臺灣網路認證股份有限公司

最高層憑證管理中心

憑證實務作業基準(CPS)

Certification Practice Statement

(第 1.4 版)

生效日期：中華民國 111 年 2 月 9 日

Effective Date： 2022/2/9

版本變更紀錄：

版 本	生效日期	發 行 者	備 註
1.0	97/12/31	TWCA PMA	初版發行
1.1	100/05/06	TWCA PMA	1. 增修本憑證管理中心的下載服務。 2. 修訂稽核紀錄檢視頻率。 3. 修訂稽核紀錄備份頻率。
1.2	101/10/23	TWCA PMA	1. 因應 TWCA Root CA 新建 4096 bits sha256 自簽憑證，增修識別名稱。 2. 增修 Mozilla, Microsoft, Opera Root Program 之要求。
1.3	109/01/30	TWCA PMA	修訂以符合 CABF Baseline Requirement.
1.4	111/02/09	TWCA PMA	更正錯別字

目 錄

摘要

臺灣網路認證最高層憑證管理中心憑證實務作業基準之重要事項說明如下：

1. 主管機關核定

本憑證實務作業基準係依據主管機關經濟部頒布之「憑證實務作業基準應載明事項準則」規範編撰，經審查後核定之文號為：

111/2/9 經濟部函 經商字第 11102403730 號

2. 簽發之憑證

(1) 憑證種類：臺灣網路認證最高層憑證管理中心(以下簡稱本憑證管理中心)簽發之憑證，係為簽發給下屬憑證機構，做為下屬憑證機構身分鑑別之憑證。

(2) 保證等級：

本憑證管理中心依其憑證政策(Certificate Policy； CP)之「第四級」保證等級之規範運作，簽發其憑證政策所定義之五種保證等級的憑證予下屬憑證機構。

以下為各保證等級說明：

測試級：供用戶或信賴憑證者測試之保證等級，僅供測試用，不可用於任何非測試用途。

第一級(Class 1)：基本級的保證等級，適用於惡意竄改之威脅很低的網路環境下提供資料完整性的識別。

第二級(Class 2)：初級的保證等級，適用於惡意竄改之威脅很低的網路環境下，提供資料完整性的識別及基本之身分鑑別。

第三級(Class 3)：中級的保證等級，適合應用於有惡意使用者會截取或竄改資訊、較為危險之網路環境。

第四級(Class 4)：高級(High)的保證等級，適合應用於潛在威脅很高、或資訊被竄改後復原的代價很高之網路環境。

(3) 適用範圍：

本憑證管理中心所簽發之下屬憑證機構憑證用以建立本憑證管理中心與下屬憑證機構間的信賴關係，以建構本基礎建設所需的憑證信賴路徑。

本憑證管理中心所簽發之憑證，主要做為身分鑑別之安全機制。

本憑證管理中心依據本作業基準規範所簽發的下屬憑證機構憑證，其對象為向本憑證管理中心申請通過可擔任下屬憑證機構之法人。下屬憑證機構憑證，可用來驗證本憑證管理中心與下屬憑證機構間的相互信賴關係，如以本憑證管理中心之公開金鑰，驗證下屬憑證機構之憑證，則可確認下屬憑證機構與本憑證管理中心之信賴關係。

3. 法律責任重要事項

(1) 下屬憑證機構如發生廢止憑證之事由(如私密金鑰資料外洩或遺失)，應立即通知本憑證管理中心，並辦理憑證廢止相關作業，但下屬憑證機構仍應承擔憑證廢止狀態未被公布前因使用該憑證所致生之風險與責任。

(2)本憑證管理中心處理下屬憑證機構註冊資料及憑證簽發作業，除可歸責於本憑證管理中心之故意或過失外，本憑證管理中心不負損害賠償責任。

(3) 本憑證管理中心如因不可抗力之天災事故（如地震等），或其他非可歸責於本憑證管理中心之事由(如戰爭等)，造成下屬憑證機構損失時，本憑證管理中心不負損害賠償責任。

(4) 本憑證管理中心未善盡保管下屬憑證機構之註冊及憑證相關資料，而造成相關資訊洩漏、被冒用、竄改或任意使用致造成第三者遭受損害時，本憑證管理中心應負損害賠償責任。

(5) 本憑證管理中心在收到憑證廢止申請後，最遲於 1 個工作日內完成憑證廢止作業，並於憑證廢止作業完成後 24 小時內簽發憑證廢止清冊及公告於儲存庫。下屬憑證機構於憑證廢止狀態未被公布之前，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致生之責任。

(6) 本憑證管理中心與下屬憑證機構，因簽發憑證或使用憑證而發生損害賠償事件時，雙方應承擔之損害賠償責任，以相關法令規定及合約所定之範圍為責任上限。

(7) 信賴憑證者接受使用本憑證管理中心簽發之憑證時，即表示已了解並同意有關

本憑證管理中心法律責任之條款，並依照本作業基準之規定範圍內信賴該憑證。

4. 其他重要事項

(1) 下屬憑證機構私密金鑰有遺失或遭破解等不安全之顧慮時，或下屬憑證機構相關之資訊有異動時，下屬憑證機構必須依相關作業之規定，向本憑證管理中心辦理申告。

(2) 下屬憑證機構應妥善產製、保管及使用私密金鑰，並遵守對於金鑰及憑證之使用限制。

(3) 下屬憑證機構申請憑證時必須提供詳實且正確之資訊，接受本憑證管理中心簽發之下屬憑證機構憑證時，必須確認憑證內容之正確性，且公開金鑰與私密金鑰為成對之金鑰。

(4) 下屬憑證機構應存放其自身憑證及憑證廢止清冊等資料於安全的儲存庫內，確保儲存庫存取之可用性，提供信賴憑證者隨時查詢。

(5) 信賴憑證者驗證憑證時應使用本憑證管理中心之自簽憑證，驗證下屬憑證機構憑證之數位簽章是否為本憑證管理中心之私密金鑰所簽發，並透過憑證廢止清冊驗證憑證狀態是否已遭廢止。

(6) 信賴憑證者在使用本憑證管理中心簽發之憑證廢止清冊時，應先驗證數位簽章，以確認該憑證廢止清冊是否有效。

(7) 本憑證管理中心至少每年各進行 1 次內部及外部稽核，有關稽核作業規範請參閱「8. 稽核及其他評估方法」。

1.簡介

1.1 概述

臺灣網路認證股份有限公司(TAIWAN-CA INC.，以下簡稱本公司或 TWCA)係由臺灣證券交易所、臺灣集中保管結算所、財金資訊股份有限公司、網際威信股份有限公司共同集資設立。

臺灣網路認證股份有限公司最高層憑證管理中心憑證實務作業基準(TWCA Root Certification Authority Certification Practice Statement； 以下簡稱本作業基準)，係根據臺灣網路認證股份有限公司公開金鑰基礎建設憑證政策(以下簡稱憑證政策)及遵循電子簽章法主管機關頒布之「憑證實務作業基準應載明事項準則」所訂定。主要為說明臺灣網路認證股份有限公司最高層憑證管理中心(以下簡稱本憑證管理中心)，如何遵循憑證政策來進行下屬憑證機構之憑證簽發及管理作業。

為建立安全及可信賴的網路交易環境，確保資訊在網路傳輸過程中不易遭致偽造、竄改或竊取，且能鑑別交易雙方的身分及防止事後否認已完成交易的事實，TWCA 建立一公開金鑰基礎建設(TWCA Public Key Infrastructure； TWCA PKI，以下簡稱本基礎建設)，並建置本憑證管理中心擔任信賴起源(Trust Anchor)之最高層憑證管理中心(Root Certification Authority； RCA)，簽發憑證予下屬憑證機構(Subordinate CA)。

1.2 文件名稱及識別

本作業基準之名稱為臺灣網路認證股份有限公司最高層憑證管理中心憑證實務作業基準。

本作業基準依據憑證政策訂定，其物件識別碼為{joint-iso-itu-t(2) country(16) Taiwan(158) TWCA(3) CA(1) CP(5) id-TWCA-PKI-CP-policy(5) }

1.3 成員及適用範圍

1.3.1 最高層憑證管理中心

本憑證管理中心為最高層憑證管理機構，擔任本基礎建設之信賴起源，由本公司負責營運及管理，主要負責以下工作：

(1) 負責下屬憑證機構憑證之簽發與管理。
(2) 管理與公告下屬憑證機構之憑證、憑證廢止清冊(Certificates Revocation List；CRL)於儲存庫。
(3) 維持儲存庫的穩定與運作。

1.3.1.1 政策管理中心

設於本公司內之組織並負責制定下列事項：

(1) 憑證政策。
(2) 本作業基準。
(3) 營運規範。

1.3.2 註冊中心

註冊中心(Registration Authority； RA)主要負責鑑別下屬憑證機構的身分及簽發憑證所需之相關資訊，供本憑證管理中心簽發下屬憑證機構憑證。

本憑證管理中心自行擔任註冊中心，不設置其他註冊中心。

1.3.3 用戶

用戶為憑證中憑證主體 (Certificate Subject)名稱所記載之個體，且持有與憑證公開金鑰相對應之私密金鑰者。

本憑證管理中心之用戶為本公司，不簽發憑證於其他法人。

1.3.4 信賴憑證者

信賴憑證者係接受本憑證管理中心簽發之自我簽發憑證，並據此驗證本憑證管理中心簽發之下屬憑證機構憑證是否有效，並以下屬憑證機構憑證內之公開金鑰，驗證下屬憑證機構數位簽章訊息有效性之個體。

信賴憑證者應以本憑證管理中心簽發之下屬憑證機構憑證所記載之資訊，來決定是否可信賴該憑證，或是否可以使用於特定用途。

1.3.5 其他參與者

無規定。

1.4 憑證用途

1.4.1 憑證適用範圍

本憑證管理中心所簽發之下屬憑證機構憑證用以建立本憑證管理中心與下屬憑證機構間的信賴關係，以建構本基礎建設所需的憑證信賴路徑。

本憑證管理中心所簽發之憑證，主要做為身分鑑別之安全機制。

本憑證管理中心依據本作業基準規範所簽發的下屬憑證機構憑證，其對象為向本憑證管理中心申請通過可擔任下屬憑證機構之法人。下屬憑證機構憑證，可用來驗證本憑證管理中心與下屬憑證機構間的相互信賴關係，如以本憑證管理中心之公開金鑰，驗證下屬憑證機構之憑證，則可確認下屬憑證機構與本憑證管理中心之信賴關係。

1.4.2 憑證之禁止使用情形

本憑證管理中心所簽發之下屬憑證機構憑證除使用於上述規定之範圍。禁止使用於會造成人身傷亡與精神侵害，或對社會秩序與公共利益有重大危害之應用或業務，且排除使用於電子簽章法或其他相關法令或各事業目的主管機關明訂排除之應用或業務。

