政府機關公開金鑰基礎建設憑證政策檢核對照表
（保證等級第三級）

申請者	憑證實務作業基準版本

憑證政策規定事項		申請交互認證之憑證實務作業基準	
章節	內容	對應章節	頁碼
1	加入本基礎建設的憑證機構必須經主管機關依據電子化政府電子認證服務分工建置之憑證機構，簽發之憑證應用於電子化政府各項應用		
1.1	憑證機構必須於憑證實務作業基準中載明所引用憑證政策之保證等級。本基礎建設之憑證機構應遵循本憑證政策，不可自訂憑證政策。未授權引用之憑證機構所引發的任何問題，概由該憑證機構自行負責		
1.2	憑證機構必須於憑證實務作業基準中載明所引用之憑證政策物件識別碼名稱及其值		
1.3	憑證機構必須於憑證實務作業基準中載明相關主要成員		
1.3.8	憑證屬於中級(Medium)的保證等級，適合應用於有惡意使用者會截取或篡改資訊、較第二級危險之網路環境，傳送的資訊包括金錢上的線上交易		
1.4	憑證機構必須於憑證實務作業基準中載明其制訂及管理機關，並載明其聯絡方式及審定與稽核權利		
2.1.1	憑證機構必須於憑證實務作業基準中載明憑證機構之職責		
2.1.2	憑證機構必須於憑證實務作業基準中載明註冊中心之職責		
2.1.3	憑證機構必須於憑證實務作業基準中載明用戶之義務		
2.1.4	憑證機構必須於憑證實務作業基準中載明信賴憑證者之義務		
2.1.5	憑證機構必須於憑證實務作業基準中載明儲存庫服務之義務		
2.2.1	憑證機構必須於憑證實務作業基準中載明憑證機構之法律責任		

2.2.2	憑證機構必須於憑證實務作業基準中載明註冊中心之法律責任		
2.3	憑證機構必須於憑證實務作業基準中載明對用戶及信賴憑證者之財務責任		
2.4	憑證機構必須於憑證實務作業基準中載明其所適用法律及紛爭處理程序		
2.5	憑證機構必須於憑證實務作業基準中載明憑證簽發、展期、查詢、憑證廢止、憑證狀態查詢和其它服務費用以及請求退費之程序		
2.6	憑證機構必須於憑證實務作業基準中載明其資訊公佈內容、公佈頻率、存取控制方式以及儲存庫相關資訊		
2.7	憑證機構必須至少每年接受一次的定期稽核，並於憑證實務作業基準中載明稽核方法，包括稽核頻率、稽核人員身份及資格、稽核人員及被稽核方關係、稽核範圍、對於稽核結果之因應方式及稽核結果公開之範圍		
2.8	憑證機構必須於憑證實務作業基準中載明其資訊保密之範圍，包括機密資訊之種類、非機密資訊之種類、憑證廢止或暫時停用資訊之公開以及應司法人員要求或民事訴訟要求或用戶要求等釋出資訊		
2.9	憑證機構必須於憑證實務作業基準中載明其所有之智慧財產權及其範圍		
3.1.1	憑證機構之憑證主體名稱應為 X.500 唯一識別名稱		
3.1.2	政府機關(構)、單位憑證之憑證主體名稱必須符合我國相關法令之規定		
3.1.3	憑證機構必須於憑證實務作業基準中載明憑證格式剖繪中各命名形式之解釋規則		
3.1.4	憑證機構必須於憑證實務作業基準中載明 X.500 名稱空間使用及確保憑證主體名稱名稱之獨特性		
3.1.5	憑證機構必須於憑證實務作業基準中載明命名爭議之解決程序		
3.1.7	憑證機構必須於憑證實務作業基準中載明擁有私密金鑰之證明方式		

