政府伺服器數位憑證管理中心

憑證實務作業基準

(Government TLS Certification Authority Certification Practice Statement)

第 1.0.6 版

主辦機關：數位發展部

執行機構：中華電信股份有限公司

中華民國 114 年 9 月 23 日

政府伺服器數位憑證管理中心憑證實務作業基準

版本修訂歷程

版本	生效日期	修訂內容說明
1.0	108/07/15	初版發行
1.0.1	109/7/13	1. 第 1.0 版發行日期誤植為 2019/05/27，修訂第 1.0.1 版版本修訂歷程中 1.0 版之生效日期為 2019/07/15。 2. 修訂 1.2 節，依此次改版，調整版本資訊、公告日期及發佈網址。 3. 修訂 1.5.2 節，載明政府伺服器數位憑證管理中心(GTLSCA)聯絡用之電子郵件信箱、電話及郵遞地址。 4. 修訂 1.5.4 節，新增政府伺服器數位憑證管理中心憑證實務作業基準(GTLSCA CPS)應配合修訂之依據。 5. 修訂 2.1 節儲存庫連結位址。 6. 修訂 4.9.10 節，調整線上憑證狀態協定(OCSP)查詢服務更新憑證狀態資訊之頻率與回應訊息之效期。 7. 修訂 6.3.2.2 節，新增用戶憑證(SSL/TLS 憑證)自 109 年 9 月 1 日起效期不得超握 398 天之說明。 8. 修訂附錄 3，更新 GTLSCA CPS 檢視之 BR 版本資訊。 9. 檢視 Baseline Requirements (BR) 1.6.6 至 1.7.0 版與 Mozilla Root Store Policy 2.7 版，並進行如下修訂： ■ 1.3.1 節：依 Mozilla Root Store Policy 規定，新增 GTLSCA CPS 適用之憑證機構憑證相關資訊。 ■ 3.2.2.2 節：依 BR 規定，修訂透過特定網頁內容變更之網域驗證方式；此外，修訂透過政府中英文網域名稱註冊系統驗證之網域驗證方式之遺漏文字。 ■ 4.9.10 節：依 BR 規定，修改 OCSP 查詢服務之說明。 ■ 4.9.12 節：依 Mozilla Root Store Policy 規定，修正金鑰被破解時之其他特殊規定之內容。 ■ 7.1.4.2 節：依 BR 規定，修改用戶憑證之主體別名擴充欄位之相關說明。 10. 修訂 GTLSCA CPS 之數字用語，依內文所述調整數字用語為阿拉伯數字或中文數字，此修訂不影響原意。異

		動章節包含：3.1.2 節、5.1.1 節、5.1.6 節、5.3.4 節、5.4.8 節、5.5.3 節、7.1.2.2 節、7.1.4.2 節以及附錄 1「名詞解釋」之「憑證效期」、「傳輸層安全」及「可信賴電腦系統安全評估準則」。 11. 修訂 GTLSCA CPS 之誤植文字、贅字、英譯用詞與遺漏之內容，並調整文句編排，此修訂不影響原意，異動章節包含：1.2 節、1.4.4 節、1.5.4 節、4.9.3.2 節、6.1.6 節、7.1.2.1 節、7.1.2.2 節、7.1.3 節、7.3 節、7.3.2 節以及附錄 1「名詞解釋」之「憑證透明度」、「私密金鑰」及「公開金鑰」。
1.0.2	110/9/30	1. 修訂 1.2 節，依此次改版，調整版本資訊、公告日期及發佈網址。 2. 修訂 2.2 節，新增 GTLSCA CPS 為 GTLSCA 公布憑證資訊之方式。 3. 修訂 4.2.2 節，刪除 GTLSCA 拒絕簽發憑證之情境中有關憑證申請資料內含通用頂級域名之相關規定。 4. 修訂 6.2.6 節，修改為私密金鑰與密碼模組間傳輸之情境，並新增其傳輸應採行之保護方式之說明。 5. 修訂 6.6.1 節，修正系統研發控管措施內容。 6. 修訂 6.7 節，新增 GTLSCA 之網路安全控管需遵照之相關標準。 7. 因應 ACME 機制導入，修訂相關章節： ■ 3.2.2.1 節：新增 ACME 機制之組織身分鑑別方式。 ■ 3.2.2.2 節：依 BR 3.2.2.4.19 節規定新增 ACME 機制之網域驗證方式。 ■ 4.2 節：新增 ACME 機制之憑證申請程序。 ■ 4.2.1 節：新增 ACME 機制之識別及鑑別作業。 ■ 4.3.1 節：新增 ACME 機制之憑證簽發作業。 ■ 4.4 節：新增 ACME 機制之憑證接受作業。 8. 檢視 BR 1.7.1 至 1.7.6 版與 Mozilla Root Store Policy 2.7.1 版，並進行如下修訂： ■ 2.3 節：依 BR 規定，新增 GTLSCA CPS 更新頻率之說明。 ■ 4.9.5 節：依 BR 規定，新增須於接受憑證廢止申請後 1 日內完成憑證廢止之事由。

		■ 4.9.12 節：依 Mozilla Root Store Policy 規定，修正金鑰被破解時之其他特殊規定之內容。 ■ 6.1.1.2 節：依 BR 規定，新增 GTLSCA 應拒絕用戶憑證請求之情境之相關說明。 ■ 6.1.5 節：依 BR 規定，新增 RSA 金鑰長度(以位元為單位)須被 8 整除之說明。 ■ 7.1.4.1 節：依 BR 規定，調整章節名稱，並修改 GTLSCA 本身憑證與用戶憑證間之憑證串鏈驗證相關說明。 ■ 7.2.2 節：新增憑證廢止清冊(CRL)之 CRL 擴充欄位與憑證廢止清冊條目(CRL Entry)擴充欄位內容之說明，並依 BR 規定，補充說明適用於本管理中心所簽發之 CRL 之 CRL Entry 擴充欄位「reasonCode」標註廢止憑證之原因代碼及其適用情境。 ■ 7.3 節：依 BR 規定，修改 OCSP 回應訊息基本欄位「憑證狀態碼」之說明，新增憑證狀態碼為 1 時尚須註記之廢止資訊。 ■ 9.12 節：依 BR 規定，新增 GTLSCA CPS 於每年定期檢視 BR 後之版本編號異動方式。 ■ 修訂附錄 3，更新 GTLSCA CPS 檢視之 BR 版本資訊。 9. 修訂 GTLSCA CPS 之誤植文字、贅字、連接詞、英譯用詞與遺漏之內容，並調整文句編排，此修訂不影響原意，異動章節包含：摘要、第 1 章、1.4.3 節、2.1 節、2.2 節、3.2.2.2 節、3.2.5 節、4.1.2 節、4.2 節、4.2.1 節、4.3.1 節、4.4 節、4.7 節、4.9.5 節、6.1.6 節、6.1.7 節、6.2.2 節、6.6.1 節、6.6.2 節、7.1.2.1 節、7.1.2.2 節、7.1.4.2 節、7.3 節、7.3.2 節。
1.0.3	112/3/5	1. 配合 GPKI 憑證相關業務由國家發展委員會移轉至數位發展部，將文件中「國家發展委員會」更改為「數位發展部」，「國發會」更改為「數位部」 2. 調整執行機構「中華電信股份有限公司數據通信分公司」更改為「中華電信股份有限公司」

		3. 修訂 1.2 節，依此次改版，調整版本資訊、公告日期及發佈網址。 4. 修訂 1.5.2 節，憑證管理中心之聯絡資料。 5. 檢視 BR 1.7.7 至 1.8.4 版，並進行如下修訂： ■ 3.1.5 節：用戶憑證主體名稱格式停止使用 organizationalUnitName(縮寫為 OU)。 ■ 5.4.1 節：相關紀錄保存之負責單位，應涵蓋委派第三方，並新增應紀錄之事件類型。 ■ 5.4.3 節：稽核紀錄保留期限調整為至少 2 年。 ■ 5.5.1 節：相關紀錄歸檔之負責單位，應涵蓋委派第三方。 ■ 7.1.4.2 節：新增完整網域名稱之格式須由 P-Labels 與 NR-LDH Label 所組成，並禁用 OU 欄位。 ■ 修訂附錄 3，更新 GTLSCA CPS 檢視之 BR 版本資訊。
1.0.4	113/3/6	1. 修訂 1.2 節，依此次改版，調整版本資訊、公告日期及發佈網址。 2. 修訂 4.4 節，調整憑證預設為接受，如有異議由申請者自行提出廢止請求。 3. 修訂 6.1.1.1 節，對 BR 提具的合格稽核員進行說明，應包含管理委員會之委員或合格稽核業者。 4. 修訂 7.1.2 節，將”本基礎建設”文字修正為 ePKI。 5. 修訂附錄 1、E，將”本基礎建設”文字修正為 ePKI。 6. 檢視 BR 1.8.5 至 2.0.2 版，並進行如下修訂： ■ 附錄 1-C：交互憑證定義。 ■ 附錄 1-E：終端個體、ePKI RootCA 定義 7. 修訂附錄 3，更新 GTLSCA CPS 檢視之 BR 版本資訊。
1.0.5	114/3/5	1. 修訂 1.2 節，依此次改版，調整版本資訊、公告日期及發佈網址。 2. 修訂 2.2 節，提供展示網址位置。 3. 參考 BR 調整內容，修訂 4.10.2 節、7.1.2.2 節、7.1.4.2 節、7.2.2 節及 7.3.2 節。 4. 修訂附錄 1，新增 HiPKI RootCA 名詞解釋。 5. 修訂附錄 3，新增一年來 BR 更新版本，自 2.0.3-2.1.3 版。

		6. 修訂誤植文字、贅字、連接詞、英譯用詞與遺漏之內容，並調整文句編排，此修訂不影響原意，異動章節包含：第 1 章、1.1 節、1.4.1 節、2.1 節、2.3 節、3.2.6 節、4.9.1 節、4.9.12 節、4.9.13 節、5.4.1 節、6.1.4 節、6.1.5 節、6.1.6 節、6.1.7 節、6.3.2.2 節、7.1 節、7.2 節、7.1.2.1 節、7.1.4 節、7.1.9 節、7.2.1 節、7.3 節、7.3.3 節、9.8 節、9.12 節、9.12.3 節、9.16.3 節。
1.0.6	114/9/23	1. 修訂 1.2 節，依此次改版，調整版本資訊、公告日期及發佈網址。 2. 參考 BR 調整內容，修訂 1.3.1、1.4.2、2.1、2.2、3.2.2.2、3.2.8、4.9.1 及 5.7.1 節。 3. 修訂附錄 3，新增本次檢視週期 BR 更新版本，自 2.1.4-2.1.7 版。

目　　錄

摘要

政府伺服器數位憑證管理中心憑證實務作業基準(以下簡稱本作業基準)之重要事項說明如下：

1. 簽發之憑證：

   (1) 種類：政府機關(構)及單位之組織驗證型 TLS 類伺服器應用軟體憑證。

   (2) 保證等級：政府伺服器數位憑證管理中心(以下簡稱本管理中心)依中華電信公開金鑰基礎建設憑證政策(以下簡稱憑證政策)保證等級第 3 級運作，簽發憑證政策所定義保證等級第 3 級之憑證。

   (3) 適用範圍：本管理中心所簽發之 TLS 憑證主要做為身分鑑別之安全機制，供信賴憑證者識別該用戶之網際網路伺服器其網域名稱及管理單位，用戶與信賴憑證者須謹慎使用本管理中心所簽發之憑證，並排除本作業基準所限制與禁止之憑證適用範圍。

2. 法律責任重要事項：

   (1) 用戶或信賴憑證者如未依本作業基準規定之適用範圍使用憑證所引發之後果，本管理中心不負任何法律責任。

   (2) 用戶或信賴憑證者如因使用憑證而發生損害賠償事件時，本管理中心之損害賠償責任，以相關法令規定所訂之責任範圍為限。

   (3) 如因不可抗拒與其他非可歸責於本管理中心之事由所衍生之損害事件，本管理中心不負任何法律責任。

(4) 註冊中心因執行註冊工作所引發之法律責任，除法令另有規定外，由註冊中心負責。

(5) 用戶提供不正確資料而導致信賴憑證者遭受損害時，相關法律責任應由用戶自行負責。

(6) 用戶之憑證如須廢止或重發，應立即通知本管理中心，並依照本作業基準相關規定辦理，用戶仍應承擔異動前所有使用該憑證之法律責任。

3. 其他重要事項：

(1) 本管理中心如有系統維護、轉換及擴充等需求時，得暫停部分憑證服務，並公告於儲存庫與通知用戶，用戶或信賴憑證者不得以此作為要求本管理中心損害賠償之理由。

(2) 註冊中心如因審驗錯誤，導致用戶或信賴憑證者遭受損害時，註冊中心之損害賠償責任，以相關法令規定所訂之責任範圍為限。

(3) 用戶申請憑證時，本管理中心預先提供該憑證之內容讓用戶審視，用戶審視憑證內容無誤並接受後，本管理中心將以此做為憑證接受之依據並簽發憑證。用戶收到本管理中心所簽發之憑證後，應依本作業基準相關規定使用憑證。

(4) 用戶與信賴憑證者應慎選安全之電腦環境與可信賴之應用系統，如因電腦環境或應用系統本身導致使用者權益受損時，應自行承擔責任。

(5) 本管理中心如因故無法正常運作時，用戶與信賴憑證者

應儘速尋求其他途徑，完成與他人應為之法律行為，不得以本管理中心無法正常運作，作為抗辯他人之事由。

(6) 信賴憑證者接受使用本管理中心簽發之憑證時，即表示已了解及同意本管理中心法律責任之條款，並依本作業基準相關規定使用憑證。

(7) 本管理中心由數位發展部委託公正第三方辦理外部稽核作業。

(8) 除另有規定外，本作業基準修訂生效後，如修訂之內容與原本作業基準有所牴觸時，以修訂之內容為準；如以附加文件方式修訂，而該附加文件內容與原作業基準牴觸時，以該附加文件內容為準。

1 簡介

政府伺服器數位憑證管理中心憑證實務作業基準(Government TLS Certification Authority Certification Practice Statement，以下簡稱本作業基準)係依據中華電信公開金鑰基礎建設憑證政策(Certificate Policy for the Chunghwa Telecom ecommerce Public Key Infrastructure，以下簡稱憑證政策)、ITU-T X.509、網際網路工程任務小組(Internet Engineering Task Force, IETF)之徵求修正意見書(如 RFC 3647 與 RFC 5280)及憑證機構與瀏覽器論壇(CA/Browser Forum)發行之 Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates 所訂定。

1.1 總覽

政府伺服器數位憑證管理中心(Government TLS Certification Authority, GTLSCA，以下簡稱本管理中心)係中華電信公開金鑰基礎建設(Chunghwa Telecom ecommerce Public Key Infrastructure, ePKI，以下簡稱本基礎建設)之下屬憑證機構(Subordinate Certification Authority)，由中華電信憑證總管理中心(ePKI Root Certification Authority, eCA，以下簡稱總管理中心)簽發憑證予本管理中心。

本管理中心負責簽發與管理政府機關(構)及單位之組織驗證型(Organization Validation, OV) TLS 類伺服器應用軟體憑證(以下簡稱 TLS 憑證)。

本作業基準係說明本管理中心之憑證簽發與管理作業符合憑證政策所訂定之保證等級第 3 級之規定。本作業基準所載明之實務作業規範僅適用於與本管理中心相關之個體，如本管理中心、註冊中心(Registration Authority, RA)、用戶(Subscriber)、信賴憑證者(Relying

Party)及儲存庫(Repository)等。

本管理中心同意遵照憑證機構與瀏覽器論壇(網址為「http://www.cabforum.org」)所發行之 Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates 正式版本，同時針對該正式版本所列各項資訊之生效日期，本管理中心皆配合辦理(參照附錄 3)。本作業基準如於 TLS 憑證簽發管理上與該論壇規範有牴觸情形時，優先遵照憑證機構與瀏覽器論壇所頒布之條款。

數位發展部(以下簡稱數位部)為本管理中心之主管機關，負責本作業基準之訂定與修訂，本作業基準須經總管理中心核可後施行。本作業基準未授權本管理中心以外之憑證機構使用，其他憑證機構如引用本作業基準而引發之任何問題，由該憑證機構自行負責。

1.2 文件名稱及識別

1. 文件名稱：政府伺服器數位憑證管理中心憑證實務作業基準
2. 版本：第 1.0.6 版
3. 核定日期：114 年 9 月 23 日
4. 發布網址：https://gtlsca.nat.gov.tw/download/GTLSCA_CPS_v1.0.6.pdf。
5. 憑證政策物件識別碼(Certificate Policy Object Identifier, CP OID)：
   - 憑證政策定義之保證等級第 3 級憑證政策物件識別碼：「1.3.6.1.4.1.23459.100.0.3」

- 憑證機構與瀏覽器論壇定義之組織驗證型 TLS 憑證政策物件識別碼：「2.23.140.1.2.2」

1.3 主要成員

本管理中心之相關成員包括：

1. 本管理中心。
2. 註冊中心。
3. 用戶。
4. 信賴憑證者。
5. 其他相關成員，包括數位部授權管理、建置及系統維運之委外單位。

1.3.1 本管理中心

負責政府機關(構)及單位之 TLS 憑證簽發與管理作業。本作業基準適用之憑證機構憑證如下：

1. 第 1 代政府伺服器數位憑證管理中心(Government TLS Certification Authority - G1)
   - 憑證序號：00 99 6d 5f e9 ad e1 6c dc 8e cd bf ed b1 4a 32 95
   - 憑證拇指紋(SHA-1)：b2 d1 51 a7 68 d3 0c 3b 99 d8 6b 8b 25 81 56 08 c2 8a b2 cb
   - 憑證拇指紋(SHA-256)：9d 1c da 1b 9e f3 95 af ce 7d e0 fe 74 de 6d 9f f5 e0 d2 a4 37 89 11 6c 00 c6 ba 5b f4 4b 98 23