1.5 政策管理

1.5.1 管理單位

本作業基準的制訂、修訂、發布等事宜，其權責單位為「臺灣網路認證股份有限公司」政策管理中心(Policy Management Authority)。

1.5.2 聯絡窗口

對本作業基準有任何修改建議時，請將詳細的建議、說明文件與聯絡資訊，E-mail 或郵寄至下述的聯絡窗口；

用戶有關憑證的註冊、申請、更新、查詢，與金鑰有遺失、不安全顧慮的申告處理作業，本公司的聯絡及處理窗口如下述：

公司名稱	臺灣網路認證股份有限公司(TAIWAN-CA INC.； TWCA)
聯絡人	客服中心
地址	台北市中正區(100002)延平南路 85 號 10 樓 10TH Floor, 85, Yen-Ping South Road, Taipei, Taiwan, R.O.C
電話	886-2-23708886
傳真	886-2-23700728
電子郵箱	ca@twca.com.tw

1.5.3 憑證實務作業基準之核定

本憑證管理中心所訂定之憑證實務作業基準，應經由政策管理中心核定。

1.5.4 憑證實務作業基準核定程序

依據電子簽章法規定，本憑證管理中心訂定之憑證實務作業基準，必須經主管機關經濟部核定後，始得對外公布本作業基準並提供憑證簽發服務。

2. 公布及儲存庫

2.1 儲存庫

本憑證管理中心之儲存庫提供憑證、憑證廢止清冊、憑證政策及憑證實務作業基準等憑證作業相關資訊之查詢或下載。

儲存庫的網址為：

https://www.twca.com.tw

2.2 憑證資訊之公布

本憑證管理中心公布之資訊如下：

(1) 憑證政策及本作業基準
(2) 本憑證管理中心之自簽憑證與相關資訊
(3) 簽發之憑證
(4) 憑證廢止清冊

2.3 公布頻率

經修改完成且經政策管理中心(PMA)核定生效後之新版憑證政策(CP)，即刻公告於本公司網站。

依照需求經修改完成且經主管機關核定生效後之新版憑證實務作業基準(CPS)，即刻公告於本公司網站。

本憑證管理中心之自簽憑證及所簽發之憑證，一經產生後於一週內公告於儲存庫。

廢止憑證清冊(CRL)之公布頻率為至少每 24 小時公布 1 次。

2.4 儲存庫之存取控制

當本憑證管理中心需要公布簽發的憑證及憑證廢止清冊時，由憑證管理相關人員以離線手動方式，將須公布的憑證及憑證廢止清冊儲存在可攜式媒體中，再將檔

案複製到儲存庫主機中公布。

本作業基準及儲存庫資訊可公開讀取，不須存取權限的安全管控；但為防止惡意竄改於更新儲存庫時須進行存取控制。

3.識別與鑑別

3.1 命名

3.1.1 名稱種類

本憑證管理中心簽發以 X.500 唯一識別名稱為主體名稱之 X.509 憑證。

本憑證管理中心簽發之自簽憑證與下屬憑證機構憑證，皆使用此唯一識別名稱格式。

3.1.2 識別名稱之意義

下屬憑證機構憑證所記載之主體識別名稱，應符合相關法令對於命名之規定，必須足以識別特定之組織、單位或個人，且必須可為信賴憑證者所識別。

3.1.3 用戶之匿名與假名

本作業基準不允許下屬憑證機構使用匿名或假名。

3.1.4 各種名稱的解釋規則

下屬憑證機構憑證所記載之名稱，其名稱形式之解釋規則依 ITU-T X.520 名稱屬性定義。

3.1.5 名稱的唯一性

本憑證管理中心將審核下屬憑證機構中、英文名稱及唯一識別名稱之獨特性，但當下屬憑證機構有相同之註冊名稱或唯一識別名稱時，以先申請註冊之下屬憑證機構優先使用。

下屬憑證機構之識別名稱格式為：

識別名稱(DN)	說　　明
1.Country(C)	憑證機構所在地之國碼
2.Organization(O)	憑證機構之之英文名稱
3.OrganizationUnit(OU)	憑證機構之憑證管理中心業務資訊英文名稱
4.CommonName(CN)	憑證機構之憑證管理中心英文名稱

本憑證管理中心有 2 張自身憑證，其識別名稱分別為：

識別名稱(DN)	說　　明
1.Country(C)	C=TW
2.Organization(O)	O=TAIWAN-CA
3. OrganizationUnit(OU)	OU=Root CA
4.CommonName(CN)	CN=TWCA Root Certification Authority

識別名稱(DN)	說　　明
1.Country(C)	C=TW
2.Organization(O)	O=TAIWAN-CA
3.OrganizationUnit(OU)	OU=Root CA
4.CommonName(CN)	CN=TWCA Global Root CA

3.1.6 識別名稱糾紛的處理

當下屬憑證機構使用之唯一識別名稱有相同時，本憑證管理中心以先申請註冊之下屬憑證機構優先使用，如有爭議時，則依照經主管機關已核定之憑證實務作業基準內載明之名稱。

當下屬憑證機構使用之唯一識別名稱，經主管機關合法文件證實為其他申請者所擁有時，本憑證管理中心應註銷已註冊之下屬憑證機構唯一識別名稱使用權並廢止已簽發之憑證，該下屬憑證機構應負擔相關之法律責任。

3.1.7 商標之辨識、鑑別及角色

本憑證管理中心尊重下屬憑證機構中、英文名稱之註冊商標，並接受下屬憑證機構使用該中、英文名稱，但不保證下屬憑證機構註冊商標之認可、鑑別與唯一性，相關的糾紛仲裁處理非為本憑證管理中心/註冊中心的管轄權責範圍，用戶應自行向主管機關提出申請。

3.2 初始鑑別

3.2.1 證明擁有私密金鑰的方式

憑證內公開金鑰及對應之私密金鑰須由下屬憑證機構自行產製，並提供 PKCS#10 憑證申請檔且以私密金鑰簽章後交付本憑證管理中心，作為擁有私密金鑰之證明。本憑證管理中心將以下屬憑證機構之公開金鑰，驗證下屬憑證機構對 PKCS#10 憑證申請檔之簽章訊息，來確認下屬憑證機構為私密金鑰擁有者、公開金鑰與私密金鑰成對及下屬憑證機構身分資訊之完整性。

3.2.2 法人身分的鑑別

法人申請擔任下屬憑證機構，於對法人進行身分鑑別時，應鑑別主管機關核發或其他可資證明法人存在之證明文件，由代表人親自至本憑證管理中心進行代表人之身分鑑別；如代表人授權代理人辦理，須鑑別代理人的相關身分證明文件及授權文件，由代理人親自辦理相關身分識別資料之鑑別。

3.2.3 個人用戶身分的鑑別

不接受自然人擔任下屬憑證機構。

3.2.4 未鑑別之用戶資訊

本憑證管理中心對所有下屬憑證機構資訊皆須驗證。

3.2.5 權限之鑑別

法人之代表人、代理人及法人之身分證明文件，應為官方核發之證明文件；註冊中心須確認代理人授權文件之真偽。

3.2.6 相互溝通方式

本憑證管理中心對與下屬憑證機構之相互溝通方式不做規範。

3.3 金鑰更新之識別與驗證

3.3.1 憑證例行性金鑰更新

隨著金鑰使用時間增加，其可能遺失或遭破解之風險也增加，下屬憑證機構應定期更新金鑰以確保金鑰之安全性。

對憑證進行金鑰更新係指於憑證即將到期前，重新產生一組公開金鑰及私密金鑰對，並重新進行如 3.2 節規定之初始驗證方式向本憑證管理中心申請憑證簽發。

3.3.2 憑證廢止後之金鑰更新

下屬憑證機構之憑證廢止後，必須重新進行如 3.2 節規定之初始驗證方式，重新申請新憑證。

3.4 憑證廢止請求

當下屬憑證機構提出憑證廢止請求時，本憑證管理中心將對憑證廢止請求進行驗證，身分鑑別之方式依 3.2 節規定辦理。如因下屬憑證機構之私密金鑰已遭破解或有遭破解之疑慮時，可對下屬憑證機構憑證相對應私密金鑰產製之簽章進行驗證，無論私密金鑰是否已遭破解；惟事後仍應依 3.2 節規定補行程序。

4. 憑證生命週期管理

4.1 憑證申請

4.1.1 憑證申請者

本公司自行擔任下屬憑證機構者，由該下屬憑證機構之憑證主管人員擔任憑證申請者。

4.1.2 申請登記程序及責任

下屬憑證機構應事先閱讀憑證使用者約定事項，了解使用憑證之權利及義務，如同意則撰寫憑證申請書並備妥相關身分證明文件正本或影本，至本憑證管理中心辦理憑證申請。

4.2 憑證申請程序

4.2.1 識別與鑑別程序

本公司自行擔任下屬憑證機構之憑證申請程序如下：

(1) 下屬憑證機構之憑證主管人員擔任申請人。

(2) 申請人出具親筆簽名之憑證申請書及PKCS#10格式憑證申請檔，並經授權人員核定。

(3) 政策管理中心審查憑證申請書內容以及憑證實務作業基準是否符合憑證政策之規定。

(4) 政策管理中心通過審查後即進入憑證簽發程序。

4.2.2 接受或拒絕憑證申請

完成 4.2.1 節識別與鑑別程序後，視為憑證申請通過，如未能完成識別與鑑別程序，應拒絕憑證申請。

4.2.3 憑證申請處理時間

無規定。

4.3 憑證簽發

4.3.1 憑證機構簽發憑證

本憑證管理中心之憑證簽發程序如下：

(1) 下屬憑證機構自行產製 PKCS#10 格式之憑證申請檔，連同憑證申請書以書函方式交付本憑證管理中心。
(2) 本憑證管理中心確認下屬憑證機構交付之憑證申請檔，確實來自下屬憑證機構。
(3) 以驗證數位簽章之方式，確認 PKCS#10 格式之憑證申請檔之完整性；檢查憑證申請檔記載之憑證主旨識別名稱，符合憑證申請書所記載之主旨識別名稱及申請使用之擴充欄位。
(4) 本憑證管理中心檢查無誤後，即簽發憑證予下屬憑證機構。簽發完成之憑證將以離線或連線的方式，交付下屬憑證機構。

4.3.2 憑證機構簽發憑證通知用戶

本憑證管理中心於憑證簽發完成後，以電話或電子郵件方式通知下屬憑證機構，經由雙方人員確認後以離線或連線的方式傳遞憑證檔案予憑證申請者。

4.4 憑證接受

4.4.1 憑證接受之程序

下屬憑證機構於收到本憑證管理中心簽發之憑證後，應進行以下程序：

(1) 確認憑證內容與申請時之一致性，且為憑證機構之正確資訊。

(2) 檢查憑證內之公開金鑰，是否與 PKCS#10 憑證申請檔內之公開金鑰資訊相同。

(3) 以本憑證管理中心之自簽憑證驗證憑證之有效性及合法性。

(4) 如未能完成前述程序，應立即告知本憑證管理中心廢止憑證，並得重新進行 4.3 節憑證簽發程序。

(5) 憑證申請者於收到所申請之憑證後，必須簽署確認接受文件並以書面方式告知本憑證管理中心，確認文件內容必須載明下屬憑證已充分了解使用憑證之權利及義務。若未能於憑證簽發後 30 個日曆天內告知本憑證管理中

