稱、統一編號及聯絡人資料等）蓋用事業主體登記及負責人之印鑑章（與事業主體登記時所使用之印鑑章相符）送交憑證註冊窗口。註冊中心將確認該事業主體確實存在，並驗證申請書上印鑑章之真確性。 當已完成事業主體登記之用戶使用事業主體之負責人自然人憑證，以線上申辦方式申請憑證時，註冊中心須驗證事業主體負責人自然人憑證之數位簽章，並確認該負責人是否具代表該事業主體之資格，以鑑別事業主體之身分。			
3.1.9 個人身分鑑別之程序 於逕行發證使用線上註冊申請作業時，註冊中心將以事業主體負責人個人身分證號碼及其民國年出生年月日作為事業申請憑證之身分鑑別依據。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。 當已完成事業主體登記之用戶使用事業主體之負責人自然人憑證，以線上申辦方式申請憑證時，註冊中心須驗	同意原提案之修訂	30-31	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
證事業主體負責人自然人憑證之數位簽章，並確認該負責人是否具代表該事業主體之資格，以鑑別事業主體之身分。			
4.1.1.1 申請發證程序 用戶以紙本憑證申請書提交予憑證註冊窗口之申請憑證IC卡正卡或申請非IC卡類憑證程序： … (3)憑證申辦人將憑證申請書，送交該事業主體登記設立主管機關所設的憑證註冊窗口辦理。 用戶以事業主體負責人自然人憑證申請憑證IC卡正卡或申請非IC卡類憑證程序： (1) 憑證申辦人連線至本管理中心網站（http://moeaca.-nat.gov.tw），閱讀用戶約定條款（Subscriber Agree-ment），如同意條款內容則填寫憑證申請書，並設定用戶代碼。 (2) 以事業主體負責人自然人憑證對非IC卡或IC卡正卡之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並完成費用繳納。	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
4.1.1.3 申請憑證 IC 附卡或換發 IC 卡正卡程序 … (2)以事業主體憑證 IC 卡正卡對 IC 卡附卡或 IC 卡正卡之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並完成費用繳納。	同意原提案之修訂	35-36	原則同意
4.2.1.1 申請發證審核程序 … 若上述 IC 卡正卡依 3.2.1 節規定辦理重新申請，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，後續發卡作業比照上述符記為 IC 卡之簽發程序。 當用戶使用事業主體之負責人自然人憑證，以線上申辦方式申請憑證時，註冊中心須驗證事業主體負責人自然人憑證之數位簽章，並確認該負責人是否具代表該事業主體之資格，後續則比照上述之簽發程序辦理。	同意原提案之修訂	36-38	原則同意
	1.4.2 聯絡資料 對本作業基準有任何建議，或用戶報告遺失金鑰等事件，請與本管理中心聯絡，本管理中心之聯絡電話：(02)412-1166，…	9	建議連絡電話加上區域號碼

附件 2：政府機關公開金鑰基礎建設憑證政策第 1.8 版 (草案)審查意見表

<table>
<tr><th>原提案修訂內容</th><th>依委員建議後修訂內容</th><th>變更後頁數</th><th>審查意見</th></tr>
<tr><td>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1.8版，公布日期為_年_月_日。</td><td>同意原提案之修訂</td><td>4</td><td>原則同意</td></tr>
<tr><td>3.1.8 組織身分鑑別之程序
對於組織(Organization)身分鑑別所需之證件數量、鑑別確認程序及是否需臨櫃辦理等，以保證等級不同有不同之規定，如下表所列：
<table>
<tr><th>保證等級</th><th>組織身分鑑別之程序</th></tr>
<tr><td>測試級</td><td>不做規定。</td></tr>
<tr><td>第1級</td><td>(1)……</td></tr>
<tr><td>第2級</td><td>(1)……</td></tr>
<tr><td>第3級</td><td>組織身分鑑別分為以下兩種情形：
(1)政府機關(構)或單位之身分鑑別……
(2)民間組織之身分鑑別
……民間組織如於申請憑證前已依法完成向主管機關設立登記程序或已於憑證機構、註冊中心或憑</td></tr>
</table></td><td>同意原提案之修訂</td><td>28</td><td>原則同意</td></tr>
</table>

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
保證等級	組織身分鑑別之程序			
	證機構信賴之機構或個人（例如公證人）完成符合上述規定之臨櫃識別與鑑別程序，並且留下登記或識別與鑑別之佐證資料（例如留下印鑑章圖記或由公證人在申請書上加蓋認證戳記等），則憑證機構或註冊中心得允許該組織於申請憑證時出示佐證資料來取代上述識別與鑑別方式。民間組織如於申請憑證前，其組織代表人已依 3.1.9 節中保證等級第三級之規定鑑別身分，則憑證機構或註冊中心得允許該組織代表人持其自然人憑證為該組織線上提出申請。[新增]……			
第 4 級	……			
			14	文中敘述「正確查驗憑證廢止及停用清冊」關於「停用清冊」一詞未見明確定義，請確認。

