中華電信金融用戶憑證管理中心

憑證實務作業基準

(ChungHwa Telecom Financial User Certification Authority Certification Practice Statement of Chunghwa Telecom，CHT FUCA CPS)

版本 1.1

中華電信股份有限公司

中華民國 106 年 9 月 7 日

作業基準版本更新歷史紀錄

版本	日　期	發行單位	描　　述	備　註
1.0	101/7/10	中華電信	初版	
1.1	106/9/7	中華電信	修訂摘要、2.3.2財務保險、2.3.3 財務稽核、2.7 稽核方法、2.7.6 稽核結果公開之範圍、3.1.4 命名獨特性、4.7 金鑰更換、6.1.5 金鑰長度、6.6.3 生命週期安全評等、7.1 憑證格式剖繪及 7.2 憑證廢止清冊之格式剖繪等節，增訂 7.3 線上憑證狀態協定服務之格式剖繪、縮寫和定義、名詞解釋等節。	

目　錄

摘要 IX

1 總則 1

1.1 本作業基準適用範圍 1

1.2 版本識別 1

1.3 主要成員及憑證適用範圍 1

1.3.1 金融公開金鑰基礎建設 2

1.3.2 中華電信金融用戶憑證管理中心 2

1.3.3 憑證註冊中心(Registration Authority) 2

1.3.4 儲存庫(Repository) 2

1.3.5 憑證用戶(Subscribers)及信賴憑證者(Relying Parties) 3

1.3.6 適用範圍 4

1.4 聯絡方式 4

1.4.1 管理單位 4

1.4.2 聯絡資料 5

1.5 名詞定義和縮寫 5

2 一般條款 6

2.1 職責與義務 6

2.1.1 憑證管理中心之義務 6

2.1.2 憑證註冊中心之義務 6

2.1.3 憑證用戶之義務 7

2.1.4 憑證信賴憑證者之義務 8

2.1.5 儲存庫職責 8

2.2 法律賠償責任 8

2.2.1 憑證管理中心之責任 8

2.2.2 憑證註冊中心責任 10

2.2.3 憑證用戶之賠償責任 10

2.3 財務責任 11

2.3.1 財務保證 11
2.3.2 財務保險 11
2.3.3 財務稽核 11
2.4 準據法及爭議之解決 11
2.4.1 準據法 11
2.4.2 可分割性及存續、合併及公告通知 12
2.4.3 金融憑證之爭議解決 12
2.5 費用 12
2.5.1 憑證簽發或展期費用 12
2.5.2 憑證查詢費用 12
2.5.3 憑證廢止或狀態查詢費用 12
2.5.4 退費規定 13
2.6 公布及儲存庫 13
2.6.1 中華電信金融用戶憑證管理中心資訊公布內容 13
2.6.2 公布方法及頻率 13
2.6.3 存取控制 14
2.6.4 儲存庫 14
2.7 稽核方法 14
2.7.1 稽核頻率 14
2.7.2 稽核人員身分及資格 15
2.7.3 稽核人員及被稽核方之關係 15
2.7.4 稽核範圍 15
2.7.5 對於稽核結果之因應方式 15
2.7.6 稽核結果公開之範圍 16
2.8 資訊保密之範圍 16
2.8.1 機密之資訊種類 16
2.8.2 非機密之資訊種類 17
2.8.3 憑證廢止或暫時停用資訊之公開 17
2.8.4 應法定程序要求釋出資訊 17
2.8.5 應用戶要求釋出資訊 17
2.8.6 其他資訊釋出之情況 18
2.8.7 隱私權保護 18

2.9 智慧財產權 18
3識別和鑑別 19
3.1 初始註冊 19
3.1.1 命名種類 19
3.1.2 命名須有意義 19
3.1.3 命名形式之解釋規則 19
3.1.4 命名獨特性 19
3.1.5 命名爭議之解決程序 20
3.1.6 商標之辨識、鑑別及角色 21
3.1.7 憑證用戶證明擁有私密金鑰之方式 21
3.1.8 憑證用戶組織身分之鑑別 21
3.1.9 憑證用戶個人身分之鑑別 22
3.2 憑證之金鑰更新(REKEY)及展期(RENEW) 22
3.2.1 金融憑證更新金鑰 22
3.2.2 金融憑證展期 22
3.3 金融憑證廢止之金鑰更新 22
3.4 金融憑證廢止 23
3.5 金融憑證暫時停用與恢復使用 23
4營運規範 24
4.1 金融憑證申請程序 24
4.2 金融憑證簽發程序 24
4.3 金融憑證接受程序 25
4.4 憑證暫時停用及廢止 25
4.4.1 廢止憑證之事由 25
4.4.2 憑證廢止之申請者 26
4.4.3 憑證廢止之程序 26
4.4.4 憑證廢止申請之處理時間 27
4.4.5 暫時停用憑證之事由 27
4.4.6 暫時停用憑證之申請者 28
4.4.7 暫時停用憑證之程序 28

4.4.8 暫時停用憑證之時間 28
4.4.9 恢復使用憑證之程序 29
4.4.10 憑證廢止清冊簽發頻率 29
4.4.11 憑證廢止清冊檢核規定 29
4.4.12 線上憑證狀態協定查詢服務 30
4.4.13 線上憑證狀態協定查詢服務之規定 30
4.4.14 其他形式廢止公告 30
4.4.15 其他形式廢止公告之檢查規定 30
4.4.16 金鑰被破解時之其他特殊需求 30
4.5 安全稽核程序 30
4.5.1 被記錄事件種類 30
4.5.2 紀錄檔處理頻率 32
4.5.3 稽核紀錄檔保留期限 32
4.5.4 稽核紀錄檔之保護 32
4.5.5 稽核紀錄檔備份程序 33
4.5.6 安全稽核系統 33
4.5.7 引起事件者之公告 33
4.5.8 弱點評估 33
4.6 紀錄歸檔 33
4.6.1 紀錄事件之類型 34
4.6.2 歸檔之保留期限 35
4.6.3 歸檔之保護 35
4.6.4 歸檔備份程序 35
4.6.5 時戳紀錄之要求 35
4.6.6 歸檔資料彙整系統 35
4.6.7 取得及驗證歸檔資料之程序 36
4.7 金鑰更換 36
4.8 金鑰遭破解或災變時之復原程序 36
4.8.1 本管理中心電腦資源、軟體或資料遭破壞之復原程序36
4.8.2 本管理中心簽章金鑰憑證被廢止之復原程序 36
4.8.3 本管理中心簽章金鑰遭破解之復原程序 37
4.8.4 本管理中心安全設施之災害復原工作 37

4.9 本管理中心之終止服務 37
5 實體、程序及人員安全的控管 39
5.1 實體控管 39
5.1.1 實體所在及結構 39
5.1.2 實體存取 39
5.1.3 電源和空調 40
5.1.4 水災防範及保護 40
5.1.5 火災防範及保護 40
5.1.6 媒體儲存 40
5.1.7 廢料處理 40
5.1.8 異地備援 41
5.2 程序控制 41
5.2.1 信賴角色 41
5.2.2 角色分派 42
5.2.3 每個任務所需之人數 43
5.2.4 識別及鑑別每一個角色 44
5.3 人員控管 45
5.3.1 身家背景、資格、經驗及安全需求 45
5.3.2 身家背景檢核程序 45
5.3.3 教育訓練需求 46
5.3.4 再教育訓練需求及頻率 47
5.3.5 工作調換頻率及順序 47
5.3.6 未授權行動之制裁 47
5.3.7 聘雇人員之規定 48
5.3.8 提供給人員之文件資料 48
6 技術安全控管 49
6.1 金鑰對產製與安裝 49
6.1.1 金鑰對產製 49
6.1.2 將私密金鑰傳送給金融憑證用戶 49
6.1.3 將憑證用戶之公開金鑰傳送給憑證管理中心 49
6.1.4 將憑證管理中心之公開金鑰傳送給信賴憑證者 49