心，則視為拒絕接受憑證，本憑證管理中心將立即廢止憑證，惟下屬憑證機構得於 30 個日曆天內要求重新進行 4.3 節憑證簽發程序。

4.4.2 憑證機構公布憑證

本憑證管理中心於下屬憑證機構完成憑證接受程序後，立即將簽發予下屬憑證機構之憑證公布於儲存庫。

4.4.3 憑證機構通知其他機構憑證簽發

無規定。

4.5 金鑰對及憑證用途

4.5.1 用戶私密金鑰及憑證使用

下屬憑證機構憑證的用途、適用範圍及限制，如 1.4 節之規定。

下屬憑證機構的私密金鑰有被冒用、曝露或遺失等不安全疑慮時，下屬憑證機構必須向本憑證管理中心辦理申告。

4.5.2 信賴憑證者公開金鑰及憑證使用

信賴憑證者於信賴本憑證管理中心簽發之下屬憑證機構憑證前，至少應進行以下必要之程序，方可使用於驗證下屬憑證機構所簽發之數位簽章：

(1) 透過適當及安全之管道，取得本憑證管理中心之自簽憑證。
(2) 檢查下屬憑證機構憑證是否已過期。
(3) 以本憑證管理中心自簽憑證內包含之公開金鑰，驗證包含於下屬憑證機構憑證內，由本憑證管理中心簽發之數位簽章。
(4) 檢查下屬憑證機構憑證未遭本憑證管理中心廢止。

如未能通過前述驗證，表示信賴憑證者取得之下屬憑證機構憑證非本憑證管理中心所簽發，或憑證已失效，信賴憑證者不應信賴該下屬憑證機構憑證。

4.6 憑證展期

憑證展期(renewal)係指用戶識別資訊不變之情況下，重新簽發一張與原有憑證具相同金鑰、不同序號、以及效期延長之憑證。

因本憑證管理中心不接受下屬憑證機構進行憑證展期，故關於有權展期憑證者、憑證展期程序、通知用戶展期憑證之簽發、展期憑證接受程序、憑證機構公布展期憑證與憑證機構通知其他機構展期憑證之簽發等規定不適用。

4.7 憑證及私密金鑰更新

對憑證進行金鑰更新係指重新產生一組公開金鑰及私密金鑰對，並以原有的註冊資訊向憑證機構申請憑證簽發。

4.7.1 憑證金鑰更新之事由

如 3.3.1 節之規定。

4.7.2 有權更新憑證金鑰者

下屬憑證機構有權更新憑證金鑰。

4.7.3 憑證金鑰更新程序

- 依照 3.3 節之規定對用戶進行身分識別與驗證。
- 依照 4.3 節之規定簽發憑證。

4.7.4 通知用戶更新金鑰憑證之簽發

依 4.3.2 節之規定。

4.7.5 更新金鑰憑證接受程序

依 4.4 節之規定。

4.7.6 憑證機構公布更新金鑰憑證

依 4.4.2 節之規定。

4.7.7 憑證機構通知其他機構更新金鑰憑證之簽發

依 4.4.3 節之規定。

4.8 憑證變更

憑證變更係指憑證之公開金鑰不變，但其所記載之用戶名稱識別資訊須變更時，重新簽發憑證予用戶。

本憑證管理中心不接受下屬憑證機構進行憑證變更，如下屬憑證機構之識別資訊或其他記載於憑證之資訊須變更時，應依 4.1、4.2、4.3、4.4 節規定重新申請憑證簽發。

4.9 憑證廢止及暫時停用

4.9.1 憑證廢止之事由

以下為有權請求廢止憑證者得請求憑證廢止之事由：

(1) 下屬憑證機構憑證欲終止憑證的使用。
(2) 下屬憑證機構憑證在有效期間內，憑證記載資訊有誤須更動時。
(3) 下屬憑證機構憑證相關的私密金鑰經證實或懷疑遭破解、毀損、遺失、曝露、被竄改時。

下屬憑證機構違反主管機關之法令、憑證政策、本憑證實務作業基準或與本公司簽署之合約時，本憑證管理中心得逕行廢止下屬憑證機構之憑證。

當上述狀況發生時，相關憑證應被廢止並加入憑證廢止清冊。遭廢止之憑證必須包含於之後所公布的憑證廢止清冊，直到憑證到期為止。

4.9.2 有權請求廢止憑證者

(1) 下屬憑證機構。
(2) 本憑證管理中心。
(3) 主管機關或法院。

4.9.3 憑證廢止程序

本公司自行擔任下屬憑證機構申請憑證廢止，及逕行廢止下屬憑證機構憑證之程序如下：

(1) 憑證主管人員擔任申請人。

(2) 申請人出具親筆簽名之憑證廢止申請書，經政策管理中心核定後，由憑證廢止執行人員於3個工作日內廢止憑證。

4.9.4 憑證廢止請求提出期限

下屬憑證機構於憑證廢止事由發生後，最遲應於 10 個工作日內提出憑證廢止申請。

4.9.5 憑證機構處理憑證廢止請求時限

本憑證管理中心於收到下屬憑證機構提出之憑證廢止申請，最遲應於 1 個工作日內完成憑證廢止。

4.9.6 信賴憑證者憑證廢止驗證規定

信賴憑證者應根據其風險、責任及可能導致之後果，自行判斷查詢(或下載)廢止資料(憑證廢止清冊)的間隔時間。

信賴憑證者在使用本憑證管理中心簽發之下屬憑證機構憑證，驗證下屬憑證機構之數位簽章時，應檢查該下屬憑證機構憑證是否為廢止狀態。

4.9.7 憑證廢止清冊簽發頻率

本憑證管理中心至少每 24 小時更新並簽發 1 次憑證廢止清冊(Certificate Revocation List； CRL)。

4.9.8 憑證廢止清冊最大潛在因素

不做規範。

4.9.9 線上憑證廢止/狀態查詢服務

本憑證管理中心提供線上憑證廢止/狀態查詢服務，供信賴憑證者查詢本憑證管理中心所簽發之憑證狀態資訊。

線上憑證狀態查詢服務之回應訊息符合 RFC6960 之規範，回應訊息包含對該訊息之數位簽章。

4.9.10 線上廢止/狀態查詢驗證規定

本憑證管理中心至少每 12 個月更新線上憑證狀態查詢服務提供之憑證狀態資訊，且於下層憑證機構憑證廢止後 24 小時內更新憑證狀態資訊。

若信賴憑證者查詢線上憑證狀態查詢服務，查詢之憑證非本憑證管理中心所簽發之憑證，將會收到憑證狀態未知之回應訊息。

4.9.11 其他形式之廢止公告

不做規範。

4.9.12 金鑰遭破解之特殊規定

本憑證管理中心之簽章金鑰遭破解時，應依照以下程序辦理：

(1) 產生新的簽章用金鑰對及相對應的新憑證。
(2) 廢止所有已簽發之憑證，使用新的簽章金鑰簽發憑證廢止清冊，憑證廢止清冊包含所有已簽發之未到期憑證資訊(含金鑰遭破解前簽發之已廢止憑證)。
(3) 告知下屬憑證機構。
(4) 安全地遞送新憑證予下屬憑證機構。
(5) 使用新的簽章用金鑰來簽發新憑證予下屬憑證機構。

下屬憑證機構之金鑰被懷疑或證實遭破解，應於 24 小時內告知本憑證管理中心。

4.9.13 憑證暫時停用之事由

因本憑證管理中心不提供憑證暫時停用服務，故以下有關於有權請求憑證暫時停用者、憑證暫時停用程序與憑證暫時停用期間限制等規定不適用。

4.9.14 有權請求憑證暫時停用者

不適用。

4.9.15 憑證暫時停用程序

不適用。

4.9.16 憑證暫時停用期間限制

不適用。

4.10 憑證狀態服務

4.10.1 服務特性

憑證狀態資訊透過憑證廢止清冊(CRL)和線上憑證狀態查詢服務提供憑證狀態資訊。已廢止憑證之憑證廢止資訊，在該憑證效期過後，才會自 CRL 和線上憑證狀態查詢服務移除。

4.10.2 服務之可用性

本憑證管理中心提供線上 24x7 之儲存庫供信賴憑證者查詢所有未過期憑證之憑證狀態。

本憑證管理中心提供 24x7 之投訴機制，用以回應重大憑證問題(例如憑證遭冒名申請或誤發)之投訴，投訴經確認後，將遭投訴之憑證逕行廢止，若有違法事件將轉知執法機構。

4.10.3 附加功能

參閱 4.9.9, 4.9.11 節之規定。

4.11 憑證終止使用

當本憑證管理中心簽發之憑證效期屆滿、下屬憑證機構廢止憑證或本憑證管理中心結束營運時，已簽發之憑證即告失效。

4.12 金鑰託管及復原

4.12.1 金鑰託管及復原政策與施行

本憑證管理中心及下屬憑證機構的金鑰不得進行金鑰託管。

4.12.2 加密期間金鑰封裝及復原政策與施行

不做規範。

5.實體、管理及作業流程控管

5.1 實體控管

5.1.1 建築物與位置

本憑證管理中心機房位於本公司，符合儲存高重要性及敏感性資訊的機房設施水準，並結合門禁、保全、入侵偵測及監視錄影等實體安全機制，以防止未經授權者存取本憑證管理中心之相關設備。

5.1.2 實體進出管制

本憑證管理中心機房之進出管制措施如下：

(1) 3 道門禁之身分查核(以智慧卡或指紋識別)識別管制，且必須同時兩人以上經過身分鑑別後才可進入；具備 24 小時 CCTV 位移監控錄影設備、及紅外線防入侵警報系統，以記錄進出機房之狀況及預防未經授權者進入機房。
(2) 本憑證管理中心運作之私密金鑰備份相關資料，皆妥善安全地存放於設有監控錄影系統保護之保險櫃內。憑證管理系統運作之相關作業人員，須兩人以上方可執行憑證管理作業，且皆有監控錄影設備之監測。
(3) 軟硬體及硬體密碼模組等設備，皆置於有監控錄影系統保護之環境下，須兩人以上方可執行金鑰管理相關作業。

5.1.3 電力與空調

本憑證管理中心機房設有柴油發電機及不斷電系統(Uninterruptible Power Supply, UPS)，當一般供電系統異常時，會自動切換至柴油發電機供電，切換過程由 UPS 提供穩定之電力。

具備獨立之空調系統，確保系統運作的穩定與提供最佳之工作環境，並定期執行維護與測試。

5.1.4 防水處理

本憑證管理中心之機房為密閉式建築物，除內部可進出之出入門外，外部皆為混凝土建築物，且樓層地板裝置高架地板無進水之顧慮。

5.1.5 防火

本憑證管理中心機房建置之材質為防火材質並配置具有中央監控系統之滅火設

備，於偵測到火災發生時，能自動啟動滅火功能。

5.1.6 媒體儲存

本憑證管理中心之媒體儲存環境，可避免媒體意外損毀，對磁性媒體具有防磁、防靜電干擾之設備與環境；重要資料備份媒體儲存於具防火功能之保險櫃，其中 1 份備份資訊之媒體儲存於具有安全管控措施之異地備援地點。

5.1.7 廢棄處理

本憑證管理中心所使用之硬體設備、磁碟機與密碼設備等，於廢棄不使用時，其所儲存之商業敏感性及隱密性資訊必須經過安全之清除與銷毀，且須經由稽核單位之驗證，並留存查核文件。