3.1.8	組織身分鑑別之程序	（一）政府機關(構)或單位申請時應以正式公文書方式申請，須確認該機關(構)或單位確實存在，並應驗證公文書之真確性		
		（二）民間組織申請時應由代表人親臨或得以書面委託書方式委任代理人臨櫃辦理，除須確認申請資料及代表人身分的真實性外，並應驗證該代表人有權以該組織之名義申請		
3.1.9	個人身分鑑別之程序	（一）書面證件核對 用戶至少應出示足以證明其身份之證件正本(例如國民身分證)，供憑證機構或註冊中心鑑別用戶身分		
		（二）個人資料提交 應與該資料主管機關所登記資料(如戶籍資料)或其它經主管機關認可之可信賴第三者的登記資料進行比對		
		（三）申請者臨櫃辦理 用戶必須親臨憑證機構或註冊中心證明其身分。若用戶無法親自臨櫃辦理，得以書面委託書委任代理人代為臨櫃申請		
3.1.10	憑證機構必須於憑證實務作業基準中載明硬體裝置或伺服軟體之鑑別程序			
3.2.1	憑證機構必須於憑證實務作業基準中載明對下屬憑證機構的用戶之金鑰更換。用戶的身分可使用現行的簽章金鑰進行鑑別，但如與初始註冊時間間隔超過 9 年時，則應依照憑證政策規定重新辦理初始註冊			
3.2.2	憑證機構必須於憑證實務作業基準中載明憑證展期			
3.3	憑證機構必須於憑證實務作業基準中載明憑證廢止之金鑰更換			

3.4	憑證機構必須於憑證實務作業基準中載明憑證廢止申請之鑑別程序			
4.1	憑證機構必須於憑證實務作業基準中載明申請憑證之程序			
4.2	憑證機構必須於憑證實務作業基準中載明簽發憑證之程序。包括憑證簽發後通知申請者的方式，或不同意簽發憑證之通知方式			
4.3	憑證機構必須於憑證實務作業基準中載明接受憑證之程序。包括在憑證機構簽發憑證後，應經憑證申請者審視憑證內容並接受所簽發的憑證後，始得將簽發之憑證公佈到儲存庫上			
4.3	接受憑證應審視事項	（一）憑證申請者確認憑證接受或拒絕的方式		
		（二）憑證申請者決定接受憑證前應審視的憑證欄位		
		（三）憑證申請者拒絕接受憑證之處理方式		
4.4	憑證機構必須於憑證實務作業基準中載明憑證廢止服務之規定，並得依憑證應用範圍及服務品質決定是否提供憑證暫時停用服務			
4.4	憑證暫時停用及廢止之規定	（一）提供全天候的憑證廢止服務		
		（二）提供全天候的憑證暫時停用服務		
4.4.1	憑證機構必須於憑證實務作業基準中載明廢止憑證之事由			
4.4.2	憑證機構必須於憑證實務作業基準中載明憑證廢止之申請者			
4.4.3	憑證機構必須於憑證實務作業基準中載明憑證廢止之程序。			
4.4.4	憑證機構必須於憑證實務作業基準中載明處理廢止憑證請求之期間			
4.4.5	憑證機構必須於憑證實務作業基準中載明暫時停用憑證之事由			
4.4.6	憑證機構必須於憑證實務作業基準中載明暫時停用憑證之申請者			

