憑證實務作業基準應載明事項檢核對照表（表三）

CPS Required Information Check List (Form 3)

申請人名稱 Applicant	憑證實務作業基準版本編號 CPS Version Number

憑證實務作業基準應載明事項 CPS Required Information			申請核定憑證實務作業基準之記載 Record Of CPS Approval Application	
條次 Article No.	憑證實務作業基準應載明事項內容 Contents of CPS Required Information		對應章節編號 Corresponding Chapter/Section Number	對應頁碼 Corresponding Page Number
第三條	憑證機構應製作憑證實務作業基準（以下簡	一、 主管機關核定文號。 1. The approval number issued by the competent authority		

Article 3	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： A certification service provider shall specify the following significant particulars on the first page of the certification practice statement (CPS):	二、 所簽發憑證之種類。 2. Types of certificates		
		三、 所簽發各種憑證之保證等級。 3. Assurance levels of certificates		
		四、 所簽發各種憑證之適用範圍及使用限制。 4. Applicability and restrictions on certificate usage		
		五、 法律責任限制及申請廢止憑證處理期間內之責任分擔。 5. Limitations of legal liability, and allocation of liability within the application period for certificate revocation		

		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。 6. Whether the certification services are audited by a third party or have been granted any logos		
第四條 Article 4	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。 A certification service provider shall specify the supported CPS, provide the OIDs of the CPS, and specify other significant documents supporting the CPS.			
第五條 Article 5	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。 A certification service provider shall specify the identities or types of entities that fill the roles of participants operating and maintaining the certification service. In the event that an entity participates in the certification service by outsourcing, the certification service provider shall also specify the name and qualification of such entity.			

第六條 Article 6	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。 A certification service provider shall specify the telephone number, mailing address and electronic mail address of a contact person to subscribers or relying parties to use for reporting the loss of a private key and when consulting on matters of the CPS.			
第七條 Article 7	憑證機構應於其作業基準中載明下列用戶應注意事項： A certification service provider shall specify the following subscriber obligations:	一、 確保在申請憑證時所提供之資訊正確無誤。 1. Ensuring accuracy of representations in certificate applications		
		二、 用戶需自行產製金鑰時，安全的產製並保管其私密金鑰。 2. Safely generating and guarding the private key where the private key is generated by the subscriber		
		三、 遵守對於金鑰及憑證之使用限制。 3. Complying with the restrictions on private key and certificate usage		

		四、就私密金鑰資料外洩或遺失等事件作出通知。 4. Notifying on matters of private key compromise or loss		
第八條 Article 8	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： A certification service provider shall specify the following replying party obligations:	一、 驗證數位簽章之責任。 1. Taking responsibilities to verify digital signatures		
		二、 僅於憑證使用目的範圍內信賴該憑證。 2. Placing reliance on the certificate within the documented scope of certificate usage		
		三、 查驗憑證狀態。 3. Inspecting the certificate status		
		四、 了解有關憑證機構法律責任之條款。 4. Acknowledging the legal liability provisions on certification service providers		
第九條	憑證機構就資訊之公布及儲存庫之維護及營運應載明下	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。 1. The methods it publishes information such as certificates, certificate status, CPS and CP		

Article 9	列事項： A certification service provider shall specify the following particulars in regards to the publication of information and the operation and maintenance of repositories:	二、 前揭資訊公布之頻率或時間。 2. When information must be published and the frequency of publication		
		三、 儲存庫之接取控管。 3. Access control on repositories		
第十條 Article 10	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。 A certification service provider shall specify a notification mechanism in the case of CPS modification.			

第十一條 Article 11	憑證機構應於其作業基準中載明下列財務責任事項： A certification service provider shall specify the following particulars in regards to financial responsibility:	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。 1. Amount of insurance coverage provided by a certification service provider for liability for potential and actual damages		
		二、 憑證機構就其經營是否加入任何保險。 2. Whether the operation of the certification service provider is covered by insurance		
		三、 憑證機構是否經由第三人進行財會稽核。 3. Whether financial audit of the certification service provider is implemented by a third party		
第十二條 Article 12	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。 A certification service provider shall specify the dispute resolution procedures and governing and applicable laws to resolve disputes arising out of the certification service or certificate usage.			