文件與媒體若有儲存商業敏感性及隱密性資訊者，於廢棄處理時必須經過安全之清除與銷毀，使該資訊無法回復與存取使用，且須經由稽核單位之驗證，並留存查核文件。

5.1.8 異地備援

本憑證管理中心設置有異地備援機房，並設置備援設備，當日常營運之設備因外力因素無法正常運作時，備援設備可提供本憑證管理中心持續營運的能力。

本憑證管理中心運作所需之相關媒體資訊與文件，經備份後儲存於具備溫濕度管控、防磁、防靜電干擾，且具有監控攝影機監控錄影，與人員進出須經過授權之高度安全管控異地備援環境。

本憑證管理中心之備份紀錄檔，皆儲存於具高度安全管控之異地備援機房。

5.2 作業程序控管

5.2.1 信賴角色

本憑證管理中心於公開金鑰基礎建設(PKI)的架構下，憑證管理作業必須在具備嚴密性、安全性的作業流程下進行。為使職務與權責之區分，及職務之備援不危及整體系統之安全性及營運之完整性，本憑證管理中心之信賴角色及其分工如下：

(1) 系統管理人員(Administrator)負責系統安裝、管理作業及環境參數設定。

(2) 憑證主管人員(Officer)負責憑證簽發及憑證廢止。

(3) 稽核人員(Auditor)負責進行內部稽核、檢視並維護稽核紀錄。

(4) 操作人員(Operator)負責例行性維護作業，如備份、還原、網站資料維護等。

5.2.2 作業人員需求人數

各種信賴角色的作業人數需求如下：

(1) 系統管理人員(Administrator)至少 2 名。
(2) 憑證主管人員(Officer)至少 2 名。
(3) 稽核人員(Auditor)至少 1 名。
(4) 操作人員(Operator)至少 2 名。

5.2.3 角色的識別與鑑別

本憑證管理中心執行憑證管理作業之系統管理人員、憑證主管人員、稽核人員與操作人員，於系統資源之使用上皆有依業務區分，並使用唯一之身分識別碼、智慧卡及相關之密碼，以達到信賴角色之身分識別與鑑別。

相關作業人員依業務需求執行之作業功能，每筆皆有詳細之紀錄，確保系統資源使用之可稽核性，並可評估系統安全威脅及風險。

5.2.4 角色隔離

角　色	憑證主管人員	系統管理人員	稽核人員
憑證主管人員	○	X	X
系統管理人員	X	○	X
稽核人員	X	X	○

5.3 人員控管

5.3.1 背景、適任條件與經歷

(1) 本憑證管理中心之作業人員，必須具備忠實、可信賴及工作之熱誠，無影響憑證作業之其他兼職工作，且無違法及信用不良之紀錄。

(2) 憑證主管人員至少具備憑證作業之實務經驗，或經過憑證相關作業之訓練而通過測驗者。

(3) 系統管理人員至少具備憑證作業之實務經驗，並具有電腦系統規劃及營運管理之經驗。

5.3.2 背景審核程序

本憑證管理中心工作人員，須由人事管理相關部門依背景審核規範，執行身分背景安全審查，並由相關作業部門執行實務與經歷審查，審查通過後始可任職。每年必須依各種作業人員之職務特性，執行實務與經歷之審查，作為該員是否適任相關之工作或作為執行工作調整之依據。

5.3.3 教育訓練

本憑證管理中心作業人員，皆依照其職務，施予本憑證管理中心系統運作所應具備之軟硬體功能、作業程序、安控程序、災變備援作業規範、金鑰管理作業及憑證政策與本作業基準與其他資訊安全相關作業規範之教育訓練，憑證系統有異動或有新系統加入時，亦須給予適當之教育訓練。

針對憑證管理系統相關硬軟體、應用系統與安全管理系統，本憑證管理中心制定有完整之教育訓練規範，於新進人員雇用或本憑證管理中心系統有異動時，均施行相關技能之教育訓練，教育訓練完成後有詳實之成果紀錄，作為相關作業人員工作委任之參考。

5.3.4 教育訓練的頻率與需求

針對憑證管理系統運作相關人員，本憑證管理中心將就其執行憑證管理系統運作之相關知識與技能，每年至少進行 1 次檢討，並給予適當之教育訓練；憑證管理系統功能之更新、或新系統之加入、或公開金鑰基礎建設相關知識與技術之進步與更新，皆對系統運作之相關人員進行教育訓練。

5.3.5 職務的輪調

(1) 系統管理人員調離原職務滿 1 年後，才可轉任憑證主管人員或稽核人員。

(2) 憑證主管人員調離原職務滿 1 年後，才可轉任系統管理人員或稽核人員。

(3) 稽核人員調離原職務滿 1 年後，才可轉任系統管理人員或憑證主管人員。

(4) 擔任操作人員滿 2 年，且已接受相關教育訓練並通過審核後，才可轉任系統管理人員、憑證主管人員及稽核人員。

5.3.6 非授權作業的處罰

本憑證管理中心憑證管理系統運作之相關作業人員，因故意或過失而執行非自己職務上之作業時，無論是否造成憑證管理系統安全之問題，皆應即刻呈報監督管

理者，並依照相關作業之規範處理。

5.3.7 委外人員需求

本憑證管理中心因人力資源不足而委由外包人員擔任操作人員時，本憑證管理中心必須對其進行如 5.3.2 節之背景審查程序後，施以職務上知識與技能之教育訓練，該外包人員除須簽訂與工作內容相關之保密合約外，並應遵守相關作業規範與法律規範；該外包人員之權利義務與本憑證管理中心內部操作人員相同。

5.3.8 作業文件需求

為使憑證管理系統正常運作，本憑證管理中心必須提供相關作業人員執行系統運轉之作業文件，至少包含如下：

(1) 硬體、軟體作業平台之操作文件、網路系統與網站相關之操作文件、亂碼化系統之操作文件。
(2) 本憑證管理中心憑證管理系統之相關操作文件。
(3) 本憑證作業基準、憑證政策及相關作業規範文件。
(4) 本憑證管理中心憑證管理系統內部作業文件，例如：系統備援與回復作業文件、異地災變備援與回復作業文件、例行工作作業文件。

5.4 稽核紀錄程序

5.4.1 事件紀錄類型

本憑證管理中心的每筆稽核紀錄，無論是採自動或手動方式記錄，均包含下列項目：

- 事件類型。
- 事件發生日期及時間。
- 事件成功或失敗之結果。
- 引發此事件之個體或人員。
- 事件內容描述。

以下是本憑證管理中心所記錄的稽核事件種類：

(1) 安全稽核

- 任何重要稽核參數之改變，如稽核事件型態、新舊參數的內容等。
- 任何嘗試刪除或修改稽核紀錄檔。

(2) 人員及信賴角色管理、識別及鑑別

- 新角色的設定不論成功或失敗。
- 身分鑑別嘗試的最高容忍次數改變。
- 使用者登入系統時身分鑑別嘗試的失敗次數之最大值。
- 管理者將已被鎖住的帳號解鎖。
- 管理者改變系統的身分鑑別機制，例如從通行密碼改為生物特徵值。

(3) 金鑰作業程序

- 產製金鑰。
- 銷毀金鑰。

(4) 私密金鑰之載入和儲存

- 載入私密金鑰到系統元件中。

(5) 可信賴公開金鑰之新增、刪除及儲存

- 可信賴公開金鑰之改變，包括新增、刪除及儲存。

(6) 私密金鑰之輸出

- 私密金鑰之輸出(不包括只用在單次或只限 1 次使用之金鑰)。

(7) 憑證之註冊

- 憑證之註冊申請過程。

(8) 廢止憑證

- 憑證之廢止申請過程。

(9) 憑證狀態改變之核可

- 核可或拒絕憑證狀態改變之申請。

(10) 組態設定

- 安全組態相關設定之改變。

(11) 帳號之管理

- 加入或刪除角色和使用者。
- 修改使用者帳號或角色之存取權限。

(12) 憑證剖繪之管理

- 憑證剖繪之改變。

(13) 憑證廢止清冊剖繪之管理

- 憑證廢止清冊剖繪之改變。

(14) 系統安裝及營運重要事件

- 安裝作業系統。
- 安裝憑證管理系統。
- 安裝硬體密碼模組。
- 移除硬體密碼模組。
- 銷毀硬體密碼模組。
- 啟動系統。
- 嘗試登入憑證管理系統。
- 硬體及軟體之接收。
- 嘗試設定通行密碼。
- 嘗試修改通行密碼。
- 本憑證管理中心之內部資料備份。
- 本憑證管理中心之內部資料回復。

- 檔案操作(例如產生、重新命名及移動等)。
- 傳送任何資訊到儲存庫。
- 存取本憑證管理中心之內部資料庫。
- 金鑰被破解。
- 本憑證管理中心或下屬憑證機構之金鑰更換。

(15) 改變本憑證管理中心伺服器之設定

- 硬體。
- 軟體。
- 作業系統。
- 修補程式 (Patches)。
- 安全剖繪。

(16) 實體存取及場所之安全

- 人員進出本憑證管理中心之機房。
- 存取本憑證管理中心之伺服器。
- 知悉或懷疑違反實體安全規定。

(17) 異常事件

- 軟體錯誤。
- 軟體檢查完整性失敗。
- 接收錯誤格式之訊息。
- 非正常路由之訊息。
- 網路攻擊(懷疑或確定)。
- 設備失效。
- 電力不當。

- 不斷電系統失效。
- 明顯及重大的網路服務或存取失敗。
- 違反本作業基準。
- 重設系統時鐘。

5.4.2 紀錄處理頻率

本憑證管理中心每 2 個月會檢視 1 次稽核紀錄，追蹤調查發生的事件。檢視工作包括驗證稽核紀錄是否被竄改、檢視所有的紀錄項目及檢查任何警示或異常等，並加以解釋及提出相對預防再發生的方案。檢視稽核紀錄之結果以文件記錄。

5.4.3 稽核紀錄保留期限

相關稽核紀錄報表與媒體資料至少於本憑證管理中心保留 7 年。

5.4.4 稽核紀錄的保護

(1) 確保只有經授權人員可以讀取稽核紀錄，只有經授權人員可以備份稽核紀錄。
(2) 使用簽章或加密技術保存目前和已歸檔之電子式稽核紀錄，並儲存於不可覆寫光碟片或其他無法更改稽核紀錄的媒體。
(3) 保護事件紀錄的金鑰不能再使用於其他用途。
(4) 紙張及實體的稽核紀錄存放於安全場所。

