# 臺灣網路認證股份有限公司

# 網路安全憑證管理中心

# 憑證政策及憑證實務作業基準

# (TWCA CYBER CA CP/CPS)

(第 2.2 版)

生效日期：中華民國 115 年 7 月 20 日

Effective Date：2026/07/20

# 版本變更紀錄

| 版本 | 修訂日期 | 修訂說明 |
|---|---|---|
| 1.0 | 民國 111 年 10 月 30 日 | 初版。 |
| 1.1 | 民國 113 年 2 月 29 日 | 調整 7.1.2.2、7.1.2.3 及 7.1.4.3.1。 |
| 2.0 | 民國 114 年 4 月 9 日 | 遵循新版電子簽章法之「數位簽章憑證實務作業基準應載明事項」進行修訂 |
| 2.1 | 民國 114 年 12 月 15 日 | 3.2.2 增加審驗紀錄效期說明<br>3.2.2.4 新增/移除網域驗證方式並增加 MPIC 要求<br>3.2.2.4 增加 DNSSEC 要求<br>3.2.2.5 增加 MPIC 要求<br>3.2.2.8 增加 MPIC 以及 DNSSEC 要求<br>3.2.2.9 增加 MPIC 要求<br>3.3.1、6.3.2 增加憑證效期限制<br>5.7.1.2 增加憑證大規模廢止計畫說明<br>7.1.4.3.1 將憑證名稱表格化 |
| 2.2 | 民國 115 年 7 月 20 日 | CP/CPS 合併。<br>1.1 增加國際規範符規聲明。<br>3.2.2 移除未使用驗證方式，增列長效驗證方法並將其表格化方便閱讀。<br>4.1、4.3、4.7、4.9 增加 ACME 自動化作業。<br>5.2 增加開發人員角色。<br>6.7 增加漏洞回應與修補時程。 |

# 目錄

摘要.....11
1. 簡介.....14
1.1 概述.....14
1.2 文件名稱及識別.....14
1.2.1 版本異動紀錄.....15
1.3 成員及適用範圍.....15
1.3.1 憑證管理中心.....16
1.3.1.1 最高層憑證管理中心.....16
1.3.1.2 用戶憑證管理中心.....17
1.3.1.3 政策管理中心.....17
1.3.2 註冊中心.....17
1.3.3 用戶.....17
1.3.4 信賴憑證者.....17
1.3.5 其他參與者.....18
1.4 憑證用途.....19
1.4.1 憑證之適用範圍.....19
1.4.2 憑證之禁止使用情形.....20
1.5 政策管理.....20
1.5.1 管理單位.....20
1.5.2 聯絡窗口.....20
1.5.3 憑證實務作業基準之核定.....21
1.5.4 憑證實務作業基準核定程序.....21
1.6 名詞定義與縮寫.....21
2. 公布及儲存庫.....22
2.1 儲存庫.....22
2.2 憑證資訊之公布.....22
2.3 公布頻率.....22
2.4 儲存庫之存取控制.....23
3. 識別與鑑別.....24
3.1 命名.....24
3.1.1 名稱種類.....24
3.1.2 識別名稱之意義.....24
3.1.3 用戶之匿名與假名.....24

3.1.4 各種名稱的解釋規則.....24
3.1.5 名稱的唯一性.....24
3.1.6 商標之辨識、鑑別及角色.....25
3.2 初始驗證.....25
3.2.1 證明擁有私密金鑰的方式.....25
3.2.2 組織身分與網域的鑑別.....25
3.2.2.1 組織鑑別程序.....26
3.2.2.2 行號鑑別程序.....27
3.2.2.3 國名識別.....27
3.2.2.4 網域主機名稱鑑別程序.....27
3.2.2.5 IP 位址查驗.....29
3.2.2.6 萬用網域驗證.....30
3.2.2.7 資訊來源準確性.....30
3.2.2.8 授權憑證機構簽發紀錄.....30
3.2.2.9 多視角驗證.....30
3.2.3 個人用戶身分的鑑別.....31
3.2.4 未驗證之用戶資訊.....31
3.2.5 權責之確認.....31
3.2.6 相互溝通方式.....31
3.3 金鑰更新之識別與鑑別.....31
3.3.1 憑證例行性金鑰更新.....31
3.3.2 憑證廢止後之金鑰更新.....32
3.4 憑證廢止請求.....32
4. 憑證生命週期管理.....33
4.1 憑證申請.....33
4.1.1 憑證申請者.....33
4.1.2 註冊申請程序及責任.....33
4.2 憑證申請程序.....33
4.2.1 識別與鑑別程序.....33
4.2.2 接受或拒絕憑證申請.....35
4.2.3 憑證申請處理時間.....36
4.3 憑證簽發.....36
4.3.1 憑證機構簽發憑證.....36
4.3.2 憑證機構簽發憑證通知用戶.....38

4.4 憑證接受.....38
4.4.1 憑證接受之程序.....38
4.4.2 憑證機構公布憑證.....38
4.4.3 憑證機構通知其他機構憑證簽發.....38
4.5 金鑰對及憑證用途.....38
4.5.1 用戶私密金鑰及憑證的使用.....38
4.5.2 信賴憑證者使用公開金鑰及憑證.....39
4.6 憑證展期.....39
4.7 憑證更新.....39
4.7.1 憑證更新之事由.....40
4.7.2 有權更新憑證者.....40
4.7.3 憑證更新程序.....40
4.7.4 憑證更新簽發之通知.....41
4.7.5 更新後憑證接受之程序.....41
4.7.6 憑證機構公布更新憑證.....41
4.7.7 更新憑證後對其他機構之通知.....41
4.8 憑證變更.....41
4.9 憑證廢止及暫時停用.....41
4.9.1 憑證廢止之事由.....41
4.9.1.1 廢止用戶憑證之事由.....41
4.9.1.2 廢止下屬憑證機構憑證之事由.....42
4.9.2 有權請求廢止憑證者.....43
4.9.3 憑證廢止程序.....43
4.9.4 憑證廢止請求提出期限.....44
4.9.5 憑證機構處理憑證廢止請求時限.....44
4.9.6 信賴憑證者憑證廢止驗證規定.....44
4.9.7 憑證廢止清冊簽發頻率.....45
4.9.8 憑證廢止清冊最大潛在因素.....45
4.9.9 線上憑證廢止/狀態查詢服務.....45
4.9.10 線上廢止/狀態查詢驗證規定.....45
4.9.11 其他形式之廢止公告.....45
4.9.12 金鑰遭破解之特殊規定.....45
4.9.13 憑證暫時停用之事由.....46
4.9.14 有權請求憑證暫時停用者.....46

4.9.15 憑證暫時停用程序.....46
4.9.16 憑證暫時停用期間限制.....46
4.10 憑證狀態服務.....47
4.10.1 服務特性.....47
4.10.2 服務之可用性.....47
4.10.3 附加功能.....47
4.11 憑證終止使用.....47
4.12 金鑰託管及復原.....47
4.12.1 金鑰託管及復原政策與施行.....47
4.12.2 加密期間金鑰封裝及復原政策與施行.....47
5. 實體、管理及作業流程控管.....48
5.1 實體控管.....48
5.1.1 建築物與位置.....48
5.1.2 實體進出管制.....48
5.1.3 電力與空調.....48
5.1.4 防水處理.....49
5.1.5 防火.....49
5.1.6 媒體儲存.....49
5.1.7 廢棄處理.....49
5.1.8 異地備援.....49
5.2 作業程序控管.....50
5.2.1 信賴角色.....50
5.2.2 作業人員需求人數.....50
5.2.3 角色的識別與鑑別.....50
5.2.4 角色隔離.....51
5.3 人員控管.....51
5.3.1 背景、適任條件與經歷.....51
5.3.2 背景審核程序.....51
5.3.3 教育訓練.....52
5.3.4 教育訓練的頻率與需求.....52
5.3.5 職務的輪調.....52
5.3.6 非授權作業的處罰.....52
5.3.7 委外人員需求.....53
5.3.8 作業文件需求.....53

5.4 稽核紀錄程序.....53
5.4.1 事件紀錄類型.....53
5.4.2 紀錄處理頻率.....56
5.4.3 稽核紀錄保留期限.....56
5.4.4 稽核紀錄的保護.....57
5.4.5 稽核紀錄備份程序.....57
5.4.6 稽核紀錄彙整系統.....57
5.4.7 對引發事件者之告知.....57
5.4.8 脆弱性評鑑.....57
5.5 紀錄歸檔.....58
5.5.1 歸檔紀錄類型.....58
5.5.2 歸檔紀錄保存期限.....58
5.5.3 歸檔紀錄的保護.....59
5.5.4 歸檔紀錄的備份程序.....59
5.5.5 歸檔紀錄之時戳要求.....59
5.5.6 歸檔紀錄彙整系統.....59
5.5.7 取得及驗證歸檔紀錄之程序.....59
5.6 金鑰更新.....60
5.6.1 用戶金鑰更新.....60
5.6.2 用戶憑證管理中心金鑰更新.....60
5.6.3 最高層憑證管理中心金鑰更新.....61
5.7 金鑰遭破解及災變復原程序.....61
5.7.1 事故及金鑰遭破解之緊急應變處理程序.....61
5.7.1.1 事故應變與災變復原計畫.....61
5.7.1.2 憑證大規模廢止計畫.....62
5.7.2 電腦資源、軟體及資料損毀之處理程序.....62
5.7.3 金鑰遭破解之處理程序.....62
5.7.4 災變後之營運持續能力.....63
5.8 憑證機構終止服務.....63
6. 技術安全控管.....64
6.1 金鑰對的產製及安裝.....64
6.1.1 金鑰對的產生.....64
6.1.2 私密金鑰遞送至用戶.....64
6.1.3 公開金鑰遞送至憑證簽發者.....64

6.1.4 憑證機構公開金鑰遞送至信賴憑證者.....64
6.1.5 金鑰長度.....65
6.1.6 公開金鑰參數的產生及參數品質檢驗.....65
6.1.7 金鑰使用目的.....65
6.1.8 用戶金鑰產製設備.....65
6.2 私密金鑰保護措施及密碼模組工程控管.....65
6.2.1 密碼模組標準.....65
6.2.2 私密金鑰分持控管.....66
6.2.3 私密金鑰託管.....66
6.2.4 私密金鑰的備份.....66
6.2.5 私密金鑰歸檔.....66
6.2.6 私密金鑰自密碼模組輸入或輸出.....66
6.2.7 私密金鑰儲存於密碼模組.....66
6.2.8 私密金鑰啟動方式.....67
6.2.9 私密金鑰停用方式.....67
6.2.10 私密金鑰銷毀.....67
6.2.11 密碼模組等級.....67
6.3 金鑰對管理的其他事項.....67
6.3.1 公開金鑰歸檔.....67
6.3.2 公開金鑰與私密金鑰的有效期限.....67
6.4 啟動資料.....68
6.4.1 啟動資料產製及安裝.....68
6.4.2 啟動資料的保護.....68
6.4.3 啟動資料的其他考量.....68
6.5 電腦安全控管.....68
6.5.1 電腦安全技術需求.....68
6.5.2 電腦系統安全等級.....69
6.6 生命週期技術控管.....69
6.6.1 系統開發控管.....69
6.6.2 安全管理控管.....69
6.6.3 生命週期安全控管.....69
6.7 網路安全控管.....70
6.8 時間戳記.....70
7. 憑證、憑證廢止清冊及線上憑證狀態查詢剖繪.....71

7.1 憑證剖繪.....71
7.1.1 版本.....71
7.1.2 憑證擴充欄位.....71
7.1.2.1 用戶憑證.....71
7.1.2.2 所有憑證.....72
7.1.2.3 RFC 5280 的應用.....72
7.1.3 演算法物件識別碼.....72
7.1.3.1 金鑰演算法.....72
7.1.3.2 簽章演算法.....73
7.1.4 識別名稱格式.....73
7.1.4.1 名稱編碼.....73
7.1.4.2 用戶憑證之主體資訊.....74
7.1.4.2.1 主體名稱擴充欄位.....74
7.1.4.2.2 主體唯一識別名稱欄位.....75
7.1.4.3 CA 憑證之主體資訊.....75
7.1.4.3.1 主體唯一識別名稱欄位.....75
7.1.5 識別名稱限制.....76
7.1.6 憑證政策物件識別碼.....76
7.1.6.1 受保留的憑證政策物件識別碼.....76
7.1.6.2 最高層憑證管理中心自身憑證.....77
7.1.6.3 用戶憑證管理中心憑證.....77
7.1.6.4 用戶憑證.....78
7.1.7 憑證政策限制擴充欄位的使用.....78
7.1.8 憑證政策限定元語法與語意.....79
7.1.9 憑證政策擴充欄位語意必要的處理.....79
7.2 憑證廢止清冊剖繪.....79
7.2.1 版本.....79
7.2.2 憑證廢止清冊與憑證廢止清冊擴充欄位.....79
7.3 線上憑證狀態查詢.....81
7.3.1 版本.....81
7.3.2 線上憑證狀態查詢擴充欄位.....82
8. 稽核及其他評估方法.....83
8.1 稽核頻率或評估事項.....83
8.2 稽核人員之識別及資格.....83

8.3 稽核者與受稽核者之關係.....83
8.4 稽核項目.....83
8.5 稽核結果之因應.....84
8.6 稽核結果之公開.....84
8.7 內部稽核.....84
9. 其他業務及法令規定.....85
9.1 收費.....85
9.1.1 憑證簽發及更新費用.....85
9.1.2 憑證查詢費用.....85
9.1.3 憑證廢止及狀態查詢費用.....85
9.1.4 其他服務費用.....85
9.1.5 退費.....85
9.2 財務責任.....85
9.2.1 保險範圍.....85
9.2.2 其他資產.....85
9.2.3 對用戶及信賴憑證者之賠償責任.....86
9.3 機密資訊.....86
9.3.1 機密資訊的種類.....86
9.3.2 非機密資訊種類.....87
9.3.3 保護機密資訊之責任.....87
9.4 個人資訊隱私.....87
9.4.1 隱私保護計畫.....87
9.4.2 個人資訊隱私種類.....87
9.4.3 非個人資訊隱私種類.....87
9.4.4 個人資訊隱私保護責任.....87
9.4.5 利用個人資訊隱私之告知與同意.....87
9.4.6 因行政法令或司法要求之揭露.....88
9.4.7 其他資訊公開情形.....88
9.5 智慧財產權.....88
9.6 職責及義務.....88
9.6.1 憑證機構之職責.....88
9.6.2 註冊機構之職責.....89
9.6.3 用戶之義務.....89
9.6.4 信賴憑證者義務.....90

9.6.5 其他成員義務.....91
9.7 除外責任.....91
9.8 責任限制.....91
9.9 賠償.....91
9.10 本文件生效與終止.....92
9.10.1 生效.....92
9.10.2 終止.....92
9.10.3 終止及存續之效力.....92
9.11 通知與聯絡方式.....92
9.12 變更及公告.....92
9.12.1 變更程序.....92
9.12.2 變更聯絡機制.....92
9.12.3 物件識別碼變更條件.....93
9.13 爭議處理程序.....93
9.14 政府管理法規.....93
9.15 法規之符合性.....93
9.16 各項條款.....94
9.16.1 完整合約.....94
9.16.2 轉讓.....94
9.16.3 可分割性.....94
9.16.4 施行.....94
9.16.5 不可抗力.....94
9.17 其他條款.....94
附錄一 詞彙(Glossary).....95
附錄二 名詞與簡稱(Acronyms and Abbreviations).....100

# 摘要

臺灣網路認證公司網路安全憑證管理中心憑證政策及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頒布之「數位簽章憑證實務作業基準應載明事項」規範編撰。經審查後核定之文號為：