4.4.7	憑證機構必須於憑證實務作業基準中載明暫時停用憑證之程序		
4.4.8	憑證機構必須於憑證實務作業基準中載明處理暫時停用憑證請求之期間及暫時停用憑證之期間		
4.4.9	憑證廢止清冊之簽發頻率必須每天至少一次		
4.4.10	信賴憑證者在使用憑證前必須查驗目前憑證的有效性，同時也必須驗證憑證廢止清冊的正確性和完整性		
4.4.11	憑證機構必須於憑證實務作業基準中載明是否提供及如何提供線上憑證狀態查詢服務		
4.4.12	信賴憑證者如不查驗憑證廢止清冊，則必須採用線上查詢憑證狀態的方式對憑證狀態進行確認		
4.5	憑證機構必須於憑證實務作業基準中載明所應具備之適當安全稽核記錄功能，並依照憑證政策之規定保留期限辦理歸檔		
4.5.1	憑證機構必須於憑證實務作業基準中載明稽核記錄應包括項目及憑證政策中規定應記錄的稽核事件		
4.5.2	憑證機構應至少每兩個月檢視稽核紀錄一次，並應對任何的惡意活動進行調查		
4.5.3	憑證機構應依照規定的管理機制保留稽核紀錄檔至少兩個月以上		
4.5.4	憑證機構之電子稽核日誌系統必須包含保護機制，手動的稽核資訊亦應加以保護，以確保不會遭未經授權的閱讀、修改及刪除		
4.5.5	憑證機構應至少每個月備份一次稽核紀錄		
4.5.6	憑證機構必須於憑證實務作業基準中載明安全稽核系統之啟用及停止		
4.5.7	憑證機構之稽核系統並不需要告知引起事件的個體		
4.5.8	憑證機構必須於憑證實務作業基準中載明安全控管弱點評估之執行項目		
4.6.1	憑證機構必須於憑證實務作業基準中載明歸檔時應記錄之事件類型及資料		
4.6.2	憑證機構應依照憑證政策之規定，至少保留稽核紀錄的歸檔資料十年以上		
4.6.3	憑證機構之歸檔資料必須儲存在憑證機構以外的地方，並提供適當的保護，且其保護等級不可低於憑證機構的保護等級		

4.6.4	憑證機構必須於憑證實務作業基準中載明歸檔記錄之備份程序			
4.6.5	憑證機構必須於憑證實務作業基準中載明時戳記錄之要求			
4.6.6	憑證機構必須於憑證實務作業基準中載明歸檔資料彙整系統			
4.6.7	憑證機構必須於憑證實務作業基準中載明取得及驗證歸檔資料之程序			
4.7.1	憑證機構之私密金鑰更換最遲應於憑證到期前二個月，更換用來簽發憑證的金鑰對			
4.7.2	用戶之私密金鑰更換最遲最遲應於憑證到期前一個月，更換用來簽發憑證的金鑰對			
4.8.1	憑證機構應至少每年進行一次電腦資源、軟體及資料遭破壞之演習			
4.8.2	憑證機構應在憑證實務作業基準或相關的文件中載明憑證機構之簽章金鑰憑證被廢止時之復原程序，並應至少每年進行一次憑證機構之簽章金鑰憑證被廢止的演習			
4.8.3	憑證機構應在憑證實務作業基準中或相關的文件中載明憑證機構之簽章金鑰遭破解時之復原程序，並應至少每年進行一次憑證機構簽章金鑰遭破解的演習			
4.8.4	憑證機構應在憑證實務作業基準或相關文件中載明在自然或其他災害後，重新建立憑證機構安全設施的步驟，並應至少每年進行一次災後復原計畫之演習			
4.9	憑證機構必須於憑證實務作業基準中載明憑證機構之終止服務應遵守的事項，並依據電子簽章法相關規定進行憑證機構之終止服務			
5.1.1	憑證機構之機房的實體所在及結構，必須符合儲存高重要性及敏感性資訊的機房設施水準，結合門禁、保全、入侵偵測及監視錄影等實體安全機制			
5.1.2	憑證機構設備之實體控管	（一）建置全天候人工或電子式監控設備		
		（二）定期維護和檢視存取記錄檔		
		（三）必須至少兩人以上共同執行電腦系統和密碼模組的實體控管作業		

