臺灣網路認證股份有限公司

公開金鑰基礎建設

憑證政策(CP)

Certificate Policy

(第 2.6.1 版)

生效日期： 中華民國 113 年 7 月 1 日

Effective Date：2024/7/1

版本變更紀錄

版 本	生效日期	發 行 者	備 註
1.0	2001/04/01	TaiCA PMA	CP 初版公告
1.1	2002/01/01	TaiCA PMA	配合 TaiCA CA PKI 系統文件(CPS,CP,…)的整合,與關貿網路公司 EDI 跨亞洲交易系統(PAA CP) 的整合而修訂
1.2	2002/04/01	TaiCA PMA	配合主管機關經濟部商業司訂定憑證實務作業基準應載明事項及憑證機構管理辦法之規範而修訂
1.3	2008/08/13	TWCA PMA	PMA 核定通過變更
1.4	2009/03/30	TWCA PMA	補充保證等級 OID 修訂公開金鑰使用期限
1.5	2009/08/04	TWCA PMA	依據 2009/07/29 PMA 會議決議修訂 6.3.2 節
1.6	2012/08/22	TWCA PMA	依據 2012/08/22 PMA 會議決議修訂 1.2 節,新增〝商務安全 EC 憑證〞之 OID
2.0	2012/11/23	TWCA PMA	依據 2012/11/23PMA 會議決議修訂 1.2 節，新增向 IANA 申請之公司 OID，調整各 CA 之 OID
2.1	2013/12/26	TWCA PMA	依據 2013/12/26PMA 會議決議修訂 1.2 節，新增設備憑證之 OID
2.2	2019/5/15	TWCA PMA	參照 CABF Baseline Requirement V1.6.4 修訂。 新增 CA/Browser Forum 憑證政策物件識別碼。 配合 Adobe AATL 信任根憑證計畫修訂。 移除網際 NB 憑證相關規定。
2.3	2021/8/4	TWCA PMA	移除 RSA 1024 位元之金鑰並新增 ECC P-256 及 P-384 之金鑰效期上限。 新增時戳憑證之 OID。
2.4	2022/5/5	TWCA PMA	設備憑證併入 TLS/SSL 憑證。 移除 TLS/SSL 憑證以及 EV SSL 憑證未使用之 OID。 增加說明 BR 適用之憑證種類。 TLS/SSL 憑證以及 EV SSL 憑證名稱一致。
2.5	2022/10/30	TWCA PMA	移除設備憑證之憑證政策識別碼。 調整 1.2 個體物件識別碼內容。 調整 1.4 憑證用途。 調整 3.2.2 法人身分的鑑別 調整 3.2.3 個人用戶身分的鑑別 調整 5.5.2 歸檔紀錄保留期限。

			調整 7.1.3 物件識別碼。 資安 UCA 憑證更名為資安憑證。 將 TLS/SSL 憑證更名為 SSL 憑證。 統一 CA/Browser Forum 規範之名詞。 新增 1.6 節、8.7 節。
2.6	2023/7/20	TWCA PMA	定義 S/MIME 憑證種類並加入 S/MIME BR 符規性之相關敘述。
2.6.1	2024/7/1	TWCA PMA	年度檢視無異動，更新版號。

目 錄

1 簡介 15

1.1 概述 15
1.2 文件名稱及識別 16
1.3 成員及適用範圍 20
1.3.1 憑證機構 20
1.3.2 註冊中心 21
1.3.3 用戶 21
1.3.4 信賴憑證者 21
1.3.5 其他參與者 22
1.4 憑證用途 22
1.4.1 憑證適用範圍 23
1.4.2 憑證之禁止使用情形 23
1.5 政策管理 23
1.5.1 管理單位 23
1.5.2 聯絡窗口 23
1.5.3 憑證實務作業基準之核定 24
1.5.4 憑證實務作業基準核定程序 24
1.6 名詞與簡稱 24

2 公布及儲存庫 25

2.1 儲存庫 25
2.2 憑證資訊之公布 25
2.3 公布頻率 25
2.4 儲存庫之存取控制 26

3 識別與鑑別 27

3.1 命名 27

3.1.1 名稱種類 27

3.1.2 識別名稱之意義 27

3.1.3 用戶之匿名與假名 27

3.1.4 各種名稱的解釋規則 27

3.1.5 名稱的唯一性 27

3.1.6 識別名稱糾紛的處理 28

3.1.7 商標之辨識、鑑別及角色 28

3.2 初始驗證 28

3.2.1 證明擁有私密金鑰的方式 28

3.2.2 法人身分的鑑別 28

3.2.3 個人用戶身分的鑑別 29

3.2.4 未驗證之用戶資訊 30

3.2.5 權限之驗證 30

3.2.6 相互溝通方式 30

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換 31

3.4 憑證廢止請求 31

4 憑證生命週期管理 32

4.1 憑證申請 32

4.1.1 憑證申請者 32

4.1.2 申請登記程序及責任 32

4.2 憑證申請程序 32

4.2.1 識別與鑑別程序 32

4.2.2 接受或拒絕憑證申請 32
4.2.3 憑證申請處理時間 32
4.3 憑證簽發 33
4.3.1 憑證機構簽發憑證 33
4.3.2 憑證機構簽發憑證通知用戶 33
4.4 憑證接受 33
4.4.1 憑證接受之程序 33
4.4.2 憑證機構公布憑證 34
4.4.3 憑證機構通知其他機構憑證簽發 34
4.5 金鑰對及憑證用途 34
4.5.1 用戶私密金鑰及憑證使用 34
4.5.2 信賴憑證者公開金鑰及憑證使用 34
4.6 憑證展期 34
4.6.1 憑證展期之事由 34
4.6.2 有權展期憑證者 34
4.6.3 憑證展期程序 35
4.6.4 通知用戶展期憑證之簽發 35
4.6.5 展期憑證接受程序 35
4.6.6 憑證機構公布展期憑證 35
4.6.7 憑證機構通知其他機構展期憑證之簽發 35
4.7 憑證及私密金鑰更新 35
4.7.1 憑證及私密金鑰更新之事由 35
4.7.2 有權更新憑證金鑰者(憑證金鑰更換申請者) 35
4.7.3 憑證金鑰更新程序 35
4.7.4 通知用戶更新金鑰憑證之簽發 36
4.7.5 更新金鑰憑證接受程序 36
4.7.6 憑證機構公布更新金鑰憑證 36

4.7.7 憑證機構通知其他機構更新金鑰憑證之簽發 36
4.8 憑證變更 36
4.8.1 憑證變更之事由 36
4.8.2 有權變更憑證者 36
4.8.3 憑證變更程序 36
4.8.4 通知用戶變更憑證之簽發 36
4.8.5 變更金鑰憑證接受程序 36
4.8.6 憑證機構公布變更憑證 37
4.8.7 憑證機構通知其他機構變更憑證之簽發 37
4.9 憑證廢止及暫禁 37
4.9.1 憑證廢止之事由 37
4.9.2 有權請求廢止憑證者 37
4.9.3 憑證廢止程序 37
4.9.4 憑證廢止請求提出期限 37
4.9.5 憑證機構處理憑證廢止請求時限 37
4.9.6 信賴憑證者憑證廢止檢驗規定 38
4.9.7 憑證廢止清冊簽發頻率 38
4.9.8 憑證廢止清冊最大潛在因素 38
4.9.9 線上廢止/狀態查詢服務 38
4.9.10 線上廢止/狀態查詢檢驗規定 38
4.9.11 其他形式之廢止公告 38
4.9.12 金鑰遭破解之特殊規定 39
4.9.13 憑證暫禁之事由 39
4.9.14 有權請求憑證暫禁者 39
4.9.15 憑證暫禁程序 39
4.9.16 憑證暫禁期間限制 39
4.10 憑證狀態服務 39

4.10.1 服務特性 39
4.10.2 服務之可用性 40
4.10.3 附加功能 40
4.11 憑證終止使用 40
4.12 金鑰託管及復原 40
4.12.1 私密金鑰託管及復原政策與施行 40
4.12.2 加密金鑰封裝及復原政策與施行 40

5 實體、管理及作業流程控管 41

5.1 實體控管 41
5.1.1 建築物與位置 41
5.1.2 實體進出管制 41
5.1.3 電力與空調 41
5.1.4 防水處理 41
5.1.5 防火 41
5.1.6 媒體儲存 41
5.1.7 廢棄處理 42
5.1.8 異地備援 42
5.2 作業程序控管 42
5.2.1 信賴角色 42
5.2.2 作業人員需求人數 42
5.2.3 角色的識別與鑑別 42
5.2.4 角色隔離 42
5.3 人員控管 43
5.3.1 背景、適任條件與經歷 43
5.3.2 背景審核程序 43
5.3.3 教育訓練 43

5.3.4 教育訓練的頻率與需求 43
5.3.5 職務的輪調 43
5.3.6 非授權作業的處罰 43
5.3.7 委外人員需求 43
5.3.8 作業文件需求 44
5.4 稽核記錄程序 44
5.4.1 事件紀錄類型 44
5.4.2 紀錄處理頻率 45
5.4.3 稽核紀錄保留期限 45
5.4.4 稽核紀錄的保護 45
5.4.5 稽核紀錄備份程序 45
5.4.6 稽核紀錄彙整系統 45
5.4.7 對引發事件者之告知 45
5.4.8 弱點評估 45
5.5 紀錄歸檔 45
5.5.1 歸檔紀錄類型 45
5.5.2 歸檔紀錄保留期限 46
5.5.3 歸檔紀錄的保護 46
5.5.4 歸檔紀錄的備份程序 46
5.5.5 歸檔紀錄之時序要求 46
5.5.6 歸檔紀錄彙整系統 46
5.5.7 取得及驗證歸檔紀錄之程序 47
5.6 金鑰更換 47
5.7 金鑰遭破解及災變復原程序 47
5.7.1 金鑰遭破解及緊急應變處理程序 47
5.7.2 電腦資源、軟體及資料損毀之處理程序 47
5.7.3 個體金鑰遭破解之處理程序 47