- 憑證效期：2019 年 7 月 19 日至 2031 年 8 月 19 日
- 金鑰種類/金鑰長度：RSA 4096 with SHA-256

本管理中心已於 2025 年 3 月 10 日起停發 TLS 憑證。

1.3.2 註冊中心

負責蒐集、驗證用戶身分及憑證相關資訊之註冊工作。註冊中心由註冊窗口組成，並有憑證註冊審驗人員，負責受理憑證之註冊申請及廢止申請等作業。本管理中心設立及授權之註冊審驗窗口皆須接受外部稽核。

註冊中心設置註冊中心伺服器，負責驗證憑證註冊審驗人員之身分與管理註冊窗口。註冊中心伺服器由註冊中心管理員負責管理，註冊中心管理員於註冊中心伺服器上設定憑證註冊審驗人員之帳號與權限，並製發憑證註冊審驗人員 IC 卡。註冊中心伺服器上裝設註冊中心之私密金鑰，註冊中心伺服器與本管理中心伺服器間之通訊，由註冊中心之私密金鑰簽章加以保護。

1.3.3 用戶

指記載於本管理中心所簽發憑證內憑證主體名稱(Subject Name)之個體，以本管理中心而言，用戶係指申請並經核發 TLS 憑證之政府機關(構)及單位。

1.3.4 信賴憑證者

指相信憑證主體名稱與公開金鑰連結關係之個體。

信賴憑證者使用本管理中心所簽發之憑證前，須以本管理中心本身之憑證與憑證狀態資訊，檢驗所使用憑證之有效性；確認憑證有效

性後，方可使用憑證識別用戶及其網路伺服器名稱，並與憑證主體間建立安全之通訊管道。

1.3.5 其他相關成員

數位部依照政府採購法委託合格廠商，負責本管理中心之建置與系統維運作業。

1.4 憑證用途

1.4.1 憑證之適用範圍

本管理中心簽發之 TLS 憑證主要應用於傳輸層安全(Transport Layer Security, TLS)通訊協定，做為身分鑑別之安全機制，供信賴憑證者識別該用戶之網際網路伺服器其網域名稱及管理單位。

1.4.2 憑證之禁止使用範圍

1. TLS 流量中間人攔截(Man-in-the-Middle TLS Traffic Interception)。
2. 會造成人身傷亡與精神侵害之用途，或對社會秩序與公共利益有重大危害之應用或業務。
3. 其他相關法令或各目的事業主管機關明訂禁止或排除之應用或業務。

用戶應遵守所有適用瀏覽器根憑證政策(Browser Root Policies)之要求，包括本作業基準規定之 24 小時以及 5 天內的廢止期限

1.5 聯絡方式

1.5.1 憑證實務作業基準之制訂及管理機構

本管理中心負責制訂及管理本作業基準。

1.5.2 聯絡資料

本管理中心聯絡方式如下：

- 電子郵件信箱：egov@service.gov.tw
- 憑證問題回報信箱：gca@gca.nat.gov.tw
- 聯絡電話：0800-770-707
- 郵遞地址：100057 臺北市中正區延平南路 143 號 數位發展部

1.5.3 憑證實務作業基準之審定

本作業基準由數位部審查後，再送交總管理中心核定，始得對外提供簽發憑證服務。

1.5.4 憑證實務作業基準變更程序

憑證實務作業基準之變更依 1.5.3 節「憑證實務作業基準之審定」規定辦理；憑證政策或總管理中心之憑證實務作業基準如有修訂並公告後，本作業基準應配合修訂。

1.6 名詞定義及縮寫

詳參附錄 1「名詞解釋」與附錄 2「英文名詞縮寫」。

2 資訊公布及儲存庫責任

2.1 儲存庫

儲存庫負責公告及儲存由本管理中心所簽發之憑證、憑證廢止清冊(Certificate Revocation List, CRL)及本作業基準，提供用戶及信賴憑證者查詢服務。網址為：

https://gcp.nat.gov.tw/views/AnnDownload/download.html。

如因故無法正常運作，將於 2 個工作天內恢復正常運作。

2.2 憑證資訊公布

本管理中心會將以下資訊公布於儲存庫：

1. 本作業基準。
2. 本管理中心所簽發之憑證。
3. 憑證廢止清冊。
4. 隱私權保護政策。
5. 最近 1 次之外部稽核結果(如 8.6 節「稽核結果公開之範圍」所述)。
6. 提供展示 TLS 憑證樣態，狀態為有效、廢止、過期等 3 個連結網址，供用戶確認格式，及確認憑證管理中心具備定期自動換發功能。

2.3 公布頻率或時間

1. 本管理中心每年檢視與更新本作業基準，本作業基準經總管理中心審查核可後擇期公告於儲存庫。

2. 本管理中心每日至少簽發並公告 1 次憑證廢止清冊。

2.4 存取控制

1. 本管理中心建置資安防護機制，外界無法直接連線至內部主機。

2. 用戶與憑證信賴者透過儲存庫查詢，儲存庫主機透過安全控管連線至本管理中心主機之資料庫。

3. 本管理中心只允許經授權之人員管理儲存庫主機。

3 識別及鑑別程序

3.1 命名

3.1.1 命名種類

1. 憑證主體名稱採用 ITU-T X.500 唯一識別名稱。

2. 用戶憑證主體別名(Subject Alternative Name)擴充欄位須為非關鍵性擴充欄位。

3.1.2 命名須有意義

1. 憑證主體名稱之命名方式應符合政府相關法令規定。

2. 憑證主體名稱與憑證主體別名須符合憑證機構與瀏覽器論壇所發行之 Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates 之規範，且應註記完整網域名稱(Fully Qualified Domain Name)。

3. 本管理中心不接受未合法註冊之網域或 IP Address 申請憑證。

4. 憑證主體名稱應包含 3.2.2 節「組織身分之鑑別程序」所驗證之組織身分資訊於其組織名稱(Organization Name)欄位屬性。

5. 多網域憑證可註記多個完整網域名稱於一張憑證之憑證主體別名欄位，用戶須具備所有網域名稱之控制權。

6. 萬用網域憑證使用萬用字元(*)，將其註記於憑證主體名稱之通用名稱欄位屬性的完整網域名稱之最左邊，以適用於該次網域內的所有網站。

3.1.3 用戶匿名或假名

本管理中心不簽發匿名憑證或假名憑證。

3.1.4 命名形式之解釋規則

依 ITU-T X.520 名稱屬性定義。

3.1.5 命名獨特性

1. 憑證機構憑證

   憑證機構憑證之 X.500 唯一識別名稱為：

   C=TW，O=行政院，CN=政府伺服器數位憑證管理中心- Gn

   其中，n=1,2…

2. 用戶憑證

   用戶憑證採用 X.520 標準所定義之命名屬性，憑證主體名稱格式如下：

   - countryName(縮寫為 C)
   - stateOrProvinceName(縮寫為 S)
   - localityName(縮寫為 L)
   - organizationName(縮寫為 O)

- commonName(縮寫為 CN)
- serialNumber

3.1.6 商標之辨識、鑑別及角色

不適用。

3.1.7 命名爭議解決程序

1. 用戶名稱所有權有爭議時，依相關法令規定辦理。
2. 網域名稱所有權有爭議時，依網域主管機關處理程序辦理。

3.2 初始註冊

3.2.1 證明擁有私密金鑰之方式

1. 用戶自行產製金鑰對，以該金鑰對產製 PKCS#10 憑證申請檔並加以簽章後交予註冊中心。
2. 註冊中心使用該用戶之公開金鑰驗證該申請檔之簽章，以證明用戶擁有相對應之私密金鑰。

3.2.2 組織身分之鑑別程序

3.2.2.1 組織身分鑑別

1. 一般申請

   用戶填寫憑證申請書後以公文提出申請，由本管理中心驗證公文之正確性，以證明該機關(構)及單位確實存在且申請獲得授權。

2. 線上申請

以有效之政府機關(構)及單位憑證 IC 卡線上申請，由註冊中心檢驗其憑證 IC 卡之數位簽章，以鑑別用戶之身分，並確認該機關(構)及單位確實存在。

3. 憑證自動換發機制

本管理中心依據 RFC 8555 規範之自動化憑證管理環境(Automatic Certificate Management Environment，ACME)，提供用戶進行憑證自動換發申請，初次申請時以有效之政府機關(構)及單位憑證 IC 卡，透過 ACME 專屬之註冊服務完成身分鑑別及主機識別金鑰之註冊，後續執行憑證自動換發時，將以此識別金鑰作為身分鑑別之依據。

3.2.2.2 網域名稱擁有者鑑別

1. 用戶申請憑證時，本管理中心依照憑證機構與瀏覽器論壇所發行之 Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates 正式版本中 3.2.2.4 節「Validation of Domain Authorization or Control」之規定，選用所建議之方式驗證用戶申請之網域確實屬該申請者所註冊擁有且對該網域具有控制權。

2. 網域名稱與組織之所有權均經憑證註冊審驗人員審查，屬於國際網域名稱之 TLS 憑證，其解碼的完整主機名稱若為具風險之名稱，將對此 TLS 憑證請求進行額外之比對，以防止國際網域名稱同態欺騙攻擊。

3. 可使用之網域驗證方式說明如下：

(1) 透過政府中英文網域名稱註冊系統驗證

依據憑證機構與瀏覽器論壇發行之 Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates 中 3.2.2.4.12 節「Validating Applicant as a Domain Contact」之規定辦理。

A. 本管理中心之主管機關同時也管理政府網域之配發，用戶申請憑證時，透過政府中英文網域名稱註冊系統，驗證該網域確實屬該申請者所註冊擁有且用戶具有控制權，並依 3.2.2 節「組織身分之鑑別程序」辦理身分鑑別。

B. 以教育部管理之網域(.edu)申請憑證時，由數位部授權教育部之審驗窗口驗證該網域確實屬該申請者所註冊擁有且用戶具有控制權，本管理中心依 3.2.2 節「組織身分之鑑別程序」辦理身分鑑別。

C. 本管理中心可針對通過驗證之完整網域及與該網域標籤結尾相同之網域簽發 TLS 憑證，此方式也適用於萬用網域之驗證。

D. 自 2025 年 1 月 15 日起生效：在頒發用戶憑證時，本管理中心不得依賴使用 HTTPS 網站取得的網域聯絡人資訊，無論先前取得的資訊是否在允許的重複使用期限內。取得所要求網域名稱的網域聯絡人資訊時，本管理中心如果使用 WHOIS 協定 (RFC 3912)，則必須查詢 IANA 的 WHOIS 伺服器並依照指引轉至對應的 WHOIS 伺服器。如果使用註冊資料存取協定 (RFC 7482)，則必須利用

IANA 的引導檔案來識別和查詢 網域的正確 RDAP 伺服器。相關資訊的取得不得依賴快取的 1) WHOIS 伺服器資訊（此資訊已超過 48 小時）或 2) 來自 IANA 的 RDAP 引導資料（此資訊已超過 48 小時），以確保其依賴的是最新且準確的資訊。

(2) 透過網域聯絡人電子郵件驗證

依據憑證機構與瀏覽器論壇發行 Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates 中 3.2.2.4.2 節「Email, Fax, SMS, or Postal Mail to Domain Contact」之規定辦理。

A. 本管理中心寄發內含隨機值之電子郵件傳送給申請網域註冊之聯絡人，收到該聯絡人之回應後，確認此申請者擁有該完整網域名稱之控制權。

B. 上述隨機值應為唯一且有效期間為 30 天

C. 本管理中心可視情況重新發送電子郵件及更新隨機值，但該電子郵件之其他內容與收件人須保持不變。

D. 本管理中心可針對通過驗證之完整網域及與該網域標籤結尾相同之網域簽發 TLS 憑證，此方式也適用於萬用網域之驗證。

E. 自 2025 年 1 月 15 日起生效：在頒發用戶憑證時，本管理中心不得依賴使用 HTTPS 網站取得的網域聯絡人資訊，無論先前取得的資訊是否在允許的重複使用期限內。取得所要求網域名稱的網域聯絡人資訊時，本管理中心如果使用 WHOIS 協定

(RFC 3912)，則必須查詢 IANA 的 WHOIS 伺服器並依照指引轉至對應的 WHOIS 伺服器。如果使用註冊資料存取協定 (RFC 7482)，則必須利用 IANA 的引導檔案來識別和查詢 網域的正確 RDAP 伺服器。相關資訊的取得不得依賴快取的 1) WHOIS 伺服器資訊（此資訊已超過 48 小時）或 2) 來自 IANA 的 RDAP 引導資料(此資訊已超過 48 小時)，以確保其依賴的是最新且準確的資訊。

F. 自 2025 年 7 月 15 日起生效：本管理中心應停用此方法，之前已使用此方法進行驗證或根據此方法收集的驗證資訊均不得用於簽發用戶憑證。

(3) 透過特定網頁內容變更

依據憑證機構與瀏覽器論壇發行 Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates 中 3.2.2.4.18 節「Agreed-Upon Change to Website v2」之規定辦理。

A. 本管理中心提供內含隨機值之特定網頁，申請者須將網頁內容置於指定目錄("/.well-known/pki-validation")，憑證管理中心透過 HTTP/HTTPS 並經授權之連接埠驗證網頁內容，藉此確認申請者具備對該完整網域之控制權。

B. 上述隨機值有效期不得超過 30 天。

C. 上述隨機值不得出現在憑證管理中心之網頁驗證請求中。

D. 本管理中心須收到來自上述網頁回傳 HTTP 代碼表

成功之回應(狀態碼為 2xx)。

E. 本管理中心不提供轉址網域之審驗服務。

F. 本管理中心不允許採用此方法進行萬用網域憑證之核發。

G. 同時，本管理中心將依照 3.2.8 節「多重視角簽發驗證機制」規定實施多重視角簽發驗證機制(Multi-Perspective Issuance Corroboration, MPIC)。為了計算佐證數量，網路視角必須觀察與主網路視角相同之挑戰訊息(即隨機值或請求符記)。

(4) 憑證自動換發機制之網域驗證方式

依據憑證機構與瀏覽器論壇發行 Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates 中 3.2.2.4.19 節「Agreed-Upon Change to Website - ACME」之規定辦理。

A. 本管理中心依據 RFC 8555 規範第 8.3 節定義之 ACME HTTP 挑戰機制，確認申請者對該完整網域具備控制權。

B. 此機制中用於驗證用之隨機值有效期不得超過 30 天。

C. 本管理中心須收到上述隨機值之用戶端伺服器回傳 HTTP 代碼表成功之回應(狀態碼為 2xx)。

D. 本管理中心不提供轉址網域之審驗服務。

E. 本管理中心不允許採用此方法進行萬用網域憑證之核發。

F. 同時，本管理中心將依照 3.2.8 節「多重視角簽發驗證機制」規定實施多重視角簽發驗證機制。為了計算佐證數量，網路視角必須觀察與主網路視角相同之挑戰訊息(即隨機值或請求符記)。

3.2.3 個人身分之鑑別程序

不適用。

3.2.4 未經驗證之用戶資訊

未經驗證之用戶資訊不得寫入憑證。

3.2.5 權責之確認

1. 用戶申請憑證時，應依 3.2.2.1 節「組織身分鑑別」規定擇一方式辦理。

2. 本管理中心依 3.2.2.2 節「網域名稱擁有者鑑別」規定鑑別其具備網域名稱之擁有權與控制權。

3.2.6 交互運作標準

不適用。

3.2.7 資料正確性

本管理中心應評估資料正確性，評估過程應考慮以下事項：

1. 所提供資料的存在時間。

2. 資料來源的更新頻率。

3. 資料提供者和資料收集的目的。

4. 資料可用性。

5. 資料可公開取得之程度。

6. 偽造或變更資料的相對困難性。

3.2.8 多重視角簽發驗證機制

自 2025 年 3 月 15 日起，本管理中心應採用憑證機構與瀏覽器論壇所發行之 Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates 中 3.2.2.9 節「Multi-Perspective Issuance Corroboration」之規定實施網域授權或控管的驗證及授權憑證機構簽發憑證(Certification Authority Authorization, CAA)紀錄檢查，多重視角簽發驗證機制可在憑證簽發之前從多個遠端網路視角輔助主網路視角做出驗證成功與否之決定(即網域驗證通過/失敗、CAA 許可/禁止)。

法定人數要求表(Quorum Requirements Table)

# of Distinct Remote Network Perspectives Used	**# of Allowed non-Corroborations**
2-5	1
6+	2

分階段實施表：

- **2025 年 3 月 15 日起**，本管理中心必須使用至少 2 個遠端網路視角進行多重視角簽發驗證。如果無法證實主網路視角所做決定的遠端網路視角(「未證實」)的數量大於上述之法定人數要求表中所允許的數量，本管理中心可以繼續簽發憑證；
- **2025 年 9 月 15 日起**，本管理中心必須使用至少 2 個遠端網路視角進行多重視角簽發驗證。本管理中心必須確保符合上述之法定

人數要求表中定義的要求，如果不符合要求，則本管理中心不得繼續簽發憑證；

- **2026 年 3 月 15 日起**，本管理中心必須使用至少 3 個遠端網路視角進行多重視角簽發驗證。本管理中心必須確保符合上述之法定人數要求表中定義的要求，並且協助主網路視角進行驗證的遠端網路視角位於至少 2 個不同的區域網際網路註冊管理機構(Regional Internet Registries)的服務區域內。如果不符合要求，則本管理中心不得繼續簽發憑證；
- **2026 年 6 月 15 日起**，本管理中心必須使用至少 4 個遠端網路視角進行多重視角簽發驗證。本管理中心必須確保符合上述之法定人數要求表中定義的要求，並且協助主網路視角進行驗證的遠端網路視角位於至少 2 個不同的區域網際網路註冊管理機構的服務區域內。如果不符合要求，則本管理中心不得繼續簽發憑證；
- **2026 年 12 月 15 日起**，本管理中心必須使用至少 5 個遠端網路視角進行多重視角簽發驗證。本管理中心必須確保符合上述之法定人數要求表中定義的要求，並且協助主網路視角進行驗證的遠端網路視角位於至少 2 個不同的區域網際網路註冊管理機構的服務區域內。如果不符合要求，則本管理中心不得繼續簽發憑證。