5.4.5 稽核紀錄備份程序

電子式稽核紀錄每 2 個月備份 1 次，並儲存於本憑證管理中心以外之具備高度安全管控的其他備援地點。

5.4.6 稽核紀錄彙整系統

稽核系統內建於本憑證管理中心憑證管理系統中，稽核程序在憑證管理系統啟動時啟用，唯有在憑證管理系統關閉時才停止。

如自動稽核系統無法正常運作，保護系統資料完整性、機密性的安全機制處於高風險狀態時，本憑證管理中心將暫停憑證簽發服務，直到問題解決後再行提供服務。

5.4.7 對引發事件者之告知

如因發生事件而被稽核系統記錄，稽核系統並不須要告知引起該事件的個體其

所引發的事件已經被系統記錄。

5.4.8 脆弱性評鑑

每年進行一次以下所列的各種脆弱性評鑑：

(1) 作業系統的脆弱性評鑑。

(2) 實體設施的脆弱性評鑑。

(3) 憑證管理系統的脆弱性評鑑。

(4) 網路的脆弱性評鑑。

5.5 紀錄歸檔

5.5.1 歸檔紀錄類型

本憑證管理中心歸檔紀錄包含以下種類：

(1) 被稽核認證(Accreditation)資料。

(2) 憑證實務作業基準。

(3) 下屬憑證機構合約。

(4) 系統與設備組態設定。

(5) 系統或組態設定修改與更新的內容。

(6) 憑證申請資料。

(7) 廢止申請資料。

(8) 憑證接受的確認文件。

(9) 已簽發或公告的憑證。

(10) 本身金鑰更換的紀錄。

(11) 已簽發或公告的憑證廢止清冊。

(12) 稽核紀錄。

(13) 用來驗證及佐證歸檔內容的其它說明資料或應用程式。

(14) 公正稽核人員要求的文件。

(15) 下屬憑證機構身分鑑別資料。

5.5.2 歸檔紀錄保存期限

本憑證管理中心之歸檔資料保存期限最少 15 年。

5.5.3 歸檔紀錄的保護

已歸檔資料不可進行寫入、修改或刪除的動作；屬於下屬憑證機構之個別已歸檔資料，允許對該下屬憑證機構或其他法規允許之機構釋出。

歸檔資料必須保存 1 份於憑證機構所在地外，具安全管控措施，且對儲存媒體具備損壞預防措施之異地備援地點。

5.5.4 歸檔紀錄的備份程序

金鑰、憑證、交易資料等相關資料，依照備份與備援回復的作業程序，每日、週、月的整理歸檔及備份，1 份儲存於本公司具安全管控措施的環境下，且 1 份保存資料儲存於具安全管控措施的異地備援環境，當憑證系統異常無法開啟時，依系統備份與回復作業手冊，以保存的備份資料執行憑證系統的異常回復作業。

5.5.5 歸檔紀錄之時序要求

歸檔之電子式紀錄(例如憑證、憑證廢止清冊及稽核紀錄等)包含日期與時間資訊，且這些紀錄皆經過適當的數位簽章或加密演算保護，可用以檢測紀錄中的日期與時間資訊是否遭到竄改。惟此電子式紀錄中的日期與時間資訊並非公正第三者所提供之電子式時戳資料，而是電腦作業系統的日期與時間。

本憑證管理中心的所有電腦系統都會定期進行校時，以確保電子式紀錄中日期與時間資訊的準確性與可信度。

歸檔的書面紀錄也將記載日期資訊，必要時並將記載時間資訊。書面紀錄的日期與時間紀錄不可任意更改，如需更改必須由稽核人員簽名確認。

5.5.6 歸檔紀錄彙整系統

本憑證管理中心作業相關的歸檔紀錄資訊，皆由本公司內部的作業人員執行，於具有資源權責獨立及安全的管控措施下產生；稽核紀錄蒐集的保存資訊亦是由內部的管控系統所產生，憑證管理系統運作的相關文件歸檔紀錄，由權責的業務相關人員蒐集與管理。

5.5.7 取得及驗證歸檔紀錄之程序

本公司憑證系統作業相關的保存紀錄資訊的驗證，依本公司的內部管理作業規範，至少 1 年 1 次抽查驗證。

5.6 金鑰更新

為降低本憑證管理中心簽章用金鑰遭破解的風險，簽章用金鑰必須定期進行更新。

本憑證管理中心簽章用金鑰有效期間等同於其對應憑證之生命週期，憑證生命週期不得超過 30 年。

本憑證管理中心進行金鑰更新時，會產製一對新的金鑰對，並產生自簽憑證後，依照 6.1.4 節規定供信賴憑證者查詢下載。

下屬憑證機構在選擇金鑰效期時，應考慮金鑰長度、保護方式、控制方式及其他各種因素，且不可違反 6.1.5 節之規定。

5.7 金鑰遭破解及災變復原程序

5.7.1 金鑰遭破解及緊急應變處理程序

若本憑證管理中心金鑰遭破解或遺失(雖尚未確定是否可能遭破解)，則須進行下列程序：

- 必須儘快透過安全電子郵件或書面方式，通知所有之下屬憑證機構。
- 依 6.1 節的規定產生新的金鑰對並產生新的自簽憑證。
- 廢止所有已簽發之憑證，使用新的簽章金鑰簽發憑證廢止清冊，憑證廢止清冊包含所有已簽發之未到期憑證資訊(含金鑰遭破解前簽發之已廢止憑證)。

- 依 4.3 節的程序，簽發新的憑證給各下屬憑證機構。

本憑證管理中心必須調查，並向政策管理中心報告金鑰遭破解或遺失之原因，以及採取何種措施以避免發生相同狀況。

本憑證管理中心為最高層憑證管理中心，本憑證管理中心之自身憑證為自簽憑證，故無以原公開金鑰驗證新公開金鑰之處理程序。

本憑證管理中心訂定有緊急應變處理程序和災變復原計畫。

本憑證管理中心以書面記載業務持續計畫與災變復原程序，內容包含當發生災難、安全性遭破解以及營運中斷事件時，對軟體商(例如瀏覽器廠商)、用戶及信賴憑證者之告知程序。

本憑證管理中心將每年定期測試、檢視與修訂這些程序。

5.7.2 電腦資源、軟體及資料損毀之處理程序

本憑證管理中心訂定電腦資源、軟體及資料遭破壞之復原程序，同時每年進行演練。

如本憑證管理中心的電腦設備遭破壞或無法運作，但簽章金鑰並未損毀，則優先回復儲存庫之運作，並迅速重建憑證簽發、廢止及管理的功能。

5.7.3 個體金鑰遭破解之處理程序

各下屬憑證機構之金鑰懷疑遭破解時，應依 4.9.3 節之方式辦理。

5.7.4 災變後之營運持續能力

在發生自然災害或其他災變，以致於無法在 24 小時內恢復憑證狀態服務時，將啟用異地備援機房之設施，並於啟用後 24 小時內恢復提供憑證狀態服務。

5.8 憑證機構終止服務

本憑證管理中心終止服務時，將依電子簽章法相關規定辦理。

本憑證管理中心因故結束其系統營運時,須對系統運作之影響減少至最低程度,而將相關憑證業務安全地轉移至其他憑證機構繼續運作。

於終止服務之日 30 日前通知主管機關。

(1) 於終止服務之日 3 個月前，將終止服務及由其他憑證機構承接相關業務之事實通知下屬憑證機構並公布於儲存庫。
(2) 於無安全顧慮之作業環境下，將結束之本憑證管理中心相關私密金鑰與憑證，移轉至承接之憑證機構。
(3) 將憑證政策、憑證實務作業基準、憑證機構相關作業手冊文件、用戶合約與註冊資料、稽核紀錄、歸檔資料、憑證狀態資料及其他業務承接所必須的相關文件，移轉至承接的憑證機構。
(4) 將本憑證管理中心之相關私密金鑰完全清除，並向下屬憑證機構正式宣告，憑證業務已移轉至承接的憑證機構繼續營運。

本憑證管理中心結束業務時，相關權利義務亦將依照與下屬憑證機構簽訂之合約辦理。

6.技術安全控管

6.1 金鑰對的產製及安裝

6.1.1 金鑰對的產生

本憑證管理中心產製自身金鑰對時：

1. 制定並遵循金鑰產製腳本。
2. 由公正第三方稽核人員見證金鑰產製程序與紀錄，且對金鑰產製程序全程錄影。
3. 由公正第三方稽核人員出具意見報告，確認本憑證管理中心金鑰產製所進行之金鑰和憑證產製程序，以及為確保金鑰對之完整性和機密性所使用之控制措施。

本憑證管理中心依照 6.2.1 節規定，使用 CNS 15135、ISO 19790 或 FIPS 140-2 等級 3 硬體密碼模組產製金鑰對，私密金鑰在硬體密碼模組內產製後一直儲存在其中而不外洩。

金鑰產製過程在第三方公正人士見證下進行，金鑰產製後由公正人士簽署金鑰產製見證書，以昭公信。

6.1.2 私密金鑰遞送至用戶

私密金鑰由下屬憑證機構自行產生。

6.1.3 公開金鑰遞送至憑證簽發者

下屬憑證機構的公開金鑰是以 PKCS#10 憑證申請檔傳送給本憑證管理中心，其傳送方式應以磁碟片或光碟連同憑證申請書以書函方式傳送。並且依 3.2.1 節所述之方式完成私密金鑰擁有的驗證程序。

6.1.4 憑證機構公開金鑰遞送至信賴憑證者

本憑證管理中心應將其自簽憑證及簽發的下屬憑證機構憑證公布至儲存庫，供信賴憑證者查詢下載。

6.1.5 金鑰長度

本憑證管理中心的 RSA 公開金鑰長度至少為 2048 位元；ECC 曲線至少為 P-

256。

下屬憑證機構的 RSA 公開金鑰長度至少為 2048 位元；ECC 曲線至少為 P-256。

6.1.6 公開金鑰參數的產生及參數品質驗證

RSA：本憑證管理中心採用 RSA 演算法，質數產生器是採用 ANSI X9.31 演算法產生 RSA 演算法所需的質數，此方法可保證該質數為強質數(Strong Prime)。模數並應包含以下特性：奇數、不是質數乘冪且並無小於 752 之因數。

ECC：本憑證管理中心使用 ECC 完整公開金鑰驗證程序(ECC Full Public Key Validation Routine)或 ECC 部分公開金鑰鑰驗證程序(ECC Partial Public Key Validation Routine)來確保所有金鑰的有效性。

6.1.7 金鑰使用目的

本憑證管理中心簽發給下屬憑證機構的憑證中，其 X.509v3 憑證金鑰用途擴充欄位的金鑰用途位元為 keyCertSign 與 cRLSign。

本憑證管理中心簽發憑證種類以下列為限：

1. 本憑證管理中心自簽憑證。
2. 下屬憑證機構憑證及交互認證憑證。
3. 為內部資訊系統架構所需之憑證。
4. 線上憑證狀態查詢服務所使用之簽章憑證。

6.1.8 用戶金鑰產製設備

下屬憑證機構應使用 CNS 15135、ISO 19790 或 FIPS 140-2 等級 3 的硬體密碼模組。

6.2 私密金鑰保護措施及密碼模組工程控管

6.2.1 密碼模組標準

本憑證管理中心使用 CNS 15135、ISO 19790 或 FIPS 140-2 等級 3 硬體密碼模組來做為私密金鑰的保護設備，並具備多人控管功能。

6.2.2 私密金鑰分持控管

本憑證管理中心之私密金鑰是採 m-out-of-n 的方式由多人分持控管，為一種完全隱密(Perfect Secret)的秘密分享(Secret Sharing)方式，可做為私密金鑰安全備份及回復方法。採用此方法可使本憑證管理中心私密金鑰的多人控管具有最高的安全度。