**民國 115 年 7 月 20 日 數位發展部函 數授產經字第 1150005460 號**

## 2. 簽發之憑證

臺灣網路認證公司網路安全憑證管理中心(以下簡稱本憑證管理中心)簽發之憑證，係簽發給用戶之網域主機，供信賴憑證者識別該主機名稱及管理單位，做為網域主機身分鑑別之憑證。憑證種類包括「SSL 憑證」與「EVSSL 憑證」，若無特別說明，則本文中所指的「用戶憑證」包含上述兩種憑證。

(1) 憑證種類及適用範圍：

| 憑證種類 | 適用範圍 |
|---|---|
| SSL 憑證 | 用於保護線上通訊安全，降低資訊被惡意截取或竄改的風險，透過組織驗證以及網域驗證，提供網站主機身分鑑別(Server Authentication)，確保使用者連線至真實合法的伺服器，適用於需要高安全的網路環境，例如網際網路環境之電子商務網站。 |
| EVSSL 憑證 | 用於保護線上通訊安全，降低資訊被惡意截取或竄改的風險，透過更強化的組織驗證以及網域驗證，提供網站主機身分鑑別(Server Authentication)，確保使用者連線至真實合法的伺服器，適用於需要極高安全的網路環境，例如網際網路環境之金融交易網站。 |
| 說明：<br>SSL 憑證在國際上定義有四種不同等級：由高至低依序為 EV(Extended-Validation)、OV(Organization-Validated)、DV(Domain-Validated)、IV(Individual-Validated)，本憑證管理中心簽發之「SSL 憑證」屬於 OV 等級憑證，而「EVSSL 憑證」屬於 EV 等級憑證，本憑證管理中心不簽發 DV 及 IV 等級憑證，特此說明。 | |

(2) 本憑證管理中心簽發之用戶憑證，其 EKU(extended key usage)延伸欄位僅具有以下用途：

- id-kp-serverAuth 及 id-kp-clientAuth；或
- id-kp-serverAuth

本憑證管理中心依據本作業基準規範所簽發的用戶憑證，其申請者須通過本憑證管理中心規定之「組織鑑別程序」及「網域鑑別程序」(「網域主機名稱鑑別程序」或「IP 位址查驗」)，以確認該申請者之身分真確且擁有該主機名稱之擁有權。以本憑證管理中心之公開金鑰驗證網域主機之憑證，可用來驗證本憑證管理中心與網域主機間的相互信賴關係；若驗證憑證之數位簽章正確，則可確認該網域主機之憑證確由本憑證管理中心所簽發，且其所記載於憑證之名稱識別資訊有效，已經通過本憑證管理中心之註冊中心之初始驗證程序。

## 3. 法律責任重要事項

(1) 用戶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，但用戶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用戶註冊資料及憑證簽發作業，除未遵照本作業基準之規定辦理，或違反相關法律規章之規定，或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(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)，造成用戶損失時，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用戶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，應於 24 小時內進行調查與初步回覆，且從收到請求到廢止完成的時間範圍不得超過 4.9.1.1 節之規定；並於憑證廢止作業完成後依據 4.9.7 節規定之頻率簽發憑證廢止清冊及公告於儲存庫。用戶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。有關廢止作業規範請參閱 4.9 節。

(6) 本憑證管理中心與用戶，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，並依本作業基準之規定範圍內信賴該憑證。

## 4. 其他重要事項

(1) 用戶之私密金鑰有遺失或遭破解等不安全之顧慮時，或用戶相關之資訊有異動時，必須依相關作業之規定，向本憑證管理中心辦理申告。

(2) 用戶應妥善產製、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) 用戶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) 信賴憑證者驗證憑證時應使用最高層憑證管理中心之自簽憑證，驗證用戶憑證管理中心憑證之數位簽章；並以用戶憑證管理中心之憑證，驗證用戶憑證之數位簽章是否為用戶憑證管理中心之私密金鑰所簽發；並透過憑證廢止清冊或 OCSP 驗證憑證狀態是否已遭廢止。

(5) 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。

(6) 本公司於 96 年 9 月取得資訊安全管理系統 ISO 27001 證書，持續維持有效，並於 113 年 6 月進行轉版，取得 ISO 27001：2022 證書。

(7) 本公司於 102 年 11 月取得個人資訊管理系統 BS 10012 證書。於 107 年 7 月進行轉版 BS 10012:2017，並同時取得隱私資訊管理系統 ISO 27701，持續維持有效至今。

(8) 本公司於 109 年 12 月取得資訊服務管理系統 ISO 20000-1 證書，持續維持有效至今。

(9) 本公司於 110 年 11 月取得營運持續管理系統 ISO 22301 證書，持續維持有效至今。

(10) 本憑證管理中心至少每季進行 1 次內部稽核，並每年自行委託會計師事務所進行至少 1 次外部稽核，以確保其運作符合憑證實務作業基準與憑證政策之規定。有關稽核作業的詳細規範，請參閱第 8 章。

# 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、臺灣集保決算所、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網路安全憑證管理中心憑證政策及憑證實務作業基準(TWCA CYBER Certification Authority Certificate Policy and Certification Practice Statement；以下簡稱本作業基準)，係根據本國主管機關頒布之「數位簽章憑證實務作業基準應載明事項」所訂定。主要為說明臺灣網路認證股份有限公司網路安全憑證管理中心(以下簡稱本憑證管理中心)，如何進行憑證簽發及管理作業。

除本國法令外，本憑證管理中心為確保簽發之憑證具備全球通用之信賴性，並致力於維護網際網路通訊安全與使用者信任，明確聲明遵守下列國際規範及各瀏覽器根憑證政策之最新規定：

- CA/瀏覽器論壇 (CA/Browser Forum)：最新版之 Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates(以下簡稱 BR)及 Guidelines for the Issuance And Management of Extended Validation Certificates(以下簡稱 EVG) ，該規範公布於 http://www.cabforum.org。
- 各瀏覽器政策：包括但不限於 Chrome Root Program Policy、Mozilla Root Store Policy、Apple Root Program 及 Microsoft Trusted Root Program。
- CCADB 政策：遵守由多家瀏覽器廠商共同維護之通用 CA 資料庫 (Common CA Database, CCADB) 政策要求。

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，且能確實鑑別網域主機名稱及其所屬法人或組織之身分供信賴憑證者識別，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)，簽發憑證予用戶憑證管理中心，再由用戶憑證管理中心簽發憑證予用戶。

## 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網路安全憑證管理中心憑證政策及憑

證實務作業基準」。本憑證管理中心使用之憑證政策識別碼請參閱 7.1.6 節。

### 1.2.1 版本異動紀錄

本作業基準遵守並符合 BR 與 EVG 規範，本公司定期檢閱該規範，並至少每年修訂本作業基準一次；除此之外，如有本作業基準與該規範或本國法令有不符之處時，本公司將進行修訂或視情況向 CA/Browser Forum 提出異議。歷次版本異動紀錄參閱本作業基準之「版本變更紀錄」章節。

## 1.3 成員及適用範圍

本憑證管理中心包含以下成員：

(1) 憑證管理中心(Certification Authority，簡稱 CA)。

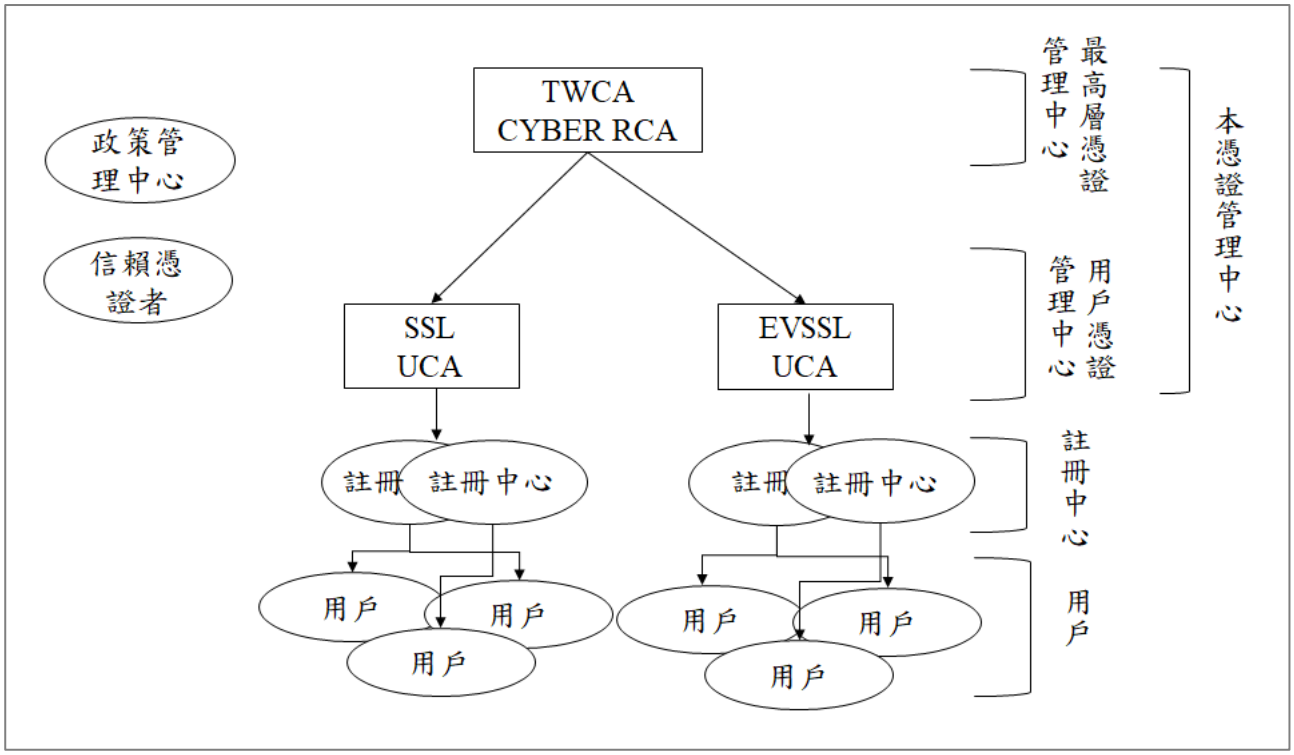
(2) 註冊中心(Registration Authority，簡稱 RA)。

(3) 用戶(Subscriber)。

(4) 信賴憑證者(Relying Party)。

(5) 政策管理中心(Policy Management Authority，簡稱 PMA)。

憑證管理中心依階層及用途分為「最高層憑證管理中心」(Root CA，簡稱 RCA)與「用戶憑證管理中心」(User CA，簡稱 UCA)，統稱「本憑證管理中心」。成員關係圖如下：




本作業基準將於第三、第四章說明本憑證管理中心如何進行用戶憑證之簽發及管理作業、用戶與信賴憑證者如何申請與使用憑證；於第五章說明最高層憑證管理中心與用戶憑證管理中心之管理準則。

### 1.3.1 憑證管理中心

#### 1.3.1.1 最高層憑證管理中心

最高層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) 負責用戶憑證管理中心憑證之簽發與管理；不可簽發用戶憑證。

(2) 管理與公告用戶憑證管理中心之憑證、憑證廢止清冊(Certificates Revocation List；CRL)於儲存庫。

(3) 提供線上憑證狀態查詢(Online Certificate Status Protocol；OCSP)服務。

(4) 維持儲存庫的穩定與運作。

(5) 建置於獨立、安全控管的作業環境下，由二位以上經授權的執行人員進行公開金鑰的產生、建置與簽發用戶憑證管理中心憑證的作業。RCA 的憑證為自簽憑證，當新產生或更新憑證時，必須以最迅速且適當之管道遞送予使用者或通知使用者至最高

層憑證管理中心索取。

#### 1.3.1.2 用戶憑證管理中心

用戶憑證管理中心由本公司負責營運及管理，主要負責以下工作：

(1) 負責用戶憑證之簽發與管理。

(2) 管理與公告用戶憑證、用戶憑證之憑證廢止清冊(CRL)於儲存庫。

(3) 提供線上憑證狀態查詢(OCSP)服務。

(4) 維持儲存庫的穩定與運作。

#### 1.3.1.3 政策管理中心

「臺灣網路認證股份有限公司」政策管理中心(Policy Management Authority，簡稱 PMA)為設於本公司內部之組織並負責制定下列事項：

(1) 憑證政策及憑證實務作業基準(CP/CPS)。

(2) 營運規範。

### 1.3.2 註冊中心

註冊中心(Registration Authority；RA)主要負責驗證申請者(用戶)的身分及簽發憑證所需之相關資訊，供本憑證管理中心作為簽發用戶憑證之依據。

本憑證管理中心自行設置註冊中心，不委派給第三方擔任註冊中心。

### 1.3.3 用戶

用戶為憑證主體(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申請憑證之法人或組織。

### 1.3.4 信賴憑證者

信賴憑證者係以本憑證管理中心憑證內之公開金鑰，驗證本憑證管理中心用戶憑證之數位簽章訊息有效性之個體。

信賴憑證者依據用戶憑證所記載之身分資訊，用以識別網域主機名稱及其所屬法人或組織之資訊。

信賴憑證者應以本憑證管理中心簽發之憑證所記載之資訊，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 憑證之適用範圍

本憑證管理中心所簽發予用戶之憑證，主要用於網站認證，確保網域主機之身分真確，並與連線端建立安全之加密傳輸通道。憑證種類及適用範圍如下：

| 憑證種類 | 適用範圍 |
|---|---|
| SSL 憑證 | 用於保護線上通訊安全，降低資訊被惡意截取或竄改的風險，透過組織驗證以及網域驗證，提供網站主機身分鑑別(Server Authentication)，確保使用者連線至真實合法的伺服器，適用於需要高安全的網路環境，例如網際網路環境之電子商務網站。 |
| EVSSL 憑證 | 用於保護線上通訊安全，降低資訊被惡意截取或竄改的風險，透過更強化的組織驗證以及網域驗證，提供網站主機身分鑑別(Server Authentication)，確保使用者連線至真實合法的伺服器，適用於需要極高安全的網路環境，例如網際網路環境之金融交易網站。 |
| 說明：<br>SSL 憑證在國際上定義有四種不同等級：由高至低依序為 EV(Extended-Validation)、OV(Organization-Validated)、DV(Domain-Validated)、IV(Individual-Validated)，本憑證管理中心簽發之「SSL 憑證」屬於 OV 等級憑證，而「EVSSL 憑證」屬於 EV 等級憑證，本憑證管理中心不簽發 DV 及 IV 等級憑證，特此說明。 | |

本憑證管理中心簽發之用戶憑證，其 EKU(extended key usage)延伸欄位僅具有以下用途：

(1) id-kp-serverAuth 及 id-kp-clientAuth；或

(2) id-kp-serverAuth

本憑證管理中心依據本作業基準規範簽發用戶憑證，其申請者須通過本憑證管理中心規定之「組織鑑別程序」及「網域鑑別程序」，以確認該申請者之身分真確且擁有該主機名稱之擁有權。鑑別程序如下：

(1) 組織鑑別程序

對法人或組織進行身分鑑別時，應先針對其代表人進行身分鑑別，並驗證足以證明該法人或組織已登記或存在事實之相關文件。

申請文件可採網路、臨櫃、郵寄或傳真等方式進行遞交，並且以其所提交之申請文件查詢第三方公開資訊或其他證明資訊，確認其申請文件內容與查證內容相符，詳情參閱 3.2.2.1 節。

(2) 網域鑑別程序

- 網域主機名稱鑑別程序：須至少通過一種以上由 3.2.2.4 節所定義之驗證方法。
- IP 位址查驗：須至少通過一種以上由 3.2.2.5 節所定義之驗證方法。