3.3 金鑰更換請求之識別及鑑別

3.3.1 例行性金鑰更換識別及鑑別

用戶私密金鑰使用期限屆滿更換金鑰對並重新申請憑證時，本管理中心應依 3.2 節「初始註冊」規定辦理。

3.3.2 憑證廢止之金鑰更換識別及鑑別

用戶因憑證廢止而申請新憑證時，本管理中心應依 3.2 節「初始註冊」規定辦理。

3.4 憑證廢止申請之識別及鑑別

憑證廢止申請之鑑別依 3.2 節「初始註冊」規定辦理。

4 憑證生命週期營運規範

4.1 憑證申請

4.1.1 憑證之申請者

政府機關(構)授權之人員。

4.1.2 註冊程序及責任

1. 憑證簽發前應確認憑證申請者之身分。

2. 憑證申請者應提供身分識別相關文件。

3. 用戶責任如下：

(1) 遵守本作業基準及用戶約定條款，並確保提供申請資料之正確性。

(2) 確認憑證內容資訊之正確性，並依 4.4 節「憑證接受」規定辦理憑證接受；若憑證內容資訊不正確，應立即通知註冊中心。

(3) 依 1.4.1 節「憑證之適用範圍」規定使用憑證。

(4) 妥善保管與使用其私密金鑰。

(5) 憑證如須廢止，應依第 4.9 節「憑證暫時停用及廢止」規定辦理，用戶應承擔憑證廢止前所有使用該憑證之相關法律責任。

4.2 申請憑證之程序

1. 一般申請

(1) 憑證申請者至本管理中心網站提出憑證申請。

(2) 憑證申請者自行產製金鑰對，使用該金鑰對產製 PKCS#10 憑證申請檔後加以簽章，並將該憑證申請檔上傳。

(3) 憑證申請者將憑證申請書以公文函送註冊窗口辦理。

2. 線上申請

(1) 憑證申請者至本管理中心網站提出憑證申請。

(2) 憑證申請者自行產製金鑰對，使用該金鑰對產製 PKCS#10 憑證申請檔後加以簽章，並將該憑證申請檔上傳。

(3) 憑證申請者以機關(構)、單位憑證 IC 卡線上申請 TLS 憑證，無須以公文函送申請書。

3. 憑證自動換發機制

憑證申請者透過憑證自動換發機制，憑證申請程序(包括:金鑰對產製、申請檔上傳)將透過 ACME 系統完成。

4.2.1 執行識別及鑑別功能

本管理中心依 3.2.2 節「組織身分之鑑別程序」規定辦理識別及鑑別程序，說明如下：

1. 用戶身分識別及鑑別

(1) 一般申請

憑證審驗人員收到公文後，應依照審驗作業規範進行公文文號與發文單位進行比對，藉此進行身分識別、鑑別並確認該申請有經過授權。

(2) 線上申請

註冊中心將驗證申請者機關(構)、單位憑證 IC 卡之數位簽章做為身分鑑別之依據。

(3) 憑證自動換發機制

初次申請時以有效之政府機關(構)及單位憑證 IC 卡做為身分鑑別之依據，完成主機識別金鑰註冊後，將以該識別金鑰做為身分鑑別之依據。

2. 網域擁有者鑑別

(1) 本管理中心僅提供政府機關(構)與單位申請憑證，並依 3.2.2.2 節「網域名稱擁有者鑑別」規定辦理網域鑑別。

(2) 本管理中心定期從具公信力之組織所公布之釣魚網站或詐騙使用之網域名稱做為網域黑名單，憑證註冊審驗人員於憑證審驗時須確認此黑名單，以防止誤發。

簽發 TLS 憑證前，對於即將簽發的 TLS 憑證註記於 subjectAltName 擴充欄位的每一個 dNSName(亦即申請者提出憑證請求所包含的每一個完全吻合網域名稱)，本管理中心會進行以下檢查：

1. CAA 紀錄檢查：依照 RFC 8659 及憑證機構與瀏覽器論壇所發行之 Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates 正式版本中 3.2.2.8 節「CAA Records」之規定檢查 TLS 憑證申請案件之網域名稱是否有註記授權憑證機構簽發憑證之「網域名稱系統資源紀錄」，本管理中心於授權憑證機構簽發憑證紀錄中登記之域名為「gtlsca.nat.gov.tw」，以下情況本管理中心得簽發憑證：

   (1) 授權憑證機構簽發憑證之「網域名稱系統資源紀錄」已將本管理中心列為授權 TLS 憑證簽發之憑證機構。

   (2) 查無授權憑證機構簽發憑證之「網域名稱系統資源紀錄」。

   (3) 未註記任何被授權簽發之憑證機構。

2. 多重視角簽發驗證機制檢查：詳情請參照 3.2.8 節，此程序可提高對相同特定前綴邊界閘道協定 (Border Gateway Protocol, BGP) 攻擊或劫持之防護。

4.2.2 憑證申請之核准或拒絕

本管理中心完成申請資料審核、身分識別及鑑別作業後，始可核准憑證申請。

本管理中心於以下狀況得拒絕簽發憑證：

1. 未能通過 3.2.2 節「組織身分之鑑別程序」之要求。
2. 申請者曾違反用戶約定條款。
3. 其他經本管理中心認定得拒絕簽發之事項。

4.2.3 處理憑證申請之時間

1. 申請資料符合相關規定下，憑證註冊窗口應於 2 個工作日內完成身分鑑別及資料審核程序。

2. 憑證申請者配合完成網域驗證後，本管理中心於 1 個工作日內完成憑證簽發之作業。

4.3 憑證簽發

4.3.1 本管理中心於憑證簽發時之作業

1. 一般申請及線上申請

   本管理中心與註冊中心於收到憑證申請資料後，依第 3 章「識別及鑑別程序」規定進行審核程序，憑證申請審核及簽發程序如下：

   (1) 憑證註冊審驗人員依 3.2.2 節「組織身分之鑑別程序」及 4.2.1 節「執行識別及鑑別功能」規定完成機關(構)身分鑑別、網域名稱擁有者鑑別及授權憑證機構簽發憑證之確認。

   (2) 由用戶預先確認將簽發之憑證內容，確認無誤並經審核通過後本管理中心進行憑證簽發，並以電子郵件通知用戶。

2. ACME 憑證自動換發機制

   用戶透過 ACME 進行憑證自動換發申請時，本管理中心於收到 ACME 傳送之憑證申請後，依第 3 章「識別及鑑別程序」規定進行審核程序，憑證申請審核及簽發程序如下：

(1) 本管理中心依 3.2.2 節「組織身分之鑑別程序」及 4.2.1 節「執行識別及鑑別功能」規定完成機關(構)身分鑑別、網域名稱擁有者鑑別及授權憑證機構簽發憑證之確認。

(2) 憑證簽發後透過 ACME 系統將憑證傳送至用戶端，由用戶確認憑證內容正確後即視為接受該憑證。

3. 本管理中心因應憑證透明度機制產生之預簽憑證不得視為本管理中心所簽發之正式憑證。

4.3.2 本管理中心對用戶之憑證簽發通知

1. 憑證簽發後以電子郵件方式通知用戶。

2. 用戶可於憑證管理中心網站查詢憑證申請進度。

3. 如不同意簽發憑證時，應以電子郵件或電話通知用戶，並明確告知不同意簽發之理由。

4.4 憑證接受

1. 一般申請及線上申請

(1) 本管理中心預先提供憑證主體名稱與憑證主體別名供憑證申請者審視。

(2) 憑證申請者確認內容正確並於審視頁面點選憑證接受後，本管理中心即視為接受該憑證，進行憑證簽發並公告於儲存庫。

(3) 憑證申請者如發現憑證內容不正確時，應立即通知本管理中心或註冊中心，並提出憑證廢止申請。

2. 憑證自動換發機制

憑證申請者須於憑證簽發後確認憑證主體名稱與憑證主體別名是否正確，如不接受憑證須於 30 個日曆天內提出憑證廢止，若於時限內無提出憑證廢止申請，將視為接受該憑證。

4.4.1 接受憑證之要件

憑證申請者確認憑證主體名稱與憑證主體別名無誤並接受後，本管理中心依此做為憑證接受之依據。

4.4.2 本管理中心之憑證發布

本管理中心將簽發之憑證公布於儲存庫，或以電子郵件將憑證傳遞用戶，完成憑證發布作業。

4.4.3 本管理中心對其他個體之憑證簽發通知

本管理中心將所簽發之憑證公布於儲存庫。

4.5 金鑰對及憑證之用途

4.5.1 用戶私密金鑰及憑證使用

1. 用戶金鑰對之產製應符合 6.1.1 節「金鑰對產製」，且用戶須有私密金鑰之控制權。
2. 用戶私密金鑰不得用於簽發憑證。
3. 用戶應保護私密金鑰不被未經授權之他人使用或揭露，且確保私密金鑰依憑證擴充欄位所註記之金鑰用途使用。
4. 用戶須依憑證政策及本作業基準之規定使用憑證。

4.5.2 信賴憑證者公開金鑰及憑證使用

1. 信賴憑證者使用憑證時須符合本作業基準規定。
2. 信賴憑證者應使用符合 ITU-T X.509、IETF RFC、憑證機構與瀏覽器論壇所發行 Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates 相關標準或規範之軟體。
3. 信賴憑證者需驗證憑證有效性，包括憑證及其憑證串鏈中所有憑證機構之憑證。
4. 信賴憑證者應檢驗簽發憑證機構與用戶憑證之憑證政策擴充欄位，以確認憑證之保證等級。
5. 信賴憑證者應確認憑證用途。

4.6 憑證展期

本管理中心不提供憑證展期。

4.6.1 憑證展期之事由

不適用。

4.6.2 憑證展期之申請者

不適用。

4.6.3 憑證展期之程序

不適用。

4.6.4 對用戶憑證展期之簽發通知

不適用。

4.6.5 接受展期憑證之要件

不適用。

4.6.6 憑證機構之展期憑證發布

不適用。

4.6.7 本管理中心對其他個體之展期憑證簽發通知

不適用。

4.7 憑證之金鑰更換

指重新產生一組金鑰對，並以原有的註冊資訊向憑證機構申請憑證簽發。

4.7.1 憑證之金鑰更換事由

4.7.1.1 本管理中心憑證之金鑰更換事由

1. 私密金鑰執行簽發憑證用途之使用期限到期。
2. 本管理中心憑證被廢止。

4.7.1.2 用戶憑證之金鑰更換事由

1. 用戶私密金鑰使用期限到期。
2. 用戶憑證被廢止。

4.7.2 更換憑證金鑰之申請者

1. 本管理中心憑證之金鑰更換

   由本管理中心授權之人員向總管理中心提出下屬憑證機構憑證之申請。

2. 用戶憑證之金鑰更換

政府機關(構)授權之人員。

4.7.3 憑證之金鑰更換程序

1. 本管理中心應依總管理中心之憑證實務作業基準相關規定重新申請憑證。

2. 用戶應依 4.1 節「申請憑證」及 4.2 節「申請憑證之程序」規定辦理。

4.7.4 對用戶憑證金鑰更換之簽發通知

依 4.3.2 節「本管理中心對用戶之憑證簽發通知」規定辦理。

4.7.5 接受金鑰更換憑證之要件

1. 本管理中心依總管理中心之憑證實務作業基準相關規定接受金鑰更換之憑證。

2. 用戶依 4.4.1 節「接受憑證之要件」規定接受金鑰更換之憑證。

4.7.6 本管理中心之更換金鑰憑證發布

本管理中心將已完成金鑰更換之憑證公布於儲存庫，或以電子郵件傳遞用戶。

4.7.7 本管理中心更換金鑰後對其他個體之通知

本管理中心將金鑰更換後之憑證公布於儲存庫。

4.8 憑證變更

4.8.1 憑證變更之事由

本管理中心不提供用戶進行憑證變更。

4.8.2 憑證變更之申請者

不適用。

4.8.3 憑證變更之程序

不適用。

4.8.4 對用戶憑證變更之簽發通知

不適用。

4.8.5 接受憑證變更之要件

不適用。

4.8.6 本管理中心之憑證變更發布

不適用。

4.8.7 本管理中心對其他個體之憑證簽發通知

不適用。

4.9 憑證暫時停用及廢止

本管理中心提供全天候(7x24)之憑證廢止服務，但不提供憑證暫時停用服務。

4.9.1 廢止憑證之事由

4.9.1.1 廢止用戶憑證之情況

以下幾種情況發生時，本管理中心應於 24 小時內廢止憑證：

(1) 用戶以書面提交憑證機構同意廢止憑證

(2) 用戶告知憑證機構原有之憑證請求未經授權，且不追溯授予授權

(3) 憑證機構證實用戶之私密金鑰遭破解，且該私密金鑰與用戶憑證中所記載之公開金鑰成配對關係

(4) 得知一種經過驗證或證明的方法，可以根據憑證中的公鑰破解用戶的私鑰

(5) 憑證機構證實憑證中所記載之完全吻合網域名稱或 IP 位址在網域授權或控制權之驗證上是不可信賴的

以下幾種情況發生時，憑證機構應於合理的時間範圍內(快則 24 小時內，最遲於 5 個工作天內)廢止憑證：

(1) 用戶違反第 6.1.5 及第 6.1.6 節對於金鑰之長度及品質檢測之規定

(2) 憑證機構證實用戶之憑證遭到誤用

(3) 用戶違反用戶約定條款規定

(4) 憑證中所記載之完全吻合網域名稱或 IP 位址已被禁用(可能原因如網域名稱遭司法機關註銷或與網域名稱註冊商之間的授權或合約到期)

(5) 憑證中所記載之資訊已變更(例如主體名稱變更、主體證號變更或主體身分因解散或死亡而消失等)

(6) 憑證未依憑證機構之本文件之規定程序簽發時

(7) 憑證中所記載之資訊不正確(inaccurate)

(8) 憑證機構之簽發憑證的權力已逾期、被廢止或被中止，且不再維運儲存庫、公布憑證廢止清冊或提供線上憑證狀態協定(Online Certificate Status Protocol, OCSP)查詢服務

(9) 本文件所規定應廢止項目

(10) 獲悉已證明或經過驗證的方法會暴露用戶的私鑰，或者有明確的證據表明用於生成私鑰的特定方法存在缺陷

本管理中心依照上述應廢止憑證之情況，得逕行廢止用戶之憑證。

4.9.2 憑證廢止之申請者

憑證廢止之申請者如下：

1. 用戶。
2. 用戶之上級機關。
3. 本管理中心(包含註冊中心)。

用戶、信賴憑證者、應用軟體供應商及其他第三方的組織可針對有問題之憑證向本管理中心提出憑證問題報告(Certificate Problem Reports)，如認為須廢止憑證，內容須敘明廢止原因，本管理中心依4.9.3.3 節「憑證問題回應機制」規定，確認憑證廢止請求是否成立。

4.9.3 憑證廢止之程序

4.9.3.1 憑證廢止方式

本管理中心依 3.4 節「憑證廢止申請之識別及鑑別」規定完成用戶身分識別及鑑別後，始可進行憑證廢止。

1. 用戶申請憑證廢止

(1) 用戶至本管理中心網站填寫憑證廢止申請書，並以公文將憑證廢止申請書函送註冊窗口。

(2) 憑證註冊審驗人員依 3.4 節「憑證廢止申請之識別及鑑別」規定完成用戶身分識別及鑑別，並檢查憑證廢止申請書之正確性。

(3) 憑證廢止申請資料審核通過後，本管理中心於 1 個工作天內完成憑證廢止作業。

2. 本管理中心逕行廢止

需經憑證註冊審驗人員確認後，始可廢止憑證。

4.9.3.2 公告與通知

1. 廢止之憑證最遲於憑證廢止清冊下次更新時間(nextUpdate)前加入憑證廢止清冊中，並將憑證狀態資訊公告於儲存庫，直至該廢止憑證到期為止。
2. 本管理中心得以電子郵件、電話或公文方式通知申請者憑證廢止申請之結果。

4.9.3.3 憑證問題回應機制

1. 問題發現者可將憑證問題反應至 1.5.2 節「聯絡資料」所提供之電子郵件信箱。
2. 本管理中心提供全天候(7x24)憑證問題通報受理與憑證問題回應。
3. 本管理中心於接收到憑證問題後 24 小時內，應提供初步調查報告給用戶與問題發現者。
4. 本管理中心應與用戶及問題發現者共同討論，如須廢止該憑證，依下述準則評估與選定憑證廢止日期：

(1) 聲稱問題的內容(範圍、內容、嚴重性、重要程度及危害風險)。

(2) 憑證廢止的後果(對用戶與信賴憑證者的直接與間接影響)。

(3) 針對該憑證或該用戶提出之憑證問題數量。

(4) 提出憑證問題的單位或人員。

(5) 相關的法律條文。

本管理中心受理憑證問題報告或接收到憑證廢止通知之處理期限應依 4.9.5 節「本管理中心處理憑證廢止請求之處理期限」規定辦理。

4.9.4 憑證廢止申請之寬限期

指憑證廢止事由經確認後必須提出憑證廢止申請的時間。

1. 本管理中心本身之憑證須廢止時，須於 1 小時內通報總管理中心。
2. 用戶憑證須廢止時，最遲應於 10 個工作天內提出憑證廢止申請，本管理中心得視情況延展其憑證廢止之寬限期。

4.9.5 本管理中心處理憑證廢止請求之處理期限

本管理中心原則於接受憑證廢止申請後 5 個日曆天內完成憑證廢止作業，但符合下列情事者，則應於 1 個日曆天內完成憑證廢止：

1. 用戶向本管理中心提出憑證廢止申請。
2. 用戶通知本管理中心，並告知其原憑證請求未經授權且亦不願意重新授予授權。

3. 本管理中心證實用戶私密金鑰遭冒用、偽造或破解。
4. 憑證管理中心得知有方法可由用戶憑證內公開金鑰計算出對應私密金鑰。
5. 本管理中心證實憑證裡記載之完整網域名稱之網域授權或控管的驗證方式不受信賴。

