中華電信公開金鑰基礎建設

憑證政策

(Certificate Policy for the Chunghwa Telecom ecommerce Public Key Infrastructure)

第 2.2 版

中華電信股份有限公司

中華民國 113 年 8 月 26 日

目　　錄

1 序論......1

1.1 概要......3

1.1.1 憑證政策......3
1.1.2 憑證政策及憑證實務作業基準之關係......3
1.1.3 憑證機構引用憑證政策物件識別碼......3

1.2 文件名稱及識別......4

1.3 主要成員......8

1.3.1 政策管理委員會......8
1.3.2 憑證機構......9
1.3.3 註冊中心......16
1.3.4 用戶......16
1.3.5 信賴憑證者......16
1.3.6 其他相關成員......17
1.3.7 終端個體......17

1.4 憑證用途......17

1.4.1 憑證之適用範圍......17
1.4.2 憑證之禁止使用範圍......22

1.5 政策管理......22

1.5.1 憑證政策之制訂及管理機構......22
1.5.2 聯絡資料......22
1.5.3 憑證實務作業基準之審定......23
1.5.4 憑證政策及憑證實務作業基準變更程序......23

1.6 名詞定義及縮寫......23

2 公布及儲存庫之責任......24

2.1 儲存庫......24

2.2 憑證機構之資訊公布 24

2.3 公布的時間或頻率 25

2.4 存取控制...25

3 識別及鑑別...26

3.1 命名...26

3.1.1 命名種類 26
3.1.2 命名須有意義 26
3.1.3 用戶之匿名或假名 26
3.1.4 不同命名形式之解釋規則 26
3.1.5 命名之獨特性 27
3.1.6 商標之辨識、鑑別及角色 27
3.1.7 命名爭議之解決程序 27

3.2 初始身分驗證..27

3.2.1 證明擁有私密金鑰之方式 27
3.2.2 組織身分鑑別 28
3.2.3 個人身分鑑別 30
3.2.4 未經驗證之用戶資訊..32
3.2.5 授權之確認...32
3.2.6 互運之準則...33
3.2.7 資料來源正確性 33

3.3 金鑰更換請求之識別及鑑別 34

3.3.1 例行性金鑰更換之識別及鑑別 34
3.3.2 憑證廢止後金鑰更換之識別及鑑別 35

3.4 憑證廢止請求之識別及鑑別 35

4 憑證生命週期營運規定 36

4.1 憑證申請...36

4.1.1 憑證之申請者 36

4.1.2 註冊程序及責任 36

4.2 申請憑證之程序 37

4.2.1 執行識別及鑑別功能 37
4.2.2 憑證申請之批准或拒絕 38
4.2.3 處理憑證申請之時間 38

4.3 憑證簽發 38

4.3.1 憑證簽發時憑證機構之作業 38
4.3.2 對用戶之憑證簽發通知 39

4.4 憑證接受 39

4.4.1 構成接受憑證之事由 39
4.4.2 憑證機構對簽發憑證之發布 40
4.4.3 憑證機構對其他個體之憑證簽發通知 40

4.5 金鑰對及憑證之用途 40

4.5.1 用戶私密金鑰及憑證之用途 40
4.5.2 信賴憑證者公開金鑰及憑證之用途 41

4.6 憑證展期 41

4.6.1 憑證展期之情況 42
4.6.2 憑證展期之申請者 42
4.6.3 憑證展期之程序 42
4.6.4 對用戶憑證展期之簽發通知 42
4.6.5 構成接受展期之憑證的事由 42
4.6.6 憑證機構對展期之憑證的發布 42
4.6.7 憑證機構對其他個體之憑證簽發通知 42

4.7 用戶憑證之金鑰更換 43

4.7.1 憑證金鑰更換之情況 43
4.7.2 更換憑證金鑰之申請者 43
4.7.3 憑證金鑰更換之程序 43
4.7.4 對用戶憑證金鑰更換之簽發通知 44
4.7.5 構成接受金鑰更換憑證之事由 44
4.7.6 憑證機構對金鑰更換之憑證的發布 44
4.7.7 憑證機構對其他個體之憑證簽發通知 44

4.8 憑證變更..44
4.8.1 憑證變更之情況...44
4.8.2 憑證變更之申請者..44
4.8.3 憑證變更之程序...44
4.8.4 對用戶憑證變更之簽發通知...44
4.8.5 構成接受變更之憑證的事由...44
4.8.6 憑證機構對變更之憑證的發布..45
4.8.7 憑證機構對其他個體之憑證簽發通知...45
4.9 憑證廢止及停用...45
4.9.1 廢止憑證之情況...45
4.9.2 憑證廢止之申請者..47
4.9.3 憑證廢止之程序...47
4.9.4 憑證廢止請求之寬限期...48
4.9.5 憑證機構處理憑證廢止請求之處理期限..48
4.9.6 信賴憑證者檢查憑證廢止之規定...48
4.9.7 憑證廢止清冊之簽發頻率..49
4.9.8 憑證機構廢止清冊及憑證廢止清冊發布之最大延遲時間...................................50
4.9.9 線上憑證廢止及狀態查驗之可用性..50
4.9.10 線上憑證廢止查驗之規定..50
4.9.11 廢止公告之其他發布形式..50
4.9.12 金鑰被破解時之其他特殊規定...51
4.9.13 憑證停用之情況..51
4.9.14 憑證停用之申請者...51
4.9.15 憑證停用之程序..51
4.9.16 憑證停用期間之限制..51
4.9.17 恢復使用憑證之程序..52
4.10 憑證狀態服務...52
4.10.1 操作特性...52
4.10.2 服務可用性..52
4.10.3 可選功能...52
4.11 訂購終止..53
4.12 私密金鑰託管及回復..53
4.12.1 金鑰託管及回復之政策及實務...53

4.12.2 會議金鑰封裝及回復之政策及實務 53

5 憑證機構設施、管理及操作控管 54

5.1 實體控管 54

5.1.1 所在位置及結構 54
5.1.2 實體存取 54
5.1.3 電力及空調 55
5.1.4 水災防範 55
5.1.5 火災防範及保護 55
5.1.6 媒體儲存 55
5.1.7 廢料處理 56
5.1.8 異地備援 56

5.2 程序控管 56

5.2.1 信賴角色 56
5.2.2 每項任務所需之人數 57
5.2.3 識別及鑑別每一個角色 57
5.2.4 需要職責分離之角色 57

5.3 人員控管 58

5.3.1 資格、經驗及清白規定 58
5.3.2 背景調查之程序 58
5.3.3 教育訓練規定 58
5.3.4 人員再教育訓練之規定及頻率 59
5.3.5 工作調換之頻率及順序 59
5.3.6 未授權行為之裁罰 59
5.3.7 承攬商派駐人員之規定 60
5.3.8 提供之文件資料 60

5.4 稽核紀錄程序 60

5.4.1 被記錄事件種類 60
5.4.2 紀錄檔處理頻率 65
5.4.3 稽核紀錄檔保留期限 66
5.4.4 稽核紀錄檔之保護 66
5.4.5 稽核紀錄檔備份程序 67
5.4.6 稽核彙整系統 67

5.4.7 對引起事件者之通知 67
5.4.8 弱點評估 67

5.5 紀錄歸檔之方法 68

5.5.1 歸檔紀錄之種類 68
5.5.2 歸檔資料之保留期限 69
5.5.3 歸檔資料之保護 69
5.5.4 歸檔資料備份程序 69
5.5.5 紀錄之時戳規定 69
5.5.6 歸檔資料彙整系統 70
5.5.7 取得及驗證歸檔資料之程序 70

5.6 憑證機構之金鑰更換 70

5.7 遭破解及災變之復原 71

5.7.1 緊急事件及系統遭破解之處理程序 71
5.7.2 電腦資源、軟體或資料遭破壞 71
5.7.3 憑證機構私密金鑰遭破解之處理程序 71
5.7.4 災變後業務持續營運能力 72

5.8 憑證機構或註冊中心之終止服務 72

6 技術性安全控管 73

6.1 金鑰對之產製及安裝 73

6.1.1 金鑰對之產製 73
6.1.2 私密金鑰傳送給用戶 74
6.1.3 公開金鑰傳送給憑證機構 75
6.1.4 憑證機構公開金鑰傳送給信賴憑證者 75
6.1.5 金鑰長度 76
6.1.6 公開金鑰參數之產製及品質檢驗 76
6.1.7 金鑰之使用目的 76

6.2 私密金鑰保護及密碼模組工程控管 77

6.2.1 密碼模組標準及控管 77
6.2.2 私密金鑰分持之多人控管 77
6.2.3 私密金鑰託管 78

6.2.4 私密金鑰備份 78
6.2.5 私密金鑰歸檔 78
6.2.6 私密金鑰匯入、匯出密碼模組 78
6.2.7 私密金鑰儲存於密碼模組 78
6.2.8 私密金鑰之啟動方式 78
6.2.9 私密金鑰之停用方式 79
6.2.10 私密金鑰之銷毀方式 79
6.2.11 密碼模組評等 79
6.3 金鑰對管理之其他規範 79
6.3.1 公開金鑰歸檔 79
6.3.2 憑證操作及金鑰對之效期 79
6.4 啟動資料 81
6.4.1 啟動資料之產生及安裝 81
6.4.2 啟動資料之保護 81
6.4.3 啟動資料之其他規範 81
6.5 電腦軟硬體安控措施 81
6.5.1 特定電腦安全技術需求 81
6.5.2 電腦安全評等 82
6.6 生命週期技術控管 82
6.6.1 系統研發控管 82
6.6.2 安全管理控管 82
6.6.3 生命週期安全控管 83
6.7 網路安全控管措施 83
6.8 時戳 84
7 憑證、憑證廢止清冊及線上憑證狀態協定之格式剖繪 85
7.1 憑證之格式剖繪 85
7.1.1 版本序號 85
7.1.2 憑證擴充欄位 85
7.1.3 演算法物件識別碼 85

7.1.4 命名形式 86
7.1.5 命名限制 86
7.1.6 憑證政策物件識別碼 86
7.1.7 政策限制擴充欄位之使用 86
7.1.8 政策限定元之語法及語意 86
7.1.9 關鍵憑證政策擴充欄位之語意處理 86

7.2 憑證廢止清冊之格式剖繪 87

7.2.1 版本序號 87
7.2.2 憑證廢止清冊及憑證廢止清冊條目之擴充欄位 87

7.3 線上憑證狀態協定之格式剖繪 87

7.3.1 版本序號 87
7.3.2 線上憑證狀態協定擴充欄位 87

8 稽核及其他評核 88

8.1 稽核頻率或評核時機 88

8.2 稽核人員之身分及資格 88

8.3 稽核人員及被稽核方之關係 89

8.4 稽核項目 89

8.5 對於稽核結果之因應方式 89

8.6 稽核結果之公開 90

8.7 自我稽核 90

9 其他業務及法律事項 91

9.1 費用 91

9.1.1 憑證簽發、展期費用 91
9.1.2 憑證查詢費用 91
9.1.3 憑證廢止、狀態查詢費用 91

9.1.4 其他服務費用 91
9.1.5 請求退費之程序 91

9.2 財務責任 91

9.2.1 保險涵蓋範圍 91
9.2.2 其他資產 91
9.2.3 對終端個體之保險或保固責任 91

9.3 業務資訊之保密 92

9.3.1 機密資訊之範圍 92
9.3.2 非機密資料之範圍 92
9.3.3 保護機密資訊之責任 92

9.4 個人資訊之隱私 92

9.4.1 隱私保護計畫 92
9.4.2 隱私之資訊 93
9.4.3 非隱私之資訊 93
9.4.4 保護隱私資訊之責任 93
9.4.5 使用隱私資訊之告知與同意 93
9.4.6 應司法或管理程序釋出資訊 93
9.4.7 其他資訊釋出之情形 94

9.5 智慧財產權 94

9.6 聲明及擔保 94

9.6.1 憑證機構之聲明及擔保 94
9.6.2 註冊中心之聲明及擔保 95
9.6.3 用戶之聲明及擔保 95
9.6.4 信賴憑證者之聲明及擔保 96
9.6.5 其他參與者之聲明及擔保 97

9.7 免責聲明 97

9.8 責任限制 97

9.9 賠償 97

9.10 本文件之生效與終止 98

9.10.1 生效 98
9.10.2 終止 98
9.10.3 終止與保留之效力 98

9.11 主要成員之個別告知及溝通........98

9.12 修訂........98

9.12.1 修訂程序 98
9.12.2 通知之機制及期限 99
9.12.3 物件識別碼必須更改之情況 99

9.13 爭議解決條款........99

9.14 管轄法律........99

9.15 適用法律........99

9.16 雜項條款........99

9.16.1 完整協議 99
9.16.2 轉讓 100
9.16.3 可分割性 100
9.16.4 契約履行 100
9.16.5 不可抗力 100

9.17 其他條款........101

附錄 1：縮寫........102

附錄 2：名詞定義........104

憑證政策修訂履歷表

版次	實施日期	修訂內容摘要
1.0	93/10	首次發行。
1.1	103/12/22	改版為 RFC 3647 版本，憑證政策增加 CABF OV/DV CP OID。
1.2	104/10/5	修訂有關憑證政策之識別增加 CABF EV/IV CP OID、保證等級、稽核結果公開之範圍、縮寫和定義、名詞解釋等處。
1.3	105/1/27	(1) 修訂 1.4.1 節各類 SSL 憑證之適用範圍說明 (2) 修訂第 8 章稽核方法、8.1 節稽核頻率與 8.6 節稽核結果之公開範圍，將所引用之稽核標準之版本序號刪除 (3) 修訂 3.2.2 及 3.2.3 節組織及個人之鑑別程序。
1.4	105/9/23	修訂 ePKI CP 有關憑證政策之識別、保證等級、縮寫和定義、名詞解釋等處。
1.5	106/12/1	(1) 第 1.3.2.2 節增訂下屬憑證機構之描述。 (2) 增訂第 2.2 憑證機構之資訊公布的項目。 (3) 依照經濟部憑證實務作業基準審查委員對於 CPS 審查意見修訂第 1.4.1 節各類 SSL 憑證之適用範圍對於可降低之風險說明。 (4) 於第 4.9.11 節線上憑證廢止查驗之規定，聲明 ePKI 各 CA 皆有支援 OCSP Stapling。 (5) 根據 CA/Browser Forum Baseline Requirement，於第 4.9.13 節及第 4.9.17 節增訂 SSL 憑證不得暫時停止使用與恢復使用憑證。 (6) 於第 4.2.1 節將憑證註冊審驗人員查詢 CAA DNS 紀錄改為強制。 (7) 修訂第 5 章之信賴角色。 (8) 第 6.3.2.2 節用戶公開金鑰及私密金鑰之使用期限，107/3/1 起限縮 OV、DV、IV SSL 憑證之效期為 825 天。 (9) 於第 7.1.4 節命名形式，增訂有關 Name Chaining 規定。
1.6	107/5/28	(1) 修訂第 1.3.1 節政策管理委員會之組成。 (2) 依照加拿大會計師公會之公告，將 Trust Service Principles and Criteria for Certification Authorities 改為 WebTrust Principles and Criteria for Certification Authorities，如第 5.4.8 節、第 6.6.2 節、第 8.6 節、第

		8.6 節與第 9.4.4 節。 (3) 於第 1.3.2.2 節和第 4.2.1 節補充對於 ePKI 之 CAA Issuer Domain Names 之說明。
1.7	108/04/30	(1) 第 1.3.2 節加入第 3 代總管理中心自簽憑證及第 3 代通用憑證管理中心憑證機構憑證之資訊。 (2) 第 1.4.1 節增加認證符記保證等級。 (3) 配合 RFC 3647 修訂中文章節標題。 (4) 修訂第 2.2 節、第 3.2 節、第 4.7.1 節、第 4.10.1 節、第 5.2 節、第 5.3.3 節、第 5.6 節、第 6.1.3 節、第 6.1.7 節、第 6.2.6 節、第 6.3.2 節、第 6.6.1 節、第 7.1 節、第 7.3 節、第 9.9 節、第 9.11 節、第 9.12.2 節及第 9.16 節。 (5) 配合 Baseline Requirement 修訂第 1.5.2 節及第 4.9 節。
1.75	108/08/12	第 1.3.2 節加入第 1 代政府伺服器數位憑證管理中心憑證機構憑證之資訊。
1.8	108/11/18	(1) 第 1.3.2 節加入第 1 代中華電信時戳服務管理中心憑證機構憑證之資訊。 (2) 修訂第 6.3.2.2 節用戶憑證效期之說明。
1.9	109/11/17	(1) 配合 Baseline Requirement 修訂憑證效期由 825 天縮短為 398 天。 (2) 修訂第 4.5.2 節、第 4.9.6 節、第 4.9.10 節、第 4.10.1 節、第 4.10.2 節、第 6.1.7 節、第 6.2 節、第 6.3.2.1 節、第 6.3.2.2 節、第 6.4.1 節、第 6.6.1 節、第 6.6.2 節、第 7.1 節、第 7.2.1 節、第 7.2.2 節及第 7.3 節。
1.95	110/04/22	(1) 第 1.3.2 節加入第 1 代中華電信安全電子郵件憑證管理中心憑證機構憑證之資訊。 (2) 修訂第 1 章、第 1.2 節、第 1.3.2 節、第 1.3.4 節、第 1.4.1 節、第 1.4.2 節、第 2.3 節、第 3.2.2 節、第 3.2.3 節、第 3.2.5 節、第 3.3.1 節、第 4.5.2 節、第 5.5.2 節、第 6.2.6 節、第 6.3.2 節、第 7.1.4 節、第 9.2.1 節、第 9.3.2 節、第 9.4.2 節、第 9.4.3 節、第 9.10 節、第 9.16.1 節、第 9.16.3 節及第 9.16.5 節。
2.0	111/04/22	修訂第 1.2、第 1.4.1、第 3.1.1、第 4.5.1、第 4.5.2、第 4.9.6、第 4.9.9、第 4.9.10、第 4.10.1、第 4.10.2、第 6.1.5-6.1.7、第 6.2.1、第 6.2.4、第 6.2.6、第 6.3、第 6.3.1、第 6.4.1、第 6.4.2、第 6.6.1-6.6.3、第 6.8、第 7.1.1-7.1.4、第 7.2.1、第 7.2.2、第 7.3、第 7.3.1、第 7.3.2 及第 8.2 節。

2.05	111/12/7	修訂第 1.2、第 1.31、第 1.3.2、第 4.12.1、第 4.3.2、第 6.2.3 等節
2.1	112/08/29	修訂第 1 章、第 1.2、第 1.5.3、第 1.5.4、第 3.2、第 6.3.2.2 節、第 8 章、第 8.1 節
2.2	113/08/26	修訂第 1.2、第 1.3.2.1、第 1.3.2.2、第 1.5.2.1、第 2.1、第 3.1.1、第 3.1.4、第 4.5.2、第 4.9.6、第 4.9.9、第 4.9.10、第 4.10.1、第 4.10.2、第 6.1.7、第 6.2、第 6.2.1、第 6.2.3、第 6.2.4、第 6.2.5、第 6.2.6、第 6.2.7、第 6.3.2.1、第 6.3.2.2、第 6.3.2.3(刪除此章節)、第 6.4.3、第 6.6.1、第 6.6.2、第 6.8、第 7.1.2、第 7.1.4、第 7.1.6、第 7.1.9、第 7.2.1、第 7.2.2、第 7.3、第 7.3.1、第 7.3.2、附錄 1 及附錄 2。

1 序論

中華電信公開金鑰基礎建設(Chunghwa Telecom ecommerce Public Key Infrastructure, ePKI，以下簡稱本基礎建設)係配合中華電信股份有限公司(以下簡稱本公司)推動電子化政策，健全電子商務基礎環境，以提供完善的電子認證服務而設立。

本憑證政策(Certificate Policy, CP)係依據電子簽章法規定及正式版國際相關標準如網際網路工程任務小組(Internet Engineering Task Force, IETF) 徵求修正意見書(Request for Comments, RFC) 3647、ITU-T X.509、RFC 5280 及憑證機構與瀏覽器論壇(CA/Browser Forum, http://www.cabforum.org) Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates(以下簡稱 Baseline Requirements)、Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates(以下簡稱 S/MIME Baseline Requirements)所訂定之政策文件，以做為 ePKI 各憑證機構訂定憑證實務作業基準(Certification Practice Statement, CPS)之依循。

本憑證政策共定義 5 種身分識別保證等級(Identity Assurance Level，以下簡稱保證等級)，依次為第 1 級、第 2 級、第 3 級、第 4 級和測試級，等級數字越大者，保證程度越高。依照 ITU-T X.509 標準，保證等級必須以憑證政策物件識別碼(Object Identifier, OID，詳見第 1.2 節)表示，而這些憑證政策物件識別碼將會記載在憑證的憑證政策擴充(certificatePolicies extension)欄位中。

保證等級係指信賴憑證者(Relying Party)對於以下項目的信任程度：

(1) 憑證機構簽發之憑證。可分為兩種情形，如簽發憑證給終端個體(End Entities, EE，參考第 1.3.7 節)時，憑證政策物件識別

碼代表該憑證申請時是依何種保證等級來做身分鑑別及簽發；如簽發憑證給憑證機構時，則該憑證機構的憑證中可能會有 1 個以上的憑證政策物件識別碼，表示該憑證機構可以簽發符合憑證政策物件識別碼之保證等級的憑證給終端個體。

(2) 憑證機構相關系統簽發、管理憑證和傳送私密金鑰(Private Key)之相關作業程序。

(3) 憑證資料中的用戶(Subscribers)或主體(Subject)是否能有效控管其憑證中所記載的公開金鑰相對應之私密金鑰，例如用戶使用軟體或硬體儲存其私密金鑰；亦即信賴憑證者能否確信憑證中所記載的憑證主體(Subject)與公開金鑰(Public Key)之連結關係(Binding)。

本基礎建設之憑證機構應引用適合的憑證政策物件識別碼，如此本基礎建設內的各憑證機構間便可進行互運(Interoperability)，並且可進一步與國內外公開金鑰基礎建設領域進行跨領域互運。本憑證政策訂定之 5 個保證等級僅適用於本基礎建設內的管理及互運，其他公開金鑰基礎建設領域只有在被核定可以政策對等(Equivalent)時，才允許在憑證政策對映擴充(policyMappings extension)欄位使用本基礎建設之憑證政策物件識別碼。

本基礎建設之憑證機構於簽發憑證時，可以選擇適當的憑證政策物件識別碼記載在憑證的憑證政策擴充欄位中，使信賴憑證者可透過憑證中記載的憑證政策物件識別碼確認該憑證的適用範圍。信賴憑證者可透過成對的憑證政策物件識別碼確認簽發憑證機構(Issuing CA)與主體憑證機構(Subject CA)之間的憑證政策對映關係。

本憑證政策訂定的項目及條款係依據相關法律規定，憑證機構一詞在本憑證政策中係指本基礎建設中所有的憑證機構，基於與本國或

外國的其他公開金鑰基礎建設互惠原則，eCA 在經本公司核准後，得與本基礎建設外之根憑證機構(Root Certification Authority, 簡稱 Root CA，中文也有稱為憑證總管理中心或最頂層憑證機構)進行交互認證(Cross-Certification)。如本基礎建設外的其他憑證機構因引用本憑證政策而引發之任何問題，概由該憑證機構自行負責。

