數位簽章憑證實務作業基準應載明事項

壹、總則

一、本事項用詞定義

（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。

二、重要事項概述

下列事項應以摘要方式置於憑證實務作業基準內容之前：

（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）憑證實務作業基準所描述的認證服務是否經第三方稽核或取得任何標章。

三、文件名稱與物件識別碼

應載明憑證實務作業基準所支援之憑證政策名稱，並提供該憑證政策之物件識別碼及補充其作業基準內容之其他重要文件。

四、成員及分工

應載明運作及維持公開金鑰基礎設施服務之主要成員及其分工，包括憑證管理中心、註冊中心、用戶、信賴憑證者及其他相關成員。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。

五、憑證用途

應載明憑證用途，包括適用範圍與禁止適用範圍。

六、政策管理

應載明負責制定、登錄、維護與更新憑證政策與作業基準之單位名稱，以及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。

七、用戶注意事項

應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。

八、信賴憑證者注意事項

應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。

九、名詞定義與縮寫

應載明憑證實務作業基準中相關名詞定義與英文名詞縮寫對照。

十、資訊公布與儲存庫責任

應載明下列事項：

（一）儲存庫之維運單位。例如：憑證管理中心、憑證產製單位或其他獨立儲存庫服務提供者。

（二）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。

（三）前揭資訊公布之頻率或時間。

（四）儲存庫之存取控管。

貳、身分識別與認證程序

十一、命名規則

應載明下列事項：

（一）命名格式類型。

（二）命名需有意義與否。

（三）用戶使用匿名或假名之限制。

（四）解讀不同命名格式之規則。

（五）命名需具獨特性與否。

（六）是否適用商標之認可或認證。

十二、用戶初始註冊之身分識別與認證

應載明用戶初始註冊之身分識別與認證程序，包括：

（一）身分識別所需文件或信物。

（三）如何認證用戶所提供之文件或信物。

（三）用戶需親臨與否。

（四）個人得否及如何代表組織申請註冊。

（五）用戶是否需證明擁有與所登記之公開金鑰相對應之私密金鑰。

（六）此身分識別與認證程序所適用之保證等級標準、其所對應之保證等級強度，及是否具數位簽章推定為用戶本人之效力。

用戶初始註冊身分識別與認證程序之保證等級強度至少應相當於下列標準之一者，始得推定為用戶本人：

（一）ISO/IEC 29115「高度」(high)以上等級。

（二）美國 NIST SP 800-63A 數位身分指引「二」(IAL2)以上等級。

（三）歐盟 eIDAS 規則定義之數位身分保證等級「實質」(Substantial)以上等級。

十三、更換金鑰請求之身分識別與認證

應載明用戶請求更換金鑰之身分識別與認證程序、身分識別與認證程序所適用之保證等級標準、其所對應之保證等級強度，及是否具前點第二項數位簽章推定為用戶本人之效力。

十四、請求廢止憑證之身分識別與認證

應載明用戶請求廢止憑證之身分識別與認證程序、身分識別與認證程序所適用之保證等級標準、其所對應之保證等級強度，及是否具第十二點第二項數位簽章推定為用戶本人之效力。

參、憑證生命週期營運規範

十五、憑證申請程序

應載明憑證申請之程序，包括申請者資格、申請註冊程序及申請處理程序。

十六、憑證簽發及用戶接受憑證之程序

應載明下列事項：

（一）憑證機構在憑證簽發過程中採取之行動。

（二）憑證簽發時憑證機構對用戶之通知機制。

（三）用戶接受憑證之行為要件。

（四）於儲存庫或其他管道發布憑證或對註冊中心等其他參與者之通知。

十七、金鑰對與憑證用途

應載明用戶之私鑰與憑證用途及使用責任，以及信賴憑證者之公鑰與憑證用途及使用責任。