第十三條 Article 13	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。 A certification service provider shall specify whether subscribers can request for refund. If applicable, it shall also specify the procedures for refund.			
第十四條 Article 14	憑證機構應於其作業基準中載明下列稽核或評核事項： A certification service provider shall specify the following particulars in regards to compliance audits or other assessments:	一、 稽核或評核之頻率。 1. Frequency of compliance auditsor other assessments		
		二、 進行稽核或評核人員之資格。 2. The qualifications of the personnel performing the audit or other assessment		
		三、 稽核或評核人員中立性之確保。 3. Assurance of the independence of the personnel performing the audit or other assessment		
		四、 稽核或評核之範圍。 4. The scope of the compliance audit or other assessment		
		五、 對於稽核或評核結果之因應方式。 5. Corrective actions taken as a result of deficiencies found during the compliance audit or other assessment		

		六、 稽核或評核報告公開之範圍及方法。 6. The scope and means used to disclose the reports of compliance audit or other assessment		
第十五條 Article 15	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： A certification service provider shall specify the types of personal information of subscribers to be protected and methods to keep the information confidential:	一、 應為機密資訊之種類。 1. Types of information to be kept confidential		
		二、 個人資料保護之相關事項。 2. Relevant particulars concerning personal information protection		

第十六條 Article 16	憑證機構應於其作業基準中載明所採用之命名規則。 A certification service provider shall specify the rules of naming it adopts.		
第十七條 Article 17	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。 A certification service provider shall specify the methods used to prove the applicant's possession of private key that corresponds to the registered public key.		
第十八條 Article 18	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。 A certification service provider shall specify the identification and authentication requirements and procedures for applicants.		

第十九條 Article 19	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。 A certification service provider shall specify a secure identification and authentication procedure for a revocation or suspension request.			
第二十條 Article 20	憑證機構應於其作業基準中載明申請各種憑證之程序。 A certification service provider shall specify the procedures to process applications for various certificates.			
第二十一條 Article 21	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。 A certification service provider shall specify conduct of subscribers that constitutes acceptance of the certificate in regards to certificate issuance, renewal, and modification.			
第二十二條	憑證機構提供憑證暫時停用服務者，	一、 得請求暫時停用憑證之事由。 1. Circumstances under which a certificate may be suspended upon request		

Article 22	應於其作業基準中載明下列事項： A certification service provider that provides certificate suspension service shall specify the following particulars:	二、 憑證機構得逕行暫時停用憑證之事由。 2. Circumstances under which a certificate may be suspended by a certification service provider		
		三、 有權請求暫時停用憑證之人。 3. Those who are entitled to request the suspension of a certificate		
		四、 請求暫時停用憑證之程序。 4. Procedures to request certificate suspension		
		五、 暫時停用之期間。 5. How long the suspension may last		
		六、 憑證機構處理暫時停用請求之期間。 6. The time within which a certification service provider must process the suspension request		
		七、 恢復使用憑證之程序。 7. Procedures to restore certificate usage		
第二十三條	憑證機構就憑證之廢止應於其作業基	一、 得請求廢止憑證之事由。 1. Circumstances under which a certificate may be revoked upon request		

Article 23	準中載明下列事項： A certification service provider shall specify the following particulars in regards to certificate revocation:	二、 憑證機構得逕行廢止憑證之事由。 2. Circumstances under which a certificate may be revoked by a certification service provider		
		三、 有權請求廢止憑證之人。 3. Those who are entitled to request the revocation of the certificate		
		四、 請求廢止憑證之程序。 4. Procedures used for certificate revocation request		
		五、 憑證機構處理廢止憑證請求之期間。 5. The time within which a certification service provider must process the revocation request		
		六、 憑證機構發出憑證廢止清冊之頻率。 6. Issuance frequency of a Certificate Revocation List (CRL) made by a certification service provider		
		七、 是否提供線上憑證狀態查詢。 7. On-line revocation/status checking availability		