5.7.4 災變後之營運持續能力 47
5.8 憑證機構終止服務 48

6 技術安全控管 49

6.1 金鑰對的產製及安裝 49
6.1.1 金鑰對的產製 49
6.1.2 私密金鑰遞送至用戶 49
6.1.3 公開金鑰遞送至憑證機構 49
6.1.4 憑證機構公開金鑰遞送至信賴憑證者 49
6.1.5 金鑰長度 49
6.1.6 公開金鑰參數的產生及參數品質檢驗 49
6.1.7 金鑰使用目的 50
6.2 私密金鑰保護措施及密碼模組工程控管 50
6.2.1 密碼模組標準 50
6.2.2 私密金鑰分持控管 50
6.2.3 私密金鑰託管、回復及保存 50
6.2.4 私密金鑰的備份 51
6.2.5 私密金鑰歸檔 51
6.2.6 私密金鑰自密碼模組輸入或輸出 51
6.2.7 私密金鑰儲存於密碼模組 51
6.2.8 私密金鑰啟動方式 51
6.2.9 私密金鑰停用方式 51
6.2.10 私密金鑰銷毀 51
6.2.11 密碼模組等級 52
6.3 金鑰對管理的其他事項 52
6.3.1 公開金鑰歸檔 52
6.3.2 公開金鑰與私密金鑰的有效期限 52

6.4 啟動資料 52
6.4.1 啟動資料產製及安裝 52
6.4.2 啟動資料的保護 53
6.4.3 啟動資料的其他考量 53
6.5 電腦安全控管 53
6.5.1 電腦安全技術需求 53
6.5.2 電腦系統安全等級 53
6.6 生命週期技術控管 54
6.6.1 系統開發控管 54
6.6.2 安全管理控管 54
6.6.3 生命週期的安全等級 54
6.7 網路安全控管 54
6.8 時間戳記 55

7 憑證、憑證廢止清冊及線上憑證狀態查詢剖繪 56

7.1 憑證剖繪 56
7.1.1 版本 56
7.1.2 憑證擴充欄位 56
7.1.3 演算法物件識別碼 56
7.1.4 識別名稱格式 56
7.1.5 識別名稱限制 57
7.1.6 憑證政策物件識別代碼 57
7.1.7 憑證政策限制擴充欄位的使用 57
7.1.8 憑證政策限定元語法與語意 57
7.1.9 憑證政策擴充欄位語意必要的處理 57
7.2 憑證廢止清冊剖繪 57
7.2.1 版本 57

7.2.2 廢止憑證清冊與廢止憑證清單擴充欄位 57
7.3 線上憑證狀態查詢剖繪 57
7.3.1 版本 58
7.3.2 線上憑證狀態查詢擴充欄位 58

8 稽核及其他評估方法 59

8.1 稽核頻率或評估事項 59
8.2 稽核人員之識別及資格 59
8.3 稽核者與受稽核者之關係 59
8.4 稽核項目 59
8.5 稽核結果之因應 59
8.6 稽核結果之公開 59
8.7 內部稽核 60

9 其他業務及法律規定 61

9.1 收費 61
9.1.1 憑證簽發及更新費用 61
9.1.2 憑證查詢費用 61
9.1.3 憑證廢止及狀態查詢費用 61
9.1.4 其他服務費用 61
9.1.5 退費 61
9.2 財務責任 61
9.2.1 賠償責任 61
9.2.2 其他資產 61
9.2.3 對用戶及信賴憑證者之賠償責任 61
9.3 機密資訊 61
9.3.1 機密資訊的種類 61

9.3.2 非機密資訊種類 62
9.3.3 保護機密資訊之責任 62
9.4 個人資訊隱私 62
9.4.1 隱私保護計畫 62
9.4.2 個人隱私資訊種類 62
9.4.3 非個人隱私資訊種類 62
9.4.4 個人隱私資訊保護責任 62
9.4.5 使用個人隱私資訊之告知與同意 62
9.4.6 因行政法令或司法要求之揭露 62
9.4.7 其他資訊公開情形 63
9.5 智慧財產權 63
9.6 職責及義務 63
9.6.1 憑證機構之職責 63
9.6.2 註冊機構之職責 64
9.6.3 用戶之義務 64
9.6.4 信賴憑證者義務 64
9.6.5 其他成員義務 64
9.7 除外責任 64
9.8 責任限制 64
9.9 賠償 65
9.10 本文件生效與終止 65
9.10.1 生效 65
9.10.2 終止 65
9.10.3 終止及存續之效力 65
9.11 通知與聯絡方式 65
9.12 變更及公告 65
9.12.1 變更程序 65

9.12.2 變更聯絡機制 65
9.12.3 物件識別碼變更條件 66
9.13 爭議處理程序 66
9.14 政府管理法規 66
9.15 法規之符合性 66
9.16 各項條款 66
9.16.1 完整合約 66
9.16.2 轉讓 66
9.16.3 存續性 66
9.16.4 施行 67
9.16.5 不可抗力 67
9.17 其他條款 67

附錄一 詞彙(Glossary) 68

附錄二 名詞與簡稱(Acronyms and Abbreviations) 71

1 簡介

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。

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)，擔任信賴起源(Trust Anchor)之最高層憑證管理中心(Root Certification Authority；RCA)，並同時建置下屬憑證管理中心(Subordinate CA)，提供用戶網路身分識別及交易認證的服務，以建立使用者對電子商務交易的信心，確保參與交易雙方的權益。

為提供用戶於從事網際網路交易時所迫切需要之憑證服務，本公司建置認證相關安全機制的網際網路認證服務系統，使用最新穎的公開金鑰密碼機制(public key cryptography)，其安全標準符合財政部「金融機構辦理電子銀行業務安全控管作業基準」，具備網路交易安全所需之不可否認(non-repudiation)、用戶身分的鑑別(authentication)、訊息完整的驗證(verification)、訊息加密的保護(encryption)及其他機制的安全控管(security control)，可用於網際網路電子銀行、網路下單交易，亦可用於保險、票債券、企業詢價報價、採購與付款交易等網際網路電子商務交易系統。

1.1 概述

臺灣網路認證股份有限公司公開金鑰基礎建設(以下簡稱本基礎建設)憑證政策(以下簡稱本政策或 TWCA PKI CP)，係依據電子簽章法及相關國際標準(如 IETF RFC 3647)所訂定之技術政策文件，以做為本基礎建設各憑證機構撰寫憑證實務作業基準之依據。

為配合各種不同行業對電子商務安全控管措施之需求，本基礎建設包含各種不同的憑證機構。各憑證機構的營運作業規範、憑證適用範圍、權責關係以及憑證管理作業的運作機制，均應遵循本憑證政策之規定。

制定本政策時，已特別考慮以下事項：

(1) 信賴憑證者是否能識別憑證記載之憑證持有人(個人戶、企業戶或相關軟硬體及應用系統之用戶)，與憑證記載之公開金鑰(Public Key)的關聯。
(2) 信賴憑證者是否能確認憑證持有人擁有相對應之私密金鑰(Private Key)。
(3) 用戶及信賴憑證者是否能信賴本基礎建設之憑證機構，及其系統、金鑰以

及程序之安全性。

(4) 電子簽章法之規範。

1.2 文件名稱及識別

1.2.1 本政策物件識別碼

本政策依照簽發憑證內容、憑證種類與適用範圍的不同，訂定相對應不同的物件識別碼(Object Identifier；OID)。

本政策之物件識別碼如下：

- { joint-iso-itu-t(2) country(16) Taiwan(158) TWCA(3) CA(1) CP(5) id-TWCA-PKI-CP-policy(5) }

  (2.16.158.3.1.5.5)

- { ISO(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) TWCA(40869) certificates(1) policies(1) }

  (1.3.6.1.4.1.40869.1.1)

依不同憑證種類其憑證政策物件識別碼如下：

商務 XML 憑證：

- { joint-iso-itu-t(2) country(16) Taiwan(158) TWCA(3) CA(1) XML(8) id-CP-policy(5) }

  (2.16.158.3.1.8.5)

- { ISO(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) TWCA (40869) certificates(1) policies(1) XML(12) }

  (1.3.6.1.4.1.40869.1.1.12)

商務 EC 憑證：

- { joint-iso-itu-t(2) country(16) Taiwan(886) TWCA(3) CA(1) EC+(3) id-CP-policy(1) }

  (2.16.886.3.1.3.1)

- { ISO(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) TWCA(40869) certificates(1) policies(1) EC(11) }

  (1.3.6.1.4.1.40869.1.1.11)

商務安全 EC 憑證：(已無使用，未來將淘汰)

- { joint-iso-itu-t(2) country(16) Taiwan(158) TWCA(3) CA(1) EC+(3) id-CP-policy(1) }

  (2.16.158.3.1.3.1)

- { ISO(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) TWCA(40869) certificates(1) policies(1) ECSECURITY(24) }

  (1.3.6.1.4.1.40869.1.1.24)

通關稅費憑證：

- { joint-iso-itu-t(2) country(16) Taiwan(158) TWCA(3) CA(1) FXML(5) id-CP-policy(5) }

  (2.16.158.3.1.5.5)

SSL 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)

- { ISO(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) T WCA(40869) certificates(1) policies(1) DeviceCert(25) }

  (1.3.6.1.4.1.40896.1.1.25) (已無使用，未來將淘汰)

EVSSL 憑證：

- { ISO(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) TWCA(40869) certificates(1) policies(1) EV(22) }

  (1.3.6.1.4.1.40869.1.1.22)

資安憑證：

- { joint-iso-itu-t(2) country(16) Taiwan(158) TWCA(3) CA(1) InfoSec(8) id-CP-policy(5) }

  (2.16.158.3.1.8.5)

- { ISO(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) TWCA(40869) certificates(1) policies(1) InfoSec(23) }

  (1.3.6.1.4.1.40869.1.1.23)

AATL 憑證： ● { ISO (1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) TWCA(40869) certificates(1) policies(1) AATLCert(26) } (1.3.6.1.4.1.40869.1.1.26)
時戳憑證： ● { ISO (1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) TWCA(40869) certificates(1) policies(1) TSACert(27) } (1.3.6.1.4.1.40869.1.1.27)
S/MIME 憑證： ● { ISO (1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) TWCA(40869) certificates(1) policies(1) SMIMECert(28) } (1.3.6.1.4.1.40869.1.1.28)

1.2.2 其他政策物件識別碼

CA/Browser Forum 憑證政策物件識別碼如下：

● {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1)} (2.23.140.1)

依不同憑證種類其憑證政策物件識別碼如下：

TLS BR Organization-validated： ● {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)
EVG： ● {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) extended-validation(1) } (2.23.140.1.1)

S/MIME BR Mailbox-validated：

- {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) mailbox-validated (1) legacy (1)}

  (2.23.140.1.5.1.1)

- {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) mailbox-validated (1) multipurpose (2)}

  (2.23.140.1.5.1.2)

- {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) mailbox-validated (1) strict(3)}

  (2.23.140.1.5.1.3)

S/MIME BR Organization-validated：

- {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) organization-validated (2) legacy (1)}

  (2.23.140.1.5.2.1)

- {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) organization-validated (2) multipurpose (2)}