4.9.6 信賴憑證者檢查憑證廢止之要求

信賴憑證者使用本管理中心所簽發之憑證前，應先檢驗本管理中心公布之憑證廢止清冊或線上憑證狀態協定回應訊息，以確認該憑證之有效性及憑證串鏈之正確性。

4.9.7 憑證廢止清冊簽發頻率

1. 憑證廢止清冊每日至少簽發 1 次，其有效期限不超過 36 小時。
2. 本管理中心於完成憑證廢止作業後的 24 小時內須重新簽發憑證廢止清冊。

4.9.8 憑證廢止清冊發布之最大延遲時間

本管理中心將提前於憑證廢止清冊所記載之下次更新時間前發布下一次憑證廢止清冊。

4.9.9 線上憑證廢止/狀態查驗之服務

1. 本管理中心提供憑證查詢與下載、憑證廢止清冊及線上憑證狀態協定查詢服務。
2. 本管理中心由線上憑證狀態協定回應伺服器(Online Certificate Status Protocol Responder, OCSP Responder)提供符

合 RFC 6960 及 RFC 5019 標準規範的線上憑證狀態協定回應訊息。

3. 本管理中心使用其簽章用私密金鑰簽發 RSA 2048 w/SHA-256 之線上憑證狀態協定回應伺服器之憑證。
4. 線上憑證狀態協定回應伺服器之憑證須包含符合 RFC 6960 規範之擴充欄位「id-pkix-ocsp-nocheck」。

4.9.10 線上憑證廢止查驗之規定

1. 信賴憑證者須以憑證廢止清冊或線上憑證狀態協定查詢服務驗證憑證之有效性。
2. 本管理中心線上憑證狀態協定回應伺服器至少可支援符合 RFC 6960 及 RFC 5019 標準規範所述之 HTTP GET 方法。
3. 線上憑證狀態協定查詢服務提供之憑證狀態資訊最晚於線上憑證狀態協定回應訊息效期之二分之一前更新，每次簽發之線上憑證狀態協定回應訊息效期至少 8 小時，最長不超過 16 小時。
4. 線上憑證狀態協定查詢封包內含之憑證序號可分為 3 種：
   (1) 已分配：本管理中心已簽發憑證之憑證序號；
   (2) 已保留：本管理中心簽發 TLS 憑證所需之預簽憑證的憑證序號；
   (3) 未使用：不符合前述條件之憑證序號。
5. 線上憑證狀態協定回應伺服器收到內含「已分配」之憑證序號的線上憑證狀態協定查詢封包時，應依該憑證序號所對應之憑證當時之狀態回覆。

6. 線上憑證狀態協定回應伺服器收到內含「未使用」之憑證序號的線上憑證狀態協定查詢封包時，不可回覆其狀態為「正常(Good)」，且本管理中心應監督線上憑證狀態協定回應伺服器對於這類請求的回覆是否符合其安全回應程序。

4.9.11 其他形式廢止公告

1. 本管理中心依據 RFC 4366 規範支援線上憑證狀態協定裝訂(OCSP Stapling)。
2. 用戶如採用上述協定查詢憑證狀態，本管理中心應透過用戶約定條款或技術檢視等方式要求用戶啟用線上憑證狀態協定裝訂。

4.9.12 金鑰被破解時之其他特殊規定

1. 本管理中心私密金鑰被破解時，由總管理中心簽發憑證廢止清冊，並通知應用軟體供應商、用戶及信賴憑證者。
2. 用戶私密金鑰被破解時、洩漏欲廢止憑證時，應通知本管理中心並依 4.9.3 節「憑證廢止之程序」規定辦理。
3. 由第三方提交私密金鑰被破解或洩漏之證據時，應依 4.9.3.3 節「憑證問題回應機制」規定辦理。本管理中心可接受該證據之方式如下：
   (1) 使用挑戰及回應之機制：由本管理中心提供隨機值或文件，由第三方以該私密金鑰對該隨機值或文件進行數位簽章，本管理中心再透過簽章驗證，確認第三方確實握有被破解或洩漏之私密金鑰。
   (2) 透過安全且可信賴之管道提供該私密金鑰。

4. 因私密金鑰被破解或洩漏而被廢止之用戶憑證，其於憑證廢止清冊註記之原因代碼為「keyCompromise(1)」。

4.9.13 暫時停用憑證之事由

依據憑證機構與瀏覽器論壇所發行之 Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates 之規定，TLS 憑證不得暫時停止使用。

4.9.14 暫時停用憑證之申請者

不適用。

4.9.15 暫時停用憑證之程序

不適用。

4.9.16 暫時停用憑證期間之限制

不適用。

4.10 憑證狀態服務

4.10.1 服務特性

憑證廢止清冊或線上憑證狀態協定回應訊息中之憑證廢止資訊，須至該被廢止之憑證已過期後始可移除。

4.10.2 服務可用性

1. 於正常運作情況下，本管理中心提供之憑證廢止清冊與線上憑證狀態協定查詢服務之回覆時間至多 10 秒。

2. 本管理中心提供全天候(7 x 24)不中斷之儲存庫服務，供應用軟體檢查所有未過期憑證之最新狀態。

3. 本管理中心提供全天候(7 x 24)回應機制處理高優先權之憑證問題報告；本管理中心可視案件情況向執法當局舉發，並得逕行廢止發生問題之憑證。

4.10.3 可選功能

不予規定。

4.11 終止服務

指憑證用戶不再使用本管理中心之服務；本管理中心同意用戶終止服務之要件如下：

1. 憑證到期。

2. 用戶廢止憑證。

4.12 私密金鑰託管及回復

4.12.1 金鑰託管及回復政策與實務

1. 本管理中心簽章用之私密金鑰不可被託管。

2. 本管理中心不提供用戶私密金鑰託管與回復。

4.12.2 通訊用金鑰封裝及回復政策與實務

本管理中心不提供通訊用金鑰封裝與回復。

5 基礎設施、安全管理及作業程序控管

5.1 實體控管

5.1.1 實體位置及結構

本管理中心機房位於台北市信義路 1 段 21 號數據通信大樓內之安全機房，具備門禁、保全、入侵偵測及監視錄影等實體安全機制。

5.1.2 實體存取

1. 本管理中心之實體控管符合保證等級第 3 級規定，包含：
   (1) 大門及大樓警衛。
   (2) 進出管制系統。
   (3) 指紋辨識系統。
   (4) 機箱監控系統。
2. 可攜式儲存媒體須檢查並確認無電腦病毒及惡意軟體。
3. 非授權人員進出機房時，須填寫進出紀錄，並由本管理中心人員全程陪同。

5.1.3 電力及空調

1. 機房之電力系統包括市電、發電機(滿載油料可連續運轉 6 天)及不斷電系統，可提供至少 6 小時以上備用電力。
2. 機房設有恆溫恆濕空調系統。

5.1.4 水災防範及保護

機房位於建築物第 3 樓層(含)以上，具備防水閘門及抽水機。

5.1.5 火災防範及保護

機房具備自動偵測火災預警功能，系統可自動啟動滅火設備，並於各機房主要出入口設置手動開關。

5.1.6 媒體儲存

稽核紀錄、歸檔及備援資料，除儲存 1 份於主機房外，另將複製 1 份送至異地備援場所儲存。

5.1.7 汰換設備處理

儲存機敏性資料之媒體不再使用時，須依政府機關資安規定或其他經數位部同意之方式辦理銷毀作業。

5.1.8 異地備援

1. 異地備援地點位於臺中，與主機房距離 30 公里以上。
2. 備援內容包括資料及系統程式，資料備份至少 1 個月執行 1 次。
3. 異地備援系統與主系統具相同之安全等級。

5.2 程序控管

各信賴角色依工作內容進行識別及鑑別，以確保作業程序之安全。

5.2.1 信賴角色

1. 信賴角色分為管理員、簽發員、稽核員、維運員及實體安全控管員，工作內容說明如下：

(1) 管理員：

- 安裝、設定及維護本管理中心系統。

- 建立及維護本管理中心系統之使用者帳號。
- 設定稽核參數。
- 產製及備份本管理中心之金鑰。

(2) 簽發員：

- 啟動或停止憑證簽發服務。
- 啟動或停止憑證廢止服務。

(3) 稽核員：

- 對稽核紀錄之查驗、維護及歸檔。
- 執行或監督內部稽核。

(4) 維運員：

- 系統及設備之運作維護。
- 系統備份作業。
- 儲存媒體之更新。
- 憑證管理系統外之軟硬體更新。
- 系統異常及網路安全事件之通報等。

(5) 實體安全控管員：

- 系統之實體安全控管。

2. 信賴角色依 5.3 節「人員控管」規定進行人員控管。

3. 各信賴角色可由多人擔任，並設有 1 名主管。

5.2.2 工作內容所需人數

各信賴角色所需之人數如下：

1. 管理員：至少 3 位。
2. 簽發員：至少 3 位。
3. 稽核員：至少 2 位。
4. 維運員：至少 2 位。
5. 實體安全控管員：至少 2 位。

各工作內容所需之人數說明如下：

工作內容	管理員	簽發員	稽核員	維運員	實體安全控管員
安裝、設定及維護本管理中心憑證管理系統	1				1
建立及維護本管理中心憑證管理系統之使用者帳號	1				1
設定稽核參數	1				1
產製及備份本管理中心之金鑰	2		1		1
啟動或停止憑證簽發服務		2			1
啟動或停止憑證廢止服務		2			1
對稽核紀錄之查驗、維護及歸檔			1		1
系統設備之日常運作維護				1	1
系統之備份作業				1	1
儲存媒體之更新				1	1
除本管理中心憑證管理系統外之軟硬體更新				1	1
網站之維護	1				1

工作內容	管理員	簽發員	稽核員	維運員	實體安全控管員
系統病毒碼與弱點之修補作業(稽核主機)	1		1	1	1
系統病毒碼與弱點之修補作業(稽核主機以外系統)	1			1	1

5.2.3 角色識別及鑑別

1. 以使用者帳號、密碼及 IC 卡等，識別及鑑別管理員、簽發員、稽核員及維運員。

2. 以中央門禁系統，識別及鑑別實體安全控管員。

5.2.4 角色權責劃分

各角色分派須符合下列規定：

1. 管理員、簽發員及稽核員不得相互兼任。

2. 實體安全控管員不得兼任其他信賴角色。

3. 不允許執行自我稽核。

5.3 人員控管

5.3.1 身家背景、資格、經驗及安全需求

1. 人員甄選及進用前須進行安全評估。

2. 人員須定期進行考核管理。

3. 人員須定期進行教育訓練。

4. 人員應遵守並簽訂保密切結。

5.3.2 身家背景之查驗程序

1. 本管理中心工作人員，須由本管理中心及人事相關部門主管依各信賴角色之資格執行實務、經歷及身分背景審查。

2. 每年依各信賴角色之職務特性，執行實務與經歷之審查，確認是否適任。

5.3.3 教育訓練需求

各信賴角色之教育訓練需求如下：

信賴角色	教育訓練需求
管理員	1. 本管理中心之安全認證機制。 2. 本管理中心系統安裝、設定及維護之操作程序。 3. 建立及維護系統用戶帳號之操作程序。 4. 設定稽核參數之操作程序。 5. 產製及備份本管理中心金鑰之操作程序。 6. 災難復原及業務永續經營之程序。
簽發員	1. 本管理中心之安全認證機制。 2. 憑證簽發之操作程序。 3. 憑證廢止之操作程序。 4. 災難復原及業務永續經營之程序。
稽核員	1. 本管理中心之安全認證機制。 2. 本管理中心稽核系統之使用及操作程序。 3. 稽核紀錄查驗、維護及歸檔之程序。 4. 災難復原及業務永續經營之程序。
維運員	1. 系統備份之作業程序。 2. 系統設備日常運作之維護程序。 3. 儲存媒體之更新程序。 4. 災難復原及業務永續經營之程序。
實體安全控管員	1. 設定實體門禁權限程序。 2. 災難復原及業務永續經營之程序。

5.3.4 人員再教育訓練之需求及頻率

1. 各信賴角色每年進行 1 次教育訓練。
2. 軟硬體升級、工作程序改變、設備更換或相關法規改變時。

5.3.5 工作調換之頻率及順序

1. 管理員調離原職務滿 1 年後，方可轉任簽發員或稽核員。
2. 簽發員調離原職務滿 1 年後，方可轉任管理員或稽核員。
3. 稽核員調離原職務滿 1 年後，方可轉任管理員或簽發員。
4. 維運員滿 2 年，且已接受相關教育訓練及通過審核，方可轉任管理員、簽發員或稽核員。

5.3.6 未授權行為之懲處

人員如違反相關規定，應接受適當之管理及懲處，如情節重大致造成損害者，本管理中心得採取法律行動追究其責任。

5.3.7 聘僱人員之規定

聘僱人員須簽訂保密協定，並依規定進行作業。

5.3.8 提供之文件資料

本管理中心提供之文件包括憑證政策、技術規範、本作業基準、系統操作手冊及電子簽章法等相關文件。

5.4 稽核紀錄程序

1. 安全相關事件均保存安全稽核紀錄(Audit Log)，且於執行稽核時可立即取得。

2. 安全稽核紀錄可為系統自動產生或人工紙本紀錄方式。

5.4.1 事件紀錄之類型

本管理中心及委派第三方應紀錄之事件類型如下：

1. 安全稽核
   - 重要稽核參數之改變。
   - 嘗試刪除或修改稽核紀錄。
2. 識別及鑑別
   - 嘗試設定新角色。
   - 管理者調整身分鑑別嘗試之最高容忍次數。
   - 登入系統失敗。
   - 帳號解鎖。
   - 改變系統之身分鑑別機制。
3. 本管理中心產製金鑰時(不包括單次使用之金鑰產製)。
4. 本管理中心私密金鑰之存取
5. 用戶憑證之簽發及廢止
6. 除單次使用之金鑰外，其餘私密金鑰之匯出。
7. 憑證註冊、廢止及狀態改變之申請及驗證過程。
8. 安全相關之組態設定改變。
9. 帳號之新增、刪除及存取權限修改
10. 憑證格式剖繪之改變
11. 憑證廢止清冊格式剖繪之改變

12. 本管理中心之伺服器設定改變
13. 實體存取及場所之安全
14. 異常事件
15. 密碼模組生命週期管理
16. 憑證廢止清冊的產製
17. 線上憑證狀態協定回應訊息的簽發
18. 本作業基準及憑證機構與瀏覽器論壇發行 Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates 正式版本
19. 憑證申請請求的核准與拒絕

5.4.2 紀錄處理頻率

本管理中心每月檢視 1 次稽核紀錄，並追蹤調查重大事件。

5.4.3 稽核紀錄保留期限

本管理中心及委派第三方應保留稽核紀錄至少 2 年，保留期限屆滿時，由稽核員移除資料，不可由其他人員代理。

5.4.4 稽核紀錄之保護

1. 使用簽章、加密技術保存之稽核紀錄，應使用無法更改紀錄之媒體儲存。
2. 簽署事件紀錄之私密金鑰不可使用於其他用途。
3. 稽核系統之私密金鑰應有安全保護措施。
4. 稽核紀錄須存放於安全場所。

5.4.5 稽核紀錄備份程序

1. 電子式稽核紀錄每月備份 1 次。
2. 稽核系統以每日、每星期及每月等周期將稽核紀錄自動歸檔。

5.4.6 稽核紀錄彙整系統

稽核紀錄彙整系統內建於本管理中心之系統，稽核程序於管理中心系統啟動時啟用。

自動稽核系統如無法正常運作，且系統資料處於高風險狀態時，本管理中心將暫停憑證簽發服務，直至問題解決後再行提供服務。

5.4.7 對引起事件者之告知

稽核系統不須告知引起事件之個體，其引發之事件已被系統紀錄。

5.4.8 弱點評估

本管理中心每年進行 1 次風險評鑑，對作業系統、實體設施、憑證管理系統及網路進行評估。

5.5 紀錄歸檔之方法

5.5.1 歸檔紀錄之類型

本管理中心及委派第三方應歸檔紀錄之類型如下：

1. 本管理中心向總管理中心申請憑證之相關資料。
2. 憑證實務作業基準。
3. 重要契約。
4. 系統或設備組態設定。

5. 系統或組態設定之修改或更新之內容。
6. 憑證申請資料。
7. 廢止申請資料。
8. 憑證接受之確認紀錄。
9. 符記啟用紀錄。
10. 已簽發或公告之憑證。
11. 本管理中心金鑰更換之紀錄。
12. 已簽發或公告之憑證廢止清冊。
13. 稽核紀錄。
14. 用以驗證及佐證歸檔內容之其它說明資料或應用程式。
15. 稽核人員所要求之文件。
16. 依 3.2.2 節「組織身分之鑑別程序」規定所定之組織身分鑑別資料。

5.5.2 歸檔紀錄保留期限

1. 歸檔紀錄及處理歸檔紀錄之應用程式，其保留期限至少為 2 年。
2. 歸檔紀錄逾保留期限後，書面資料應以安全方式銷毀；電子形式之資料檔得另備份至其他儲存媒體並提供適當保護，或以安全方式銷毀。