(3) 自然人鑑別程序

不接受自然人申請。

### 1.4.2 憑證之禁止使用情形

本憑證管理中心所簽發之憑證除使用於 1.4.1 節規定之範圍，禁止用於以下用途：

(1) 竊聽或攔截第三方通訊之用途。

(2) 造成人身傷亡與精神侵害之用途。

(3) 對社會秩序與公共利益有重大危害之應用或業務。

(4) 電子簽章法、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。

## 1.5 政策管理

### 1.5.1 管理單位

本作業基準的制定、修訂、發布等事宜，其權責單位為政策管理中心(PMA)。

### 1.5.2 聯絡窗口

對本作業基準有任何疑義，或相關資安通報(如金鑰外洩疑慮或憑證誤發等)，可將詳細內容與聯絡資訊透過下列窗口進行聯繫：

| | |
|---|---|
| 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(100)延平南路 85 號 10 樓<br>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經由政策管理中心(PMA)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，必須經主管機關核定後，始得對外公布本作業基準並提供憑證簽發服務。

## 1.6 名詞定義與縮寫

請參閱附錄一、附錄二。

# 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(CRL)、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；另亦提供線上憑證狀態查詢(OCSP)服務。

儲存庫的網址為：https://www.twca.com.tw/repository

CRL 與 OCSP 之儲存庫位址載明於憑證擴充欄位中，詳細資訊參閱第 7 章。

## 2.2 憑證資訊之公布

本憑證管理中心公布之資訊如下：

(1) 歷年憑證政策及憑證實務作業基準。

(2) 本憑證管理中心憑證與相關資訊。

(3) 簽發之憑證。

(4) CRL。

(5) OCSP 服務。

(6) 憑證測試網站，包括有效憑證、過期憑證、廢止憑證之測試網站，其網站位置公布於 CCADB。

(7) 歷年稽核報告。

(8) 組織註冊機構列表 (參考 3.2.2.7 節)。

## 2.3 公布頻率

本作業基準，修改完成且經政策管理中心(PMA)核定後，將送主管機關核定，本公司於收到核定公文後 7 個工作天內公布於儲存庫。

本憑證管理中心憑證，一經簽發後，其憑證鏈以及憑證相關資訊於 7 個工作天內公布於本儲存庫供用戶或信賴憑證者查詢使用，其中 CRL 之簽發頻率參考 4.9.7 節之規定。

本憑證管理中心定期檢閱本作業基準，並至少每年修訂本作業基準 1 次。

## 2.4 儲存庫之存取控制

儲存庫以唯讀方式供用戶或信賴憑證者公開查詢使用，但為防止惡意攻擊或竄改，於更新儲存庫資訊或流量異常時須進行存取控制。

# 3. 識別與鑑別

## 3.1 命名

### 3.1.1 名稱種類

本憑證管理中心及用戶之憑證，其憑證主體識別名稱 (Subject DN)與發行者識別名稱(Issuer DN)皆符合 X.500 唯一識別名稱(Distinguished Name；DN)之命名方式，其一般名稱(Common Name；CN)或主體名稱擴充欄位(Subject Alternative Name；SAN)不得使用內部名稱或是保留 IP，該名稱的屬性及內容遵循 RFC 5280、BR 及 EVG 之相關規定。

### 3.1.2 識別名稱之意義

用戶憑證所記載之主體識別名稱，應符合相關法令及規範對於命名之規定，必須足以識別特定之法人或組織單位及網域主機名稱，且必須可為信賴憑證者所識別。

### 3.1.3 用戶之匿名與假名

本作業基準不允許用戶使用匿名、假名、別名或筆名等，但可接受使用 Punycode 方式對國際化域名(Internationalized Domain Names；IDNs)進行編碼。

### 3.1.4 各種名稱的解釋規則

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用戶中、英文名稱、網域主機名稱及法人或組織識別名稱之唯一性；相同的網域主機名稱不可由不同法人或組織使用，但同一網域主機名稱可能有多張憑證簽發予同一法人或組織使用。

當用戶憑證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並通過組織身分與網域鑑別之用戶優先使用，後申請註冊用戶若較先申請註冊用戶先通過身分資訊確認得優先使用。

如因識別名稱之使用有爭議時，經主管機關/機構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用戶唯一識別名稱使用權，並廢止已簽發之憑證，且該用戶應負擔相關法律責任。

### 3.1.6 商標之辨識、鑑別及角色

本憑證管理中心尊重用戶中、英文名稱之註冊商標，於查證後接受用戶使用該中、英文名稱，但不保證用戶註冊商標之認可、驗證與唯一性。若註冊商標發生糾紛時，用戶應自行循法律途徑處理。

## 3.2 初始驗證

### 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用戶自行產製，並由用戶提供 PKCS#10 格式之憑證請求檔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用戶之公開金鑰，驗證請求檔內之簽章值，確認用戶為私密金鑰擁有者且其公開金鑰與私密金鑰為成對。

### 3.2.2 組織身分與網域的鑑別

簽發用戶憑證前須進行「組織鑑別程序」及「網域鑑別程序」(「網域主機名稱鑑別程序」或「IP 位址查驗」)，確認申請者是否為合法之法人或組織，以及確認申請者是否具有欲申請網域之所有權及控制權。

本憑證中心之「組織鑑別程序」及「網域鑑別程序」審驗紀錄最大效期如下所示，若查無有效之審驗紀錄，將依本節規定重新進行初始驗證程序。

審驗紀錄最大效期依照 BR 4.2.1 節之要求將逐年縮短如下：

**「組織鑑別程序」審驗紀錄效期**

| 憑證 NTB >= | 憑證 NTB < | 審驗紀錄最大效期 |
|---|---|---|
| - | 2026 年 3 月 15 日 | 825 天 |
| 2026 年 3 月 15 日 | - | 398 天 |

**「網域鑑別程序」審驗紀錄效期**

| 憑證 NTB >= | 憑證 NTB < | 審驗紀錄最大效期 |
|---|---|---|
| - | 2026 年 3 月 15 日 | 398 天 |
| 2026 年 3 月 15 日 | 2027 年 3 月 15 日 | 200 天 |
| 2027 年 3 月 15 日 | 2029 年 3 月 15 日 | 100 天 |

| | | |
|---|---|---|
| 2029 年 3 月 15 日 | - | 10 天 |

### 3.2.2.1 組織鑑別程序

本程序適用於法人或組織鑑別，本節將統一名詞以「組織」進行說明。對組織進行身分鑑別時，應驗證主管機關核發或其他可資證明組織存在之證明文件，且須進行代表人之身分鑑別，申請文件之遞交可採網路、臨櫃、郵寄或傳真方式辦理。

針對用戶提供之申請文件應查詢第三方公開之組織註冊機構或其他證明資訊，核實申請人的合法存在與身分識別資訊，並確認其申請文件內容與查證內容相符，如組織登記之名稱、行號、國別，以滿足 BR 或 EVG 之身分鑑別要求。

若核發之憑證類型為 EVSSL 憑證時，核發前必須進一步對申請組織完成以下鑑別程序(下列程序中提及之註冊機構指的是組織註冊機構，非憑證註冊機構)：

(1) 組織名稱必須為完整法定名稱，可以縮寫組織名稱中的組織前綴或後綴，如“Company Name Incorporated”可縮寫為“Company Name, Inc.”。

(2) 確認組織類型必須為以下之一：私人組織(Private Organization)、政府實體(Government Entity)、商業實體(Business Entity)或非商業實體(Non-Commercial Entity)。

(3) 登記於憑證欄位中有關司法管轄所在地之資料(如：Jurisdiction of Incorporation Locality Name)不得為註冊機構無記載之資料。

(4) 註冊機構中記載之內容若無組織註冊編號(統一編號)，則於憑證欄位中之組織註冊編號輸入該組織成立或註冊的日期。

(5) 登記於憑證欄位中營業所在地址必須為組織實體營業地址。

(6) 若申請者為表示個人之商業實體(Business Entity)，則必須採用臨櫃面對面方式驗證負責人身分。

(7) 透過第三方可信賴註冊機構管道，如：經濟部工商狀態查詢、財政部財政資訊中心，驗證組織登記之資料與其公司狀態，該管道必須出自於「組織註冊機構列表」。本憑證管理中心使用之「組織註冊機構列表」揭示於官網首頁之儲存庫中，其來源均為政府單位之官方儲存庫。

(8) 依據 EVG 11.6 節規定確認申請人代表之組織是否真實存在。

(9) 申請 EVSSL 憑證，必須填具憑證申請人(Certificate Requestor)、憑證核准人(Certificate Approver)及合約簽署人(Contract Signer)等資訊。

### 3.2.2.2 行號鑑別程序

依 3.2.2.1 節之規定。

### 3.2.2.3 國名識別

依 3.2.2.1 節之規定。

### 3.2.2.4 網域主機名稱鑑別程序

本憑證管理中心(以下簡稱本中心)至少依一項下述之「網域主機名稱鑑別程序」，對申請者欲申請憑證之一般名稱(CN)及主體名稱擴充欄位(SAN)進行所有權查驗：

| **驗證方式名稱**<br>**(**遵循之 BR 章節**)** | **說明** |
|---|---|
| Email 驗證<br>(BR 3.2.2.4.4) | 本中心使用電子郵件傳遞一個唯一且效期 30 天之亂數值給指定收件人，再由本中心驗證該亂數值，其中收件人電子郵件地址限定：admin 或 administrator 或 webmaster 或 hostmaster 或 postmaster 等名稱再接續“@”及欲驗證網域名稱。<br><br>限制及要求：<br>• 2028/3/15 之後本中心將不使用此驗證方式。 |
| DNS 變更驗證<br>(BR 3.2.2.4.7) | 申請單位於欲驗證網域 DNS 服務內之 CNAME、TXT 或 CAA 等資源紀錄中以欲驗證網域名稱或欲驗證網域名稱前放置以底線符號(Underscore)開頭之標籤值(Label)命名之，再於其中放置一個唯一之 Request Token 值後，由本中心確認之。<br><br>限制及要求：<br>• 此驗證方式本中心將實施多視角驗證。 |
| 網站變更驗證<br>(BR 3.2.2.4.18) | 申請單位於欲驗證網域之指定網站目錄：“/.well-known/pki-validation”內，放置一個由本中心指定之唯一 Request Token 值後，再由本中心發動 HTTP 請求確認之，其中 HTTP 回應的狀態碼必須 |

| | |
|---|---|
| | 是成功(2xx)，若為轉址，僅限 HTTP 層轉址(HTTP 回應狀態碼限：301、302、307 或 308)，轉到的網址必須是使用 HTTP/HTTPS 協定且被授權的 Port。<br><br>限制及要求：<br>• 此驗證方式本中心將實施多視角驗證。<br>• 萬用網域憑證不得使用本方法進行查驗。 |
| 網站變更驗證<br>(ACME)<br>(BR 3.2.2.4.19) | 申請單位使用 ACME 協定中之 HTTP 挑戰方式(定義於 RFC 8555)來證明其具有網域控制權，再由本中心驗證之。<br><br>限制及要求：<br>• 此驗證方式本中心將實施多視角驗證。<br>• 萬用網域憑證不得使用本方法進行查驗。 |
| DNS 變更驗證<br>(ACME)<br>(BR 3.2.2.4.21) | 申請單位使用 dns-account-01 的網域驗證方法，允許透過在 DNS 中新增一個特定格式的 TXT 紀錄來證明網域所有權，這個紀錄包含一個僅 30 天內有效的 token。<br><br>限制及要求：<br>• 此驗證方式本中心將實施多視角驗證。 |
| DNS 長效驗證<br>(BR 3.2.2.4.22) | 申請單位使用「持久性 DNS TXT 紀錄」之網域驗證方法，於 DNS 的 _validation-persist 標籤下新增特定格式之 TXT 紀錄。該紀錄須包含本中心認可之帳號識別資訊 (accounturi)；若設有效期限 (persistUntil)，查驗時須在該期限內。此驗證方式完成後，其驗證資料之有效期間最長為 10 天，本中心之代表網域名稱 (Issuer Domain Names)請參閱 4.2.1 節規定。<br><br>限制及要求：<br>• 本憑證管理中心之代表網域名稱為 twca.com.tw。<br>• 此驗證方式本中心將實施多視角驗證。 |

本憑證管理中心之審驗紀錄皆包含其申請的完整網域(Fully-Qualified Domain Name；FQDN)、使用之驗證方法、完成驗證之網域(Authorization Domain Name)及遵循之 BR 版本。上述審驗方式除(4)外，其餘查驗方式使用 Public Suffix List 資訊，應用於網域名稱查驗。

本憑證管理中心在執行「網域主機名稱鑑別程序」時，主視角（Primary Network Perspective）查詢 DNS 紀錄所使用的 DNS 解析器，必須建立至 IANA DNSSEC root trust anchor 的驗證鏈，並進行 DNSSEC 驗證。

### 3.2.2.5 IP 位址查驗

本憑證管理中心(以下簡稱本中心)至少依一項下述之「IP 位址查驗程序」，對申請者欲於憑證內申請之所有 IP 位址進行所有權之查驗：

| **驗證方式名稱**<br>**(**遵循之 BR 章節**)** | **說明** |
|---|---|
| 網站變更驗證<br>(BR 3.2.2.5.1) | 申請單位於欲驗證 IP 之指定網站目錄："/.well-known/pki-validation"內，放置一個由本中心指定之唯一 Request Token 值後，再由本中心發動 HTTP 請求確認之。<br><br>限制及要求：<br><br>• 此驗證方式本中心將實施多視角驗證。 |
| IP 反向查詢驗證<br>(BR 3.2.2.5.3 ) | 藉由對該 IP 位址進行「反向查詢」（Reverse-IP lookup）以取得與其關聯的網域名稱，接著依照第 3.2.2.4 節允許之網域驗證方式對該 FQDN 進行控制權驗證，藉此確認申請人對該 IP 位址的控制能力。<br><br>限制及要求：<br><br>• 此驗證方式本中心將實施多視角驗證。<br><br>• 2027/3/15 之後本中心將不使用此驗證方式。 |
| 網站變更驗證<br>(ACME)<br>(BR 3.2.2.5.6) | 使用 ACME 協定中之 http-01 方式(定義於 RFC 8555)進行查驗。<br><br>限制及要求： |

| | |
|---|---|
| | • 此驗證方式本中心將實施多視角驗證。 |

### 3.2.2.6 萬用網域驗證

申請之網域去除「*.」後之網域名稱不可出現於 Public Suffix 清單中，相關要求遵循 BR 3.2.2.6 節之要求，其餘規範依 3.2.2.4 節規定。

### 3.2.2.7 資訊來源準確性

本憑證管理中心進行組織鑑別程序與所使用的「組織註冊機構列表」揭示於官網首頁之儲存庫中，並定期進行清單確認與更新。

本憑證管理中心使用之「組織註冊機構列表」其來源為政府單位之官方儲存庫或其他業內普遍接受之資訊管道。

### 3.2.2.8 授權憑證機構簽發紀錄

本憑證管理中心於進行申請者網域之憑證頒發機構授權（CAA）記錄驗證時，依 RFC 8659（或其後續更新版本）透過網域名稱查詢系統（DNS）檢查該網域是否設定授權；如 CAA 記錄授權本憑證管理中心，得核准憑證申請，未授權者應予拒絕。驗證過程中，主視角（Primary Network Perspective）所使用之 DNS 解析器必須自 IANA DNSSEC root trust anchor 建立完整之驗證鏈並執行 DNSSEC 驗證，以確保查詢之完整性與安全性。查驗方式遵循 BR 3.2.2.8 節，詳細規範見 4.2.1 節（7）。