6.1.5 金鑰長度 50
6.1.6 公開金鑰參數產製 50
6.1.7 金鑰參數品質檢核 50
6.1.8 金鑰經軟體或硬體產製 50
6.1.9 金鑰之使用目的 50
6.2 私密金鑰保護 51
6.2.1 密碼模組標準 51
6.2.2 金鑰分持之多人控管 51
6.2.3 私密金鑰託管 51
6.2.4 金鑰備份 51
6.2.5 金鑰歸檔 51
6.2.6 私密金鑰輸入密碼模組 52
6.2.7 私密金鑰啟動方式 52
6.2.8 私密金鑰停用方式 52
6.2.9 私密金鑰銷毀方式 52
6.3 金鑰對管理之其他要點..... 53
6.3.1 公開金鑰之歸檔 53
6.3.2 公開金鑰及私密金鑰之使用期限 53
6.4 啟動資料 54
6.4.1 啟動資料的產生及安裝 54
6.4.2 啟動資料之保護 54
6.4.3 其他啟動資料之要點 55
6.5 電腦軟硬體安全管控措施..... 55
6.5.1 特定電腦安全技術需求 55
6.5.2 電腦安全評等 55
6.6 生命週期技術控管 55
6.6.1 系統研發控管措施 55
6.6.2 安全管理控管措施 56
6.6.3 生命週期安全評等 56
6.7 網路安全管控措施 56
6.8 密碼模組安全管控措施..... 56

7憑證及憑證廢止清冊之格式剖繪 57
7.1 憑證格式剖繪 57
7.1.1 版本序號 57
7.1.2 憑證擴充欄位 57
7.1.3 演算法物件識別碼 57
7.1.4 命名形式 57
7.1.5 命名限制 58
7.1.6 憑證政策物件識別碼 58
7.1.7 政策限制擴充欄位之使用 58
7.1.8 政策限定元的語法及語意 58
7.1.9 關鍵憑證政策擴充欄位之語意處理 58
7.2 憑證廢止清冊之格式剖繪..... 58
7.2.1 版本序號 58
7.2.2 憑證廢止清冊擴充欄位 58
7.3 線上憑證狀態協定之格式剖繪..... 58
7.3.1 版本序號 59
7.3.2 線上憑證狀態協定擴充欄位 59
7.3.3 線上憑證狀態協定服務運轉規範 60
8憑證實務作業基準之維護 61
8.1 變更程序 61
8.1.1 變更時不另作通知之變更項目 61
8.1.2 應通知之變更項目 61
8.2 公告及通知之規定 62
8.3 憑證實務作業基準之審定程序..... 62
附錄 1：縮寫和定義 63
附錄 2：名詞解釋 64

摘要

中華電信股份有限公司依據電子簽章法第十一條及經濟部頒訂之『憑證實務作業基準應載明事項準則』之規定，制定中華電信金融用戶憑證管理中心（以下簡稱本管理中心）憑證實務作業基準(以下簡稱本作業基準)。本作業基準之制定及修訂應經主管機關核定後，並公布於網站，始得提供簽發憑證服務。

一、主管機關核定文號：經商字第 10602418630 號

二、所簽發的憑證種類：

依據中華民國銀行公會制定之「金融公開金鑰基礎建設憑證政策」規範所簽發應用於金融交易之自然人或法人憑證，以下簡稱 FPKI 金融憑證。

三、憑證保證等級(Assurance Level)：

本管理中心之憑證保證等級係依據 FPKI 之憑證保證等級制訂。

四、應用範圍：

適用於開放式網路環境，針對資訊的傳遞提供加密及身分識別之用，業務範圍包括網路銀行、網路報稅、電子發票等金融相關交易。

本管理中心的用戶及相關信賴憑證者，必須謹慎的使用本管理中心所簽發之憑證，不得逾越本作業基準、相關法令規定及本管理中心與用戶及相關信賴憑證者之契約約定所限制及禁止的憑證應用範圍。

五、有關法律責任重要事項

1. 本管理中心及憑證註冊中心損害賠償責任

本管理中心或憑證註冊中心處理用戶憑證相關作業，若故意或過失未遵照本作業基準及相關作業規定，致用戶或信賴憑證者受有損害時，分別由本管理中心或憑證註冊中心負賠償責任。用戶得依與本管理中心或憑證註冊中心所訂契約相關約定，請求損害賠償；信賴憑證者得依相關法律規定，請求損害賠償。

2.本管理中心責任之免除

用戶或信賴憑證者如未依照本作業基準、相關法令規定及本管理中心與用戶及相關信賴憑證者之契約約定所引發之損害，或任何損害之發生，係不可歸責於本管理中心者，應由該用戶或信賴憑證者自負損害賠償之責。

3.憑證註冊中心責任之免除

如因可歸責於用戶之事由，導致信賴憑證者遭受損害時，或任何損害之發生，係不可歸責於憑證註冊中心時，應由用戶或信賴憑證者自負損害賠償之責。

用戶或信賴憑證者未依照本作業基準、相關法令規定及憑證註冊中心與用戶及相關信賴憑證者之契約約定所引發之損害，或任何損害之造成係不可歸責於憑證註冊中心時，應由該用戶或信賴憑證者自負損害賠償之責。

4.除外條款

如因不可抗力及其他非可歸責於本管理中心及憑證註冊中心之事由，所導致之損害，本管理中心及憑證註冊中心不負任何法律責任。本管理中心及憑證註冊中心就憑證之使用範圍已設有明確限制，對逾越該使用範圍所生之損害，不負任何法律責任。

如因本管理中心之系統維護、轉換及擴充等需要，得事先公告於儲存庫並通知憑證註冊中心，暫停部分憑證服務，

用戶或信賴憑證者不得以此作為要求本管理中心損害賠償之理由。

5.財務責任

本管理中心以中華電信股份有限公司為財務擔保；本管理中心財務依相關法律規定辦理財務稽核。

6.用戶責任

用戶應妥善保管及使用其私密金鑰(Private Key)。用戶之憑證如須暫停使用、廢止或辦理展期，應遵守本作業基準第4章規定辦理，但仍應承擔異動前所有使用該憑證之義務。

六、其他重要注意事項

1. 用戶應遵守本作業基準相關之規定，並確保所提供申請資料之正確性。

2. 信賴憑證者在合理信賴本管理中心所簽發之憑證時，應確認欲信賴憑證之正確性、有效性與用途限制。

3. 本公司將委託公正之第三人，就本管理中心的運作進行稽核。稽核採用的標準為 Trust Service Principles and Criteria for Certification Authorities。

4. 外部稽核結果以 WebTrust® for CA 標章之方式呈現於本管理中心網站首頁，點選標章後可閱覽外稽報告與管理聲明書。

5. 提供 FPKI 金融憑證服務之憑證註冊中心，僅限金融機構擔任。

1 總則

本文件的名稱為中華電信金融用戶憑證管理中心憑證實務作業基準(ChungHwa Telecom Financial User Certification Authority Certification Practice Statement of Chunghwa Telecom；以下簡稱為本作業基準)。

本管理中心由中華電信股份有限公司負責建置及營運，本管理中心為「銀行公會金融公開金鑰基礎建設(Financial Public Key Infrastructure，FPKI)」的用戶憑證管理中心(Financial User Cerfiicate Authority，FUCA)。

本管理中心所簽發應用於金融交易之自然人或法人憑證，以下簡稱 FPKI 金融憑證。

本作業基準有關金融憑證簽發及管理運作機制，係遵循中華民國銀行公會制定之「金融公開金鑰基礎建設憑證政策」(Certificate Policy for the Financial Public Key Infrastructure)所訂定。

1.1 本作業基準適用範圍

本作業基準所載明之實務作業規範適用於本管理中心、憑證註冊中心(Registration Authority)、憑證用戶(Subscribers)、信賴憑證者(Relying Parties)及儲存庫(Repository)等。