1.1 概要

1.1.1 憑證政策

憑證政策是 1 種網路認證資訊科技(Information Technology)的指導原則(Guideline)。憑證政策是指明某一憑證所適用之對象或情況所列舉之 1 套規則，該對象或情況可為特定之社群或具共同安全需求之應用。本基礎建設已註冊 5 個保證等級的憑證政策物件識別碼，供憑證機構在簽發某一特定用途憑證時標示保證度，憑證機構可直接引用已註冊的憑證政策物件識別碼，信賴憑證者可透過憑證政策物件識別碼檢驗憑證機構簽發憑證的適用性是否正確。

eCA 的憑證是自簽(Self-Signed)憑證，也是本基礎建設的信賴起源，信賴憑證者應直接信賴 eCA 的憑證。依照國際標準及慣例，eCA 的憑證並無標示憑證政策物件識別碼，因應 eCA 必須具備高公信力，以保證等級第 4 級運作。

1.1.2 憑證政策及憑證實務作業基準之關係

憑證機構必須於憑證實務作業基準中說明如何達成所引用憑證政策之保證等級。

1.1.3 憑證機構引用憑證政策物件識別碼

本基礎建設之憑證機構應遵循本憑證政策，不可自訂憑證政策。

憑證機構引用本基礎建設之憑證政策物件識別碼必須經本公司同意，如對憑證政策有相關建議，可與本公司聯繫。

1.2 文件名稱及識別

本政策之名稱為中華電信公開金鑰基礎建設憑證政策(Certificate Policy for the Chunghwa Telecom ecommerce Public Key Infrastructure），本憑證政策之最新版本可在以下網頁取得：https://eca.hinet.net 或 https://ePKI.com.tw。憑證機構簽發的憑證(不含自簽憑證)必須在憑證政策擴充欄位記載憑證的憑證政策。下表為在 id-cht arc 註冊的憑證政策物件識別碼：

id-cht ::= {2 16 886 1}
id-cht-ePKI ::= {2 16 886 1 100}
id-cht-ePKI-certpolicy::= {id-cht-ePKI 0}

保證等級	物件識別碼名稱	物件識別碼值
測試級	id-cht-ePKI-certpolicy-testAssurance	{id-cht-ePKI-certpolicy 0}
第 1 級	id-cht-ePKI-certpolicy-class1Assurance	{id-cht-ePKI-certpolicy 1}
第 2 級	id-cht-ePKI-certpolicy-class2Assurance	{id-cht-ePKI-certpolicy 2}
第 3 級	id-cht-ePKI-certpolicy-class3Assurance	{id-cht-ePKI-certpolicy 3}
第 4 級	id-cht-ePKI-certpolicy- class4Assurance	{id-cht-ePKI-certpolicy 4}

前述物件識別碼其數值自民國 103 年 12 月起漸進移轉使用於網路通訊協定註冊中心(Internet Assigned Numbers Authority, IANA)註冊之私人企業數值(Private Enterprise Number, PEN)註冊的 id-pen-cht arc 的憑證政策物件識別碼

id-pen-cht ::= {1 3 6 1 4 1 23459}
id-pen-cht-ePKI ::= {1 3 6 1 4 1 23459 100}

id-pen-cht-ePKI-certpolicy::= { id-pen-cht-ePKI 0}

保證等級	物件識別碼名稱	物件識別碼值
測試級	id-pen-cht-ePKI-certpolicy-testAssurance	{id-pen-cht-ePKI-certpolicy 0}
第 1 級	id-pen-cht-ePKI-certpolicy-class1Assurance	{id-pen-cht-ePKI-certpolicy 1}
第 2 級	id-pen-cht-ePKI-certpolicy-class2Assurance	{id-pen-cht-ePKI-certpolicy 2}
第 3 級	id-pen-cht-ePKI-certpolicy-class3Assurance	{id-pen-cht-ePKI-certpolicy 3}
第 4 級	id-pen-cht-ePKI-certpolicy-class4Assurance	{id-pen-cht-ePKI-certpolicy 4}

若本憑證政策或憑證機構之憑證實務作業基準在 SSL 憑證簽發上與 Baseline Requirements 現行版本有任何不一致的情形，將優先遵循 Baseline Requirements 的條款。

下屬憑證機構其憑證簽發符合 Baseline Requirements 並通過 WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security (以下簡稱 WebTrust for CA－SSL Baseline)外稽標準者，下屬憑證機構的憑證及用戶之 SSL 憑證可使用 CA/Browser Forum 之組織驗證(Organization Validation, OV)型 SSL 憑證政策物件識別碼({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))、網域驗證(Domain Validation, DV)型 SSL 憑證政策物件識別碼({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))與個人驗證(Individual Validation, IV)型 SSL 憑證政策物件識別碼({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))。

下屬憑證機構的憑證及應用於 PDF 文件簽章之用戶憑證(簽發給組織或個人之保證等級第 1、2 或 3 級憑證)可使用物件識別碼 1.3.6.1.4.1.23459.100.0.9，此物件識別碼為 Adobe 認可信賴清單(Adobe Approved Trust List, AATL)所信賴。

若本憑證政策或憑證機構之憑證實務作業基準在 S/MIME 憑證簽發上與 S/MIME Baseline Requirements 現行版本有任何不一致的情形，將優先遵循 S/MIME Baseline Requirements 的條款。

下屬憑證機構其電子郵件憑證簽發符合 S/MIME Baseline Requirements 者，下屬憑證機構的憑證及用戶之 S/MIME 憑證可使用下表之物件識別碼:

物件名稱	物件識別碼
CA/Browser Forum S/MIME Baseline Requirements	2.23.140.1.5
電子郵件信箱驗證	
電子郵件信箱驗證傳統型(Mailbox-validated Legacy)安全電子郵件憑證	2.23.140.1.5.1.1
電子郵件信箱多用途型(Mailbox-validated Multipurpose)安全電子郵件憑證	2.23.140.1.5.1.2
電子郵件信箱嚴格型(Mailbox-validated Strict)安全電子郵件憑證	2.23.140.1.5.1.3
組織驗證	
組織驗證傳統型(Organization-validated Legacy)安全電子郵件憑證	2.23.140.1.5.2.1
組織驗證多用途型(Organization-validated Multipurpose)安全電子郵件憑證	2.23.140.1.5.2.2

物件名稱	物件識別碼
組織驗證嚴格型(Organization-validated Strict)安全電子郵件憑證	2.23.140.1.5.2.3
組織內個人驗證	
組織內個人驗證傳統型(Sponsor-validated Legacy)安全電子郵件憑證	2.23.140.1.5.3.1
組織內個人驗證多用途型(Sponsor-validated Multipurpose)安全電子憑證	2.23.140.1.5.3.2
組織內個人驗證嚴格型(Sponsor-validated Strict)安全電子郵件憑證	2.23.140.1.5.3.3
個人驗證	
個人驗證傳統型(Individual-validated Legacy)安全電子郵件憑證	2.23.140.1.5.4.1
個人驗證多用途型(Individual-validated Multipurpose)安全電子郵件憑證	2.23.140.1.5.4.2
個人驗證嚴格型(Individual-validated Strict)安全電子郵件憑證	2.23.140.1.5.4.3

上表之安全電子郵件憑證類型請參考下表之說明:

安全電子郵件憑證類別	描述
電子郵件信箱驗證型	憑證主體限制為 subject:emailAddress 和/或 subject:serialNumber attributes
組織驗證型	憑證主體資訊只包含組織之資訊
組織內個人驗證型(Sponsor)	主體結合組織資訊以及個人的屬性，例如機關內的職員
個人驗證型	憑證主體欄位只包含個人(自然人)屬性

對於這些憑證類型，每個世代:傳統(Legacy)、多用途(Multipurpose)和嚴格(Strict)，在 S/MIME Baseline Requirements 都有特定規定，既承認了安全電子郵件證當前多樣性的實務，也表明了隨著時間的推移，朝著更加明確的實務方向發展的渴望。

嚴格型(Strict)安全電子郵件憑證剖繪為安全電子郵件憑證剖繪的長期目標，擴充金鑰用途限制為 id-kp-emailProtection 並針對憑證主體唯一識別名稱屬性和其它屬性嚴格使用。多用途型(Multipurpose)安全電子郵件憑證相對於嚴格型，此類憑證具有允許於安全電子郵件與文件簽署(Document Signing)交叉使用的彈性。S/MIME 傳統型憑證提供了現有合理的 S/MIME 憑證實務，在 S/MIME Baseline Requirements 要求下可受稽核的彈性，包括主體唯一識別名稱屬性、extKeyUsage 和其他擴充選項，但將來可能被 CA/Browser Forum 淘汰。嚴格型與多用途型安全電子郵件憑證最大效期皆為 825 天，傳統型憑證則最大效期為 1185 天。

1.3 主要成員

1.3.1 政策管理委員會

每個公開金鑰基礎建設都需要有 1 個政策管理機構，以確保此基礎建設的持續及正常運作。以本基礎建設而言，本公司特別設立中華電信憑證政策管理委員會(Chunghwa Telecom Certificate Policy Management Authority，以下簡稱政策管理委員會)以負責本公司對本基礎建設的管理工作，政策管理委員會的組成係依照政策管理委員會設置要點，由資訊技術分公司總經理指派副總經理或相當層級擔任召集人 1 人，並指派 6 至 9 名委員，執行秘書 1 人由資訊技術分公司數據營運及資安應用處處長兼任，副執行秘書 1 人由資訊技術分公司數據營運及資安應用處副處長兼任。政策管理委員會的工作任務說明如下：

(1) 授權及監督 ePKI 各憑證機構之金鑰產製。

(2) 審查 ePKI 憑證政策。

(3)審查 ePKI 相關技術規範。

(4)審查 ePKI 憑證實務作業基準。

(5)審查交互認證憑證機構的互通申請。

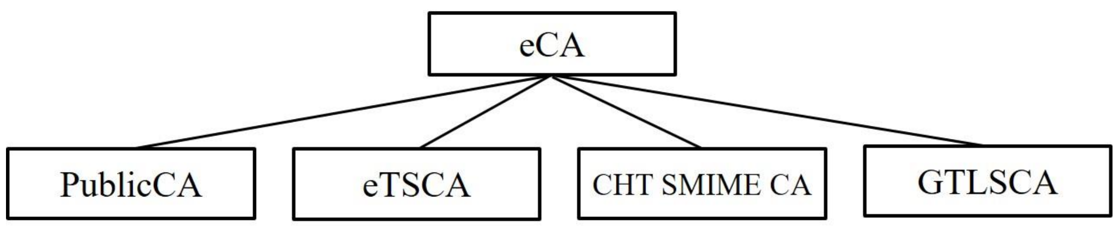
(6)審查及核可加入 ePKI 或是與 ePKI 交互認證憑證機構的憑證政策之對映關係。

(7)監督交互認證憑證機構對於所允許憑證政策的遵照，以利互通機制持續運作。

(8)審查 ePKI 時戳服務政策及 ePKI 時戳實務作業基準。

1.3.2 憑證機構

本基礎建設是依照 ITU-T X.509 標準建置的階層式(Hierarchy)公開金鑰基礎建設，包括本基礎建設的信賴起源(Trust Anchor)－中華電信憑證總管理中心(ePKI Root Certification Authority，以下簡稱 eCA)及本公司所設立的中華電信通用憑證管理中心(Public Certification Authority，以下簡稱 PublicCA)、中華電信時戳憑證管理中心(ePKI Timestamping Certification Authority，以下簡稱 eTSCA)及中華電信安全電子郵件憑證管理中心(CHT SMIME Certification Authority，以下簡稱 CHT SMIME CA)，與數位發展部委託維運的政府伺服器數位憑證管理中心(Government TLS Certification Authority，以下簡稱 GTLSCA)等 4 個下屬憑證機構，本基礎建設之架構如下所示：



1.3.2.1 中華電信憑證總管理中心

eCA 為本基礎建設的最頂層憑證機構(Root CA)，也是代表本基礎建設的主要憑證機構(Principal CA)，主要工作說明如下：

(1) 負責 eCA 之自簽憑證、自發憑證(Self-Issued Certificate)與下屬憑證機構憑證之簽發及管理。

(2) 訂定與本基礎建設領域外憑證機構間的交互認證(Cross-Certification)程序，包括簽發及管理其他本基礎建設外憑證機構的交互認證憑證。

(3) 將簽發的憑證及憑證廢止清冊(Certification Revocation List, CRL)公布於儲存庫(Repository)，並且確保儲存庫之正常運作。

eCA 應於憑證實務作業基準中訂定下屬憑證機構之識別與鑑別程序與外部憑證機構交互認證的程序。

符合本憑證政策並通報各大應用軟體廠商之根憑證機構計畫申請植入，且於外稽報告與管理聲明書揭露並登錄於 Mozilla 與 Microsoft 之 Common CA Database (CCADB)之總管理中心自簽憑證的下載點、憑證序號、憑證 SHA-1 拇指紋、SHA-256 拇指紋重要資訊如下：

(1) 第 1 代中華電信憑證總管理中心自簽憑證

<u>ePKI Root Certification Authority</u>

憑證序號：

15 c8 bd 65 47 5c af b8 97 00 5e e4 06 d2 bc 9d

憑證拇指紋(SHA-1)：

67 65 0d f1 7e 8e 7e 5b 82 40 a4 f4 56 4b cf e2 3d 69 c6 f0

憑證拇指紋(SHA-256)：

C0 A6 F4 DC 63 A2 4B FD CF 54 EF 2A 6A 08 2A 0A 72 DE 35 80 3E 2F F5 FF 52 7A E5 D8 72 06 DF D5

憑證效期：2004 年 12 月 20 日至 2034 年 12 月 20 日

金鑰種類/金鑰長度：RSA 4096 with SHA-1

(2) 第 2 代中華電信憑證總管理中心自簽憑證

ePKI Root Certification Authority - G2

憑證序號：

00 d6 96 2e c1 0a 15 93 12 af 8f 63 bc d4 44 c9 5b

憑證指紋(SHA-1)：

d9 9b 10 42 98 59 47 63 f0 b9 a9 27 b7 92 69 cb 47 dd 15 8b

憑證指紋(SHA-256)：

1E 51 94 2B 84 FD 46 7B F7 7D 1C 89 DA 24 1C 04 25 4D C8 F3 EF 4C 22 45 1F E7 A8 99 78 BD CD 4F

憑證效期：2015 年 11 月 17 日至 2037 年 12 月 31 日止

金鑰種類/金鑰長度：RSA 4096 with SHA-256

(3) 第 3 代中華電信憑證總管理中心自簽憑證

ePKI Root Certification Authority - G3

憑證序號：

62 37 e0 1b 9a ae 4e 4d f8 62 29 bb 44 49 7b 01

憑證指紋(SHA-1)：

cf 5f 43 17 b8 e5 55 3f 65 8e 18 02 ff 80 63 44 7a c1 76 15

憑證指紋(SHA-256)：

55 8F AB 7F 4B 5D FF 16 B6 8B A4 E4 0D 1D 3E 94 0E FA 9B 01 33 50 61 7D 6F 37 7C 17 24 D9 D4 21

憑證效期：2019 年 04 月 30 日至 2037 年 12 月 31 日止

金鑰種類/金鑰長度：RSA 4096 with SHA-256

(4) 第 4 代中華電信憑證總管理中心自簽憑證

ePKI Root Certification Authority - G4

憑證序號：

00 f6 70 f9 59 88 f4 52 05 8e 31 e1 68 86 3e fa 7a

憑證指紋(SHA-1)：

85 a6 69 3e d1 2c 4a ad 8d b6 9c 88 60 b5 80 13 4e bf 2c 77

憑證指紋(SHA-256)：

19 a2 fa 09 33 2c 6d 8e ac 13 93 d5 f3 03 71 dd 8b 4d d6 87 b0 e1 e5 0a 6b 48 ae 76 2c ab a2 b5

憑證效期：2022 年 11 月 3 日至 2047 年 11 月 3 日止

金鑰種類/金鑰長度：RSA 4096 with SHA-256

1.3.2.2 下屬憑證機構

下屬憑證機構為本基礎建設中的另一種憑證機構，主要負責簽發及管理終端個體的憑證，必要時也可依階層式公開金鑰基礎建設的建構方式，由第 1 層下屬憑證機構簽發憑證給第 2 層下屬憑證機構，或由第 2 層下屬憑證機構簽發憑證給第 3 層下屬憑證機構，依此類推而建構 1 個多層次的 PKI。但下屬憑證機構不可以直接與本基礎建設外的憑證機構進行交互認證。

下屬憑證機構之建置應依照憑證政策相關規定，並設置聯絡窗口，負責與 eCA 及其他下屬憑證機構之互運工作。

目前本基礎建設包含 PublicCA、eTSCA、CHT SMIME CA 及 GTLSCA 等 4 個下屬憑證機構。下屬憑證機構憑證除於外稽報告與管理聲明書揭露外，並登錄於 Mozilla 與 Microsoft 之 Common CA Database (CCADB)。其中，中華電信通用憑證管理中心第 1 代與第 2 代之憑證機構憑證，可串接至第 1.3.2.1 節總管理中心自簽憑證並仍有在使用的揭露於下，此部分之憑證主要係更新憑證政策擴充欄位、憑證序號等資訊，尚有少數仍可在用戶端有使用但沒揭露於本憑證政策之憑證機構憑證，參見總管理中心網站儲存庫或外稽報告與管理聲明書附錄：

(1) 第 1 代中華電信通用憑證管理中心之憑證機構憑證

Public Certification Authority

憑證序號：

00 97 3c c9 4d 44 cf e9 a2 e1 4f 52 e9 a5 94 a1 5a

憑證拇指紋(SHA-1)：

d6 d5 c7 92 ad 6b 2e 3a b9 b4 23 01 4e 1b 40 e5 76 d8 ec bf

憑證拇指紋(SHA-256)：

4B D1 6F 49 55 F3 F3 C9 C8 EA 48 EF 99 95 32 4D A5 12 17 24 F8 99 15 D5 F2 C9 1E B0 BA EF 23 37

憑證效期：2007 年 5 月 16 日至 2027 年 5 月 16 日

金鑰種類/金鑰長度：RSA 2048 with SHA-1

(2) 第 2 代中華電信通用憑證管理中心之憑證機構憑證

A1. Public Certification Authority - G2

憑證序號：

14 35 96 f2 44 1a 71 67 98 3f fc 95 97 41 9b 53

憑證指紋(SHA-1)：

78 62 ca ba b6 3a c7 a7 4e 07 56 a8 f8 6a 2c 02 1a 9f 69 b3

憑證指紋(SHA-256)：

DA E3 43 4F 69 6F C9 F0 F6 52 E1 B2 A6 F6 9B 5E 92 73 D0 9F
43 BD 3B DD 47 17 D6 14 1F 8C D2 C2

憑證效期：2014 年 12 月 11 日至 2034 年 12 月 11 日

金鑰種類/金鑰長度：RSA 2048 with SHA-256

A2. Public Certification Authority - G2

憑證序號：

00 ce 60 97 fd 33 e1 2d a0 75 ce dc 96 5d c0 c4 a3

憑證指紋(SHA-1)：

dd b1 3c 36 50 3d ba d9 4a b0 b2 e3 89 e3 bb f4 91 31 3e 5f

憑證指紋(SHA-256)：

F5 FB 67 C8 45 3E DA 34 DB EC 8A 76 65 74 F0 7A 03 54 8C 08
4A F2 F5 E6 45 5E A7 69 60 8D 9A D5

憑證效期：2014 年 12 月 11 日至 2034 年 12 月 11 日

金鑰種類/金鑰長度：RSA 2048 with SHA-256

(3) 第 3 代中華電信通用憑證管理中心之憑證機構憑證

Public Certification Authority - G3

憑證序號：

00 88 c1 80 7b a0 ab b6 2e 1f 49 a4 2a 02 8b e4 3e

憑證指紋(SHA-1)：

74 fb 76 84 87 88 37 53 3d f7 d9 19 81 66 4b 3c 6d 67 ab 8d

憑證指紋(SHA-256)：

B0 F1 F7 C7 DF 83 7B DF 88 82 5A 44 44 44 E4 81 5D A7 E0 89
97 28 A0 7A E8 76 7D 5F 65 B5 09 95

憑證效期：2019 年 04 月 30 日至 2037 年 12 月 31 日

金鑰種類/金鑰長度：RSA 2048 with SHA-256

(4) 第 4 代中華電信通用憑證管理中心之憑證機構憑證

Public Certification Authority - G4

憑證序號：

29 1c 0c 63 c0 17 2b b1 25 9f 5a 42 5a af 24 e3

憑證指紋(SHA-1)：

8d f3 51 d1 17 26 64 b7 54 8e 58 2d 91 47 53 3f 74 3b 67 59

憑證指紋(SHA-256)：

8f af 35 aa 59 eb b9 71 fb 4f c6 13 1d d9 c2 da 41 c1 84 21 c8 6f de c2 74 60 6e c3 1e be 54 36

憑證效期：2022 年 11 月 3 日至 2042 年 11 月 3 日

金鑰種類/金鑰長度：RSA 4096 with SHA-256

(5) 第 1 代中華電信時戳憑證管理中心之憑證機構憑證

ePKI Timestamping Certification Authority - G1

憑證序號：

00 b2 14 37 d0 d6 7c 63 87 48 44 f8 46 1c 5f 4b 54

憑證指紋(SHA-1)：

29 7e 0d 74 47 74 35 6e c8 09 04 d6 57 7d 14 c5 40 e4 9c be

憑證指紋(SHA-256)：

DA 31 29 3D 65 97 81 C6 9E 00 85 C7 32 A2 81 1D B5 0E 5C C5 76 90 91 49 B8 0A 98 A9 B0 F9 3F D9

憑證效期：2019 年 10 月 18 日至 2037 年 12 月 30 日

金鑰種類/金鑰長度：RSA 4096 with SHA-256

(6) 第 1 代中華電信安全電子郵件憑證管理中心之憑證機構憑證

CHT SMIME Certification Authority - G1

憑證序號：

38 78 d7 6c 81 39 e4 15 89 8a 37 34 5e 51 46 50

憑證指紋(SHA-1)：

4e 62 9a ab 84 fc 5a 13 6e 50 aa 24 fd c0 0e 5c e4 ee 6c a1

憑證指紋(SHA-256)：

4A B2 72 8F EC 21 14 76 94 61 A2 F5 C2 F5 13 22 49 7C 7B 92
3A 0D 81 53 E2 38 F2 AB 07 3E 3C 2F

憑證效期：2021 年 01 月 07 日至 2037 年 12 月 30 日

金鑰種類/金鑰長度：RSA 4096 with SHA-256

(7) 第 2 代中華電信安全電子郵件憑證管理中心之憑證機構憑證

CHT SMIME Certification Authority - G2

憑證序號：

09 d9 4e ad 4f 0a 92 6b 3c c6 38 7c 35 82 ea b5

憑證指紋(SHA-1)：

11 04 66 57 ad 89 33 b3 4b fc f4 84 be 84 fb bb 98 01 25 0d

憑證指紋(SHA-256)：

15 DC 43 B3 BD A2 9D F4 54 60 08 A4 FC 30 6D E8 11 F3 E7 8D
80 4E 1B 98 9C 2D E1 1D 53 36 DA 1A

憑證效期：2023 年 12 月 21 日至 2038 年 12 月 21 日

金鑰種類/金鑰長度：RSA 4096 with SHA-256

(8) 第 1 代政府伺服器數位憑證管理中心之憑證機構憑證

Government TLS Certification Authority - G1

憑證序號：

00 99 6d 5f e9 ad e1 6c dc 8e cd bf ed b1 4a 32 95

憑證指紋(SHA-1)：

b2 d1 51 a7 68 d3 0c 3b 99 d8 6b 8b 25 81 56 08 c2 8a b2 cb

憑證指紋(SHA-256)：

9d 1c da 1b 9e f3 95 af ce 7d e0 fe 74 de 6d 9f f5 e0 d2 a4 37 89 11
6c 00 c6 ba 5b f4 4b 98 23