### 3.2.2.9 多視角驗證

針對「網域所有權」查驗以及「授權憑證機構簽發紀錄(CAA)」查驗，本中心將實施多視角驗證(MPIC)。相關要求及規定遵循 BR 3.2.2.9 節。

**遠端視角數量要求：**

| 生效日期 | 遠端視角最低數量 |
|---|---|
| 2025 年 9 月 15 日 | 2 個 |
| 2026 年 3 月 15 日 | 3 個 |
| 2026 年 6 月 15 日 | 4 個 |
| 2026 年 12 月 15 日 | 5 個 |

**遠端視角允許不一致數量：**

| 遠端視角數量 | 允許不一致數量 |
|---|---|
| 2~5 個 | 1 個 |
| 6 個(含)以上 | 2 個 |

### 3.2.3 個人用戶身分的鑑別

不接受自然人申請。

### 3.2.4 未驗證之用戶資訊

本憑證管理中心所簽發憑證記載之用戶資訊皆經過驗證。

### 3.2.5 權責之確認

本憑證管理中心依據 3.2.2.1 節組織鑑別程序取得可靠的通訊方式，以驗證該法人或組織及其代表人、代理人(下稱該等人)之身分，包含憑證申請書上之姓名、職務、親簽或公司章之真偽，必要時須聯繫該法人或組織，以確認該等人有權進行憑證之申請。

### 3.2.6 相互溝通方式

不做規範。

## 3.3 金鑰更新之識別與鑑別

### 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增加，用戶應定期更新金鑰(Rekey)以確保金鑰之安全性。本憑證管理中心簽發之用戶憑證效期最長 200 天(私密金鑰效期與憑證效期相同)，用戶憑證最大效期將根據 6.3.2 節規定逐年縮短。

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，向本憑證管理中心申請憑證簽發。本憑證中心將檢驗是否有有效之審驗紀錄，若查無有效之審驗紀錄，則本憑證管理中心必須依 3.2 節規定重新進行初始驗證程序。

### 3.3.2 憑證廢止後之金鑰更新

用戶之憑證廢止後，必須進行依 3.2 節規定之初始驗證程序，重新申請新憑證。

## 3.4 憑證廢止請求

當憑證發生符合第 4.9.1 節規定之廢止事由時，有權請求廢止者（如第 4.9.2 節所述）應向本憑證管理中心提出廢止請求。本中心針對不同業務流程，採取下列識別與鑑別程序：

| 業務流程 | 說明 |
|---|---|
| **人工流程** | • 本憑證管理中心或註冊中心應確認申請者之身分（如：原申請人、法人代表人或受委託之代理人）。<br>• 除檢核身分外，應依 3.2 節規定檢驗請求資料之真偽，必要時需聯繫該法人或組織，以確認憑證欲廢止之具體事實。<br>• 若透過代理人辦理，須滿足 3.2.5 節之授權要求。 |
| **自主流程** | • 申請者須使用原開設之自主簽發平台帳戶登入。<br>• 登入時須使用本憑證管理中心核發之晶片卡進行數位簽章，系統驗章通過後視為身分識別通過。<br>• 系統將比對該帳戶是否具備管理該憑證之權限。 |
| **ACME 自動化流程** | • 廢止請求必須符合 RFC 8555 規範。ACME Client 須使用該憑證對應之 ACME 帳戶私鑰 對廢止請求訊息進行簽署。<br>• 本憑證管理中心接收請求後，將使用資料庫中綁定之 ACME 帳戶公鑰進行數位簽章驗證。<br>• 系統驗證該 ACME 帳戶是否為原申請該憑證之合法帳戶，驗證通過後始接受該交易請求。 |

# 4. 憑證生命週期管理

## 4.1 憑證申請

本憑證管理中心依照不同業務流程分為「人工簽發憑證」、「自主簽發憑證」以及「ACME 自動化簽發憑證」。

### 4.1.1 憑證申請者

欲申請憑證之法人或組織，其代表人或代理人為憑證申請者。

### 4.1.2 註冊申請程序及責任

憑證申請者應事先閱讀使用者約定事項，充分了解使用憑證之權利及義務。申請者可透過線上註冊系統完成身份驗證並確認同意相關約定，或以書面方式撰寫並簽署憑證申請書，遞送至本憑證管理中心辦理憑證申請程序。

憑證申請者必須自行產生憑證之金鑰對，及其對應之 PKCS#10 憑證請求檔(以下簡稱 CSR)，並透過本憑證管理中心提供之安全管道遞送。

## 4.2 憑證申請程序

本憑證管理中心依照不同業務分為「人工簽發流程」、「自主簽發流程」以及「ACME 自動化簽發流程」。

### 4.2.1 識別與鑑別程序

用戶之憑證申請識別與鑑別程序如下：

(1) 由法人或組織之代表人，或由其指定之代理人擔任憑證申請者。

(2) 各業務流程識別與鑑別程序概述：

| 業務流程 | 說明 |
|---|---|
| 人工流程 | • 申請者無需事先開設帳戶。<br>• 首次申請，申請者應備妥憑證申請書正本，並加蓋組織公章（如：公司章、發票章）及申請人簽名，郵寄至本憑證管理 |

| | |
|---|---|
| | 中心辦理。<br>• 本憑證管理中心人工驗證申請資料之真偽。<br>• 申請者應備妥憑證申請書，加蓋申請單位部門章及申請人簽名（或單位二位人員簽名），透過傳真、郵寄或電子郵件寄送至註冊中心。<br>• 申請者須自行產製 CSR，並透過安全管道將其與申請書表單編號一併交付本憑證管理中心。 |
| **自主流程** | • 申請者須開設自主簽發平台帳戶。<br>• 申請者須事先與本憑證管理中心簽訂合約，並於合約中指定網域名稱。經本憑證管理中心審查通過後開設平台帳號，並將該帳戶綁定於網域名稱白名單。<br>• 申請者須使用本憑證管理中心核發之晶片卡作為登入憑據，登入時進行數位簽章，驗章通過後始可進行憑證作業。<br>• 若為憑證更新由申請者自行登入簽發平台進行作業；若為增購網域，則需另與本憑證管理中心簽訂合約。<br>• 申請者須自行產製 CSR，並自行登入簽發平台，透過上傳檔案方式完成憑證申請請求。 |
| **ACME 自動化流程** | • 申請者須開設自動化簽發平台帳戶。<br>• 首次申請前應簽訂合約並載明網域名稱。申請者須提供組織登記證明，於線上平台註冊自動化帳戶，經本憑證管理中心審查通過後開設，並綁定網域名稱白名單。<br>• 申請者須事先安裝 ACME 用戶端（Client），並取得外部帳戶綁定（EAB）金鑰以完成帳戶關聯。本憑證管理中心將用戶身分與 ACME 帳戶公鑰進行綁定。<br>• 執行 ACME 交易時，須使用 ACME 帳戶私鑰對交易訊息簽章，經本憑證管理中心驗章通過後始接受該交易請求。<br>• 若為憑證更新，於合約效期內，申請者可使用 ACME 用戶 |

| | |
|---|---|
| | 端（Client）直接與本憑證管理中心取得新憑證；若為增購網域，則需另與本憑證管理中心簽訂合約。<br>• ACME 用戶端（Client）自動產製金鑰對及 CSR，並將憑證請求資訊透過 ACME 協定傳送至本憑證管理中心。 |

(3) 通用查驗規範

| 驗證要求 | 說明 |
|---|---|
| 驗證紀錄有效性檢查 | 本憑證管理中心依第 3.2 節規定執行驗證。若查無有效之「組織鑑別紀錄」或「網域鑑別紀錄」，必須重新執行完整驗證程序。驗證紀錄效期參考 3.2.2 節之規定。 |
| 金鑰合規性 | 本憑證管理中心將會檢查 CSR 內之公開金鑰，透過 badkeys 資料庫進行查詢(https://badkeys.info/)，不得為各類已知弱金鑰（如 Debian Weak Key），且不得與本憑證管理中心資料庫中現有憑證金鑰重複，若檢查不通過將不予以簽發。 |
| 主體名稱限制 | 本憑證管理中心將會檢查憑證主體名稱（CN）或主體替代名稱（SAN）不可包含內部名稱（Internal Name）或保留 IP 位址，且不可列於 Google Safe Browsing 惡意軟體清單中。 |
| EVSSL 憑證限制 | 申請擴充驗證（EV）憑證時，CN 或 SAN 之 dNSName 不得包含萬用網域（Wildcard）。 |

(4) 審核結果

- 本 CA 驗證申請資料後，依查驗結果決定接受申請、要求補件或駁回申請。決定接受後進入簽發程序。

### 4.2.2 接受或拒絕憑證申請

凡順利完成第 4.2.1 節「識別與鑑別程序」之申請案，視為通過審核，申請者即取得本憑證管理中心之用戶身分。若申請者未能通過上述程序，本中心應拒絕其憑證申請。

為符合國際安全標準，本憑證管理中心嚴格禁止簽發包含以下屬性之憑證：

- 內部名稱 (Internal Names)：憑證之主體別名 (CN) 或主體替代名稱 (SAN) 不得使用內部名稱。即其網域後綴必須列於 IANA Root Zone Database 清單中(https://www.iana.org/domains/root/db)；若網域結尾不在該清單內，則視為非公開解析之內部名稱。

- 保留 IP 位址 (Reserved IP Addresses)： 憑證之 CN 或 SAN 不得包含保留 IP 位址。其定義依據 IANA IPv4 特殊用途登錄表 及 IANA IPv6 特殊用途登錄表之規定 (https://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml 及 https://www.iana.org/assignments/iana-ipv6-special-registry/iana-ipv6-special-registry.xhtml)。

### 4.2.3 憑證申請處理時間

無規定。

## 4.3 憑證簽發

本憑證管理中心依照不同業務分為「人工流程」、「自主流程」以及「ACME 自動化流程」。

### 4.3.1 憑證機構簽發憑證

本憑證管理中心依下列流程執行憑證簽發：

(1) 各業務流程簽發憑證概述：

| 業務流程 | 說明 |
|---|---|
| 人工流程 | • 系統自動檢查 CSR 之數位簽章以確認完整性與私鑰所有權證明；同時檢查主體識別名稱（DN）與擴充欄位是否與申請書一致，且不含內部名稱或保留 IP。<br>• 本審查人員透過雙因子驗證登入管理後台，執行第 3.2 節定義之組織與網域驗證。採「雙人覆核制」，由另一名人員確認無誤後簽發。<br>• 此流程之網域驗證不得使用 BR 3.2.2.4.19 及 BR 3.2.2.4.21 方法。 |
| 自主流程 | • 用戶登入自主簽發平台帳戶，自行產製 CSR，並發動憑證申請請求。<br>• 系統自動判斷組織及網域驗證紀錄是否仍有效，若紀錄有效則即時核發；若無效則終止程序，轉由本憑證管理中心人員 |

| | |
|---|---|
| | 進行人工審驗。<br>• 此流程之網域驗證不得使用 BR 3.2.2.4.19 及 BR 3.2.2.4.21 方法。 |
| **ACME 自動化流程** | • ACME 用戶端自動產生金鑰與 CSR，透過符合 RFC 8555 規範之 TLS 通道傳輸。<br>• ACME 伺服器自動驗證簽章、私鑰所有權及網域白名單合規性。若查驗通過將自動簽發憑證，若失敗則終止自動程序，轉由本憑證管理中心人員進行人工帳戶設定。<br>• 此流程之網域驗證僅限使用 BR 3.2.2.4.19、BR 3.2.2.4.21 或 BR 3.2.2.4.22 方法。 |

(2) 簽發前通用查驗規範

| **驗證要求** | **說明** |
|---|---|
| 憑證 lint 檢查 | 本憑證管理中心使用第三方工具（Zlint 及 pkilint）查驗，確保憑證符合 RFC 5280、CABF BR 與 EVG 規範。若檢核失敗將不予以核發。 |
| CAA 記錄檢查 | 本憑證管理中心之代表網域名稱為 twca.com.tw。<br>本憑證管理中心於憑證簽發前將會進行 CAA 紀錄檢查，若查驗失敗將不予以核發。參考 3.2.2.8 節之規範。 |

(3) 憑證透明度

- 本憑證管理中心於核發正式憑證前將會上傳預簽憑證(Precertificate)至 CT(Certificate Transparency)紀錄伺服器，並於取得足夠數量之 SCT(Signed Certificate Timestamp)資訊後簽發憑證；且於簽發憑證後會將正式憑證 (final certificate) 上傳至 CT 紀錄伺服器。

(4) 憑證效期限制

- 本憑證管理中心簽發之用戶憑證中的憑證起始日不回溯過去時間，即憑證起始日不會早於憑證簽發之當下時間。

### 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用戶。若使用 ACME 自動化簽發憑證之用戶，將不再另行通知。

## 4.4 憑證接受

### 4.4.1 憑證接受之程序

用戶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，且為用戶之正確資訊。

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

(3) 用戶必須驗證該憑證之憑證鏈，檢驗其每張憑證的正確性、完整性與有效性，該憑證是否已廢止、憑證有效期限是否已結束、是否確為本憑證管理中心所簽發。

(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) 用戶於收到所申請之憑證後，必須確認已充分了解並同意其使用憑證之權利及義務，若不同意則視為拒絕接受憑證，本憑證管理中心應廢止憑證。

本憑證管理中心僅接受用戶於憑證核發後 7 天內，向本憑證中心提出憑證變更請求。

### 4.4.2 憑證機構公布憑證

本憑證管理中心於完成憑證簽發程序後，即將用戶憑證公布於儲存庫。

### 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的使用

用戶憑證的用途、適用範圍及限制，依 1.4 節之規定。

用戶應妥善保護其私密金鑰，若有被冒用、曝露或遺失等不安全疑慮時，必須向本憑證

管理中心辦理申告。

### 4.5.2 信賴憑證者使用公開金鑰及憑證

信賴憑證者於信賴本憑證管理中心簽發之用戶憑證前，至少應進行以下程序以決定是否信賴該憑證：

(1) 透過適當及安全之管道，取得本憑證管理中心之最高層憑證管理中心自簽憑證。

(2) 檢查最高層憑證管理中心自簽憑證、用戶憑證管理中心憑證及用戶憑證是否已過期。

(3) 以最高層憑證管理中心自簽憑證之公開金鑰，驗證用戶憑證管理中心憑證之數位簽章是否有效且並未被廢止。

(4) 以用戶憑證管理中心憑證之公開金鑰，驗證用戶憑證之數位簽章是否有效。

(5) 檢查用戶憑證未遭用戶憑證管理中心廢止。

如未能通過前述驗證，表示信賴憑證者取得之用戶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用戶憑證。

## 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。

本憑證管理中心不提供憑證展期服務。

## 4.7 憑證更新

憑證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。依照不同業務流程描述如下：

| 業務流程 | 說明 |
|---|---|
| 人工流程 | • 申請者應備妥憑證申請書，加蓋申請單位部門章及申請人簽名（或單位二位人員簽名），透過傳真或電子郵件寄送至註冊中心。<br>• 申請者須自行產製 CSR，並透過安全管道將其與申請書表單編號一 |

| | |
|---|---|
| | 併交付本憑證管理中心。<br>• 審查人員透過雙因子驗證登入管理後台，執行第 3.2 節定義之組織與網域驗證。採「雙人覆核制」，由另一名人員確認無誤後簽發。 |
| **自主流程** | • 申請者透過自主簽發平台帳戶完成憑證更新流程。<br>• 申請者須使用本憑證管理中心核發之晶片卡作為登入憑據，登入平台時進行數位簽章，驗章通過後始可進行憑證更新作業。<br>• 申請者須自行產製 CSR，並於平台內透過上傳檔案方式完成。<br>• 系統自動判斷組織及網域驗證紀錄是否仍有效。若紀錄有效則即時核發；若無效則終止程序，轉由本憑證管理中心人員進行人工審驗。 |
| **ACME 自動化流程** | • ACME 用戶端自動產生金鑰與 CSR，透過符合 RFC 8555 規範之 TLS 通道傳輸。<br>• ACME 伺服器自動驗證簽章、私鑰所有權及網域白名單合規性。若查驗通過將自動簽發憑證，若失敗則終止自動程序，轉由本憑證管理中心人員進行人工帳戶設定。 |