  (2.23.140.1.5.2.2)

- {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) organization-validated (2) strict (3)}

  (2.23.140.1.5.2.3)

S/MIME BR Sponsor-validated：

- {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) sponsor-validated (3) legacy (1)}

  (2.23.140.1.5.3.1)

- {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) sponsor-validated (3) multipurpose (2)}

  (2.23.140.1.5.3.2)

- {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) sponsor-validated (3) strict (3)}

  (2.23.140.1.5.3.3)

S/MIME BR Individual-validated：

- {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) individual-validated (4) legacy (1)}

  (2.23.140.1.5.4.1)

- {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) individual-validated (4) multipurpose (2)}

  (2.23.140.1.5.4.2)

- {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) individual-validated (4) strict(3)}

  (2.23.140.1.5.4.3)

本基礎建設之各憑證機構，應於憑證實務作業基準中，記載引用之本政策物件識別碼；如因新增憑證適用範圍，須新增物件識別碼以茲識別，必須在本政策定義之各項憑證政策物件識別碼之下進行擴充。

1.3 成員及適用範圍

所有引用本政策之個體，皆為本基礎建設之成員。

本政策規範之自然人或法人的公開金鑰憑證，使用於應用交易系統時，可提供交易的啟動者與交易的接受者之身分識別的驗證、訊息完整性的驗證、訊息隱密性的保護、不可否認性機制的適用性、權責義務及憑證使用時應遵循之作業規範。

1.3.1 憑證機構

憑證機構主要負責憑證之簽發與管理，依照其營運特性區分為最高層憑證機構與下屬憑證機構。

本基礎建設之各憑證機構均應遵循本政策相關規定，並設置聯絡窗口，若憑證機構擔任其他公開金鑰基礎建設之下屬憑證機構時，其上層憑證機構不適用本政策之規範。

最高層憑證機構為本基礎建設之信賴起源(Trust Anchor)，須維持最高的公信力，其營運應依照本政策安全規定之最高等級來運作。

下屬憑證機構為本基礎建設之第二層或第三層憑證機構，第二層憑證機構之憑證係由最高層憑證機構所簽發，第三層憑證機構之憑證係由第二層憑證機構所簽發。

本公司營運管理之 TWCA 最高層憑證管理中心為本基礎建設之最高層憑證機構，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。

下屬憑證機構主要負責以下工作：

(1) 負責用戶憑證之簽發與管理。
(2) 負責註冊中心憑證之簽發與管理。
(3) 管理與公告用戶憑證、憑證廢止清冊於儲存庫。
(4) 維持儲存庫的穩定與運作。

如下屬憑證機構有再簽發憑證予其下屬憑證機構，亦須負責以下工作：

(5) 負責下屬憑證機構憑證之簽發與管理。
(6) 管理與公告下屬憑證機構之憑證及憑證廢止資訊於儲存庫。

1.3.2 註冊中心

註冊中心(Registration Authority；RA)主要負責驗證用戶的身分及憑證所需相關資訊，供憑證機構簽發用戶憑證。

本基礎建設之各憑證機構應於憑證實務作業基準中載明擔任註冊中心之規定。

本基礎建設之各憑證機構，於簽發憑證予下屬憑證機構時，應自行擔任註冊中心，並依其憑證實務作業基準規定執行註冊中心之工作。

1.3.3 用戶

用戶為憑證中憑證主體名稱(Certificate Subject)所記載之終端個體，且持有與憑證公開金鑰相對應之私密金鑰者。用戶憑證之適用範圍，應載明於「憑證實務作業基準」。因應用系統非法律定義具行為能力之個體，若憑證係簽發予應用系統做為識別之用，該憑證用戶為申請憑證之自然人或法人。

1.3.4 信賴憑證者

信賴憑證者即為接受他人(用戶)的憑證，用以驗證簽章訊息之有效性，或使用用戶的憑證作訊息的加密後，將加密的訊息傳送至用戶，以達到通訊雙方訊息內容的私密性。

信賴憑證者應以憑證上所記載之資訊，來決定憑證是否可信賴，或是否可以使用於特定用途。

1.3.5 其他參與者

本基礎建設若有其他新成員欲加入時，必須經由「臺灣網路認證股份有限公司」政策管理中心核定；例如：各憑證機構須與非屬本基礎建設之憑證機構進行交互認證時。

1.4 憑證用途

本政策定義之憑證保證等級及適用範圍概述如下：

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，針對用戶之身分僅有少許可信度，適用於惡意篡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，提供基本之身分鑑別，針對用戶之身分具某種程度可信度，適用於資訊可能被篡改，但不會有惡意篡改之低風險網路環境。
第三級(Class 3)： 中級的保證等級，提供進階之身分鑑別，針對用戶之身分具高可信度，適合應用於有惡意使用者會截取或篡改資訊、較為危險之網路環境。
第四級(Class 4)： 高級(High)的保證等級，提供最高階之身分鑑別，針對用戶之身分具極高可信度，適合應用於潛在威脅很高、或資訊被篡改後復原的代價很高之網路環境。 僅提供憑證機構申請使用。

不同憑證種類適用之保證等級如下：

保證等級	憑證種類
測試級	商務 XML 憑證、商務 EC 憑證、商務安全 EC 憑證、資安憑證
第一級(Class 1)	商務 XML 憑證、商務 EC 憑證、商務安全 EC 憑證、資安憑證
第二級(Class 2)	商務 XML 憑證、商務 EC 憑證、商務安全 EC 憑證、資安憑證、AATL 憑證
第三級(Class 3)	商務 XML 憑證、商務 EC 憑證、商務安全 EC 憑證、資安憑證、AATL 憑證、時戳憑證、SSL 憑證、EVSSL 憑證、S/MIME 憑證
第四級(Class 4)	僅提供憑證機構申請使用。

各憑證機構針對簽發憑證引用本政策之保證等級，以及各保證等級憑證適用範圍之限制，應載明於憑證實務作業基準。用戶及信賴憑證者必須依照憑證實務作業基準載明之憑證保證等級及適用範圍，選擇適用之憑證。

1.4.1 憑證適用範圍

依各憑證機構憑證實務作業基準之規定。

1.4.2 憑證之禁止使用情形

依各憑證機構憑證實務作業基準之規定。

1.5 政策管理

1.5.1 管理單位

本政策的制定、更新、及發布等事宜，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，簡稱 PMA)。

1.5.2 聯絡窗口

用戶對憑證政策有任何修改建議時，請將詳細的建議、說明文件與聯絡資訊，Email 或郵寄至下述的聯絡窗口：

公司名稱	臺灣網路認證股份有限公司(TAIWAN-CA INC.；TWCA)
聯絡人	政策管理中心(Policy Management Authority；PMA)
地址	台北市中正區(100)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

本基礎建設之各憑證機構所訂定之憑證實務作業基準，應經由 PMA 核定。

1.5.4 憑證實務作業基準核定程序

各憑證機構應訂定憑證實務作業基準(Certification Practice Statement；CPS)，並確保其憑證實務作業基準與本政策規範相符；另依據電子簽章法規定，憑證機構訂定之憑證實務作業基準，必須經主管機關經濟部核定後，始得對外提供簽發憑證服務。

1.6 名詞與簡稱

參考附錄二。

2 公布及儲存庫

2.1 儲存庫

儲存庫係提供憑證、憑證廢止清冊、憑證狀態、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。本基礎建設之各憑證機構至少需有一個對外服務的儲存庫，並應於憑證實務作業基準中載明儲存庫的網址，並確保儲存庫之可用性、存取控制及資料完整性。

2.2 憑證資訊之公布

憑證機構應將用戶及信賴憑證者使用憑證必需之資訊，包括但不限於憑證實務作業基準、憑證廢止清冊等資訊加以公布。其他應行公布之憑證機構資訊，依各憑證機構之憑證實務作業基準之規定。

憑證機構若簽發 SSL 憑證、EVSSL 憑證或 S/MIME 憑證，其憑證實務作業基準須滿足 CA/Browser Forum 制定之「Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates」(以下簡稱 TLS BR)或「Guidelines for the Issuance and Management of Extended Validation Certificates」(以下簡稱 EVG)或「Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates」(以下簡稱 S/MIME BR)之規定。

2.3 公布頻率

憑證機構資訊之公布頻率，依各憑證機構之憑證實務作業基準之規定。

廢止憑證清冊(CRL)之公布頻率，必須於憑證實務作業基準中規範。

假如 CA 簽發公開信任的憑證，CA 必須開發、建置、執行與修訂 CP/CPS 以詳細載明這些要求的最新狀況。

憑證機構若簽發 SSL 憑證、EVSSL 憑證或 S/MIME 憑證，必須每年對憑證政策和憑證實務作業基準進行檢閱或修訂，並說明如何符合 TLS BR 或 EVG 或 S/MIME BR 之規定。

2.4 儲存庫之存取控制

憑證機構應於憑證實務作業基準中，訂定儲存庫存取控制之規範。

3 識別與鑑別

本基礎建設之各憑證機構，必須於憑證實務作業基準與註冊作業規範，訂定用戶身分識別與鑑別的作業程序。

3.1 命名

3.1.1 名稱種類

各憑證機構必須可簽發以 X.500 唯一識別名稱為主體名稱之 X.509 憑證。憑證機構應於其憑證實務作業基準中，規範其名稱種類。

憑證機構可視需要使用擴充的主體別名(Subject Alternate Name)擴充欄位，但不可單獨使用主體別名而主體名稱為空白，且主體別名亦須符合 X.500 標準的命名方式。

3.1.2 識別名稱之意義

憑證所記載之主體識別名稱，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

本政策不允許用戶使用匿名、假名、別名或筆名等。

3.1.4 各種名稱的解釋規則

用戶名稱的解釋規則，應依照各主管機關訂定的規範處理，例如網際網路帳號的識別名稱，為依照財政部賦稅署財稅資料中心編訂的銀行代碼，及銀行使用的用戶帳號之規範處理，個人的身分證統一編號識別名稱，為依照內政部訂定的規範處理，企業的營利事業統一編號識別名稱，為依照經濟部訂定的規範處理，其他用戶識別名稱解釋規則，則依照各憑證機構的憑證實務作業基準處理。