1.2 版本識別

本作業基準為第 1.1 版，版本發行日期為中華民國 106 年 9 月 7 日。本作業基準之最新版本可在以下網頁取得：

http://fca.hinet.net

本作業基準對應之「金融公開金鑰基礎建設憑證政策」物件識別碼(Object Identifier, OID)為：2.16.158.3.1.3.5。

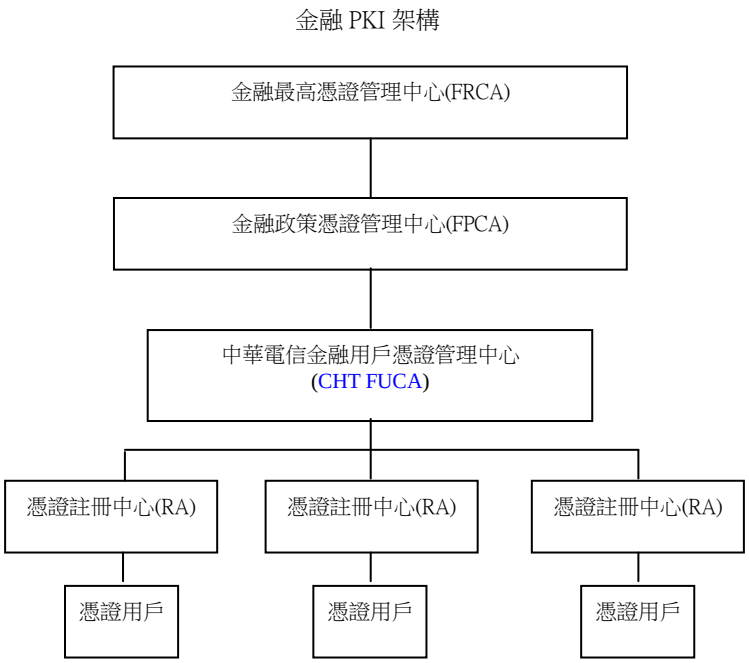
1.3 主要成員及憑證適用範圍

本管理中心由中華電信股份有限公司負責建置及營運，本管理中心為「銀行公會金融公開金鑰基礎建設(Financial Public Key Infrastructure，FPKI)」

的用戶憑證管理中心(Financial User Cerfiicate Authority，FUCA)。

1.3.1 金融公開金鑰基礎建設

「金融公開金鑰基礎建設」憑證管理中心架構圖示如下:



1.3.2 中華電信金融用戶憑證管理中心

中華電信金融用戶憑證管理中心，由中華電信股份有限公司負責建置及營運，依照「金融公開金鑰基礎建設憑證政策」之規定運作。

1.3.3 憑證註冊中心(Registration Authority)

憑證註冊中心是負責蒐集和驗證用戶的身分及憑證相關資訊之註冊工作。憑證註冊中心由多個註冊窗口（RA Counter）組成，由本管理中心授權核可之組織擔任，註冊窗口設有憑證註冊審驗人員（RA Officer，RAO），負責受理憑證申請、廢止等作業。

1.3.4 儲存庫(Repository)

本管理中心儲存庫是負責公告及儲存由本管理中心所簽發之憑證及憑證廢止清冊，提供憑證用戶及信賴憑證者查詢服務。儲存庫提供 24 小時全天的服務，

本管理中心儲存庫的網址為：http://fca.hinet.net。

1.3.5 憑證用戶(Subscribers)及信賴憑證者(Relying Parties)

1.3.5.1憑證用戶

憑證用戶指憑證中所命名或識別之主體，且其持有與憑證中所載公開金鑰(Public Key)相對應之私密金鑰(Private Key)者。憑證用戶可以是自然人或組織/法人。

憑證用戶與憑證主體之關係如下表所示：

憑證主體	憑證用戶	憑證類別
自然人	本人	FPKI 金融憑證
組織/法人	組織授權之委任人	FPKI 金融憑證

憑證用戶金鑰對(Key Pair)的產製應符合本作業基準6.1.1節之規定，並且憑證用戶必須獨自擁有控制憑證相對應私密金鑰的權力與能力。

1.3.5.2信賴憑證者

信賴憑證者係指相信憑證主體名稱與公開金鑰間連結(Binding)關係之第三人。信賴憑證者必須依照相對的憑證管理中心憑證及憑證狀態資訊，以驗證所使用憑證的有效性。在確認憑證的有效性後，才可使用憑證進行以下作業：

(1)驗證具有數位簽章(Digital Signature)的電子文件之完整性(Integrity)。

(2)驗證文件簽章產生者的身分。

(3)與用戶間建立安全之通訊管道。

1.3.6 適用範圍

1.3.6.1金融憑證適用範圍

憑證用戶為一般自然人或法人，憑證可使用範圍如下表所示，若有約定則從其約定。

憑證適用對象	憑證適用範圍
自然人、法人	適用於開放式網路環境，針對資訊的傳遞提供加密及身分識別之用，業務範圍包括網路銀行、網路報稅、電子發票等金融相關交易。

憑證用戶之身分驗證及鑑別依據 3.1.8 及 3.1.9 節規範執行，無不同層級的身分驗證及鑑別程序(Authentication)。

1.3.6.2金融憑證限制事項

憑證用戶及信賴憑證者皆應依本作業基準 1.3.6.1 節記載之適用範圍使用於適用之業務範圍內，並須遵循用途及交易之限制。

1.3.6.3憑證禁止事項

憑證用戶之憑證除使用於上述規定之範圍外，不得使用於會造成人體身心與精神之傷害、死亡或對社會秩序與社會環境有重大危害之應用或業務，且不得使用於電子簽章法與相關法令規範、主管機關及銀行公會明訂禁止之應用或業務。

1.4 聯絡方式

1.4.1 管理單位

本作業基準之訂定、更新及發布之管理機關為中華電信股份有限公司。本公司依據 8.3 節規定辦理憑證實務作業基準之審定。

1.4.2 聯絡資料

對本作業基準有任何疑慮或用戶報告遺失金鑰等事件，可直接與本管理中心聯絡。

聯絡電話:0800-080-365。

郵遞地址：台北市信義路一段 21 號數據通信大樓 中華電信金融用戶憑證管理中心。

電子郵件信箱：caservice@cht.com.tw。

其他聯絡資料或聯絡資料有所更動，請上 http://fca.hinet.net 查詢。

1.5 名詞定義和縮寫

參見附錄 1 縮寫和定義與附錄 2 名詞解釋。

2 一般條款

2.1 職責與義務

2.1.1 憑證管理中心之義務

(1)訂定並公告憑證實務作業基準。

(2)公告憑證廢止清冊（Certificate Revocation List, CRL）的內容。

(3)簽發、管理、遞送與廢止用戶之憑證。

(4)公告、管理憑證作業程序與驗證的作業規範。

(5)本管理中心遞送的用戶憑證，必須提供用戶憑證適時更新的機制。

(6)依據憑證實務作業基準之規範，執行相關之作業程序。

(7)管理與公告憑證廢止清冊與線上憑證狀態協定（Online Certificate Status Protocol，以下簡稱 OCSP）查詢服務資訊時的作業程序與身分驗證及訊息安全管控措施的作業規範。

(8)依據第 4 章及第 6 章規定提供相關控制。

2.1.2 憑證註冊中心之義務

提供 FPKI 金融憑證服務之憑證註冊中心僅限金融機構擔任，惟金融機構得委託其他單位代為處理憑證註冊中心之事務，但應就該單位之行為與自己之行為負同一之責任。

由於憑證註冊中心係代理憑證管理中心執行身分識別工作，於其引發的所有責任，憑證註冊中心應依其與本管理中心約定之權利義務而定。

憑證註冊中心之義務如下：

(1)負責確認憑證申請人之身分，但不負責簽發及管理憑證。

(2)管理與公告用戶註冊申請的作業程序與身分驗證的作業規範。

(3)驗證用戶憑證之簽發與廢止及查詢等申請訊息、身分合法性與訊息

正確性。

(4)遞送用戶的申請憑證、廢止憑證、查詢申請等訊息至憑證管理中心，並驗證回覆訊息的正確性後傳回用戶。

(5)管理、公告並提供用戶憑證查詢、廢止及憑證管理中心的憑證鏈。

(6)用戶申請或廢止、暫時停用等憑證作業時必須驗證用戶身分，用戶憑證相關申請訊息轉送至憑證管理中心時，必須驗證訊息的安全性與正確性

(7)憑證註冊中心與其作業人員必須善盡保管用戶資料及相關訊息之責任、避免相關資訊洩漏、被冒用、篡改及任意使用。

(8)憑證註冊中心與憑證相對應的私密金鑰有被冒用、曝露及遺失等不安全的顧慮時，或憑證內註冊中心相關的資訊有異動時，必須依相關作業的規定，即刻向本管理中心辦理申告與處理。

