行政機關電子憑證推行小組第 22 次委員會議紀錄

一、時間：101 年 8 月 8 日（星期三）下午 2 時 00 分

二、地點：本會 8 樓視訊會議室

三、主席：何處長全德　　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）原則同意政府憑證總管理中心(GRCA)與政府憑證管理中心(GCA)依所規劃方式進行金鑰更換及簽章演算法升級作業，另對於本案所規劃各項重點工作之辦理時程，建請明確以利追蹤掌握。

（二）配合本次各憑證機構更換金鑰及升級簽章演算法作業，請各憑證機構妥善規劃完整執行方案及相關配套措施，包含技術支援、諮詢輔導、專案管理等，以確保所有應用系統能順利配合本次作業完成系統更新。

（三）同意「政府公開金鑰基礎建設憑證政策第 1.6 版(草案)」之修訂(如附件 1)，請針對委員意見修正內容，並公布於政府憑證總管理中心網站及通告政府公開金鑰基礎建設下屬各憑證管理中心。

（四）同意「政府憑證總管理中心憑證實務作業基準第 1.3 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。

（五）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 1.7 版(草案)」之修訂(如附件 3) ，請針對委員意見修正內容，並公布於政府憑證總管理中心網站。

七、散會：下午 4 時 30 分。

附件 1：政府公開金鑰基礎建設憑證政策第 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
	全文	將文中有關雜湊演算法 SHA-2、SHA-256 之用語統一
1.2 憑證政策之識別	4	原則同意
1.3.1 行政機關電子憑證推行小組	5	原則同意
1.3.2 政府憑證總管理中心	6	原則同意
1.3.5 儲存庫	7	原則同意
1.3.8.2 憑證使用之限制	10	原則同意
2.1.1 憑證機構之職責	13	原則同意
2.1.4 信賴憑證者之義務	14	原則同意
2.1.5 儲存庫服務之義務	15	原則同意
2.6.1 憑證機構之資訊公佈	18	原則同意
2.6.2 公佈頻率	18	原則同意
2.7.6 稽核結果公開之範圍	21	原則同意
4.1 申請憑證之程序	35	原則同意
4.2 簽發憑證之程序	36	原則同意，並建議修改: .....並得簽發數張自發憑證(Self-Issued Certificate) ，以因[新

變更後記載內容	變更後頁數	審查意見
		增]應本身金鑰及憑證政策的更換
4.3 接受憑證之程序	36	原則同意
4.4 憑證暫時停用及廢止	38	原則同意
4.4.9 憑證機構廢止清冊及憑證廢止清冊之簽發頻率	41	原則同意
4.5.1 被記錄事件種類	47	原則同意
4.6.2 歸檔之保留期限	54	原則同意
4.7.1 憑證機構之金鑰更換	55	原則同意，並建議修改: 總管理中心最遲應於自簽憑證到期前 3 個月，更換用來簽發下屬憑證機構[新增]憑證的金鑰對
5.3.6 未授權行動之制裁	66	原則同意
6.1.1 金鑰對之產製	67	原則同意
6.1.4 憑證機構公開金鑰安全傳送給信賴憑證者	69	原則同意
6.1.5 金鑰長度	70	原則同意，並建議將各憑證機構更換 SHA-2 演算法簽發憑證之期限更改為民國 105 年 12 月 31 日前，以符合第 20 次行政機關電子憑證推行小組會議之決議
6.2.1 密碼模組標準	72	原則同意

變更後記載內容	變更後頁數	審查意見
6.3.2.1 憑證機構公開金鑰及私密金鑰之使用期限	75	原則同意，並請新增 RSA3072 位元之金鑰使用期限。
6.3.2.2 用戶公開金鑰及私密金鑰之使用期限	76	原則同意
7.1.2　憑證擴充欄位	81	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
8.2 公告及通知之規定	85	原則同意
8.3 憑證實務作業基準變更程序	86	原則同意

附件2：政府憑證總管理中心憑證實務作業基準第1.3版(草案)審查意見表

變更後記載內容	變更後頁數	審查意見
	全文	將文中有關雜湊演算法 SHA-2、SHA-256 之用語統一
	47、62	建議將「5.1.8 異地備援」、「6.2.9 私密金鑰之銷毀方式」中「本管理中心」之用語統一改為「總管理中心」
摘要 1、主管機關核定文號	VIII	原則同意
摘要 2、簽發之憑證：	VIII	原則同意
摘要 4、其他重要事項：	X	原則同意
1 序論	1	原則同意
1.2 憑證實務作業基準之識別	2	原則同意
1.3.1 政府憑證總管理中心	3	原則同意
1.3.6.1 憑證之適用範圍	5	原則同意
1.3.6.2 憑證之使用限制	5-6	原則同意
2.1.1 政府憑證總管理中心之職責	8	原則同意
2.1.3 信賴憑證者之義務	10-11	原則同意
2.6.1 政府憑證總管理中心之資訊公布	15-16	原則同意
2.7.2 稽核人員之身分及資格	17	原則同意

變更後記載內容	變更後頁數	審查意見
2.8.1 機密之資訊種類	18-19	原則同意
2.9 權利歸屬	20-21	原則同意
3.1.1 命名種類	22	原則同意
3.1.4 命名之獨特性	22	原則同意
3.2.1 憑證之金鑰更換	24	原則同意
3.2.2 憑證展期	25	原則同意
4.1 申請憑證之程序	27	原則同意
4.6.2 歸檔之保留期限	40	原則同意，並建議修改: 歸檔資料逾保留期限後，書面資料得[刪除]應[新增]以安全方式銷毀；電子形式資料檔得另備份至其他儲存媒體並提供適當保護，或逕行以安全方式銷毀。
4.6.5 時戳紀錄之要求	41	原則同意
4.7 金鑰更換	42	原則同意，關於舊金鑰於更換後仍須保護至不再簽發憑證廢止清冊後再進行銷毀之敘述，建議於「6.2.9 私密金鑰之銷毀方式」統一說明即可
5.1.4 水災防範及保護	46	原則同意
5.2.1 信賴角色	48	原則同意