3.1.5 名稱的唯一性

各憑證機構應確保其所簽發之憑證名稱之唯一性，並於其憑證實務作業基準中訂定命名之原則及如何確保其唯一性。

3.1.6 識別名稱糾紛的處理

當註冊之識別名稱有相同時，憑證機構應以先申請註冊者優先使用為原則，惟其他申請者提出相關主管機關/機構出具證明文件時，憑證機構應進行命名糾紛之處理。

各憑證機構應於憑證實務作業基準中，規範命名糾紛之處理程序。

3.1.7 商標之辨識、鑑別及角色

依各憑證機構之憑證實務作業基準之規定。

3.2 初始驗證

3.2.1 證明擁有私密金鑰的方式

若憑證內公開金鑰及對應之私密金鑰由憑證用戶自行產製，則憑證機構必須要求用戶提供擁有私密金鑰之證明，如以簽章訊息之驗證來確認用戶為私密金鑰擁有者(如使用 RFC 2314、RFC 2510、RFC 2511 標準中之方法)。

若由註冊中心、憑證機構或其他經授權之第三者為用戶產製私密金鑰，則不須驗證用戶是否為私密金鑰之擁有者，但必須於憑證實務作業基準中規範傳送私密金鑰給憑證用戶的安全控管措施。

3.2.2 法人身分的鑑別

對組織進行身分鑑別時，組織必須提供主管機關核發，或其他可資證明組織存在之證明文件，並驗證代表人之身份，以及是否經組織授權。如為組織授權代理人辦理，須驗證代理人的相關身分證明文件，以書面資料遞交或由代理人以等同於當面辦理認證強度的方式辦理。

憑證機構必須於憑證實務作業基準中訂定法人用戶身分鑑別程序，且註冊中心應遵循憑證實務作業基準之規範發布法人用戶身分鑑別策略，並根據已發布之策略執行法人用戶身分鑑別。

以下為各保證等級對法人身分鑑別程序之要求：

測試級： 若憑證機構有簽發法人測試級憑證，則各憑證機構應於憑證實務作業基準中規範。
第一級： 1. 法人用戶以自我主張之身分資訊進行註冊。 2. 註冊中心應檢核該資訊之唯一性並進行有限之查證。

第二級： 1. 應滿足前述第一級相關檢核。 2. 法人用戶應提交證據證明其法人身分資訊。 3. 註冊中心應檢核該證據的存在性和有效性。
第三級： 1. 應滿足前述第二級相關檢核。 2. 代表人或持有授權文件之代理人，應提供足以識別法人身分之證明文件。 3. 註冊中心應以類似於當面認證強度的方式辦理，並查詢信賴的第三方權威資訊，檢查法人用戶主張之身分資訊或只有該法人用戶所知的資訊。
第四級： 1. 應滿足前述第三級相關檢核。 2. 註冊中心應以當面認證的方式辦理。

對於法人擁有之資訊或通訊軟硬體設備(如路由器、防火牆、伺服器等)初始驗證時，另需由其設備管理者提供下列註冊資訊：

(1) 設備識別(如序號)或服務名稱(如網域名稱)。
(2) 設備公開金鑰。
(3) 設備授權用途及屬性(如授權用途或屬性須被包含在憑證中才須提供)。
(4) 供註冊中心或憑證機構進行聯繫之管理者聯絡資訊。
(5) 憑證機構應以相當於所申請憑證保證等級之方式驗證註冊資料。驗證方式包括但不限於本節所訂定之方式，對用戶進行身分鑑別或以用戶之數位簽章為之(簽章之憑證必須是遵循本政策所簽發)。

針對 SSL 憑證以及 EVSSL 憑證，憑證機構應依遵循 TLS BR 及 EVG 之規範，對申請者所提供之網域、IP 進行所有權查驗作業，且憑證機構使用之查驗方式須於憑證實務作業基準中載明。

針對 S/MIME 憑證，憑證機構應依遵循 S/MIME BR 之規範，對申請者所提供之 Email 網域、Email 信箱進行所有權查驗作業，且憑證機構使用之查驗方式須於憑證實務作業基準中載明。

申請者或會被要求提供更多資訊、進行更多驗證作業方式以符合同等級之信任要求。

3.2.3 個人用戶身分的鑑別

憑證機構必須於憑證實務作業基準中訂定個人用戶身分鑑別程序，且註冊中心應遵循憑證實務作業基準之規範發布個人用戶身分鑑別策略，並根據已發布之策略執行個人用戶身分鑑別。

以下為各保證等級對個人用戶身分鑑別程序之要求：

測試級： 若憑證機構有簽發個人測試級憑證,則各憑證機構應於憑證實務作業基準中規範。
第一級： 1. 個人用戶以自我主張之身分資訊進行註冊。 2. 註冊中心應檢核該資訊之唯一性並進行有限之查證。
第二級： 1. 應滿足前述第一級相關檢核。 2. 個人用戶應提交證據證明其個人身分資訊。 3. 註冊中心應檢核該證據的存在性和有效性。
第三級： 1. 應滿足前述第二級相關檢核。 2. 本人或持有授權文件之代理人，應提供足以識別個人身分之證明文件。 3. 註冊中心應以類似於當面認證強度的方式辦理，並查詢信賴的第三方權威資訊，檢查個人用戶主張之身分資訊或只有該個人用戶所知的資訊。
第四級： 不適用。

對個人持有之資訊或通訊軟硬體設備，個人等同設備管理人，應依照 3.2.2 節規定辦理。

3.2.4 未驗證之用戶資訊

無規定。

3.2.5 權限之驗證

個人、法人之代表人、代理人及法人(下稱該等人)之身分證明文件，應為官方核發之證明文件(下稱該文件)；註冊中心須確認代理人授權文件之真偽，該等人應具結該文件為真實。

3.2.6 相互溝通方式

無規定。

3.3 金鑰更新之識別與鑑別

各憑證機構之用戶應依據下列之身分鑑別需求，進行金鑰更新作業之用戶身分識別與鑑別：

測試級： 無規定。
第一級： 無規定。
第二級： 可使用約定之帳號密碼或目前之簽章用金鑰進行身分鑑別。
第三級： 可使用目前之簽章用金鑰進行身分鑑別。
第四級： 每次金鑰更新皆須進行初始驗證。

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。故對憑證用戶而言，應定期更換金鑰以確保金鑰之安全性。對憑證進行金鑰更換係指重新產生一組公開金鑰及私密金鑰對，並以舊有的註冊資訊向憑證機構申請憑證簽發。金鑰更新後之新憑證與舊有憑證具有相同的特徵及保證等級。

憑證機構應於憑證實務作業基準中規範，例行性金鑰更新之用戶身分識別與鑑別需求。

3.3.2 憑證廢止後之金鑰更換

用戶憑證廢止後，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

憑證機構應對憑證廢止請求進行鑑別。對憑證廢止請求之鑑別，可以對憑證相對應之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。

4 憑證生命週期管理

4.1 憑證申請

4.1.1 憑證申請者

憑證使用者為自然人時，本人即為憑證申請者；憑證使用者為法人時，法人之代表人或其代理人即為憑證申請者。

4.1.2 申請登記程序及責任

憑證申請者應事先閱讀憑證使用約定事項，於同意後填寫憑證申請表格交予註冊中心。

憑證機構必須於憑證實務作業基準中訂定傳送公開金鑰至憑證簽發者之方式。

4.2 憑證申請程序

4.2.1 識別與鑑別程序

當憑證申請者申請憑證時，註冊中心應遵循以下規範：

(1) 依照 3.2 節規定，取得申請者之憑證申請相關資料。
(2) 依照 3.2 節規定，驗證並記錄申請者之識別資料。
(3) 依照 3.2 節規定，取得申請者之公開金鑰並檢核其與私密金鑰之關聯。
(4) 確認將記載在憑證內的資訊是否正確。

上述規範的詳細進行步驟，由各憑證機構自行訂定並載明於憑證實務作業基準；上述規範事項，應於憑證簽發前完成。

4.2.2 接受或拒絕憑證申請

完成 4.2.1 識別與鑑別程序後，視為接受憑證申請，如未能完成識別與鑑別程序，應拒絕憑證申請。

若憑證機構和註冊機構簽發 SSL 憑證、EVSSL 憑證或 S/MIME 憑證，於接受憑證申請和簽發憑證時應遵循業界標準(例如 TLS BR、EVG 或 S/MIME BR)，並於憑證時務作業基準中載明。

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

所有註冊中心與憑證機構之間的通訊均應進行身分鑑別，通訊的方式可採連線或離線的方式，通訊時應保護資訊的完整性和隱密性。

憑證申請者之公開金鑰在傳送至憑證機構時，憑證機構必須確認其申請資料與公開金鑰正確連結無誤。憑證機構可以使用密碼學的方法來確保此連結，亦可使用非密碼學之實體上或程序上方法來進行，包括但不限於使用磁碟片(或其他儲存裝置)以掛號或快遞來傳送。

憑證機構收到憑證簽發要求時應：

(1) 驗證傳送者的身分。
(2) 檢查傳送資料之完整性。
(3) 確認憑證簽發要求的內容，符合簽發憑證內容之規定後，方產製並簽發憑證。

4.3.2 憑證機構簽發憑證通知用戶

憑證機構於簽發憑證後，應以適當的方式通知憑證已簽發，並傳遞憑證予用戶；如憑證機構不同意簽發憑證，應以適當之方式通知用戶，並明確告知不同意簽發憑證的理由；上述之通知及傳遞，亦可透過註冊中心執行。

除憑證簽發要求未能通過驗證之原因外，憑證機構得因其他事由不同意簽發憑證。

4.4 憑證接受

憑證機構之憑證實務作業基準應規範：

(1) 用戶憑證接受程序。
(2) 憑證申請者接受憑證前已確實了解使用憑證之責任與義務。
(3) 如何告知憑證申請者簽發之憑證內容。
(4) 若憑證申請者審視憑證內容後，拒絕接受所簽發之憑證，則註冊中心應通知憑證機構廢止該憑證。

4.4.1 憑證接受之程序

憑證用戶於收到憑證後，應確認憑證記載的內容是否正確，並確實了解憑證使用之

約定條款後，方可開始使用憑證。

4.4.2 憑證機構公布憑證

各憑證機構於簽發憑證後，得將憑證公布於儲存庫。

4.4.3 憑證機構通知其他機構憑證簽發

各憑證機構於簽發憑證後，除傳遞憑證予憑證用戶外，亦可傳遞憑證予註冊中心。

4.5 金鑰對及憑證用途

4.5.1 用戶私密金鑰及憑證使用

用戶為持有與憑證公開金鑰相對應之私密金鑰者，憑證適用範圍決定了用戶私密金鑰的用途。各憑證機構簽發之用戶憑證，其適用範圍應載明於「憑證實務作業基準」。

用戶的私密金鑰有被冒用、曝露及遺失等疑慮時，用戶必須依憑證機構之憑證實務作業基準之規定，向註冊中心或憑證機構辦理申告。

用戶憑證與其相對應私密金鑰的使用範圍和限制，必須遵循本政策與憑證機構之憑證實務作業基準的規定。

4.5.2 信賴憑證者公開金鑰及憑證使用

本政策未規定信賴憑證者在決定信任憑證時必須進行之檢驗步驟。信賴憑證者檢驗憑證時，仍應依循各憑證機構之憑證實務作業基準相關規定，進行憑證信賴路徑建立、憑證驗證，以作為是否信任憑證之參考依據；信賴憑證者應於信任憑證後，方可將其用於檢驗電子文件數位簽章之正確性及檢驗電子文件簽章者身分。