保護私密金鑰相關資訊之智慧卡與個人通行密碼，分別由職務獨立之不同管理人員管控，並儲存於具安全管控措施之環境。

6.2.3 私密金鑰託管

本憑證管理中心之私密金鑰不可被託管，亦不提供下屬憑證機構私密金鑰託管服務。

6.2.4 私密金鑰的備份

(1) 本憑證管理中心之私密金鑰經加密後儲存於硬體密碼模組內，且依照 6.2.2 節以分持控管方法將私密金鑰加密後進行備份，並將加密金鑰分持資訊儲存於高安全性之智慧卡中。
(2) 儲存加密金鑰分持資訊之智慧卡，存放於經雙重控管之安全環境內，由安全控管人員密封保管。
(3) 加密金鑰之分持資訊至少保留 2 份，1 份存放於本憑證管理中心內之安全地點，另 1 份存放於具安全管控之異地備援地點。

6.2.5 私密金鑰歸檔

本憑證管理中心之私密金鑰不進行歸檔。

6.2.6 私密金鑰自密碼模組輸入或輸出

本憑證管理中心之私密金鑰是在硬體密碼模組中產生及儲存，並且只有在進行金鑰備份回復時，才能將私密金鑰輸入至另一個硬體密碼模組中；自密碼模組輸出時，依 6.2.4 節規定辦理。

6.2.7 私密金鑰儲存於密碼模組

本憑證管理中心之私密金鑰係以加密型態儲存於密碼模組。

6.2.8 私密金鑰啟動方式

儲存於密碼模組內的私密金鑰必須由 2 人以上之授權憑證主管人員，經身分鑑

別後啟動，啟動之方式係透過智慧卡鑑別憑證主管人員身分，且啟動之程序控管措施必須符合 5.2 節之規定。

6.2.9 私密金鑰停用方式

本憑證管理中心採離線作業方式，因此平常本憑證管理中心的金鑰對是處於停用(Deactivation)狀態，避免私密金鑰遭到非法使用。

私密金鑰在啟動後，其停用方式是將密碼模組以手動關閉或指定時間內無動作後自動登出成為停用狀態，以避免私密金鑰遭非法使用。

6.2.10 私密金鑰銷毀

本憑證管理中心在私密金鑰生命週期屆滿時將加以銷毀。因此，在私密金鑰生命週期屆滿後，將會把硬體密碼模組中存放之舊私密金鑰的記憶位置零值化(Zeroization)，以銷毀硬體密碼模組中舊的私密金鑰。

除了銷毀硬體密碼模組中之舊私密金鑰外，該舊私密金鑰之備份副本(保留三代)，也將於備份過期時進行實體銷毀，惟遇到必須以金鑰備份副本進行還原時，如還原之金鑰中有已過期之金鑰時，將立即進行刪除。

6.2.11 密碼模組等級

本憑證管理中心使用之硬體密碼模組等級，必須為 CNS 15135、ISO 19790 或 FIPS 140-2 等級 3。

6.3 金鑰對管理的其他事項

6.3.1 公開金鑰歸檔

本憑證管理中心所簽發憑證生命週期到期時，將會進行憑證歸檔，並將公開金鑰同時歸檔。

6.3.2 公開金鑰與私密金鑰的有效期限

本憑證管理中心公開金鑰與私密金鑰之有效期限相同。

本憑證管理中心及下屬憑證機構之公開金鑰與私密金鑰，依金鑰長度不同而有不同之有效期限，說明如下：

(1) RSA 2048 位元以上之金鑰對：有效期限至多為 30 年。

(2) RSA 4096 位元之金鑰對：有效期限至多為 50 年。
(3) ECC P-256 金鑰對：有效期限至多為 30 年。
(4) ECC P-384 金鑰對：有效期限至多為 50 年。

6.4 啟動資料

6.4.1 啟動資料產製及安裝

啟動簽章用私密金鑰的啟動資料由多張智慧卡個別產生，並使用多人控管的權限分離(Duty Separation)機制，智慧卡中的啟動資料由讀卡機存取，並以智慧卡的個人識別碼(以下簡稱 PIN 碼)做為啟動資料存取身分鑑別之用。

6.4.2 啟動資料的保護

啟動資料由控管智慧卡組保護，智慧卡的 PIN 碼由保管人員負責保存，不得記錄於任何媒體上，如登入的失敗次數超過 3 次，則鎖住此智慧卡；智慧卡移交時，新的保管人員必須重新設定新的 PIN 碼。

6.4.3 啟動資料的其他考量

無規定。

6.5 電腦安全控管

6.5.1 電腦安全技術需求

本憑證管理中心和相關輔助系統透過作業系統，或結合作業系統、軟體和實體的保護措施提供以下安全控管功能：

(1) 具備身分鑑別的登入。

(2) 提供自行定義存取控制。

(3) 提供安全稽核能力。

(4) 對於各種憑證服務和信賴角色存取控制的限制。

(5) 具備信賴角色及身分的識別和鑑別。

(6) 確保通訊和資料庫之安全。

(7) 具備信賴角色和相關身分識別的安全及可信賴的管道。

(8) 具備程序完整性及安全控管保護。

本憑證管理中心之安全控管亦須遵循「CA-Browser Forum NETWORK AND CERTIFCATE SYSTEM SECURITY REQUIREMENTS」之規範。

6.5.2 電腦系統安全等級

本憑證管理中心使用之電腦作業系統，其安全等級符合 TCSEC C2 或同等級國際安全標準。

6.6 生命週期技術控管

6.6.1 系統開發控管

本憑證管理中心的系統開發遵循 ISO/CNS 27001 的規範。

本憑證管理中心之硬體和軟體是專用的，僅能使用符合安全政策的元件，不安裝與運作無關的硬體裝置、網路連接或元件軟體，並且在每次使用時會檢查是否有惡意程式碼。

6.6.2 安全管理控管

本憑證管理中心的軟體在首次安裝時，將確認是由開發人員提供正確的版本且未被修改。系統安裝後，每次啟動時驗證軟體的完整性。

本憑證管理中心將記錄和控管系統的組態與功能變更。

6.6.3 生命週期的安全等級

無規定。

6.7 網路安全控管

本憑證管理中心憑證管理系統為離線、獨立之系統，且須經授權後由業務相關之作業人員才可以人工方式執行作業。為防範網路入侵與破壞，安裝及建置有防火牆、入侵防禦與防毒系統等，以增進網路安全。

本憑證管理中心的主機和內部資料庫不與外部網路連接，儲存庫連接到網際網

路(Internet)上，提供不中斷之憑證及憑證廢止清冊查詢服務(必要之維護或備援狀況除外)。

本憑證管理中心之儲存庫資料(如憑證廢止清冊)，採用手動離線方式更新公布。

本憑證管理中心的儲存庫透過系統修補程式的更新、系統弱點掃描、入侵防禦系統、防火牆系統等加以保護，以防範阻絕服務及入侵等攻擊。

6.8 時間戳記

無規定。

7.憑證、憑證廢止清冊及線上憑證狀態查詢剖繪

7.1 憑證剖繪

7.1.1 版本

本憑證管理中心之自簽憑證及簽發予下屬憑證機構之憑證版本為 X.509 v3。

7.1.2 憑證擴充欄位

擴充欄位之使用符合 IETF RFC 5280 標準。其憑證各欄位詳細內容請見本憑證管理中心憑證及憑證廢止清冊剖繪。

7.1.3 演算法物件識別碼

本憑證管理中心簽發憑證時使用的演算法物件識別碼如下：

演算法類型	演算法 (Algorithm)	物件識別碼(OID)
金鑰	rsaEncryption	{iso(1)member-body(2)us{840}rsadsi(113549)pkcs(1)pkcs-1(1)1}
金鑰	ecPublicKey	{iso(1)member-body(2)us(840)ansi-X-9-62(10045)keyType(2)ecPublicKey(1)}
簽章	sha1WithRSAEncryption	{iso(1)member-body(2)us{840}rsadsi(113549)pkcs(1)pkcs-1(1)5}
簽章	sha256WithRSAEncryption	{iso(1)member-body(2)us{840}rsadsi(113549)pkcs(1)pkcs-1(1)11}
簽章	ECDSAWithSHA256	{iso(1)member-body(2)us(840)ansi-X9-62(10045)signatures(4)ecdsa-with-SHA2(3)2}
簽章	ECDSAWithSHA384	{iso(1)member-body(2)us(840)ansi-X9-62(10045)signatures(4)ecdsa-with-SHA2(3)3}

7.1.4 識別名稱格式

本憑證管理中心及下屬憑證機構之憑證，其憑證主體與發行者名稱皆符合 X.500 唯一識別名稱(Distinguished Name； DN)之命名方式，此名稱的屬性型態遵循 RFC 5280 相關規定。

7.1.5 識別名稱限制

本憑證管理中心簽發之憑證，可視需要使用「名稱限制」(nameConstraints)擴

充欄位。

7.1.6 憑證政策物件識別代碼

本憑證管理中心所簽發之憑證，在憑證內的「憑證政策」(certificatePolicies)擴充欄位中，使用憑證政策所定義的憑證政策物件識別碼。

7.1.7 憑證政策限制擴充欄位的使用

本憑證管理中心所簽發之憑證可視需要包含「政策限制」(policyConstraints)擴充欄位。

7.1.8 憑證政策限定元語法與語意

本憑證管理中心所簽發之憑證皆可視需要包含「政策限定元」(policyQualifier)語法。

7.1.9 憑證政策擴充欄位語意必要的處理

無規定。

7.2 憑證廢止清冊剖繪

7.2.1 版本

本憑證管理中心簽發 X.509 v2 格式的憑證廢止清冊。

7.2.2 憑證廢止清冊與憑證廢止清冊擴充欄位

各欄位詳細內容請見本憑證管理中心憑證及憑證廢止清冊剖繪。

7.3 線上憑證狀態查詢剖繪

7.3.1 版本

本憑證管理中心之線上憑證狀態查詢使用 RFC 6960 v1 格式。

7.3.2 線上憑證狀態查詢擴充欄位

無規定。

8. 稽核及其他評估方法

8.1 稽核頻率或評估事項

本憑證管理中心至少每年各進行 1 次內部及外部稽核。

8.2 稽核人員之識別及資格

本憑證管理中心執行內部和外部稽核作業之稽核人員至少必須具備憑證機構、資訊系統安全稽核之知識，有 2 年以上之稽核相關經驗，且須熟悉本作業基準之運作規範，以及具有應用系統之作業及電腦硬軟體系統之相關知識與經驗。若主管機關就稽核人員之適任條件有相關規範時，以該規範為準據。

進行外部稽核作業時，應委託具專業能力之稽核業者，執行外部稽核之工作人員，應具有國家稽核人員正式資格或國際上認可之稽核資歷，並具有稽核之相關實務經驗，以提供公正客觀的稽核服務。本憑證管理中心於進行稽核時，應對稽核人員進行身分鑑別。

8.3 稽核者與受稽核者之關係

本憑證管理中心執行稽核作業之內部稽核人員與被稽核單位的權責為獨立分工，無任何利害關係足以影響稽核之客觀性，並以獨立、公正、客觀之態度執行查核評估。

本憑證管理中心之外部稽核作業，將委託稽核業者就本憑證管理中心之運作進行稽核。

8.4 稽核項目

稽核內容包括下列項目：

(1) 是否訂定與公告憑證實務作業基準及相關作業規範，包括依憑證實務作業基準所訂定之作業規範。
(2) 是否依照憑證實務作業基準及相關作業規範執行憑證管理等相關作業，以符合憑證服務之完整性及本憑證管理中心環境之安全控管等相關需求。
(3) 憑證實務作業基準是否符合憑證政策之規定。