5.5.3 歸檔紀錄之保護

1. 不允許新增、修改或刪除歸檔紀錄。

2. 歸檔紀錄移至另一個儲存媒體，其保護等級不得低於原保護等級。

3. 歸檔紀錄應存放於安全場所。

5.5.4 歸檔紀錄備份程序

1. 電子式紀錄定期備份至異地備援中心。

2. 紙本紀錄將由本管理中心授權之人員定期整理歸檔。

5.5.5 歸檔紀錄之時戳要求

1. 歸檔之電子式紀錄內容應包含日期及時間資訊，並經適當之數位簽章保護，用以檢測紀錄中之日期及時間資訊是否遭篡改。

2. 電子式紀錄中之日期及時間資訊，係為電腦作業系統之日期及時間，非第三方所提供之電子式時戳資料。

3. 本管理中心所有電腦系統均定期進行校時。

4. 歸檔之書面紀錄亦記載日期資訊，必要時得記載時間資訊。紀錄之日期及時間紀錄如有更改時須由稽核人員簽名確認。

5.5.6 歸檔紀錄彙整系統

本管理中心無歸檔紀錄彙整系統。

5.5.7 取得及驗證歸檔紀錄之程序

1. 歸檔紀錄須以書面申請並經同意後方可取得。

2. 稽核員負責驗證歸檔紀錄，書面文件須驗證文件簽署者及日期等之真偽；電子檔須驗證歸檔紀錄之數位簽章。

5.6 金鑰更換

1. 本管理中心私密金鑰於簽發憑證用途之使用期限到期前，應完成用以簽發憑證之金鑰對更換作業，並取得總管理中心核發之下屬憑證機構憑證。

2. 用戶之私密金鑰依 6.3.2 節「公開金鑰及私密金鑰之使用期限」規定定期更換，用戶更換金鑰並申請憑證時，應依 4.2 節「申請憑證之程序」規定辦理。

5.7 破解或災害時之復原程序

5.7.1 緊急事件及系統遭破解之處理程序

本管理中心訂定緊急事件及系統遭破解之通報與處理程序，每年依該程序進行演練。本管理中心為防止延遲廢止 TLS 憑證，每年定期舉行憑證大批廢止之演練。

5.7.2 電腦資源、軟體或資料遭破壞之復原程序

本管理中心訂定電腦資源、軟體或資料遭破壞之復原程序，且每年依該程序進行演練。

電腦設備遭破壞無法運作時，須優先回復儲存庫之運作，並迅速重建憑證簽發及管理之能力。

5.7.3 本管理中心簽章金鑰遭破解之復原程序

本管理中心訂有簽章金鑰遭破解之復原程序，且每年依該程序進行演練。

5.7.4 本管理中心安全設施之災後復原工作

1. 本管理中心每年對安全設施之災難復原工作進行演練。

2. 當發生災害時，將啟動災害復原程序，優先回復本管理中心儲存庫之運作，並迅速重建憑證簽發及管理的能力。

5.8 本管理中心之終止服務

1. 除無法通知者外，管理中心於預定終止服務 3 個月前，應通知所有未廢止及未過期憑證之用戶，並公告於儲存庫。

2. 廢止全部有效憑證，並進行檔案紀錄之保管及移交工作。

6 技術性安全控管

6.1 金鑰對產製及安裝

6.1.1 金鑰對產製

6.1.1.1 本管理中心金鑰對之產製

1. 本管理中心依 6.2.1 節「密碼模組標準及控管」規定於硬體密碼模組內產製金鑰對，其金鑰產製過程採用符合 NIST FIPS 140-2 規範之亂數產生機制與 RSA 金鑰演算法。
2. 私密金鑰之匯出與匯入依 6.2.2 節「金鑰分持多人控管」與 6.2.6 節「私密金鑰及密碼模組間傳輸」規定進行。
3. 金鑰產製須準備與遵循金鑰產製腳本，由本管理中心相關人員及合格稽核員(Qualified Auditor)見證下進行，且金鑰產製過程須錄影留存。
4. 合格稽核員應出具金鑰產製典禮見證報告，確認本管理中心金鑰產製過程依循其金鑰產製腳本與管控措施，確保金鑰對之完整性及機密性。

6.1.1.2 用戶金鑰對之產製

用戶須自行產製金鑰對，如發生以下情事者，本管理中心應拒絕該用戶憑證請求：

1. 金鑰對不符合 6.1.5 節「金鑰長度」與 6.1.6 節「公開金鑰參數之產製與品質檢驗」之規定。
2. 確認金鑰產製方法有瑕疵。
3. 證實使用可揭露私密金鑰並致使其遭破解之方法。

4. 本管理中心事先得知用戶私密金鑰已被破解時。
5. 憑證管理中心得知有方法可由公開金鑰計算出對應私密金鑰。

6.1.2 私密金鑰安全傳送予用戶

不適用。

6.1.3 公開金鑰安全傳送予本管理中心

用戶自行產製金鑰對，並以 PKCS#10 憑證申請檔之格式將公開金鑰傳送至註冊中心，註冊中心依照 3.2.1 節「證明擁有私密金鑰之方式」規定，檢驗用戶確實擁有相對應之私密金鑰後，再以傳輸層安全協定或安全強度相同之資料加密傳送方式將用戶之公開金鑰傳送至管理中心。

6.1.4 本管理中心公開金鑰安全傳送予信賴憑證者

本管理中心之之憑證由總管理中心簽發，並公布於總管理中心及本管理中心之儲存庫，供用戶及信賴憑證者直接下載與使用。

6.1.5 金鑰長度

1. 本管理中心使用金鑰長度為 4096 位元之 RSA 金鑰，並以 SHA-256、SHA-384 或 SHA-512 雜湊函數演算法簽發憑證。
2. 用戶使用金鑰長度至少須為 2048 位元之 RSA 金鑰。
3. 本管理中心與用戶使用之 RSA 金鑰長度(以位元為單位)須可被 8 整除。

6.1.6 公開金鑰參數之產製與品質檢驗

1. RSA 演算法之公開金鑰參數為空值。

2. 本管理中心簽章用金鑰對採用 ANSI X9.31 演算法或 NIST FIPS 186-4 規範產生 RSA 演算法所需之質數，並確保該質數為強質數。
3. 用戶於軟硬體密碼模組中產製 RSA 演算法所需之質數，需確保該質數為強質數。
4. 本管理中心依據 NIST SP 800-89 第 5.3.3 節之規定，確認 RSA 演算法所使用之公開指數值為大於 3 的奇數，且其值介於 $2^{16}+1$ 與 $2^{256}-1$ 之間。此外，模數應具有奇數、非質數的指數次方且沒有小於 752 的因數等性質。

6.1.7 金鑰使用目的

1. 本管理中心簽章用私密金鑰僅用於簽發憑證、憑證廢止清冊及線上憑證狀態協定回應訊息。
2. 本管理中心憑證之金鑰用途(Key Usage)擴充欄位設定為 digitalSignature、keyCertSign 及 cRLSign。
3. TLS 憑證之金鑰用途擴充欄位設定為 digitalSignature 與 keyEncipherment，其延伸金鑰用途(Extended Key Usage)擴充欄位包含 serverAuth 與 clientAuth。

6.2 私密金鑰保護及密碼模組安全控管措施

6.2.1 密碼模組標準及控管

本管理中心使用通過 FIPS 140-2 安全等級第 3 級認證之硬體密碼模組。

6.2.2 金鑰分持多人控管

1. 本管理中心之金鑰分持多人控管採 m-out-of-n 方法，做為金鑰啟動與停用以及金鑰分持備份與回復之方式。

2. 本管理中心於金鑰產製後，將金鑰分為 5 份，分別存放於不同之安全地點，須取得至少 3 份方能執行金鑰回復。

6.2.3 私密金鑰託管

1. 本管理中心簽章用之私密金鑰不可被託管。

2. 本管理中心不提供用戶私密金鑰託管。

6.2.4 私密金鑰備份

本管理中心採用金鑰分持多人控管方法備份私密金鑰，並使用通過 FIPS 140-2 安全等級第 2 級以上驗證之 IC 卡做為秘密分持之儲存媒體。

6.2.5 私密金鑰歸檔

1. 本管理中心簽章用私密金鑰不可被歸檔，但相對應的公開金鑰依 5.5 節「紀錄歸檔之方法」規定，以憑證檔案格式進行歸檔。

2. 用戶簽章用私密金鑰，本管理中心不進行歸檔。

6.2.6 私密金鑰及密碼模組間傳輸

1. 本管理中心於下列情況進行私密金鑰與密碼模組間傳輸：

   (1) 金鑰備份與金鑰回復。

   (2) 更換密碼模組。

2. 本管理中心之私密金鑰匯入、匯出密碼模組時，採加密或金鑰分持多人控管方式保護。

6.2.7 私密金鑰儲存於密碼模組

1. 私密金鑰依規定儲存於密碼模組內。
2. 密碼模組如不需使用時，須離線並儲存於安全場所。

6.2.8 私密金鑰之啟動方式

1. 本管理中心私密金鑰之啟動是由多人控管 IC 卡控制，IC 卡組分別由管理員與簽發員保管。
2. 用戶私密金鑰啟動方式依私密金鑰儲存媒體類別說明如下：

(1) 硬體密碼模組：私密金鑰之啟動方式須由多人控管 IC 卡來控制。

(2) 其他私密金鑰載具：用戶應使用高強度通行碼或相同等級的鑑別方式啟動私密金鑰。

6.2.9 私密金鑰之停用方式

1. 本管理中心私密金鑰之停用以多人控管方式進行。
2. 本管理中心不提供用戶之私密金鑰停用。

6.2.10 私密金鑰之銷毀方式

1. 本管理中心私密金鑰之銷毀方式說明如下：

(1) 舊私密金鑰不再使用時，本管理中心將硬體密碼模組中存放舊私密金鑰之記憶位址進行零值化(Zeroization)處

理，以銷毀硬體密碼模組中舊私密金鑰，同時將對應之金鑰備援秘密持份 IC 卡進行實體銷毀。

(2) 硬體密碼模組汰除時，硬體密碼模組中所有的私密金鑰皆應被銷毀，並於銷毀後使用該硬體密碼模組之金鑰管理工具確認所有私密金鑰已銷毀。

2. 用戶之私密金鑰銷毀方式，不另做規定。

6.2.11 密碼模組評等

密碼模組評等方式依憑證政策 6.2.1 節「密碼模組標準及控管」規定辦理。

6.3 金鑰對管理之其他規定

本管理中心不負責保管用戶之私密金鑰。

6.3.1 公開金鑰之歸檔

本管理中心依 5.5 節「紀錄歸檔之方法」規定進行用戶憑證之歸檔。

6.3.2 公開金鑰及私密金鑰之使用期限

6.3.2.1 本管理中心公開金鑰及私密金鑰之使用期限

1. 本管理中心公開金鑰與私密金鑰使用期限至多為 20 年
2. 以私密金鑰執行簽發用戶憑證用途之使用期限至多為 10 年
3. 私密金鑰執行簽發用戶憑證用途之使用期限到期後，仍須簽發憑證廢止清冊或線上憑證狀態協定回應伺服器憑證，持續至該私密金鑰簽發之所有用戶憑證到期為止。

6.3.2.2 用戶公開金鑰及私密金鑰之使用期限

依照憑證機構與瀏覽器論壇發行 Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates 正式版本之規定，用戶憑證效期不得超過 398 天。

6.4 啟動資料

6.4.1 啟動資料之產生及安裝

本管理中心私密金鑰之啟動資料由硬體密碼模組亂數產生並寫入硬體密碼模組後，再寫入至多人分持控管 IC 卡中。

6.4.2 啟動資料之保護

1. 本管理中心之啟動資料由多人分持控管 IC 卡保護，須透過硬體密碼模組內建之讀卡機存取，並於硬體密碼模組內建之鍵盤上輸入 IC 卡個人識別碼(以下簡稱為 PIN 碼)。
2. 上述 IC 卡之 PIN 碼不得記錄於任何媒體上。
3. 登入之失敗次數如超過 3 次時，該 IC 卡即被鎖住。
4. IC 卡移交時，保管人員須重新設定 PIN 碼。

6.4.3 啟動資料之其他規範

不予規定。

6.5 電腦軟硬體安控措施

6.5.1 特定電腦安全技術需求

本管理中心提供安全控管功能說明如下：

1. 具備身分鑑別之登入。
2. 提供自行定義存取控制。
3. 提供安全稽核能力 。
4. 對各種憑證服務與公開金鑰基礎建設信賴角色存取控制之限制。
5. 具備公開金鑰基礎建設信賴角色與相關身分之識別及鑑別。
6. 以密碼技術確保每次通訊與資料庫之安全。
7. 具備公開金鑰基礎建設信賴角色與相關身分識別之安全與可信賴管道。
8. 具備程序完整性與安全控管保護。
9. 有權簽發憑證的帳號均應使用多因子認證方式驗證身分。

6.5.2 電腦安全評等

本管理中心採用安全強度與 C2(TCSEC)、E2(ITSEC)或 EAL3(CC)等級相當之電腦作業系統，且系統及運作環境符合 WebTrust Principles and Criteria for Certification Authorities 之安全控管原則。

6.6 生命週期技術控管措施

6.6.1 系統研發控管措施

1. 依主管機關認可之軟體工程發展方法與品質管理規範進行開發與品質控管。
2. 系統開發環境、測試環境及正式環境應獨立運作，以防止未經授權存取或變更之風險。

3. 使用專用且獲得授權之軟硬體。
4. 軟體於初次使用或更新版本前須完成源碼掃描安全檢測，並定期執行安全性掃描作業。
5. 各項交付本管理中心之產品或程式應提供交付清單、測試報告及原始程式碼安全性掃描報告，並進行程式版本控管。

6.6.2 安全管理控管措施

1. 不得安裝與運作無關之軟硬體或元件。
2. 軟體安裝時應確認版本完整性及正確性，並每日自動檢查軟體之完整性。
3. 系統之變動均須紀錄與控管。
4. 須具備修改系統軟體或組態之偵測機制。

6.6.3 生命週期安全控管措施

本管理中心每年至少進行 1 次現行金鑰是否有被破解之風險評估。

6.7 網路安全控管措施

1. 本管理中心遵照憑證機構與瀏覽器論壇所發行之 Network and Certificate System Security Requirements 之規定進行網路安全控管。
2. 本管理中心之主機與儲存庫透過資安防護設備進行隔離。
3. 儲存庫置於資安防護設備對外服務區，連接至網際網路。

4. 本管理中心之儲存庫係透過系統修補程式之更新及資安系統加以保護，以防範阻絕服務與入侵等攻擊。

6.8 時戳

為確保下述時間之正確性，本管理中心定期依據受信賴之時間源進行系統校時，且系統校時作業須可被稽核。

1. 用戶憑證簽發時間。
2. 用戶憑證廢止時間。
3. 憑證廢止清冊之簽發時間。
4. 系統事件之發生時間。

7 憑證、憑證廢止清冊及線上憑證狀態協定格式剖繪

7.1 憑證之格式剖繪

本管理中心簽發之憑證遵照 ITU-T X.509、憑證機構與瀏覽器論壇所發行之 Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates 及 RFC 5280 或其最新版相關之規定。

本管理中心透過密碼學安全偽亂數生成器(Cryptographically Secure Pseudorandom Number Generator, CSPRNG)產生其所簽發之憑證的憑證序號，此憑證序號為長度至少 64 位元且非循序之正整數。

7.1.1 版本序號

本管理中心簽發遵照 RFC 5280 與 ITU-T X.509 v3 版本之憑證。

7.1.2 憑證擴充欄位

憑證擴充欄位遵照 ITU-T X.509、憑證機構與瀏覽器論壇所發行之 Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates、RFC 5280 及 ePKI 技術規範相關規定。

7.1.2.1 本管理中心憑證

本管理中心憑證之擴充欄位內容如下：

擴充欄位名稱	必要性	關鍵性	內容
憑證機構金鑰識別碼 (Authority Key Identifier)	必要	FALSE	總管理中心之公開金鑰 SHA-1 雜湊值

擴充欄位名稱	必要性	關鍵性	內容
主體金鑰識別碼 (Subject Key Identifier)	必要	FALSE	本管理中心之公開金鑰 SHA-1 雜湊值
憑證政策 (Certificate Policies)	必要	FALSE	此擴充欄位標示本管理中心經總管理中心核准並允許使用之憑證政策物件識別碼，包含： ■ 憑證政策定義之保證等級第 3 級憑證政策物件識別碼。 ■ 憑證機構與瀏覽器論壇定義之組織驗證型 TLS 憑證政策物件識別碼「2.23.140.1.2.2」。
憑證廢止清冊發布點 (CRL Distribution Points)	必要	FALSE	總管理中心公告之憑證廢止清冊的下載網址
憑證機構資訊存取 (Authority Information Access)	必要	FALSE	此擴充欄位包含以下兩項資訊： ■ 總管理中心之自簽憑證下載網址 ■ 總管理中心所提供之線上憑證狀態協定查詢服務的網址
基本限制 (Basic Constraints)	必要	TRUE	Subject Type=CA Path Length Constraint=0 (本管理中心不再向下簽發下屬憑證機構憑證，故 pathLenConstraint 欄位設定為 0)
金鑰用途	必要	TRUE	keyCertSign、digitalSignature 及 cRLSign (本管理中心為保留未來使用簽章用私密金鑰簽線上憑證狀態協定回應訊息的可能性，故金鑰用途擴充欄包含 digitalSignature)
名稱限制 (Name Constraints)	禁用	TRUE	本管理中心不使用此擴充欄位
延伸金鑰用途	必要	FALSE	伺服器驗證 (1.3.6.1.5.5.7.3.1) 用戶端驗證 (1.3.6.1.5.5.7.3.2)

7.1.2.2 用戶憑證

用戶憑證之擴充欄位內容如下：

擴充欄位名稱	必要性	關鍵性	內容
憑證機構金鑰識別碼	必要	FALSE	本管理中心之公開金鑰 SHA-1 雜湊值
主體金鑰識別碼	可選	FALSE	用戶之公開金鑰 SHA-1 雜湊值
憑證政策	必要	FALSE	此擴充欄位標示本管理中心使用之憑證政策物件識別碼，包含： ■ 憑證政策定義之保證等級第 3 級憑證政策物件識別碼。 ■ 憑證機構與瀏覽器論壇定義之組織驗證型 TLS 憑證政策物件識別碼「2.23.140.1.2.2」。
憑證廢止清冊發布點	必要	FALSE	本管理中心公告憑證廢止清冊的下載網址
憑證機構資訊存取	必要	FALSE	此擴充欄位包含以下兩項資訊： ■ 本管理中心之憑證機構憑證下載網址 ■ 本管理中心所提供線上憑證狀態協定查詢服務網址
基本限制	可選	TRUE	Subject Type=End Entity Path Length Constraint=None (本管理中心目前未使用此擴充欄位)
金鑰用途	必要	TRUE	digitalSignature 與 keyEncipherment
延伸金鑰用途	必要	FALSE	伺服器驗證 (1.3.6.1.5.5.7.3.1) 用戶端驗證 (1.3.6.1.5.5.7.3.2)
主體別名	必要	FALSE	記錄此 TLS 憑證所包含的完整網域名稱(此擴充欄位至少包含 1 筆完整網域名稱)
已簽憑證時間戳記清	必要	FALSE	此擴充欄位記載由數個憑證透明度日誌伺服器(Certificate Transparency

擴充欄位名稱	必要性	關鍵性	內容
單 (Signed Certificate Timestamp List)			Log Server)回傳之已簽憑證時間戳記(Signed Certificate Timestamp, SCT)