4.6 憑證展期

4.6.1 憑證展期之事由

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。

本基礎建設之各憑證機構，可自行決定是否接受憑證展期。

4.6.2 有權展期憑證者

憑證用戶有權展期憑證。

4.6.3 憑證展期程序

(1) 用戶於憑證有效期結束前，應使用原有的用戶註冊資料及公開金鑰向註冊中心/憑證機構申請新憑證的簽發。
(2) 用戶進行憑證展期時，憑證機構應確認註冊資料及公開金鑰的正確性。
(3) 依照 4.3 節之規定簽發憑證。

4.6.4 通知用戶展期憑證之簽發

依 4.3.2 節之規定。

4.6.5 展期憑證接受程序

依 4.4 節之規定。

4.6.6 憑證機構公布展期憑證

依 4.4.2 節之規定。

4.6.7 憑證機構通知其他機構展期憑證之簽發

依 4.4.3 節之規定。

4.7 憑證及私密金鑰更新

4.7.1 憑證及私密金鑰更新之事由

對憑證進行金鑰更換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。

本基礎建設之各憑證機構，應自行規範憑證及私密金鑰更新之程序。

4.7.2 有權更新憑證金鑰者(憑證金鑰更換申請者)

憑證用戶有權更新憑證金鑰。

4.7.3 憑證金鑰更新程序

(1) 依照 3.3 節之規定對用戶進行身分識別與鑑別。
(2) 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。

4.8.1 憑證變更之事由

依各憑證機構憑證實務作業基準之規定。

4.8.2 有權變更憑證者

依各憑證機構憑證實務作業基準之規定。

4.8.3 憑證變更程序

依各憑證機構憑證實務作業基準之規定。

4.8.4 通知用戶變更憑證之簽發

依各憑證機構憑證實務作業基準之規定。

4.8.5 變更金鑰憑證接受程序

依各憑證機構憑證實務作業基準之規定。

4.8.6 憑證機構公布變更憑證

依各憑證機構憑證實務作業基準之規定。

4.8.7 憑證機構通知其他機構變更憑證之簽發

依各憑證機構憑證實務作業基準之規定。

4.9 憑證廢止及暫禁

若憑證機構係簽發 SSL 憑證、EVSSL 憑證或 S/MIME 憑證，其憑證廢止作業規範須符合 TLS BR、EVG 或 S/MIME BR 之規定並於憑證實務作業基準中載明。

4.9.1 憑證廢止之事由

(1) 用戶欲終止該憑證的使用，或用戶憑證相關合約的終止。
(2) 憑證在有效期間內，憑證內的用戶相關資訊有更動時。
(3) 與憑證相關的私密金鑰經證實或懷疑遭破解、毀損、遺失、曝露、被篡改時。
(4) 用戶違反憑證政策、憑證實務作業基準或用戶合約時。
(5) 憑證機構簽章用金鑰證實或懷疑遭破解。

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，直到憑證過期為止。

4.9.2 有權請求廢止憑證者

各憑證機構應於其憑證實務作業基準中載明有權請求廢止憑證者之規範。

4.9.3 憑證廢止程序

憑證廢止請求須指明欲廢止之憑證並提出廢止原因，各憑證機構應於其憑證實務作業基準中載明廢止憑證之程序。

4.9.4 憑證廢止請求提出期限

各憑證機構應於憑證實務作業基準中規範用戶提出憑證廢止請求之期限。

4.9.5 憑證機構處理憑證廢止請求時限

各憑證機構應於憑證實務作業基準中規範處理憑證廢止請求之時限。

4.9.6 信賴憑證者憑證廢止檢驗規定

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。信賴憑證者在使用用戶憑證，驗證用戶之數位簽章時，應檢查用戶憑證是否為廢止狀態。

憑證機構應於憑證實務作業基準中載明，信賴憑證者查驗憑證廢止清冊之需求。

4.9.7 憑證廢止清冊簽發頻率

憑證機構原則上應定期產生憑證廢止清冊(Certificate Revocation List；CRL)，處理完成之憑證廢止資訊應於 CRL 內之「下次更新」欄位記載之時間內進行更新，並於 CRL 下次更新時加入該廢止資訊供信賴憑證者查詢；於 CRL 產生頻率之間隔時間內沒有用戶申請廢止憑證時，憑證機構亦必須執行 CRL 的簽發作業。

憑證機構產生憑證廢止清冊(CRL)的頻率，原則上為每 24 小時一次，但可依各別憑證機構實務需求而有不同的產生頻率。

各憑證機構應於憑證實務作業基準中，規範簽發 CRL 之頻率。

4.9.8 憑證廢止清冊最大潛在因素

憑證廢止清冊最大潛在因素係指 CRL 產生到實際公布於儲存庫之時間落差。

本政策不做規範。

4.9.9 線上廢止/狀態查詢服務

各憑證機構可視需要提供線上憑證狀態查詢服務(Online Certificate Status Protocol；OCSP)。由於並非所有信賴憑證者端之應用軟體都可進行即時之查詢，各憑證機構至少應提供憑證廢止清冊下載服務，並於憑證實務作業基準中載明，是否提供線上憑證狀態查詢服務。

4.9.10 線上廢止/狀態查詢檢驗規定

由各憑證機構於憑證實務作業基準中規範。

4.9.11 其他形式之廢止公告

憑證機構以其他形式提供之憑證狀態查詢功能，必須於憑證實務作業基準規範其作業方式，且資料保護方式至少應等同憑證廢止清冊之方式實施。

4.9.12 金鑰遭破解之特殊規定

各憑證機構之簽章金鑰遭破解時，應依照以下原則辦理：

(1) 廢止已簽發之有效憑證。
(2) 更新憑證廢止清冊或線上憑證狀態查詢服務之憑證狀態資訊。
(3) 產生新的簽章用金鑰對及相對應的新憑證。
(4) 告知下層憑證機構金鑰已被破解。
(5) 若為下層憑證機構之金鑰遭破解，應於 24 小時內告知其上層憑證機構。
(6) 使用新的簽章用金鑰依照 4.2、4.3 節之規定重新簽發憑證。
(7) 依 6.1.4 節之規定遞送新憑證。

各憑證機構應於憑證實務作業基準中載明金鑰遭破解之處理程序。

4.9.13 憑證暫禁之事由

依各憑證機構之憑證實務作業基準之規定。

4.9.14 有權請求憑證暫禁者

依各憑證機構之憑證實務作業基準之規定。

4.9.15 憑證暫禁程序

除簽發用戶憑證之憑證機構外，不得提供憑證暫禁服務。

簽發用戶憑證之憑證機構若提供用戶憑證暫禁服務時，應於其憑證實務作業基準中載明憑證暫禁程序。

4.9.16 憑證暫禁期間限制

依各憑證機構之憑證實務作業基準之規定。

4.10 憑證狀態服務

4.10.1 服務特性

參閱 4.9.9、4.9.11 及 4.9.13 節之規定。

憑證機構須在廢止之用戶憑證效期到期後，方可將憑證廢止資訊自憑證狀態服務中移除。

4.10.2 服務之可用性

參閱 4.9.9、4.9.11 及 4.9.13 節之規定。

若憑證機構簽發 SSL 憑證、EVSSL 憑證或 S/MIME 憑證，憑證狀態服務之可用性須符合 TLS BR、EVG 或 S/MIME BR 之規定並於憑證實務作業基準中載明。

4.10.3 附加功能

參閱 4.9.9、4.9.11 及 4.9.13 節之規定。

4.11 憑證終止使用

各憑證機構簽發之憑證，於憑證廢止、效期屆滿或憑證機構結束營運時即失效。

4.12 金鑰託管及復原

4.12.1 私密金鑰託管及復原政策與施行

參閱 6.2.3 節。

4.12.2 加密金鑰封裝及復原政策與施行

不做規定。

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

各憑證機構設備所在位置之建築，應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憑證機構相關設備。

5.1.2 實體進出管制

各憑證機構之實體進出管制至少須滿足以下要求：

(1) 防止未授權者存取硬體設備。
(2) 確保所有內含敏感性資訊之可移除式媒體或紙本文件，皆存放在安全的地點。
(3) 全天候以人工或自動化方式監控及記錄未經授權的存取。
(4) 定期檢視存取紀錄並確保其可用性。

各憑證機構放置憑證簽發設備之機房須具備存取控制措施，至少須要兩人以上方可進行存取。

5.1.3 電力與空調

各憑證機構須具備足夠的電力及空調備援設備，當受到外在因素影響時，能夠正常運作或關閉設備。同時，必須提供備用電力系統，至少提供 6 小時的備用電力以供儲存庫備援資料。

5.1.4 防水處理

各憑證機構之設備，應安裝於能防止水災的地點。

5.1.5 防火

各憑證機構之機房應具有自動滅火設備，於偵測到發生火災時，能自動啟動滅火功能，並設置手動開關於各主要出入口，以供現場人員於緊急情況時以手動方式操作。

5.1.6 媒體儲存

各憑證機構之媒體儲存環境，應能防止媒體的意外毀損；重要之資料備份媒體須儲存於憑證機構所在地以外的地點。

5.1.7 廢棄處理

各憑證機構對敏感性資訊必須制定安全的清除與銷毀程序，且應載明於憑證實務作業基準。

5.1.8 異地備援

各憑證機構應具備異地備援設施，並於憑證實務作業基準中載明異地備援機制。

5.2 作業程序控管

5.2.1 信賴角色

各憑證機構之憑證管理作業必須在嚴密、安全的作業流程下進行。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，各憑證機構應於憑證實務作業基準中規範信賴角色及其分工。

本政策定義四種信賴角色及其概略分工如下：

(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)負責產生憑證申請請求檔、執行憑證廢止及簽發。
(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

