# 行政機關電子憑證推行小組第31次委員會議紀錄

一、時間：106年7月12日（星期三）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：政府根憑證植入瀏覽器信賴清單現況說明**

同意產製第1.5代GRCA金鑰，並重新啟用第一代GRCA之金鑰對第1.5代GRCA金鑰簽發自發憑證，並妥善處理後續公告、憑證散佈等事宜。

**報告案二： HCA行動化憑證規劃說明**

原則同意HCA行動化憑證之規劃，請妥善處理後續試辦執行等相關事宜。

**整體建議**

(一) 原則同意申請組織及團體憑證(XCA)向用戶收取新臺幣420元之憑證製發相關費用，收費時程授權國發會決定後實施；政府憑證(GCA)收費部分，考量電子化政府整體運用及簡化機關購買之行政流程，仍維持由國發會統一編列預算購置；另針對國營事業因具營利特性且符合工商憑證申請資格，請國發會評估改為申請工商憑證之可行性，惟因修改憑證類別涉及後端應用程式修改，請國發會訂定相關期程後辦理。

(二) 本委員會召開之主要目的係針對憑證相關政策、發展及技術規範進行討論，後續召開委員會議宜就前述議

題進行討論，至於各憑證管理中心作業基準文件修訂，建議簡化審查流程，以提升會議效率。

(三) GPKI 各文件主要提供國內民眾及憑證利害關係人進行閱覽，而非提供給國外人士，爰文件應以國內用語為主，另建議將「數位簽章」之用詞統一改為「電子簽章」。

(四) 行動自然人憑證應用服務立意良好，考量現行採雲端保密器方案尚有管理用戶私鑰之疑慮，為兼顧既有行動自然人憑證用戶及已導入行動自然人憑證應用服務廠商之相關權益，同意在現行範圍內續試辦 1 年，請內政部憑證管理中心評估其他行動化方案之可能性。

(五) 有關 GPKI 各 CPS 中異地備援章節，請依照 GPKI CP 第5.1.8節之敘述方式敘述並區別「全部資料」及「稽核資料」之備份方式。

(六) 請補述 GPKI 各文件專有名詞說明(如 ITUT-T、X.509 及何謂保證度)，俾利用戶了解，提高文件可讀性。

**審查案一：「政府機關公開金鑰基礎建設憑證政策第1.9版(草案)」修正案**

原則同意「政府機關公開金鑰基礎建設憑證政策第1.9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。

**審查案二：「政府憑證總管理中心憑證實務作業基準第1.5版（草案）」修正案**

原則同意「政府憑證總管理中心憑證實務作業基準第1.5版(草案)」之修訂，請依審查建議修訂後，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1.9版（草案）」修正案**

原則同意「政府憑證管理中心憑證實務作業基準第1.9版(草案)」之修訂，請依審查建議修訂後，依「電子簽章法」規定函送經濟部審查。

**審查案四：「工商憑證管理中心憑證實務作業基準第2.2版(草案)」修正案**

原則同意「工商憑證管理中心憑證實務作業基準第2.2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。

**審查案五：「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2.2版(草案)」修正案**

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2.2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。

七、臨時動議

八、散會：上午12時30分。

附件1：政府機關公開金鑰基礎建設憑證政策第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 |
|---|---|---|---|
| **1.1.2憑證政策及憑證實務作業基準之關係**<br>憑證機構必須於憑證實務作業基準中說明如何達成所引用本憑證政策之保證等級。<br>本憑證政策及有簽發伺服器應用軟體憑證之憑證機構，須另遵循憑證機構與瀏覽器論壇（CA/Browser Forum）所發行之 Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates 正式版本(http://www.cabforum.org)，同時針對該正式版本中第1.2.1節所列各項要求，本憑證政策皆配合辦理(參照附錄1)。 | 同意原提案之修訂 | 3-4 | 原則同意 |
| **1.2憑證實務作業基準之識別**<br>本政策之名稱為政府機關公開金鑰基礎建設憑證政策(Certificate Policy for the Government Public Key Infrastructure)，本版本為第1.9版，公布日期為__年__月__日。<br>本憑證政策定義五個保證等級的憑證政策物件識別碼，註冊於id-tw-gpki arc之下：<br>id-tw OBJECT IDENTIFIER ::= {2 16 886}<br>id-tw-gov OBJECT IDENTIFIER ::= {id-tw | 同意原提案之修訂 | 4-6 | 原則同意 |