第二十四條 Article 24	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。 A certification service provider shall specify the physical, procedural, and personnel security controls it adopts.			
第二十五條 Article 25	憑證機構應於其作業基準中載明下列紀錄歸檔事項： A certification service provider shall specify the following particulars in regards to archival records:	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。 1. Types of records that are archived, which shall include all the data information necessary for certificate verification		
		二、 歸檔保留期間。 2. Retention period for an archive		
		三、 歸檔之保護。 3. Protection of an archive		
		四、 歸檔備份程序。 4. Archive backup procedures		
		五、 紀錄對於時戳之要求。 5. Requirements for time-stamping of records		

		六、 紀錄檔處理頻率。 6. Management frequency of archived records		
第二十六條 Article 26	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： A certification service provider shall specify the following procedures for key change over:	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。 1. For certificate verification, the procedures of certifying the new public key with the old public key		
		二、 提供新的公開金鑰之方法。 2. The methods used to provide a new public key		
第二十七條 Article 27	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。 A certification service provider shall specify the plan relating to the recovery procedures in the event of data compromise or disaster.			

第二十八條 Article 28	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： A certification service provider shall specify the following procedures for termination of any certification issuance service:	一、 通知及公告之程序。 1. Procedures for notification and publication		
		二、 現行有效憑證之因應處理。 2. Arrangements for the use of still valid certificates		
		三、 紀錄檔案移交或保管年限。 3. The transfer of archival records and the retention period		
第二十九條	憑證機構就金鑰對	一、 用戶金鑰對由誰產製。 1. Who generates the subscriber's public, private key pair		

Article 29	之產製及安裝，應於其作業基準中載明下列事項： A certification service provider shall specify the following particulars in regards to key pair generation and installation:	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。 2. Where the key pair is not generated by the subscriber, how is the private key provided securely to the subscriber		
		三、 憑證機構公開金鑰如何安全傳送予用戶或信賴憑證者。 3. How is the certification service provider's public key provided securely to subscribers or relying parties		
		四、 金鑰長度。 4. Key sizes		
		五、 金鑰生成參數及參數品質檢驗。 5. Public key parameters generation and quality checking		
		六、 金鑰之使用目的。 6. Key usage purposes		

第三十條 Article 30	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： A certification service provider shall specify the following particulars in regards to private key protection:	一、 密碼模組是否符合特定標準。 1. Whether cryptographic module meets certain standards		
		二、 是否採行金鑰分持之多人控管。 2. Whether the private key is under n out of m multi-person control		
		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。 3. Whether the private key is escrowed, backed up, archived, or transferred and stored in a cryptographic module; if applicable, what methods and procedures are implemented		
		四、 私密金鑰之啟動、停用及銷毀方式。 4. Methods of activating, deactivating, and destroying the private key		

第三十一條 Article 31	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。 A certification service provider shall specify the operational period of the certificates, whether the public key is archived, and the usage periods for the key pair.			
第三十二條 Article 32	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。 A certification service provider shall specify the protection mechanism for activation data.			
第三十三條 Article 33	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。 A certification service provider shall specify measures for software system and network security controls.			
第三十四條	憑證機構就憑證之	一、 版本序號。 1. Version numbers		

Article 34	格式剖繪應於其作業基準中載明下列事項： A certification service provider shall specify the following particulars in regards to certificate profile:	二、 憑證擴充欄位。 2. Certificate extension		
		三、 演算法物件識別碼。 3. Algorithm object identifiers		
		四、 命名形式。 4. Naming format		
		五、 命名限制。 5. Naming constraints		
		六、 憑證政策物件識別碼。 6. CP OIDs		
		七、 政策限制擴充欄位之使用。 7. Usage of policy constraints extension		
		八、 對關鍵憑證政策擴充欄位之語意處理。 8. Processing semantics for the critical CP extension		

第三十五條 Article 35	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： A certification service provider shall specify the following particulars in regards to CRL profile:	一、 版本序號。 1. Version numbers		
		二、 憑證廢止清冊及憑證廢止清冊擴充欄位。 2. CRL and CRL entry extensions		