各憑證機構應於憑證實務作業基準中，規範作業人員之需求人數，且須符合 5.2.1 節之規定。

若憑證機構簽發 EVSSL 憑證，簽發憑證前必須至少通過 2 人確認後方可執行憑證簽發。

5.2.3 角色的識別與鑑別

作業人員必須經過身分識別與鑑別方可執行各角色任務。

5.2.4 角色隔離

各憑證機構應依以下原則進行角色隔離：

(1) 具備 5.2.1 所述之四種信賴角色。
(2) 憑證主管人員與系統管理人員不得兼任。

(3) 憑證主管人員與稽核人員不得兼任。
(4) 系統管理人員與稽核人員不得兼任。
(5) 操作人員與憑證主管人員不得兼任。
(6) 操作人員與稽核人員不得兼任。

5.3 人員控管

5.3.1 背景、適任條件與經歷

各憑證機構必須訂定執行憑證管理作業人員的適任條件，至少必須具備忠實、可信賴之特性，並無違法或信用不良之紀錄。憑證實務作業基準亦應訂定作業人員之適任條件，如有須進用委外人員之需求時，亦須訂定委外人員職務擔任的適任條件。

5.3.2 背景審核程序

各憑證機構對於負責執行憑證管理系統之作業人員，必須訂定身分背景與執行職務的審核規範，並符合 5.3.1 節之要求。

5.3.3 教育訓練

各憑證機構的作業人員，應依照其職務，施予憑證管理系統運作所應具備的軟硬體功能、作業程序、安控程序、CP、CPS 及其他相關技術與作業規範的訓練。

5.3.4 教育訓練的頻率與需求

各憑證機構對於營運環境變更或安全管理機制變更時，須再給予人員提供適當的教育訓練，並於憑證實務作業基準中規範教育訓練計畫與頻率。

5.3.5 職務的輪調

各憑證機構可訂定職務輪調的作業規範，並載明於憑證實務作業基準。

5.3.6 非授權作業的處罰

各憑證機構應於憑證實務作業基準中載明發生非授權作業之懲處程序。

5.3.7 委外人員需求

各憑證機構應於憑證實務作業基準中載明委外人員之控管程序。

5.3.8 作業文件需求

各憑證機構之作業文件，至少須能滿足各角色人員執行維運作業所需。憑證機構應於憑證實務作業基準中載明作業文件需求。

5.4 稽核記錄程序

5.4.1 事件紀錄類型

各憑證機構之稽核紀錄無論是手動或自動，至少須包含如下項目：

(1) 事件類型。
(2) 事件發生的日期與時間。
(3) 事件發生之地點或位置。
(4) 執行憑證簽發或廢止作業時，其成功或失敗的結果。
(5) 引發事件之個體或個人。

事件發生時，稽核紀錄可由憑證機構自行決定以電子或實體方式記錄，憑證機構應記錄之稽核事件種類如下：

(1) 安全稽核管理作業。
(2) 人員及信賴角色管理、識別、鑑別。
(3) 用戶資訊的建置、修改與刪除。
(4) 憑證機構金鑰產製。
(5) 私密金鑰及受信賴公開金鑰的變更。
(6) 憑證申請、簽發、廢止、狀態變更。
(7) 憑證管理系統組態設定及變更。
(8) 系統及應用程式啟動或關閉。
(9) 人員登入及登出系統及應用程式。
(10) 密碼模組安裝、移除及銷毀。
(11) 門禁管理及實體環境存取。
(12) 硬體及軟體系統之更新。
(13) 資料備份及復原。
(14) 未授權之檔案系統存取。
(15) 異常網路系統存取。
(16) 金鑰遭破解、系統異常及危害。
(17) 憑證政策及憑證實務作業基準之違反。

5.4.2 紀錄處理頻率

各憑證機構至少應每月一次進行稽核紀錄檢視。檢視時應檢查稽核紀錄的完整性，確保稽核紀錄未被竄改，並審視所有紀錄項目，對於不正常或任何警訊應審慎加以調查。檢視結果之因應方案必須以文件記錄之。

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應於憑證機構所在處保留 2 個月，除錄影媒體紀錄外，相關稽核紀錄移除前應進行紀錄歸檔。

5.4.4 稽核紀錄的保護

各憑證機構必須防止未經授權人員讀取稽核紀錄及進行稽核紀錄的備份，並防止稽核紀錄遭竄改。

5.4.5 稽核紀錄備份程序

各憑證機構必須於憑證實務作業基準中訂定稽核紀錄的備份程序，至少每個月進行一次稽核紀錄的備份，且儲存一份備份在憑證機構所在地之外的備援地點。

5.4.6 稽核紀錄彙整系統

稽核紀錄的蒐集，可於憑證機構之憑證管理系統外部或內部進行。自動稽核程序應由憑證管理系統啟動，且須持續到憑證管理系統關閉為止。稽核紀錄之蒐集可經由作業系統、憑證管理系統與憑證管理作業人員，以電腦自動或人員手動的方式記錄之。

5.4.7 對引發事件者之告知

當出現之事件被稽核系統記錄時，無須通知產生該事件之相關人員。出現異常事件紀錄之通報程序，應於各憑證機構之憑證實務作業基準中規範。

5.4.8 弱點評估

各憑證機構應針對安全控制進行定期之弱點評估。

5.5 紀錄歸檔

5.5.1 歸檔紀錄類型

各憑證機構之歸檔紀錄至少應包含以下種類：

(1) 憑證機構接受外部評鑑的資料
(2) 憑證實務作業基準
(3) 與憑證機構營運相關之合約
(4) 系統環境建置與設定檔
(5) 系統變更紀錄
(6) 憑證申請檔
(7) 所有簽發與公告之憑證
(8) 金鑰更換紀錄
(9) 稽核資料檔
(10) 廢止要求紀錄
(11) 用戶註冊資料
(12) 用戶合約
(13) 廢止憑證資料檔
(14) 用來驗證歸檔紀錄之資料與工具
(15) 稽核人員所要求之文件

若憑證機構有代管用戶之加密金鑰，亦應一併進行歸檔。

5.5.2 歸檔紀錄保留期限

各憑證機構之歸檔資料保存期間最少 7 年且不得早於相關金鑰銷毀、憑證過期或廢止後 2 年，並應於憑證實務作業基準中規範歸檔資料之保存期間。

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。屬於用戶之已歸檔個別資料，允許提供予該用戶、該用戶授權之人員及法規允許之機構。歸檔資料必須保存一份於具安全管控措施，且對儲存媒體無害的其他地點。

5.5.4 歸檔紀錄的備份程序

各憑證機構於憑證實務作業基準中自行規定。

5.5.5 歸檔紀錄之時序要求

各憑證機構於憑證實務作業基準中自行規定。

5.5.6 歸檔紀錄彙整系統

各憑證機構於憑證實務作業基準中自行規定。

5.5.7 取得及驗證歸檔紀錄之程序

各憑證機構於憑證實務作業基準中自行規定。

5.6 金鑰更換

為降低憑證機構簽章用金鑰遭破解的風險，憑證機構之金鑰必須定期進行更換(Key Changeover)，完成更換後，原金鑰即不可用於簽發憑證。

各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，且不可超過本政策 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

各憑證機構應訂定緊急應變處理程序和災變復原計畫。

各憑證機構應以書面記載業務持續計畫與災變復原程序，內容應包含當發生災難、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。

若憑證機構簽發 SSL 憑證、EVSSL 憑證或 S/MIME 憑證，其金鑰遭破解及緊急應變處理程序應符合 TLS BR、EVG 或 S/MIME BR 之規定，並於憑證實務作業基準中載明。

5.7.2 電腦資源、軟體及資料損毀之處理程序

各憑證機構使用的設備有異常毀損時，必須盡快重新建置，並以能產製憑證狀態資訊為優先考量。各憑證機構應於憑證實務作業基準規範其復原程序，且至少每年進行一次電腦資源、軟體與資料毀損之復原演練。

5.7.3 個體金鑰遭破解之處理程序

各憑證機構應於憑證實務作業基準或相關文件中載明，本基礎建設各成員之簽章金鑰遭破解之處理程序。

5.7.4 災變後之營運持續能力

各憑證機構應於憑證實務作業基準中載明，發生自然災害或其他災變時，在安全環境重建前，憑證機構用以救援其設備及持續營運之程序。

5.8 憑證機構終止服務

各憑證機構應於憑證實務作業基準，載明結束營運時應進行之程序，並應符合電子簽章法之規定。

6 技術安全控管

6.1 金鑰對的產製及安裝

6.1.1 金鑰對的產製

金鑰產製過程應載明於憑證實務作業基準。憑證機構之金鑰產製設備至少應符合 FIPS 140-2 Level 3 或 FIPS 140-3 Level 3 的硬體密碼模組。

各憑證機構應於憑證實務作業基準中載明用戶金鑰對產製之規定。

6.1.2 私密金鑰遞送至用戶

各憑證機構如提供代替用戶產生金鑰對的服務時，應於憑證實務作業基準中載明私密金鑰遞送之安全控管措施。

6.1.3 公開金鑰遞送至憑證機構

用戶之公開金鑰傳送至憑證機構時，應確保資料的鑑別性。公開金鑰的傳遞方式可採電子簽章的訊息、實體媒體(如磁片)透過快遞或申請人親自送達或其他方式傳送。

各憑證機構之憑證實務作業基準，應制定用戶公開金鑰傳送至憑證機構的方式。

6.1.4 憑證機構公開金鑰遞送至信賴憑證者

各憑證機構之公開金鑰有遞送需求時，公開金鑰憑證至少必須具有訊息完整性的保護。

6.1.5 金鑰長度

憑證機構之 RSA 金鑰長度至少必須為 2048 bits(含)以上；ECC 金鑰使用之曲線其安全強度必須至少為 P-256。

用戶憑證之 RSA 金鑰長度至少必須為 2048 bits(含)以上；ECC 金鑰使用之曲線其安全強度必須至少為 P-256。

6.1.6 公開金鑰參數的產生及參數品質檢驗

各憑證機構公開金鑰參數的產生與選取，必須由符合 FIPS 186-4 或類似此規範的亂數產生器(random number generator)產生質數參數，或其公開金鑰參數亂數的產生符合 FIPS 140-2 或 FIPS 140-3 規範標準。

如用戶使用硬體密碼模組(如 IC 卡)，建議使用至少符合 FIPS 140-2 Level 2 或 FIPS 140-3 Level 2 或符合此安全等級規範的硬體密碼模組。

6.1.7 金鑰使用目的

金鑰使用目的限制，記載於 X.509 憑證之金鑰使用目的擴充欄位中。

憑證機構憑證應只設定 keyCertSign 及 cRLSign 兩位元，僅可用來作憑證簽發及憑證廢止清冊簽發。

用戶之簽章憑證應設定 digitalSignaure 及(或) nonRepudiation 位元，加密憑證則應設定 keyEncipherment 及(或) dataEncipherment 位元。