(9)為使金融機構能提供客戶完整的客戶服務，憑證相關作業一律需經過憑證註冊中心並留存相關資料於憑證註冊中心。

(10)憑證註冊中心應通知憑證即將到期的用戶辦理更新憑證作業。

2.1.3 憑證用戶之義務

(1)向憑證註冊中心申請憑證時，必須提供詳細且正確的身分證明文件與資料供憑證註冊中心審核。

(2)其憑證與憑證對應的私密金鑰使用的業務範圍，皆依本作業基準之規範，運用於相關業務上。

(3)合法且正確的使用私密金鑰與憑證，無任何違反相關法律的規定與侵害第三者的權利。

(4)用戶需確實且妥善安全的保護其私密金鑰，除本人外絕無其他人知悉與使用，私密金鑰有被冒用、曝露及遺失等不安全的顧慮時，即刻向憑證註冊中心辦理申告與處理。

(5)憑證內用戶相關的資訊有異動時，用戶必須依相關作業的規定，即刻向憑證註冊中心辦理申告與處理。

2.1.4 憑證信賴憑證者之義務

(1)必須了解且同意本作業基準與「金融公開金鑰基礎建設憑證政策」相關作業規範的規定，且依規範所訂定的業務範圍應用於相關的業務，無任何違反相關法律的規定與侵害第三者的權利。

(2)驗證憑證時必須由憑證鏈逐一驗證該憑證的正確性及有效性，也需利用憑證廢止清冊(CRL)或線上憑證狀態協定(OCSP)查詢服務，檢核此憑證是否為廢止或暫時停用憑證。

2.1.5 儲存庫職責

(1)依 2.6 節規定，應由憑證管理中心定期公布所簽發憑證、已廢止憑證、憑證廢止清冊至儲存庫。

(2)公布本作業基準的最新資訊。

(3)儲存庫之存取控制依照 2.6.3 節之規定。

(4)公布外部稽核（Audit）之結果。

(5)維持儲存庫資訊之可接取狀態及可用性。

(6)新簽發憑證用戶憑證或憑證廢止清冊時，提供用戶查詢最新的資訊，除系統維護的需求得暫時停止服務(上限 24 小時)外，每天 24 小時提供正常服務。

2.2 法律賠償責任

2.2.1 憑證管理中心之責任

本管理中心所提供之 FPKI 金融憑證服務作業項目與內容，皆訂定於本作業基準 1.3.6 節，FPKI 金融憑證用於非本作業基準所訂之內容，皆排除於賠償責任之外

如因本管理中心作業人員故意或過失，未依憑證實務作業基準及相關之規定，辦理憑證用戶之簽發、更新、暫時停用與廢止作業，或違反相關法律規範而造成憑證用戶之損失時，本管理中心應依規定賠償憑證用戶之直接損失；有關用戶單一 FPKI 金融憑證之最高賠償金額如下表所示，如用戶與本公司訂有合約，另行規範憑證使用範圍與交易賠償限額者，從其約定。

憑證用戶	賠償總金額上限 （新台幣:元）
自然人	1,000,000
法人	2,000,000

此賠償上限為對用戶單一 FPKI 金融憑證賠償金額之最高額度，亦即不論交易次數多寡，單一憑證之累積賠償金額均不得超過賠償限額。

(1)如非作業人員之故意或過失，造成網際網路傳輸的中斷或設備的故障或其他不可抗拒的天災事故(例如戰爭或地震等)，致所簽發之FPKI金融憑證造成憑證用戶損失時，本管理中心不負任何損害賠償責任。

(2)憑證用戶或其他有權者提出廢止憑證用戶憑證之要求後，至本管理中心實際完成廢止該憑證用戶憑證為止之期間內，當該憑證用戶憑證被用以進行非法交易，或進行交易後產生法律糾紛時，本管理中心如依據本作業基準與相關之作業規範執行處理作業時，則不負任何損害賠償責任。

(3)憑證用戶或其他有權者提出暫時停用憑證用戶之憑證要求後，至本管理中心實際完成暫時停用該憑證用戶憑證為止之期間內，當該憑證用戶憑證被用以進行非法交易，或進行交易後產生法律糾紛時，本管理中心如依據本作業基準與相關之作業規範執行處理作業時，則不負任何損害賠償責任。

(4)憑證用戶之賠償追究有效期限,依主管機關與相關法律之規範辦理。

2.2.2 憑證註冊中心責任

憑證註冊中心與其作業人員未善盡保管憑證用戶之註冊及FPKI金融憑證相關資料，而造成相關資訊洩漏、被冒用、篡改及任意使用致造成憑證用戶或信賴憑證者遭受損害時， 憑證註冊中心與該作業人員應依與憑證用戶合約之規定負損害賠償責任。

(1)憑證註冊中心如因作業人員故意或過失，未遵照本作業基準及憑證註冊中心相關作業規範的規定辦理註冊作業，或違反相關法律規範而造成憑證用戶的損失，或致信賴憑證者受有損失者，由憑證註冊中心負該損害賠償責任。

(2)憑證註冊中心因應用系統或軟體之錯誤，未能於本作業基準及憑證註冊中心作業規範所規定之作業時間內，將憑證用戶憑證申請、更新、暫時停用及廢止之請求訊息傳送至本管理中心處理，而導致憑證用戶或信賴憑證者之損失時,憑證註冊中心應負該損害賠償責任。

2.2.3 憑證用戶之賠償責任

(1)憑證用戶向憑證註冊中心申請註冊時，因故意、過失或不正當意圖而提供不實資料，致造成本管理中心或信賴憑證者遭受損害時，應由該憑證用戶負該損害賠償責任。

(2)憑證用戶應妥善保管其私密金鑰與密碼，不得洩漏或交付予他人使用，如因故意或過失，致造成本管理中心、憑證註冊中心或信賴憑證者遭受損害時，應由該憑證用戶負該損害賠償責任。

(3)憑證用戶使用FPKI金融憑證，有違反本作業基準及相關作業之規範，或FPKI金融憑證使用於非本作業基準規定之其他業務範圍時，該憑證用戶應自行負該損害賠償責任。

(4)憑證用戶或其他有權利者提出憑證廢止/暫時停用憑證申請後,至本管理中心實際完成廢止/暫時停用該憑證用戶之憑證期間,若憑證用戶之私密金鑰遭受冒用或進行非法交易後產生法律糾紛時，本管理中心已依據本作業基準之相關作業規範執行處理作業，則本管理中心不負憑證用戶及

信賴評者所遭受之連帶損害賠償責任。

(5)其他與業務相關之償責，訂定於業務相關之作業規範與憑證用戶之業務合約規範。

2.3 財務責任

2.3.1 財務保證

本管理中心由中華電信股份有限公司營運，其財務責任由中華電信股份有限公司負責，每年定期委由公正第三方作財務稽核。

2.3.2 財務保險

本公司已投保最高賠償金額為新台幣 120,000,000 元的一般責任險，並會遵循憑證業務主管機關之財務保險規範。

2.3.3 財務稽核

本管理中心之財務，係屬中華電信股份有限公司整體財務之一部。中華電信股份有限公司為股票上市公司，依證券交易法第 36 條之規定，應於每營業年度終了後 3 個月內公告，並向主管機關申報，經會計師查核簽證，董事會通過及監察人承認之年度財務報告。並於每會計年度第 1 季、第 2 季及第 3 季終了後 45 日內，公告並申報經會計師核閱及提報董事會之財務報告。於每月 10 日以前，公告並申報上月份營運情形。本管理中心可提供自我擔保之資產價值依本公司年度財務報告為準。本公司的財務具備若發生損害時足夠的賠償能力，有關流動資產是否符合 CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates 之金額要求，且流動資產與流動負債比符合不低於1.0，可透過檢視會計師查核簽證之最新年度財務報告取得。