本管理中心不允許簽發下述兩種情境之憑證：

1. 憑證的擴充欄位內含無法應用於公眾網路的設定。

2. 憑證的內容包含可能誤導信賴憑證者相信該憑證資訊已經由本管理中心驗證之語意。

本管理中心採用「X.509 v3 擴充欄位」之方法支援憑證透明度(Certificate Transparency, CT)，做法如下：

1. 本管理中心傳送符合 RFC 6962 所定義且尚未簽章之預簽憑證至數個憑證透明度日誌，待其個別回覆已簽憑證時間戳記。

2. 將已取得且數量符合規定之已簽憑證時間戳記封裝至預簽憑證的 X.509 v3 擴充欄位，並對該預簽憑證進行簽章與封裝，完成該憑證的簽發作業。

3. 前述作業所提之預簽憑證僅用於憑證透明度之「X.509 v3 擴充欄位」方法，其不可視為符合 RFC 5280 之憑證。

7.1.3 演算法物件識別碼

本管理中心使用之演算法物件識別碼(Object Identifier)如下。

類型	演算法	演算法物件識別碼
簽章	sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)}
	sha384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha384WithRSAEncryption(12)}
	sha512WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha512WithRSAEncryption(13)}
金鑰產製	rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) rsaEncryption(1)}

7.1.4 命名形式

憑證之主體與簽發者兩個欄位使用 X.500 唯一識別名稱，其欄位屬性型態係遵照 ITU-T X.509、RFC 5280 及憑證機構與瀏覽器論壇所發行之 Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates 或其最新版相關規定，憑證主體名稱欄位說明參考 3.1.5 節「命名獨特性」。

7.1.4.1 命名編碼

依據憑證機構與瀏覽器論壇發行之 Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates 第 7.1.4.1 節規定，本管理中心所簽發之用戶憑證，其簽發者唯一識別名稱欄位(Issuer Distinguished Name)編碼內容須與本管理中心本身憑證之主體唯一識別名稱欄位(Subject Distinguished Name)編碼形式完全相同。

7.1.4.2 用戶憑證之主體資訊

1. 用戶憑證主體名稱之通用名稱欄位屬性以及憑證主體別名擴充欄位僅註記已通過 3.2.2.2 節「網域名稱擁有者鑑別」之驗證的完整網域名稱。

2. 用戶憑證主體名稱若包含通用名稱欄位屬性時，該欄位屬性僅可註記憑證主體別名擴充欄位之其中一個完整網域名稱。

3. 用戶憑證主體之欄位屬性不得僅註記「.」、「-」及「 」(空白)等字元，或任何暗示該值不存在、不完整或不適用之說明。

4. 用戶憑證之憑證主體別名擴充欄位至少註記 1 個完整網域名稱，完整網域名稱之格式須滿足下述規定：

   - 符合 RFC 5280 規範之首選名稱語法(Preferred Name Syntax)，不可包含下底線符號「_」。
   - 符合憑證機構與瀏覽器論壇發行之 Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates 第 7.1.2.7.12 節之規定，該名稱由 P-Labels 與 NR-LDH Label 所組成。

5. 用戶憑證之憑證主體別名擴充欄位的關鍵性與格式於 7.1.2.2 節「用戶憑證」敘明。

6. 用戶憑證主體唯一識別名稱欄位之必要說明如下：

主體唯一識別名稱欄位	必要性
subject:commonName (OID 2.5.4.3)	可選
subject:organizationUnitName(OID2.5.4.11)	禁用
subject:givenName (OID 2.5.4.42)	禁用
subject:surname (OID 2.5.4.4)	禁用
subject:organizationName (OID 2.5.4.10)	必要
subject:streetAddress (OID 2.5.4.9)	可選
subject:postalCode(OID 2.5.4.17)	可選
subject:localityName (OID 2.5.4.7)或 subject:stateOrProvinceName (OID 2.5.4.8)	必須包含至少 1 項
subject:countryName(OID 2.5.4.6)	必要

7.1.4.3 本管理中心之主體資訊

本管理中心之憑證機構憑證主體唯一識別名稱包含 3 個屬性，分別為通用名稱(commonName)、組織名稱(organizationName)與國家代碼(countryName)，說明如下：

1. 通用名稱：可識別本管理中心之名稱，此名稱為此憑證的唯一識別碼，可作為與其他憑證區分之用。
2. 組織名稱：本管理中心所屬的正式組織名稱。
3. 國家代碼：本管理中心營業地點所在之國家，依 ISO 3166-1 國際標準之規範註記為「TW」。

7.1.5 命名限制

本管理中心簽發之憑證不採用命名限制(nameConstraints)。

7.1.6 憑證政策物件識別碼

憑證政策擴充欄位除憑證政策物件識別碼外，亦包含憑證機構與瀏覽器論壇定義之組織驗證型 TLS 憑證的憑證政策物件識別碼「2.23.140.1.2.2」。

7.1.7 政策限制擴充欄位之使用

本管理中心簽發之憑證不含政策限制擴充欄位(policyConstraints)。

7.1.8 政策限定元之語法及語意

本管理中心簽發之憑證不含政策限定元(policyQualifiers)。

7.1.9 關鍵憑證政策擴充欄位之語意處理

本管理中心簽發之用戶憑證，其關鍵憑證政策擴充欄位之語意依

ITU-T X.509、憑證機構與瀏覽器論壇所發行之 Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates 及 RFC 5280 規定辦理。

7.2 憑證廢止清冊格式剖繪

7.2.1 版本序號

本管理中心簽發遵照 RFC 5280 與 ITU-T X.509 v2 版本之憑證廢止清冊。

7.2.2 憑證廢止清冊與憑證廢止清冊條目之擴充欄位

1. 憑證廢止清冊擴充欄位(crlExtensions)與憑證廢止清冊條目擴充欄位(crlEntryExtensions)依照 ITU-T X.509、憑證機構與瀏覽器論壇所發行之 Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates 及 RFC 5280 或其最新版相關之規定。

2. 憑證廢止清冊擴充欄位與憑證廢止清冊條目擴充欄位內容如下所述。

(1) 憑證廢止清冊擴充欄位

擴充欄位名稱	必要性	關鍵性	內容
憑證機構金鑰識別碼	必要	FALSE	本管理中心之公開金鑰 SHA-1 雜湊值
憑證廢止清冊數目 (CRL Number)	必要	FALSE	憑證廢止清冊之序號
發行發布點 (Issuing Distribution Point)	可選	TRUE	此擴充欄位僅適用於部分憑證廢止清冊(Partitioned CRL)，用於註記此憑證廢止清冊之發布點、廢止資訊可涵蓋的範圍(包括僅限用戶憑證、僅限憑證機構憑證、僅限屬性憑證或僅限特

擴充欄位名稱	必要性	關鍵性	內容
			定廢止原因代碼)以及是否為間接憑證廢止清冊；其中，鑑於此憑證廢止清冊涵蓋範圍僅包含本管理中心簽發之憑證，故間接憑證廢止清冊說明欄位須設為 FALSE。

(2) 憑證廢止清冊條目擴充欄位

擴充欄位名稱	必要性	關鍵性	內容
憑證廢止清冊原因代碼 (Reason Code)	必要	FALSE	此擴充欄位用於標示本管理中心廢止憑證之原因代碼，可使用之原因代碼如下： ■ keyCompromise(1) ■ affiliationChanged(3) ■ superseded(4) ■ cessationOfOperation(5) ■ privilegeWithdrawn(9)

7.3 線上憑證狀態協定格式剖繪

1. 本管理中心提供符合 RFC 6960 及 RFC 5019 標準規範之線上憑證狀態協定查詢服務，並於憑證之憑證機構存取資訊擴充欄位中註明本管理中心線上憑證狀態協定查詢服務之網址。
2. 本管理中心可接受之線上憑證狀態協定查詢封包，應包括資訊如下：
   - 協定版本
   - 待查詢憑證識別碼(Target Certificate Identifier)
3. 本管理中心線上憑證狀態協定回應伺服器簽發之線上憑證狀態協定回應訊息至少包含線上憑證狀態協定回應訊息狀

態欄位，用於說明前述線上憑證狀態協定查詢封包之處理狀態；當狀態為成功時，線上憑證狀態協定回應訊息須再包含下述欄位：

欄位	說明
版本序號(Version)	v.1 (0x0)
線上憑證狀態協定回應伺服器 ID(Responder ID)	線上憑證狀態協定回應伺服器之主體名稱
產製時間(Produced Time)	回應訊息簽署時間
待查詢憑證識別碼(Target Certificate Identifier)	包括雜湊函數演算法、憑證簽發者名稱之雜湊值、憑證簽發者公開金鑰之雜湊值及待查詢憑證之憑證序號
憑證狀態碼(Certificate Status)	憑證狀態碼說明如下： ■ 0：表示憑證狀態有效。 ■ 1：表示憑證已被廢止。當此欄位註記憑證已被廢止時，尚需註記此憑證廢止之時間與廢止原因，廢止原因應與憑證廢止清冊所註記之原因代碼相符。 ■ 2：表示憑證狀態未知。
效期(thisUpdate/nextUpdate)	此回應訊息建議之效期區間，包括生效時間(thisUpdate)與下次更新時間
簽章演算法(Signature Algorithm)	回應訊息之簽章演算法，可為 sha256WithRSAEncryption
簽章(Signature)	線上憑證狀態協定回應伺服器之簽章
憑證(Certificates)	線上憑證狀態協定回應伺服器之憑證

7.3.1 版本序號

版本序號以 RFC 5019 及 RFC 6960 規定為依據。

7.3.2 線上憑證狀態協定擴充欄位

1. 線上憑證狀態協定擴充欄位依照憑證機構與瀏覽器論壇所發行之 Baseline Requirements for the Issuance and

Management of Publicly-Trusted TLS Server Certificates、RFC 5019 及 RFC 6960 之規定。

2. 線上憑證狀態協定回應訊息擴充欄位應包括線上憑證狀態協定回應伺服器之憑證機構金鑰識別碼。

3. 線上憑證狀態協定查詢封包有隨機數欄位時，線上憑證狀態協定回應訊息亦須包括相同之隨機數欄位。

4. 線上憑證狀態協定回應訊息中之 singleExtensions 不得包含憑證廢止清冊條目擴充欄位「原因代碼(reasonCode，其物件識別碼為 2.5.29.21)」。

7.3.3 線上憑證狀態協定服務運轉規範

本管理中心線上憑證狀態協定查詢服務運轉作業說明如下：

1. 至少可以處理與接受 HTTP GET 方法所傳送線上憑證狀態協定用戶端之線上憑證狀態協定查詢封包。

2. 線上憑證狀態協定回應伺服器使用短效期憑證，由本管理中心定期簽發與更新。

8 稽核方法

8.1 稽核頻率或評估事項

1. 本管理中心每年執行 1 次內部稽核。

2. 本管理中心每年接受 1 次外部稽核，且查核區間不可超過 12 個月。

3. 稽核採用之標準為 WebTrust Principles and Criteria for Certification Authorities 及 WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security。

8.2 稽核人員之身分及資格

1. 稽核方須經 WebTrust 認證標章管理單位授權可於我國執行 WebTrust Principles and Criteria for Certification Authorities 及 WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security 稽核標準之合格稽核業者。

2. 稽核人員應通過國際電腦稽核師(Certified Information Systems Auditor, CISA)認證或具同等資格。

3. 本管理中心於稽核時應對稽核人員進行身分識別。

8.3 稽核人員及被稽核方之關係

稽核人員應獨立於被稽核之憑證管理中心，為獨立且公正之第三方人員。

8.4 稽核之範圍

1. 本作業基準是否符合憑證政策及總管理中心憑證實務作業基準之規定。

2. 本管理中心及註冊中心是否遵照本作業基準運作。

3. 本管理中心依據憑證機構與瀏覽器論壇所發行最新 Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates 之規定，每季隨機抽樣至少 3%(不足 1 張則隨機抽樣 1 張)憑證進行審驗。

8.5 對於稽核結果之因應方式

1. 本管理中心對不符合規定之項目進行改善，並於完成後通知原稽核人員進行複核。

2. 依不符合情形之種類、嚴重性及修正所需時間，本管理中心得採取必要措施。

8.6 稽核結果公開之範圍

1. 除可能導致系統安全風險及依 9.3 節「業務資訊保密」規定外，本管理中心應於查核區間結束後 3 個月內將最近 1 次外部稽核報告與管理聲明書公布於儲存庫，若延遲公布，應提供合格稽核業者簽署之解釋函。

2. 稽核結果以 WebTrust Principles and Criteria for Certification Authorities 及 WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security 認證標章之

方式呈現於本管理中心網站首頁，點選認證標章後可閱覽外稽報告與管理聲明書。

3. 公開之稽核文件內容須符合各瀏覽器信賴根憑證計畫相關規定。

9 其他業務與法律事項

9.1 費用

暫不收費。

9.1.1 憑證簽發、展期費用

暫不收費。

9.1.2 憑證查詢費用

暫不收費。

9.1.3 憑證廢止、狀態查詢費用

暫不收費。

9.1.4 其他服務費用

暫不收費。

9.1.5 請求退費程序

不適用。

9.2 財務責任

本管理中心之營運由政府編列預算維持，未向保險公司投保，財務責任依政府法令規定辦理。

9.2.1 保險範圍

不適用。

9.2.2 其他資產

不予規定。

9.2.3 對終端個體之保險或保固責任

不適用。

9.3 業務資訊保密

9.3.1 機敏性資訊之範圍

1. 本管理中心營運之私密金鑰與通行碼。
2. 本管理中心金鑰分持之相關資料。
3. 未經同意公開之用戶資料。
4. 本管理中心產生或保管之可供稽核與追蹤之紀錄。
5. 稽核人員於稽核過程中產生之稽核紀錄與發現，不得被完整公開者。
6. 本管理中心列為不得公開之營運相關文件。
7. 其它經法令規定不得公開之資料。

9.3.2 非機敏性資訊之範圍

非 9.3.1 節「機敏性資訊之範圍」規定之資訊，原則皆屬非機敏性資訊。

9.3.3 保護機敏性資訊之責任

本管理中心依電子簽章法、WebTrust Principles and Criteria for

Certification Authorities 、 WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security、憑證機構與瀏覽器論壇所發行之 Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates 及個人資料保護法等規定，處理本管理中心之機敏性資訊。

9.4 個人資訊之隱私性

9.4.1 隱私保護計畫

1. 本管理中心於網站公告隱私權保護政策。

2. 本管理中心實施隱私衝擊分析與個資風險評鑑等措施。

9.4.2 隱私資料之種類

1. 憑證申請時記載之個人資訊。

2. 本管理中心運作所取得之個人資訊。

9.4.3 非隱私資料之種類

非 9.4.2 節「隱私資料之種類」規定之資訊，原則皆屬非隱私資料。

9.4.4 保護隱私資料之責任

依網站公告之隱私權保護政策、WebTrust Principles and Criteria for Certification Authorities 標準、WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security、憑證機構與瀏覽器論壇所發行之 Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates 以及個人資料

保護法等相關規定進行隱私資料保護。

9.4.5 使用隱私資訊之公告與同意

1. 隱私權保護政策公告於網站。

2. 使用個人隱私資訊須經用戶同意。

9.4.6 應司法或管理程序釋出資訊

司法機關或檢調單位如因調查或蒐集證據需要，須查詢機敏性資訊時，本管理中心依法辦理，不另通知用戶。

9.4.7 其他資訊釋出之情形

依相關規定法令辦理。

9.5 智慧財產權

除個人資料外，本管理中心產製之文件(含電子檔案)，其智慧財產權皆屬本管理中心所有，重製或散布須依網站公布之著作權聲明規定辦理。

9.6 職責與義務

9.6.1 本管理中心之職責與義務

1. 依憑證政策保證等級第 3 級規定與本作業基準運作。

2. 執行憑證申請之識別及鑑別程序。

3. 簽發、公布、廢止憑證。

4. 簽發與公布憑證廢止清冊。

5. 提供線上憑證狀態協定查詢服務。
6. 產製及管理本管理中心之私密金鑰。

9.6.2 註冊中心之職責與義務

1. 提供憑證申請服務。
2. 執行憑證申請之識別及鑑別程序。
3. 管理註冊中心之私密金鑰，且不得用於憑證註冊以外作業。

9.6.3 用戶之義務

1. 提供正確完整之資訊。
2. 遵守本作業基準相關規定。
3. 妥善管理與使用私密金鑰。
4. 私密金鑰遭冒用、破解或遺失時，應立即通知本管理中心廢止憑證，惟用戶仍應承擔異動前所有使用該憑證之法律責任。
5. 安全產製其私密金鑰並避免遭受破解。
6. 用戶應慎選安全之電腦環境與可信賴之應用系統，如因電腦環境或應用系統本身因素，導致信賴憑證者權益受損時，用戶應自行承擔責任。
7. 本管理中心如因故無法正常運作時，用戶應儘速尋求其他途徑完成與他人應為之法律行為，不得以本管理中心無法正常運作，作為抗辯他人之事由。

9.6.4 信賴憑證者之義務

1. 遵守本作業基準相關規定。
2. 正確檢驗憑證數位簽章、有效性及金鑰用途。
3. 信賴憑證者應確保憑證使用環境之安全，如非可歸責於本管理中心之事由導致權益受損時，應自行承擔責任。
4. 本管理中心如因故無法正常運作時，信賴憑證者應儘速尋求其他途徑完成與他人應為之法律行為，不得以本管理中心無法正常運作，作為抗辯他人之事由。

9.6.5 其他參與者之義務

本管理中心由數位部依政府採購法規定辦理委外服務，承商依契約規定辦理。

9.7 免責聲明

用戶或信賴憑證者如未依本作業基準相關規定申請、管理及使用憑證，產生因不可抗拒與其他非可歸責於本管理中心之事由，而造成之損害，由用戶或信賴憑證者自行負責，本管理中心不負任何法律責任。

9.8 責任限制

1. 本管理中心如因系統維護、轉換及擴充等事由，須暫停部分憑證服務時，得於 3 日前公告於儲存庫。用戶或信賴憑證者不得以此作為要求本管理中心損害賠償之理由。
2. 本管理中心遵照憑證機構與瀏覽器論壇所發行的 Baseline Requirements for the Issuance and Management of Publicly-