除簽章及加密憑證的需求外，憑證機構如簽發其他用途的憑證時，必須於憑證實務作業基準中載明金鑰使用目的。

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

憑證機構的密碼模組,必須至少使用通過 FIPS 140-2 Level 3 或 FIPS 140-3 Level 3，或符合此安全等級規範的硬體密碼模組。

註冊中心使用硬體憑證載具時，建議使用至少符合 FIPS 140-2 Level 2 或 FIPS 140-3 Level 2，或符合此安全等級規範的硬體憑證載具。

用戶使用硬體憑證載具時,建議使用至少符合 FIPS 140-2 Level 2 或 FIPS 140-3 Level 2，或符合此安全等級規範的硬體憑證載具。

各憑證機構之密碼模組，其安全管制措施必須具備多人控管之功能。

6.2.2 私密金鑰分持控管

憑證機構的簽章用私密金鑰，必須符合第 5 章之多人控管程序。

6.2.3 私密金鑰託管、回復及保存

各憑證機構的簽章用私密金鑰不得進行託管。

各憑證機構如提供用戶私密金鑰的託管、回復及保存時，於憑證實務作業基準必須訂定相關的作業規範。

6.2.4 私密金鑰的備份

憑證機構私密金鑰儲存於加密後的硬體密碼模組內，備份時必須以多人分持控管的方式進行，並儲存於備援場所；私密金鑰備份程序應載明於憑證實務作業基準。

註冊中心及用戶私密金鑰的備份與保存，本政策不做規範。

6.2.5 私密金鑰歸檔

憑證機構簽章用私密金鑰不得進行歸檔。

憑證機構加密用私密金鑰可進行歸檔，憑證機構應於憑證實務作業基準中載明加密用私密金鑰歸檔之程序。

註冊中心及用戶私密金鑰的歸檔，本政策不做規範。

6.2.6 私密金鑰自密碼模組輸入或輸出

私密金鑰應於密碼模組內產製，如私密金鑰必須從一密碼模組，傳遞到另一密碼模組，傳遞時必須由經授權人員執行，且私密金鑰不得以明文方式存在於密碼模組之外；用來加密私密金鑰用的加密金鑰必須受保護以防止洩漏。

6.2.7 私密金鑰儲存於密碼模組

私密金鑰得以明文或密文方式，儲存於密碼模組內。

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授權人員，經身分鑑別後啟動，鑑別之方式包含但不限於密碼、個人通行碼或生物特徵識別。啟動資料於輸入時必須加以保護以防止洩漏。

6.2.9 私密金鑰停用方式

停用私密金鑰時須由授權人員方可執行。

憑證機構應於憑證實務作業基準中載明私密金鑰停用的作業程序。

6.2.10 私密金鑰銷毀

各憑證機構簽章用私密金鑰不使用，或相對應的公開金鑰失效、廢止時，對密碼模組內之私密金鑰，必須以零數位化(Zeroization)的覆蓋方式清除。

6.2.11 密碼模組等級

憑證機構使用的密碼模組,必須使用至少通過 FIPS 140-2 Level 3 或 FIPS 140-3 Level 3，或符合此安全等級規範的硬體密碼模組。

用戶使用的密碼模組，由各憑證機構於憑證實務作業基準自行規範。

6.3 金鑰對管理的其他事項

6.3.1 公開金鑰歸檔

憑證歸檔時即已進行公開金鑰的歸檔，故不再進行公開金鑰之歸檔。

6.3.2 公開金鑰與私密金鑰的有效期限

本基礎建設各成員之公開金鑰與私密金鑰之有效期限可相同,依強度等級(金鑰長度)不同，使用期限說明如下：

(1) RSA 4096 位元之金鑰對：有效期限至多為 40 年。
(2) RSA 2048 位元之金鑰對：有效期限至多為 30 年。
(3) ECC P-384 之金鑰對：有效期限至多為 40 年。
(4) ECC P-256 之金鑰對：有效期限至多為 30 年。

憑證機構應於其憑證實務作業基準或相關作業規範中，載明下層憑證機構及用戶之金鑰對有效期限。

6.4 啟動資料

憑證機構應於其憑證實務作業基準中載明對於啟動資料之保護，包括從產生、歸檔到銷毀之間整個生命週期之保護。

6.4.1 啟動資料產製及安裝

用來解開憑證機構或憑證用戶私密金鑰的啟動資料，與其他相關存取控制機制，必須有適當的保護。

憑證機構之啟動資料得由使用者自行選擇，並使用多人分持的方式進行，啟動資料必須使用生物特徵資料，或有密碼模組強化的安全機制。

用戶的啟動資料可自行選擇，若啟動資料必須預先產製後傳遞，必須透過適當安全保護的管道遞送。

6.4.2 啟動資料的保護

各憑證機構之啟動資料，必須以密碼學或實體存取控制方式加以保護。

6.4.3 啟動資料的其他考量

各憑證機構於憑證實務作業基準，可依照憑證適用範圍對安全度的需求來訂定啟動資料的作業規範。

6.5 電腦安全控管

6.5.1 電腦安全技術需求

各憑證機構應藉由作業系統，或結合作業系統、軟體、實體之防護技術來提供以下安全措施：

(1) 具有用戶身分識別及驗證的登入
(2) 提供自訂的存取控制
(3) 提供安全稽核能力。
(4) 對各種憑證服務和公開金鑰基礎建設信賴角色存取控制的限制。
(5) 具備公開金鑰基礎建設信賴角色和相關身分的識別和鑑別。
(6) 確保通訊和資料庫安全。
(7) 具備公開金鑰基礎建設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。

憑證機構若簽發公開受瀏覽器或電腦作業系統信任的憑證，憑證機構應建置符合CA/Browser Forum 公布之「NETWORK AND CERTIFCATE SYSTEM SECURITY REQUIREMENTS」資訊安全控管措施。

6.5.2 電腦系統安全等級

各憑證機構使用的電腦作業系統平台，至少需具備 EAL3[ISO / IEC 15408 Common Criteria]或 C2[TCSEC]或 E2[ITSEC]等級的安全標準。

各憑證機構應於憑證實務作業基準或相關作業規範中，規範其使用的電腦作業系統平台安全等級的標準。

6.6 生命週期技術控管

6.6.1 系統開發控管

各憑證機構其憑證管理系統之開發控管應符合以下需求：

(1) 應具詳細之說明文件。
(2) 憑證管理系統軟硬體之採購必須具備可以降低組件遭竄改之程序。
(3) 專為憑證機構所開發之軟硬體必須於可控管之環境下進行，開發過程應加以定義並提供文件。

6.6.2 安全管理控管

各憑證機構於憑證管理系統之設定、修改或升級，必須完整控制並留下文件紀錄，並應該有未經授權修改軟體或變更設定的偵測機制。

各憑證機構應有確保憑證管理系統軟體完整性之控制措施。

各憑證機構對憑證管理系統使用的軟硬體設備，應有軟硬體設備生命週期的安全管控作業規範。軟硬體設備於接收時須有安全保護之查核措施。

各憑證機構對憑證管理系統使用的軟硬體設備，只可安裝憑證作業有關軟體且執行相關作業，不可安裝其他與 CA 業務無關的軟體與執行其他非憑證相關作業。軟硬體設備的安裝與更新，應制定相關的作業規範，並於具安全管控的環境下進行。

6.6.3 生命週期的安全等級

不做規範。

6.7 網路安全控管

各憑證機構之憑證管理系統，必須具備獨立之作業管理系統，且須經授權之作業人員方可進行操作。

為確保網路防入侵與防破壞的安全功能，憑證機構必須安裝及建置防火牆、防入侵偵測與防病毒管理系統，以增進網路管理系統的安全控管措施。

最高層憑證管理機構之憑證管理系統，須安裝於獨立安全控管環境，日常未執行作業時必須處於離線(Off-Line)狀態，須經授權後才可啟用。

6.8 時間戳記

不做規範。

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

各憑證機構簽發之憑證，其格式應訂定於憑證實務作業基準或相關作業規範。

7.1.1 版本

各憑證機構應簽發 X.509 V3(ITU-T X.509 06/1997, ISO 9594-8)版本的憑證。

7.1.2 憑證擴充欄位

憑證擴充欄位之使用，應以符合 ITUT X.509 或 IETF RFC 5280 標準為原則。

7.1.3 演算法物件識別碼

憑證機構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) rsaEncryption(1)}
金鑰	ecPublicKey	{iso(1) member-body(2) us(840) ansi-X9-62(10045) keyType(2) ecPublicKey(1)}
簽章	sha1WithRSAEncryption	{iso(1) member-body(2) us{840} rsadsi(113549) pkcs(1) pkcs-1(1) sha1-with-rsa-signature(5)}
簽章	sha256WithRSAEncryption	{iso(1) member-body(2) us{840} rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)}
簽章	sha384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha384WithRSAEncryption(12)}
簽章	ECDSAWithSHA256	{iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA256(2)}
簽章	ECDSAWithSHA384	{iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA384(3)}

各憑證機構應於憑證實務作業基準明定使用的演算法物件識別碼。

7.1.4 識別名稱格式

各憑證機構所簽發之憑證,使用的憑證主旨識別名稱格式須符合 X.500 Distinguished

Name(DN)的命名方式。

7.1.5 識別名稱限制

各憑證機構簽發之憑證，可視需要使用「名稱限制」擴充欄位。

7.1.6 憑證政策物件識別代碼

各憑證機構簽發的憑證，可視需要包含本憑證政策定義的物件識別碼。

7.1.7 憑證政策限制擴充欄位的使用

各憑證機構可視需要使用憑證政策限制擴充欄位。

7.1.8 憑證政策限定元語法與語意

各憑證機構可視需要使用憑證政策限定元。

7.1.9 憑證政策擴充欄位語意必要的處理

不做規範。

7.2 憑證廢止清冊剖繪

各憑證機構簽發之憑證廢止清冊，其詳細內容應訂定於憑證實務作業基準或相關作業規範。

7.2.1 版本

各憑證機構應簽發 X.509 V2 格式的憑證廢止清冊。

7.2.2 廢止憑證清冊與廢止憑證清單擴充欄位

各憑證機構於憑證廢止清冊有使用廢止憑證清冊擴充欄位時，應將其格式訂定於憑證實務作業基準或相關作業規範。

7.3 線上憑證狀態查詢剖繪

各憑證機構，如有提供線上憑證狀態查詢服務時，回應訊息應加上數位簽章。

7.3.1 版本

不做規範。

7.3.2 線上憑證狀態查詢擴充欄位

不做規範。

8 稽核及其他評估方法

8.1 稽核頻率或評估事項

最高層憑證機構至少每年一次進行內部稽核及外部稽核，其他憑證機構必須於憑證實務作業基準規範其稽核頻率。

8.2 稽核人員之識別及資格

各憑證機構之稽核者至少必須熟悉憑證實務作業基準及本政策，並且熟悉符合性稽核之稽核準則。

8.3 稽核者與受稽核者之關係

各憑證機構之稽核者必須以獨立、公正、客觀的態度對受稽核者進行稽核作業。

8.4 稽核項目

各憑證機構的稽核內容，應至少包含以下項目：

(1) 憑證實務作業基準是否符合本憑證政策之規範。
(2) 憑證機構是否依憑證實務作業基準執行憑證管理(相關)作業。

憑證機構如簽發公開受瀏覽器或電腦作業系統信任地憑證，例如 SSL 憑證，必須在憑證實務作業基準中揭露稽核計畫。

8.5 稽核結果之因應

各憑證機構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性的等級詳細條列，並將結果通知稽核單位與受稽核有關的單位。受稽核單位必須依缺失提出及執行矯正預防措施，並追蹤後續改善情形。