<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>
101}<br>
id-tw-gpki OBJECT IDENTIFIER ::= {id-tw-gov 0}<br>
id-tw-gpki –certpolicy OBJECT IDENTIFIER ::= {id-tw-gkpi 3}<br>
表1-1憑證政策物件識別碼
<table>
<tr><th>保證等級</th><th>物件識別碼名稱</th><th>物件識別碼值</th></tr>
<tr><td>測試級</td><td>id-tw-gpki-certpolicy-testAssurance</td><td>{id-tw-gpki-certpolicy 0}</td></tr>
<tr><td>第1級</td><td>id-tw-gpki-certpolicy-class1Assurance</td><td>{id-tw-gpki-certpolicy 1}</td></tr>
<tr><td>第2級</td><td>id-tw-gpki-certpolicy-class2Assurance</td><td>{id-tw-gpki-certpolicy 2}</td></tr>
<tr><td>第3級</td><td>id-tw-gpki-certpolicy-class3Assurance</td><td>{id-tw-gpki-certpolicy 3}</td></tr>
<tr><td>第4級</td><td>id-tw-gpki-certpolicy-class4Assurance</td><td>{id-tw-gpki-certpolicy 4}</td></tr>
</table>
本憑證政策於伺服器應用軟體憑證之簽發遵循憑證機構與瀏覽器論壇(CA/Browser Forum)所發行的Baseline Requirements Ceritificate Policy for the Issuance and Management of Publicly-Trusted Certificates 現
</td><td></td><td></td><td></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 |
| --- | --- | --- | --- |
| 行正式版本(http://www.cabforum.org)，若本憑證政策或憑證機構之憑證實務作業基準於伺服器應用軟體憑證之簽發上有任何與 Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates 現行正式版本不一致的情形，將優先遵循 Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates 的條款。<br>下屬憑證機構(目前僅有政府憑證管理中心)其憑證簽發符合 CA/Browser Forum Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates 並通過 AICPA/CPA SM/TM WebTrust Principles and Criteria for Certification Authorities–SSL Baseline with Network Security 外稽標準者，下屬憑證機構的憑證及用戶之伺服器應用軟體憑證可使用 CA/Browser Forum 之組織驗證(Organization Validation, OV) SSL 憑證政策物件識別碼，其物件識別碼為{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) organization-validated(2)} (2.23.140.1.2.2)。 | | | |
| **2.2.1.1保證範圍及其限制條件**<br>如憑證機構在簽發的憑 | 同意原提案之修訂 | 16 | 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 |
| --- | --- | --- | --- |
| 證中，引用憑證政策所訂的任何保證等級之物件識別碼，即表示該憑證機構保證其所簽發憑證之內容資訊已遵守憑證政策之規定。除非憑證機構確實遵守憑證政策之規定，否則不得在所簽發的憑證中引用憑證政策所訂的任何保證等級之憑證政策物件識別碼。<br><br>憑證機構如有簽發伺服器應用軟體憑證，須另遵循憑證機構與瀏覽器論壇（CA/Browser Forum）所發行之 Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates 正式版本 (http://www.cabforum.org)。 | | | |
| **2.4.2可分割性、存續、合併及公告通知**<br>如本憑證政策的任一章節不正確或無效時，其他章節仍然有效，憑證政策的修訂依照8.1節規定。<br><br>本憑證政策另遵循憑證機構與瀏覽器論壇(CA/Browser Forum)所發行的Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates 正式版本 (http://www.cabforum.org)，惟Baseline Requirements 相關規定與本政策所依循之我國相關法律或法規產生衝突時，本政策得小幅度調整相關作法以滿足法律或法規之要 | 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 |
| --- | --- | --- | --- |
| 求，並將變更調整之部分通知 CA/Browser Forum；若我國法律或法規已不再適用時，或 Baseline Requirements 修訂相關內容使其規定可相容於我國法律時，則本政策需撤除並修訂原先所調整修訂之內容，上述作業須於90天內完成。 | | | |
| **4.8.1緊急事件與系統遭破解之處理程序**<br>憑證機構依據緊急事件與系統遭破解的種類執行相關復原程序，並定期執行必要的資料備份作業。<br><br>**※原4.8.1~4.8.4節更改標號為4.8.2~4.8.5節** | 同意原提案之修訂 | 57 | 原則同意 |
| **8.1變更程序**<br>本會至少每年應檢視本憑證政策1次，憑證機構至少每年應檢視憑證實務作業基準1次，以維持其保證度。憑證政策的修改不影響憑證政策所聲明的憑證使用目的與保證度時，憑證政策之物件識別碼不需修改，憑證政策之物件識別碼變更，憑證實務作業基準應作相對應之變更。<br><br>此外，若憑證機構提供伺服器應用軟體憑證簽發與管理之服務，則該憑證機構每年應定期檢視憑證機構與瀏覽器論壇(CA/Browser Forum)所發行的 Baseline Requirements Certificate Policy for the Issuance and Management of Publicly- | 同意原提案之修訂 | 85 | 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 |
| --- | --- | --- | --- |
| Trusted Certificates 正式版本(http://www.cabforum.org)所頒布之條款，評估其憑證實務作業基是否需要修訂。倘若該憑證實務作業基準於伺服器應用軟體憑證之簽發與管理的敘述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，並進行憑證實務作業基準之修訂。 | | | |
| **附錄1：BR-Section 1.2.1 Revisions**<br>……(內容省略) | 同意原提案之修訂 | 88-90 | 原則同意 |
| | | | 建議文中有關「本國」之用詞統一調整為「我國」。 |
| | | | 建議將「數位簽章」之用詞統一改為「電子簽章」 |
| | | | 變更內容對照表中多處對應頁數誤植，請更正為正確頁數 |