憑證效期：2019 年 07 月 19 日至 2031 年 08 月 19 日

金鑰種類/金鑰長度：RSA 4096 with SHA-256

1.3.2.3 交互認證憑證機構(Cross-Certified CA)

目前總管理中心並無與任何本基礎建設以外之根憑證機構進行交互認證。

1.3.3 註冊中心

註冊中心(Registration Authority, RA)主要負責蒐集及驗證用戶(Subscribers)的身分、屬性和聯絡等相關資訊，以便於憑證機構之憑證簽發、廢止、憑證之金鑰更換、變更、展期、停用與復用等管理作業。

eCA 自行擔任註冊中心角色，並依政策管理委員會核定之憑證實務作業基準執行註冊中心的工作。

下屬憑證機構則可另外設立註冊中心，並於憑證實務作業基準中規範其工作。下屬憑證機構之註冊中心可分為由下屬憑證機構所直接設立與維運，或由本公司簽約之客戶自行建置與維運。無論何種註冊中心都必須遵循本憑證政策與其憑證實務作業基準之規定運作。由本公司簽約之客戶自行建置與維運之註冊中心也可依照其內部需求與規定採用比本憑證政策或其所屬憑證機構之憑證實務作業基準更嚴格之安全控制實務。

1.3.4 用戶

用戶係指不具備憑證簽發能力之憑證主體，並擁有與憑證記載之公開金鑰相對應之私密金鑰的個體。在本憑證政策中並不稱根憑證機構、下屬憑證機構或交互認證憑證機構為用戶，因其具有憑證簽發之能力。

1.3.5 信賴憑證者

信賴憑證者(Relying Parties)係指相信憑證之憑證主體名稱與某公開金鑰連結關係的個體。信賴憑證者必須依據憑證機構之憑證狀態資訊，檢驗所收到憑證的有效性。

信賴憑證者可使用憑證來驗證數位簽章訊息的完整性、確認發送訊息者的身分，及建立與用戶間的秘密通訊管道。同時，信賴憑證者

也可使用憑證中的訊息(例如憑證政策物件識別碼)，檢視此憑證的使用時機是否適當。

1.3.6 其他相關成員

憑證機構可選擇其他相關提供信賴服務的機構做為協同運作的夥伴，例如稽核機構、屬性憑證機構(Attribute Authority)、時戳服務機構(Time Stamp Authority)、資料存證服務機構(Data Archiving Service Authority)及卡管中心(Card Management Center)等，並應在憑證實務作業基準中訂定相互運作機制及彼此的權利與義務關係，以確保憑證機構服務品質的有效及可靠。

1.3.7 終端個體

終端個體在本基礎建設中包括以下兩類個體：

(1) 負責保管及應用憑證的私密金鑰擁有者。

(2) 信賴本基礎建設憑證機構所簽發憑證的第三者(不是私密金鑰擁有者，也不是憑證機構)。

1.4 憑證用途

本憑證政策依照不同安全需求訂定 5 種保證等級，以因應各種不同應用需要。憑證機構在決定所要簽發憑證之保證等級時，應依應用範圍審慎評估各種風險，環境的潛在危機、可能弱點和憑證的用途及應用的重要性，以選擇合乎安全保證等級的方式進行憑證機構的運作，及簽發與管理憑證。

1.4.1 憑證之適用範圍

本憑證政策對於各保證等級的憑證適用範圍並不強制規定，也不限定各保證等級所適用的社群對象，建議之適用範圍說明如下：

保證等級	適用範圍
測試級	僅供測試(Test)用，對於傳送的資料不負任何法律責任。
第 1 級	以電子郵件方式確認申請人確實可操作該電子郵件帳號，適合應用於遭到惡意篡改威脅很低的網路環境，或無法提供較高保證等級時，應用於數位簽章時可識別用戶來自於某一個特定電子郵件帳號及保證被簽署文件的完整性；應用於加密時，信賴憑證者可藉由用戶憑證之公鑰加密傳送訊息或對稱式金鑰以保障其機密性，但不適合應用於需要鑑別身分與不可否認服務/內容承諾(contentCommitment)的線上交易。
第 2 級	適合應用於資訊可能被篡改，但不會有惡意篡改之網路環境(資訊可能被截取但機率不高)；不適合做為重要文件(與生命及高金額相關的交易之文件)的簽署。例如小額度電子商務交易所需之資料加密與身分認證。
第 3 級	適合應用於有惡意使用者會截取或篡改資訊、並較第 2 級危險之網路環境，傳送的資訊可包括金錢或財產的線上交易。
第 4 級	適合應用於潛在威脅很高之網路環境、或資訊被篡改後復原的代價很高，傳送的資訊包括高金額的線上交易或極機密的文件。

本憑證政策對於 SSL 憑證，其適用範圍之說明如下：

憑證類別	適用範圍
網域驗證型	• 純粹只提供通訊管道之加密及保護(通訊管道之加密是指「促成加密金鑰之交換以達到用戶之瀏覽器和網站之間資訊傳遞的加密」) • 適合下列應用範圍： (1) 為發生惡意行為機率較低的非金錢或非財產交易之環境提供一般認證
組織驗證型/個人驗證型	• 通訊管道之加密及保護 • 鑑別網域名稱擁有者屬於哪一個組織/自然人

	● 適合下列應用範圍： (1) 電子商務交易 (2) 電子化政府 (3) 發生惡意行為機率為中等之環境

本憑證政策提供 3 種認證符記保證等級(Authenticator Assurance Level, AAL)供各憑證機構及憑證信賴者有所依循，認證符記保證等級說明如下表所示：

認證符記保證等級	**說明**
第 1 級	對認證符記控管者是否確實綁定用戶帳號僅提供部分保證，其使用任何可取得的驗證技術來進行單因子或多因子驗證，成功的驗證須可透過一個安全驗證協定來確認該用戶確實擁有且控管該認證符記。 (1) 允許的認證符記類型：可使用下述任一種類型。 ■ 記憶型秘密：例如：密碼通行碼或個人識別碼 ■ 單因子加密軟體 ■ 單因子加密設備 ■ 多因子加密軟體 ■ 多因子加密設備 (2) 認證符記與驗證器的需求： ■ 加密認證符記應使用經認可的加密技術，軟體認證符記亦可嘗試偵測該終端設備是否有惡意攻擊的可能性(例如有安裝惡意軟體)，若發現時，則終止該認證作業。 ■ 認證符記擁有者與驗證器應透過授權且安全加密的管道進行溝通，以避免中間人攻擊。
第 2 級	對認證符記控管者是否確實綁定用戶帳號提供高信賴度的保證，其須於安全驗證協定的環境下使用兩種驗證因子來

<table>
<tr><th>認證符記
保證等級</th><th>說明</th></tr>
<tr><td></td><td>進行認證，其認證方式應包含經核准的加密技術。

(1) 允許的認證符記類型：驗證作業應透過多因子驗證或雙因子驗證。
■ 當採用多因子驗證時，可使用的認證符記類型包括：
➢ 多因子加密軟體
➢ 多因子加密設備
■ 當採用雙因子驗證時，則應包含一種記憶型秘密認證符記，以及下述任一種一次性擁有的驗證符記：
➢ 單因子加密軟體
➢ 單因子加密設備

(2) 認證符記與驗證器的需求：
■ 加密認證符記應使用經認可的加密技術，認證符記應通過 FIPS 140 Level 1 認證，軟體認證符記亦可嘗試偵測該終端設備是否有惡意攻擊的可能性(例如有安裝惡意軟體)，若發現時，則終止該認證作業。此外，至少應使用一種認證符記，其具備重送攻擊防阻的能力，例如動態密碼。
■ 認證符記擁有者與驗證器應透過授權且安全加密的管道進行溝通，以避免中間人攻擊。
■ 若驗證過程中使用如行動裝置之類的設備時，則該設備原有的解鎖功能(例如：指紋辨識或個人識別碼驗證)不可視為一種驗證因子。</td></tr>
<tr><td>第 3 級</td><td>對認證符記控管者是否確實綁定用戶帳號提供非常高度的信賴保證，其須透過加密協定來驗證用戶金鑰的擁有權，驗證作業應使用硬體密碼認證符記以及可提供防範驗證器遭冒充能力的認證符記(亦可使用同時具備前述功能的設備)，且於安全驗證協定的環境下使用兩種驗證因子來進行認證。其認證方式應包含經核准的加密技術。

(1) 允許的認證符記類型：可使用下述任一種認證符記的結合。</td></tr>
</table>

認證符記保證等級	**說明**
	■ 多因子加密設備 ■ 單因子加密設備與記憶型秘密的結合 (2) 認證符記與驗證器的需求： ■ 認證符記擁有者與驗證器應透過授權且安全加密的管道進行溝通，以避免中間人攻擊。所有加密設備認證符記應具備驗證器防冒充與重送攻擊防阻的能力。 ■ 認證符記應為通過 FIPS 140 Level 2(含)以上或符合 Global Platform Trusted Execution Environment 的密碼模組。 ■ 若驗證過程中使用如行動裝置之類的設備時，則該設備原有的解鎖功能(例如：指紋辨識或個人識別碼驗證)不可視為一種驗證因子。

本憑證政策之認證符記保證等級所用物件識別碼如下表:：

認證符記保證等級	物件識別碼名稱	物件識別碼值
第 1 級	id-cht-ePKI-tokenAssurance 1	1.3.6.1.4.1.23459.100.4.1
第 2 級	id-cht-ePKI-tokenAssurance 2	1.3.6.1.4.1.23459.100.4.2
第 3 級	id-cht-ePKI-tokenAssurance 3	1.3.6.1.4.1.23459.100.4.3

用戶應依據應用系統所必須具備的安全需求，選擇使用合適保證等級的憑證。用戶在使用私密金鑰時，應選擇安全及可信賴的電腦環境及應用系統，以避免私密金鑰被盜取，因而權益受損。

信賴憑證者必須依照第 6.1.7 節金鑰之使用目的之規定，適當地使用金鑰，並使用符合國際標準(例如 ITU-T X.509 標準或 IETF RFC 5280 等)定義之憑證驗證(Certificate Validation)方法來驗證憑證的有效性(Validity)。

1.4.2 憑證之禁止使用範圍

本基礎建設之憑證機構簽發的憑證禁止使用於以下範圍：

(1) 犯罪。

(2) 軍令戰情及核生化武器管制。

(3) 核能運轉設備。

(4) 航空飛行及管制系統。

(5) TLS 流量中間人攔截(man-in-the-middle TLS traffic interception)。

1.5 政策管理

1.5.1 憑證政策之制訂及管理機構

中華電信股份有限公司。

1.5.2 聯絡資料

1.5.2.1 憑證政策建議

如對本憑證政策有任何建議，請利用以下資訊與本公司聯繫。

聯絡電話：0800-080-365

郵遞地址：10048 台北市信義路一段 21 號數據通信大樓 4F

中華電信憑證總管理中心

電子郵件信箱：caservice@cht.com.tw

也可至 https://eca.hinet.net 或 https://chtca.hinet.net/repository.html 查詢聯絡資料。

1.5.2.2 憑證問題報告

憑證機構應於憑證政策實務作業基準敘明憑證問題報告(Certificate Problem Report)之聯絡窗口。

1.5.3 憑證實務作業基準之審定

憑證機構應先自行檢查憑證實務作業基準是否符合憑證政策相關規定後，再送政策管理委員會進行審查及核定。在核定後憑證機構便可正式引用本基礎建設的憑證政策。

另依據中華民國電子簽章法規定，憑證機構訂定之憑證實務作業基準，必須經主管機關數位發展部核定後，始得對外提供簽發憑證服務。

本公司對於憑證機構是否遵循憑證政策，具有稽核的權利(依照第 8 章之規定)，憑證機構也應定期自行稽核，以證明遵照引用於本憑證政策的保證等級進行營運。

為使本基礎建設所發之憑證順暢運作於各作業系統、瀏覽器與軟體平台，本基礎建設已經申請參與各作業系統、瀏覽器與軟體平台之根憑證計畫(Root Certificate Program)，將中華電信憑證總管理中心之自簽憑證廣泛部署於各軟體平台之憑證機構信賴清單(CA Trust List)。依據根憑證計畫之規定，採連續不中斷涵蓋整個公開金鑰基礎建設之外稽原則，本基礎建設之憑證機構必須每年提供最新之憑證實務作業基準與外部稽核的結果。

1.5.4 憑證政策及憑證實務作業基準變更程序

憑證機構之憑證實務作業基準必須遵循相關法律及符合本憑證政策規定，並經中華電信及電子簽章法主管機關數位發展部核定。如本憑證政策修訂公布後，憑證機構之憑證實務作業基準應配合修訂，並送交政策管理委員會及電子簽章法主管機關數位發展部核定。

1.6 名詞定義及縮寫

參見附錄 1 及附錄 2。

2 公布及儲存庫之責任

2.1 儲存庫

儲存庫提供各憑證機構所簽發的憑證、憑證廢止清冊及憑證狀態等資訊的查詢及下載服務，並公布憑證政策及憑證實務作業基準等憑證簽發及管理作業相關資訊。

儲存庫可由憑證機構或其他機構營運，1 個憑證機構不限定只有 1 個儲存庫，但必須至少有 1 個主要對外服務的儲存庫，憑證機構應在憑證實務作業基準中說明儲存庫的網址，並確保儲存庫之可用性、適當的存取控制及資料完整性。憑證機構之憑證實務作業基準應載明儲存庫之相關資訊。

2.2 憑證機構之資訊公布

憑證機構應在固定的儲存庫公布：

(1) 憑證政策及憑證實務作業基準。

(2) 憑證廢止清冊，包括憑證廢止清冊之簽發時間與效期、憑證廢止時間。

(3) 線上憑證狀態協定(Online Certificate Status Protocol, OCSP)查詢服務

(4) 憑證機構本身之憑證，至少應使用到該憑證相對應之私密金鑰所簽發的所有憑證效期到期為止。

(5) 簽發之所有憑證(包括簽發給其他憑證機構之憑證)。

(6) 簽發之憑證機構廢止清冊(如憑證機構簽發憑證給其他憑證機構)。

(7) 隱私權保護政策。

(8) 最近 1 次之外部稽核結果。

(9) 相關最新消息。

除上述資訊外，憑證機構應公布可驗證數位簽章之必要資訊。

憑證機構之憑證實務作業基準應載明儲存庫暫停服務時間之上限。憑證機構應於憑證實務作業基準載明公布及通知之規定。

本基礎建設使用 pki.hinet.net、eca.hinet.net 及 epki.com.tw 代表授權憑證機構簽發憑證((Certification Authority Authorization, CAA) Issuer Domain Name。

2.3 公布的時間或頻率

憑證廢止清冊之公布頻率請依照第 4.9.7 節規定。憑證政策之公布與後續修訂應於政策管理委員會核准後儘速於 eCA 儲存庫公告。憑證機構應於收到主管機關之憑證實務作業基準核准公文後儘速將最新版本之憑證實務作業基準公布於儲存庫。

2.4 存取控制

(1) 憑證政策與憑證機構之憑證實務作業基準的取得不需存取控制。

(2) 憑證由憑證機構自行決定是否需存取控制。

(3) 憑證機構應保護儲存庫的資訊，以防止被惡意的公開散播或修改。公鑰憑證及憑證狀態資訊應經由網際網路公開取得。

3 識別及鑑別

3.1 命名

3.1.1 命名種類

憑證主體名稱應為 ITU-T X.500 唯一識別名稱(Distinguished Name, DN)。

用戶申請之憑證提出主體別名(Subject Alternative Name)時，憑證機構具有准駁寫入憑證之權利；若憑證中寫入主體別名時，該欄位須標示為非關鍵性擴充欄位。

3.1.2 命名須有意義

組織及個人之憑證主體名稱必須符合中華民國相關法律對該主體命名之規定，並且使用正式登記的名稱。

設備或伺服軟體之憑證主體名稱必須為該設備或伺服軟體之管理者的名稱，同時其中的通用名稱(Common Name)應以易於瞭解為原則，例如是模組的名稱或序號或應用的程序等。

伺服軟體憑證之主體名稱與憑證主體別名依照 CA/Browser Forum 之規範不得使用內部名稱(Internal Name)或保留 IP 位址(Reserved IP Addresses)。

3.1.3 用戶之匿名或假名

第 1 層下屬憑證機構可簽發匿名或假名憑證給終端用戶，如果這些憑證不被其所適用之政策(例如憑證種類、保證等級或憑證格式剖繪)禁止且能確保命名空間之唯一性。

3.1.4 不同命名形式之解釋規則

憑證機構應於憑證實務作業基準中敘明命名形式之解釋規則。

3.1.5 命名之獨特性

憑證主體名稱在本基礎建設中必須具獨特性，本公司負責建立憑證機構使用 X.500 名稱空間(Name Space)相關規範，以確保名稱命名的獨特性，憑證機構必須在憑證實務作業基準中載明如何使用 X.500 名稱空間，同時對於同名的憑證主體在命名時如何確保憑證主體名稱的獨特性。

3.1.6 商標之辨識、鑑別及角色

當憑證主體名稱可能包含商標時，則其命名必須符合中華民國商標相關法規。

3.1.7 命名爭議之解決程序

命名所有權依中華民國相關法律規定之命名規則辦理(例如公司法、姓名法、國民教育法等)，憑證機構應於憑證實務作業基準中訂定命名爭議之解決程序，依照保證等級測試級運作之憑證機構則不做規定。

本公司為本基礎建設命名爭議的仲裁機構。

3.2 初始身分驗證

簽發安全電子郵件憑證的機構應依照 S/MIME Baseline Requirements 以下章節進行初始身分驗證:

憑證類別	電子郵件信箱控制	組織身分	個人身分
電子郵件信箱驗證	第 3.2.2 節	不適用	不適用
組織驗證	第 3.2.2 節	第 3.2.3 節	不適用
組織內個人驗證	第 3.2.2 節	第 3.2.3 節	第 3.2.4 節
個人驗證	第 3.2.2 節	不適用	第 3.2.4 節

3.2.1 證明擁有私密金鑰之方式

憑證機構在憑證申請時，應驗證申請者擁有之私密金鑰與將記載

於憑證上的公開金鑰成對。

不同的金鑰產製者必須採用不同的方法來證明擁有私密金鑰，憑證政策認可之證明方法有以下 2 種方式：

(1) 由可信賴的第三者(例如發卡中心)為用戶產製金鑰對時：

憑證機構或註冊中心必須依照第 6.1.3 節規定透過安全管道向可信賴的第三者取得用戶之公開金鑰，用戶不必證明擁有相對應之私密金鑰，但必須依照第 3.2.2 及第 3.2.3 節規定接受身分鑑別，以取得私密金鑰及啟動資料，且私密金鑰應依照第 6.1.2 節規定傳送給用戶。

(2) 由用戶自行產製金鑰對時：

可由用戶使用私密金鑰產生 1 個簽章，並將該簽章依照第 6.1.3 節規定提供給憑證機構或註冊中心，由憑證機構或註冊中心使用用戶的公開金鑰驗證該簽章，以證明用戶擁有該私密金鑰。憑證政策允許使用其他安全程度相當的方法(例如 RFC 2510 或 RFC 2511 所列的各種方法)證明私密金鑰的擁有。

3.2.2 組織身分鑑別

對於組織(Organization)身分鑑別所需之證件數量、鑑別確認程序及是否需臨櫃辦理等，以保證等級不同有不同之規定，如下表所列：

保證等級	組織身分鑑別之程序
測試級	不做規定。
第 1 級	(1) 可不做證件核對。 (2) 只要申請者具有自己的電子郵件地址即可申請憑證，可不進行鑑別確認程序。 (3) 不需臨櫃辦理。
第 2 級	(1) 可不做證件核對。 (2) 用戶提交組織資料，例如組織識別碼(如扣繳單位稅

保證等級	組織身分鑑別之程序
	籍統一編號)、組織名稱等，應與憑證機構認可之資料進行比對。 (3) 不需臨櫃辦理。
第 3 級	組織身分鑑別方式可分為臨櫃辦理與非臨櫃辦理： (1) 臨櫃辦理，可採用下列方式(擇一)進行申請人身分鑑別： (a) 提供所在地管轄之政府機關(構)所核發之相關證明文件或公文書 (b) 由合格的政府資訊來源(Qualified Government Information Source, QGIS)如經濟部工商登記資料庫或合格的政府稅收資訊來源(Qualified Government Tax Information Source, QTIS)如財政部財稅資料中心取得之公示資料 (c) 中華電信所屬組織以紙本表單申請憑證 (2) 非臨櫃辦理可採用下列方式(擇一)進行申請人身分鑑別，詳細作業程序於各註冊中心內控制度中制訂之： (a) 透過政府公開金鑰基礎建設或本基礎建設所核發之保證等級第 3 級組織憑證數位簽章申請 (b) 已依法向主管機關完成設立登記程序，同(1)之(a)或(b)，並郵寄相關證明文件申請 (c) 公證人、律師或會計師的認證文書(Attestation Letter) (d) 由憑證管理中心人員或所信賴的人員到點訪視確認 (e) 中華電信所屬組織以電子表單申請憑證
第 4 級	組織身分鑑別分為以下兩種情形： (1) 民間組織之身分鑑別 申請資料應包括組織名稱、所在地及代表人名稱等足以識別該組織之資料。憑證機構或註冊中心除需驗證申請資料及代表人身分的真實性外，並應驗證該代表人有權以該組織之名義申請憑證。申請時應由代表人親臨憑證機構或註冊中心辦理。

保證等級	組織身分鑑別之程序
	以上所稱民間組織係指私法人團體、非法人團體或以上兩者之附屬組織。 (2) 中華電信所屬組織之身分鑑別 中華電信所屬組織必須以正式公文書指派憑證機構或註冊中心可鑑別之個人，代表該機構或單位親臨憑證機構或註冊中心申請憑證，憑證機構或註冊中心應確認該機構或單位確實存在，並驗證公文書之真確性，並依第 3.2.3 節中保證等級第 4 級之規定鑑別代表該機構或單位之個人之身分
網域驗證型 SSL 憑證	適用 Baseline Requireements 及本節針對保證等級第 1 級之規定。
組織驗證型 SSL 憑證	適用 Baseline Requireements 及本節針對保證等級第 3 級之規定。

3.2.3 個人身分鑑別

對於個人(Individual)身分鑑別之證件數量、鑑別確認程序及是否需臨櫃辦理等，依各保證等級不同有不同之規定，如下表所列：

保證等級	個人身分鑑別之程序
測試級	不做規定。
第 1 級	(1) 可不做證件核對。 (2) 只要申請者具有自己的電子郵件地址即可申請憑證，可不進行鑑別確認程序。 (3) 不需臨櫃辦理。
第 2 級	(1) 可不做證件核對。 (2) 用戶提交個人資料，例如個人識別碼(如身分證字號)、姓名等，應與憑證機構認可之資料進行比對。 (3) 不需臨櫃辦理。
第 3 級	(1) 核對證件： 在申請憑證時，用戶至少應出示 1 張被認