變更後記載內容	變更後頁數	審查意見
5.2.3 每個任務所需之人數	50-51	原則同意
5.3.7 聘僱人員之規定	54-55	原則同意
6.1.1 金鑰對之產製	56	原則同意，並建議修改: 總管理中心依照 6.2.1 節規定，於硬體密碼模組內產製金鑰對，採符合 FIPS140 亂數產生機制及 RSA 金鑰演算法，私密金鑰在硬體密碼模組內產製後，除金鑰備份回復及更換密碼模組情形外，皆應儲存於硬體密碼模組內不得匯出[新增]~~不外洩~~[刪除]。
6.1.4 政府憑證總管理中心公開金鑰安全傳送給信賴憑證者	57	原則同意
6.1.5 金鑰長度	58	原則同意
6.1.7 金鑰參數品質之檢驗	58	原則同意
6.1.9 金鑰之使用目的	59	原則同意
6.2.1 密碼模組標準	59	原則同意
6.2.5 私密金鑰歸檔	61	原則同意
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 政府憑證總管理中心公開金鑰及私密金鑰之使用期限	63	原則同意，並建議修改: 總管理中心公開金鑰及私密金鑰之金鑰長度為 RSA 4096 位元，~~公~~

變更後記載內容	變更後頁數	審查意見
		~~開金鑰憑證之~~[刪除]使用期限至多為 30 年，~~私密金鑰~~[刪除]但以其執行簽發憑證用途[新增]之使用期限至多為 10 年。
6.3.2.2 交互認證憑證機構公開金鑰及私密金鑰之使用期限	63	原則同意
6.6.3 生命週期安全評等	66	原則同意
7.1.3 演算法物件識別碼	68-69	原則同意
7.1.9 關鍵憑證政策擴充欄位之語意處理	69-70	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1.7版(草案)審查意見表

變更後記載內容	變更後頁數	審查意見
	全文	將文中有關雜湊演算法 SHA-2、SHA-256 之用語統一
	i-ii	調整目錄格式
1.1.1 CA 公鑰憑證的種類 (2)自發憑證（Self-Issued Certificate）：	1	原則同意
1.1.2 CA 公鑰憑證的設計原則	2	原則同意
1.1.3 CA 公鑰憑證的欄位	3-6	原則同意，並建議修改: 第 5 頁「Self-Issued Certificate」的表格中，欄位名稱有誤，原「Cross Certificate」應改為「Self-Issued Certificate」
1.2.1 用戶公鑰憑證的種類	7-9	原則同意，並建議修改: GPKI 之用戶公鑰憑證的種類目前包括政府機關(構)公鑰憑證、政府單位公鑰憑證、公司憑證、分公司憑證、商號憑證、社團法人憑證、財團法人憑證、學校憑證、自由職業事務所憑證、其他組織或團體憑證、自然人憑證、伺服器應用軟體憑證、~~自然人憑證~~[刪除]、OCSP 伺服器憑證[新

變更後記載內容	變更後頁數	審查意見
		增]，各憑證的相關用戶為：
1.3 憑證格式	12	原則同意
1.3.1 To-Be-Signed 自簽憑證格式	13-16	原則同意
1.3.2 To-Be-Signed 自發憑證格式	17-26	原則同意
1.3.3 To-Be-Signed 交互憑證格式	26	原則同意
1.3.4 To-Be-Signed 政府機關憑證格式	35	原則同意
1.3.5 To-Be-Signed 政府單位憑證格式	43	原則同意
1.3.6 To-Be-Signed 公司憑證格式	51-52	原則同意
1.3.7 To-Be-Signed 分公司憑證格式	59-60	原則同意
1.3.8 To-Be-Signed 商號憑證格式	68	原則同意
1.3.9 To-Be-Signed 社團法人憑證格式	76	原則同意
1.3.10 To-Be-Signed 財團法人憑證格式	84	原則同意
1.3.11 To-Be-Signed 學校憑證格式	93	原則同意
1.3.12 To-Be-Signed 醫事機構憑證格式	101	原則同意
1.3.13 To-Be-Signed 自由職業事務所憑證格式	109-110	原則同意
1.3.14 To-Be-Signed 其他組織或團體憑證格式	118	原則同意
1.3.15 To-Be-Signed 自然人憑證格式	126	原則同意

變更後記載內容	變更後頁數	審查意見
1.3.16 To-Be-Signed 醫事人員憑證格式	134	原則同意
1.3.17.1 To-Be-Signed SSL 類伺服應用軟體憑證格式	143-151	原則同意
1.3.17.2 To-Be-Signed 專屬類伺服應用軟體憑證格式	152	原則同意
1.3.17.3 To-Be-Signed 時戳伺服應用軟體憑證格式	161	原則同意
1.3.18 To-Be-Signed OCSP 伺服器憑證格式	169-176	原則同意
2.4 憑證廢止清冊格式	179	原則同意
2.4.1 To-Be-Signed 完整憑證廢止清冊(Complete CRL)的內容	180	原則同意
2.4.2 To-Be-Signed 異動憑證廢止清冊(Delta CRL)的內容	187	原則同意
2.4.3 To-Be-Signed 部分憑證廢止清冊(Partitioned CRL)的內容	195	原則同意