附件2：政府憑證總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**<br>1、主管機關核定文號：經商字第____號 | 同意原提案之修訂 | i | |
| **1.1概要**<br>……(略)<br>本作業基準主要說明總管理中心的憑證作業實務，以確保總管理中心的憑證簽發及管理作業符合憑證政策訂定之保證等級第4級之規定。本作業基準所載明之實務作業規範僅適用於與總管理中心相關之個體，如總管理中心、交互認證憑證機構(Subject CA)、信賴憑證者(Relying Parties)及儲存庫(Repository)等。<br>總管理中心及有簽發伺服器應用軟體憑證之交互認證憑證機構，須另遵循憑證機構與瀏覽器論壇（CA/Browser Forum）所發行之 Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates 正式版本(http://www.cabforum.org)，同時針對該正式版本中第1.2.1節所列之各項資訊的生效日期，總管理中心皆配合辦理(參照附錄1)。 | 同意原提案之修訂 | 1-2 | 原則同意 |
| **1.2憑證實務作業基準之識別**<br>本作業基準之名稱為政府憑證總管理中心憑證實務作業基準(Government Root Certification Authority Certification Practice Statement)，本版本為第1.5 | 同意原提案之修訂 | 2-3 | 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 |
| --- | --- | --- | --- |
| 版，公布日期為106年_月日。最新版本的本作業基準可在以下網頁取得：http://grca.nat.gov.tw/download/GRCA_CPS_v1.5.pdf。 | | | |
| **2.2.1保證範圍及其限制條件**<br>總管理中心依憑證政策保證等級第4級運作，並遵守本作業基準規定之程序簽發及廢止憑證、簽發並公布憑證機構廢止清冊及維持儲存庫正常運作。<br>總管理中心另遵循憑證機構與瀏覽器論壇(CA/Browser Forum)所發行的Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates 正式版本(http://www.cabforum.org)之規範簽發及管理憑證。 | 同意原提案之修訂 | 12 | 原則同意 |
| **2.4.2可分割性、存續、合併及公告通知**<br>如本作業基準的任何一章節不正確或無效時，其他章節仍然有效，本作業基準的修訂依照第8章規定辦理。<br>總管理中心之憑證簽發及管理另遵循憑證機構與瀏覽器論壇(CA/Browser Forum)所發行的 Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates 正式版本(http://www.cabforum.org)，惟Baseline Requirements 相關規定與憑證管理中心所依循之我國相關法律或法規產生衝突時，總管理中心得小幅度 | 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 |
| --- | --- | --- | --- |
| 調整相關作法以滿足法律或法規之要求，並將變更調整之部分於簽發新憑證前通知CA/Browser Forum；若我國法律或法規已不再適用時，或 Baseline Requirements 修訂相關內容使其規定可相容於我國法律時，則總管理中心需撤除並修訂原先 CPS 所調整修訂之內容，上述作業須於90天內完成。 | | | |
| **3.1.4命名之獨特性**<br>總管理中心將審核申請成為下屬憑證機構與交互認證憑證機構所提出的憑證機構名稱之獨特性，如名稱重複時得要求該憑證機構修改名稱。<br>總管理中心第1代與第2代的自簽憑證使用以下名稱格式：<br>C=TW，O=Government Root Certification Authority<br>因總管理中心第1代及第2代自簽憑證主體同名造成其相互簽發之自發憑證被誤認為自簽憑證，而導致瀏覽器驗證憑證信賴路徑時產生錯誤，故總管理中心產製第1.5代金鑰，簽發自發憑證，重新建構第1代及第2代自簽憑證之信賴路徑，並使用以下名稱格式：<br>C=TW，<br>O=行政院，<br>CN=Government Root Certification Authority - G1.5<br>為便於與國際互通，總管理中心第3代起的自簽憑證使用以下名稱格式： | 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 |
| --- | --- | --- | --- |
| C=TW，<br>O=行政院，<br>CN=Government Root Certification Authority - Gn<br>其中，n=3,4…<br>此外，總管理中心之自簽憑證中，憑證簽發者與憑證主體名稱相同。 | | | |
| **4.4.1廢止憑證之事由**<br>……(略)<br>另外，總管理中心得就以下情形逕行廢止憑證，毋須事先經過交互認證憑證機構同意：<br>(1) 確認憑證記載之內容不實。<br>(2) 確認交互認證憑證機構之簽章用私密金鑰遭冒用、偽造或破解。<br>(3) 確認總管理中心之私密金鑰或系統遭冒用、偽造或破解，則廢止總管理中心簽發的所有交互認證憑證機構之憑證。<br>(4) 確認交互認證憑證機構的憑證未依本作業基準之程序簽發。<br>(5) 確認交互認證憑證機構違反其憑證實務作業基準或交互認證協議書或相關法令規定。<br>(6) 依據交互認證憑證機構主管機關之通知或相關法令規定。 | 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 |