2.4 準據法及爭議之解決

2.4.1 準據法

本作業基準的執行、詮釋及效力皆以中華民國法律為準據法。

2.4.2 可分割性及存續、合併及公告通知

本作業基準的任何一節無效時，除去無效之該部分外，本作業基準的其他章節仍繼續維持其有效性，直到本作業基準修改為止，本作業基準的修改如第8章所述。

2.4.3 金融憑證之爭議解決

加入金融公開金鑰基礎建設之憑證管理中心、憑證註冊中心、所有用戶因FPKI 金融憑證服務發生爭議時，應秉持誠信原則協商解決之。若無法於爭議發生後14天內解決爭議，得經雙方同意由「銀行公會憑證政策管理委員會」協助解決雙方之爭議；若爭議發生後1個月內爭議仍未解決者，則除雙方另合意提交仲裁外，雙方合意以台灣台北地方法院為第一審管轄法院。

於爭議協商、訴訟處理過程所發生之費用分攤，依據協商或相關之法律規範處理。

如為跨國或跨區域之爭議處理，無法以上述之處理方式解決時，則必須依照相關之跨國或跨區域之糾紛仲裁規範處理。

2.5 費用

2.5.1 憑證簽發或展期費用

本管理中心與用戶之間的憑證申請、簽發、展期等計費架構，於相關業務契約條款中訂定。

2.5.2 憑證查詢費用

憑證查詢計費架構於相關業務契約條款中訂定。

2.5.3 憑證廢止或狀態查詢費用

用戶下載查詢憑證廢止清冊不收費；線上憑證狀態協定查詢服務計費架構依據「銀行公會憑證政策管理委員會」規定，於相關業務契約條款中訂定。

2.5.4 退費規定

本管理中心所收取之憑證簽發或展期收費， 如因本管理中心之過失致用戶憑證無法使用，經本管理中心查明後得予以重新簽發憑證， 若用戶不接受重新簽發憑證者，本管理中心依實際使用比例計算，退還用戶本項費用，詳細退費流程於相關業務契約條款中訂定。除前述情形及 4.9 節之情形外， 其他費用均不退費。

2.6 公布及儲存庫

2.6.1 中華電信金融用戶憑證管理中心資訊公布內容

(1)本作業基準。

(2)憑證廢止清冊。

(3)本管理中心本身之憑證(至與該憑證之公開金鑰相對應之私密金鑰所簽發的所有憑證效期到期為止)。

(4)簽發之所有憑證。

(5)隱私權保護政策。

(6)本管理中心相關最新訊息。

(7)憑證政策。

(8) 線上憑證狀態協定查詢服務。

2.6.2 公布方法及頻率

(1)本作業基準於主管機關核准後公布，本作業基準修訂依照第 8 章規定公布於儲存庫。

(2)本管理中心每天簽發 1 次憑證廢止清冊，公布於儲存庫。

(3)本管理中心本身之憑證，於簽發時公布於儲存庫。

(4)簽發之憑證，於簽發時公布於儲存庫。

2.6.3 存取控制

本管理中心主機建置於防火牆(Firewall)內部，外界無法直接連線，儲存庫透過內部的防火牆連線至本管理中心憑證管理資料庫，以擷取憑證資訊或下載憑證。只允許經過授權的本管理中心相關人員管理儲存庫主機。

有關 2.6.1 節本作業基準、本管理中心本身之憑證、隱私權保護政策及本管理中心相關最新訊息，主要提供用戶與信賴憑證者使用瀏覽器查詢之用，因此開放提供閱覽存取，並為保障儲存庫之安全應進行存取控制，且應維持其可接取狀態及可用性。

用戶憑證、憑證廢止清冊及線上憑證狀態協定查詢服務訂定適當之存取控制，以確保儲存庫之安全性。

2.6.4 儲存庫

儲存庫由本管理中心負責管理，除因故無法正常運作(上限 24 小時)外，每天 24 小時提供正常服務，儲存庫之網址為：http://fca.hinet.net。

2.7 稽核方法

本公司將委外辦理本管理中心之外部稽核作業，委託熟悉本管理中心運作並經 WebTrust for CA 標章管理單位授權可於中華民國執行 Trust Service Principles and Criteria for Certification Authorities 標準之合格會計師事務所，提供公正客觀的稽核服務。

外部稽核報告經由金融最高層憑證管理中心審核後送金融政策管理委員會核備，以確保其 FPKI 金融憑證服務之運作遵照本作業基準與銀行公會「金融公開金鑰基礎建設憑證政策」之規定。

2.7.1 稽核頻率

本管理中心接受 1 年至少 1 次的外部稽核與不定期的內部稽核，以確認本管理中心的運作確實遵循本作業基準所訂的安全規定與程序。

本管理中心必要時將接受「銀行公會憑證政策管理委員會」派員執行專案查核。

2.7.2 稽核人員身分及資格

執行外部稽核機構應具備資訊系統稽核師(Certified Information System Audit，CISA)及國際認證內部稽核師(CIA)資格或具同等資格之人員參與稽核工作，且具備 2 年以上之憑證管理中心稽核或資訊安全管理稽核相關經驗，本管理中心於稽核時應對稽核人員進行身分識別。

2.7.3 稽核人員及被稽核方之關係

本公司將委託公正之第三方，就本管理中心的運作進行稽核，稽核人員應獨立於本管理中心外，並遵循中華民國會計師公會職業道德規範公報第十號對於「正直、公正客觀及獨立性」之相關規範或相當之國際專業團體職業道德規範。

2.7.4 稽核範圍

稽核範圍如下所述：

(1)本作業基準是否符合憑證政策之規定。

(2)本管理中心是否遵照本作業基準運作，包括實體環境控管、人員程序控管、金鑰生命週期管理、憑證生命週期控管、硬體密碼模組控管等管理及技術稽核。

(3)確認憑證註冊中心是否遵照本作業基準及相關程序運作。

2.7.5 對於稽核結果之因應方式

如稽核人員發現本管理中心或憑證註冊中心之建置與維運不符合本作業基準規定時，採取以下行動：

(1)記錄不符合情形。

(2)將不符合情形通知本管理中心。

(3)對於不符合規定之項目，本管理中心將於 30 日內提出改善計畫，儘速執行，並列入後續稽核追蹤項目。有關憑證註冊中心之缺失將通知憑證註冊中心改善。

如本管理中心接獲外部稽核報告，未於限定時間內改善者，「銀行公會憑證政策管理委員會」得暫停本管理中心FPKI金融憑證的營運；發現重大缺失時，「銀行公會憑證政策管理委員會」亦得撤銷該本管理中心擔任金融用戶憑證管理中心之資格。

2.7.6 稽核結果公開之範圍

本管理中心將公布稽核者所提供之應公開說明資訊，並於儲存庫公布最近1次的稽核結果。稽核結果以 WebTrust® for CA 標章之方式呈現於本管理中心網站首頁，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應於查核區間結束後 3 個月內公布於儲存庫。若因故延遲公布最近 1 次稽核結果，本管理中心將提供合格稽核業者簽署之解釋函。

2.8 資訊保密之範圍

2.8.1 機密之資訊種類

本管理中心對於用戶於申請憑證時所提供的相關資訊，除用戶憑證內容可公開的資訊外，均視為機密資訊，並依據本管理中心的安全管控措施妥善的保護，除經由用戶的同意或法令之規定外，不得對外公開。

對於用戶機密資訊的保護，除符合本作業基準外，亦符合政府相關之規定(如個人資料保護法)。

本管理中心對於用戶機密性資訊的保護，非經由用戶的允許絕不以任意方式對外公開、銷售、租借。

本管理中心為憑證管理作業的需求而使用與存取用戶資訊時，將依照業務的需求與採取嚴謹的安全管控措施，由有權存取的作業人員執行。相關作業將留存稽核軌跡，以供查核之用。本管理中心及憑證註冊中心之現職及退職人員對於機密資訊均嚴守秘密。

以下由本管理中心或憑證註冊中心產生、接收或保管之資料，均視為機密資訊。

(1)營運相關的私密金鑰及通行碼(passphrase)。

(2)金鑰分持的保管資料。

(3)用戶之申請資料。

(4)產生或保管之可供稽核及追蹤之紀錄。

(5)稽核人員於稽核過程中產生之稽核紀錄及稽核發現。

(6)列為機密等級的營運相關文件。

2.8.2 非機密之資訊種類

(1)本管理中心儲存庫公布之憑證政策、本作業基準、本管理中心憑證及用戶憑證、已廢止憑證、憑證廢止清冊及憑證狀態(提供憑證有效性狀態查詢功能時)為可公開之非機密性資訊。