### 4.7.1 憑證更新之事由

依 3.3.1 節之規定。

### 4.7.2 有權更新憑證者

用戶有權更新憑證。

### 4.7.3 憑證更新程序

(1) 依 3.3 節之規定對用戶進行身分識別與鑑別。

(2) 依 4.3 節之規定簽發憑證。

### 4.7.4 憑證更新簽發之通知

依 4.3.2 節之規定。

### 4.7.5 更新後憑證接受之程序

依 4.4 節之規定。

### 4.7.6 憑證機構公布更新憑證

依 4.4.2 節之規定。

### 4.7.7 更新憑證後對其他機構之通知

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(產生新憑證序號)予用戶。

本憑證管理中心僅接受用戶於憑證核發後 7 天內，向本憑證中心提出憑證變更請求；若超過 7 天，用戶之識別資訊或其他記載於憑證之資訊須變更時應依 4.9 節之規定廢止憑證後，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

當廢止狀況發生時，相關憑證應被廢止並加入 CRL/OCSP，遭廢止之憑證必須包含於之後所公布的 CRL/OCSP，直到憑證到期為止。

### 4.9.1 憑證廢止之事由

#### 4.9.1.1 廢止用戶憑證之事由

以下幾種情況發生時，本憑證管理中心應於 24 小時內廢止憑證：

(1) 用戶以書面形式申請終止憑證的使用。

(2) 用戶告知原始憑證申請未獲得授權。

(3) 用戶憑證相關的私密金鑰經證實或懷疑遭破解時。

(4) 用戶使用的金鑰對為弱金鑰(例如 Debian Weak Key)。

(5) 用戶之網域主機名稱或 IP 位址之驗證資料是不可信賴的。

以下幾種情況發生時，本憑證管理中心應於 5 天內廢止憑證：

(1) 用戶使用之金鑰違反第 6.1.5 及第 6.1.6 節之規定。

(2) 用戶之憑證遭到誤用。

(3) 用戶違反主管機關之法令、憑證政策、本憑證實務作業基準或用戶合約時。

(4) 用戶已不被允許合法使用憑證中記載之網域主機名稱或 IP 位址。

(5) 萬用網域憑證被用於詐欺用途的網域。

(6) 憑證中所記載之資訊異動。

(7) 憑證未依本憑證管理中心之憑證政策或憑證實務作業基準之規定程序簽發時。

(8) 憑證中所記載之資訊不正確。

(9) 本憑證管理中心簽發憑證之權力已逾期、被廢止或被中止；除非已安排其他計畫繼續維護 CRL 與 OCSP 服務。

(10) 憑證政策規定應廢止項目。

(11) 已知有方法可破解用戶之金鑰或用戶金鑰產製之方法有已知弱點。

(12) 用戶憑證相關的私密金鑰遺失或損毀。

(13) 或 4.8 節憑證變更之事由。

#### 4.9.1.2 廢止下屬憑證機構憑證之事由

以下幾種情況發生時，最高層憑證管理中心應於 7 天內廢止憑證：

(1) 下屬憑證機構以書面形式請求撤銷。

(2) 下屬憑證機構告知原始憑證申請未獲得授權。

(3) 下屬憑證機構使用之金鑰違反第 6.1.5 及第 6.1.6 節之規定。

(4) 下屬憑證機構之憑證遭到誤用。

(5) 下屬憑證機構之憑證未依憑證政策或本憑證實務作業基準之規定程序簽發時。

(6) 憑證中所記載之資訊不正確。

(7) 最高層憑證管理中心或下屬憑證機構終止營運，且未安排其他憑證機構承接以提供憑證廢止服務。

(8) 最高層憑證管理中心或下屬憑證機構簽發憑證之權力已逾期、被廢止或被中止；除非已安排其他計畫繼續維護 CRL 與 OCSP 服務。

(9) 憑證政策規定應廢止項目。

### 4.9.2 有權請求廢止憑證者

(1) 用戶。

(2) 本憑證管理中心。

(3) 主管機關或法院。

非上述等人若懷疑憑證金鑰遭破解或有其他安全事項，亦可通知本憑證管理中心，由本憑證管理中心於確認屬實後進行憑證廢止程序，聯絡方式參閱 1.5.2 節。

### 4.9.3 憑證廢止程序

本憑證管理中心 7 x 24 接受憑證廢止請求，申請者依 3.4 節提出憑證廢止請求，憑證廢止程序依照不同業務流程描述如下：

| 業務流程 | 說明 |
|---|---|
| 人工流程 | • 依 4.9.2 節定義之有權請求廢止憑證者，申請憑證廢止。<br>• 若為憑證用戶提出憑證廢止申請，以 3.4 節之規定鑑別，其他憑證廢止申請依 4.9.1 節定義之憑證廢止事由進行查證。<br>• 本憑證管理中心鑑別完成後，依據 4.9.1 節規定時限內完成廢止作業。 |
| 自主流程 | • 用戶登入自主簽發平台帳戶，提出憑證廢止請求，包含欲廢止之憑證資訊並選填廢止事由（Reason Code）。 |

| | |
|---|---|
| | • 系統將即時執行憑證廢止作業。 |
| **ACME 自動化流程** | • ACME 帳戶擁有者（即用戶）得透過 ACME Client 進行自動化憑證廢止作業。該請求須依據 RFC 8555 規範，包含欲廢止之憑證資訊並選填廢止事由（Reason Code）。<br>• ACME client 須傳送經由 ACME 帳戶私鑰簽署之廢止請求訊息至本憑證管理中心，以確保請求來源之合法性與不可否認性。<br>• 本憑證管理中心接收請求後，將立即使用該 ACME 帳戶公鑰對訊息進行數位簽章驗證。若驗證權限無誤，系統將即時執行憑證廢止作業。 |

### 4.9.4 憑證廢止請求提出期限

用戶於憑證廢止事由發生後，應於一般商業運作慣例之合理期限內提出憑證廢止請求，本作業基準不強制規定期限。如懷疑或證實金鑰遭破解或有其他安全事項須廢止憑證，用戶應於 24 小時內提出。

### 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用戶提出之憑證廢止申請，應於 24 小時內進行調查與初步回覆。在需要廢止的情況下，從收到請求到廢止完成的時間範圍不得超過 4.9.1.1 節之規定。

### 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，自行決定透過 CRL 或 OCSP 來確認憑證狀態，並決定查詢頻率。

若信賴憑證者透過本憑證管理中心簽發之 CRL 檢查憑證狀態，使用前應驗證 CRL 是否為本憑證管理中心簽發，包含驗證 CRL 數位簽章之正確性與有效性，其他驗證時注意事項須滿足 RFC 5280 相關要求。

若信賴憑證者透過本憑證管理中心提供之 OCSP 訊息檢查憑證狀態，使用前應驗證 OCSP 訊息是否為本憑證管理中心之 OCSP Responder 簽發，包含驗證 OCSP 訊息數位簽章之正確性與有效性，其他驗證時注意事項須滿足 RFC 6960 相關要求。

### 4.9.7 憑證廢止清冊簽發頻率

本憑證管理中心每 24 小時更新並簽發 1 次 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 OCSP 服務，支援以 HTTP GET 或 POST 方式查詢 OCSP 服務，其回應訊息符合 RFC 6960 之規範，內容包含對該訊息之數位簽章。

本憑證管理中心至少每 2 天更新 OCSP 服務提供之憑證狀態資訊，效期最長為 4 天，其他相關內容請參閱 7.3 節。

### 4.9.10 線上廢止/狀態查詢驗證規定

信賴憑證者於決定信賴本憑證管理中心簽發之憑證前，必須檢查其憑證狀態；若信賴憑證者未使用本憑證管理中心簽發之 CRL 來檢查憑證狀態，則信賴憑證者必須以 4.9.9 節規定之方式，透過 OCSP 服務來檢查憑證狀態。

針對已上傳至 CT(Certificate Transparency)紀錄伺服器之預簽憑證(Precertificate)，若交易逾時且未簽發憑證予用戶，則本憑證管理中心將對預簽憑證進行廢止並加入 CRL/OCSP 中，CRL 與 OCSP 服務之更新頻率與其他相關內容請參考 4.9.7、4.9.9、7.2、7.3 節。

### 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

若金鑰疑似遭到破解，通報者可將證明資訊以合法之管道(參閱 1.5.2 節)，聯繫本憑證管理中心之適當窗口，本憑證管理中心接受以下方式證明金鑰疑似遭到破解：

提供以疑似遭到破解金鑰簽發之 CSR(使用標準 PKCS#10 格式)進行證明，其中 CSR 之 CN 必須為「Proof of Key Compromise for TWCA」，以供本憑證中心驗證其真偽。

本憑證管理中心之簽章金鑰遭破解時，應依以下程序辦理：

(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 CRL，CRL 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) 告知用戶。

(4) 提供本憑證管理中心新的簽章金鑰對應之憑證。

(5) 使用新的簽章金鑰簽發憑證予用戶。

用戶之金鑰被懷疑或證實遭破解，應於知悉該事實 24 小時內告知本憑證管理中心廢止憑證。

### 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，故以下關於有權請求憑證暫時停用者、憑證暫時停用程序、憑證暫時停用期間限制等規定不適用。

若金鑰遭破解不得使用憑證暫禁之程序，應依 4.9.12 節辦理。

### 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

(1) 用戶透過本憑證管理中心提供之 CRL、OCSP 服務查詢憑證狀態。

(2) 憑證廢止清冊之下載點註記於憑證 *cRLDistributionPoints* 延伸欄位中。

(3) 已廢止憑證之憑證廢止資訊，在該憑證效期屆滿後，才會自 CRL、OCSP 服務中移除。

### 4.10.2 服務之可用性

本憑證管理中心提供 24x7 之憑證狀態服務，供信賴憑證者查詢所有未過期憑證之狀態。

正常網路環境下，本憑證管理中心提供之 CRL、OCSP 服務的回應時間通常在 10 秒以內，CRL 簽發頻率參考 4.9.7 節之說明。

本憑證管理中心提供 24x7 之聯繫機制，用以通知重大憑證問題(例如憑證遭冒名申請或誤發)，經確認後將逕行廢止問題憑證，若有違法事件將轉知執法機構。本憑證管理中心之聯繫窗口參考 1.5.2 節。

### 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、憑證廢止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

本憑證管理中心之私密金鑰不允許託管。用戶之私密金鑰不禁止被託管。

### 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

本憑證管理中心之安全控管除遵循憑證政策外，亦遵循由 CA/Browser Forum 所訂定之「NETWORK AND CERTIFCATE SYSTEM SECURITY REQUIREMENTS」規範。

## 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，其中至少 2 道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、磁碟機與亂碼化設備等，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須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) 開發人員(Developer)負責系統設計與開發。

### 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) 開發人員(Developer)至少 1 名。

程式碼開發完成並申請併入正式環境前，至少須由兩位授權之受信任人員進行審核與確認，並確保程式碼符合業務邏輯與安全規範後方可核准發布。

簽發用戶憑證前至少須 2 名信賴角色人員確認，方可執行用戶憑證簽發。

### 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、智慧卡及相關之身分識別驗證密碼，以達到信賴角色之身分識別與鑑別。

本憑證管理中心之開發人員對於原始碼之存取，統一透過程式碼版控管理平台進行，並整合 Active Directory (AD) 帳號權限控管機制，依據開發任務授予對應之專案存取權限。

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 | 操作人員 | 開發人員 |
|---|---|---|---|---|---|
| 憑證主管人員 | ○ | X | X | X | X |
| 系統管理人員 | X | ○ | X | ○ | X |
| 稽核人員 | X | X | ○ | X | X |
| 操作人員 | X | ○ | X | ○ | X |
| 開發人員 | X | X | 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。

(4) 稽核人員至少具備資訊安全或系統稽核之專業知識，並具有獨立審查作業流程之經驗。

(5) 操作人員至少經過憑證生命週期管理及系統管理之訓練。

(6) 開發人員至少具備安全程式碼撰寫與系統開發之能力。

### 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、憑證核發審驗程序、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、憑證主管人員或稽核人員。

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

### 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，並依相關作業之規範處理。

### 5.3.7 委外人員需求

若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依 5.3.2 節之背景審查程序後，施以 5.3.3 節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紀錄，均包含下列項目：

(1) 事件類型。

(2) 事件發生日期及時間。

(3) 事件成功或失敗之結果。

(4) 引發此事件之個體或人員。

(5) 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。
- CRL 產製記錄。
- OCSP 服務簽章記錄。

(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) CRL 剖繪之管理

- CRL 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紀錄。

### 5.4.3 稽核紀錄保留期限

本憑證管理中心相關稽核紀錄報表與媒體資料至少保留 7 年且不得早於相關金鑰銷毀、憑證過期、廢止後 2 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

電子式稽核紀錄每月備份 1 次，並儲存於本憑證管理中心以外之備援地點。

### 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紀錄，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紀錄。

### 5.4.8 脆弱性評鑑

每年進行 1 次以下所列的各種脆弱性評鑑：

(1) 識別可預見的內部和外部威脅，這些威脅可能導致未經授權存取，資訊洩露，資訊濫用，資料遭竄改或破壞任何憑證資料或憑證管理流程。

(2) 評鑑威脅發生的可能性，以及發生時憑證資料和憑證管理流程可能的損害。

(3) 評鑑本憑證管理中心目前適用之資訊安全政策、管理程序、資訊技術以及其他防護措施，是否足以防禦威脅。

## 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) 被稽核驗證(Accreditation)資料。

(2) 憑證實務作業基準。

(3) 用戶合約。

(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 CRL。

(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) 用戶身分鑑別資料。

### 5.5.2 歸檔紀錄保存期限

本憑證管理中心之歸檔資料至少保留 7 年且不得早於相關金鑰銷毀、憑證過期、廢止後 2 年。

### 5.5.3 歸檔紀錄的保護

歸檔資料不可進行寫入、修改或刪除的動作；屬於用戶之個別已歸檔資料，允許對該用戶或其他法規允許之機構釋出。

歸檔資料必須保存 1 份於本憑證管理中心所在地外，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回復作業。

### 5.5.5 歸檔紀錄之時戳要求

歸檔之電子式紀錄(例如憑證、CRL 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，如須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

必須以書面申請獲得正式授權後，才可取得歸檔資料；歸檔資料由稽核人員負責驗證，書面文件必須驗證文件簽發者及日期等之真偽，電子檔則驗證歸檔資料的數位簽章或以密碼

學方式驗證。

## 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。

用戶憑證管理中心進行金鑰更新時，會產製一對新的金鑰對，交由最高層憑證管理中心簽發憑證後，依 6.1.4 節規定供信賴憑證者查詢下載。

用戶之金鑰效期，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。

### 5.6.1 用戶金鑰更新

用戶憑證管理中心訂定用戶使用金鑰的生命週期，與用戶憑證管理中心簽發予用戶憑證的生命週期相同；即是用戶憑證的有效期限結束後，用戶金鑰即刻失效不可使用。

用戶金鑰使用有效期限結束前，用戶可以產生新金鑰對向用戶憑證管理中心或註冊中心申請新憑證的簽發，相關作業參考 3.3.1 節之規定。

當舊金鑰有不安全顧慮且有效期限尚未結束時，必須先向用戶憑證管理中心或註冊中心申請廢止舊憑證的使用，然後才可以產生新金鑰對，依註冊中心的作業規範申請新憑證的簽發，憑證廢止作業參考 4.9 節之規定。

