法規名稱：憑證實務作業基準應載明事項準則

發布日期：民國 93 年 07 月 07 日

第 一 章 總則

第 1 條

本準則依電子簽章法第十一條第二項規定訂定之。

第 2 條

本準則用詞之定義如下：

一、保證：指得據以信賴該個體已符合特定安全要件之基礎。

二、保證等級：指在具相對性保證層級中之某一級數。

三、憑證政策：指為指明某一憑證所適用之對象或情況所列舉之一套規則，該對象或情況可為特定之社群或具共同安全需求之應用。

四、物件識別碼：指一種以字母或數字組成之唯一識別碼，該識別碼必須依國際標準組織所訂定之註冊標準加以註冊，並可被用以識別唯一與之對應之憑證政策；憑證政策修訂時，其物件識別碼不必然隨之變更。

五、用戶：指憑證中所命名或識別之主體，且其持有與憑證中所載公開金鑰相對應之私密金鑰者。

六、信賴憑證者：指信賴所收受之憑證者。

七、儲存庫：指用以儲存及供檢索憑證與其他相關憑證資訊之系統。

八、憑證廢止清冊：指由憑證機構以數位方式簽署之已廢止憑證表列。

九、啟動資訊：操作密碼模組時所要求且必須被保護之金鑰以外資料值。

第 3 條

憑證機構應製作憑證實務作業基準（以下簡稱作業基準）重要事項置於其作業基準之首頁，載明下列事項：

一、主管機關核定文號。

二、所簽發憑證之種類。

三、所簽發各種憑證之保證等級。

四、所簽發各種憑證之適用範圍及使用限制。

五、法律責任限制及申請廢止憑證處理期間內之責任分擔。

六、其作業基準所描述的認證服務是否經第三人稽核或取得任何標章。

第 4 條

憑證機構應於其作業基準中載明其所支援憑證政策之名稱，並提供該憑證政策之物件識別碼及應載明補充其作業基準內容之其他重要文件。

第 5 條

憑證機構應於其作業基準中載明參與認證服務運作及維持之重要成員及其分工；如係以委外方式參與提供服務者，並應載明受任者之名稱或資格。

第 6 條

憑證機構應於其作業基準中載明可供用戶或信賴憑證者報告遺失私密金鑰等事件及諮詢作業基準疑義之聯絡電話、郵遞地址及電子郵件信箱。

第 7 條

憑證機構應於其作業基準中載明下列用戶應注意事項：

一、確保在申請憑證時所提供之資訊正確無誤。

二、用戶需自行產製金鑰時，安全的產製並保管其私密金鑰。

三、遵守對於金鑰及憑證之使用限制。

四、就私密金鑰資料外洩或遺失等事件作出通知。

第 8 條

憑證機構應於其作業基準中載明下列信賴憑證者之注意事項：

一、驗證數位簽章之責任。

二、僅於憑證使用目的範圍內信賴該憑證。

三、查驗憑證狀態。

四、了解有關憑證機構法律責任之條款。

第 9 條

憑證機構就資訊之公布及儲存庫之維護及營運應載明下列事項：

一、憑證、憑證狀態、憑證實務作業基準及憑證政策等資訊之公布方法。

二、前揭資訊公布之頻率或時間。

三、儲存庫之接取控管。

第 10 條

憑證機構應於其作業基準中載明作業基準變更時通知之方法。

第 11 條

憑證機構應於其作業基準中載明下列財務責任事項：

一、憑證機構就其可能或實際發生之賠償責任所提供之財務保證。

二、憑證機構就其經營是否加入任何保險。

三、憑證機構是否經由第三人進行財會稽核。

第 12 條

憑證機構應於其作業基準中載明就所提供之認證服務或憑證之使用所生糾紛之處理程序及所適用

之法律。

第 13 條

憑證機構應於其作業基準中載明用戶是否得請求退費；用戶得請求退費者，並應載明請求退費之程序。

第 14 條

憑證機構應於其作業基準中載明下列稽核或評核事項：

一、稽核或評核之頻率。

二、進行稽核或評核人員之資格。

三、稽核或評核人員中立性之確保。

四、稽核或評核之範圍。

五、對於稽核或評核結果之因應方式。

六、稽核或評核報告公開之範圍及方法。

第 15 條

憑證機構應於其作業基準中載明其所保護用戶個人資料之種類及維持資訊保密之方法：

一、應為機密資訊之種類。

二、個人資料保護之相關事項。

第 二 章 識別及鑑別程序