保證等級	個人身分鑑別之程序
	可並附照片之證件正本(例如國民身分證、護照或健保卡)，供憑證機構或註冊中心鑑別用戶之身分。 如用戶(例如未成年人)無上述之附照片證件，可使用由政府發給之足以證明用戶身分的證明文件(例如戶口名簿)取代，並由 1 位完全行為能力人以書面保證用戶之身分；出具保證之成年人之身分必須經過上述之鑑別。 (2) 用戶提交之個人資料，例如個人的識別碼(如身分證字號)、姓名及地址(如戶籍地址)等，應與該資料主管機關的登記資料(如戶籍資料)或其它經主管機關認可之可信賴第三者的登記資料進行比對。 (3) 臨櫃辦理： 用戶必須親臨憑證機構或註冊中心證明其身分。若用戶無法親自臨櫃辦理，得以委託書委任代理人代為臨櫃申請，但憑證機構或註冊中心必須確認該委託書之真偽(例如比對委託書上之用戶印鑑章或透過可信賴之資料來源提供的通訊方式查證代理人之身分)，並依上述規定鑑別代理人之身分。 個人如果事前已經受憑證機構、註冊中心或憑證機構信賴之機構或個人(例如戶政事務所、公證人或本公司經授權之人員)進行過符合上述規定之臨櫃識別與鑑別程序，並且留下該識別與鑑別之佐證資料(例如印鑑證明)，則個人不需親臨辦理，憑證機構或註冊中心將驗證該佐證資料。 (4) 使用自然人憑證辦理 使用內政部憑證管理中心簽發之保證等級第 3 級憑證簽章辦理，用戶不需親臨憑證機構或註冊中心證明其身分，憑證機構或註冊中心應驗證其數位簽章是否有效。 (5) 硬體裝置或伺服軟體憑證申請資料透過本基礎

保證等級	個人身分鑑別之程序
	建設核發之保證等級第 3 級個人憑證簽章時，代表人不需親臨辦理，憑證機構或註冊中心將驗證申請資料之數位簽章。
第 4 級	(1) 核對證件： 在申請憑證時，用戶應至少出示 1 張被認可並附照片之證件(例如國民身分證)正本，供憑證機構或註冊中心鑑別用戶之身分。 (2) 用戶提交之個人資料，例如個人的識別碼(如身分證字號)、姓名及地址等(如戶籍地址)，應與該資料主管機關的登記資料(如戶籍資料)進行比對。 (3) 臨櫃辦理，用戶必須親臨憑證機構或註冊中心證明其身分。

3.2.4 未經驗證之用戶資訊

憑證機構可不需要驗證保證等級第1級或測試級的個人憑證其通用名稱(Common Name)是否為憑證申請者的法定名稱。

3.2.5 授權之確認

當某個個人(憑證申請者)與憑證主體之名稱有關連，進行憑證生命週期活動如憑證申請或廢止請求時，憑證機構應於憑證實務作業基準說明憑證機構或其註冊中心如何進行授權之確認(Validation of Authority)，確認該個人可代表憑證主體，例如：

(1) 藉由Baseline Requirements第3.2.2.1節中所述之可靠來源所提供之電話、郵件、電子郵件等聯絡方式或其他相當之程序確認該個人確實任職於該憑證主體(某組織或公司)且得到授權代表該憑證主體。

(2) 藉由臨櫃面對面核對身分或其他可信賴的通訊方式確認該個人代表組織。

網域驗證型(DV)之SSL憑證申請，必須依照Baseline Requirements所建議之方式鑑別用戶具備網域之控制權；組織驗證型(OV)與個人驗證型(IV)之SSL憑證申請，除了依照網域驗證型SSL憑證鑑別用戶具備網域之控制權外，尚須依照第3.2.2或第3.2.3節規定進行組織或個人的身分鑑別。下屬憑證機構若有簽發SSL憑證應於憑證實務作業基準描述網域控制權授權之確認方式。

3.2.6 互運之準則

互運之準則(Criteria of Interoperation)至少包含審查欲成為交互認證的根憑證機構其所屬公開金鑰基礎建設應具備憑證政策、憑證實務作業基準以及簽發的憑證種類，所轄的憑證機構皆應通過WebTrust for CA系列稽核，且簽發SSL憑證之交互憑證機構應配合本基礎建設填寫及更新Self-assessment表，以確認其憑證政策及憑證實務作業基準持續符合Baseline Requirements規定。

3.2.7 資料來源正確性

在使用任何資料來源作為可靠資料來源之前，憑證機構應評估此來源的可靠性、正確性和對變更或偽造的抵抗性。憑證機構在評估過程中應考慮下列事項：

(1) 所提供資訊的存在時間

(2) 資訊來源的更新頻率

(3) 資料提供者和資料蒐集的目的

(4) 資料可用性的公用可存取性

(5) 偽造或變更資料的相對困難性

由憑證機構、其擁有者或其附屬公司所維護的資料庫，如果資料庫的主要目的是為了滿足Baseline Requirements第3.2節的驗證要求而蒐集的資訊，則不符合可靠資料來源。

3.3 金鑰更換請求之識別及鑑別

3.3.1 例行性金鑰更換之識別及鑑別

憑證之金鑰更換係指簽發 1 張與舊憑證具有相同特徵及保證等級的新憑證，而新的憑證除有新的、不同的公開金鑰(對應新的、不同的私密金鑰)及不同的序號外，亦可能被指定不同的有效期限。

當下屬憑證機構更換金鑰對時，簽發下屬憑證機構憑證的憑證機構，應依照第 3.2 節規定進行識別及鑑別，簽發新的憑證給下屬憑證機構。

下屬憑證機構的用戶需要更換金鑰時，須符合下表所列的鑑別要求。

保證等級	對用戶憑證更換金鑰的鑑別要求
測試級	不做規定。
第1級	用戶的身分可使用現行的簽章金鑰進行鑑別或依照第3.2節初始註冊之鑑別程序進行鑑別。
第2級	用戶的身分可使用現行的簽章金鑰進行鑑別或依照第3.2節初始註冊之鑑別程序進行鑑別,但如與初始註冊時間間隔超過15年時,則應依照第3.2節規定重新辦理初始註冊。
第3級	用戶的身分可使用現行的簽章金鑰進行鑑別或依照第3.2節初始註冊之鑑別程序進行鑑別,但如與初始註冊時間間隔超過9年時，則應依照第3.2節規定重新辦理初始註冊。
第4級	用戶的身分可使用現行的簽章金鑰進行鑑別或依照第3.2節初始註冊之鑑別程序進行鑑別,但如與初始註冊時間間隔超過3年時，則應依照第3.2節規定重新辦理初始註冊。

保證等級第 1 級網域驗證型(DV)、保證等級第 3 級組織驗證型(OV)及保證等級第 3 級個人驗證型(IV)之 SSL 憑證依照 Baseline

Requirements 及本憑證政策第 6.3.2.2 節之規定，金鑰更換之請求如與初始註冊時間間隔超過 398 天，則必須依照第 3.2 節重新辦理初始註冊。

3.3.2 憑證廢止後金鑰更換之識別及鑑別

憑證廢止後，新憑證的簽發應依照第 3.2 節規定，必須重新辦理初始註冊程序。

3.4 憑證廢止請求之識別及鑑別

憑證機構或註冊中心必須對於憑證廢止申請進行鑑別，憑證機構應依照第 4.9 節規定在憑證實務作業基準中載明申請者之身分鑑別方式，以確認申請者為有權提出憑證廢止之申請者。

無論私密金鑰是否遭破解，皆可使用私密金鑰之簽章及欲廢止之憑證來鑑別憑證廢止申請者之身分。

4 憑證生命週期營運規定

4.1 憑證申請

4.1.1 憑證之申請者

總管理中心之憑證申請者包括 eCA 及本公司所設立之下屬憑證機構或是由本基礎建設外之根憑證機構。

下屬憑證機構之憑證申請者包括組織或個人。

電腦及通訊設備(如路由器、防火牆、負載平衡器等)、伺服軟體(如 Web Server 或 SSL Server)或程式碼，因在法律上不具行為能力，必須由組織或個人以設備管理者或程式碼擁有者的身分提出憑證申請。

4.1.2 註冊程序及責任

憑證機構負責確保憑證申請者之身分在憑證簽發前依據憑證政策與適用的憑證實務作業基準確認，憑證申請者要負責提供足夠充分與正確的資訊與身分證明文件給憑證機構或其註冊中心在憑證簽發前執行必要的身分識別與鑑別工作。接受憑證機構簽發憑證的用戶應負以下義務：

(1) 遵守第 3 及第 4 章規定程序。

(2) 正確地使用憑證。

(3) 妥善地保管及使用私密金鑰。(以保證等級測試級簽發之憑證不做規定)。

(4) 當私密金鑰被破解時，應立即通知憑證機構。(以保證等級測試級簽發之憑證不做規定)。

4.2 申請憑證之程序

憑證機構必須在憑證實務作業基準中載明有關初始註冊、憑證展期及憑證之金鑰更換等之申請程序、申辦地點或網址。

eCA 可接受本公司所設立之憑證機構申請憑證，以成為本基礎建設之第 1 層下屬憑證機構，其申請程序由政策管理委員會另訂之。

本基礎建設外之根憑證機構向 eCA 申請交互憑證(Cross-Certificate)的程序由政策管理委員會另訂之。

本基礎建設中所有層級之下屬憑證機構，除非經其上層憑證機構之同意，否則不得接受其他憑證機構申請成為其下層憑證機構。

eCA 簽發交互憑證給本基礎建設外之憑證機構前，應由政策管理委員會與該憑證機構協商以決定是否承認該憑證機構簽發給其他憑證機構的交互憑證。

4.2.1 執行識別及鑑別功能

簽發憑證機構必須確保系統與程序足以鑑別用戶身分以符合憑證政策與憑證實務作業基準之規定。初始註冊程序依照本憑證政策第 3.2 節之規定執行，憑證申請者應據實提供正確且完整之資料。申請憑證所需之資料含必要資料及選擇性資料，只有憑證格式剖繪中所列的資料才會記錄於憑證中。於申請過程中之聯繫以及由憑證申請者申請憑證時提供之資訊必須由憑證機構與註冊中心依憑證政策及憑證實務作業基準之規定以安全也可被稽核之方式妥善保管。

核發 SSL 憑證前，對於註記在憑證之 subjectAltName 擴充欄位的每一個 dNSName(亦即申請者提出憑證請求所包含的每一個完全吻合網域名稱)，憑證註冊審驗人員必須向網域名稱系統(Domain Name

System, DNS)檢查依據 RFC 6844(經勘誤表 5065 修訂)所規範之授權憑證機構簽發憑證網域名稱系統資源紀錄(CAA DNS Resource Record)，通過後始准予發放。本基礎建設的 CAA 發布者網域名稱(Issuer Domain Names)包括 pki.hinet.net、publicca.hinet.net、eca.hinet.net 與 epki.com.tw。憑證機構應於憑證實務作業基準清楚指定該憑證機構確認於 CAA 紀錄屬於"issue"或"issuewild"而允許簽發 SSL 憑證的發布者網域名稱列表。

4.2.2 憑證申請之批准或拒絕

如果所有驗證身分之工作在遵循相關規定與最佳實務下可以成功執行，憑證簽發機構可以批准憑證之申請。

若各項驗證身分的工作無法成功完成，憑證機構得以拒絕憑證之申請。除因申請者之身分識別與鑑別之原因外，憑證機構得因其他原因不同意簽發憑證。憑證簽發機構可能因為申請者先前曾遭拒絕憑證申請或因曾違反用戶約定條款而遭拒絕其憑證申請。

4.2.3 處理憑證申請之時間

在申請者提交的資料齊全且符合憑證政策及憑證實務作業基準的要求下，憑證機構及註冊中心應於合理時間內完成憑證申請之受理。處理憑證申請的時間可記載於憑證實務作業基準或用戶約定條款或與憑證申請者之契約。

4.3 憑證簽發

4.3.1 憑證簽發時憑證機構之作業

憑證機構簽發憑證應依照第 5.2 節及憑證實務作業基準的規定，由適當人員執行憑證簽發之相關任務，憑證簽發後憑證機構或註冊中

心應以適當方式通知申請者。

eCA 應在每個金鑰生命週期簽發 1 張自簽憑證(Self-Signed Certificate)以建立憑證信賴起源；並得簽發數張自發憑證(Self-Issued Certficate)，以因應本身金鑰及憑證政策的更換。eCA 的自簽憑證及自發憑證簽發前必須由政策管理委員會確認其內容，新簽發的自簽憑證依照第 6.1.4 節規定傳送給信賴憑證者，自發憑證公布在儲存庫供信賴憑證者下載。

eCA 簽發交互憑證時，應在 basicConstraints 擴充欄位中明確標示憑證路徑長度限制(Path Length Constraint)，以確保憑證互運路徑是被允許的，憑證路徑長度限制的設定值，則視被允許的憑證互運路徑長度做設定。

4.3.2 對用戶之憑證簽發通知

憑證機構應於憑證實務作業基準中載明憑證簽發後通知申請者的方式。

憑證機構或註冊中心如不同意簽發憑證，應以適當方式通知憑證申請者，並明確告知不同意簽發的理由。除因申請者之身分識別與鑑別之原因外，憑證機構得因其他原因不同意簽發憑證。憑證機構，應於憑證實務作業基準中載明不同意簽發憑證之通知方式。

4.4 憑證接受

4.4.1 構成接受憑證之事由

簽發保證等級第 2、第 3 及第 4 級憑證之憑證機構，應經憑證申請者(1)預先審視將簽發之憑證內容；或(2)在簽發憑證後審視憑證內容，代表接受所簽發的憑證後，始得將簽發之憑證公布到儲存庫上。

若憑證申請者(1)審視將簽發之憑證內容後，拒絕接受所註記於憑證之資訊則憑證不予簽發；或(2)審視已經簽發之憑證內容後，拒絕接受所簽發的憑證，則憑證機構應廢止該憑證。以保證等級第 2、第 3 及第 4 級運作之憑證機構，應於憑證實務作業基準中載明以下事項：

(1) 憑證申請者確認憑證接受或拒絕的方式。

(2) 憑證申請者在決定接受憑證前應審視的憑證欄位。

(3) 憑證申請者拒絕接受憑證之處理方式。

上述憑證申請者在決定接受憑證前應審視的憑證欄位，至少應包括憑證主體名稱。憑證申請者在接受 SSL 類伺服器憑證前尚須審視憑證主體別名欄位。組織或個人憑證之申請者若有安全電子郵件之應用需求而於憑證註記電子郵件地址，也須審視憑證主體別名欄位。

憑證申請者拒絕接受憑證之處理方式，如涉及收費或退費問題時，應依據消費者保護法及公平交易原則訂定。

4.4.2 憑證機構對簽發憑證之發布

憑證機構的儲存庫服務應定期公布所簽發之憑證。註冊中心得與憑證機構協議將憑證透過註冊中心傳遞給用戶。

4.4.3 憑證機構對其他個體之憑證簽發通知

不做規定。

4.5 金鑰對及憑證之用途

4.5.1 用戶私密金鑰及憑證之用途

用戶金鑰對之產製應符合本憑證政策第 6.1.1 節之規定，且用戶須擁有私密金鑰之控制權，該私密金鑰不得用於簽發憑證。

用戶應保護私密金鑰不被未經授權之他人使用或揭露，且確保私密金鑰依憑證擴充欄位所註記之金鑰用途使用。用戶須依本憑證政策與憑證機構之憑證實務作業基準之規定使用憑證。

4.5.2 信賴憑證者公開金鑰及憑證之用途

信賴憑證者使用憑證時，應確認憑證用途，並依本憑證政策與憑證機構之憑證實務作業基準規定使用。信賴憑證者應使用符合其用途且滿足 ITU-T X.509、IETF RFCs 或 Baseline Requirements 等國際標準或規範之工具或方法。

信賴憑證者選用之工具或方法須於使用憑證前，驗證憑證路徑中所有憑證之欄位內容正確性、簽章完整性以及憑證狀態有效性；其中，憑證狀態資訊可透過憑證廢止清冊或線上憑證狀態協定查詢服務取得。待憑證驗證完成後，始可使用憑證路徑中之用戶憑證進行以下作業：

(1) 驗證電子文件數位簽章之完整性。

(2) 驗證文件簽章者之身分。

(3) 建立與用戶間安全通訊管道。

信賴憑證者亦應檢驗簽發憑證機構憑證與用戶憑證之憑證政策擴充欄位，以確認憑證之保證等級。

4.6 憑證展期

憑證機構的憑證不可展期，只有用戶的憑證才可展期。過期、停用、廢止之憑證不得展期；憑證最多展期至第 6.3.2.2 節規定之用戶公開金鑰使用期限上限為止，以維護金鑰對的安全。

4.6.1 憑證展期之情況

用戶憑證即將到期，未停用或廢止且符合以下情況可進行展期：

(1)憑證記載之公開金鑰尚未達到第 6.3.2.2 節所規定之使用期限。

(2)用戶及其身分屬性資料仍保持一致。

(3)憑證所記載之公開金鑰其相對應之私密金鑰仍然有效，未遺失或遭破解。

4.6.2 憑證展期之申請者

憑證將到期且為原本之憑證用戶之主體或經授權之代表人。

4.6.3 憑證展期之程序

用戶申請憑證展期時，使用其私密金鑰對憑證申請檔加以簽章，並將該憑證申請檔交給註冊中心，註冊中心將使用該用戶的公開金鑰驗證該憑證申請檔的數位簽章，以識別用戶之身分。

4.6.4 對用戶憑證展期之簽發通知

如第 4.3.2 節所述。

4.6.5 構成接受展期之憑證的事由

如第 4.4.1 節所述。

4.6.6 憑證機構對展期之憑證的發布

如第 4.4.2 節所述。

4.6.7 憑證機構對其他個體之憑證簽發通知

不做規定。

4.7 用戶憑證之金鑰更換

4.7.1 憑證金鑰更換之情況

(1)用戶之私密金鑰必須依照第 6.3.2 節規定定期更換。

(2)金鑰更換包括但不限於以下的情況：

(a)憑證因金鑰遭到破解而廢止

(b)憑證到期，且其金鑰效期也過期

持有保證等級第 2、第 3 及第 4 級之用戶，如其憑證沒有被廢止，下屬憑證機構或其註冊中心可於該用戶私密金鑰使用期限到期前 2 個月開始受理其更換金鑰並申請新的憑證，申請新憑證之程序依照 4.2 節規定辦理。

簽發保證等級第 2、第 3 及第 4 級之憑證的憑證機構，如其憑證沒有被廢止，總管理中心可於該憑證機構私密金鑰使用期限到期前 1 個月開始受理其更換金鑰並申請新的憑證機構憑證，申請新憑證機構憑證之程序依照第 4.2 節規定辦理。

4.7.2 更換憑證金鑰之申請者

憑證機構可接受更換憑證金鑰之請求，只要是符合金鑰與憑證生命週期管理且負責保管該憑證相對應之私密金鑰的原本用戶或者經授權之代表人。更換憑證金鑰所提供之憑證請求檔必須包含新的公開金鑰。

4.7.3 憑證金鑰更換之程序

憑證機構在處理金鑰更換時得要求憑證申請者提供額外之資訊或是重新驗證用戶之身分包含先前曾驗證過之身分資訊，透過適當的挑戰與回應機制進行身分鑑別。相關程序必須依照第 3.1、第 3.2、第 3.3、第 4.1 及第 4.2 節之規定辦理。

4.7.4 對用戶憑證金鑰更換之簽發通知

如第 4.3.2 節所述。

4.7.5 構成接受金鑰更換憑證之事由

如第 4.4.1 節所述。

4.7.6 憑證機構對金鑰更換之憑證的發布

如第 4.4.2 節所述。

4.7.7 憑證機構對其他個體之憑證簽發通知

不做規定。

4.8 憑證變更

4.8.1 憑證變更之情況

憑證變更係指對同一憑證主體提供 1 張新的憑證，其記載資訊和舊的憑證有些許不同，新的憑證有新的憑證序號，但新憑證和舊憑證的公開金鑰及憑證到期日相同。

4.8.2 憑證變更之申請者

憑證用戶之主體或經授權之代表人。

4.8.3 憑證變更之程序

如第 4.2 節所述。

4.8.4 對用戶憑證變更之簽發通知

如第 4.3.2 節所述。

4.8.5 構成接受變更之憑證的事由

如第 4.4.1 節所述。

4.8.6 憑證機構對變更之憑證的發布

如第 4.4.2 節所述。

4.8.7 憑證機構對其他個體之憑證簽發通知

不做規定。

4.9 憑證廢止及停用

除以保證等級測試級運作之憑證機構外，其他憑證機構皆應提供憑證廢止服務。憑證機構應於憑證實務作業基準中敘明憑證廢止請求及憑證問題報告之受理及回應的機制，並依憑證應用範圍及服務品質決定是否提供憑證停用服務。

對於已過期之憑證，憑證機構得不受理該憑證之廢止或停用申請，亦得不將該憑證之廢止或停用資訊列入憑證廢止清冊(或憑證機構廢止清冊)中。但對於過期前被廢止或停用之憑證，憑證機構應將其廢止或停用資訊列入憑證廢止清冊(或憑證機構廢止清冊)中至少 1 次，待憑證效期到期或被恢復使用後始可移除。

4.9.1 廢止憑證之情況

4.9.1.1 廢除用戶憑證之情況

以下幾種情況發生時，憑證機構應於 24 小時內廢止憑證：

(1) 用戶以書面提交憑證機構同意廢止憑證

(2) 用戶告知憑證機構原有之憑證請求未經授權

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

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

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

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

(2) 憑證機構證實用戶之憑證遭到誤用

(3) 用戶違反用戶約定條款規定

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

(5) 萬用網域憑證被用於詐欺或釣魚網站用途

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

(7) 憑證未依憑證機構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已過時(inaccurate)

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

(10) 憑證政策或憑證實務作業基準所規定應廢止項目

(11) 金鑰產製的過程有漏洞，可能導致用戶金鑰遭破解

4.9.1.2 廢除下屬憑證機構憑證之情況

以下幾種情況發生時，憑證機構應於 7 天內廢止下屬憑證機構之憑證：

(1) 下屬憑證機構以書面提交廢止憑證申請

(2) 下屬憑證機構告知憑證機構原有之憑證請求未經授權

(3) 憑證機構證實下屬憑證機構之私密金鑰遭破解或違反第 6.1.5 及第 6.1.6 節對於金鑰之長度及品質檢測之規定，且該私密金鑰與下屬憑證機構憑證中所記載之公開金鑰成配對關係

(4) 憑證機構證實下屬憑證機構憑證遭到誤用

(5) 憑證未依憑證機構之憑證政策或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已過時(inaccurate)或已變更

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

(9) 憑證機構之憑證政策或憑證實務作業基準所規定應廢止項目

憑證機構依照上述應廢止憑證之情況，得逕行廢止用戶、下屬憑證機構或交互認證憑證機構之憑證。

4.9.2 憑證廢止之申請者

用戶或擁有私密金鑰的個體得於憑證有效期限內向簽發其憑證之憑證機構或註冊中心提出憑證廢止請求。用戶、信賴憑證者、應用軟體廠商及其他第三方可向憑證機構提出憑證問題報告告知合理之原因以廢止憑證。

4.9.3 憑證廢止之程序

在收到憑證廢止申請後，憑證機構或註冊中心應依照第 4.9 節及憑證實務作業基準規定，對申請者進行身分識別及鑑別，若身分識別及鑑別無誤，以及憑證廢止的理由合理，例如不得無故選擇憑證機構