(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。

2.8.3 憑證廢止或暫時停用資訊之公開

用戶憑證廢止或暫時停用依據 4.4 節規範處理，憑證廢止或暫時停用資訊公布於本管理中心儲存庫。

2.8.4 應法定程序要求釋出資訊

司法機關、監察機關或治安機關如因下列之一之條件，必須查詢 2.8.1 節機密資訊時，依法定程序辦理：

(1)政府法律、規章之規定並經由權責管理單位合法之授權。

(2)法院處理因使用憑證產生的糾紛與仲裁而合法之申請需求。

否則憑證用戶之註冊基本資料與身分識別相關資料絕不任意提供予權責管理單位，或其他任何人知悉使用；惟本管理中心保留向申請查詢之機關收取合理費用之權利。

2.8.5 應用戶要求釋出資訊

用戶本人得使用電子簽章或親自簽名的證明文件授權查詢 2.8.1 節第(3)款之申請資料；惟本管理中心保留向申請查詢之用戶收取合理費用之權利。

2.8.6 其他資訊釋出之情況

本管理中心於操作中取得用戶之個人資料，將遵守相關法令規範，不對外揭露以確保用戶個人隱私。但法令另有規定時，不在此限。

2.8.7 隱私權保護

本管理中心依照個人資料保護法處理用戶申請資料。

2.9 智慧財產權

下列項目為本管理中心之智慧財產:

(1)因執行本管理中心憑證管理作業而撰寫的相關文件或研發之系統。

(2)本管理中心所簽發的憑證及憑證廢止清冊。

(3)本作業基準。

本公司同意本作業基準可由本管理中心儲存庫自由下載，或依著作權法相關規定重製或散布，但必須保證是完整複製，並註明著作權為中華電信股份有限公司所擁有。重製或散布本作業基準者，不得向他人收取費用，對於不當使用或散布本作業基準之侵害，本公司將依法予以追訴。

3 識別和鑑別

3.1 初始註冊

本管理中心簽發 FPKI 金融憑證，本管理中心及憑證註冊中心依據「金融公開金鑰基礎建設憑證政策」規定，建置與訂定符合安全管控措施的作業管理程序。對於憑證申請者(Applicant)的身分識別與驗證，選定適當的作業管理人員，以確實完成用戶的身分識別與驗證。

3.1.1 命名種類

本管理中心所簽發憑證之憑證主體名稱採用 X.500 唯一識別名稱(Distinguished Name， DN)，以確保憑證申請者識別名稱的明確與唯一性。

3.1.2 命名須有意義

本管理中心所簽發的憑證，其憑證申請者名稱符合我國法律對該主體命名之相關規定，以代表該主體的名稱。

憑證內容之簽發者(Issuer)與主體(Subject)的識別名稱所存放的內容，為具有意義的內容，且為可以唯一識別憑證簽發者與申請者身分的資訊，不可存放空白的資訊、或匿名、或不可辨識的識別名稱。

3.1.3 命名形式之解釋規則

名稱形式的解釋規則依據 ITU-T X.520 名稱屬性定義。

憑證用戶憑證識別名稱之命名規則使用 X.500 之命名規範，並依據銀行公會制訂的「金融 XML 憑證共通性技術規範」訂定詳細的命名規則。

3.1.4 命名獨特性

本管理中心第 3 代核發 FPKI 金融憑證使用的 X.500 唯一識別名稱為：

C=TW，

O=Chunghwa Telecom Co., Ltd.，

OU=Financial UCA

CN=UCA of Financial PKI

自第 4 代起核發 FPKI 金融憑證使用的 X.500 唯一識別名稱為：

C=TW，

O=Chunghwa Telecom Co., Ltd.，

OU=Financial UCA - Gn

CN =UCA of Financial PKI - Gn

其中,n=4,5…

本管理中心將採用 X.520 標準所定義的各種命名屬性加以組合以確保用戶憑證主體名稱在本管理中心所認知的 X.500 名稱空間內具備獨特性。本管理中心之用戶憑證主體名稱允許(但不限於)使用以下 X.520 標準所定義的各種命名屬性加以組合而成：

- countryName（縮寫為 C）
- organizationName（縮寫為 O）
- organizationalUnitName（縮寫為 OU）
- commonName（縮寫為 CN）

3.1.5 命名爭議之解決程序

當憑證用戶之憑證識別名稱相同時，以先申請之用戶優先使用，後申請者於註冊名稱後加區分欄位碼或流水號以資區別與識別不同的用戶。

相關之糾紛或仲裁處理，非本管理中心之權責範圍，由用戶向相關主管機關或法院提出申請。

憑證用戶之憑證識別名稱使用發生爭議時，仲裁機構為「銀行公會金融公開金鑰基礎建設政策管理委員會」。

當憑證用戶使用之憑證識別名稱，經相關主管機關或有權解釋機關證實為其他申請者擁有時，由該用戶負擔相關的法律權責，本管理中心得逕行廢止該用戶之憑證。

3.1.6 商標之辨識、鑑別及角色

憑證用戶提供之憑證主體名稱須符合我國商標法及公平交易法之相關規定，本管理中心不保證用戶註冊商標、商號、公司名稱、或其他特殊意義之名稱的認可、與驗證。本管理中心不可於明確已知曉的情況下，接受已為相關主管機關或司法機關禁止使用之用戶識別名稱或用戶註冊名稱與註冊商標；但本管理中心無驗證用戶註冊名稱與註冊商標的權責。

相關糾紛或仲裁處理非本管理中心權責範圍，由用戶依據一般行政或司法救濟途徑處理之。

3.1.7 憑證用戶證明擁有私密金鑰之方式

憑證用戶自行產生公開/私密金鑰對後，以公開金鑰向本管理中心申請用戶憑證的簽發時，用戶使用其私密金鑰對申請訊息簽署 PKCS#10 格式之數位簽章，當憑證管理中心驗證 PKCS#10 之數位簽章無誤後，即為確定用戶擁有此私密金鑰。

3.1.8 憑證用戶組織身分之鑑別

憑證註冊中心處理組織用戶的身分驗證時，將驗證組織名稱、所在地及代表人名稱等足以識別該組織之資料。憑證註冊中心除需驗證申請資料及代表人身分之合法性外，並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註冊中心辦理。

若憑證用戶無法親自臨櫃辦理，得以書面委託書委任代理人代為臨櫃申請，但憑證註冊中心必須確認該委託書之真偽，並依下述(個人身分之鑑別)規定驗證代理人身分。

如依司法或檢調機關之通知或依相關法律之規定逕行廢止憑證，憑證註冊中心需驗證該申請文件之合法性。

3.1.9 憑證用戶個人身分之鑑別

憑證註冊中心處理個人之用戶註冊的身分驗證時，需進行臨櫃身分驗證，並比對身分證明文件。若憑證用戶無法親自臨櫃辦理，得以書面委託書委任代理人代為臨櫃申請，但憑證註冊中心必須確認該委託書之真偽，並依上述規定驗證代理人身分。

3.2 憑證之金鑰更新(rekey)及展期(renew)

3.2.1 金融憑證更新金鑰

於 FPKI 金融憑證有效期限屆滿前，憑證註冊中心必須通知用戶執行憑證更新，而用戶重新產生新的公開金鑰，於舊有 FPKI 金融憑證尚未廢止或過期之前，使用已註冊的用戶資訊向本管理中心申請簽發用戶憑證。於舊有 FPKI 金融憑證尚未廢止或過期之前且新 FPKI 金融憑證簽發之交替期間，同一憑證主體名稱與同一 UNIQUE_ID（放置於憑證主體目錄屬性(SubjectDirectoryAttributes)延伸欄位）會擁有超過 1 張以上之憑證，新舊憑證其憑證序號與公開金鑰不同。