5.1.3	憑證機構之電力及空調設備必須具備足夠的備援設施，至少提供六小時以上之備用電力供儲存庫備援資料		
5.1.4	憑證機構之機房設置必須免於受到水災損害		
5.1.5	憑證機構之機房必須具備火災偵測及預警，能自動啟動滅火設備，並在必要時得以手動方式操作		
5.1.6	憑證機構必須保護系統相關的儲存媒體免於遭受天然意外的損害		
5.1.7	憑證機構必須於憑證實務作業基準中載明廢料處理方式		
5.1.8	憑證機構必須定期進行異地備援，必須至少每個星期執行一次完整的資料備份。異地備援地點必須與憑證機構機房距離三十公里以上，備援內容至少應包含資料與系統程式		
5.2.1	憑證機構必須於憑證實務作業基準中載明規定之信賴角色及其負責執行之相關任務		
5.2.2	憑證機構必須至少安排憑證政策規定的四種信賴角色，並允許一個人同時兼任一個以上的角色，但簽發員不可以再兼任管理員或稽核員		
5.2.3	憑證機構必須於憑證實務作業基準中載明每個任務所需之人數		
5.2.4	憑證機構必須在人員執行角色分派任務時，識別和鑑別人員的身份		
5.3.1	憑證機構必須於憑證實務作業基準中載明人員的身家背景、資格、經驗及安全需求之資格、遴選、監督和稽核相關辦法		
5.3.2	憑證機構必須於憑證實務作業基準中載明身家背景之查驗程序		
5.3.3	憑證機構必須於憑證實務作業基準中載明人員之教育訓練需求		
5.3.4	憑證機構必須於憑證實務作業基準中載明人員再教育訓練之需求及頻率		
5.3.5	憑證機構必須於憑證實務作業基準中載明工作調換之頻率及順序		
5.3.6	憑證機構必須於憑證實務作業基準中載明未授權行動之制裁		

5.3.7	憑證機構必須於憑證實務作業基準中載明聘僱人員之規定		
5.3.8	憑證機構必須於憑證實務作業基準中載明憑證機構應提供之文件資料		
6.1.1	憑證機構簽發憑證所使用的密碼模組，必須使用經由本會核可的密碼模組來產製金鑰。儲存在密碼模組內之私密金鑰，應防止其由密碼模組中外洩。憑證機構應採取適當措施確保用戶的公開金鑰在該憑證機構所轄之公開金鑰基礎建設領域內具有唯一性		
6.1.2	憑證機構必須於憑證實務作業基準中載明私密金鑰安全傳送給用戶的方式		
6.1.3	憑證機構必須於憑證實務作業基準中載明公開金鑰安全傳送給憑證機構的方式		
6.1.4	憑證機構必須於憑證實務作業基準中載明公開金鑰安全傳送給信賴憑證者的方式		
6.1.5	憑證機構之對稱金鑰長度至少必須具備 3-DES (3 Keys)或安全強度相當的其他種類金鑰；憑證機構之公開金鑰長度至少必須使用 1024 位元的 RSA 金鑰或安全強度相當的其他種類金鑰		
6.1.6	憑證機構之公開金鑰參數須依照相關的國際標準（對 RSA 而言，公鑰參數必須為 Null）		
6.1.7	對於 RSA 演算法而言，憑證機構必須於憑證實務作業基準中載明質數相關的測試方式；對於其他演算法而言，則依相關的國際標準，並應包括質數的測試		
6.1.8	用戶隨機亂數、金鑰對和對稱金鑰之產製得使用軟體或硬體方式		
6.1.9	憑證機構必須於憑證實務作業基準中載明金鑰之使用目的		
6.2.1	憑證機構及註冊中心之密碼模組安全等級應使用硬體實作方式且等級 2 以上，而用戶之密碼模組安全等級得以等級 1 以上之硬體或軟體實作方式		
6.2.2	憑證機構之簽章用私密金鑰必須符合憑證政策規定之多人控管程序		
6.2.3	憑證機構之簽章用私密金鑰不可被託管		
6.2.4.1	憑證機構之簽章用私密金鑰必須在多人控管程序下進行備份，並保存在備援場所		