的金鑰被破解，則便可核准憑證廢止的申請。

如同意憑證廢止申請或決定逕行廢止憑證，則憑證機構或註冊中心應依照第 5.2 節及憑證實務作業基準規定，由適當人員執行憑證廢止之相關任務，憑證廢止後憑證機構或註冊中心應以適當的方式通知用戶。憑證機構，應於憑證實務作業基準中載明憑證廢止後通知用戶的方式。

如不同意廢止憑證，則憑證機構或註冊中心應以適當方式通知用戶，並明確告知不同意廢止的理由。憑證機構應於憑證實務作業基準中載明不同意廢止憑證之通知方式。

4.9.4 憑證廢止請求之寬限期

用戶於憑證廢止事由已經確認後，應儘速提出憑證廢止申請。若憑證機構和註冊中心之私密金鑰疑似遭破解，必須在 1 小時內通報該事由給簽發其憑證的憑證機構。憑證機構必要時得逐案延展其憑證廢止之寬限期。

4.9.5 憑證機構處理憑證廢止請求之處理期限

憑證機構應於收到憑證憑證問題報告後 24 小時內，調查有關的事實及情況，並提供一份初步的調查報告給用戶及回報者。

憑證機構應於其憑證實務作業基準敘明在接收到憑證廢止申請或憑證問題報告後，確認該憑證廢止請求是否成立之準則及程序，其處理期限依第 4.9.1 節所規定之合理的時間範圍來辦理。

4.9.6 信賴憑證者檢查憑證廢止之規定

使用保證等級第 2 級(含)以上憑證之信賴憑證者，於使用憑證前須透過憑證廢止清冊或是線上憑證狀態協定查詢服務查驗憑證之狀態。信賴憑證者須考量承擔之風險、責任及影響，自行決定擷取憑證

廢止資訊之時間。

憑證機構應於憑證實務作業基準中敘明信賴憑證者檢查憑證廢止清冊之要求。

4.9.7 憑證廢止清冊之簽發頻率

eCA 應簽發憑證機構廢止清冊，下屬憑證機構及交互認證憑證機構應簽發憑證機構廢止清冊或憑證廢止清冊。在簽發憑證機構廢止清冊或憑證廢止清冊前，應檢查其內容，確認資訊之正確性。例如，使用軟體掃瞄憑證機構廢止清冊或憑證廢止清冊，以檢查資料之正確性。憑證機構廢止清冊或憑證廢止清冊應定期發布，即使憑證狀態沒有改變也要簽發，以確保憑證狀態資訊的即時性。

憑證狀態資訊之公告應在下一次憑證狀態資訊更新時完成，如此將有助於離線或遠端作業的應用系統，將憑證狀態資訊儲存成近端快取(Local Cache)。憑證機構應加強與儲存庫間之配合，降低從憑證狀態資訊產生到公告於儲存庫的時間，憑證實務作業基準應規定以那一個儲存庫為主，以便用戶可以到該儲存庫取得最新的憑證狀態資訊。

當憑證狀態資訊公告時，過時的憑證狀態資訊應自儲存庫中移除。下表說明憑證機構廢止清冊及憑證廢止清冊之簽發頻率相關規定。

保證等級	憑證機構廢止清冊簽發頻率	憑證廢止清冊簽發頻率
測試級	不適用	不做規定
第 1 級	不適用	不做規定
第 2 級	不適用	每 3 天至少 1 次
第 3 級	每天至少 1 次	每天至少 1 次
第 4 級	每天至少 1 次	每天至少 1 次

4.9.8 憑證機構廢止清冊及憑證廢止清冊發布之最大延遲時間

憑證機構最遲應在憑證機構廢止清冊或憑證廢止清冊所記載之下次更新時間(the nextUpdate)前將憑證機構廢止清冊或憑證廢止清冊公布。

4.9.9 線上憑證廢止及狀態查驗之可用性

憑證機構至少應提供憑證廢止清冊，並於憑證實務作業基準中敘明是否提供線上憑證狀態協定查詢服務；若提供時，則其線上憑證狀態協定查詢服務須符合 RFC 6960 與 RFC 5019 之規範。

4.9.10 線上憑證廢止查驗之規定

憑證機構須於憑證實務作業基準中敘明信賴憑證者線上憑證廢止查驗之方式；其中，若憑證機構提供線上憑證狀態協定查詢服務，則其線上憑證狀態協定回應伺服器至少應支援符合 RFC 6960 與 RFC 5019 規範所述之 HTTP-based GET 方法。

4.9.11 廢止公告之其他發布形式

為了加速高流量網站的 SSL 憑證之驗證，以完成即時憑證狀態之驗證作業，本基礎建設所有憑證機構皆支援線上憑證狀態協定裝訂(OCSP Stapling)運作。

憑證機構可使用其他發布形式進行憑證廢止公告，替代方法必須滿足以下規定：

(1) 替代方法應敘明於憑證機構已被核准之憑證實務作業基準中

(2) 替代方法應提供與將廢止憑證之保證等級相當之鑑別與完整度服務

(3) 替代方法應滿足第 4.9.7 及第 4.9.8 節對於憑證廢止清冊之簽發及延遲的規定

4.9.12 金鑰被破解時之其他特殊規定

如果用戶確認私密金鑰遭破解，用戶必須立即通知憑證機構依照第 4.9.1、第 4.9.2 及第 4.9.3 節之相關規定廢止該憑證(註明該憑證廢止的原因為金鑰遭破解)，並簽發憑證廢止清冊以通知信賴憑證者該憑證不再受信任。

若總管理中心私密金鑰遭破解或洩漏，應透過網站或媒體等方式儘速通知應用軟體供應商、用戶及信賴憑證者。若下屬憑證機構私密金鑰遭破解或洩漏，將由總管理中心簽發憑證機構廢止清冊。並通知應用軟體供應商、用戶及信賴憑證者。

第三方提交私密金鑰遭破解的證據可接受的方式為：

(1) 由憑證機構提供隨機值或文件，由第三方以該私密金鑰對隨機值或文件數位簽章，經驗章而確認第三方握有遭破解之私密金鑰

(2) 提交該私密金鑰

4.9.13 憑證停用之情況

依照 Baseline Requirements 第 4.9.13 節之規定，不得提供 SSL 憑證之暫時停用服務。憑證機構應於憑證實務作業基準中敘明是否提供憑證停用及復用之服務。

4.9.14 憑證停用之申請者

針對 SSL 憑證不適用。

4.9.15 憑證停用之程序

針對 SSL 憑證不適用。

4.9.16 憑證停用期間之限制

針對 SSL 憑證不適用。

4.9.17 恢復使用憑證之程序

提供暫時停用憑證服務的憑證機構應於憑證實務作業基準中載明恢復使用憑證之程序。

依照 Baseline Requirements 第 4.9.13 節之規定，不得提供 SSL 憑證之恢復使用服務。

4.10 憑證狀態服務

4.10.1 操作特性

憑證機構應提供憑證廢止清冊或同時提供憑證廢止清冊與線上憑證狀態協定查詢服務。憑證廢止清冊或線上憑證狀態協定回應訊息中所註記之憑證廢止資訊，須至該被廢止之憑證已過期後始可移除，若憑證廢止資訊包含已停用之憑證時，須待該已停用之憑證恢復使用或已過期後始可移除。

4.10.2 服務可用性

憑證機構提供之憑證廢止清冊與選擇性提供之線上憑證狀態協定查詢服務，其回覆時間於正常運作情況下至多 10 秒。

憑證機構應提供 7 天 x 24 小時不中斷之憑證狀態服務，供應用軟體檢查所有未過期憑證之最新狀態。

憑證機構應提供 7 天 x 24 小時之回應機制，以因應高優先權之憑證問題報告，並可視案件情況向執法當局舉發，同時逕行廢止發生問題之憑證。

4.10.3 可選功能

不做規定。

4.11 訂購終止

訂購終止是指憑證用戶終止使用憑證機構的服務，憑證機構應允許用戶藉由廢止憑證或憑證到期而不做更新或是用戶約定條款失效而終止其對於憑證服務之訂購。

4.12 私密金鑰託管及回復

4.12.1 金鑰託管及回復之政策及實務

憑證機構簽章用之私密金鑰不可被託管(Escrowed)。

4.12.2 會議金鑰封裝及回復之政策及實務

憑證機構若有支援會議金鑰(Session Key)封裝及回復(Encapsulation and Recovery)應於其憑證實務作業基準描述其實務做法。

5 憑證機構設施、管理及操作控管

5.1 實體控管

5.1.1 所在位置及結構

除依照保證等級測試級及第 1 級運作之憑證機構不做規定外，依照保證等級第 2 級以上運作之憑證機構機房的實體所在及結構，必須符合儲存高重要性及敏感性資訊的機房設施水準，結合門禁、保全、入侵偵測及監視錄影等實體安全機制，以防止未經授權存取憑證機構之相關設備。

5.1.2 實體存取

除依照保證等級測試級及第 1 級運作之憑證機構不做規定外，依照保證等級第 2 級以上運作之憑證機構，在安裝及啟用密碼模組後，必須對憑證機構的設備進行實體控管，以防止遭受未經授權之存取。即使在沒有安裝或啟動密碼模組時，亦應對憑證機構的相關設備進行實體控管，以降低設備遭受非法開啟或破壞的風險。各保證等級之實體控管規定說明如下：

依照保證等級第 1 及第 2 級運作之憑證機構之實體控管規定：

(1) 確保能防止未經授權之侵入。

(2) 確保包含敏感性明文資料的可攜式儲存媒體和文件是保存在安全的場所。

依照保證等級第 3 及第 4 級運作之憑證機構之實體控管規定：

(1) 建置全天候人工或電子式監控設備，以防止未經授權之侵入。

(2) 定期維護和檢視存取記錄檔。

(3) 進行電腦系統和密碼模組實體控管時，必須至少兩人以上共

同執行。

eCA 因為必須簽發所有保證等級憑證，因此設備環境的安全機制依照保證等級第 4 級運作的實體控管規定。對於依照保證等級測試級運作之憑證機構的實體控管則不做規定，但應於憑證實務作業基準中說明。

在離開憑證機構機房時，應查驗以下事項以防止憑證機構機房被未經許可人員接近：

(1)必須適當地保全安全機箱。

(2)實體安全系統(例如門鎖、出入門禁)運作正常。

5.1.3 電力及空調

除依照保證等級測試級及第 1 級運作之憑證機構不做規定外，依照保證等級第 2 級以上運作之憑證機構，電力及空調設備必須具備足夠的備援設施，能支援憑證機構的相關系統，以因應外在因素影響時，能正常運作或關機。同時，必須提供不斷電系統，至少 6 小時以上之備用電力，以供儲存庫備援資料(包括已簽發憑證和憑證廢止清冊)。

5.1.4 水災防範

憑證機構之設置地點必須免於受到水災損害。

5.1.5 火災防範及保護

除依照保證等級測試級及第 1 級運作之憑證機構不做規定外，依照保證等級第 2 級以上運作之憑證機構機房必須具備自動偵測火災預警功能，系統能自動啟動滅火設備，並設置手動開關於各主要出入口處，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

除依照保證等級測試級及第 1 級運作之憑證機構不做規定外，依

照保證等級第 2 級以上運作之憑證機構必須保護系統相關的儲存媒體免於遭受意外的損害(如水、火、電磁場等)。

5.1.7 廢料處理

不做規定。

5.1.8 異地備援

憑證機構應於憑證實務作業基準敘明有無異地備援，備援的地點與憑證機構機房距離以及備援的項目。

5.2 程序控管

5.2.1 信賴角色

憑證機構必須安排信賴角色負責執行相關任務，以作為憑證機構信賴的基礎，如因意外或人為疏失而未能達到安全目標，則可能降低憑證機構的公正性。憑證機構可採用以下兩種方法增加安全性：

(1)保證擔任每種角色的人員已接受適當訓練且可充分信賴。

(2)適當的區隔每種任務，同一任務分派給 1 人以上，以防止 1 個人有機執行惡意活動。

規定之信賴角色如下：

(1)管理員：安裝、設定和維護憑證機構相關系統，並負責建立和維護系統之用戶帳號及設定稽核參數和產生元件金鑰。

(2)簽發員：啟動/停止憑證簽發/廢止服務。

(3)稽核員：查驗和維護稽核日誌、執行內部稽核。

(4)維運員：執行系統備份和故障排除。

(5)實體安全控管員：實體安全控管。

(6)網路安全專員：網路及網路設備之安全防護。

(7) 防毒防駭專員：提供防毒防駭、防惡意軟體等威脅之技術或措施。

(8) 註冊審驗人員：負責受理憑證申請、廢止及更換金鑰之申請，包括註冊及身分識別與鑑別等作業。

5.2.2 每項任務所需之人數

每項任務所需的人數應在憑證實務作業基準中說明。

5.2.3 識別及鑑別每一個角色

除依照保證等級測試級及第 1 級運作之憑證機構不做規定外，依照保證等級第 2 級以上運作之憑證機構其相關人員在執行角色分派任務前，必須識別和鑑別是否為本人。

5.2.4 需要職責分離之角色

為確保憑證機構設備及維運之安全性達到最佳化，憑證機構之角色需要職責分離的規定如下：

保證等級	角色分派原則
測試級	不做規定。
第1級	不做規定。
第2級	憑證機構之相關人員應依第5.2.1節規定指定擔任信賴角色，但必須符合以下規定： (1) 管理員、簽發員、稽核員和網路安全專員不得相互兼任 (2) 管理員、簽發員、稽核員可兼任維運員 (3) 實體安全控管員不得兼任管理員、簽發員、稽核員和維運員。 (4) 註冊審驗人員不得兼任管理員、稽核員及維運員 (5) 任何1個角色均不允許執行自我稽核功能。

保證等級	角色分派原則
第3級	同第2級之規定。
第4級	同第2級之規定。

5.3 人員控管

憑證機構必須確實掌握所有執行憑證機構或註冊中心運作之相關人員，人員任務指派的安全控管必須符合以下規定：

(1)以書面方式指派工作。

(2)以法規或契約規定執行任務之條件。

(3)接受任務之相關訓練。

(4)以法規或契約規定不可洩漏敏感之憑證機構相關安全資訊及憑證用戶資料。

(5)指派工作應符合利益迴避原則。

5.3.1 資格、經驗及清白規定

憑證機構必須進行人員的識別作業，忠誠、可信賴、正直和中華民國國民是遴選信賴角色人員的必備條件，人員的資格、遴選、監督和稽核相關辦法應在憑證實務作業基準中說明。

5.3.2 背景調查之程序

身家背景之調查程序應在憑證實務作業基準中說明。

5.3.3 教育訓練規定

憑證機構有義務提供相關人員以下之技能訓練：

(1)公開金鑰基礎架構基本知識

(2)憑證政策或憑證實務作業基準中載明之鑑別及審驗程序

(3)憑證申請資訊驗證過程常見之威脅，包含釣魚或其他社交工

程手法

(4) 災後復原及業務永續經營之程序

(5) 憑證機構及註冊中心之安全認證機制

(6) Baseline Requirements (只針對簽發 TLS/SSL 憑證之憑證機構)

憑證機構應要求註冊審驗人員通過憑證機構所提供有關 Baseline Requirements 對於資訊驗證規定之測驗，並留下紀錄以確保憑證註冊審驗人員維持足夠之知識與技能執行相關任務。憑證機構應以文件證明註冊審驗人員具備某項任務所需之技能。

5.3.4 人員再教育訓練之規定及頻率

擔任信賴角色之相關人員必須熟悉憑證機構相關工作程序及法規的改變。在任何重大變動時，例如憑證機構的軟體或硬體升級、工作程序改變及設備更換等，必須再接受教育訓練並記錄受訓情形。

新進人員也必須比照辦理，憑證機構必須每年進行檢視相關人員之受訓情形。

5.3.5 工作調換之頻率及順序

不做規定。

5.3.6 未授權行為之裁罰

憑證機構應訂定適當的管理辦法，以防止人員未經授權存取資料，並將相關規定公布在憑證實務作業基準中。對於違反憑證政策或憑證實務作業基準相關規定的人員，憑證機構必須採取適當的管理和懲處。

對於執行 eCA 及儲存庫主機的相關人員，如違反憑證政策或憑證實務作業基準或其他 eCA 公布之程序，必須採取適當的管理和懲處。

5.3.7 承攬商派駐人員之規定

承攬商派駐人員若擔任信賴角色，其職責、未授權行為之裁罰及應提供之教育訓練文件遵照第 5.3 節規定；操作行為之稽核與監控及相關紀錄保存遵照第 5.4.1 節規定。

5.3.8 提供之文件資料

憑證機構必須提供憑證政策、憑證實務作業基準及其他規定、政策、契約等相關文件，給憑證機構和註冊中心相關人員。

5.4 稽核紀錄程序

以保證等級測試級運作之憑證機構得不具備稽核記錄功能，簽發其他保證等級憑證之憑證機構，對於安全相關事件應具備適當的稽核紀錄(Audit Log)功能。稽核紀錄應儘可能由系統自動產生，如無法由系統自動產生，亦可使用工作記錄本、紙張或其他實體機制。所有安全稽核紀錄不論是電子或非電子的，均應妥善保存，並且在執行稽核時可立即正確取得。安全稽核紀錄之維護應依照第 5.5.2 節歸檔保留期限規定辦理。

5.4.1 被記錄事件種類

憑證機構之安全稽核功能，應包括憑證管理系統及憑證管理系統所依存的電腦作業系統(Operating System)的安全稽核。每筆稽核記錄至少應包括以下項目(不論是自動或手動記錄的稽核事件)：

(1) 事件種類。

(2) 引起事件的個體和操作者之身分。

(3) 事件發生之地點或位置

(4) 事件發生之時間和日期。

(5) 憑證機構執行憑證簽發及廢止程序之結果記錄(不論成功或失

敗)。

當事件發生時，稽核記錄可由憑證機構自行決定以電子或實體方式記錄，下表說明依各保證等級運作之憑證機構應紀錄的稽核事件，由於這些稽核事件都是需要憑證機構加以記錄或加以回應處理的，所以又被稱為可稽核事件(Auditable Event)：

可稽核事件／保證等級	**第 1 級**	**第 2 級**	**第 3 級**	**第 4 級**
A.1 安全稽核				
A.1.1 任何重要稽核參數之改變，如稽核頻率、稽核事件型態及新舊參數的內容等		✓	✓	✓
A.1.2 任何嘗試刪除或修改稽核紀錄檔		✓	✓	✓
A.2 識別與鑑別				
A.2.1 嘗試新角色的設定不論成功或失敗		✓	✓	✓
A.2.2 身分鑑別嘗試的最高容忍次數改變		✓	✓	✓
A.2.3 使用者登入系統時身分鑑別嘗試的失敗次數之最大值		✓	✓	✓
A.2.4 如管理者將已被鎖住的帳號解鎖，而且該帳號是因為多次失敗的身分鑑別嘗試而被鎖住的		✓	✓	✓
A.2.5 管理者改變系統的身分鑑別機制，例如從通行碼改為生物特徵值		✓	✓	✓
A.3 金鑰之產製				

可稽核事件／保證等級	第 1 級	第 2 級	第 3 級	第 4 級
A.3.1 當憑證機構產製金鑰時(不限制在單次或只限一次使用的金鑰產生)	✓	✓	✓	✓
A.4 私密金鑰之載入和儲存				
A.4.1 載入私密金鑰到系統元件中	✓	✓	✓	✓
A.4.2 所有為進行金鑰回復工作，對保存在憑證機構的憑證主體之私密金鑰所做的存取	✓	✓	✓	✓
A.5 可信賴公開金鑰之新增、刪除及儲存				
A.5.1 所有可信賴公開金鑰之改變，包括新增及刪除	✓	✓	✓	✓
A.6 私密金鑰之輸出				
A.6.1 私密金鑰之輸出(不包括只使用在單次或只限一次使用之金鑰)	✓	✓	✓	✓
A.7 憑證之註冊				
A.7.1 所有憑證之註冊申請過程	✓	✓	✓	✓
A.8 廢止之憑證				
A.8.1 所有憑證之廢止申請過程		✓	✓	✓
A.9 憑證狀態改變之核可				
A.9.1 核可或拒絕憑證狀態改變之申請		✓	✓	✓
A.10 憑證機構之組態設定				
A.10.1 任何與憑證機構安全相關之組態設定改變		✓	✓	✓

可稽核事件／保證等級	第 1 級	第 2 級	第 3 級	第 4 級
A.11 帳號之管理				
A.11.1 加入或刪除角色和使用者	✓	✓	✓	✓
A.11.2 使用者帳號或角色之存取權限修改	✓	✓	✓	✓
A.12 憑證格式剖繪之管理				
A.12.1 所有憑證格式剖繪之改變	✓	✓	✓	✓
A.13 憑證機構廢止清冊及廢止清冊格式剖繪之管理				
A.13.1 所有憑證機構廢止清冊及憑證廢止清冊格式剖繪之改變		✓	✓	✓
A.14 其他				
A.14.1 安裝作業系統		✓	✓	✓
A.14.2 安裝憑證機構系統		✓	✓	✓
A.14.3 安裝硬體密碼模組			✓	✓
A.14.4 移除硬體密碼模組			✓	✓
A.14.5 銷毀硬體密碼模組		✓	✓	✓
A.14.6 啟動系統		✓	✓	✓
A.14.7 嘗試登入憑證機構的應用作業		✓	✓	✓
A.14.8 硬體及軟體之接收			✓	✓
A.14.9 嘗試設定通行碼		✓	✓	✓
A.14.10 嘗試修改通行碼		✓	✓	✓
A.14.11 憑證機構之內部資料備份		✓	✓	✓

可稽核事件／保證等級	第 1 級	第 2 級	第 3 級	第 4 級
A.14.12 憑證機構之內部資料回復		✓	✓	✓
A.14.13 檔案操作(例如產生、重新命名及移動等)			✓	✓
A.14.14 傳送任何資訊到儲存庫公布			✓	✓
A.14.15 存取憑證機構之內部資料庫			✓	✓
A.14.16 任何憑證被破解之申告		✓	✓	✓
A.14.17 憑證載入符記			✓	✓
A.14.18 符記之傳遞過程			✓	✓
A.14.19 符記之零值化		✓	✓	✓
A.14.20 憑證機構之金鑰更換	✓	✓	✓	✓
A.15 憑證機構之伺服器設定改變				
A.15.1 硬體		✓	✓	✓
A.15.2 軟體		✓	✓	✓
A.15.3 作業系統		✓	✓	✓
A.15.4 修補程式(Patches)		✓	✓	✓
A.15.5 安全格式剖繪			✓	✓
A.16 實體存取及場所之安全				
A.16.1 人員進出憑證機構之機房			✓	✓
A.16.2 存取憑證機構之伺服器			✓	✓
A.16.3 得知或懷疑違反實體		✓	✓	✓

可稽核事件／保證等級	第 1 級	第 2 級	第 3 級	第 4 級
安全規定				
A.17 異常				
A.17.1 軟體錯誤		✓	✓	✓
A.17.2 軟體檢查完整性失敗		✓	✓	✓
A.17.3 接收不合適訊息			✓	✓
A.17.4 非正常路由之訊息			✓	✓
A.17.5 網路攻擊(懷疑或確定)		✓	✓	✓
A.17.6 設備失效	✓	✓	✓	✓
A.17.7 電力不當			✓	✓
A.17.8 不斷電系統 (Uninterrupted Power System, UPS)失敗			✓	✓
A.17.9 明顯及重大的網路服務或存取失敗			✓	✓
A.17.10 憑證政策之違反	✓	✓	✓	✓
A.17.11 憑證實務作業基準之違反	✓	✓	✓	✓
A.17.12 重設系統時鐘		✓	✓	✓