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2.1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　因應微軟Trusted Root Certificate Program的最新要求：「2017年2月1日起，所有用戶憑證皆須包含擴充欄位『增強金鑰使用方法(Extended Key Usage)』，用以說明該憑證之延伸用途」，修訂「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1.2.3節用戶公鑰憑證的欄位中有關extKeyUsage擴充欄位的標示說明，將該欄位修改為必要擴充欄位；同時，修訂GCA、XCA、MOICA、MOEACA、HCA以及伺服應用軟體之憑證格式，新增extKeyUsage欄位，以表示該憑證之延伸用途，修訂範圍包括下述18個憑證格式，修訂內容為新增下述18個憑證格式中有關extKeyUsage欄位的欄位說明。 ● 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 ● 1.3.9 To-Be-Signed 有限合夥憑證格式 ● 1.3.10 To-Be-Signed 有限合夥分支機構憑證格式 ● 1.3.11 To-Be-Signed 社團法	同意原提案之修訂	12 42-43 51-52 61 70-71 79-80 89 98-99 108 117-118 126-127 136-137 145-146 155 164-165 174 183-184 193 213	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 ● 1.3.18 To-Be-Signed 自然人憑證格式 ● 1.3.19 To-Be-Signed 外來人口自然人憑證格式 ● 1.3.20 To-Be-Signed 醫事人員憑證格式 ● 1.3.21.2 To-Be-Signed 專屬類伺服應用軟體憑證格式			
二　因應內政部憑證管理中心可提供行動自然人以及金門縣民卡之憑證簽發，修訂自然人憑證格式之subjectDirectoryAttributes欄位的cardHolderRank屬性，新增持卡人為正卡、附卡與行動載具時的相關說明。修訂內容如下 修訂「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1.3.18節To-Be-Signed自然人憑證格式中有關subjectDirectoryAttributes欄位屬性的相關說明。	同意原提案之修訂	173	原則同意，但請確認cardHolderRank此欄位之說明：「此屬性用來區分此憑證Subject之卡片持有人的是正卡或附卡持有人」此句語意是否正確。

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
三　因應公司同名但統編不同時亦可申請憑證之需求，修訂公司憑證格式與分公司憑證格式之subject欄位，新增DN項目serialNumber，用於記錄憑證管理中心自動給定用戶之唯一序號。此外，亦修訂商號憑證格式之subject欄位，修改DN項目serialNumber為記錄憑證管理中心自動給定用戶之唯一序號。修訂內容如下：修訂「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1.3.6節To-Be-Signed公司憑證格式、第1.3.7節To-Be-Signed分公司憑證格式以及第1.3.8節To-Be-Signed商號憑證格式中有關subject欄位的相關說明。	同意原提案之修訂	56 65 75	原則同意
四　依據CA/Browser Forum Baseline Requirements文件之規定，修訂SSL類伺服應用軟體憑證格式之serialNumber欄位，補充說明憑證序號需透過加密安全虛擬亂數產生器（Cryptographically Secure Pseudorandom Number Generator，CSPRNG）所產生之相關說明 。修訂內容如下：修訂「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1.3.21.1節To-Be-Signed SSL類伺服應用軟體憑證格式中有關serialNumber欄位的相關說明	同意原提案之修訂	196-197	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　依據CA/Browser Forum Baseline Requirements文件之規定，修訂SSL類伺服應用軟體憑證格式之subjectAltName欄位，修改此欄位為必要欄位(Required)，以及修改此欄位可記錄的資訊內容為憑證簽發對象(Subject)之完全吻合網域名稱或網路位址。修訂內容如下：修訂「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1.3.21.1節To-Be-Signed SSL類伺服應用軟體憑證格式中有關subjectAltName欄位的相關說明。	同意原提案之修訂	202	原則同意
六　因應憑證與憑證廢止清冊格式剖繪之規格所遵循的國際規範已提供新版標準，因此，將「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」中提及之標準「RFC 3280」修改為新版標準「RFC 5280」，同時，更新參考文獻來源說明。修訂範圍包括下述4個章節與23個憑證格式，修訂內容為修訂「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」中提及標準「RFC 3280」之相關說明，包括第1.1.2節CA公鑰憑證的設計原則、第1.2.2節用戶公鑰憑證的設計原則以及第2.2節憑證廢止清冊的設計原則等3個章節、下述23個憑證格式中有關authorityInfoAccess擴充欄位的AccessDescription之欄位說明、以及SSL類伺服應用軟體憑證格式、時戳伺服應用軟體憑證格式、OCSP伺服器憑證格式等3個憑證格式之extKeyUsage欄位，同時，修訂第3章節參考文獻中有關標準「RFC 5280」之內容。	同意原提案之修訂	2 10 26 35 45 54 63-64 73 82 91-92 101 110 120 129 139 148 157 167 176 186 195 203-206 215 222 224-225 230 232 257-258	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
● 1.1.2 CA 公鑰憑證的設計原則 ● 1.2.2 用戶公鑰憑證的設計原則 ● 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 ● 1.3.9 To-Be-Signed 有限合夥憑證格式 ● 1.3.10 To-Be-Signed 有限合夥分支機構憑證格式 ● 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			