十八、憑證展期

應載明下列事項：

（一）展期事由。

（二）請求展期者之資格或條件。

（三）展期處理程序。

（四）對用戶簽發展期憑證之通知。

（五）用戶接受展期憑證之行為要件。

（六）於儲存庫或其他管道發布展期憑證或對註冊中心等其他參與者之通知。

十九、憑證之金鑰更換

應載明下列事項：

（一）金鑰更換事由。

（二）更換金鑰請求者之資格或條件。

（三）金鑰更換處理程序。

（四）對用戶更換金鑰之通知。

（五）用戶接受金鑰更換之行為要件。

（六）於儲存庫或其他管道發布金鑰更換或對註冊中心等其他參與者之通知。

二十、憑證變更

應載明下列事項：

（一）憑證變更事由。

（二）憑證變更請求者之資格或條件。

（三）憑證變更處理程序。

（四）對用戶簽發新憑證之通知。

（五）用戶接受新憑證之行為要件。

（六）於儲存庫或其他管道發布新憑證或對註冊中心等其他參與者之通知。

二十一、憑證暫停使用

應載明下列事項：

（一）暫時停用憑證之事由。

（二）暫時停用憑證請求者之資格或條件。

（三）請求暫時停用憑證之程序。

（四）暫時停用之期間。

（五）恢復使用憑證之程序。

（六）金鑰被破解時是否適用憑證暫停使用程序。

二十二、憑證廢止

應載明下列事項：

（一）憑證廢止之事由。

（二）憑證廢止請求者之資格或條件。

（三）請求憑證廢止之程序與申請寬限期。

（四）憑證機構處理憑證廢止請求之期間。

（五）是否使用憑證廢止清冊、其發布頻率及距離下次發布之最遲時間。

（六）是否提供線上憑證廢止及狀態查詢服務與查詢服務相關規定。

（七）是否提供其他形式之廢止公告。

（八）金鑰被破解時是否適用憑證廢止程序。

二十三、憑證狀態服務

針對憑證狀態確認之服務應載明下列事項：

（一）服務特性。

（二）服務可用性及無法正常運作時之因應政策。

（三）是否有其他可選用之功能。

二十四、憑證服務終止

應載明憑證服務終止之處理程序。

二十五、私密金鑰託管與復原

應載明私密金鑰託管政策及復原作法。

肆、設施、管理及作業控管

二十六、實體安全控管措施

應載明下列事項：

（一）實體所在位置與結構。

（二）實體存取機制。

（三）電力與空調控管。

（四）水災防範。

（五）火災防範。

（六）媒體儲存機制。

（七）汰除設備處理。

（八）異地備援機制。

二十七、運作程序控管措施

應載明下列事項：

（一）各運作程序所需之信賴角色、任務與權責劃分。同一位人員不應兼任二種以上信賴角色。

（二）執行各運作程序任務所需之人數。

（三）識別各運作程序執行人員身分之方式。

二十八、人員安全控管措施

應載明下列事項：

（一）不同信賴角色所需人員之資格、背景、經歷與條件。

（二）前款人員資格、背景、經歷與條件之查驗程序。

（三）教育訓練及其頻率要求。

（四）不同信賴角色職務輪調之頻率與次序。

（五）人員違規之懲處。

（六）約聘人員之控管。

（七）提供給人員之文件控管。

二十九、稽核紀錄程序

應載明下列事項：

（一）記錄之事件類型。

（二）稽核紀錄處理或歸檔頻率。

（三）稽核紀錄保存期限。

（四）保護稽核紀錄之方法。

（五）稽核紀錄備份程序。

（六）稽核紀錄彙整系統建於憑證機構內或外。

（七）稽核事件發起人是否需被通知。

（八）弱點評估。

三十、紀錄歸檔

應載明下列事項：

（一）所歸檔之紀錄類型，如所有稽核資料、憑證申請資訊及文件。

（二）歸檔保留期間。

（三）歸檔之保護。

（四）歸檔備份程序。

（五）歸檔紀錄之時戳要求。

（六）歸檔彙整系統建於憑證機構內或外。

（七）取得及驗證歸檔資訊之程序。

三十一、金鑰變更處理

應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。

三十二、危害及災變復原

應載明下列事項：

（一）事故識別、危害通報與處理程序。

（二）電腦資源、軟體及資料遭破壞或疑似遭破壞之復原程序。

（三）憑證機構金鑰遭破解之復原程序。

（四）災變後憑證機構確保營運持續之能力與程序。

三十三、憑證管理中心或註冊中心終止服務

應載明下列憑證管理中心或註冊中心終止服務之處理程序：