Trusted TLS Server Certificates 正式版本之規範簽發與管理 TLS 憑證。

3. 用戶如有廢止憑證事由時，應依 4.9 節「憑證暫時停用及廢止」規定提出憑證廢止申請。廢止憑證申請核定後，本管理中心將於 1 個工作天內完成憑證廢止作業、簽發憑證廢止清冊與公告於儲存庫。

4. 用戶於憑證廢止狀態未被公布前，應採取適當之行動，以減少對信賴憑證者之影響，並承擔所有因使用該憑證所引發之責任。

9.9 賠償

9.9.1 本管理中心之賠償責任

本管理中心如未依本作業基準及相關法令規定導致利害關係人權益損害時，由本管理中心負賠償責任；用戶及信賴憑證者得依相關法律規定請求損害賠償。

9.9.2 註冊中心之賠償責任

註冊中心如未依本作業基準及相關法令規定導致利害關係人權益損害時，由註冊中心負賠償責任；用戶及信賴憑證者得依相關法律規定請求損害賠償。

9.10 有效期限與終止

9.10.1 有效期限

本作業基準由總管理中心核定並公告後生效，直至被新版本取代前仍然有效。

9.10.2 終止

本作業基準之終止須由數位部決議，並經總管理中心核定。

9.10.3 終止與存續之效力

1. 本作業基準效力終止之說明，應公告於本管理中心儲存庫。

2. 本作業基準終止後，其效力須維持至所簽發之最後一張憑證失效為止。

9.11 對參與者之個別通知及溝通

本管理中心、註冊中心、用戶及信賴憑證者間得採網站公告、儲存庫、公文、書信、電話、傳真、電子郵件等方式建立通知與聯絡管道。

9.12 修訂

本管理中心每年檢視憑證機構與瀏覽器論壇所發行的 Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates 正式版本所頒布之條款，評估本作業基準是否需要修訂，並以版本編號異動表示已完成檢視或進行更新，相關紀錄記載於版本修訂歷程。倘若本作業基準在 TLS 憑證簽發管理之敘述與該論壇規範有牴觸情形，將優先遵照憑證機構與瀏覽器論壇所頒布之條款進行本作業基準之修訂，並經總管理中心核定後實施。

9.12.1 修訂程序

本作業基準之修訂經數位部審查，並經總管理中心核定後公告。

9.12.2 通知機制與期限

9.12.2.1 通知機制

所有變更項目將公告於儲存庫。

9.12.2.2 變更項目

依變更項目對用戶或信賴憑證者影響程度之不同，經數位部審查後公告草案於儲存庫，其通知期限如下：

1. 影響程度大者，至少於儲存庫公告 15 個日曆天，始得提交總管理中心進行審查。
2. 影響程度小者，至少於儲存庫公告 7 個日曆天，始得提交總管理中心進行審查。

本作業基準如重新排版、辭彙變更或錯別字修訂時，則不另行公告。

9.12.2.3 意見反應期限

用戶或信賴憑證者對變更項目有意見時，其反應期限如下：

1. 影響程度大者，反應期限為自公告日起 15 個日曆天內。
2. 影響程度小者，反應期限為自公告日起 7 個日曆天內。

9.12.2.4 處理意見機制

1. 對變更項目有意見者於回覆期限截止前，將意見以電子郵件方式提供給本管理中心。
2. 本管理中心進行評估後回覆反應者。

9.12.2.5 最後公告期限

本作業基準之修訂，於總管理中心核定後 10 個日曆天內公告。

9.12.3 須修改憑證政策物件識別碼之事由

憑證政策之修訂不影響憑證政策所聲明之憑證使用目的與保證等級時，憑證政策物件識別碼不需修改；然其憑證政策物件識別碼變更時，本作業基準應作相對應之變更。

9.13 紛爭之處理程序

用戶與本管理中心發生爭議時，雙方應本誠信原則先進行協商，由本管理中心就本作業基準相關條文提出解釋。

9.14 管轄法律

依我國相關法令規定辦理。

9.15 適用法律

依我國相關法令規定辦理。

9.16 雜項條款

9.16.1 完整協議

本作業基準所約定者，構成主要成員間最終且完整之約定，主要成員包括本管理中心、註冊中心、用戶及信賴憑證者。主要成員間就同一事項縱使以口頭或書面進行其他表示，最終仍應以本作業基準之約定為準。

9.16.2 轉讓

本作業基準所敘述之主要成員間權利或責任，不得於未通知本管理中心下以任何形式轉讓予其他方。

9.16.3 可分割性

1. 本作業基準之任一章節不適用而須修正時，其他章節仍屬有效。
2. 本管理中心遵照憑證機構與瀏覽器論壇所發行的 Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates 正式版本，惟其相關規定與我國相關法律或法規產生衝突時，本管理中心得小幅度調整相關作法以滿足法律或法規之要求，並將變更調整之部分於簽發新憑證前通知瀏覽器論壇；若發生以下情況時，應刪除並修訂原憑證實務作業基準所調整之內容，並經數位部審查通過與總管理中心核定，上述作業須於 90 天內完成。
   (1) 與憑證機構與瀏覽器論壇所發行的 Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates 相關規定產生衝突之我國法律或法規已修訂或刪除。
   (2) 憑證機構與瀏覽器論壇已修訂 Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates 規定，並已相容於我國法律或法規。

9.16.4 契約履行

1. 用戶或憑證信賴者違反本作業基準相關規定，致本管理中心遭受損害，如可歸責於用戶或憑證信賴者之故意或過失時，本管理中心除得請求損害賠償外，亦得向可歸責之一方請求支付處理該爭議或訴訟之律師費用。
2. 本管理中心未向違反本作業基準相關規定者主張權利，不代表本管理中心有拋棄權利主張之意思。

9.16.5 不可抗力

因不可抗拒與其他非可歸責於本管理中心所導致之損害事件，本管理中心不負任何法律責任。

9.17 其他條款

不予規定。

附錄 1：名詞解釋

◆ A

- **啟動資料(Activation Data)**：存取密碼模組時(例如用以開啟私密金鑰以進行簽章或解密)，除金鑰外所需之隱密資料。

- **申請者(Applicant)**：向憑證機構申請憑證，而尚未完成憑證作業程序之用戶。

- **歸檔(Archive)**：實體上(與主要資料存放處)分隔之長期資料儲存處，可用以支援稽核服務、可用性服務或完整性服務等用途。

- **保證(Assurance)**：據以信賴該個體已符合特定安全要件之基礎。

- **保證等級(Assurance Level)**：具相對性保證層級中之某一級數。

- **稽核(Audit)**：評估系統控制是否恰當，以確保符合既定之政策與營運程序，並對現有之控制、政策與程序等，建議必要之改善所進行之獨立檢閱與調查。

- **稽核紀錄(Audit Log)**：依發生時間順序之系統活動紀錄，可用以重建或調查事件發生之順序與某個事件中之變化。

- **鑑別(Authenticate)**：驗證某個聲稱的身分是合法且屬於提出此聲稱者的程序。

- **鑑別程序(Authentication)**

- 建立使用者或資訊系統身分信賴程度的程序。
- 用以建立資料傳送、訊息、來源者之安全措施，或是驗證個人接收特定種類資訊權限之方法。

◆ C

- **憑證(Certificate)**
  - 指載有簽章驗證資料，用以確認簽署人身分、資格之電子形式證明。
  - 資訊之數位呈現內容包括：
    - ✓ 簽發之憑證機構。
    - ✓ 用戶之名稱或身分。
    - ✓ 用戶之公開金鑰。
    - ✓ 憑證之有效期間。
    - ✓ 憑證機構數位簽章。

- **憑證政策(Certificate Policy, CP)**：係為透過憑證管理執行之電子交易所訂定具專門格式之管理政策。憑證政策中包括與數位憑證相關之生成、產製、傳送、稽核、被破解後復原及其管理等各項議題。憑證政策與其相關技術可提供特定應用所需之安全服務。

- **憑證問題報告(Certificate Problem Report)**：問題發現者發現疑似金鑰遭破解、憑證被誤用、或憑證遭偽造、破解、濫用或不當使用之投訴。

- **憑證廢止清冊(Certificate Revocation List, CRL)**
  - 憑證機構以數位方式簽章，並可供信賴憑證者使用之已廢止憑證表列。
  - 由憑證機構維護之清單，清單中記載由此憑證機構所簽發

且於到期日前被廢止之憑證。

- **憑證機構(Certification Authority, CA)**
  - 簽發憑證之機關。
  - 為使用者所信任之權威機構，其業務為簽發並管理 X.509 格式之憑證與憑證廢止清冊。

- **授權憑證機構簽發憑證(Certification Authority Authorization , CAA)**：根據 RFC 6844 規定，授權憑證機構簽發憑證網域名稱系統資源紀錄(The Certification Authority Authorization DNS Resource Record)允許網域名稱系統之網域名擁有者指定憑證機構(一個或多個)取得授權幫該網域簽發憑證。發布授權憑證機構簽發憑證網域名稱系統資源紀錄允許公眾信賴之憑證機構實施額外之控制降低非預期之憑證誤發風險。

- **憑證實務作業基準(Certification Practice Statement, CPS)**
  - 由憑證機構對外公告，用以陳述憑證機構據以簽發憑證與處理其他認證業務之作業準則。
  - 宣告某憑證機構對憑證之作業程序(包括簽發、停用、廢止、展期及存取等)符合特定需求之聲明(需求敘明於憑證政策或其他服務契約中)。

- **憑證透明度(Certificate Transparency, CT)**：為一個公開監控與稽核網際網路上所有憑證之開放性架構(現以 TLS 憑證為優先目標)，透過公開憑證的簽發與存在等資訊，供網域所有者、憑證機構及網域使用者判斷憑證是否被錯誤或惡意簽發；換言之，其目的係提供一個可用於監控 TLS 憑證機制與審核特定 TLS 憑證的公開監控與資訊公開的環境，以遏止憑證相關威脅。憑證透明化機制，主要由憑證透明度日

誌、憑證監控者及憑證稽核者等要素所組成。

- **國際電腦稽核師(Certified Information Systems Auditor, CISA)**：國際電腦稽核協會(Information Systems Audit and Control Association, ISACA)於 1978 年推出之稽核認證，其以資訊系統的觀點檢視營運流程，為現今電腦稽核、控管、確認與安全等專業領域之資格標準。需通過國際電腦稽核協會之考試並滿足維持證照有效性之要求始可獲證。

- **資訊技術安全評估共同準則(Common Criteria for Information Technology Security Evaluation)**：簡稱為「共同準則」(Common Criteria, CC)，為美國、英國、德國、法國及加拿大等國家所制訂之資安產品評估及驗證規範，於 1999 年 8 月正式成為 ISO 國際標準(ISO/IEC 15408)，其經過標準評估的產品可獲得「評估保證等級」(Evaluation Assurance Level, EAL)，用於說明該產品安全規範檢測之結果與界定之安全等級，可分為 7 個安全評估等級，最低等級為 EAL 1，最高等級為 EAL 7，為現今多數國家認定之經第三方實驗室驗證、最高層級的 IT 產品安全性認證，可作為資訊產品使用者採購及使用的依據。

- **破解(Compromise)**：資訊洩漏予未經授權人士或違反資訊安全政策，造成物件未經授權蓄意、非蓄意洩漏、修改、毀壞或遺失。

- **交互憑證(Cross-Certificate)**：在兩個憑證機構之間建立信賴關係的一種憑證，屬於一種憑證機構憑證，而非用戶憑證。

- **密碼模組(Cryptographic Module)**：一組硬體、軟體、韌體或前述之組合，用以執行密碼之邏輯或程序(包含密碼演算

法)，且被包含於此模組之密碼邊界內。

- **密碼學安全偽亂數生成器(Cryptographically Secure Pseudorandom Number Generator, CSPRNG)**：用於加密系統之亂數生成器。

◆ **D**

- **數位簽章(Digital Signature)**：將電子文件以數學演算法或其他方式運算為一定長度之數位資料，以簽署人之私密金鑰對其加密，形成電子簽章，並得以公開金鑰加以驗證者。

- **憑證效期(Duration)**：憑證欄位，由有效期限起始時間與有效期限截止時間 2 個子欄位所組成。

◆ **E**

- **終端個體(End Entity, EE)**：在 ePKI 中包括以下兩類個體：
  - 負責保管與應用憑證的私密金鑰擁有者。
  - 信賴憑證機構所簽發憑證的第三者(不是私密金鑰擁有者，也不是憑證機構)，亦即終端個體為用戶與信賴憑證者，包括人員、組織、客戶、裝置或站台。

- **中華電信憑證總管理中心(ePKI Root Certification Authority)**：ePKI 之根憑證機構，在此階層式公開架構中最頂層之憑證機構，其公開金鑰為信賴之起源。

◆ **F**

- **聯邦資訊處理標準(Federal Information Processing Standard, FIPS)**：為美國聯邦政府制定除軍事機構外，所有

政府機構與政府承包商所引用之資訊處理標準。其中密碼模組安全需求標準為 FIPS 第 140 號標準(簡稱 FIPS 140)，FIPS 140-2 將密碼模組區分為 11 類安全需求，每一個安全需求類別再分成 4 個安全等級。

- **完整網域名稱(Fully Qualified Domain Name, FQDN)**：一種用於指定電腦在網域階層中確切位置的明確網域名稱，由主機名稱(服務名稱)與網域名稱組成，且主機名稱須放置於該名稱之起始位置。其參考範例如下：
  - 「ourserver.ourdomain.com.tw」：ourserver 是主機名稱，ourdomain.com.tw 是網域名稱，其中 ourdomain 是第 3 層網域名稱，com 則是次級網域名稱，tw 則是國碼頂級網域名稱。
  - 「www.ourdomain.com」：www 是主機名稱，ourdomain 是次級網域名稱，com 則是通用頂級網域名稱。

◆ H

- **HiPKI 中華電信憑證總管理中心(HiPKI Root Certification Authority)**：HiPKI 之根憑證機構，為中華電信新一代的 RootCA，在此階層式公開架構中最頂層之憑證機構，其公開金鑰為信賴之起源，未來將取代 ePKI RootCA 作為信賴起源之根憑證。

◆ **I**

- **資訊技術安全評估準則(Information Technology Security Evaluation Criteria, ITSEC)**：於 1991 年由英、法、德、荷等歐洲國家提出，為歐洲安全評估準則，其定義了 7 種安全評估等級，分別為 E0 至 E6。與可信賴電腦系統安全評估準

則不同，其僅說明技術安全之要求，將機密性作為安全增強功能，同時，強調對資訊安全之機密性、完整性及可用性的重要性。

- **網際網路工程任務小組(Internet Engineering Task Force, IETF)**：負責網際網路標準之開發與推動，其願景係藉由產製高品質之技術文件影響人類設計、使用與管理網際網路，使得網際網路運作更順暢。(官方網站：https://www.ietf.org)

- **簽發憑證機構(Issuing CA)**：對一張憑證而言，簽發該憑證之憑證機構即稱為該憑證之簽發憑證機構。

◆ **K**

- **金鑰託管(Key Escrow)**：依用戶須遵守之託管協議(或類似契約)所規定相關資訊，將用戶之私密金鑰進行存放，此託管協議條款要求一個或以上之代理機構，基於有益於用戶、雇主或另一方之前提下，依協議規定擁有用戶之金鑰。

- **金鑰對(Key Pair)**：兩把數學上有相關性之金鑰，其特性如下：
  - 其中一把金鑰用以進行訊息加密，而此加密訊息僅有另一把可解密。
  - 從其中一把金鑰要推出另一把金鑰(從計算之角度而言)是不可行。

◆ **O**

- **物件識別碼(Object Identifier, OID)**
  - 一種以字母或數字組成之唯一識別碼，該識別碼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。

- 向國際標準機構(International Organization for Standardization)註冊之特別形式數碼，當提及某物件或物件類別時，可以引用此唯一之數碼進行辨識。例如於公開金鑰基礎架構中以此數碼指明使用之憑證政策與使用之密碼演算法。

- **線上憑證狀態協定(Online Certificate Status Protocol, OCSP)**：一種線上憑證檢查協定，使信賴憑證者應用軟體可決定某張憑證之狀態(例如已廢止、有效等)。

- **線上憑證狀態協定回應伺服器(Online Certificate Status Protocol Responder, OCSP Responder)**：由憑證管理中心授權維運之線上伺服器，其連接至儲存庫，以處理憑證狀態查詢請求。

- **線上憑證狀態協定裝訂(OCSP Stapling)**

  - 一種 TLS 憑證狀態請求擴充欄位，可替代線上憑證狀態協定成為另一種檢查 X.509 憑證狀態的方法。其運作機制如下：

    ✓ 網站向線上憑證狀態協定回應伺服器取得具有「時間限制」之線上憑證狀態協定回應訊息，並暫存之。
    ✓ 於每次 TLS 連線初始過程中，網站將此暫存之線上憑證狀態協定回應訊息傳送給用戶(通常為瀏覽器)，用戶僅需驗證該回應訊息之有效性，無需向憑證機構發送線上憑證狀態協定查詢封包。
  - 此機制可透過網站轉發線上憑證狀態協定回應伺服器定期簽發之 TLS 憑證有效性訊息，減少用戶向憑證機構查詢

TLS 憑證狀態之頻率，減輕憑證機構之負擔。

- **組織驗證(Organization Validation, OV)**：TLS 憑證核發過程中，除了識別及鑑別用戶之網域名稱控制權外，並且依照憑證的保證等級識別及鑑別用戶之組織或個人身分。故連結安裝組織驗證型 TLS 憑證之網站，可提供 TLS 加密通道，知道該網站之擁有者是誰，並確保傳遞資料之完整性。

◆ P

- **私密金鑰(Private Key)**：
  - 簽章金鑰對中用以產生數位簽章之金鑰。
  - 加解密金鑰對中用以對機敏性資訊解密之金鑰。

- **公開金鑰(Public Key)**：
  - 簽章金鑰對中用以驗證數位簽章有效之金鑰。
  - 加解密金鑰對中用以對機敏性資訊加密之金鑰。

- **公開金鑰基礎建設(Public Key Infrastructure, PKI)**：由法律、政策、規範、人員、設備、設施、技術、流程、稽核及服務之集合，在廣泛尺度上發展與管理非對稱式密碼學及憑證。