5.4.2 紀錄檔處理頻率

稽核紀錄應依據下表進行檢視，並且在稽核報表中對重大事件加以解釋。檢視工作應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。因應稽核檢視之結果所採取的行動亦應以文件記錄。

保證等級	紀錄檔之處理頻率
測試級	不做規定。
第 1 級	不做規定。
第 2 級	不做規定。
第 3 級	至少每兩個月 1 次。 憑證機構自上次稽核檢視後所發生的重大安全稽核紀錄應加以檢視，並且對任何可能之惡意活動應進一步調查。
第 4 級	至少每個月 1 次。 憑證機構自上次稽核檢視後所發生的重大安全稽核紀錄應加以檢視，並且對任何可能之惡意活動應進一步調查。

5.4.3 稽核紀錄檔保留期限

以保證等級測試級及第 1 級憑證運作的憑證機構，稽核紀錄檔之保留期限不做規定。

以保證等級第 2、第 3 及第 4 級憑證運作的憑證機構，稽核紀錄檔應在憑證機構所在處至少保留兩個月，並依照第 5.4.4、第 5.4.5、第 5.4.6 及第 5.5 節記錄保留管理機制等相關規定辦理。

當稽核紀錄檔的保留期限屆滿時，如須移除該資料，必須由稽核員移除，不可由其他人員代理。

5.4.4 稽核紀錄檔之保護

以保證等級測試級及第 1 級運作的憑證機構，稽核紀錄檔的保護不做規定。

以保證等級第 2、第 3 及第 4 級運作的憑證機構，電子稽核日誌系統(Electronic Audit Log System)必須包含保護機制，手動的稽核資訊亦應加以保護，以確保不會遭未經授權的閱讀、修改及刪除。

5.4.5 稽核紀錄檔備份程序

保證等級	稽核記錄檔之備份程序
測試級	不做規定。
第1級	
第2級	稽核記錄檔至少每月應備份1次。
第3級	
第4級	稽核記錄檔至少每月應備份1次，至少每月應異地(off-site)備援1次，異地備援相關程序應於憑證實務作業基準中規定。

5.4.6 稽核彙整系統

稽核系統可以在憑證管理系統之內部或外部。稽核程序應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。

5.4.7 對引起事件者之通知

當事件發生而被稽核系統紀錄時，稽核系統並不需要告知引起該事件的個體其所引發的事件已經被系統所紀錄。

5.4.8 弱點評估

以保證等級第 3 及第 4 級運作之憑證機構，應執行例行的弱點評估，以保證等級測試級、第 1 及第 2 級憑證運作之憑證機構則不做規定。

簽發 SSL 憑證之憑證機構應遵照 WebTrust for CA－SSL Baseline 及 CA/Browser Forum Network and Certificate System Security Requirements 規定之方式與頻率執行弱點評估與滲透測試。

5.5 紀錄歸檔之方法

5.5.1 歸檔紀錄之種類

依各保證等級的安全需求，應在歸檔時記錄以下資料(以保證等級測試級運作的憑證機構則不做規定)。

應歸檔資料／保證等級	第 1 級	第 2 級	第 3 級	第 4 級
憑證機構被主管機關認證(Accreditation)的資料(假設適用)	✓	✓	✓	✓
憑證實務作業基準	✓	✓	✓	✓
重要契約	✓	✓	✓	✓
系統與設備組態設定	✓	✓	✓	✓
系統或組態設定修改與更新的內容	✓	✓	✓	✓
憑證申請資料	✓	✓	✓	✓
廢止申請資料		✓	✓	✓
3.2.3 節訂定的用戶身分識別資料		✓	✓	✓
文件的簽收及憑證的接受		✓	✓	✓
符記啟用紀錄		✓	✓	✓
所有已簽發或公告的憑證	✓	✓	✓	✓
憑證機構金鑰更換的紀錄	✓	✓	✓	✓
所有被簽發或公告的憑證機構廢止清冊和憑證廢止清冊		✓	✓	✓
所有稽核記錄	✓	✓	✓	✓
用來驗證及佐證歸檔內容的其它說明資料或應用程式		✓	✓	✓
稽核人員所要求的文件		✓	✓	✓

5.5.2 歸檔資料之保留期限

歸檔資料的最低保留期限規定如下：

保證等級	最低保留期限
測試級	不做規定
第 1 級	2 年
第 2 級	2 年
第 3 級	2 年
第 4 級	20 年

如使用的儲存媒體無法達到上述的保留期限規定，則必須建立定期將歸檔資料轉換到新的儲存媒體之機制。同時用來處理歸檔資料的應用程式也必須被維護一定期間(時間長短由該憑證機構的主管機關決定)。

5.5.3 歸檔資料之保護

以保證等級測試級及第 1 級運作的憑證機構，歸檔資料之保護不做規定。

以保證等級第 2、第 3 及第 4 級運作的憑證機構，歸檔資料必須儲存在憑證機構以外的地方，並提供適當的保護，保護等級不可低於憑證機構所在處之保護等級。

5.5.4 歸檔資料備份程序

不做規定。

5.5.5 紀錄之時戳規定

不做規定。

5.5.6 歸檔資料彙整系統

不做規定。

5.5.7 取得及驗證歸檔資料之程序

憑證機構建立、核對、格式化及封包、移轉及儲存歸檔資料之程序，應在憑證實務作業基準中載明。

5.6 憑證機構之金鑰更換

憑證機構之私密金鑰必須依照第 6.3.2 節規定定期更換，以新私密金鑰取代舊私密金鑰簽發憑證，並應適時對信賴該憑證機構憑證的所有個體公告。

eCA 最遲應於其私密金鑰簽發憑證用途的使用期限到期前，更換用來簽發憑證的金鑰對，並簽發 1 張新的自簽憑證及使用新舊私密金鑰相互簽發 1 張自發憑證，此 3 張新憑證的簽發程序依照第 4.3 節規定。

下層憑證機構最遲應於其私密金鑰簽發憑證用途的使用期限到期前，更換用來簽發憑證的金鑰對。下層憑證機構更換金鑰對後，應依照第 4.1 節規定向上層憑證機構申請新的憑證，上層憑證機構必須於下層憑證機構憑證到期前，簽發並公告下層憑證機構的新憑證。

與 eCA 交互認證之本基礎建設外的根憑證機構，其金鑰更換時間由該憑證機構自行依其所遵循之憑證政策決定，該憑證機構更換金鑰後是否需要繼續向 eCA 申請交互憑證，則視該憑證機構與本公司之協議或契約而定。若該憑證機構更換金鑰需要繼續向 eCA 申請交互憑證，應依第 4.3 節規定辦理，並須保留足夠時間供政策管理委員會及 eCA 處理其交互認證申請，以確保 eCA 能夠在該憑證機構之交

互憑證過期前，簽發並公告該憑證機構之新交互憑證。

若舊私密金鑰仍須簽發憑證廢止清冊(或憑證機構廢止清冊)或線上憑證狀態的回應，則維持與保護該舊私密金鑰至以舊私密金鑰簽發的所有用戶憑證到期為止。

5.7 遭破解及災變之復原

5.7.1 緊急事件及系統遭破解之處理程序

憑證機構應訂定緊急事件和系統遭破解後之通報與處理程序，同時每年進行演練。

5.7.2 電腦資源、軟體或資料遭破壞

憑證機構必須以永續經營為目標，依據憑證政策及憑證實務作業基準規定確實做好各種備援措施，儘可能將電腦資源、軟體及資料遭破壞之災害損失減至最低，並迅速恢復憑證之簽發及管理作業。

以保證等級第 3 及第 4 級運作之憑證機構至少每年應進行 1 次電腦資源、軟體及資料遭破壞之演練。

5.7.3 憑證機構私密金鑰遭破解之處理程序

以保證等級第 2、第 3 及第 4 級運作之憑證機構，應在憑證實務作業基準中或相關的文件中載明憑證機構之簽章金鑰遭破解時之復原程序，以迅速恢復憑證之簽發及管理作業能力。

以保證等級第 3 及第 4 級運作之憑證機構至少每年應進行 1 次憑證機構私密金鑰遭破解之演練。

憑證機構私密金鑰遭破解時，應立即通知應用軟體供應商、用戶及信賴憑證者。

5.7.4 災變後業務持續營運能力

以保證等級第 2、第 3 及第 4 級運作之憑證機構應在憑證實務作業基準敘明在災變後，恢復憑證機構設施運作的步驟。

以保證等級第 3 及第 4 級運作之憑證機構至少每年應進行 1 次災後復原計畫之演練。

5.8 憑證機構或註冊中心之終止服務

憑證機構應依據電子簽章法相關規定進行終止服務。

6 技術性安全控管

6.1 金鑰對之產製及安裝

6.1.1 金鑰對之產製

憑證機構簽發憑證所使用的密碼模組，必須經由中華電信核可之安全等級相當的密碼模組來產製金鑰。

金鑰產製過程中所採用之隨機亂數依照 NIST FIPS 140-2 規範之演算法，其長度及亂度即使提供足夠的資訊和設備，欲計算出相同的亂數序列是不可行的(Computationally Infeasible)。

儲存在密碼模組內之私密金鑰，應防止其由密碼模組中外洩。如私密金鑰在密碼模組內產製，該金鑰應一直保存在該密碼模組中或加密儲存於主機中。如私密金鑰在密碼模組外產製，該金鑰應在不離開金鑰產製的環境下匯入密碼模組中，該環境應保證沒有人員可用任何方法，在不被偵測的情形下取得已經產製的私密金鑰，當私密金鑰儲存在密碼模組後，該金鑰應立即由金鑰產製的環境中刪除。

憑證機構應採取適當的措施來確保用戶的公開金鑰在該憑證機構所轄之公開金鑰基礎建設領域內是唯一的。

任何被用於金鑰產製的隨機亂數，必須經由中華電信認可。用戶隨機亂數、金鑰對和對稱金鑰之產製，使用軟體或硬體之相關規定如下表所列：

保證等級	金鑰產製機制
測試級	軟體或硬體
第1級	軟體或硬體
第2級	軟體或硬體

保證等級	金鑰產製機制
第3級	軟體或硬體
第4級	只限硬體

6.1.2 私密金鑰傳送給用戶

如私密金鑰在用戶的密碼模組內被產製及儲存時，無需傳送其私密金鑰。

如由個體(例如憑證用戶或 IC 卡發卡中心)所擁有的符記(Token)直接產製金鑰，或由另一個金鑰產製者產製金鑰後，再傳送金鑰到該個體的符記中，則此個體在私密金鑰產生及接受時，已被視為擁有該私密金鑰。但若上述的個體並不是憑證申請的用戶時，則應以安全及可稽核的方法傳送私密金鑰給用戶，以完成私密金鑰的傳送。

對於所有保證等級，如存放金鑰的硬體傳送給用戶時，應確保將正確的符記及其啟動資料(Activation Data)傳送給用戶。憑證機構必須維護 1 份確認用戶已收到該符記的紀錄。當使用任何包含秘密共享(如密碼或 PIN 碼)的機制，則該機制必須確保只有申請者及 eCA 或下屬憑證機構是唯一擁有該秘密的個體。

如私密金鑰由憑證機構或註冊中心或可信賴的第三者代為產製，則此密碼模組必須安全傳送至用戶，用戶必須作收受私密金鑰的確認。密碼模組的存放位置及狀態之追溯紀錄必須被妥善保存，至少到用戶確認接受該密碼模組為止。

在任何情況下，除了用戶外，其他人皆不能取得或控制簽章用私密金鑰。任何替用戶產製簽章用之私密金鑰的個體，也不可保留該金鑰的備份。

6.1.3 公開金鑰傳送給憑證機構

在憑證機構對用戶做身分鑑別時，用戶必須將其公開金鑰傳送給憑證機構，傳送的方式包括：

(1) 由註冊中心代為發出憑證申請的電子訊息
(2) 由第三者產製金鑰時，憑證機構或註冊中心必須透過可稽核之安全管道，取得用戶之公開金鑰
(3) 其它安全的電子化機制來完成
(4) 安全的非電子化方式來完成，如經由掛號郵件或快遞傳送儲存用戶公開金鑰之媒體

6.1.4 憑證機構公開金鑰傳送給信賴憑證者

eCA 之公開金鑰必須隨時可取得。下屬憑證機構必須以可信賴的方式將 eCA 自簽憑證或公開金鑰傳遞給信賴憑證者。可信賴之憑證傳送方式包括以下幾種：

(1) 憑證機構以符記儲存 eCA 之自簽憑證或公開金鑰，並以安全方式傳送至信賴憑證者。
(2) 透過特殊安全的管道(out-of-band)傳送 eCA 之自簽憑證或公開金鑰。
(3) 透過特殊安全的管道(out-of-band)傳送 eCA 之自簽憑證或公開金鑰之雜湊值或指紋，供使用者比對(與憑證一起在線上公布(in-band)的雜湊值或指紋，不被視為是合格的安全管道)。
(4) 其他政策管理委員會核可之方式。

以上所述之特殊安全管道應在eCA的憑證實務作業基準中說明。eCA簽發的下屬憑證機構憑證須公布在該憑證機構的儲存庫中。

6.1.5 金鑰長度

保證等級	公開金鑰
測試級 第1級 第2級 第3級	(1) 民國102年12月31日(含)之前，至少須使用RSA 1024位元的金鑰或其他安全強度相當之金鑰。 (2) 民國103年1月1日(含)起至民國119年12月31日(含)之前，至少須使用RSA 2048 位元金鑰或其他安全強度相當之金鑰。 (3) 民國120年1月1日(含)起，應使用RSA 3072 位元金鑰或其他安全強度相當之金鑰。
第4級	至少必須使用RSA 4096位元的金鑰或其他安全強度相當之金鑰。

6.1.6 公開金鑰參數之產製及品質檢驗

RSA演算法之公開金鑰參數須為空值(Null)，可無須進行參數品質檢驗，但須執行質數之測試，憑證機構應於憑證實務作業基準中說明如何執行相關測試。

使用其他演算法時，憑證機構應依相關國際標準(如NIST SP 800-89)進行公開金鑰參數之設定與參數品質檢驗。

6.1.7 金鑰之使用目的

憑證機構憑證之金鑰用途擴充欄位須包含金鑰用途位元keyCertSign與cRLSign；若憑證機構欲使用其簽章用私密金鑰簽發線上憑證狀態協定回應訊息時，此擴充欄位應再包含金鑰用途位元digitalSignature。

憑證機構簽發之用戶憑證之金鑰用途擴充欄位須依其金鑰對產製所使用之演算法與金鑰用途設定所需之金鑰用途位元，但不可包含cRLSign與keyCertSign。

6.2 私密金鑰保護及密碼模組工程控管

憑證機構應提供實體與邏輯保護措施，以防止未經授權之憑證簽發。憑證機構之私密金鑰若存在於密碼模組之外，則其應採用實體安全機制、加密或兩者結合等方式保護，避免憑證機構私密金鑰遭洩漏。憑證機構應使用具備防範密碼分析攻擊之演算法與金鑰長度來加密其私密金鑰。

6.2.1 密碼模組標準及控管

政策管理委員會應確認本基礎建設所使用的密碼模組之安全需求符合FIPS 140-2系列或安全強度相當之國際標準。

對於本基礎建設之各個個體，除用戶須盡可能遵照外，其餘個體應參照下表做為密碼模組之最低安全要求，亦可使用更高之安全等級，此表中所列之等級係參照FIPS 140-2系列之定義。

個體 / 保證等級	eCA	下屬憑證機構	註冊中心	用戶
測試級	不適用	不做規定	不做規定	不做規定
第1級	不適用	等級1 (硬體/軟體)	等級1 (硬體/軟體)	不做規定
第2級	不適用	等級2 (硬體)	等級1 (硬體/軟體)	等級1 (硬體/軟體)
第3級	不適用	等級3 (硬體)	等級2 (硬體)	等級1 (硬體/軟體)
第4級	等級3 (硬體)	等級3 (硬體)	等級2 (硬體)	等級2 (硬體)

6.2.2 私密金鑰分持之多人控管

簽發保證等級第3與第4級憑證的憑證機構之簽章用私密金鑰，必須符合第5章規定之多人控管程序。

6.2.3 私密金鑰託管

憑證機構之簽章用私密金鑰不可被託管。

6.2.4 私密金鑰備份

憑證機構之簽章用私密金鑰應在多人控管程序下進行備份，並保存在備援場所；金鑰備份之程序須於憑證實務作業基準中說明。

6.2.5 私密金鑰歸檔

憑證機構之簽章用私密金鑰不可以被歸檔。

6.2.6 私密金鑰匯入、匯出密碼模組

私密金鑰僅於金鑰備份、金鑰回復或更換密碼模組時，始可從密碼模組匯出至備份專用之符記，亦或從備份專用之符記匯入至密碼模組，其匯入或匯出過程之控管方式應遵照第6.2.2節之規定。私密金鑰從密碼模組匯出或於密碼模組間傳輸時，憑證機構及其註冊中心應使用加密或金鑰分持多人控管方式保護，確保私密金鑰不曾以明碼呈現。私密金鑰匯入完成後，須將匯入過程產製之相關機密參數完全銷毀。

若上層憑證機構發現有下層憑證機構之私密金鑰洩漏給未授權人員或不屬於下層憑證機構之組織之情形，上層憑證機構應將與該私密金鑰相關之憑證廢止。

6.2.7 私密金鑰儲存於密碼模組

依照第6.1.1與第6.2.1節規定。

6.2.8 私密金鑰之啟動方式

儲存在密碼模組中的私密金鑰在啟動時必須對啟動者做身分鑑別。可接受的鑑別方式包含(但不限於)通行詞組(Pass-Phrase)、個人符記、個人識別碼(Personal Identification Number, PIN)或生物識別，但

輸入的啟動資料必須避免被洩露(不應被顯示出來)。

已啟動的私密金鑰不應沒人看管或是容許未經授權的存取。

6.2.9 私密金鑰之停用方式

密碼模組不需要使用時必須停止運作；透過手動的登出程序，或經過一段時間沒有運作後(時間的長度在憑證實務作業基準中訂定)自動停止運作。如硬體密碼模組不再使用時，必須與主機分離並儲存至安全場所。

6.2.10 私密金鑰之銷毀方式

當簽章用私密金鑰及其備份不再需要、憑證到期或被廢止時，私密金鑰必須被銷毀。對於軟體密碼模組而言，必須將亂數資料複寫至原簽章用私密金鑰佔用的記憶體或儲存媒體。對於硬體密碼模組而言，必須執行零值化(Zeroize)動作，但不需做實體銷毀。

6.2.11 密碼模組評等

參見第6.2.1節。

6.3 金鑰對管理之其他規範

6.3.1 公開金鑰歸檔

憑證依第5.5節規定歸檔後，得無須再進行公開金鑰之歸檔。

6.3.2 憑證操作及金鑰對之效期

6.3.2.1 憑證機構憑證操作及金鑰對之效期

憑證機構之憑證及其私密金鑰最長效期如下：

憑證機構	私密金鑰效期	憑證效期
根憑證機構	■ 簽發自簽憑證：15年 ■ 簽發自發憑證：不做規定 ■ 簽發交互憑證：不做規定 ■ 簽發下屬憑證機構憑證：15年 ■ 簽發憑證廢止清冊、線上憑證狀態協定回應伺服器憑證或線上憑證狀態協定回應訊息：30年	30年
下屬憑證機構/交互認證憑證機構	■ 簽發用戶憑證：10年 ■ 簽發憑證廢止清冊、線上憑證狀態協定回應伺服器憑證或線上憑證狀態協定回應訊息：20年	20年

根憑證機構簽發之下屬憑證機構憑證或交互憑證之效期不得超過根憑證機構自簽憑證之效期。

根憑證機構新舊金鑰互簽之自發憑證之效期應至根憑證機構舊金鑰簽發之自簽憑證效期到期為止。

6.3.2.2 用戶憑證操作及金鑰對之效期

用戶憑證及其私密金鑰最長效期如下：

憑證類型	私密金鑰效期	憑證效期
TLS憑證	不做規定	398天
嚴格型和多用途型S/MIME憑證	不做規定	825天
傳統型S/MIME憑證	不做規定	1185天
時戳憑證	15個月	135個月
其他類憑證	10年	10年

用戶憑證(包含展期後憑證)之有效效期不得超過其簽發憑證機構之憑證效期。

6.4 啟動資料

6.4.1 啟動資料之產生及安裝

私密金鑰之啟動資料與其他相關存取控制機制必須適當地保護。對於以保證等級第1、第2及第3級運作之憑證機構，其啟動資料得由其適任之信賴角色人員自行選擇管理方式。對於以保證等級第4級運作之憑證機構，其啟動資料除須交由適任之信賴角色人員管理外，亦應採用生物特徵資料或密碼模組之安全機制進行保護。如果啟動資料必須傳送，其傳送方法必須保持啟動資料之機密性與完整性。

6.4.2 啟動資料之保護

用來啟動私密金鑰之啟動資料，必須使用結合密碼與存取控制機制加以保護，以防止揭露。啟動資料得以生物特徵或記憶方式保存。若需留下紀錄，必須使用與該資料安全等級相當的密碼模組來保護，以確保其安全。若登入失敗次數超過憑證實務作業基準規定之最大預設值時，保護機制必須能即時鎖住此帳號或終止應用程式。

6.4.3 啟動資料之其他規範

不做規定。

6.5 電腦軟硬體安控措施

6.5.1 特定電腦安全技術需求

依照保證等級第3及第4級運作之憑證機構和其相關輔助系統必須包含以下特定電腦之功能，這些功能可由作業系統，或結合作業系統、軟體和實體的保護措施提供。

(1) 具備身分鑑別的登入

(2) 依所擔任之角色定義存取權限

(3)提供安全稽核能力

(4)以密碼技術確保每次通訊和資料庫安全。

(5)具備程序完整性及安全控管保護。

憑證機構設備必須建構在經過安全評估的作業平臺上，且憑證機構相關系統(硬體、軟體、作業系統)必須在經過安全評估的組態下運作。憑證機構應對能夠導致簽發憑證之帳號實施多因子認證。

6.5.2 電腦安全評等

不做規定。

6.6 生命週期技術控管

6.6.1 系統研發控管

憑證機構之系統研發控管措施說明如下：

保證等級	系統研發控管措施
測試級	不做規定。
第1級	不做規定。
第2級 第3級 第4級	(1)須確保使用之軟體係依軟體工程發展方法開發。 (2)硬體與軟體須專用且獲得授權。 (3)須防止惡意軟體安裝於憑證機構設備。 (4)註冊中心之軟體於初次使用或更新版本前須進行惡意程式碼檢查，並定期執行安全性掃描作業。 (5)系統開發環境與測試環境應與上線環境有所區隔。 (6)憑證機構之系統研發單位應善盡良善管理責任，諸如簽署安全遵循保證書，確保無後門或惡意程式，並提供程式或硬體交付清單、測試報告及管理手冊。

6.6.2 安全管理控管

憑證機構之安全管理控管措施說明如下：

保證等級	安全管理控管措施
測試級 第1級 第2級 第3級	(1)不得安裝與運作無關之軟硬體。 (2)須記錄與控管憑證機構相關系統組態及系統修訂歷程。 (3)具備偵測未經許可修改憑證機構之軟體或組態機制。 (4)安裝軟體時，須確認該軟體為正確版本且未被竄改。 (5)遵循WebTrust for CA之規定執行安全管理控管措施。
第4級	(1)不得安裝與運作無關之軟硬體。 (2)須記錄與控管憑證機構相關系統組態及系統修訂歷程。 (3)具備偵測未經許可修改憑證機構之軟體或組態機制。 (4)安裝軟體時，須確認該軟體為正確版本且未被竄改。 (5)每次執行前驗證憑證機構軟體之完整性。 (6)遵循WebTrust for CA之規定執行安全管理控管措施。