| --- | --- | --- | --- |
| (7) 總管理中心或交互認證憑證機構[新增]終止服務並且未安排另一個憑證管理中心來提供憑證廢止服務[新增]。<br>(8) 總管理中心或交互認證憑證機構簽發憑證的權利已經逾期或被廢止、中止，除非總憑證管理中心有安排繼續維運 CRL/OCSP 儲存庫的服務。<br>(9) 依據總管理中心憑證政策或憑證實務作業基準要求的廢止。<br>(10) 憑證的技術內容或格式對應用軟體提供者或依賴方可能產生無法接受的風險。[新增]<br>如憑證之憑證主體資訊必須變更時，由總管理中心審查是否同意廢止憑證申請。 | | | |
| **4.4.4憑證廢止申請之寬限期**<br>在接收到憑證問題報告的24小時內應以下述規則調查確認憑證廢止請求是否成立：<br>1.聲稱問題的內容<br>2.該憑證或用戶的憑證問題報告的數目<br>3.用戶問題的等級<br>4.相關的法律條文[新增]<br>交互認證憑證機構如發生4.4.1節之情形，最遲應於10個工作天內提出憑證廢止申請，並且儘可能於總管理 | 同意原提案之修訂 | 34 | 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 |
| --- | --- | --- | --- |
| 中心下一次簽發憑證機構廢止清冊前提出。<br>總管理中心在收到憑證廢止申請後，最遲於10個工作天內完成憑證廢止相關作業。 | | | |
| **4.4.10憑證機構廢止清冊之簽發頻率**<br>憑證機構廢止清冊之簽發頻率為每天1次，且憑證機構廢止清冊之「下次更新時間(nextUpdate)」欄位內容值不可超過「生效時間(thisUpdate)」欄位內容值12個月。更新後之憑證機構廢止清冊公布於儲存庫。 | 同意原提案之修訂 | 35 | 原則同意 |
| **4.8.1緊急事件與系統遭破解之處理程序**<br>總管理中心依據緊急事件與系統遭破解的種類執行相關復原程序，並定期執行必要的資料備份作業。<br><br>**※原4.8.1~4.8.4節更改標號為4.8.2~4.8.5節** | 同意原提案之修訂 | 45-46 | 原則同意 |
| **6.1.5金鑰長度**<br>總管理中心使用 4096 位元的 RSA 金鑰及 SHA-2雜湊函數演算法簽發憑證。<br>交互認證之憑證機構必須依照憑證政策之規定選擇適當的金鑰長度；總管理中心於簽發交互憑證前將審查該憑證機構所選擇的金鑰長度是否恰當。 | 同意原提案之修訂 | 61 | 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 |
|---|---|---|---|
| **7.1.3演算法物件識別碼**<br>總管理中心簽署在憑證中的簽章其演算法的物件識別碼可為其下任一種：<br>Sha256WithRSAEncryption {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}<br>(OID：1.2.840.113549.1.1.11)<br>……(略) | 同意原提案之修訂 | 71-72 | 原則同意 |
| **7.1.6憑證政策物件識別碼**<br>總管理中心的自簽憑證不含憑證政策(certificatePolicies)擴充欄位。總管理中心簽發給下層憑證管理中心的交互憑證，其憑證政策(Certificate Policy)欄位必須使用本基礎建設之憑證政策物件識別碼。此外亦可包含 CA/Browser Forum Baseline Requirements 指定之憑證政策物件識別碼「2.23.140.1.2.2」。 | 同意原提案之修訂 | 72 | 原則同意 |
| **8.1變更程序**<br>本作業基準每年定期評估是否需要修訂，以維持其保證度。修訂方式包括以附加文件方式修訂及直接修訂本作業基準的內容。如憑證政策修訂或物件識別碼變更時，本作業基準將配合修訂。<br>此外，總憑證管理中心每年定期檢視憑證機構與瀏覽器論壇(CA/Browser Forum)所發行的 Baseline Requirements Certificate Policy for the Issuance and | 同意原提案之修訂 | 74 | 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 |
| --- | --- | --- | --- |
| Management of Publicly-Trusted Certificates 正式版本(http://www.cabforum.org)所頒布之條款，評估本作業基準是否需要修訂。倘若本作業基準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，並進行本作業基準之修訂。 | | | |
| **附錄1：BR-Section 1.2.1 Revisions**<br>……(內容省略) | 同意原提案之修訂 | 77-78 | 原則同意 |
| | | | 建議文中有關「本國」之用詞統一調整為「我國」。 |
| | | | 建議將「數位簽章」之用詞統一改為「電子簽章」 |
| | | 49 | 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」，請依照GPKI CP 第5.1.8節之敘述方式敘述並區別「全部資料」及「稽核資料」之備份方式。 |
| | **1.緒論**<br>政府憑證總管理中心憑證實務作業基準.....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」相關規定.....。 | 1 | 建議調整此段敘述 |
| | | | 請修訂變更內容對照表中頁數誤植之部分 |