◆ Q

- **合格稽員(Qualified Auditor)**：符合憑證機構與瀏覽器論壇所發行之 Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates 第 8.2 節規定之稽核資格要求，且與受稽方獨立之的會計師事務所、法人或個人。

◆ **R**

- **註冊中心(Registration Authority, RA)**
  - 負責確認憑證申請人之身分或其他屬性，惟不簽發憑證亦不管理憑證。註冊中心是否需為其行為負責及其應負責任之範圍，依所適用之憑證政策或協議訂之。
  - 負責對憑證主體做身分識別及鑑別，惟不做憑證簽發。

- **金鑰更換(Re-key a Certificate)**：憑證金鑰更換指簽發一張與舊憑證具有相同特徵與保證等級之新憑證，新憑證除具有全新、不同之公開金鑰(對應新且不同之私密金鑰)及不同序號外，亦可被指定不同之有效期限。

- **信賴憑證者(Relying Party)**
  - 信賴所收受之憑證與可用憑證中所載之公開金鑰加以驗證之數位簽章者，或信賴憑證中所命名主體之身分(或其他屬性) 與憑證所載公開金鑰之對應關係者。
  - 個人或機構收到包含憑證與數位簽章之資訊，且可能信賴這些資訊(此數位簽章可藉由憑證上所列之公開金鑰做驗證)。

- **憑證展期(Renew a Certificate)**：指簽發一張與舊憑證具有相同憑證主體名稱、金鑰及相關資訊之新憑證，使憑證之有效期限予以展延，並付予一個新序號。

- **儲存庫(Repository)**
  - 用以儲存與檢索憑證或其他憑證相關資訊之可信賴系統(Trustworthy System)。
  - 包含憑證政策、憑證實務作業基準及憑證相關資訊之資料庫。

- **憑證廢止(Revoke a Certificate)**：在憑證之有效期間內，提前終止憑證之運作。

- **根憑證機構(Root Certification Authority, Root CA)**：公開金鑰基礎建設中最頂層的憑證機構，除了簽發下屬 CA 憑證與自簽憑證外，其自簽憑證由應用軟體供應商負責散布。亦可稱為憑證總管理中心或最頂層憑證機構。

◆ **S**

- **自簽憑證(Self-Signed Certificate)**：指憑證的簽發者名稱與憑證主體的名稱相同的一種憑證。亦即使用同一對金鑰對的私密金鑰針對其成配對關係的公開金鑰與其他資訊所簽發的憑證。一個公開金鑰基礎建設內的自簽憑證，可做為憑證路徑信賴的起源，其簽發對象為總管理中心本身，內含總管理中心的公開金鑰，且憑證簽發者名稱與憑證主體名稱相同，可供信賴憑證者用於驗證總管理中心簽發之自發憑證、下屬憑證機構憑證、交互憑證以及憑證廢止清冊的數位簽章。

- **下屬憑證機構(Subordinate Certification Authority)**：階層架構之公開金鑰基礎建設中，憑證由另一個憑證機構所簽發，且其活動受限於此另一憑證機構之憑證機構。

- **用戶(Subscriber)**
  - 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。
  - 具下列特性之個體，包括(但不限於)個人、機構或網路裝置：
    - ✓ 簽發憑證上所敘明之主體。
    - ✓ 擁有與憑證上所列公開金鑰對應之私密金鑰。

✓ 本身不簽發憑證予其他方。

- **安全插座層(Secure Sockets Layer, SSL)**：由網景公司(Netscape)所設計，主要用於全球資訊網(Web)之安全通訊協定，其可於傳輸層進行網路通信之加密，確保傳送之資料完整性，並可對伺服器端與用戶端進行身分驗證。其應用獨立於應用層協定，故應用層通訊前，即可透過此安全通訊協定完成加密演算、通信密鑰之協商及伺服器認證作業。

◆ **T**

- **傳輸層安全(Transport Layer Security, TLS)**：為一種安全通訊協定，1999 年網際網路工程任務小組將 SSL 進行標準化，公告第 1 版 TLS 標準(即為 RFC 2246)，隨後陸續公布 RFC 4346、RFC 5246、RFC 6176 與 RFC 8446 等更新版本，分別說明 TLS 1.1、TLS 1.2 與 TLS 1.3 版。
- **可信賴電腦系統安全評估準則(Trusted Computer System Evaluation Criteria,TCSEC)**：為電腦系統安全評估的第一個正式標準，於 1970 年由美國國防科學委員會提出，1985 年由美國國防部公布，其將電腦系統之安全劃分為 4 個等級與 7 種安全等級，主要著重於作業系統的安全性，非強調系統之整體性。
- **可信賴系統(Trustworthy System)**：具有下列性質之電腦硬體、軟體與程序：
  - 對於入侵與誤用有相當之保護功能。
  - 提供合理之可用性、可靠度及正確操作。
  - 適當地執行預定功能。
  - 與一般為人所接受之安全程序一致。

◆ **Z**

- **零值化(Zeroization)**：清除電子式儲存資料之方法，藉由改變資料儲存，以防止資料被復原。

附錄 2：英文名詞縮寫

縮寫	全稱
AIA	Authority Info Access
CA	Certification Authority
CAA	Certification Authority Authorization
CC	Common Criteria for Information Technology Security Evaluation
CISA	Certified Information Systems Auditor
CP	Certificate Policy
CP OID	Certificate Policy Object Identifier
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSPRNG	Cryptographically Secure Pseudorandom Number Generator
DN	Distinguished Name
DNS	Domain Name System
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
IETF	Internet Engineering Task Force
ITSEC	Information Technology Security Evaluation Criteria
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OV	Organization Validation
PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standard

縮寫	全稱
PKI	Public Key Infrastructure
RA	Registration Authority
RFC	Request for Comments
SSL	Security Sockets Layer
TCSEC	Trusted Computer System Evaluation Criteria
TLS	Transport Layer Security

附錄 3：BRs-Section 1.2.1 Revisions

本作業基準所檢視之憑證機構與瀏覽器論壇之 Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates 版本為 2.1.7。

Ver.	Ballot	Description	Adopted	Effective*	Implementation
1.0.0	62	Version 1.0 of the Baseline Requirements Adopted	22-Nov-11	01-Jul-12	—
1.0.1	71	Revised Auditor Qualifications	08-May-12	01-Jan-13	Compliant
1.0.2	75	Non-critical Name Constraints allowed as exception to RFC 5280	08-Jun-12	08-Jun-12	Compliant
1.0.3	78	Revised Domain/IP Address Validation, High Risk Requests, and Data Sources	22-Jun-12	22-Jun-12	Compliant
1.0.4	80	OCSP responses for non-issued certificates	02-Aug-12	01-Feb-13 01-Aug-13	Completed
--	83	Network and Certificate System Security Requirements adopted	03-Aug-13	01-Jan-13	Compliant
1.0.5	88	User-assigned country code of XX allowed	12-Sep-12	12-Sep-12	Compliant
1.1.0	--	Published as Version 1.1 with no changes from 1.0.5	14-Sep-12	14-Sep-12	—
1.1.1	93	Reasons for Revocation and Public Key Parameter checking	07-Nov-12	07-Nov-12 01-Jan-13	Compliant
1.1.2	96	Wildcard certificates and new gTLDs	20-Feb-13	20-Feb-13 01-Sep-13	Compliant
1.1.3	97	Prevention of Unknown Certificate Contents	21-Feb-13	21-Feb-13	Compliant
1.1.4	99	Add DSA Keys (BR v.1.1.4)	3-May-2013	3-May-2013	Compliant
1.1.5	102	Revision to subject domainComponent language in section 9.2.3	31-May-2013	31-May-2013	Compliant
1.1.6	105	Technical Constraints for Subordinate Certificate Authorities	29-July-2013	29-July-2013	Compliant
1.1.7	112	Replace Definition of “Internal Server Name” with “Internal Name”	3-April-2014	3-April-2014	Compliant
1.1.8	120	Affiliate Authority to Verify Domain	5-June-2014	5-June-2014	Compliant

1.1.9	129	Clarification of PSL mentioned in Section 11.1.3	4-Aug-2014	4-Aug-2014	Compliant
1.2.0	125	CAA Records	14-Oct-2014	15-Apr-2015	Compliant
1.2.1	118	SHA-1 Sunset	16-Oct-2014	16-Jan-2015 1-Jan-2016 1-Jan-2017	Compliant
1.2.2	134	Application of RFC 5280 to Pre-certificates	16-Oct-2014	16-Oct-2014	Compliant
1.2.3	135	ETSI Auditor Qualifications	16-Oct-2014	16-Oct-2014	—
1.2.4	144	Validation Rules for .onion Names	18-Feb-2015	18-Feb-2015	Compliant
1.2.5	148	Issuer Field Correction	2-April-2015	2-April-2015	Compliant
1.3.0	146	Convert Baseline Requirements to RFC 3647 Framework	16-Apr-2015	16-Apr-2015	—
1.3.1	151	Addition of Optional OIDs for Indicating Level of Validation	28-Sep-2015	28-Sep-2015	Compliant
1.3.2	156	Amend Sections 1 and 2 of Baseline Requirements	3-Dec-2015	3-Dec-2016	Compliant
1.3.3	160	Amend Section 4 of Baseline Requirements	4-Feb-2016	4-Feb-2016	Compliant
1.3.4	162	Sunset of Exceptions	15-Mar-2016	15-Mar-2016	Compliant
1.3.5	168	Baseline Requirements Corrections (Revised)	10-May-2016	10-May-2016	Compliant
1.3.6	171	Updating ETSI Standards in CABF documents	1-July-2016	1-July-2016	—
1.3.7	164	Certificate Serial Number Entropy	8-July-2016	30-Sep-2016	Compliant
1.3.8	169	Revised Validation Requirements	5-Aug-2016	1-Mar-2017	Compliant
1.3.9	174	Reform of Requirements Relating to Conflicts with Local Law	29-Aug-2016	27-Nov-2016	Compliant
1.4.0	173	Removal of requirement to cease use of public key due to incorrect info	28-July-2016	11-Sep-2016	Compliant
1.4.1	175	Addition of givenName and surname	7-Sept-2016	7-Sept-2016	Compliant
1.4.2	181	Removal of some validation methods listed in section 3.2.2.4	7-Jan-2017	7-Jan-2017	Compliant
1.4.3	187	Make CAA Checking Mandatory	8-Mar-2017	8-Sep-2017	Compliant
1.4.4	193	825-day Certificate Lifetimes	17-Mar-2017	1-Mar-2018	Compliant
1.4.5	189	Amend Section 6.1.7 of Baseline Requirements	14-Apr-2017	14-May-2017	Compliant
1.4.6	195	CAA Fixup	17-Apr-2017	18-May-2017	Compliant

1.4.7	196	Define “Audit Period”	17-Apr-2017	18-May-2017	—
1.4.8	199	Require commonName in Root and Intermediate Certificates 9	9-May-2017	8-June-2017	Compliant
1.4.9	204	Forbid DTPs from doing Domain/IP Ownership	11-July-2017	11-Aug-2017	Compliant
1.5.0	212	Canonicalise formal name of the Baseline Requirements	1-Sept-2017	1-Oct-2017	Compliant
1.5.1	197	Effective Date of Ballot 193 Provisions	1-May-2017	2-June-2017	Compliant
1.5.2	190	Add Validation Methods with Minor Corrections	19-Sept-2017	19-Oct-2017	Compliant
1.5.3	214	CAA Discovery CNAME Errata	27-Sept-2017	27-Oct-2017	Compliant
1.5.4	215	Fix Ballot 190 Errata	4-Oct-2017	5-Nov-2017	Compliant
1.5.5	217	Sunset RFC 2527	21-Dec-2017	9-Mar-2018	Compliant
1.5.6	218	Remove validation methods #1 and #5	5-Feb-2018	9-Mar-2018	Compliant
1.5.7	220	Minor Cleanups (Spring 2018)	30-Mar-2018	29-Apr-2018	Compliant
1.5.8	219	Clarify handling of CAA Record Sets with no "issue"/"issuewild" property tag	10-Apr-2018	10-May-2018	Compliant
1.5.9	223	Update BR Section 8.4 for CA audit criteria	15-May-2018	14-June-2018	Compliant
1.6.0	224	WhoIs and RDAP	22-May-2018	22-June-2018	Compliant
1.6.1	SC6	Revocation Timeline Extension	14-Sep-2018	14-Oct-2018	Compliant
1.6.2	SC12	Sunset of Underscores in dNSNames	9-Nov-2018	10-Dec-2018	Compliant
1.6.3	SC13	CAA Contact Property and Associated E-mail Validation Methods	25-Dec-2018	1-Feb-2019	Compliant
1.6.4	SC14	Updated Phone Validation Methods	31-Jan-20	16-Mar-2019	Compliant
	SC15	Remove Validation Method Number 9	5-Feb-2019		
	SC7	Update IP Address Validation Methods	8-Feb-2019		
1.6.5	SC16	Other Subject Attributes	15-Mar-2019	16-April-2019	Compliant
1.6.6	SC19	Phone Contact with DNS CAA Phone Contact v2	20-May-2019	9-Sep-2019	Compliant
1.6.7	SC23	Precertificates	14-Nov-2019	19-Dec-2019	Compliant
	SC24	Fall Cleanup v2	12-Nov-2019		
1.6.8	SC25	Define New HTTP Domain Validation Methods v2	31-Jan-2020	3-Mar-2020	Compliant
1.6.9	SC27	Version 3 Onion Certificates	19-Feb-2020	27-Mar-2020	Compliant
1.7.0	SC29	Pandoc-Friendly Markdown	20-Mar-2020	4-May-2020	Compliant

		Formatting Changes			
1.7.1	SC30	Disclosure of Registration / Incorporating Agency	13-Jul-2020	20-Aug-2020	Compliant
	SC31	Browser Alignment	16-Jul-2020	20-Aug-2020	
1.7.2	SC33	TLS Using ALPN Method	14-Aug-2020	22-Sept-2020	Compliant
1.7.3	SC28	Logging and Log Retention	10-Sep-2020	19-Oct-2020	Compliant
	SC35	Cleanups and Clarifications	9-Sep-2020		
1.7.4	SC41	Reformat the BRs, EVGs, and NCSSRs	24-Feb-2021	5-Apr-2021	Compliant
1.7.5	SC42	398-day Re-use Period	22-Apr-2021	2-Jun-2021	Compliant
1.7.6	SC44	Clarify Acceptable Status Codes	30-Apr-2021	3-Jun-2021	Compliant
1.7.7	SC46	Sunset the CAA Exception for DNS Operator	2-Jun-2021	12-Jul-2021	Compliant
1.7.8	SC45	Wildcard Domain Validation	2-Jun-2021	13-Jul-2021	Compliant
1.7.9	SC47	Sunset subject: organizationalUnitName	30-Jun-2021	16-Aug-2021	Compliant
1.8.0	SC48	Domain Name and IP Address Encoding	22-Jul-2021	25-Aug-2021	Compliant
1.8.1	SC50	Remove the requirements of 4.1.1	22-Nov-2021	23-Dec-2021	Compliant
1.8.2	SC53	Sunset for SHA-1 OCSP Signing	26-Jan-2022	4-Mar-2022	Compliant
1.8.3	SC51	Reduce and Clarify Log and Records Archival Retention Requirements	01-Mar-2021	15-Apr-2022	Compliant
1.8.4	SC54	Onion Cleanup	24-Mar-2022	23-Apr-2022	Compliant
1.8.5	SC56	2022 Cleanup	25-Oct-2022	30-Nov-2022	Compliant
1.8.6	SC58	Require distributionPoint in sharded CRLs	7-Nov-2022	11-Dec-2022	Compliant
1.8.7	SC61	New CRL entries must have a Revocation Reason Code	1-Apr-2023	15-Jul-2023	Compliant
2.0.0	SC62	Certificate Profiles Update	22-Apr-2023	15-Sep-2023	Compliant
2.0.1	SC63	Make OCSP optional, require CRLs, and incentivize automation	17-Aug-2023	15-Mar-2024	Compliant
2.0.2	SC66	2023 Cleanup	23-Nov-2023	8-Jan-2024	Compliant
2.0.3	SC69	Clarify router and firewall logging requirements	13-Mar-2024	15-Apr-2024	Compliant
2.0.4	SC65	Convert EVGs into RFC 3647 format	15-Mar-2024	15-May-2024	Compliant
2.0.5	SC73	Compromised and weak keys	3-May-2024	1-Jul-2024	Compliant
2.0.6	SC75	Pre-sign linting	28-Jun-2024	6-Aug-2024	Compliant
2.0.7	SC67	Require Multi-Perspective Issuance Corroboration	2-Aug-2024	6-Sep-2024	Compliant
2.0.8	SC77	Update WebTrust Audit name in Section 8.4 and References	2-Sep-2024	2-Oct-2024	Compliant
2.0.9	SC78	Subject organizationName	2-Oct-2024	8-Nov-2024	Compliant

		alignment for DBA / Assumed Name			
2.1.0	SC76	Clarify and improve OCSP requirements	26-Sep-2024	14-Nov-2024	Compliant
2.1.1	SC79	Allow more than one Certificate Policy in a Cross-Certified Subordinate CA Certificate	30-Sep-2024	14-Nov-2024	Compliant
2.1.2	SC80	Strengthen WHOIS lookups and Sunset Methods 3.2.2.4.2 and 3.2.2.4.15	7-Nov-2024	16-Dec-2024	Compliant
2.1.3	SC83	Winter 2024-2025 Cleanup Ballot	23-Jan-2025	24-Feb-2025	Compliant
2.1.4	SC84	DNS Labeled with ACME Account ID Validation Method	28-Jan-2025	1-Mar-2025	Compliant
2.1.5	SC81	Introduce Schedule of Reducing Validity and Data Reuse Periods	11-Apr-2025	16-May-2025	Compliant
2.1.6	SC85	Require Validation of DNSSEC (when present) for CAA and DCV Lookups	19-Jun-2025	21-Jul-2025	Compliant
2.1.7	SC89	Mass Revocation Planning	23-Jul-2025	25-Aug-2025	Compliant

* Effective Date and Additionally Relevant Compliance Date(s)