### 5.6.2 用戶憑證管理中心金鑰更新

用戶憑證管理中心簽發用戶憑證之金鑰，其有效期間等同於對應憑證之生命週期，不得超過 10 年。

用戶憑證管理中心進行金鑰更新時，會產製一對新的金鑰對，交由最高層憑證管理中心簽發憑證後，依 6.1.4 節規定供信賴憑證者查詢下載。

用戶憑證管理中心金鑰使用有效期限結束時，可以產生新金鑰對向最高層憑證管理中心申請新憑證的簽發，並即刻通知註冊中心，完成後以新私密金鑰簽發用戶憑證，舊金鑰將繼續簽發 CRL，直至該舊金鑰的生命週期結束。

當用戶憑證管理中心舊金鑰有不安全顧慮且有效期限尚未結束時，必須先向最高憑證管理中心申請廢止舊憑證，才可以產生新金鑰對並簽發新憑證，完成後以新私密金鑰簽發用戶憑證與 CRL，並即刻通知用戶與註冊中心，先前使用用戶憑證管理中心之舊私密金鑰所簽發的用戶憑證與 CRL 皆失效，用戶必須重新產生新金鑰對向用戶憑證管理中心申請新憑證的簽

發。

### 5.6.3 最高層憑證管理中心金鑰更新

最高層憑證管理中心簽發下屬憑證之金鑰，其有效期間等同於對應憑證之生命週期，不得超過 25 年。

最高層憑證管理中心於金鑰使用有效期限結束前，產製一對新金鑰對及自簽憑證，並立即公告此新自簽憑證，且即刻通知下屬憑證管理中心。原舊金鑰繼續簽發 CRL，直至該舊金鑰的生命週期結束。

當最高層憑證管理中心憑證有效期限尚未結束之金鑰有不安全疑慮時,必須先廢止憑證,才可以產生新金鑰對及自簽憑證，並即刻通知下屬憑證管理中心，此時，下屬憑證管理中心的憑證皆已無效，必須重新產生新金鑰對向最高層憑證管理中心申請新憑證的簽發。

當最高層憑證管理中心私密金鑰遭破解時，應廢止全部下屬憑證管理中心的憑證，並通知下屬憑證管理中心，逕行廢止全部用戶的憑證，且通知業務應用系統停止使用下屬憑證管理中心所簽發的憑證。

## 5.7 金鑰遭破解及災變復原程序

### 5.7.1 事故及金鑰遭破解之緊急應變處理程序

#### 5.7.1.1 事故應變與災變復原計畫

若用戶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：

(1) 必須儘快透過安全電子郵件或書面方式，通知所有用戶及最高層憑證管理中心。

(2) 依 6.1 節的規定產生新的金鑰對並交由最高層憑證管理中心簽發新憑證。

(3) 廢止所有已簽發之憑證，使用新的簽章金鑰簽發 CRL，CRL 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)。

(4) 依 4.3 節的程序，簽發新的憑證給各用戶。

(5) 將事故資訊通報並揭露給信賴憑證者及各 Root CA 信賴清單維護組織。

若最高憑證管理中心金鑰遭破解或遺失，則須進行下列程序：

(1) 必須儘快透過安全電子郵件或書面方式，通知所有下屬憑證管理中心，逕行廢止全部用戶的憑證。

(2) 廢止所有已簽發之憑證。

(3) 依 6.1 節的規定產生新的金鑰對與自簽憑證。

(4) 簽發新的憑證給下屬憑證管理中心。

(5) 將事故資訊通報並揭露給信賴憑證者及各 Root CA 信賴清單維護組織。

本憑證管理中心必須調查，並向 PMA 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。

本憑證管理中心訂定有緊急應變處理程序和災變復原計畫，以書面記載業務持續計畫與災變復原程序，內容包含當發生災變、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;以上程序本憑證管理中心將每年定期檢視或修訂。

若本憑證管理中心誤發或未依本作業基準簽發用戶憑證時，亦會將事故揭示於 Bugzilla 中。

#### 5.7.1.2 憑證大規模廢止計畫

本憑證管理中心訂定有憑證大規模廢止計畫，詳列憑證大規模廢止事件發生時之處理程序，內容包含「來源確認」、「影響範圍確認」、「內部通報及組織應變小組」、「應變作為及程序」、「計畫培訓、測試與持續改進」以及「第三方評估」，並於每年進行模擬演練，將演練或實際事件所獲得之經驗納入計畫，以持續改進並提升應變能力。

### 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 金鑰遭破解之處理程序

用戶之金鑰懷疑遭破解時，應依 4.9.3 節之方式辦理。

憑證管理中心之金鑰懷疑遭破解時，應依 5.7.1 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。

於業務正常結束、或合約終止、或公司重整而無安全之考量因素時：

(1) 於終止服務日 30 天前通知主管機關。

(2) 於終止服務日 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用戶並公布於儲存庫。

(3) 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。

(4) 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。

(5) 將本憑證管理中心之相關私密金鑰完全清除，並向用戶正式宣告，憑證業務已移轉至承接的憑證機構繼續營運。

於業務異常結束時(法院宣告破產、或不合法)，本憑證管理中心必須儘早向用戶告知事實，且必須執行業務正常結束時的作業程序，將影響減少至最低程度。

本憑證管理中心結束業務時，相關權利義務亦將依用戶合約辦理。

# 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

本憑證管理中心金鑰對：

(1) 由本憑證管理中心制定金鑰產製腳本，並遵循腳本自行產製金鑰對。

(2) 本憑證管理中心依 6.2.1 節規定，使用至少符合 CNS 15135、ISO 19790、FIPS 140-2 Level 3 或 FIPS 140-3 Level 3 之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。

(3) 金鑰產製過程在第三方公正人士見證下進行，金鑰產製程序全程錄影，金鑰產製後由公正人士簽署金鑰產製見證書，以昭公信。

用戶金鑰對：

(1) 由用戶驅動使用安全的方式產製金鑰。

(2) 本憑證管理中心會檢查用戶上傳之金鑰是否重複、是否為弱金鑰以及金鑰品質是否具有缺陷，若未通過檢測將不予以簽發憑證。

### 6.1.2 私密金鑰遞送至用戶

私密金鑰由憑證用戶自行產製並妥善保管，故無須遞送。

### 6.1.3 公開金鑰遞送至憑證簽發者

用戶的公開金鑰是以 PKCS#10 憑證請求檔傳送給本憑證管理中心，其傳送方式應以受安全保護的管道傳送。並且依 3.2.1 節所述之方式完成擁有私密金鑰的驗證程序。

### 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簽發的憑證公布至儲存庫，供用戶及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，且位元長度必可整除 8；ECC 公開金鑰使用之曲線其安全強度至少為 P-256。

用戶的 RSA 公開金鑰長度至少為 2048 位元，且位元長度必可整除 8；ECC 公開金鑰使用之曲線其安全強度至少為 P-256。

### 6.1.6 公開金鑰參數的產生及參數品質檢驗

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)。其中指數(Exponent)應包含以下特性：大於等於 3 的奇數且介於 2^16 + 1 與 2^256 - 1 之間；模數(Modulus)應包含以下特性：奇數、不是質數乘冪且無小於 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 部分公開金鑰驗證程序(ECC Partial Public Key Validation Routine)來確保所有金鑰的有效性。

本憑證管理中心會針對自身產製之金鑰或用戶產製之金鑰，進行弱金鑰(例如 Debian Weak Key)檢查，若未通過檢核則不允許作為憑證金鑰使用。

### 6.1.7 金鑰使用目的

本憑證管理中心簽發之憑證，金鑰用途參考 7.1.2 節擴充欄位之金鑰用途(Key Usage)及延伸金鑰用途(Extended Key Usage)。

### 6.1.8 用戶金鑰產製設備

用戶之金鑰對產製裝置，通常係使用網站伺服器或網路設備內建之金鑰產製裝置。

## 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至少符合 CNS 15135、ISO 19790、FIPS 140-2 Level 3 或 FIPS 140-3 Level 3 之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啟動資料是採 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啟用、備份及回復方法。

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允許託管，亦不提供憑證用戶私密金鑰託管服務。

### 6.2.4 私密金鑰的備份

(1) 本憑證管理中心之私密金鑰儲存於硬體密碼模組內,且依 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，另一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至少符合 CNS 15135、ISO 19790、FIPS140-2 Level 3 或 FIPS 140-3 Level 3 之硬體密碼模組，並具備多人控管功能。

### 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

私密金鑰在啟動後，其停用方式是將密碼模組經身分鑑別後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使用期限屆滿時,於隔年在第三方公正人士見證下銷毀金鑰,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，必須至少符合 CNS 15135、ISO 19790、FIPS 140-2 Level 3 或 FIPS 140-3 Level 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

以下公開金鑰與私密金鑰之有效期限相同。

(1) 最高層憑證管理中心之金鑰對有效期限上限為 25 年。

(2) 用戶憑證管理中心之金鑰對有效期限上限為 10 年。

(3) 用戶之金鑰對有效期限上限為 200 天。根據 BR 6.3.2 節要求，用戶憑證最大效期將逐年縮短如下：

| 憑證 NTB >= | 憑證 NTB < | 用戶憑證最大效期 |
|---|---|---|
| - | 2026 年 3 月 15 日 | 398 天 |
| 2026 年 3 月 15 日 | 2027 年 3 月 15 日 | 200 天 |
| 2027 年 3 月 15 日 | 2029 年 3 月 15 日 | 100 天 |
| 2029 年 3 月 15 日 | - | 47 天 |

## 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) 具備身分鑑別與多因子的登入。

(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。

### 6.5.2 電腦系統安全等級

本憑證管理中心作業使用的相關系統，其電腦系統安全應通過 Common Criteria(CC, ISO/IEC15408)的 GPOSPP(General Purpose Operating Systems Protection Profile)驗證或 EAL4+驗證或經內部安全性評估認可使用。

## 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 27001 的規範。

本憑證管理中心之硬體和軟體僅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

本憑證管理中心遵循 ISO 27001 及 WebTrust for CA(AICPA/CICA)的標準規範運作。

憑證管理中心的軟體在安裝或更新時，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，每次啟動時檢驗軟體的完整性。

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 生命週期安全控管

本憑證管理中心每年定期審視現行演算法或金鑰是否有遭破解之風險。

## 6.7 網路安全控管

最高層憑證管理中心憑證系統為離線(Off-Line)、獨立的作業管理系統，且須經授權後由業務相關的作業人員才可以人工方式執行作業。

本憑證管理中心之憑證管理系統須經授權後，始能由業務相關之作業人員執行管理作業，於執行管理作業時，憑證管理系統將對作業人員進行身分鑑別，通過後方可允許執行作業。

為防範網路入侵與破壞，本憑證管理中心之各主機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，並定期執行系統修補程式更新、系統弱點掃描以加強防護。本憑證管理中心針對已識別漏洞進行風險評估，並確保於下表時限內完成回應與補救：

| 漏洞風險等級 | 審查與回應期限 | 補救/修復期限 |
|---|---|---|
| 高(High) | 5 個工作日內 | 30 個日曆日內 |
| 中(Medium) | 10 個工作日內 | 90 個日曆日內 |

本憑證管理中心的主機和內部資料庫僅與內部網路連接並以防火牆隔離，僅允許內部主機連線且必須經過身分鑑別，確認係經授權之人員或系統方可存取。

儲存庫連接到網際網路(Internet)上，提供不中斷之憑證、CRL 及 OCSP 查詢服務(必要之維護或備援狀況除外)。

## 6.8 時間戳記

本憑證管理中心定時透過信賴時間源進行校時，確保本憑證管理中心各項作業時間值之準確性，包含但不限於以下時間值：

(1) 憑證簽發時間。

(2) 憑證廢止時間。

(3) CRL 簽發時間。

(4) OCSP 簽發時間。

# 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

本憑證管理中心使用之憑證序號，其編碼方式為非循序且大於零之自訂格式，內含由密碼學安全偽亂數生成器(Cryptographically Secure Pseudorandom Number Generator；CSPRNG)產生至少 64 位元亂數。

### 7.1.1 版本

本憑證管理中心之憑證及簽發予用戶之憑證版本為 X.509 v3，具有以下欄位(欄位定義滿足 RFC 5280 標準)：

| 欄位 | 內容說明 |
|---|---|
| 版本 | 固定為 v3 |
| 序號 | 憑證序號 |
| 簽章雜湊演算法 | 簽發憑證所使用的簽章雜湊演算法，本憑證管理中心支援：<br>sha256WithRSAEncryption<br>sha384WithRSAEncryption<br>ECDSAWithSHA256<br>ECDSAWithSHA384 |
| 簽章值 | 簽發者簽署產生之簽章值 |
| 簽發者 | 簽發此憑證對應 CA 之主體資訊 |
| 憑證起始日 | 憑證起始日 |
| 憑證結束日 | 憑證結束日 |
| 主體 | 憑證主體資訊，參閱 7.1.4.2、7.1.4.3 節 |
| 公開金鑰 | 憑證對應之公開金鑰 |
| 擴充欄位 | 參閱 7.1.2 節 |

### 7.1.2 憑證擴充欄位

本憑證管理中心使用之擴充欄位符合 RFC 5280 標準及 BR 7.1.2 節之相關要求。

#### 7.1.2.1 用戶憑證

用戶憑證管理中心簽發之用戶憑證擴充欄位設定如下：

| 憑證擴充欄位 | 是否使用 | 內容說明 |
|---|---|---|
| 授權單位金鑰識別元 | ○ | 使用 SHA-1 演算法 |
| 主體金鑰識別碼 | ○ | 使用 SHA-1 或 SHA-256 演算法 |
| CRL 發布點 | ○ | 內容含 CRL 下載位置 |
| 主體別名 | ○ | 內容包含至少一個主體資訊(參考 7.1.4.2.1 節) |
| 授權資訊存取 | ○* | 內容含<br>憑證授權單位簽發者<br>(accessMethod= 1.3.6.1.5.5.7.48.2)(必要)、<br>線上憑證狀態通訊協定(accessMethod=1.3.6.1.5.5.7.48.1)(選用) |
| 憑證原則 | ○ | 內容含<br>certificatePolicies:policyIdentifier<br>certificatePolicies:policyQualifiers:policyQualifierId<br>certificatePolicies:policyQualifiers:qualifier:cPSuri |
| 基本限制 | ○ | cA=false、pathLenConstraint=None |
| 金鑰使用方法 | ○ | digitalSignature(必要)、keyEncipherment(選用) |
| 增強金鑰使用方法 | ○ | serverAuth(1.3.6.1.5.5.7.3.1)(必要)<br>clientAuth(1.3.6.1.5.5.7.3.2)(選用) |
| SCT 清單 | ○ | 一至多個 Signed Certificate Timestamp 簽章值 |

*授權資訊存取，自 2024 年 3 月 15 日起，線上憑證狀態通訊協定為非必要資訊。

#### 7.1.2.2 所有憑證

其餘所有擴充欄位使用須符合 RFC 5280 標準、BR 7.1.2.4 節規範。

#### 7.1.2.3 RFC 5280 的應用

預簽憑證(Precertificate)不被視為需要符合 RFC 5280 的憑證。

### 7.1.3 演算法物件識別碼

#### 7.1.3.1 金鑰演算法

本憑證管理中心簽發憑證時使用的金鑰識別碼如下：

| 金鑰演算法 | 物件識別碼(OID) |
|---|---|

| | |
|---|---|
| rsaEncryption | {iso(1) member-body(2) us{840} rsadsi(113549) pkcs(1) pkcs-1(1) rsaEncryption(1)} (1.2.840.113549.1.1.1) |
| ecPublicKey | {iso(1) member-body(2) us(840) ansi-X9-62(10045) keyType(2) ecPublicKey(1)} (1.2.840.10045.2.1) |