附件3：政府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**<br>1、主管機關核定文號：經商字第____號 | 同意原提案之修訂 | i | 原則同意 |
| **1.1概要**<br>……(略)<br>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)所發行的 Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates 正式版本(http://www.cabforum.org)，同時針對該正式版本中第1.2.1節所列之各項資訊的生效日期，本管理中心皆配合辦理(參照附錄1)，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。<br>……(略) | 同意原提案之修訂 | 1-2 | 原則同意 |
| **1.2憑證實務作業基準之識別**<br>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1.9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_v1.9.pdf。 | 同意原提案之修訂 | 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 |
| --- | --- | --- | --- |
| **2.2.1.1保證範圍及其限制條件**<br>本管理中心依憑證政策保證等級第3級運作，並遵守本作業基準規定之程序簽發及管理憑證、簽發並公布憑證廢止清冊及維持儲存庫正常運作。<br>本管理中心另遵循憑證機構與瀏覽器論壇(CA/Browser Forum)所發行的Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates 正式版本(http://www.cabforum.org)之規範簽發及管理伺服器應用軟體憑證憑證。 | 同意原提案之修訂 | 11 | 原則同意 |
| **2.4.2可分割性、存續、合併、公告通知**<br>如本作業基準的任何一章節不正確或無效時，其他章節仍然有效，本作業基準的修訂依照第8章規定辦理。<br>本管理中心之伺服器應用軟體憑證之簽發及管理，另遵循憑證機構與瀏覽器論壇(CA/Browser Forum)所發行的 Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates 正式版本(http://www.cabforum.org)，惟Baseline Requirements 相關規定與憑證管理中心所依循之我國相關法律或法規產生衝突時，憑證管理中心得小幅度調整相關作法以滿足法律或法規之要求，並將變更調整之部分於簽發新憑證前通知 CA/Browser Forum；若我 | 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 |
| --- | --- | --- | --- |
| 國法律或法規已不再適用時，或 Baseline Requirements 修訂相關內容使其規定可相容於我國法律時，則憑證管理中心需撤除並修訂原先 CPS 所調整修訂之內容，上述作業須於90天內完成。 | | | |
| **2.8.3憑證廢止或暫時停用資訊之公開**<br>憑證廢止或暫時停用資訊公布於本管理中心儲存庫。在憑證廢止清冊(CRL)或線上憑證狀態服務(OCSP)回覆封包中的憑證廢止或暫時停用資訊，必須直到該被廢止或停用憑證已過期後才能加以移除。 | 同意原提案之修訂 | 19 | 原則同意 |
| **3.1.4命名之獨特性**<br>本管理中心第1代與第二代的憑證機構憑證其 X.500唯一識別名稱為：<br>C=TW，O=行政院，OU=政府憑證管理中心<br>為便於與國際互通，本管理中心第3代起的憑證機構憑證其 X.500唯一識別名稱使用以下格式：<br>C=TW，O=行政院，CN=政府憑證管理中心 - Gn<br>其中，n=3,4…<br>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：<br>……(略) | 同意原提案之修訂 | 21-23 | 原則同意 |
| **3.1.9個人身分鑑別之程序**<br>政府機關單位申請伺服器應用軟體憑證時, 必須透過正式公文書申請，此正式公文書須經由該單位主管簽核，以此證明此伺服器應用 | 同意原提案之修訂 | 25 | 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 |
| --- | --- | --- | --- |
| 軟體憑證之申請是獲得單位授權。 | | | |
| **3.1.12網域名稱擁有者識別程序**<br>用戶申請伺服器應用軟體憑證(SSL Certificate)時(包含：單網域 SSL 憑證、多網域 SSL 憑證及萬用網域 SSL 憑證)，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；另應擇一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：<br>■ 政府 WHOIS 主機-政府中英文網域名稱註冊系統 (https://rs.gsn.gov.tw)<br>■ TWNIC Whois Data-base (http://whois.twnic.net.tw)<br>■ ICANN WHOIS（https://whois.icann.org/en）(適用通用頂級網域)<br>■ 透過與網域名稱註冊管理單位(Domain Name Registrar)接觸，驗證申請者具備該網域之控制權<br>若用戶以政府網際服務網(Government Service Network, GSN)之 IP Address 申請伺服器應用軟體憑證時，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 IP Address 確實存在且屬該 | 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 |
| --- | --- | --- | --- |
| 申請者所註冊擁有：<br>■ TWNIC Whois Data-base (http://whois.twnic.net.tw)<br>透過與 GSN IP 註冊管理單位接觸，驗證該 IP Address 確實存在且屬該申請者所註冊擁有。 | | | |
| **4.1申請憑證之程序**<br>……(略)<br>本管理中心僅接受政府機關(構)或單位提出之憑證申請，該憑證申請需要透過正式公文，並經過單位主管層層簽核過後才能遞交至憑證審驗單位進行憑證申請。當 RAO 審驗人員收到公文後，其會依照審驗作業規範進行公文文號及發文單位進行比對，僅有符合要求的憑證申請才會予以通過。<br>申請憑證時，憑證申請人應提供正確資料。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。<br>此外，本管理中心僅提供政府機關(構)及單位之 SSL 類伺服器應用軟體憑證申請，其多數申請之網域均已透過 GSN 註冊，且申請之網域為政府機關(構)及單位能註冊使用之「.gov」。此外，有 | 同意原提案之修訂 | 29-32 | 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 |
| --- | --- | --- | --- |
| 少數國營單位使用「.com」的網域，但此網域之申請需經嚴密的審核及管控，因此，本管理中心並無有高風險憑證申請問題。<br>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。<br>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。<br>依據 RFC 6844，本管理中心檢查網域名稱系統(Domain Name System, DNS)查閱 SSL 憑證申請案件所註記之完整網域名稱(Fully Qualified Domain Names, FQDN)是否有授權憑證機構簽發憑證(Certification Authority Authorization, CAA)DNS 資源紀錄(DNS Resource Record)。若授權憑證機構簽發憑證 DNS 資源紀錄存在且未將本管理中心列為授權 SSL 憑證簽發之憑證管理中心，本管理中心會視該憑證申請為同意授權本管理中心針對該網域簽發 SSL 憑證，並請用戶可前往其網域名稱系統更新授權憑證機構簽發憑證 DNS 資源紀錄將本管理中心列入。<br>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 |
| --- | --- | --- | --- |
| GCA 不簽發交互認證憑證(Cross Certificate)給其他 CA。 | | | |
| **4.2.3政府機關伺服器應用軟體憑證**<br>政府機關(構)伺服器應用軟體憑證之簽發審核程序如下：<br>(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。<br>(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。<br>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。<br>此外，本管理中心不執行預簽憑證(Precertificate)的簽發，即便未來本管理中心因應憑證透明度機制而執行預簽憑證的簽發時，該預簽憑證亦不得視為本管理中心所簽發的憑證。 | 同意原提案之修訂 | 34-35 | 原則同意 |
| **4.4.1廢止憑證之事由**<br>用戶在以下情形時(但不限)必須向註冊中心提出廢止憑證申請：<br>(1) 懷疑或證實私密金鑰遭到破解。<br>(2) 憑證所記載之資訊重大改變，足以影響其信賴度。例如用戶之機關(構)或單 | 同意原提案之修訂 | 36-37 | 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 |
| --- | --- | --- | --- |
| 位裁撤或合併，或唯一識別名稱需要做變更，這包含用戶的名稱已變更，或其上級機關已變更。<br>(3) 憑證不再需要使用，包括不再授權原憑證請求且不再追溯相關授權。<br>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：<br>(1) 確認憑證記載之內容不實。<br>(2) 確認用戶之簽章用私密金鑰遭冒用、偽造或破解。<br>(3) 確認本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。<br>(4) 確認用戶之機關(構)或單位裁撤或合併。<br>(5) 確認用戶之憑證未依本作業基準規定之程序簽發。<br>(6) 確認用戶違反本作業基準或相關法令規定。<br>(7) 依據司法機關、監察機關或治安機關之通知。<br>(8) 依用戶之上級機關或政府組織之主管機關之通知。<br>(9) 政府機關(構)、單位如因非自發性的名稱變更，而需做原 | | | |