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
● 1.3.17 To-Be-Signed 其他組織或團體憑證格式 ● 1.3.18 To-Be-Signed 自然人憑證格式 ● 1.3.19 To-Be-Signed 外來人口自然人憑證格式 ● 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 ● 1.3.22 To-Be-Signed OCSP 伺服器憑證格式 ● 2.2 憑證廢止清冊的設計原則 ● 3 參考文獻			
七　因文字遺漏，故修訂財團法人憑證格式之signature欄位，新增簽章演算法sha256WithRSAEncryption之OID資訊。修訂內容如下：修訂「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1.3.12節To-Be-Signed財團法人憑證格式中有關signature欄位的欄位說明。	同意原提案之修訂	111	原則同意
八　因文字誤植，故修訂財團法人憑證格式之subjectDirectoryAttrubutes欄位，修改其entityOID屬性的說明，將原用詞為「社團法人」的文字修正為「財團法人」。修訂內容如下：修訂「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1.3.12節To-Be-	同意原提案之修訂	117	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
Signed財團法人憑證格式中有關subjectDirectoryAttrubutes欄位的相關文字。			
九　因文字誤植，故修訂醫事機構憑證格式之subjectDirectoryAttrubutes欄位，修改其cardHolderRank屬性的說明，將原用詞為「副卡」的文字修正為「附卡」。修訂內容如下修訂「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1.3.14節To-Be-Signed醫事機構憑證格式中有關subjectDirectoryAttrubutes欄位的相關文字。	同意原提案之修訂	135-136	原則同意
十　因英文拼音有誤，故修訂SSL類伺服應用軟體憑證格式、時戳伺服應用軟體憑證格式以及OCSP伺服器憑證格式等3個憑證格式的extKeyUsage欄位，將該欄位中英文拼音為「Extneded」的文字修正為「Extended」。修訂內容如下：修訂「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1.3.21.1節To-Be-Signed SSL類伺服應用軟體憑證格式、第1.3.21.3節To-Be-Signed 時戳伺服應用軟體憑證格式、以及第1.3.22節To-Be-Signed OCSP伺服器憑證格式等3個憑證格式之extKeyUsage欄位的欄位說明。	同意原提案之修訂	203 222 229	原則同意
十一　因贅字造成語句不順，故修訂專屬類伺服應用軟體憑證格式與時戳伺服應用軟體憑證格式的subjectAltName欄位，刪除其說明資訊中的贅字「或」。修訂內容如下：修訂「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1.3.21.2節To-Be-Signed專屬類伺服應用軟體憑證格式以及第1.3.21.3節To-Be-	同意原提案之修訂	212 221	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
Signed 時戳伺服應用軟體憑證格式之subjectAltName欄位的欄位說明。			
十二　因文字誤植，故修訂自發憑證格式之certificatePolicies欄位的說明，將原用詞為「Cross Certificate」的文字修正為「Self-Issued Certificate」。修訂內容如下：修訂「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1.3.2節To-Be-Signed自發憑證格式中有關certificatePolicies欄位的相關文字。	同意原提案之修訂	21-22	原則同意
十三　依據微軟Trusted Root Certificate Program技術條款以及CA/Browser Forum之最新規範及其Baseline Requirements文件之規定，各類SSL憑證皆須依其憑證類別，於其擴充欄位certificatePolicies新增符合該憑證類別之CA/Browser Forum定義的Certificate Policy OID，且簽發該SSL憑證之CA憑證與自發憑證亦須包含該新增之Certificate Policy OID，故修訂自發憑證格式、交互憑證格式以及SSL類伺服應用軟體憑證格式的certificatePolicies欄位，新增有關該憑證類別使用CA/Browser Forum定義之Certificate Policy OID的相關說明。修訂內容如下：修訂「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1.3.2節To-Be-Signed自發憑證格式、第1.3.3節To-Be-Signed交互憑證格式以及第1.3.21.1節To-Be-Signed SSL類伺服應用軟體憑證格式之certificatePolicies欄位的欄位	同意原提案之修訂	22 31 201-202	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
說明。			