#### 7.1.3.2 簽章演算法

本憑證管理中心簽發憑證時使用的簽章演算法物件識別碼如下：

| 簽章演算法 | 物件識別碼(OID) |
|---|---|
| sha256WithRSAEncryption | {iso(1) member-body(2) us{840} rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)} (1.2.840.113549.1.1.11) |
| sha384WithRSAEncryption | {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha384WithRSAEncryption(12)} (1.2.840.113549.1.1.12) |
| ECDSAWithSHA256 | {iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA256(2)} (1.2.840.10045.4.3.2) |
| ECDSAWithSHA384 | {iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA384(3)} (1.2.840.10045.4.3.3) |

### 7.1.4 識別名稱格式

#### 7.1.4.1 名稱編碼

本憑證管理中心及用戶之憑證，其憑證主體識別名稱與發行者識別名稱皆符合 X.500 唯一識別名稱(DN)之命名方式，此名稱的屬性型態遵循 RFC 5280 相關規定。

本憑證管理中心所簽發之用戶憑證，其簽發者唯一識別名稱(Issuer DN)與發行者(Issuer)憑證之主體唯一識別名稱(Subject DN)編碼必須完全相同；所有 CA 憑證依 RFC 5280 DN 比

對演算法為相同的 Subject DN，其編碼必須完全相同。

#### 7.1.4.2 用戶憑證之主體資訊

本憑證管理中心所簽發之用戶憑證，其主體資訊之驗證程序遵照本作業基準之 3.2.2 節之要求進行，並確保簽發前各項驗證程序均正確無誤。

本憑證管理中心所簽發之用戶憑證，其主體中各屬性不得使用不完整、不適用或預設值；除主體資訊中之 CN 屬性，其他屬性皆不可為網域名稱或 IP 位址。

##### 7.1.4.2.1 主體名稱擴充欄位

本憑證管理中心所簽發之用戶憑證必定具有主體名稱擴充欄位(SAN)，其值必須為 dNSName 或 iPAddress 形式，不得使用內部名稱或保留 IP，且至少具有一個主體資訊 CN 之值。根據 RFC 5280 之要求，dNSName 內容中不得使用下底線(“_”)。

#### 7.1.4.2.2 主體唯一識別名稱欄位

本憑證管理中心簽發之用戶憑證唯一識別名稱(DN)屬性如下表所示；另須注意本憑證管理中心簽發的憑證其 SAN 必須存在一個主體資訊 CN 之值，該值內容參考 7.1.4.2.1 節。

| 主體名稱屬性 | 說明 | SSL 憑證 | EVSSL 憑證 |
|---|---|---|---|
| | | 是否使用 | 是否使用 |
| Common Name(CN) | 網域主機識別名稱 | ○ | ○ |
| Organization(O) | 組織註冊名稱 | ○ | ○ |
| GivenName/Surname | 自然人姓名 | X | X |
| Street Address | 組織營業所在地址 | X | ○ |
| Locality(L) | 城市名 | ○ | ○ |
| State or Province(S) | 省或地區名 | ○ | ○ |
| Postal Code | 組織所在地郵遞區號 | X | ○ |
| Country(C) | 國別 | ○ | ○ |
| Organizational Unit(OU) | 組織單位名稱 | X | X |
| Business Category | 組織類型 | X | ○ |
| Jurisdiction of Incorporation Locality Name | 司法管轄所在地之城市名 | X | ○ |
| Jurisdiction of Incorporation State or ProvinceName | 司法管轄所在地之省或地區名 | X | ○ |
| Jurisdiction of Incorporation Country Name | 司法管轄所在地之國名 | X | ○ |
| Serial Number | 組織註冊編號 | X | ○ |
| Other Subject Attributes | 其他主體屬性 | X | X |

### 7.1.4.3 CA 憑證之主體資訊

最高層憑證管理中心所簽發之自簽憑證與用戶憑證管理中心之憑證，遵循憑證政策簽發並確保簽發前各項主體資訊正確無誤。

#### 7.1.4.3.1 主體唯一識別名稱欄位

(1) 用戶憑證管理中心自身憑證之識別名稱為：

- SSL UCA

| 識別名稱(DN) |
|---|
| C=TW, O=TAIWAN-CA, OU=Global SSL Sub-CA, CN=TWCA Global SSL Certification Authority |
| C=TW, O=TAIWAN-CA, OU=Secure SSL Sub-CA, CN=TWCA Secure SSL Certification Authority |
| C=TW, O=TAIWAN-CA, OU=SSL Sub-CA, CN=TWCA SSL Certification Authority |
| C=TW, O=TAIWAN-CA, CN=TWCA Secure SSL Certification Authority |
| C=TW, O=TAIWAN-CA, CN=TWCA SSL Certification Authority |

- EVSSL UCA

| 識別名稱(DN) |
|---|
| C=TW, O=TAIWAN-CA, OU=Global EVSSL Sub-CA, CN=TWCA Global EVSSL Certification Authority |
| C=TW, O=TAIWAN-CA, OU=EVSSL Sub-CA, CN=TWCA EVSSL Certification Authority |
| C=TW, O=TAIWAN-CA, CN=TWCA EVSSL Certification Authority |

(2) 最高層憑證管理中心自身憑證之識別名稱為：

| 識別名稱(DN) |
|---|
| C=TW, O=TAIWAN-CA, OU=Root CA, CN=TWCA Root Certification Authority |
| C=TW, O=TAIWAN-CA, OU=Root CA, CN=TWCA Global Root CA |
| C=TW, O=TAIWAN-CA, OU=Root CA, CN=TWCA CYBER Root CA |

### 7.1.5 識別名稱限制

本憑證管理中心之自身憑證與簽發之憑證皆無使用「名稱限制」(Name Constraint)擴充欄位。

### 7.1.6 憑證政策物件識別碼

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

#### 7.1.6.1 受保留的憑證政策物件識別碼

下列為受 CABF BR 保留之憑證政策物件識別碼：

| 物件識別碼 | 使用狀況 |
|---|---|

| | |
|---|---|
| {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) domain-validated(1)} (2.23.140.1.2.1) | 未使用(本憑證管理中心無簽發 DV 憑證) |
| {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) organization-validated(2)} (2.23.140.1.2.2) | SSL CA 憑證、SSL 憑證使用 |
| {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) individual-validated(3)} (2.23.140.1.2.3) | 未使用(本憑證管理中心無簽發 IV 憑證) |
| {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) ev-guidelines(1)} (2.23.140.1.1) | EVSSL CA 憑證、EVSSL 憑證使用 |

### 7.1.6.2 最高層憑證管理中心自身憑證

最高層憑證管理中心之憑證不具有憑證政策(Certificate Policy)延伸欄位。

### 7.1.6.3 用戶憑證管理中心憑證

用戶憑證管理中心之憑證，其具有憑證政策(Certificate Policy)延伸欄位，並使用以下憑證政策物件識別碼：

| 憑證種類 | 物件識別碼 |
|---|---|
| SSL CA 憑證 | {ISO(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) TWCA(40869) certificates(1) policies(1) SSL(21) (1.3.6.1.4.1.40869.1.1.21)<br><br>{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) organization-validated(2)} (2.23.140.1.2.2) |
| EVSSL CA 憑證 | {ISO(1) identified-organization(3) dod(6) internet(1) private(4) |

| | |
|---|---|
| | enterprise(1) TWCA(40869) certificates(1) policies(1) EV(22) class3(3) }<br>(1.3.6.1.4.1.40869.1.1.22.3)<br><br>{joint-iso-itu-t(2) international-organization(23) ca-browser-forum(140) certificate-policies(1) extended-validation(1)}<br>(2.23.140.1.1) |

#### 7.1.6.4 用戶憑證

用戶憑證管理中心簽發之用戶憑證，其具有憑證政策(Certificate Policy)延伸欄位，並使用以下憑證政策物件識別碼：

| 憑證種類 | 物件識別碼 |
|---|---|
| SSL 憑證 | {ISO(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) TWCA(40869) certificates(1) policies(1) SSL(21)<br>(1.3.6.1.4.1.40869.1.1.21)<br><br>{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) organization-validated(2)}<br>(2.23.140.1.2.2) |
| EVSSL 憑證 | {ISO(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) TWCA(40869) certificates(1) policies(1) EV(22) class3(3) }<br>(1.3.6.1.4.1.40869.1.1.22.3)<br><br>{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) extended-validation(1)}<br>(2.23.140.1.1) |

### 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」(Policy Constraint)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」(Policy Qualifier)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

可於用戶憑證之 CRL 發布點(CRL Distribution Points)擴充欄位中取得服務網址。本憑證管理中心簽發 CRL 之頻率依 4.9.7 節規定。

### 7.2.1 版本

本憑證管理中心簽發 X.509 v2 格式的 CRL，滿足 RFC 5280 之規範，具有以下欄位：

| 欄位 | 內容說明 |
|---|---|
| 版本號 | 固定為 v2 |
| 簽發者 | 簽發者 CA 的 Subject DN |
| 有效日期 | CRL 簽發時間 |
| 下次更新 | 下次簽發時間 |
| 簽章雜湊演算法 | 簽發 CRL 所使用的簽章雜湊演算法，本憑證管理中心支援：<br>sha256WithRSAEncryption<br>sha384WithRSAEncryption<br>ECDSAWithSHA256<br>ECDSAWithSHA384 |
| 憑證廢止清單 | 被廢止的憑證清單，內容包含憑證序號及廢止時間 |
| 簽章值 | 簽發者簽署產生之簽章值 |

### 7.2.2 憑證廢止清冊與憑證廢止清冊擴充欄位

本憑證管理中心簽發之 CRL 具有以下擴充欄位：

| 擴充欄位 | 內容說明 |
|---|---|
| CRL 編號 | 遞增之流水號，識別每一代 CRL |
| 主體金鑰識別碼 | 識別簽發之 CA |

| 廢止代碼 | 識別憑證廢止原因(參考下方說明) |
|---|---|

用戶憑證允許之廢止原因為：金鑰外洩(Key Compromised)、資訊變更(Affiliation Changed)、憑證已被取代(Superseded)、停止營運(Cessation of Operation)、撤銷使用權(Privilege Withdrawn)、不指定(Unspecified)。

各廢止原因使用之情境說明如下：

| **廢止原因** | **說明** |
|---|---|
| Key Compromised (1) | ● CA 取得私鑰已外洩的證據。<br>● CA 得知一個已被證明或展示的破解私鑰方法。<br>● 有明確證據證明產生私鑰的方法有缺陷。<br>● CA 得知一個已被證明或展示的從公鑰計算私鑰方法(例如 Debian Weak Key)。<br>● 任何人要求廢止憑證(不限於用戶)且可以證明目前持有私鑰(依 CA CPS 規定之證明方式)時，CA 必須廢止所有相同公鑰的憑證，不限於申請廢止的用戶的憑證。<br><br>* 用戶要求廢止憑證，但無法證明其持有私鑰時，CA 可廢止此用戶的憑證，但不可視為私鑰已外洩(使用 KeyCompromised 原因)；CA 可選擇阻擋不再簽發此公鑰的憑證。 |
| Affiliation Changed (3) | ● 用戶要求以此理由廢止憑證。<br>● CA 因主旨身分資訊變更而換發憑證，沒有其他廢止理由時。 |
| Superseded (4) | ● 用戶要求以此理由廢止憑證。<br>● CA 因網域驗證或符規性問題廢止憑證，且問題與金鑰外洩或撤銷使用權無關時。 |
| Cessation of Operation (5) | ● 當申請者不再擁有或不被授權使用憑證中的所有網域名稱。<br>● 使用憑證的網站不再營運。<br>● CA 得知憑證中的網域名稱或 IP 已不能合法使用，例如法院判決。 |
| Privilege Withdrawn (9) | ● CA 取得憑證被誤用的證據。<br>● CA 得知用戶違反用戶合約或使用條款。<br>● CA 得知萬用網域憑證被用於有誤導詐騙性的子網域。<br>● CA 得知憑證中的資訊有變更。<br>● CA 判斷或得知憑證中的資訊有誤。 |

| | |
|---|---|
| | ● CA 得知憑證申請未經授權。 |
| Unspecified (0) | 廢止原因不屬於上述情況時。 |

CRL 中簽發者(Issuer)憑證之識別名稱(Subject DN)與簽發此 CRL 之簽發者識別名稱(Issuer DN)編碼必須完全相同。

## 7.3 線上憑證狀態查詢

可於用戶憑證之憑證機構資訊存取(Authority Info Access)擴充欄位中取得服務網址，本憑證管理中心提供之 OCSP 服務具有以下特性：

(1) 回覆訊息使用之簽章憑證禁止使用 SHA-1 演算法且此憑證由本憑證管理中心簽發。

(2) 回覆訊息之簽章值禁止使用 SHA-1 演算法。

(3) 回覆訊息之憑證狀態支援：正常(good)、已廢止(revoked)、未知(unknown)。

(4) 當接收到非本憑證管理中心簽發憑證之狀態查詢請求時，將會回覆憑證狀態未知(unknown)之訊息。

其餘內容參考 4.9.9 節規定。

### 7.3.1 版本

本憑證管理中心之線上憑證狀態查詢版本為 1.0，符合 RFC 6960 規範。本憑證管理中心簽發之 OCSP 回應訊息，具有以下欄位：

| 欄位 | 內容說明 |
|---|---|
| 版本 | 固定為 v1 |
| 回應伺服器 ID | 內容為回應伺服器憑證公鑰(SubjectPublicKeyInfo)之 SHA-1 雜湊值 |
| 產製時間 | OCSP 回應簽署時間 |
| 憑證狀態 | 本憑證管理中心支援以下憑證狀態：<br>正常(good)<br>被廢止(revoked)<br>未知(unknown) |
| 效期 | OCSP 回應之效期，包含本次更新時間(ThisUpdate)及下次更新時間(NextUpdate) |

| | |
|---|---|
| 簽章雜湊演算法 | 簽發 OCSP 回應所使用的簽章雜湊演算法，本憑證管理中心支援：<br>sha256WithRSAEncryption<br>sha384WithRSAEncryption<br>ECDSAWithSHA256<br>ECDSAWithSHA384 |
| 簽章值 | OCSP 回應伺服器簽署 OCSP 回應產生之簽章值 |
| 簽章者憑證 | OCSP 回應伺服器之憑證 |

### 7.3.2 線上憑證狀態查詢擴充欄位

本憑證管理中心之線上憑證狀態查詢，其擴充欄位的使用符合 RFC 6960 規範。

# 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進行 1 次外部稽核，每季進行 1 次內部稽核。

## 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或憑證實務作業經驗，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，委託之稽核業者須符合 BR 及 MRSP(Mozilla Root Store Policy)之規定且具有國家稽核人員正式資格或國際上認可之稽核資歷，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，會先對稽核人員進行資格確認，完成稽核後，稽核報告中亦會條列稽核人員之稽核資歷、具備之稽核證照。

## 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。

本憑證管理中心的稽核規範遵循以下標準：

- WebTrust Principles and Criteria for Certification Authorities – Version 2.2.2 或更新版本。

- WebTrust Principles and Criteria for Certification Authorities – Extended Validation TLS – Version 2.0.1 或更新版本。
- WebTrust Principles and Criteria for Certification Authorities – TLS Baseline – Version 2.10 或更新版本。
- WebTrust Principles and Criteria for Certification Authorities – Network Security – Version 2.0.5 或更新版本。