| 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 |
| --- | --- | --- | --- |
| 先憑證的廢止時，本管理中心得視需要延後逕行廢止憑證，此憑證廢止的寬限期將公布在本管理中心儲存庫。<br>(10) 憑證內的完整網域名稱或者網路位址不再被授權給該用戶。<br>(11) 萬用字元憑證被用來認證一個錯誤誤導的下屬完整域名。<br>(12) 本憑證管理中心停止服務並且未安排另一個憑證管理中心來提供憑證廢止服務。<br>(13) 本憑證管理中心簽發憑證的權利已經逾期或被廢止、中止，除非本憑證管理中心有安排繼續維運 CRL/OCSP 儲存庫的服務。<br>(14) 依據憑證政策或憑證實務作業基準要求的廢止。<br>憑證的技術內容或格式對應用軟體提供者或依賴方可能產生無法接受的風險。 | | | |
| **4.4.4憑證廢止申請之寬限期**<br>在接收到憑證問題報告的24小時內應以下述規則調查確認憑證廢止請求是否成立：<br>(1) 聲稱問題的內容<br>(2) 該憑證或用戶的憑證問題報告的數目<br>(3) 用戶問題的等級 | 同意原提案之修訂 | 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 |
| --- | --- | --- | --- |
| (4) 相關的法律條文<br>用戶如發生4.4.1節第1項之情形，最遲應於10個工作天內提出憑證廢止申請。 | | | |
| **4.4.10憑證廢止清冊之簽發頻率**<br>憑證廢止清冊之簽發頻率為每天1次，且憑證廢止清冊之「下次更新時間(nextUpdate)」欄位內容值不可超過「生效時間(thisUpdate)」欄位內容值10天。更新後之憑證廢止清冊公布於儲存庫。 | 同意原提案之修訂 | 42 | 原則同意 |
| **4.4.12線上憑證狀態查詢服務**<br>本管理中心提供符合RFC 6960及 RFC 5019標準規範之線上憑證狀態查詢協定(OCSP)服務，其中 OCSP 回應封包需經簽發此待廢止憑證的 CA 做簽章。本管理中心支援使用 GET 方法的 OCSP 服務。本管理中心至少每四天應更新透過 OCSP 提供的資訊。OCSP 回應封包最遲十天逾期。如果 OCSP 提供回應者收到對於一個還未簽發的憑證之狀態請求，則不可回覆其狀態為正常；並且本管理中心應監督 OCSP 提供回應者對於這類請求的回覆是否符合上述安全回應程序。更多相關說明請參閱儲存庫。 | 同意原提案之修訂 | 42 | 原則同意 |
| **4.4.14其他形式廢止公告**<br>不提供。此外，本管理中心須確保使用者可在憑證的 TLS 交握(TLS handshake)中可對 OCSP 回應使用封套(OCSP Stapling)方法，並確認透過說明或技術量測等來實 | 同意原提案之修訂 | 43 | 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。 | | | |
| **4.8.1緊急事件與系統遭破解之處理程序**<br>本管理中心依據緊急事件與系統遭破解的種類執行相關復原程序，並定期執行必要的資料備份作業。<br><br>**※原4.8.1~4.8.4節更改標號為4.8.2~4.8.5節** | 同意原提案之修訂 | 52 | 原則同意 |
| **6.1.5金鑰長度**<br>本管理中心使用2048位元的 RSA 金鑰以及 SHA256、SHA384或 SHA512 雜湊函數演算法簽發憑證，用戶使用2048位元的 RSA 金鑰。 | 同意原提案之修訂 | 65-66 | 原則同意 |
| **6.1.7金鑰參數品質之檢驗**<br>本管理中心採用 ANSI X9.31演算法或 FIPS 186-3規範產生 RSA 演算法所需的質數，並確保該質數為強質數(Strong Prime)。<br>用戶金鑰可於 IC 卡內部或其他軟硬體密碼模組產生 RSA 演算法中所需的質數，本管理中心會檢查用戶金鑰必須符合強質數，若用戶使用 RAS 金鑰時，金鑰的指數(exponent)必須為大於3的奇數。 | ……若用戶使用 RSA 金鑰時，產製金鑰之指數(exponent)必須為大於3之奇數。 | 66 | 原則同意，請修正演算法 RSA 而非 RAS，並建議修訂「金鑰的指數」之敘述。 |
| **6.3.2.2用戶公開金鑰及私密金鑰之使用期限**<br>用戶之公開金鑰及私密金鑰之金鑰長度為 RSA 2048位元，公開金鑰憑證之使用期限至多為9年，私密金鑰之使用期限至多為9年。<br>用戶申請之伺服器應用軟體憑證(SSL Certificate)之金鑰長度為 RSA 2048位元，其 | 同意原提案之修訂 | 69 | 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 |
| --- | --- | --- | --- |
| 公開金鑰憑證之使用期限遵循憑證機構與瀏覽器論壇(CA/Browser Forum)所發行的Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates 正式版本(http://www.cabforum.org)之規定，107年3月1日後之伺服器應用軟體憑證效期不得超過825天，105年7月1日至107年2月28日間簽發之伺服器應用軟體憑證效期不得超過39個月。 | | | |
| **7.1.3 演算法物件識別碼**<br>本管理中心所簽發憑證中的簽章之演算法的物件識別碼可為其下任一種：<br>sha256WithRSAEncryption {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}<br>(OID：1.2.840.113549.1.1.11)<br>……(略) | 同意原提案之修訂 | 73 | 原則同意 |
| **7.1.6憑證政策物件識別碼**<br>本管理中心所簽發憑證之憑證政策擴充欄位使用本基礎建設之憑證政策物件識別碼。<br>本管理中心所簽發伺服器應用軟體憑證在憑證管理及憑證信賴保證上，除符合本基礎建設保證等級要求外，還符合 CA/Browser Forum Baseline Requirements 的規範。因此，本管理中心所簽發伺服器應用軟體憑證 | 同意原提案之修訂 | 74 | 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 |
| --- | --- | --- | --- |
| 之憑證政策擴充欄位中除前述本基礎建設之憑證政策物件識別碼外，還必須包括CA/Browser Forum Baseline Requirements 指定之憑證政策物件識別碼「2.23.140.1.2.2」。 | | | |
| **8.1變更程序**<br>本作業基準每年定期評估是否需要修訂，以維持其保證度。修訂方式包括以附加文件方式修訂及直接修訂本作業基準的內容。如憑證政策修訂或物件識別碼變更時，本作業基準將配合修訂。<br>此外，本憑證管理中心每年定期檢視憑證機構與瀏覽器論壇(CA/Browser Forum)所發行的 Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates 正式版本(http://www.cabforum.org)所頒布之條款，評估本作業基準是否需要修訂。倘若本作業基準在 SSL 類憑證簽發管理之敘述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，並進行本作業基準之修訂。 | 同意原提案之修訂 | 76 | 原則同意 |
| **附錄1：BR-Section 1.2.1 Revisions**<br>……(內容省略) | 同意原提案之修訂 | 79-80 | 原則同意 |
| | | | 建議文中有關「本國」之用詞統一調整為「我國」。 |
| | | | 建議將「數位簽章」之用詞統一改 |