6.2.4.2	用戶之簽章用私密金鑰必須由用戶控制進行備份或拷貝但不可被歸檔			
6.2.5	憑證機構之簽章用私密金鑰不可被歸檔			
6.2.6	憑證機構必須於憑證實務作業基準中載明私密金鑰輸入至密碼模組的方式			
6.2.7	憑證機構必須於憑證實務作業基準中載明私密金鑰之啟動方式。包括對啟動者做身分鑑別			
6.2.8	憑證機構必須於憑證實務作業基準中載明私密金鑰之停用方式。包括透過手動的登出程序或經過一段時間沒有運作後自動停止運作			
6.2.9	憑證機構必須於憑證實務作業基準中載明私密金鑰之銷毀方式			
6.3.1	憑證歸檔後得不必再進行公開金鑰之歸檔			
6.3.2.1	憑證機構之私密金鑰使用期限至多為 10 年，而公鑰憑證有效期限至多為 20 年			
6.3.2.2	用戶之私密金鑰使用期限至多為 5 年而公鑰憑證有效期限至多為 5 年			
6.4.1	用來解開憑證機構或憑證用戶私密金鑰的啟動資料，與其他相關存取控制機制，必須適當的保護。			
6.4.2	用來解開私密金鑰的啟動資料，必須使用結合密碼和存取控制的安全機制加以保護以防止揭露。啟動資料得以生物特徵或記憶方式保存			
6.5.1	特定電腦安全之技術需求	（一）具備身分鑑別之登入機制		
		（二）提供自行定義之存取控制		
		（三）提供安全稽核能力		
		（四）對各種憑證服務和信賴角色之存取控制		
		（五）具備信賴角色和相關身分的識別和鑑別		
		（六）以密碼技術確保每次通訊和資料庫安全		
		（七）具備信賴角色和相關身分識別的安全及可信賴的管道		
		（八）具備程序完整性及安全控管保護		

6.5.2	憑證機構得於憑證實務作業基準中載明電腦安全評等結果			
6.6.1	系統研發之控管措施	（一）必須依照良好的軟體工程方法開發軟體系統		
		（二）憑證機構之硬體和軟體必須是專用		
		（三）憑證機構之運作僅能使用安全政策授權的元件		
		（四）註冊中心之硬體和軟體必須在初次使用時檢查是否有惡意程式碼並定期掃瞄		
6.6.2	憑證機構之安全控管措施必須記錄和控管憑證機構相關系統的組態，並具備偵測未經許可修改憑證機構之軟體或組態的機制。在首次安裝憑證機構軟體時，必須確認是由供應商提供且未被修改過且為正確的版本			
6.7	憑證機構必須於憑證實務作業基準中載明其網路安全之控管措施			
6.8	憑證機構必須於憑證實務作業基準中載明密碼模組安全之控管措施			
7.1.1	憑證機構應簽發 X.509 v3 版本的憑證			
7.1.2	憑證機構應在其憑證格式剖繪中訂定憑證擴充欄位的使用、處理方式、欄位值設定以及自行擴充欄位等相關規定。憑證機構應遵循憑證政策中憑證及憑證廢止清冊格式剖繪的規定			
7.1.3	憑證機構應遵循憑證政策規定之簽章演算法及產製金鑰演算法之物件識別碼			
7.1.4	憑證的主體及簽發者兩欄位須使用 X.500 唯一識別名稱，且其屬性型態必須遵循 RFC 2459 的規定			
7.1.6	憑證機構所簽發的憑證必須引用憑證政策的物件識別碼且須與憑證的保證等級相符			
7.1.8	憑證機構所簽發的憑證不得包含政策限定元			
7.1.9	憑證機構所簽發的憑證之關鍵憑證政策的擴充欄位之語意處理，必須遵循憑證及憑證廢止清冊格式剖繪的規定			
7.2.1	憑證機構所簽發的憑證廢止清冊(CRL)必須符合 X.509 v2 的規定			

7.2.2	憑證廢止清冊(CRL)的格式剖繪中的每一個擴充欄位皆須遵循憑證及憑證廢止清冊格式剖繪的規定		
8.1	憑證機構應至少每年檢視其憑證實務作業基準一次		
8.1.2.1	憑證機構必須於憑證實務作業基準載明應通知之變更項目		
8.1.2.2	憑證機構必須於憑證實務作業基準載明變更項目通知機制		
8.1.2.3	憑證機構必須於憑證實務作業基準載明意見之回覆期限		
8.1.2.4	憑證機構必須於憑證實務作業基準載明處理意見機制		
8.1.2.5	憑證機構必須於憑證實務作業基準載明最後公告期限		
8.2	憑證機構必須於憑證實務作業基準載明公告及通知之規定		
8.3	憑證機構必須於憑證實務作業基準載明憑證實務作業基準變更程序		