## 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；本憑證管理中心取得事故內容後會主動將重大缺失揭示於 Bugzilla。

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歷次 WebTrust 稽核報告，同時本公司於官網記載取得之國際標章，點擊標章圖示亦可閱覽 WebTrust 稽核報告。

## 8.7 內部稽核

本憑證管理中心監督其是否遵循憑證政策及憑證實務作業基準，每季至少進行 1 次內部查核來嚴格控制服務品質，其中至少隨機抽樣稽核區間內所核發之憑證 3% 進行內部稽核。

# 9. 其他業務及法令規定

## 9.1 收費

### 9.1.1 憑證簽發及更新費用

本憑證管理中心簽發憑證予用戶，由本憑證管理中心向用戶收取憑證費用；憑證費用規範於憑證申請書、憑證報價單、憑證用戶合約，或公布於本憑證管理中心網站。

### 9.1.2 憑證查詢費用

不收費。

### 9.1.3 憑證廢止及狀態查詢費用

不收費。

### 9.1.4 其他服務費用

無規定。

### 9.1.5 退費

用戶於完成憑證申請，但憑證尚未簽發前申請退費者，扣除參仟元的處理工本費後，餘無息退還予用戶；於完成憑證簽發後用戶始申請退費時，按比例扣除使用月份之費用後，再扣除參仟元的處理工本費，餘無息退費。

## 9.2 財務責任

### 9.2.1 保險範圍

於憑證管理作業有關的風險管理，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，已投保 200 萬美元之一般責任險和 500 萬美元之專業責任險。

### 9.2.2 其他資產

本憑證管理中心執行憑證業務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。

### 9.2.3 對用戶及信賴憑證者之賠償責任

(1) 本憑證管理中心所提供的驗證服務作業項目與內容，皆訂定於本作業基準 1.4.1 節，非本作業基準所訂定的內容，皆排除於賠償責任之外。

(2) 本憑證管理中心處理用戶註冊資料及憑證簽發作業，除未遵照本作業基準、憑證政策及相關作業規範的規定辦理而造成用戶的損失，且可歸責於本憑證管理中心之過失外，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的天災事故(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)，造成用戶損失時，本公司不負損害賠償責任。

(4) 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用戶的損害時，本憑證管理中心應依規定賠償用戶損害，賠償上限依 9.8 節責任限制之規定。

(5) 本憑證管理中心或其他有權者提出廢止用戶憑證之要求後，至本憑證管理中心實際公布廢止該用戶憑證(記載於 CRL)為止之期間內，如因使用該用戶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。

(6) 用戶使用非法假造、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。

(7) 用戶的損害賠償請求權時效期間，依相關法律的規範辦理。

## 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) 用戶申請憑證時，擔任憑證申請者代表人及代理人之個人資料。

(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 CRL、外部稽核結果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，否則用戶之註冊基本資料與身分驗證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) 具有合法司法管轄權之法院或仲裁機構處理因憑證產生之糾紛或仲裁，而依法定程序申請之需求。

## 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「個人資料保護法相關規範」，及其他政府單位相關的規範運作。具體個資及隱私權管理於憑證申請書中載明。

本公司已於 102 年 11 月取得個人資訊管理系統 BS 10012 證書。於 107 年 7 月進行轉版 BS10012：2017，並同時取得隱私資訊管理系統 ISO 27701，持續維持有效至今。

### 9.4.2 個人資訊隱私種類

依 9.4.1 節之規定。

### 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 利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

依 9.3.3 節之規定。

### 9.4.7 其他資訊公開情形

依 9.3.3 節之規定。

## 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 CRL 為本公司之智慧財產。

(3) 用戶的金鑰對為用戶之智慧財產，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用戶名稱之正確性，但不保證記載於用戶憑證主體識別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。

(8) 本憑證管理中心對於不當使用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用戶註冊資料、憑證資料及相關憑證作業訊息之責任，避免機密資訊洩漏、被冒用、竄改或任意使用。

(2) 本憑證管理中心應依憑證政策及憑證實務作業基準之規範，接受用戶之憑證申請、憑證更新及憑證廢止訊息，確認用戶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，及將相關回覆訊息遞送予用戶。

(3) 本憑證管理中心執行用戶憑證簽發時,必須驗證申請文件與用戶身分之正確性及合法性。

(4) 用戶憑證管理中心之私密金鑰有安全之顧慮時，用戶憑證管理中心必須通知用戶及最高

層憑證管理中心；最高層憑證管理中心之私密金鑰有安全之顧慮時，最高層憑證管理中心必須通知所有用戶憑證管理中心。

(5) 本憑證管理中心簽發憑證時，須依本作業基準之規範，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用戶憑證時，應依本作業基準之規範，產生 CRL，並安全地遞送至儲存庫。

(7) 本憑證管理中心應於用戶申請憑證前，應提供憑證申請程序及用戶合約，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 CRL 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。

本憑證管理中心審查並擔保下列內容：

- 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。
- 沒有誤導性之資訊：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 註冊機構之職責

依 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法人或組織機構，其義務規範如下：

(1) 用戶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) 用戶私密金鑰有遺失或遭破解等不安全之顧慮時，或用戶憑證相關之資訊有異動時，必須依相關作業之規定，向本憑證管理中心辦理申告。

(3) 用戶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用戶憑證時，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) 用戶應妥善產製、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) 用戶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，但用戶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，用戶應儘速尋求其他途徑完成與他人應為之法律行為，不得以本憑證管理中心無法正常運作，作為抗辯他人之事由。

(7) 用戶 TLS 憑證安裝之技術人員或委託單位應具備 24 小時或 5 天內更換憑證之能力，避免因憑證廢止而影響站台之運作。

(8) 根據 4.9.1 節之規定，當發生滿足憑證廢止事由之情事，依照廢止事由分類，應於事發後 24 小時(例如金鑰外洩)或 5 天內(例如憑證內容不正確)廢止，用戶不得申請延長廢止期限，認證中心將於廢止期限屆期時主動廢止憑證不另行通知。

### 9.6.4 信賴憑證者義務

(1) 信賴憑證者應依本憑證實務作業基準之規範，取得用戶憑證管理中心及最高層憑證管理中心之自簽憑證。

(2) 信賴憑證者利用用戶憑證管理中心憑證及最高層憑證管理中心所提供之自簽憑證，進行憑證鏈之建立、驗證，以決定是否信任用戶憑證。

(3) 信賴憑證者驗證憑證時應使用最高層憑證管理中心之自簽憑證，驗證用戶憑證管理中心憑證之數位簽章是否為最高層憑證管理中心之私密金鑰所簽發，並透過 CRL 驗證憑證狀態是否已遭廢止。

(4) 信賴憑證者驗證用戶憑證時應使用用戶憑證管理中心之憑證，驗證用戶憑證之數位簽章是否為用戶憑證管理中心之私密金鑰所簽發，並透過 CRL 或 OCSP 服務驗證憑證狀態是否已遭廢止。

(5) 信賴憑證者在使用本憑證管理中心簽發之 CRL 時，應先驗證數位簽章，並檢查 CRL 記載之下次更新時間，如已超過下次更新時間，應取得最新 CRL。若使用 OCSP 服務時，應先檢查 OCSP 回應之數位簽章。

(6) 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。

(7) 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。

(8) 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用戶註冊資料及憑證簽發作業，除未遵照本作業基準之規定辦理，或違反相關法律規章之規定，或可歸責於本憑證管理中心之過失外，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)，造成用戶及信賴憑證者損失時，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用戶之註冊及憑證相關機密資料，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。

(4) 本憑證管理中心在收到憑證廢止申請後，應於 24 小時內進行調查與初步回覆，且從收到請求到廢止完成的時間範圍不得超過 4.9.1.1 節之規定；並於憑證廢止作業完成後依據 4.9.7 節規定之頻率簽發憑證廢止清冊及公告於儲存庫。用戶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。有關廢止作業規範請參閱 4.9 節。

## 9.8 責任限制

用戶及信賴憑證者，因簽發憑證或使用憑證而發生損害賠償事件時，本憑證管理中心應承擔之損害賠償責任，以相關法令規定、用戶合約或本公司保險責任額所定之範圍為責任上限。

## 9.9 賠償

依 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，與用戶建立聯絡管道，包括但不限以下方式：電話、傳真或 Email。

## 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 PMA，每年至少更新本作業基準 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(例如 BR)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，將依第 2 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 Email 至 1.5.2 節的聯絡窗口，交由 PMA 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，做為與用戶間之變更聯絡機制。

### 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

用戶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 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。

(3) 爭議之雙方如無法於 60 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，無法以上述的處理方式解決時，則必須依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令規定辦理，且遵循本國之相關法律規範。

## 9.15 法規之符合性

本作業基準及本憑證管理中心應符合本國電子簽章法及其施行細則之規定，不得牴觸本國法令。

本憑證管理中心亦遵守並符合最新版本 BR 及 EVG 規範之要求。若本作業基準與上述規範之要求不一致時，應以上述規範為主。若上述規範與本國法令相牴觸時，應以本國法令為主，並由本憑證管理中心向 CA/Browser Forum 提出異議。

## 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 可分割性

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。

當我國之法律要求與 BR 或 EVG 發生衝突時，本憑證管理中心將調整本作業基準以符合我國之法律要求、將該法條列於本節、並即時通知 CA/Browser Forum。

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

本憑證管理中心如因不可抗力之天災事故(例如地震等)或其他不可歸責於本憑證管理中心之事由(例如戰爭等)，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 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)

由 NIST 於 FIPS 186-3 中所制定之橢圓曲線標準，其定義了橢圓曲線之相關參數 p, a, b, G, n, h，其中曲線之基點 G 的 x、y 座標長度分別為 256 bits。

(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) 自動憑證更新環境(Automated Certificate Management Environment；ACME)

一種通訊協議，用於自動化執行憑證機構(CA)與其用戶端 Web 伺服器之間的憑證相關管理作業(例如憑證申請)，允許用戶以極低的成本自動化部署公鑰基礎設施。該協議主要透過 HTTPS 傳輸格式化之 JSON 訊息，相關標準定義於 RFC 8555 中。

(18) 憑證簽名請求(Certificate Signing request；CSR)

一種經過編碼的檔案，讓憑證申請者透過標準化的方式，把公開金鑰、憑證相關資訊(例如網域名稱)傳給憑證機構進行憑證簽發。該檔案可具體證明申請者為私鑰之擁有者。

(19) 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。

(20) 公用後綴列表(Public Suffix List；PSL)

由 Mozilla 創建的公共資源，列表位於 https://publicsuffix.org/，該列表由兩部分組成：一部分是由 ICANN 提供的 TLD(Top Level Domain；頂級域名)列表，一部分是由個人或機構提供的 PRIVATE 列表。

(21) Punycode

是一種表示 Unicode 碼和 ASCII 碼的有限的字符集，例如中文「台灣」會被編碼為「xn--kpry57d」。Punycode 的目的是在於國際化域名標籤的框架中，使這些多語言的域名可以編碼為 ASCII。

(22) Bugzilla

由 Mozilla 維護之瀏覽器問題的追蹤管理網路程式，當 CA 發生重大缺失時，必須回報於此處。位於 https://bugzilla.mozilla.org/home。

(23) 內部名稱

指網域主機名稱無法透過公眾網域名稱服務(Public DNS)進行解析。

(24) 保留 IP

在網際網路定址結構中，IETF(Internet Engineering Task Force，網際網路工程小組)和 IANA(Internet Assigned Numbers Authority，網際網路號碼分配局)保留用於特殊目的的網際協定位址(IP)。可於以下網址進行查詢：
https://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml
https://www.iana.org/assignments/iana-ipv6-special-registry/iana-ipv6-special-registry.xhtml

(25) 憑證透明度(Certificate Transparency；CT)

定義於 RFC 6962 中，目的是監控 CA 核發之憑證。透過 CA 將憑證上傳至公開的伺服器(Log server)，憑證透明度可以讓網站使用者和網域擁有者辨識不當或惡意簽發的憑證，同時也可以監視 CA 不當的作業行為。

(26) 預簽憑證(Precertificate)

定義於 RFC 6962 中，CT 中的一種特殊憑證，為一種供稽核查驗 CA 簽發紀錄之憑證，該憑證必須於實際簽發予用戶前預先簽發，並將之上傳至 CT 紀錄伺服器中取得 SCT(Signed Certificate Timestamp)，而實際簽發予用戶之憑證內容將包含這些 SCT 以證明先前已經成功上傳至 CT 紀錄伺服器。

(27) 授權憑證機構簽發(CAA)

是一種 DNS 資源紀錄，它允許網站所有者指定哪些 CA 有權為其網域發行 TLS 憑證。透過設定 CAA 紀錄，網站管理者可以限制憑證的發行權限，有效防止未經授權的 CA 意外或惡意地為其網域頒發憑證，從而增強網域憑證的安全性。

(28) 多視角驗證(MPIC)

多視角驗證要求 CA 在核發憑證前，必須由多個地理位置分散的驗證節點交叉確認 DNS 記錄與網域驗證結果是否一致，以降低因 BGP 劫持、DNS 汙染或區域性網路攻擊所導致的錯誤驗證風險。在 MPIC 架構中，驗證流程包含兩種視角：

主視角驗證（Primary Perspective）

由 CA 的主要驗證節點執行，負責取得 DNS、CAA、HTTP-01 或 TLS-ALPN-01 等基礎驗證資料，作為後續比對的基準。主視角主要用於確認申請端是否具備基本且可被正常觀測的驗證配置。

遠端視角驗證（Remote Perspective）

由分布於不同於主視角之地理區域、不同網路路徑的節點執行。這些節點必須能取得與主視角一致的驗證資訊，以確認該網域的設定在全球皆呈現一致狀態，並排除僅發生在 CA 主視角附近的路由或 DNS 欺騙情形。

CA 只有在主視角與所有遠端視角均取得一致結果時，方可視該網域驗證為有效，並據以簽發憑證；若任一視角觀測不一致，驗證即視為失敗。

(29) 通用 CA 資料庫(Common CA Database；CCADB)

是由 Google、Apple、Microsoft 及 Mozilla 等主流瀏覽器廠商共同維護的通用 CA 資料庫，用於集中管理與追蹤全球 CA 的稽核報告、政策文件及根憑證資訊，是確保憑證能被各大系統信賴的關鍵管理平台。

# 附錄二 名詞與簡稱(Acronyms and Abbreviations)

| | |
|---|---|
| ACME | Automated Certificate Management Environment |
| ANSI | American National Standard Institute |
| BR | Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates |
| CA | Certification Authority |
| CAA | Certificate Authority Authorization |
| CABF | CA/Browser Forum |
| CC | Common Criteria |
| CCADB | Common CA Database |
| CN | Common Name |
| CP | Certificate Policy |
| CPS | Certification Practice Statement |
| CRL | Certificate Revocation List |
| CSR | Certificate Signing request |
| DN | Distinguished Name |
| DNSSEC | Domain Name System Security Extensions |
| ECC | Elliptic Curve Cryptography |
| EVG | Guidelines for the Issuance and Management of Extended Validation Certificates |
| EVSSL | Extended Validation SSL |
| FIPS | Federal Information Processing Standard |

| | |
|---|---|
| IDNs | Internationalized Domain Names |
| ISO/IEC | The International Organization for Standardization/The International Electrotechnical Commission |
| ITSEC | Information Technology Security Evaluation Criteria |
| LDAP | Lightweight Directory Access Protocol |
| MPIC | Multi-Perspective Issuance Corroboration |
| MRSP | Mozilla Root Store Policy |
| OCSP | Online Certificates Status Protocol |
| OID | Object Identifier |
| 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) |
| SAN | Subject Alternative Name |
| SSL | Secure Socket Layer |
| TCSEC | Trusted Computer System Evaluation Criteria |
| URL | Universal Resources Location |