6.6.3 生命週期安全控管

憑證機構得依需求自行決定生命週期之安全控管措施，並於憑證實務作業基準中規定。

6.7 網路安全控管措施

憑證機構之主機不得與任何外部網路連接，而其儲存庫則必須連接到網際網路(Internet)上，以提供不中斷服務(除必要之維護或備援外)。憑證機構之主機所簽發的憑證與憑證機構廢止資訊以手動方式，從與外部網際網路實體隔離的憑證機構之主機傳送到儲存庫，而且所有資訊(憑證與憑證機構廢止清冊)都以數位簽章保護。儲存庫透過系統修補程式的更新、弱點掃描、入侵偵測系統、防火牆、過濾路由器(Filtering Router)等加以保護，以防範阻絕服務和入侵等攻擊。

6.8 時戳

憑證機構之系統應定期與受信賴時間源進行同步，以維持系統時間正確性，並確保以下時間之正確性：

(1)憑證簽發時間。

(2)憑證廢止時間。

(3)憑證廢止清冊之簽發時間。

(4)系統事件之發生時間。

憑證機構系統校時動作為可稽核事件(參見第5.4.1節)。

7 憑證、憑證廢止清冊及線上憑證狀態協定之格式剖繪

7.1 憑證之格式剖繪

憑證機構須透過密碼學安全偽亂數生成器(Cryptographically Secure Pseudorandom Number Generator, CSPRNG)產生大於零、非循序、且至少包含64位元的亂度之憑證序號。

7.1.1 版本序號

憑證機構須簽發ITU-T X.509 v3版本之憑證。

7.1.2 憑證擴充欄位

憑證機構須遵循 ITU-T X.509、Baseline Requirements 及 RFC 5280 規定使用憑證擴充欄位。若須另訂欲使用之擴充欄位時，應於憑證實務作業基準中說明，並註明該擴充欄位之關鍵性。

7.1.3 演算法物件識別碼

憑證機構簽發之憑證可使用之演算法物件識別碼如下：

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

7.1.4 命名形式

憑證之主體與簽發者欄位須使用 ITU-T X.500 的唯一識別名稱，且該欄位屬性型態須遵照 ITU-T X.509、Baseline Requirements 及 RFC 5280 之規定。

依據 Baseline Requirements 第 7.1.4.1 節規定，憑證路徑中的每張憑證，其簽發者欄位之編碼內容須與簽發憑證機構憑證之主體欄位的編碼形式完全相同。此外，前述憑證機構憑證若存在多張主體欄位內容相符之憑證(包含過期與廢止之憑證)，則其主體欄位之編碼內容應皆完全相同。

7.1.5 命名限制

不做規定。

7.1.6 憑證政策物件識別碼

當憑證機構簽發之憑證引用第 1.2 節中所訂之憑證政策物件識別碼時，則應表示該憑證已遵照該憑證政策物件識別碼規範之規定進行簽發與管理。

7.1.7 政策限制擴充欄位之使用

不做規定。

7.1.8 政策限定元之語法及語意

不做規定。

7.1.9 關鍵憑證政策擴充欄位之語意處理

關鍵憑證政策擴充欄位之語意處理須遵照 ITU-T X.509、Baseline Requirements 及 RFC 5280 之規定。

7.2 憑證廢止清冊之格式剖繪

7.2.1 版本序號

憑證廢止清冊須符合 ITU-T X.509 v2 版本之規定。

7.2.2 憑證廢止清冊及憑證廢止清冊條目之擴充欄位

憑證廢止清冊之憑證廢止清冊擴充欄位與憑證廢止清冊條目擴充欄位皆須遵循 ITU-T X.509、Baseline Requirements 及 RFC 5280 之規定。

7.3 線上憑證狀態協定之格式剖繪

憑證機構若提供線上憑證狀態協定查詢服務，應於其憑證實務作業基準敘明線上憑證狀態協定版本序號與擴充欄位所採用之標準，其查詢服務網址應可於憑證之憑證機構資訊存取(Authority Information Access, AIA)擴充欄位中取得。

7.3.1 版本序號

線上憑證狀態協定查詢服務應符合 RFC 5019 與 RFC 6960 規範。

7.3.2 線上憑證狀態協定擴充欄位

線上憑證狀態協定擴充欄位應遵循 Baseline Requirements、RFC 5019 及 RFC 6960 之規定。

8 稽核及其他評核

簽發保證等級第 2、第 3 及第 4 級憑證之憑證機構，應依照 WebTrust for CA 執行公正之稽核(Compliance Audit)，以確保其運作遵照憑證實務作業基準與憑證政策之規定。簽發組織驗證型、網域驗證型及個人驗證型 SSL 憑證之憑證機構另須通過 WebTrust for CA－SSL Baseline 外稽。

若憑證機構未執行過上述之任一項稽核，則該憑證機構在核發 SSL 憑證前須通過準備度稽核(point-in-time readiness assessment)。

簽發安全電子郵件憑證之憑證機構另須通過 WebTrust for CA- S/MIME 及 WebTrust for CA - Network Security 外稽。

8.1 稽核頻率或評核時機

憑證機構應接受定期稽核，依照保證等級第 3 及第 4 級運作之憑證機構至少每年 1 次，且查核期間不可超過 12 個月。依照保證等級第 2 級運作之憑證機構至少每兩年 1 次。依照保證等級測試級及第 1 級運作之憑證機構則不做規定。

憑證機構得對其下屬憑證機構及註冊中心進行定期及不定期稽核，以確認下屬個體遵照憑證實務作業基準運作。

8.2 稽核人員之身分及資格

稽核人員應獨立於被稽核的憑證機構外，可由以下個體擔任：

(1) 第三公正人員。

(2) 組織劃分上與被稽核的憑證機構有所區別的另一獨立個體。

稽核人員應提供公正及獨立的評估。本公司委託熟悉憑證機構運

作並經 WebTrust for CA 系列標章管理單位授權可於中華民國執行 WebTrust for CA 及 WebTrust for CA – SSL Baseline 之稽核業者，提供公正客觀的稽核服務。稽核人員應為合格授權之資訊系統稽核員(Certified Information System Auditor)或具同等資格，且具備 2 場次 4 人天以上之憑證機構 WebTrust for CA 系列標章稽核或 2 場次共計 8 人天憑證機構資訊安全管理稽核相關經驗，且熟悉憑證機構簽發、管理憑證的相關規定。憑證機構於稽核時應對稽核人員進行身分識別。

8.3 稽核人員及被稽核方之關係

依照第 8.2 節規定，稽核人員應獨立於被稽核的憑證機構外。

8.4 稽核項目

稽核項目如下所述：

(1) 憑證機構是否遵照憑證實務作業基準運作。

(2) 憑證機構之憑證實務作業基準是否符合憑證政策之規定。

(3) 稽核人員可對憑證機構之相關營運單位如註冊中心進行稽核。

(4) 憑證機構與其他根憑證機構簽訂交互認證協議書(Cross Certification Agreement, CCA)時，稽核之項目應涵蓋該根憑證機構是否符合交互認證協議書之規定。

8.5 對於稽核結果之因應方式

當稽核人員發現憑證機構之建置及維運不符合憑證政策或交互認證協議書之規定時，必須採取以下行動：

(1) 稽核人員應記錄不符合情形。

(2) 稽核人員應通知發生不符合情形憑證機構之維運管理單位，如不符合情形為嚴重缺失，稽核人員應通知政策管理委員會。

發生不符合情形之憑證機構，應依據稽核報告及憑證政策或交互認證協議書之規定，執行修正。

8.6 稽核結果之公開

除可能導致系統被攻擊以及第 9.3 節規定之範圍外，憑證機構應公布與信賴該憑證機構之信賴憑證者有關的最近 1 次外部稽核結果。稽核結果由憑證機構依照其適用的標準懸掛 WebTrust for CA 標章或 WebTrust for CA – SSL Baseline 標章呈現於憑證機構網站首頁，點選標章後可閱覽外稽報告與管理聲明書。最近 1 次的外稽報告與管理聲明書亦應於查核區間結束後 3 個月內公布於憑證機構之儲存庫。若因故延遲公布最近 1 次稽核結果，憑證機構應提供合格稽核業者簽署之解釋函。

8.7 自我稽核

簽發 SSL 憑證之憑證機構另須安排稽核員依據 Baseline Requirements 及 WebTrust for CA – SSL Baseline，自前 1 次抽樣後至少每季，隨機選擇 3% 或至少 1 張 SSL 憑證執行內部稽核。

簽發 S/MIME 憑證之憑證機構另須安排稽核員依據 S/MIME Baseline Requirements 及 WebTrust for CA – S/MIME Baseline，自前 1 次抽樣後至少每季，隨機選擇 3% 或至少 1 張 S/MIME 憑證執行內部稽核。

9 其他業務及法律事項

9.1 費用

9.1.1 憑證簽發、展期費用

不做規定。

9.1.2 憑證查詢費用

不做規定。

9.1.3 憑證廢止、狀態查詢費用

不做規定。

9.1.4 其他服務費用

不做規定。

9.1.5 請求退費之程序

不做規定。

9.2 財務責任

9.2.1 保險涵蓋範圍

不做規定。

9.2.2 其他資產

參見第 9.2.1 節

9.2.3 對終端個體之保險或保固責任

不做規定。

9.3 業務資訊之保密

9.3.1 機密資訊之範圍

由憑證機構產生、接收或保管之資料，現職及曾任職於憑證機構之人員與各類稽核人員對於機密資訊均負保密責任。機密資訊至少包括：

(1) 任何在憑證申請時記載之個人或組織資訊皆為機密資訊，未經用戶同意或依法律規定不得公開。

(2) 用於憑證機構營運的私密金鑰及通行碼皆為機密資訊，不得公開。

(3) 稽核紀錄除第 8.6 節規定情形外，不得被完整公開。

憑證機構之憑證實務作業基準中應載明機密之資訊種類。

9.3.2 非機密資料之範圍

(1) 憑證、憑證廢止清冊及廢止或停用資訊不視為機密資訊。憑證廢止或暫時停用資訊屬於非機密資訊，應對外公開。

(2) 識別資訊或記載於憑證的資訊，除特別約定外，不視為機密資訊與隱私資訊。

憑證機構之憑證實務作業基準應載明非機密資料之種類。

9.3.3 保護機密資訊之責任

憑證機構應實施安控措施防止機密資訊遭洩漏或破壞。

9.4 個人資訊之隱私

9.4.1 隱私保護計畫

憑證機構應於網站公告個人資料保護與隱私權聲明。憑證機構宜實施隱私衝擊分析、個資風險評估等措施以訂定隱私保護計畫。

9.4.2 隱私之資訊

任何在憑證申請時記載之個人資訊，未經用戶同意或依法律規定不得公開。無法透過憑證、憑證廢止清冊所記載之資訊或憑證目錄服務所取得的用戶資訊、憑證機構信賴角色維運之可識別的個人資料如姓名搭配掌紋與指紋特徵、保密協定或契約之個人資訊等應視為隱私資料加以保護，憑證機構及註冊中心應實施安控措施防止可識別之個人資料遭未經授權的揭露、洩漏或破壞。

9.4.3 非隱私之資訊

識別資訊或記載於憑證的資訊與憑證，除特別約定外，不視為機密資訊與隱私資訊。

儲存庫公布之簽發憑證、已廢止憑證或暫時停用資訊及憑證廢止清冊非機密與隱私資訊。

9.4.4 保護隱私資訊之責任

配合憑證機構運作所需之個人資料必須安全存放與受到保護，符合電子簽章法、WebTrust for CA 標準及個人資料保護法相關規定。憑證機構並須與註冊中心協議保護隱私資訊的責任。

9.4.5 使用隱私資訊之告知與同意

遵循個人資料保護法，非經用戶同意或個人資料保護與隱私權聲明與本憑證政策另有規範，不會將個人資料用於其他地方。憑證機構之憑證實務作業基準應訂定有關提供第 9.3.1 節機密資訊第(3)款之相關規定。

9.4.6 應司法或管理程序釋出資訊

除非經本憑證政策允許，或經法律或政府規章要求或配合司法審

判，憑證機構不應揭露隱私資訊給任何第三方。憑證機構之憑證實務作業基準應訂定有關提供司法人員第 9.4.2 節隱私資訊之相關規定。

9.4.7 其他資訊釋出之情形

依相關法律規定辦理。憑證機構之憑證實務作業基準應訂定有關提供用戶第 9.3.1 節機密資訊之相關規定。

9.5 智慧財產權

本憑證政策為本公司之智慧財產，可依著作權法相關規定複製或散布，並註明著作權為本公司所擁有。複製或散布本憑證政策者，不得向他人收取費用，對於不當使用或散布本憑證政策之侵害，本公司將依法予以追訴。

9.6 聲明及擔保

9.6.1 憑證機構之聲明及擔保

憑證機構必須聲明及擔保以下責任：

(1) 如憑證機構在簽發的憑證中，引用憑證政策所訂的任何保證等級之物件識別碼，即表示該憑證機構保證其所簽發憑證之內容資訊已遵守憑證政策之規定。除非憑證機構確實遵守憑證政策之規定，否則不得在所簽發的憑證中引用憑證政策所訂的任何保證等級之憑證政策物件識別碼。

(2) 執行憑證申請之識別與鑑別程序。

(3) 簽發及公布憑證。

(4) 廢止憑證。

(5) 簽發及公布憑證廢止清冊。

(6) 簽發及提供線上憑證狀態查詢協定回應訊息。

(7) 執行憑證機構人員之識別與鑑別程序。

(8) 安全產製憑證機構之私密金鑰。

(9) 保護憑證機構之私密金鑰。

(10) 若有將憑證註冊工作委託註冊中心時，應於憑證實務作業基準或與註冊中心之契約或協議中載明註冊中心之責任。

9.6.2 註冊中心之聲明及擔保

註冊中心必須聲明及擔保以下責任：

(1)提供憑證申請服務。

(2)對憑證申請進行識別及鑑別。

(3)告知用戶關於憑證機構、註冊中心的義務與責任。

(4)告知用戶於取得或使用憑證機構所簽發之憑證，應遵守憑證政策及憑證實務作業基準之相關規定。

(5)執行憑證註冊審驗人員之識別與鑑別程序。

(6)管理註冊中心之私密金鑰。

(7)因執行註冊工作所引發之法律責任。

9.6.3 用戶之聲明及擔保

用戶應聲明及擔保以下之責任：

(1)安全地產製其私密金鑰並避免遭受破解。

(2)提供憑證機構與註冊中心正確與完整的資訊。

(3)遵守第 3 及第 4 章規定程序。

(4)於使用憑證前確認憑證資料的正確性。

(5)妥善地保管及使用私密金鑰。(以保證等級測試級簽發之憑證不做規定)。

(6) 當私密金鑰被破解時，應立即通知憑證機構。(以保證等級測試級簽發之憑證不做規定)。

(7) 適當地停止使用憑證並通知憑證機構，包括(a)如果提供給憑證機構之資訊或是記載於憑證中的資訊已經變更有可能誤導(b)有任何實際或懷疑的憑證所記載之公鑰其相對應的私密金鑰遭誤用或破解

(8) 正確地使用憑證，只使用於符合憑證實務作業基準與用戶接受條款的合法與經授權的使用目的，包含只安裝 SSL 憑證於憑證中所註記之完全吻合網域名稱的伺服器、不使用程式碼簽章憑證相對應之私密金鑰簽署惡意軟體。

(9) 於憑證到期後合宜地停止使用憑證與其對應之私密金鑰。

9.6.4 信賴憑證者之聲明及擔保

使用憑證機構簽發憑證的信賴憑證者應應承諾與擔保以下之責任：

(1) 熟知憑證之應用範圍及保證等級。

(2) 依憑證之適用範圍使用憑證。

(3) 正確檢驗數位簽章。

(4) 正確查驗憑證機構廢止清冊、憑證廢止清冊或線上憑證狀態協定回應訊息以確認憑證是否有效。(以保證等級測試級簽發之憑證不做規定)

(5) 應確認憑證所記載之金鑰用途。

(6) 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信賴憑證者權益受損時，應自行承擔責任。

(7) 憑證機構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，不得以憑證機構無法正

常運作，作為抗辯他人之事由。

(8)接受使用憑證機構簽發之憑證時，即表示已了解同意有關憑證機構法律責任之條款，依照憑證實務作業基準所規定範圍使用憑證。

9.6.5 其他參與者之聲明及擔保

不做規定。

9.7 免責聲明

憑證機構得在憑證實務作業基準中載明否認聲明及其限制條件(Disclaimers and Limitations)，以排除不屬憑證機構責任之錯誤。但憑證機構不得將因自行疏忽所引起之後果列入排除條件中。

9.8 責任限制

憑證機構得在憑證實務作業基準中載明責任限制。

9.9 賠償

依據電子簽章法第十四條，「憑證機構對因其經營或提供認證服務之相關作業程序，致當事人受有損害，或致善意第三人因信賴該憑證而受有損害者，應負賠償責任。但能證明其行為無過失者，不在此限。憑證機構就憑證之使用範圍設有明確限制時，對逾越該使用範圍所生之損害，不負賠償責任。」。憑證機構之憑證實務作業基準應載明對用戶及信賴憑證者的賠償責任，例如：

(1)於用戶約定協議要求用戶因於憑證申請時之虛假或欺詐的陳述，造成憑證機構簽發了不正確的憑證之損失的賠償條款。

(2)於信賴憑證者約定協議要求信賴憑證者若使用憑證時沒有適

當檢查憑證廢止資訊或逾越憑證機構憑證之使用範圍，造成憑證機構之損害或損失的賠償條款。

9.10 本文件之生效與終止

9.10.1 生效

本憑證政策於 eCA 儲存庫公布後即生效。

9.10.2 終止

本憑證政策新版本經政策管理委員會核定後公布，現有版本即告終止。

9.10.3 終止與保留之效力

本憑證政策之效力，維持至遵循本憑證政策所簽發之最後一張憑證到期或廢止為止。

9.11 主要成員之個別告知及溝通

本公司接受對於有關憑證政策之意見以安全電子郵件或書面告知(notice) ，透過本憑證政策第 1.5.2 節之聯絡資料可將這些意見送至 eCA。告知在發文者收到有效(使用數位簽章)之回執時才有效，如果回執在 5 天內沒有收到，可改採書面以快遞或掛號方式執行。

憑證機構可在其憑證實務作業基準中敘明對主要成員之個別告知及溝通的方式，如組織架構有重大變更時。

9.12 修訂

9.12.1 修訂程序

政策管理委員會至少每年應檢視本憑證政策 1 次，憑證機構至少每年應檢視憑證實務作業基準 1 次，以維持其保證度。

9.12.2 通知之機制及期限

對用戶可能產生重大影響之變更項目，憑證機構應公告於儲存庫，並於憑證實務作業基準敘明變更項目通知機制及公告期限。

9.12.3 物件識別碼必須更改之情況

憑證政策的修改不影響憑證政策所聲明的憑證使用目的與保證度時，憑證政策之物件識別碼不需修改，憑證政策之物件識別碼變更，憑證實務作業基準應作相對應之變更。

9.13 爭議解決條款

當對憑證政策內容之解釋有爭議時，爭議之雙方應儘量自行協商以取得共識。若協商不成，可向本公司另請求解釋。憑證機構應在憑證實務作業基準中敘明爭議之解決條款。

9.14 管轄法律

牽涉本基礎建設所簽發之憑證的任何爭議由中華民國相關法律規定管轄。

9.15 適用法律

依據憑證政策所進行之所有憑證機構之操作，必須遵循中華民國相關法律及規定。

9.16 雜項條款

9.16.1 完整協議

本憑證政策所約定者，係主要成員(如第 1.3 節所述)間最終且完整的約定。

憑證機構應透過合約或協議賦予註冊中心符合憑證政策和可適用的業界標準與指引。憑證機構應透過協議要求用戶及信賴憑證者依照協議內容使用產品或服務。

9.16.2 轉讓

本憑證政策所敘述的主要成員之間的權利或責任，不能在未通知本公司就以任何形式轉讓給其他方。

9.16.3 可分割性

如本憑證政策的任一章節不正確或無效時，其他章節仍然有效。

本憑證政策遵循 Baseline Requirements 對憑證機構之要求，惟 Baseline Requirements 之相關規定若與本憑證政策所依循之本國相關法律或法規產生衝突時，本憑證政策得調整相關作法以滿足法律或法規之要求，並將變更調整之部分通知憑證機構與瀏覽器論壇；若本國法律或法規已不再適用時，或憑證機構與瀏覽器論壇修訂 Baseline Requirement 之相關內容使其規定可相容於本國法律時，則本憑證政策將刪除並修訂原先所調整之內容，上述作業須於 90 天內完成。

9.16.4 契約履行

因可歸責於用戶或信賴憑證者之故意或過失違反本憑證政策相關規定，致總管理中心受有損害時，總管理中心除得請求損害賠償以外，並得向可歸責之一方請求支付為處理該爭議或訴訟之律師費用。總管理中心未向違反本憑證政策相關規定者主張權利，不代表總管理中心對於其繼續或未來違反本憑證政策情事，有拋棄權利主張之意思。

9.16.5 不可抗力

因不可抗力或其他非可歸責於憑證機構之事由致用戶或信賴憑證者受有損害，包含因天然災害、戰爭、恐怖攻擊等致電信網路中斷

之事件，憑證機構不負任何法律責任。憑證機構得在憑證實務作業基準中載明其他除外條款，但憑證機構不得將因自行疏忽所引起之錯誤列入排除條件中。

9.17 其他條款

不做規定。

附錄 1：縮寫

英文縮寫	英文全稱	中文名詞或定義
AAL	Authenticator Assurance Level	認證符記保證等級
AATL	Adobe Approved Trust List	Adobe 認可信賴清單
AIA	Authority Infomation Access	憑證機構資訊存取，參見附錄 2。
CA	Certification Authority	憑證機構，參見附錄 2。
CAA	Certification Authority Authorization	授權憑證機構簽發憑證，參見附錄 2。
CCA	Cross Certification Agreement	交互認證協議書，參見附錄 2。
CMMI	Capability Maturity Model Integration	能力成熟度模型，參見附錄 2。
CP	Certificate Policy	憑證政策，參見附錄 2。
CPS	Certification Practice Statement	憑證實務作業基準，參見附錄 2。
CRL	Certificate Revocation List	憑證廢止清冊，參見附錄 2。
CT	Certificate Transparency	憑證透明化，參見附錄 2。
DN	Distinguished Name	唯一識別名稱。
DNS	Domain Name System	網域名稱系統。
DV	Domain Validation	網域驗證，參見附錄 2。
eCA	ePKI Root Certification Authority	中華電信憑證總管理中心，參見附錄 2。
EE	End Entities	終端個體，參見附錄 2。
ePKI	Chunghwa Telecom ecommerce Public Key Infrastructure	中華電信公開金鑰基礎建設，參見附錄 2。
FIPS	(US Government) Federal	(美國)聯邦資訊處理標