8.6 稽核結果之公開

各憑證機構之稽核結果，應提交予 PMA。

8.7 內部稽核

憑證機構若簽發 SSL 憑證、EVSSL 憑證或 S/MIME 憑證，其憑證實務作業基準應遵循 TLS BR 或 EVG 或 S/MIME BR 之相關要求並訂定內部查核頻率以及查核樣本數來嚴格控管服務品質。

9 其他業務及法律規定

9.1 收費

9.1.1 憑證簽發及更新費用

各憑證機構應於憑證實務作業基準訂定，本政策不做規範。

9.1.2 憑證查詢費用

各憑證機構應於憑證實務作業基準訂定，本政策不做規範。

9.1.3 憑證廢止及狀態查詢費用

各憑證機構應於憑證實務作業基準訂定，本政策不做規範。

9.1.4 其他服務費用

各憑證機構應於憑證實務作業基準訂定，本政策不做規範。

9.1.5 退費

各憑證機構應於憑證實務作業基準訂定，本政策不做規範。

9.2 財務責任

9.2.1 賠償責任

由各憑證機構於憑證實務作業基準中規範。

9.2.2 其他資產

不做規範。

9.2.3 對用戶及信賴憑證者之賠償責任

由各憑證機構於憑證實務作業基準中規範。

9.3 機密資訊

9.3.1 機密資訊的種類

由各憑證機構於憑證實務作業基準中規範，並應依相關法令規定辦理。

9.3.2 非機密資訊種類

由各憑證機構於憑證實務作業基準中規範，並應依相關法令規定辦理。

9.3.3 保護機密資訊之責任

由各憑證機構於憑證實務作業基準中規範，並應依相關法令規定辦理。

9.4 個人資訊隱私

9.4.1 隱私保護計畫

各憑證機構應依照「電腦處理個人資料保護法」的規範，或其他政府單位相關的規範運作；各憑證機構於進行跨國合作時，亦必須符合 OECD 個人資料隱密性的保護規範(OECD；Organization for Economic Co-operation and Development, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data)。

9.4.2 個人隱私資訊種類

各憑證機構應保密之個人隱私資料種類，必須於憑證實務作業基準或隱私權保護政策中訂定。

9.4.3 非個人隱私資訊種類

各憑證機構於憑證實務作業基準必須規範可公開資料種類，例如用戶憑證、憑證廢止與暫禁資訊，及憑證實務作業基準等。

若有其他因作業需求而須公開的資訊，應訂定於憑證實務作業基準。

9.4.4 個人隱私資訊保護責任

由各憑證機構於憑證實務作業基準中規範，並應依相關法令規定辦理。

9.4.5 使用個人隱私資訊之告知與同意

由各憑證機構於憑證實務作業基準中規範，並應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

各憑證機構應於憑證實務作業基準中規範，有關因行政法令規定及司法要求提供應保護之資料種類之規定。

9.4.7 其他資訊公開情形

憑證機構應於憑證實務作業基準中規範，有關依用戶要求提供應保護之資料種類之規定，並應依相關法令規定辦理。

9.5 智慧財產權

本政策之智慧財產權為臺灣網路認證股份有限公司所有。

9.6 職責及義務

9.6.1 憑證機構之職責

(1) 依據本政策訂定憑證實務作業基準。
(2) 公布憑證實務作業基準並確保各項作業及提供之服務皆符合憑證實務作業基準中所訂定之規範。
(3) 進行憑證簽發及公布，並留存適當的證明資訊。
(4) 確認用戶約定條款符合基準要求。
(5) 對違反用戶義務或基準指定因素之用戶廢止其憑證。
(6) 進行憑證廢止清冊之簽發及公布。
(7) 提供如第 2 章所述之儲存庫服務。

若憑證機構簽發 SSL 憑證或 EVSSL 憑證，根據 TLS BR 要求，憑證機構應審查以下內容：

- 使用網域或 IP 位址之權利。
- 申請憑證之授權。
- 資訊的正確性。
- 沒有誤導性之資訊。
- 申請者的身分。

若憑證機構簽發 S/MIME 憑證，根據 S/MIME BR 要求，憑證機構應審查以下內容：

- 使用 Email 信箱之權利。
- 申請憑證之授權。
- 資訊的正確性。
- 沒有誤導性之資訊。
- 申請者的身分。

9.6.2 註冊機構之職責

(1) 依本政策及憑證機構之憑證實務作業基準之規範，執行用戶註冊相關作業。
(2) 依照本政策及憑證機構之憑證實務作業基準之安全性規定運作，執行用戶註冊相關作業。
(3) 接受憑證申請請求資訊，並留存足以驗證憑證申請請求資訊正確性之證明資料。
(4) 確認用戶於註冊申請時，確實了解且同意用戶之義務。

9.6.3 用戶之義務

(1) 用戶向註冊中心註冊時，必須提供詳細且正確的身分證明文件與資料。
(2) 依照本政策、憑證機構之憑證實務作業基準規範，確實且妥善安全的保護其私密金鑰。
(3) 確實了解並同意本政策及憑證機構之憑證實務作業基準有關憑證接受及使用之規範，並且於同意接受後始可使用憑證。
(4) 憑證相對應的私密金鑰有被冒用、曝露及遺失等疑慮時，用戶必須依憑證機構之憑證實務作業基準之規定，向註冊中心辦理申告。
(5) 憑證與其相對應私密金鑰的使用範圍和限制，必須依照本政策與憑證機構之憑證實務作業基準的規定。

9.6.4 信賴憑證者義務

信賴憑證者於檢驗憑證時，應依循各憑證機構之憑證實務作業基準相關規定，進行憑證信賴路徑建立、憑證驗證，以作為是否信任憑證之參考依據。

9.6.5 其他成員義務

不做規範。

9.7 除外責任

由各憑證機構於憑證實務作業基準中規範。

9.8 責任限制

由各憑證機構於憑證實務作業基準中規範。

9.9 賠償

各憑證機構應於憑證實務作業基準中，載明憑證機構、註冊中心、用戶及信賴憑證者之賠償責任，且應符合電子簽章法之相關規定。

9.10 本文件生效與終止

9.10.1 生效

本政策由 PMA 審議通過後即生效。

9.10.2 終止

本政策之終止，須由 PMA 裁示。

9.10.3 終止及存續之效力

本政策經終止後，其效力維持至遵循本政策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

PMA 將以適當的方式，與本基礎建設之各憑證機構建立聯絡管道，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

本憑證政策的管理單位為 PMA，每年至少應檢視本政策一次，引用本政策之憑證機構每年至少應檢視其憑證實務作業基準一次。

本政策因法律規範改變、國際標準更新等因素而須變更時，憑證機構之憑證實務作業基準應做相對應的變更。

本政策之變更，應經 PMA 審議通過。

9.12.2 變更聯絡機制

對本政策若有更新建議時，請將建議文件郵寄或 Email 至 1.5.2 的聯絡窗口，交由

PMA 審議。

9.12.3 物件識別碼變更條件

本政策之物件識別碼之變更，須經 PMA 審議通過。

9.13 爭議處理程序

因使用憑證所產生之爭議，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。

各憑證機構應於其憑證實務作業基準中，訂定憑證使用爭議之處理程序。

9.14 政府管理法規

本政策訂定的內容與憑證機構相關業務的執行與釋義，皆依據主管機關相關法律的規範而訂定，且受中華民國相關法律規範的管轄。

9.15 法規之符合性

各憑證機構應於其憑證實務作業基準中載明其適用法規。

9.16 各項條款

9.16.1 完整合約

不做規範。

9.16.2 轉讓

不做規範。

9.16.3 存續性

本憑證政策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，直到新版之憑證政策的更新完成並公告。

憑證政策之更新，依本政策 9.12 節規定辦理。

9.16.4 施行

不做規範。

9.16.5 不可抗力

如因不可抗力及其他不可歸責於各憑證機構之事由(例如戰爭或地震等)，致其所簽發之憑證造成損失時，各憑證機構得不負損害賠償責任。

9.17 其他條款

不做規範。

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).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。

(4).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。

(5).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。

(6).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。

(7).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。

(8).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。

(9).<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。

(10).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。

(11).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。

(12).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。

(13).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。

(14).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。

(15).CABF(CA/Browser Forum)：

是由 CA 和瀏覽器開發商組成的非營利性組織。該組織的主要目標是制定和推動憑證的行業標準，確保憑證得到信任並得到廣泛接受。目前該組織針對 TLS 憑證、CodeSign 憑證已及 S/MIME 憑證均有定義相關規範，CA 在簽發該類憑證時，應遵守相關規範，其所簽發之憑證始能受到公眾信任(https://cabforum.org/)。

附錄二 名詞與簡稱(Acronyms and Abbreviations)

TLS BR	Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates
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
EAL	Evaluation Assurance Level
EVG	Guidelines for the Issuance and Management of Extended Validation Certificates
EVSSL	Extended Validation SSL
FIPS	Federal Information Processing Standard
ISO/IEC	the International Organization for Standardization, The International Electrotechnical Commission
ITSEC	Information Technology Security Evaluation Criteria
LDAP	Lightweight Directory Access Protocol
NB	Network Banking
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OECD	Organization for Economic Co-operation and Development

PMA	Policy Management Authority
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
RA	Registration Authority
RCA	Root Certification Authority
RSA	Rivest, Shamir, Adleman(encryption algorithm)
S/MIME BR	Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates
SSL	Secure Socket Layer
TCSEC	Trusted Computer System Evaluation Criteria
URL	Universal Resources Location