| 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 |
| --- | --- | --- | --- |
| | | | 為「電子簽章」 |
| | | 56 | 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」，請依照GPKI CP 第5.1.8節之敘述方式敘述並區別「全部資料」及「稽核資料」之備份方式。 |
| | **1.緒論**<br>政府憑證管理中心憑證實務作業基準.....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」相關規定.....。 | 1 | 建議調整此段敘述 |

附件4：工商憑證管理中心憑證實務作業基準第2.2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**<br>2.　簽發之憑證<br>(1)　種類：<br>A.我國登記設立之公司、分公司、商業、有限合夥及有限合夥分支機構等事業主體（以下統稱事業主體，包括簽章用及加解密用的兩種憑證）憑證。<br>B.我國登記設立之公司、商業及有限合夥等事業主體使用於「公司與商業及有限合夥一站式線上申請作業」網站之專屬授權憑證(以下簡稱一站式專屬授權憑證)。<br>…<br>(3)　適用範圍：<br>A.事業主體憑證適用於電子化政府暨電子商務等符合事業主體業務活動之相關應用服務所需的身分認證及資料加密，所傳送的資料可以包含金錢上的交易。<br>B.一站式專屬授權憑證僅可用於「公司與商業及有限合夥一站式線上申請作業」網站。<br>…<br><br>3.　法律責任重要事項<br>…<br>(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，但在異動前，用戶仍應承擔使用該憑證之法律責任。 | 同意原提案之修訂 | VIII-XI | |