8.5 稽核結果之因應

本憑證管理中心的運作經詳細查核評估後，若有不符合憑證實務作業基準的規範時，稽核者應依缺失嚴重等級詳細條列，將結果通知本憑證管理中心。

本憑證管理中心必須依缺失提出矯正與預防措施，並追蹤後續改善情形。

8.6 稽核結果之公開

本憑證管理中心將於儲存庫公布最近一次的外部稽核結果，但不包括會對本憑證管理中心造成安全疑慮之資訊。

9. 其他業務及法律規定

9.1 收費

不適用。

9.2 財務責任

9.2.1 賠償責任

(1) 本憑證管理中心處理下屬憑證機構註冊資料及憑證簽發作業，除可歸責於本憑證管理中心之故意或過失外，本憑證管理中心不負損害賠償責任。
(2) 如非為本憑證管理中心的故意或過失，或其他不可抗拒的天災事故〈例如地震等〉，致所簽發之憑證造成下屬憑證機構損失時，本憑證管理中心不負損害賠償責任。
(3) 本憑證管理中心如因作業人員故意或過失、未遵照本作業基準、憑證政策及相關作業規範的規定，辦理註冊、憑證的簽發與廢止作業，或違反相關法律規範而造成下屬憑證機構的損害時，本憑證管理中心應依規定賠償下屬憑證機構的直接損害；有關下屬憑證機構之最高賠償金額，將於本憑證管理中心與下屬憑證機構雙方之合約規定。
(4) 本憑證管理中心或其他有權者提出廢止下屬憑證機構憑證之要求後，至本憑證管理中心實際公布廢止該下屬憑證機構憑證(記載於憑證廢止清冊)為止之期間內，如因使用該下屬憑證機構憑證而產生法律糾紛時，本憑證管理中心如依據本作業基準與相關的作業規範執行處理作業者，則不負損害賠償責任。
(5) 下屬憑證機構使用非法假造、錯誤的憑證而造成損害時，本憑證管理中心不負損害賠償責任。
(6) 下屬憑證機構的損害賠償請求權時效期間，依相關法律的規範辦理。
(7) 本憑證管理中心有關財務運作的稽核作業，每年定期委由公正、客觀的第三機構執行財務運作的查核。
(8) 本憑證管理中心有關的風險管理，除已投保建築物與硬體設施的地震及火險外，為分散業務的營運風險，目前積極洽詢國內外相關的保險公司投保認證業務責任險。

9.2.2 其他資產

本憑證管理中心為本公司憑證業務之一員。本公司於完成保險作業之前，先行

提撥新台幣參仟萬元作為執行憑證業務時產生賠償責任風險的財務保證基金。

9.2.3 對用戶及信賴憑證者之賠償責任

用戶之賠償責任如 9.2.1 節之規定。

信賴憑證者除須遵守 9.6.4 節之義務外，如有違反本作業基準之規範或非可歸責於本憑證管理中心之過失時，本憑證管理中心不負損害賠償責任。

9.3 機密資訊

9.3.1 機密資訊的種類

機密資訊包括：

(1) 用於本憑證管理中心營運的私密金鑰及通行密碼。

(2) 控管本憑證管理中心私密金鑰之分持資料。

(3) 下屬憑證機構之申請資料。

(4) 本憑證管理中心產生或保管之可供稽核及追蹤之紀錄。

(5) 稽核人員於稽核過程中產生之稽核紀錄及文件。

(6) 列為機密等級的營運相關文件。

9.3.2 非機密資訊種類

憑證政策、本作業基準、本憑證管理中心簽發之憑證、本憑證管理中心簽發之憑證廢止清冊、外部稽核結果（但不包括會對本憑證管理中心造成安全疑慮之資訊）等皆為可公開之資訊。

9.3.3 保護機密資訊之責任

除非符合下列條件之一，否則下屬憑證機構之註冊基本資料與身分鑑別相關資料絕不任意提供予權責管理單位，或其他任何人知悉：

(1) 依法令之規定並經由權責管理單位依法定程序授權。

(2) 具管轄權之法院或仲裁機構處理因憑證產生之糾紛與仲裁，而依法定程序申請之要求或申請者。

9.4 個人資訊隱私

9.4.1 隱私保護計畫

本憑證管理中心依據我國個人資料保護法相關規範運作。

9.4.2 個人資訊隱私種類

依 9.4.1 之規定。

下屬憑證機構應保密之資訊種類，必須於其憑證實務作業基準或隱私權保密政策中訂定。

9.4.3 非個人資訊隱私種類

無規定。

9.4.4 個人資訊隱私保護責任

依相關法令規定辦理。

9.4.5 使用個人資訊隱私之告知與同意

依相關法令規定辦理。

9.4.6 因行政法令或司法要求之揭露

如 9.3.3 節之規定。

9.4.7 其他資訊公開情形

下屬憑證機構之相關資訊，必須由下屬憑證機構以書面文件提出申請，本憑證管理中心始得提供。若他人要求提供下屬憑證機構之相關資訊時，須經該下屬憑證機構書面授權同意，本憑證管理中心始得提供。

9.5 智慧財產權

(1) 本憑證管理中心產製之金鑰對及金鑰分持，其產出為本公司之智慧財產。

(2) 本憑證管理中心所簽發之憑證及憑證廢止清冊為本公司之智慧財產。

(3) 下屬憑證機構的金鑰對為該下屬憑證機構之智慧財產，但其公開金鑰經本憑證管理中心簽發成憑證時，該憑證為本公司之智慧財產。

(4) 本憑證管理中心將確保下屬憑證機構名稱之正確性，但不保證下屬憑證機構名稱之智慧財產權歸屬。

(5) 本憑證管理中心因執行憑證管理作業而撰寫的相關文件，其智慧財產權為本公司擁有。

(6) 本作業基準之智慧財產權由本公司擁有。

(7) 本作業基準可由本憑證管理中心儲存庫自由下載，或依著作權法相關規定散布。

(8) 散布本作業基準者，不得向他人收取費用。

(9) 本憑證管理中心對於不當使用或散布本作業基準所引發之一切結果，不負任何法律責任。

9.6 職責及義務

9.6.1 憑證機構之職責

(1) 本憑證管理中心必須善盡保管下屬憑證機構註冊資料、憑證資料及相關訊息之責任，避免相關資訊洩漏、被冒用、竄改及任意使用。

(2) 本憑證管理中心應依照憑證政策及憑證實務作業基準之規範，接受下屬憑證機構之憑證申請、憑證更新及憑證廢止訊息，確認下屬憑證機構發送至本憑證管理中心之相關訊息之正確性與完整性，並執行憑證簽發與憑證廢止之相關作業，及將相關回覆訊息正確及安全地遞送至下屬憑證機構。

(3) 本憑證管理中心執行下屬憑證機構憑證簽發時，必須鑑別下屬憑證機構申請文件與身分之正確性及合法性。

(4) 本憑證管理中心之私密金鑰有安全之顧慮時，本憑證管理中心必須立即告知下屬憑證機構。

(5) 本憑證管理中心簽發憑證時，須依照本作業基準之規範，將所簽發之憑證安全地遞送至儲存庫。

(6) 本憑證管理中心於廢止下屬憑證機構憑證時，應依照本作業基準之規範，產生憑證廢止清冊，並安全地遞送至儲存庫。

(7) 本憑證管理中心與下屬憑證機構簽訂合約前，應詳細說明憑證申請、更新、廢止與使用之作業規範，及相關之權利與義務關係。

(8) 本憑證管理中心簽發憑證與憑證廢止清冊之私密金鑰必須獨立使用，禁止與其他功能共用。如有其他訊息簽章與加密之需求時，必須使用不同之私密金鑰。

根據「CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates」基準要求，最高層憑證管理中心必須對下屬憑證管理中心的效能和保證負責，包含下屬憑證機構審查之以下內容：

- 使用網域或 IP 位址之權利：參考第 3.2.2 節內容。
- 申請憑證之授權：參考第 3.2.2 節內容。
- 資訊的正確性：參考第 3.2.2 節內容。
- 申請者的身分：參考第 3.2.2 節內容。

9.6.2 註冊中心之職責

因本憑證管理中心自行擔任註冊中心，故註冊中心之職責如 9.6.1 節之規定。

9.6.3 用戶之義務

本憑證管理中心之用戶為下屬憑證機構，其義務規範如下：

(1) 下屬憑證機構向本憑證管理中心申請憑證時，必須確實了解並同意申請書與合約書之權利與義務，及本作業基準等相關規範之內容。

(2) 下屬憑證機構私密金鑰有遺失或遭破解等不安全之顧慮時，或下屬憑證機構相關之資訊有異動時，下屬憑證機構必須依相關作業之規定，向本憑證管理中心辦理申告。

(3) 下屬憑證機構申請憑證時必須提供詳實且正確之資訊，接受本憑證管理中心簽發之下屬憑證機構憑證時，必須確認憑證內容之正確性，且公開金鑰與私密金鑰為成對之金鑰。

(4) 下屬憑證機構應妥善產製、保管及使用私密金鑰，並遵守對於金鑰及憑證之使用限制。

(5) 下屬憑證機構如發生廢止憑證之事由(如私密金鑰資料外洩或遺失)，應立即通知本憑證管理中心，並辦理憑證廢止相關作業，但下屬憑證機構仍應承擔憑證廢止狀態未被公布前因使用該憑證所致生之風險與責任。

(6) 本憑證管理中心如因故無法正常運作時，下屬憑證機構應儘速尋求其他途徑完成與他人應為之法律行為，不得以本憑證管理中心無法正常運作，作為抗辯他人之事由。

(7) 下屬憑證機構應存放其自身憑證及憑證廢止清冊等資料於安全的儲存庫內，確保儲存庫存取之可用性，提供信賴憑證者隨時查詢。

9.6.4 信賴憑證者義務

(1) 信賴憑證者應依照本憑證實務作業基準之規範，取得本憑證管理中心之自簽憑證及下屬憑證機構憑證。

(2) 信賴憑證者利用本憑證管理中心所提供之自簽憑證，進行憑證鏈之建立、驗證，以決定是否信任下屬憑證機構憑證。

(3) 信賴憑證者驗證憑證時應使用本憑證管理中心之自簽憑證，驗證下屬憑證機構憑證之數位簽章是否為本憑證管理中心之私密金鑰所簽署，並透過憑證廢止清冊驗證憑證狀態是否已遭廢止。

(4) 信賴憑證者在使用本憑證管理中心簽發之憑證廢止清冊時，應先驗證數位簽章，並檢查憑證廢止清冊記載之下次更新時間，如已超過下次更新時間，應取得最新憑證廢止清冊。

(5) 信賴憑證者應慎選安全的電腦環境及可信賴的應用系統，如因電腦環境或應用系統本身因素導致使用者權益受損時，信賴憑證者應自行承擔責任。

(6) 本憑證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，不得以本憑證管理中心無法正常運作，作為抗辯他人之事由。