用戶 FPKI 金融憑證已廢止或有效期限已過期時，不可執行FPKI 金融憑證及私密金鑰的更新。

用戶每 9 年應重新進行註冊，重新註冊時之身分鑑別程序比照 3.1.8 或 3.1.9 節規定辦理。

本管理中心及憑證註冊中心對於用戶 FPKI 金融憑證及私密金鑰的更新，具有身分識別、驗證與資料完整性(Data Integrity)的安全管控措施。

3.2.2 金融憑證展期

FPKI 金融憑證不提供憑證展期服務。

3.3 金融憑證廢止之金鑰更新

FPKI 金融憑證用戶憑證已廢止後，不得執行FPKI 金融憑證及私密金鑰的更新，新憑證的簽發應依照3.1.8或3.1.9節規定，用戶必須重新辦理憑證申請作業。

3.4 金融憑證廢止

FPKI 金融憑證廢止申請之鑑別程序與 3.1.8 或 3.1.9 節規定相同，並依照 4.4 節規定辦理。無論私密金鑰是否遭破解(Compromise)，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。

3.5 金融憑證暫時停用與恢復使用

憑證用戶連線至儲存庫提出申請時，憑證註冊中心系統將以用戶輸入之通行碼鑑別其身分。

憑證用戶如透過電話申請時，憑證註冊中心人員將依據用戶留存之資料鑑別用戶之身分。

憑證用戶郵寄或臨櫃申請時，憑證註冊中心人員將比對用戶身分證明文件進行身分識別。

4 營運規範

4.1 金融憑證申請程序

憑證用戶向憑證註冊中心提出註冊及憑證申請，為確保安全性只允許金融機構擔任憑證註冊中心。

(1)憑證註冊中心必須確實說明申請單與合約書上之權利與義務規範，相關業務運作之作業流程，憑證用戶同意後確認。

(2)憑證用戶應正確且詳實填寫相關申請單並提供相關證明文件。憑證用戶依據申請之憑證等級，提供憑證註冊中心適當之身分證明文件(例如身分證、公司之設立登記表或公司變更登記表)及相關資訊。

(3)憑證註冊中心依據 3.1.8 及 3.1.9 節之作業規範，驗證憑證用戶之身分；身分驗證程序完成後，憑證註冊中心提供憑證用戶身分識別代碼及保護密碼，完成憑證用戶註冊及憑證申請作業。

(4)憑證用戶自行產生公開/私密金鑰對及 PKCS#10 憑證申請檔，透過憑證註冊中心驗證無誤後，由憑證註冊中心向本管理中心申請憑證用戶憑證之簽發。

4.2 金融憑證簽發程序

(1) 憑證註冊中心完成憑證用戶註冊及憑證申請審核作業後，依本管理中心之作業規範將憑證用戶之身分識別及申請資料安全的傳遞至本管理中心。

(2) 本管理中心於接收到憑證註冊中心上傳的憑證用戶憑證申請訊息時，驗證憑證用戶身分之合法性，及憑證申請訊息之完整性及有效性(例如：憑證用戶簽章)，正確無誤後載入資料庫，並簽發 FPKI 金融憑證予 FPKI 金融憑證用戶。

(3) 本管理中心於產生憑證用戶憑證後，即刻更新資料庫之 FPKI 金融憑證資訊供憑證用戶查詢使用。

(4) 當憑證用戶憑證申請訊息為本管理中心拒絕時，此失敗交易本管理中心必須立刻通知憑證註冊中心；惟交易失敗之原因，憑證註冊中心應以電子郵件方式、電話或其他適當方式告知 FPKI 金融憑證申請者不同意簽發的理由；若主管機關或相關法律有特別規範則不在此限。

4.3 金融憑證接受程序

憑證用戶申請 FPKI 金融憑證簽發完成且透過憑證註冊中心或由本管理中心儲存庫取得 FPKI 金融憑證時，憑證用戶應依下列規定處理：

(1)確認 FPKI 金融憑證內容之憑證用戶相關資訊與憑證用戶註冊時之一致性，且為憑證用戶之正確資訊。

(2)憑證用戶憑證之公開金鑰與所對應之私密金鑰為相關之一組且為憑證用戶所擁有。

(3)憑證用戶於接受所申請之憑證後，即是接受本作業基準、「金融公開金鑰基礎建設憑證政策」與合約上之權利與義務之關係。

(4)當 FPKI 金融憑證之公開金鑰與申請者憑證請求不一致或 FPKI 金融憑證之欄位未依本作業基準核發時，FPKI 金融憑證申請者得以拒絕，本管理中心應廢止該 FPKI 金融憑證。

4.4 憑證暫時停用及廢止

本節主要描述在何種情形下憑證得（或必須）予以暫停使用或廢止，並說明憑證暫停使用、廢止等程序。

4.4.1 廢止憑證之事由

遇有任何下列情況時(包括但不限於)，憑證用戶應向憑證註冊中心提出要求廢止憑證之申請：

(1)私密金鑰遺失、遭竊、改變及未經授權之揭露或其他破壞或盜用；

(2)憑證所載資訊發生足以影響對用戶信賴之重大改變；

(3)憑證不再需要使用或因其他因素要求廢止。

另外，本管理中心得就下列情形逕行廢止憑證，毋須事先通知用戶。

(1)確知憑證所載之部分事項不真實；

(2)確知憑證用戶之簽章私密金鑰遭冒用、偽造或破解；

(3)確知本管理中心之私密金鑰或資訊系統遭冒用、偽造或破解，致影響憑證之可信賴性；

(4)確知該憑證未依本作業基準之規定程序簽發時；

(5)用戶已經違反或無法擔負本作業基準或任何其他合約及相關法令之規定或責任時；

(6)依司法或檢調機關之通知或依相關法律之規定；

4.4.2 憑證廢止之申請者

與憑證用戶有關之憑證註冊中心、本管理中心、主管機關或合法授權之第三者與憑證用戶皆有權執行憑證之廢止。

4.4.3 憑證廢止之程序

(1)憑證用戶填寫申請表單、述明理由及簽名確認，或以具有憑證用戶簽章之廢止憑證申請訊息，主管機關或合法授權之第三者亦須依據憑證註冊中心制訂之作業規範提出憑證廢止請求，向憑證註冊中心申請。憑證註冊中心在接到憑證廢止請求後，即進行相關的審核程序，並保留所有憑證廢止請求紀錄，包含申請者名稱、聯絡資料、廢止原因、廢止時間與日期等，以作為後續權責歸屬之依據，本管理中心將於憑證廢止清冊或線上憑證狀態協定查詢回應訊息載明憑證廢止原因。

(2)憑證註冊中心完成審核作業後，將憑證廢止申請訊息傳送至本管理中心。

(3)本管理中心接獲憑證註冊中心送來之憑證廢止申請資料時，先檢核相關憑證註冊中心之授權狀態，確認其被授權之保證等級與範圍，再依據憑證註冊中心所送之憑證廢止請求廢止該憑證。

(4)本管理中心將憑證用戶憑證廢止回覆訊息，正確且安全傳回憑證註冊中心，並定期產生憑證廢止清冊(CRL)。憑證註冊中心於收到回覆訊息後，即刻通知憑證用戶憑證廢止之作業完成。

(5)如以上之檢核不通過時，本管理中心將回傳相關錯誤信息給憑證註冊中心，並拒絕後續相關作業；若憑證註冊中心有任何疑問，應主動聯絡本管理中心，確實瞭解問題之所在。

(6)為確保本管理中心及憑證註冊中心間傳輸資料之機密、完整及不可否認性(Non-Repudiation)，透過網路傳輸之憑證申請資料，係經數位簽章及傳輸層安全 (Transport Layer Security)協定加密傳送。

(7)憑證在廢止後，將置於最新 1 次公告之憑證廢止清冊中，並更新憑證資料庫以提供線上憑證狀態協定查詢服務。憑證廢止資訊一直到憑證過期後，才自憑證廢止清冊(CRL)中移除。憑證廢止清冊及憑證狀態資訊之異動，將留存適當稽核軌跡。

4.4.4 憑證廢止申請之處理時間

用戶提出憑證廢止申請後，憑證註冊中心應儘速於 1 個工作天內完成審核程序，審核通過後，本管理中心將於 24 小時內完成廢止憑證作業。

4.4.5 暫時停用憑證之事由

用戶在以下情形得申請憑證之暫時停用：

(1)憑證金鑰對懷疑遭盜用或可能遺失時。

(2)自行認定必須申請憑證之暫時停用。

(3)憑證用戶欲暫時停止使用該憑證一段時間。

(4)憑證用戶使用憑證而為有權第三者(例如：本管理中心或憑證註冊中心)宣告未履行應盡義務(例如：費用)，或不當使用憑證而有可能違反政府法律、規章、本作業基準或業務使用規範之疑慮時。