| 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 |
| --- | --- | --- | --- |
| **2.1.4用戶之義務**<br>…<br>(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，但在異動前，用戶仍應承擔使用該憑證之法律責任。 | 同意原提案之修訂 | 11-12 | 原則同意 |
| **2.2.1.4其他除外條款**<br>…<br>如因4.4.1節廢止憑證之事由，用戶應依照4.4.3節憑證廢止程序提出廢止憑證申請。本管理中心將在核定廢止憑證申請後1個工作天內完成憑證廢止作業、簽發憑證廢止清冊及公告於儲存庫。用戶於憑證廢止狀態未被公布之前，應採取適當的行動，以減少對信賴憑證者之影響，並承擔因使用該憑證所引發之責任。 | 同意原提案之修訂 | 14-15 | 原則同意 |
| **3.1.4命名之獨特性**<br>本管理中心的 X.500唯一識別名稱為：<br>…<br>2.分公司憑證<br>C=TW<br>L=縣市名稱<br>O=公司的正式登記名稱<br>serialNumber=憑證管理中心自動給定用戶之唯一序號<br>OU=分公司的正式登記名稱<br>…<br>6.一站式專屬授權憑證<br>C=TW<br>L=縣市名稱(選擇性欄位，只適用於商業)<br>O=公司、商業或有限合夥的 | 同意原提案之修訂 | 26-28 | 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 |
| --- | --- | --- | --- |
| 正式登記名稱 serialNumber=憑證管理中心自動給定用戶之唯一序號(選擇性欄位，只適用於公司及商業) | | | |
| **3.1.5命名爭議之解決程序**<br>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**<br>…<br>用戶申請IC卡附卡或一站式專屬授權憑證時，需先取得IC卡正卡後，採線上申請方式辦理，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 | 29-30 | 原則同意 |
| **3.1.11寫入憑證內之電子郵件信箱驗證**<br>…<br>(2) 用戶申請符記為非IC卡用戶得依照需求於於本管理中心網站(http://moeaca.nat.gov.tw)申請非IC卡類憑證或一站式專屬授權憑證時，一併申請電子郵件信箱寫入憑證。 | 同意原提案之修訂 | 31-32 | 原則同意 |
| **4.1.1.1 申請發證程序**<br>用戶以紙本憑證申請書提交予憑證註冊窗口之憑證IC卡正卡或非IC卡類憑證申請程序：<br>…<br>(3)憑證申辦人將憑證申請書，送交該事業主體登記設 | 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 |
| --- | --- | --- | --- |
| 立主管機關所設的憑證註冊窗口辦理。<br>用戶以事業主體負責人自然人憑證申請憑證 IC 卡正卡或非 IC 卡類憑證程序：<br>(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 Agreement），如同意條款內容則填寫憑證申請書，並設定用戶代碼。<br>(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。 | | | |
| **4.1.1.3申請憑證 IC 附卡、一站式專屬授權憑證或換發 IC 卡正卡程序**<br>…<br>(2)以事業主體憑證 IC 卡正卡對 IC 卡附卡、一站式專屬授權憑證或 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 |
| **4.2.2 IC 卡附卡及一站式專屬授權憑證簽發程序**<br>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。IC 卡附卡後續簽發程序比照4.2.1.1節符記為 IC 卡之簽發步驟；一站式專屬授權憑證後續簽發程序則為由本管理中心簽發憑證後，將私密金鑰及憑證以用戶設定之密碼加密封 | 同意原提案之修訂 | 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 |
| --- | --- | --- | --- |
| 裝為 PKCS#12之個人資訊交換檔案格式供用戶使用。 | | | |
| **4.3.1申請發證**<br>(1)用戶使用符記為 IC 卡時，申請發證之用戶完成 IC 卡接受作業，相關程序如下：<br>…<br>(2)用戶申請非 IC 卡類憑證時，接受憑證之程序如下：<br>…<br>(3)用戶申請一站式專屬授權憑證時，於4.1.1.3節之申請過程中，需先行確認申請資料及接受將簽發之憑證內容後始可送出申請。<br>(4)在用戶完成憑證接受作業後，所簽發的憑證將會公布至儲存庫中。 | 同意原提案之修訂 | 40-41 | 原則同意 |
| **4.4.7暫時停用憑證之程序**<br>用戶提出憑證暫時停用申請，其程序如下：<br>(1)用戶使用符記為 IC 卡：<br>…<br>(2)用戶使用符記為非 IC 卡類： | 同意原提案之修訂 | 46-47 | 原則同意 |
| **4.4.9恢復使用憑證之程序**<br>用戶申請恢復使用憑證（僅限於恢復之前用戶自行上網申請停用之憑證）之程序如下：<br>(1) 連線至本管理中心網站（http://moeaca.nat.gov.tw/），填寫 IC 卡號（使用符記為 IC 卡時）或憑證序號（使用符記為非 IC 卡類時）及用戶代碼，線上申請恢復使用憑證。<br>(2) 註冊中心在檢驗 IC 卡之卡號（使用符記為 IC 卡時）或憑證序號（使用符記為非 IC 卡類時）及用戶代碼正確 | 同意原提案之修訂 | 48-49 | 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 |
| --- | --- | --- | --- |
| 無誤後，加簽數位簽章上傳至本管理中心。 | | | |
| **6.3.2.2用戶公開金鑰及私密金鑰之使用期限**<br>當用戶之公開金鑰及私密金鑰之金鑰長度為1024位元時，公開金鑰憑證之使用期限至多為5年，私密金鑰之使用期限至多為5年。當金鑰長度為2048位元時，公開金鑰憑證之使用期限至多為10年，私密金鑰之使用期限至多為10年。一站式專屬授權憑證之使用期限至多為1年。 | 同意原提案之修訂 | 80 | 原則同意 |
| | | | 建議將「數位簽章」之用詞統一改為「電子簽章」 |
| | | 65 | 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」，請依照GPKI CP 第5.1.8節之敘述方式敘述並區別「全部資料」及「稽核資料」之備份方式。 |
| | | 77 | 有關 m-out-of-n 定義及描述，請調整與 GCA CPS 相關內容一致 |
| | **1.2憑證實務作業基準之識別**<br>……. 最新版本的本作業基準可在以下網頁取得：<br>http://moeaca.nat.gov.tw/download/download_4.html | 2 | CPS 下載位址建議列直接可下載網頁位址而非列網站網址 |

附件5：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2.2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 |
|---|---|---|---|
| **1.2.1用戶公鑰憑證的種類**<br>GPKI之用戶公鑰憑證的種類目前包括.....、OCSP伺服器憑證、公司與商業及有限合夥一站式線上申請作業網站之專屬授權憑證(以下簡稱一站式專屬授權憑證)，各憑證的相關用戶為：<br>.....<br>(20)一站式專屬授權憑證<br>簽發對象為公司、商業及有限合夥之一站式線上申請作業網站授權使用者。 | 同意原提案之修訂 | 7<br>10 | 原則同意 |
| **1.3.23 To-Be-Signed 一站式專屬授權憑證格式**<br>**.....(內容省略)** | 同意原提案之修訂 | 232-241 | 原則同意 |
| **1.3.7To-Be-Signed 分公司憑證格式**<br>分公司的X.500 Name格式如下：<br>C=TW<br>O=公司的正式登記名稱<br>serialNumber=憑證管理中心自動給定用戶之唯一序號<br>OU=分公司的正式登記名稱<br>（依PKIX規定，所有ASN.1 DirectoryString文字編碼一律使用UTF-8編碼） | 同意原提案之修訂 | 65-66 | 原則同意 |
| | 「公司與商業及有限合夥一站式線上申請作業網站」 | 234 | 「公司、商業及有限合夥一站式線上申請作業網站」名稱誤植，請修訂為「公司與商業及有限合夥一站式線上申 |

| 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 |
| --- | --- | --- | --- |
| | | | 請作業網站」。 |
| | | | 請一併修訂剖繪本文中關於SHA-1雜湊函數之敘述 |