第 16 條

憑證機構應於其作業基準中載明所採用之命名規則。

第 17 條

憑證機構應於其作業基準中載明申請人證明擁有與所登記之公開金鑰相對應私密金鑰之方式。

第 18 條

憑證機構應於其作業基準中載明申請人身分鑑別之要件及程序。

第 19 條

憑證機構應於其作業基準中載明憑證機構於廢止憑證及暫時停用憑證申請時，安全識別及鑑別用戶之程序。

第 三 章 營運規範

第 20 條

憑證機構應於其作業基準中載明申請各種憑證之程序。

第 21 條

憑證機構應於其作業基準中載明簽發憑證、憑證展期及憑證內容修改時，用戶接受憑證之程序。

第 22 條

憑證機構提供憑證暫時停用服務者，應於其作業基準中載明下列事項：

一、得請求暫時停用憑證之事由。

二、憑證機構得逕行暫時停用憑證之事由。

三、有權請求暫時停用憑證之人。

四、請求暫時停用憑證之程序。

五、暫時停用之期間。

六、憑證機構處理暫時停用請求之期間。

七、恢復使用憑證之程序。

第 23 條

憑證機構就憑證之廢止應於其作業基準中載明下列事項：

一、得請求廢止憑證之事由。

二、憑證機構得逕行廢止憑證之事由。

三、有權請求廢止憑證之人。

四、請求廢止憑證之程序。

五、憑證機構處理廢止憑證請求之期間。

六、憑證機構發出憑證廢止清冊之頻率。

七、是否提供線上憑證狀態查詢。

第 四 章 非技術性安全控管

第 24 條

憑證機構應於其作業基準中載明其所採行之實體、運作程序及人員安全之控管措施。

第 25 條

憑證機構應於其作業基準中載明下列紀錄歸檔事項：

一、所記錄事件之類型，應包括所有驗證憑證內容所必須之檔案資料。

二、歸檔保留期間。

三、歸檔之保護。

四、歸檔備份程序。

五、紀錄對於時戳之要求。

六、紀錄檔處理頻率。

第 26 條

憑證機構應於其作業基準中載明下列憑證機構金鑰變更時之處理程序：

一、因應驗證憑證需求，以原公開金鑰驗證新公開金鑰之處理程序。

二、提供新的公開金鑰之方法。

第 27 條

憑證機構應於其作業基準中載明危害及災變復原程序之規劃。

第 28 條

憑證機構應於其作業基準中載明下列終止任一憑證簽發服務時之處理程序：

一、通知及公告之程序。

二、現行有效憑證之因應處理。

三、紀錄檔案移交或保管年限。

第 五 章 技術性安全控管

第 29 條

憑證機構就金鑰對之產製及安裝，應於其作業基準中載明下列事項：

一、用戶金鑰對由誰產製。

二、金鑰對非由用戶自行產製時，私密金鑰如何安全傳送予用戶。

三、憑證機構公開金鑰如何安全傳送予用戶或信賴憑證者。

四、金鑰長度。

五、金鑰生成參數及參數品質檢驗。

六、金鑰之使用目的。

第 30 條

憑證機構就私密金鑰保護，應於其作業基準中載明下列事項：

一、密碼模組是否符合特定標準。

二、是否採行金鑰分持之多人控管。

三、私密金鑰是否託管、備份、歸檔或輸入至密碼模組；如進行託管、備份、歸檔或輸入至密碼模組者，其方法及程序。

四、私密金鑰之啟動、停用及銷毀方式。

第 31 條

憑證機構應於其作業基準中載明憑證有效期限、公開金鑰是否歸檔及公開金鑰與私密金鑰各別之使用期限。

第 32 條

憑證機構應於其作業基準中載明對於啟動資訊之保護措施。

第 33 條

憑證機構應於其作業基準中載明所採行之系統軟體及網路安全控管措施。

第 六 章 格式剖繪

第 34 條

憑證機構就憑證之格式剖繪應於其作業基準中載明下列事項：

一、版本序號。

二、憑證擴充欄位。

三、演算法物件識別碼。

四、命名形式。

五、命名限制。

六、憑證政策物件識別碼。

七、政策限制擴充欄位之使用。

八、對關鍵憑證政策擴充欄位之語意處理。

第 35 條

憑證機構就憑證廢止清冊之格式剖繪應於其作業基準中載明下列事項：

一、版本序號。

二、憑證廢止清冊及憑證廢止清冊擴充欄位。

第 36 條

本準則自發布日施行。