(7) 信賴憑證者接受使用本憑證管理中心簽發之憑證時，即表示已了解並同意有關本憑證管理中心法律責任之條款，並依照本作業基準之規定範圍內信賴該憑證。

9.6.5 其他成員義務

無規定。

9.7 除外責任

(1) 本憑證管理中心處理下屬憑證機構註冊資料及憑證簽發作業，除可歸責於本憑證管理中心之故意或過失外，本憑證管理中心不負損害賠償責任。

(2) 本憑證管理中心如因不可抗力之天災事故（例如地震等），或其他非可歸責於本憑證管理中心之事由(例如戰爭等)，造成下屬憑證機構損失時，本憑證管理中心不負損害賠償責任。

(3) 本憑證管理中心未善盡保管下屬憑證機構之註冊及憑證相關資料，而造成相關資訊洩漏、被冒用、竄改及任意使用致造成第三者遭受損害時，本憑證管理中心應負損害賠償責任。

(4) 本憑證管理中心在收到憑證廢止申請後，最遲於 1 個工作日內完成憑證廢止作業，並於 1 天內簽發憑證廢止清冊及公告於儲存庫。下屬憑證機構於憑證廢止狀態未被公布之前，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。

9.8 責任限制

本憑證管理中心與下屬憑證機構，因簽發憑證或使用憑證而發生損害賠償事件時，雙方應承擔之損害賠償責任，以相關法令規定及合約所定之範圍為責任上限。

9.9 賠償

如 9.2.1 節之規定。

9.10 本文件生效與終止

9.10.1 生效

本作業基準於主管機關依電子簽章法核定通過後，於本憑證管理中心儲存庫公布後即生效。

9.10.2 終止

本作業基準新版本經主管機關核定後公布，現有版本即告終止。

9.10.3 終止及存續之效力

本作業基準之效力，維持至遵循本作業基準所簽發之最後一張憑證到期或廢止為止。

9.11 通知與聯絡方式

本憑證管理中心將以適當的方式，與下屬憑證機構建立聯絡管道，包括但不限以下方式：電話、傳真或 e-mail。

9.12 變更及公告

9.12.1 變更程序

(1) 本作業基準之權責管理單位為本憑證管理中心，每年至少檢視本作業基準 1 次。修訂方式包括以附加文件方式修訂或直接修訂本作業基準的內容。
(2) 如憑證政策修訂或物件識別碼變更時，本作業基準將配合修訂。
(3) 如因法律規範改變、國際標準更新等因素而須變更時，本作業基準亦將做相對應的變更。
(4) 本作業基準之修訂經主管機關審查核定後，將依照第三章規定公布於儲存庫。

9.12.2 變更聯絡機制

(1) 對本作業基準有建議更新時，請將詳細的建議文件郵寄或 E-mail 至 1.5.2 節的聯絡窗口，交由 TWCA 政策管理中心審議。
(2) 本作業基準之修訂經主管機關審查核定後，公布於本憑證管理中心之儲存庫供下載。
(3) 除另有規定外，本憑證管理中心以 9.11 節規定之方式，做為與下屬憑證機構間之變更聯絡機制。

9.12.3 物件識別碼變更條件

本作業基準引用之憑證政策物件識別碼，於本作業基準內容變更時不會更動，僅增加本作業基準之版本識別代碼。

9.13 爭議處理程序

下屬憑證機構對本憑證管理中心服務或其簽發憑證之使用如有爭議時，依以下規定辦理：

(1) 爭議之雙方應本誠信原則，於合理的方式下雙方盡力協商解決之。
(2) 爭議之雙方如無法於30日曆天內合理的協商解決爭議，則必須指派具適任能力的公正第三協調者，以進行協調並解決爭議，且雙方必須同意協調者的

協商與裁決。

(3) 爭議之雙方如無法於60日曆天內同意協調者的協商與裁決，雙方同意以臺北地方法院為第一審管轄法院。

(4) 於爭議協商、訴訟處理過程所發生的費用分擔，依據協商或相關的法律規範處理。

(5) 如遇跨國或跨區域之爭議，無法以上面的處理方式解決時，則必須依照相關的跨國或跨區域的糾紛仲裁規範處理。

9.14 政府管理法規

本作業基準訂定的內容與本憑證管理中心相關業務的執行與釋義，皆遵循主管機關之相關法律規定辦理，且遵循中華民國之相關法律規範。

9.15 法規之符合性

本作業基準及本憑證管理中心應符合電子簽章法及其相關子法之規定。

9.16 各項條款

9.16.1 完整合約

無規定。

9.16.2 轉讓

無規定。

9.16.3 存續性

本作業基準的某些章節規定有不適用而必須修正時,其他條文的規定仍屬有效,不受該項不適用之規定影響，直到新版之本作業基準更新完成並公告。

本作業基準之更新，依 9.12 節規定辦理。

9.16.4 施行

無規定。

9.16.5 不可抗力

如因不可抗力或其他不可歸責於本憑證管理中心之事由(例如戰爭或地震等)，本憑證管理中心不負損害賠償責任。

9.17 其他條款

無規定。

附錄一(Appendix 1) 詞彙(Glossary)

(1).網際網路(Internet)

許多不同的電腦網路相互連結，經過標準的通訊協定，得以相互交換資訊。

(2).(電子)訊息((Electronic)Message)

指文字、聲音、影像、符號或其他資料，以電子、磁性或人之知覺無法直接認識之方式，所製成足以表示其用意之紀錄，而供電子處理之用者。

(3).RSA 演算法(RSA Algorithm)

是一種非對稱加密演算法，由 Ron Rivest、Adi Shamir 和 Leonard Adleman 於 1977 年提出，其安全強度建構於針對大數做質因數分解的困難性上。

(4).橢圓曲線密碼學(Elliptic Curve Cryptography；ECC)

是一種基於橢圓曲線數學的公開密鑰加密演算法，由 Neal Koblitz 和 Victor Miller 於 1985 年提出，其安全強度建構於解決橢圓曲線離散對數問題的困難性上。

(5). ECC P-256 曲線 (ECC P-256 Curve)

採用 NIST FIPS 186-3 中所制定之橢圓曲線標準。

(6).電子簽章(Electronic Signature)

指以電子型式存在之資料訊息，依附在電子文件可用以辨識及確認電子文件簽署人身分及簽署人以數位、聲音、指紋、或其他生物光學技術的特性產生的訊息，其依附在電子訊息上，具有與簽名同等的效力，可用以辨識及確認電子文件簽署人的身分，及辨識簽署訊息的完整性。

(7).加密(Encrypt/Encipher)

指利用數學演算法或其他方法，將電子文件以亂碼方式處理，以確保資料傳輸的安全。

(8).解密(decrypt/Decipher)

將經加密後形成人無法辨識其代表意義的訊息，以相關的數學演算法或其他方法將該訊息還原為人可以辨識其代表意義的訊息。

(9).數位簽章(Digital Signature)

數位簽章為電子簽章的一種，係指採用非對稱型的密碼演算法(Asymmetric Cryptosystem)及雜湊函數(Hash Function)，對一定長度的數位訊息壓縮後再以簽署人的私密金鑰予以加密，其相對應的公開金鑰可以驗證此加密後的數位訊息，形成一可供辨識簽署人身分及電子文件真偽之資料訊息。

(10).私密金鑰(Private Key)

指用以製作及驗證數位簽章具有配對關係之一組數位資料而由簽署人保有者，該數位資料除作為製作數位簽章之用外，尚可用作電子訊息解密之用。

(11).公開金鑰(Public Key)

於非對稱型密碼演算法之數位簽章，指用以製作及驗證數位簽章之一組具有配對關係之數位資料中對外公開者；其可用以執行驗證簽署人簽章過的訊息資料的正確性，於執行訊息隱密性功能時可以將傳遞訊息加密。

(12).<公開金鑰>憑證或電子憑證(<Public Key>Certification or Certificate)

一筆以電腦為媒介基礎由憑證機構簽發之數位式的紀錄，內含申請者的註冊識別名稱、公開金鑰、該公開金鑰的有效期限、憑證機構的註冊識別名稱與簽章，及其他用以識別的相關訊息，用以確認簽署人之身分，並證明其擁有相配對之公開金鑰及私密金鑰。

(13).認證中心/憑證機構 (Certification Authority or Certificates Authority；CA)指提供數位簽章製作及電子認證服務之機構，亦即係指居於公正客觀地位，查驗憑證申請人身分資料之正確性，及其與待驗證公開金鑰及私密金鑰間之關連性與合法性，並據以簽發公開金鑰憑證之單位。

(14).憑證實務作業基準 (Certification Practice Statement；CPS)

憑證機構向所服務的對象公告其執行憑證簽發、廢止、查詢等管理的作業規範及申請程序，內含憑證運作的公開金鑰架構與安全機制、作業規範與程序、憑證機構軟硬體施行的安全機制、權責的管理及相關的規範。

(15).非對稱型的密碼演算法(亂碼系統)(Asymmetric Cryptosystem)

以電腦為媒介基礎的一種數學演算法，可以產生及使用一組數學運算上相關連的安全金鑰對。其中私密金鑰用以對訊息作簽章，對應的公開金鑰則用以對簽章後的訊

息作驗證；公開金鑰亦可用以對訊息作加密，而對應的私密金鑰則用以對加密後的訊息作解密。

(16).雜湊函數(Hash Function)

一種可以將一長串的位元訊息轉換成固定長度位元訊息的數學演算法。相同的訊息輸入經由壓縮函數運算產生輸出結果必定相同，且決無法由輸出產生的結果推算出輸入的訊息。

(17).簽發憑證(電子認證)(Issue a Certificate)

係指認證中心(憑證機構)依憑證實務作業基準，審驗公開金鑰憑證申請人之身分資格、相關文件，並驗證其公開金鑰及私密金鑰之配對關係後，簽發公開金鑰憑證或其他憑證。

(18).實體銷毀

係指備份金鑰以光碟片方式備份存放，過期時，將光碟片剪碎。

(19)公正第三方稽核人員

係指會計師事務所之會計師。

附錄二(Appendix 2) 名詞與簡稱(Acronyms and Abbreviations)

AICPA American Institute of Certified Public Accountants, Inc.

ANS American National Standard

CA Certification Authority

CC Common Criteria

CCITSE Common Criteria for Information Technology Security Evaluation

CP Certificate Policy

CPS Certification Practice Statement

CRL Certificate Revocation List

DN Distinguished Name

ECC Elliptic Curve Cryptography

FIPS Federal Information Processing Standard

ISO/IEC the International Organization for Standardisation, The International Electrotechnical Commission

ITSEC Information Technology Security Evaluation Criteria

LDAP Lightweight Directory Access Protocol

OCSP Online Certificates Status Protocol

OID Object Identifier

OECD Organization for Economic Co-operation and Development

PMA Policy Management Authority

PIN Personal Identification number

PKCS Public Key Cryptography Standard

PKI	Public Key Infrastructure
RA	Registration Authority
RCA	Root Certification Authority
RSA	Rivest,Shamir,Adleman(encryption algorithm)
TCSEC	Trusted Computer System Evaluation Criteria
URL	Universal Resources Location