（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。

伍、技術性安全控管

三十四、金鑰對產製及安裝

應載明下列事項：

（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。

三十五、私密金鑰保護及密碼模組工程控管措施

應載明下列事項：

（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。

（四）私密金鑰與密碼模組間傳輸之情況。

（五）私密金鑰如何儲存於密碼模組。

（六）私密金鑰之啟動、停用及銷毀方式。

三十六、金鑰對管理其他事項

應載明憑證有效期限、公開金鑰是否歸檔及公開金鑰與私密金鑰之使用期限。

三十七、啟動資料

應載明啟動資料之產生與保護措施。

三十八、電腦安全控管措施

應載明電腦安全控管措施，包括採用可信任運算基礎概念等特定電腦安全技術要求及電腦安全評等。

三十九、生命週期安全控管措施

應載明系統生命週期安全控管措施，包括系統開發、安全管理及其他處理生命週期評等相關措施。

四十、網路安全控管措施

應載明網路安全相關控管措施，包括防火牆。

四十一、時間戳記

應載明針對不同資料所使用之時間戳記要求。

陸、格式剖繪

四十二、憑證格式剖繪

應載明下列事項：

（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）政策限定元之語法與語意。

（九）對關鍵憑證政策擴充欄位之語意處理。

四十三、憑證廢止清冊之格式剖繪

應載明下列事項：

（一）版本序號。

（二）憑證廢止清冊及憑證廢止清冊擴充欄位。

四十四、線上憑證狀態協定之格式剖繪

應載明下列事項：

（一）版本序號。

（二）線上憑證狀態協定擴充欄位。

柒、稽核與評估

四十五、稽核及評估事項

應載明下列事項：

（一）稽核或評估之範圍或事項列表。

（二）稽核或評估之執行方法與頻率。

（三）執行稽核或評估人員之身分與資格。

（四）稽核或評估方與被稽核或被評估方之關係，包括稽核或評估方之獨立性程度。

（五）對稽核或評估結果之因應作為。

（六）稽核或評估結果公開之範圍、對象及方法。

捌、其他業務與法律事項

四十六、費用

應載明下列事項：

（一）憑證簽發或展期費用。

（二）憑證查詢費用。

（三）憑證廢止或狀態資訊查詢費用。

（四）憑證實務作業或作業基準相關資訊查詢等其他服務費用。

（五）退費政策。

四十七、財務責任

應載明下列事項：

（一）經營憑證服務所需之基本資產狀況。

（二）經營憑證服務對他人可能造成或實際發生損害賠償責任之保險涵蓋範圍。

（三）憑證機構第一方保險或對終端使用者之保固。

四十八、業務資訊保密

應載明下列事項：

（一）機密資訊界定方式與範圍。

（二）機密資訊接收者之保密義務。

四十九、個人資料隱私保護

應載明下列事項：

（一）個人資料或隱私保護計畫。

（二）個人資料或隱私資訊之界定方式與範圍。

（三）蒐集、處理、利用個人資料或隱私資訊之責任。

（四）個人資料或隱私資訊揭露予非公務機關及公務機關之程序與作法，如告知個人資料或隱私資訊當事人、取得同意等。

五十、智慧財產權

應載明智慧財產權保護事項，包括著作權、商標、專利及營業秘密。

五十一、承諾、責任與賠償

應載明下列事項：

（一）憑證管理中心、註冊中心、用戶、信賴方及其他參與者之保證與承諾事項。

（二）免責聲明事項。

（三）責任限制事項。

（四）賠償事項。

五十二、憑證實務作業基準有效期限與終止

應載明下列事項：

（一）憑證實務作業基準有效期限。

（二）憑證實務作業基準終止條件。

（三）憑證實務作業基準終止之效果。

五十三、個別通知與通訊

應載明對相關參與者之個別通知與通訊方式。

五十四、憑證實務作業基準修訂程序與變更通知

應載明憑證實務作業基準內容修訂程序與修訂後之處理程序，例如通知用戶與信賴方之方法與程序。

五十五、紛爭處理與準據法

應載明下列事項：

（一）針對所提供之認證服務或憑證使用所生糾紛之紛爭處理程序。

（二）解釋與執行作業基準之準據法。

五十六、其他適用法律

憑證機構若有其他相關法律必須遵循，應予載明。