英文縮寫	英文全稱	中文名詞或定義
	Information Processing Standard	準，參見附錄 2。
IANA	Internet Assigned Numbers Authority	網路通訊協定註冊中心，參見附錄 2。
IETF	Internet Engineering Task Force	網際網路工程任務小組，參見附錄 2。
IV	Individual Validation	個人驗證，參見附錄 2。
NIST	(US Government) National Institute of Standards and Technology	(美國)國家標準和技術研究院，參見附錄 2。
OCSP	Online Certificate Status Protocol	線上憑證狀態協定。
OID	Object Identifier	物件識別碼，參見附錄 2。
OV	Organization Validation	組織驗證，參見附錄 2。
PIN	Personal Identification Number	個人識別碼。
PKCS	Public Key Cryptography Standards	公開金鑰密碼學標準，參見附錄 2。
RA	Registration Authority	註冊中心，參見附錄 2。
RFC	Request for Comments	徵求修正意見書，參見附錄 2。
SSL	Secure Sockets Layer	安全插座層，參見附錄 2。
TLS	Transport Layer Security	傳輸層安全，參見附錄 2。
UPS	Uninterrupted Power System	不斷電系統，參見附錄 2。

附錄 2：名詞定義

中/英文名詞	定義
存取(Access)	運用系統資源處理資訊的能力。
存取控制 (Access Control)	對於授權的使用者、程式、程序或其他系統給予資訊系統資源存取權限的處理過程。
啟動資料 (Activation Data)	在存取密碼模組時(例如用來開啟私密金鑰以進行簽章或解密)，除金鑰外所需的隱密資料。
申請者(Applicant)	向憑證機構申請憑證，而尚未完成憑證簽發作業程序的用戶。
歸檔(Archive)	實體上(與主要資料存放處)分隔的長期資料儲存處，可用來支援稽核服務、可用性服務或完整性服務等用途。
保證(Assurance)	據以信賴該個體已符合特定安全要件之基礎。[憑證實務作業基準應載明事項準則第 1 章第 2 條第 1 項]
保證等級(Assurance Level)	具相對性保證層級中之某 1 級數。[憑證實務作業基準應載明事項準則第 1 章第 2 條第 2 項]
稽核(Audit)	評估系統控制的是否恰當、確保符合既定的政策及營運程序、並對現有的控制、政策及程序建議必要的改善而進行的獨立檢閱及調查。
稽核紀錄 (Audit Data)	依照發生時間順序之系統活動紀錄，可用以重建或調查事件發生的順序及某個事件中的變化。
鑑別(Authenticate)	當某個體出示身分時，確認其身分之正確性。
鑑別程序 (Authentication)	(1) 建立使用者到資訊系統身分信賴程度的程序。[NIST.SP.800-63-2 Electronic Authentication Guideline]

中/英文名詞	定義
	(2)用以建立資料傳送、訊息、來源者之安全措施，或是驗證個人接收特定種類資訊權限之方法。 (3)鑑別是身分的證明程序。[A Guide to Understanding Identification and Authentication in Trusted Systems] 而所謂的相互鑑別(Mutual Authentication)是指發生在進行通訊活動的兩方彼此進行鑑別。
憑證機構資訊存取(Authority Infomation Access, AIA)	記載有關存取憑證機構資訊的擴充欄位，內容可包含：線上憑證狀態查詢協定(OCSP)的服務位址，以及簽發憑證機構之憑證驗證路徑的下載位址等。微軟之視窗作業系統中文版將此名詞翻譯為授權存取資訊。
備份(Backup)	將資料或程式複製，必要時可供復原之用。
連結、繫結(Binding)	將兩個相關的資訊元素做連結(結合)的過程。
生物特徵值(Biometric)	人的身體或行為的特徵。
憑證機構憑證(CA Certificate)	簽發給憑證機構的憑證。
能力成熟度模型(Capability Maturity Model Integration, CMMI)	由美國卡內基美隆大學(Carnegie Mellon University)的軟體工程研究所(Software Engineering Institute)自 CMM 之後提出的修訂版本。CMMI 模型能為開發或改進用於達成一個組織的商業目標的過程提供指導，其目的是協助提升組織的績效。
憑證(Certificate)	(1)指載有簽章驗證資料，用以確認簽署人身分、資格之電子形式證明。[電子簽章法第 2 條第 6 款] (2)資訊之數位呈現，內容包括： A. 簽發的憑證機構。 B. 用戶之名稱或身分。

中/英文名詞	定義
	C. 用戶的公開金鑰。 D. 憑證之有效期間。 E. 簽發憑證機構之數位簽章。 在本憑證政策中所提及的“憑證”特別指其格式為 X.509 v.3，且在其“憑證政策”欄位中明確地引用本憑證政策之物件識別碼的憑證。
憑證遞件核准者 (Certificate Approver)	憑證遞件核准者應為自然人，屬申請人、申請人所聘雇之員工，或有權代表申請人進行意思表示之授權代理人：(i)擔任憑證請求者和授權其他員工或第三方擔任憑證請求者(ii)核准其他憑證請求者所提交之 SSL 伺服器憑證申請。
憑證機構 (Certification Authority, CA)	(1) 簽發憑證之機關、法人。[電子簽章法第 2 條第 5 款] (2) 為使用者所信任之權威機構，其業務為簽發並管理 ITU-T X.509 格式之公開金鑰憑證及憑證機構廢止清冊或憑證廢止清冊。
授權憑證機構簽發憑證 (Certification Authority Authorization, CAA)	CAA 網域名稱系統資源紀錄(DNS Resource Record)允許網域名稱系統之網域名擁有者指定憑證機構(一個或多個)取得授權幫該網域簽發憑證。發布 CAA 資源紀錄允許公眾信賴之憑證機構實施額外之控制，降低非預期之憑證誤發的風險。[RFC 6844]
憑證政策 (Certificate Policy, CP)	(1) 某 1 憑證所適用之對象或情況所列舉之 1 套規則，該對象或情況可為特定之社群或具共同安全需求之應用。[憑證實務作業基準應載明事項準則第 1 章第 2 條第 3 項] (2) 憑證政策係為透過憑證管理執行的電子交易所訂定之具專門格式的管理政策。憑證政策中包括與數位憑證相關之生成、產製、傳送、稽核、被破解後的復原以及其管理等各項議題。憑證政策亦可間接地控制運

中/英文名詞	定義
	用憑證之安全系統，以保護通訊系統所進行的交易。藉由控制關鍵的憑證擴充欄位方式，憑證政策及其相關技術可提供特定應用所需的安全服務。
憑證實務作業基準 (Certification Practice Statement, CPS)	(1) 由憑證機構對外公告，用以陳述憑證機構據以簽發憑證及處理其他認證業務之作業準則。[電子簽章法第 2 條第 7 款] (2) 宣告某憑證機構對憑證之作業程序(包括簽發、停用、廢止、展期及金鑰更換等)符合特定需求(載明於憑證政策或其他服務契約中)之聲明。
憑證廢止清冊 (Certificate Revocation List, CRL)	(1) 由憑證機構以數位方式簽署之已廢止憑證清冊。[憑證實務作業基準應載明事項準則第 1 章第 2 條第 8 項] (2) 由憑證機構維護之清單，清單中記載由此憑證機構所簽發且在到期日之前被廢止之憑證。
憑證透明化(Certificate Transparency, CT)	憑證透明化機制為一個公開監控與稽核網際網路上所有憑證的開放性架構(現階段以 SSL 憑證為優先目標)，透過公開憑證的簽發與存在等資訊給網域所有者、CA 憑證機構、以及網域使用者，供其判斷憑證是否被錯誤或惡意簽發；換言之，其目的係提供一個可用於監控 TLS/SSL 憑證機制與審核特定 TLS/SSL 憑證的公開監控與資訊公開的環境，以遏止憑證相關威脅。憑證透明化機制，主要由憑證日誌、憑證監控者、以及憑證稽核者等三個要素所組成。
破解 (Compromise)	資訊洩漏給未經授權的人士或違反資訊安全政策造成物件未經授權蓄意、非蓄意的洩漏、修改、毀壞或遺失。
機密性 (Confidentiality)	資訊不會遭受未經授權的個體或程序獲知或取用。

中/英文名詞	定義
合約簽署者(Contract Signer)	申請人、申請人所聘雇之員工，或有權代表申請人進行意思表示之授權代理人，或有權代表申請人簽署購買協議的自然人。
交互憑證 (Cross-Certificate)	在兩個憑證總管理中心(Root CA)之間建立信賴關係的 1 種憑證，屬於 1 種憑證機構憑證 (CA Certificate)，而非用戶憑證。
交互認證協議書(Cross Certification Agreement, CCA)	總管理中心與交互認證憑證機構就交互憑證機構申請加入本公開金鑰基礎建設所必須遵守之事項及個別責任義務歸屬的協議。
密碼模組 (Cryptographic Module)	1 組硬體、軟體、韌體或前述的組合，用以執行密碼的邏輯或程序(包含密碼演算法)，並且被包含在此模組的密碼邊界之內。
資料完整性(Data Integrity)	保證資料從產製到被接受都未遭竄改。
網域名稱(Domain Name)	在網域名稱系統分配給一個節點(node)的標籤(label)。亦即轉換 IP 位址為人類容易記憶之文字名稱。
網域名稱系統(Domain Name System, DNS)	將網域名稱轉換為 IP 位址的網路服務。
網域驗證(Domain Validation, DV)	SSL 憑證之核發，鑑別用戶之網域控制權但並未鑑別用戶之組織或個人身分。故連結安裝網域驗證型 SSL 憑證之網站，可提供 TLS 加密通道，但無法知道該網站之擁有者是誰。
數位簽章 (Digital Signature)	將電子文件以數學演算法或其他方式運算為一定長度之數位資料，以簽署人之私密金鑰對其加密，形成電子簽章，並得以公開金鑰加以驗證者。[電子簽章法第 2 條第 3 款]
憑證效期(Duration)	1 憑證欄位，由“有效期限起始時間”(notBefore) 及 “有效期限截止時間”(notAfter)兩個子欄位所組成。
電子商務 (E-commerce)	使用網路科技(特別是網際網路)以提供買賣貨物及相關服務。

中/英文名詞	定義
終端個體 (End Entity)	在本基礎建設中包括以下兩類個體： (1) 負責保管及應用憑證的私密金鑰擁有者。 (2) 信賴本基礎建設憑證機構所簽發憑證的第三者(不是私密金鑰擁有者，也不是憑證機構)，亦即終端個體為用戶及信賴憑證者，包括人員、組織、客戶(Account)、裝置或站台(Site)。
中華電信公開金鑰基礎建設(Chunghwa Telecom ecommerce Public Key Infrastructure, ePKI)	中華電信股份有限公司為推動電子化政策，健全電子商務基礎環境，依照 ITU-T X.509 標準建置的階層式公開金鑰基礎建設，可適用於電子商務與電子化政府的各項應用。
中華電信憑證政策管理委員會(Chunghwa Telecom Certificate Policy Management Authority，簡稱政策管理委員會)	1 組織，其設立目的為：研議本基礎建設憑證政策及電子憑證體系架構、審核下屬憑證機構與交互證認證憑證機構的互運申請及其他如審議憑證實務作業基準等電子憑證管理事項。
中華電信憑證總管理中心(ePKI Root CA, eCA)	中華電信公開金鑰基礎建設的根憑證機構(Root Certification Authority, Root CA)，在此階層式公開金鑰基礎建設架構中屬於最頂層的憑證機構，其公開金鑰為信賴之起源。
聯邦資訊處理標準 (Federal Information Processing Standard, FIPS)	為美國聯邦政府制定除軍事機構外，所有政府機構及政府承包商所引用之資訊處理標準。其中密碼模組安全需求標準為 FIPS 第 140 號標準(簡稱 FIPS 140)，FIPS 140-2 將密碼模組區分為 11 類安全需求，每一個安全需求類別再分成 4 個安全等級。
防火牆 (Firewall)	符合近端(區域)安全政策而對網路之間做接取限制的閘道器。
完全吻合網域名稱 (Fully Qualified Domain Name, FQDN)	1 種用於指定電腦在網域階層中確切位置的明確網域名稱。完全吻合網域名稱包含主機名稱(服務名稱)與網域名稱兩部分。例如 ourserver.ourdomain.com.tw。ourserver 是主機

中/英文名詞	定義
	名稱，ourdomain.com.tw 是網域名稱，其中 ourdomain 是第 3 層網域名稱，. com 則是次級網域名稱(Second-Level Domain)，.tw 則是國碼頂級網域名稱(Country Code Top-Level Domain, ccTLD)。完全吻合網域名稱的開頭一定是主機名稱。
個人驗證(Individual Validation, IV)	SSL 憑證核發過程中，除了識別與鑑別自然人用戶之網域控制權外並且依照憑證的保證等級識別與鑑別用戶之個人身分。故連結安裝個人驗證型 SSL 憑證之網站，可提供 TLS 加密通道，知道該網站之擁有者是那一個人並確保傳遞資料之完整性。
完整性 (Integrity)	對資訊的保護，使其不受未經授權的修改或破壞。資訊從來源產製後，經傳送、儲存到最終被收受方接收的期間中都維持不被篡改的一種狀態。
網際網路工程任務小組 (Internet Engineering Task Force, IETF)	負責網際網路標準的開發和推動之組織，包含網際網路架構及操作，使得網際網路運作更順暢，官方網站位於 https://www.ietf.org/。
金鑰託管 (Key Escrow)	將用戶的私密金鑰及依據用戶必須遵守的託管協議(或類似的契約)所規定的相關資訊進行存放，此託管協議的條款要求 1 個或 1 個以上的代理機構基於有益於用戶、雇主或另一方的前提下，依據協議的規定，擁有用戶的金鑰。
金鑰對(Key Pair)	兩把數學上有相關性的金鑰，具有下列特性： (1) 其中 1 把金鑰用來做訊息加密，而此加密訊息只有用成對關係的另 1 把金鑰可以解密。 (2) 從其中 1 把金鑰要推出另 1 把金鑰(從計算的角度而言)是不可行的。
網際網路號碼分配機構 (Internet Assigned	負責管理國際網際網路中使用的 IP 位址、網域名稱和許多其它參數之組織。

中/英文名詞	定義
Numbers Authority, IANA)	
簽發憑證機構(Issuing CA)	對於 1 張憑證而言，簽發該憑證的憑證機構即稱為該憑證的簽發憑證機構。
命名機構(Naming Authority)	負責指定唯一識別名稱並確保每個唯一識別名稱有意義且在其領域內為唯一的權責單位。
美國國家標準和技術研究院(National Institute of Standards and Technology, NIST)	官方網站在 http://www.nist.gov/，類似我國的經濟部國家標準檢驗局，其使命係促進美國的創新和產業競爭力，推動度量衡學、標準、技術以提高經濟安全並改善生活品質。其所制訂之硬體密碼模組標準及驗證、金鑰安全評估報告或聯邦政府的公務員和承包商身分卡標準廣泛被參考或引用。
不可否認性(Non-Repudiation)	對資料傳送方提供傳送證明以及對資料收受方提供傳送方的身分之保證，因而兩方在事後皆無法否認曾經處理過此項資料。技術上的不可否認性是指對信賴憑證者而言，如果某個公開金鑰可用以驗核某個數位簽章，保證此簽章必定是由相對應的私密金鑰所簽署。在法律上，不可否認性是指建立私密簽章金鑰之擁有或控管機制。
物件識別碼(Object Identifier, OID)	(1) 1 種以字母或數字組成之唯一識別碼，該識別碼必須依國際標準組織所訂定之註冊標準加以註冊，並可被用以識別唯一與之對應之憑證政策；憑證政策修訂時，其物件識別碼不必然隨之變更。[憑證實務作業基準應載明事項準則第 1 章第 2 條第 4 項] (2) 向國際認可之標準機構(ISO)註冊的特別形式的數碼，當提及某物件或物件類別時，可以引用此唯一的數碼做辨識。例如在公開金鑰基礎架構中，可以此數碼來指明使用的憑證政策及使用的密碼演算法。
線上憑證狀態查詢協定	線上憑證狀態查詢協定(Online Certificate

中/英文名詞	定義
(Online Certificate Status Protocol, OCSP)	Status Protocol)是一種線上憑證檢查協定，使信賴憑證者應用軟體可決定某張憑證之狀態(例如已廢止、有效等)。
特殊安全管道 (Out-of-Band)	不同於現有之線上通訊方式，例如使用實體掛號信與他人進行通訊，此一方式可視為一種特殊安全管道。
組織驗證(Organization Validation, OV)	SSL 憑證核發過程中,除了識別與鑑別用戶之網域控制權外並且依照憑證的保證等級識別與鑑別用戶之組織或個人身分。故連結安裝組織驗證型 SSL 憑證之網站，可提供 TLS 加密通道，知道該網站之擁有者是誰並確保傳遞資料之完整性。
私密金鑰(Private Key)	(1) 在簽章金鑰對中，用以產生數位簽章的金鑰。 (2) 在加解密金鑰對中，用以對機密資訊解密的金鑰。 在這兩種情境中，此金鑰皆須保密。
公開金鑰(Public Key)	(1) 在簽章金鑰對中，用以驗證數位簽章有效的金鑰。 (2) 在加解密金鑰對中，用以對機密資訊加密的金鑰。 在這兩種情境中，此金鑰皆須(一般以數位憑證的形式)公開可得。
公開金鑰密碼學標準 (Public Key Cryptography Standards, PKCS)	RSA 資訊安全公司旗下的 RSA 實驗室為促進公開金鑰技術的使用，所發展一系列的公開金鑰密碼編譯標準，廣為業界採用。
公開金鑰基礎建設 (Public Key Infrastructure, PKI)	由法律、政策、規範、人員、設備、設施、技術、流程、稽核和服務之集合，在廣泛尺度上發展與管理非對稱式密碼學及公鑰憑證。

中/英文名詞	定義
註冊中心 (Registration Authority, RA)	通常為憑證機構一部分之個體，負責對憑證的主體做身分識別及鑑別，但不做憑證簽發。
金鑰更換(Re-key (a certificate))	改變在密碼系統應用程式中所使用之金鑰之值。通常必須藉由對新的公開金鑰簽發新的憑證來達成。
信賴憑證者 (Relying Party)	指信賴所收受之憑證者。[憑證實務作業基準應載明事項準則第 1 章第 2 條第 6 項]
憑證展期(Renew (a certificate)	藉由簽發新的憑證，以延展公開金鑰憑證所連結資料有效性的程序。
儲存庫 (Repository)	(1) 用以儲存與檢索憑證或其他憑證相關資訊之可信賴系統(Trustworthy System)。[憑證實務作業基準應載明事項準則第 1 章第 2 條第 7 項] (2) 包含本憑證政策與憑證相關資訊的資料庫。
保留 IP 位址(Reserved IP Addresses)	IANA 設定為保留的 IPv4 或 IPv6 位址，參見 http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml 與 http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml
憑證廢止(Revoke a Certificate)	在憑證的有效期間內，提前終止憑證的運作。
徵求修正意見書 (Request for Comments,RFC)	由網際網路工程任務小組(IETF)發行的一系列備忘錄。包含網際網路、UNIX 和網際網路社群的規範、協定、流程等的標準檔案，以編號排定。
根憑證機構(Root Certification Authority, Root CA)	一個公開金鑰基礎建設中最頂層的憑證機構，除了簽發下屬 CA 憑證與自簽憑證外，其自簽憑證由應用軟體廠商負責散布，中文也有稱為憑證總管理中心或最頂層憑證機構。
安全插座層(Secure	網景公司(Netscape)推出 Web 瀏覽器時所提出

中/英文名詞	定義
Sockets Layer, SSL)	的協定，可於傳輸層對網路通信進行加密，並確保傳送資料之完整性以及對於伺服器端與用戶端進行身分鑑別。 安全插座層協定的優勢在於它與應用層協定獨立無關。高層的應用層協定(例如：HTTP、FTP、Telnet 等)能透通地建立於 SSL 協定之上。SSL 協定在應用層協定通信之前就已經完成加密演算法、通信密鑰的協商以及伺服器認證工作。此協定之繼任者是 TLS(Transport Layer Security)協定。
自發憑證(Self-Issued Certificate)	自發憑證為根憑證機構更換金鑰或憑證政策需要時所簽發之憑證，由兩代根憑證機構使用其私密金鑰相互簽發，用以建立新舊金鑰間或憑證政策互通憑證信賴路徑之用。
自簽憑證(Self-Signed Certificate)	自簽憑證係指憑證的簽發者名稱與憑證主體的名稱相同的一種憑證。亦即使用同一對金鑰對的私密金鑰針對其成配對關係的公開金鑰與其他資訊所簽發的憑證。 一個公開金鑰基礎建設內的自簽憑證，可做為憑證路信賴徑的起源，其簽發對象為總管理中心本身，內含總管理中心的公開金鑰，且憑證簽發者名稱與憑證主體名稱相同，可供信賴憑證者用於驗證總管理中心簽發之自發憑證、下屬憑證機構憑證、交互憑證以及憑證機構廢止清冊的數位簽章。
主體憑證機構(Subject CA)	對於 1 張憑證機構憑證(CA Certificate)而言，該憑證的憑證主體(Subject)所指的憑證機構即稱為該憑證的主體憑證機構。
下屬憑證機構(Subordinate CA)	在階層架構的公開金鑰基礎建設中，憑證由另 1 個憑證機構所簽發，且其活動受限於此另 1 憑證機構的憑證機構。
用戶(Subscriber)	具下列特性之個體，包括(但不限於)個人、機構、應用程式或網路裝置：

中/英文名詞	定義
	(a) 簽發憑證上所載明之主體。 (b) 擁有與憑證上所列公開金鑰對應之私密金鑰。 (c) 本身不簽發憑證給其他方。
威脅 (Threat)	對資訊系統可能造成損害(包括損毀、揭露、惡意修改資料或拒絕服務)的任何狀況或事件。可分為內部威脅(Internal Threat)與外部威脅(External Threat)。內部威脅是指利用授與之權限，可能透過資料的破壞、揭露、篡改或拒絕服務等方式造成對資訊系統的損害。外部威脅是指來自外部未經授權，且對資訊系統具有潛在破壞能力(包括對資料的毀壞、篡改、洩漏，或是造成阻斷服務)的個體。
時戳 (Time-stamp)	由可信賴的權威機構以數位方式簽署，證明某特定數位物件在某特別時間之存在。
傳輸層安全(Transport Layer Security, TLS)	由 IETF 將 SSL 3.0 協定制訂為 RFC 2246，並將其稱為 TLS 1.0 協定，後續於 RFC 5246 及 RFC 6176 更新版本，亦即 TLS 1.2 協定。2018 年 IETF 公告最新版本 RFC 8446，即 TLS 1.3 協定。
信賴清單 (Trust List)	可信賴憑證之清單，信賴憑證者用以鑑別憑證。
可信賴憑證 (Trusted Certificate)	為信賴憑證者所信賴且經由安全可靠之傳送方式取得的憑證。此類憑證中所包含的公開金鑰用於信賴路徑之起始，又稱為信賴起源。
不斷電系統 (Uninterrupted Power System, UPS)	在電力異常(如停電、干擾或電湧)的情況下 不間斷地提供負載設備後備電源，以維持諸如伺服器或交換機等關鍵設備或精密儀器的不間斷運作，防止運算數據遺失，通信網路中斷或儀器失去控制。
驗證(Validation)	憑證申請者的識別流程。驗證是識別(identification)的子集合，是指建立憑證申請

中/英文名詞	定義
	者的身分背景之識別。[RFC 3647]
WebTrust	加拿大會計師公會(Chartered Professional Accountants Canada, CPA Canada)針對憑證機構的 WebTrust Program 項目所制定的規範。加拿大會計師公會也是 WebTrust for CA 系列標章之管理單位。
零值化(Zeroize)	清除電子式儲存資料之方法，藉由改變資料儲存以防止資料被復原。