4.4.6 暫時停用憑證之申請者

暫時停用之請求只允許由憑證用戶提出，本管理中心或憑證註冊中心不可主動對任何一使用者憑證做憑證之暫時停用。

4.4.7 暫時停用憑證之程序

(1)FPKI 金融憑證用戶依照憑證註冊中心之憑證用戶身分驗證規範，或以具有憑證憑證用戶簽章之暫時停用憑證申請訊息，依照憑證註冊中心之安全管控措施，經由郵寄或網際網路向憑證註冊中心申請。

(2)憑證註冊中心收到憑證用戶之暫時停用憑證申請資料，檢核憑證用戶身分之合法性與訊息之安全性，且此憑證為憑證用戶之有效憑證，經檢核正確無誤後，即時將具有憑證註冊中心簽章之憑證用戶暫時停用憑證申請訊息，加簽數位簽章上傳至本管理中心申請暫時停用憑證。

(3)憑證註冊中心為提供憑證用戶於緊急，或特殊之異常狀況下申請憑證暫時停用之作業程序(例如：電話、傳真)，則依照各業務之相關作業規範之規定辦理，但亦需具有完整之身分驗證之安全管控措施。

(4)本管理中心收到憑證註冊中心之憑證用戶暫時停用憑證申請訊息時，驗證憑證註冊中心身分之合法性，與憑證用戶暫時停用憑證申請訊息之安全性，正確無誤後，將暫時停用金融用戶之憑證。

(5)本管理中心將憑證用戶暫時停用憑證申請結果訊息，正確且安全地傳回憑證註冊中心，並即時更新憑證資料庫以提供線上憑證狀態協定查詢服務，且定期產生憑證廢止清冊(CRL)。FPKI 金融憑證暫時停用資訊必須一直到憑證恢復使用或過期後，才自憑證廢止清冊中移除。

4.4.8 暫時停用憑證之時間

用戶提出憑證暫時停用申請後，憑證註冊中心應儘速於 1 個工作天內完成審核程序，審核通過後，本管理中心將於 24 小時內完成憑證暫時停用處理程序。

用戶在申請暫時停用憑證時，不必申告所需停用的期間，本管理中心所設

定憑證暫時停用的最長期間為自核可申請時間到該憑證到期的時間。

如果在憑證暫時停用期間，用戶取消憑證暫時停用，即恢復使用憑證，則該憑證恢復為有效的(Valid)。

4.4.9 恢復使用憑證之程序

(1)憑證用戶依照憑證註冊中心之憑證用戶身分驗證規範，或以具有憑證用戶簽章之恢復使用憑證申請訊息，依照憑證註冊中心之安全管控措施，經由郵寄或網際網路向憑證註冊中心申請。

(2)憑證註冊中心收到憑證用戶之恢復使用憑證申請表單，檢核憑證用戶身分之合法性與訊息之安全性，且此 FPKI 金融憑證為憑證用戶之有效憑證，經檢核正確無誤後，即時將具有憑證註冊中心簽章之憑證用戶恢復使用憑證申請訊息,加簽數位簽章上傳至本管理中心申請恢復使用憑證。

(3)憑證註冊中心為提供憑證用戶於緊急，或特殊之異常狀況下申請憑證恢復使用之作業程序(例如：電話、傳真)，則依照各業務之相關作業規範之規定辦理，但亦需具有完整之身分驗證之安全管控措施。

(4)本管理中心收到憑證註冊中心之憑證用戶恢復使用憑證申請訊息時，驗證憑證註冊中心身分之合法性，與憑證用戶恢復使用憑證申請訊息之安全性，正確無誤後，將允許用戶恢復使用憑證。

4.4.10 憑證廢止清冊簽發頻率

本管理中心之憑證廢止清冊簽發頻率為每天 2 次。於更新後公布於儲存庫。

4.4.11 憑證廢止清冊檢核規定

信賴憑證者使用本管理中心所簽發之憑證前，應先檢核本管理中心公布之憑證廢止清冊或使用線上憑證狀態協定查詢服務，以確定該憑證是否有效。

信賴憑證者參考憑證廢止清冊時一定需確認：

(1)　憑證廢止清冊的來源正確性與資料完整性；

(2) 憑證廢止清冊尚未過期。

4.4.12 線上憑證狀態協定查詢服務

信賴憑證者使用線上憑證狀態協定查詢服務時,須檢核相關查詢結果資料之數位簽章，確認資料來源之正確性及完整性。

4.4.13 線上憑證狀態協定查詢服務之規定

如信賴憑證者無法依照 4.4.11 節之規定查詢憑證廢止清冊，則必須使用 4.4.12 節之線上憑證狀態協定查詢服務，檢核所使用的憑證是否有效。

4.4.14 其他形式廢止公告

目前沒有提供其他形式的廢止公告。

4.4.15 其他形式廢止公告之檢查規定

目前沒有提供其他形式的廢止公告。

4.4.16 金鑰被破解時之其他特殊需求

沒有其他不同於 4.4.1、4.4.2 及 4.4.3 節的規定。

4.5 安全稽核程序

本管理中心對於處理註冊與憑證相關作業的紙本文件、與電腦媒體紀錄，無論由實體環境設施、設備至電腦系統與憑證管理系統、及人工處理的事件紀錄，將詳實留存，包含處理事件型態、發生時間、事件發生與結束過程、訊息的發送與接收者、成功與失敗、事件處理者等。

所有本管理中心安全相關的事件，均做安全稽核紀錄(audit log)。安全稽核紀錄採自動產生、工作紀錄本、紙張等其他實體機制。所有安全稽核紀錄都被保存，且可供稽核時取得。可稽核事件之安全稽核紀錄遵循 4.6.2 節所述之歸檔(Archive)保留期限的維護方式進行。

4.5.1 被記錄事件種類

處理事件的紀錄種類包含實體環境門禁進出之人員授權的管理、電腦硬體

設備與設施的維護與異動管理、系統軟體與憑證管理系統的安裝建置與變更管理、註冊與憑證相關處理作業生命週期的管理、網路系統資源與稽核處理作業的管理、文件與資訊保存的管理等，應保存之資訊至少包含:

(1)金鑰產製

- 本管理中心產製金鑰時(但是並不強制規定在單次或只限 1 次使用的金鑰的產製)。

(2)私密金鑰之載入和儲存

- 載入私密金鑰到系統元件中。
- 所有為進行金鑰回復的工作，對保存在本管理中心之私密金鑰所做的存取。

(3)憑證之註冊

- 憑證註冊申請過程之交易處理與交易結果成功或失敗之紀錄。

(4)廢止憑證

- 憑證廢止申請過程之交易處理與交易結果成功或失敗之紀錄。

(5)帳號之管理

- 加入或刪除角色和使用者。
- 使用者帳號或角色之存取權限修改。

(6)憑證格式剖繪之管理

- 憑證格式剖繪之改變。

(7)憑證廢止清冊格式剖繪之管理

- 憑證廢止清冊格式剖繪之改變。

(8)實體存取及場所之安全

- 進出本管理中心機房人員之授權管理

■ 得知或懷疑違反實體安全規定。

(9)異常

■ 軟體錯誤。

■ 違反本作業基準。

■ 重設系統時鐘。

4.5.2 紀錄檔處理頻率

本管理中心定期檢視稽核紀錄，解釋重大事件。檢視的工作包括檢視所有的紀錄項目，最後完整地檢查任何警示或異常，當有任何異常或警訊的紀錄時，必須更進一步詳細追蹤查核，稽核檢視之結果以文件記錄。

本管理中心每週由授權之稽核員檢視稽核紀錄，非權責管理人員無法任意存取與竄改。

4.5.3 稽核紀錄檔保留期限

稽核資料現場保留 2 個月，依 4.5.4 節、4.5.5 節及 4.5.6 節所描述做為資料保留的管理機制。

稽核資料必須符合權責主管機關與司法管轄機關的法律管理規範，並依 4.6.2 節歸檔期限保存最少保留 10 年，當稽核資料的保留期限到期時，由稽核員移除資料，其他角色的人員不可移除。

4.5.4 稽核紀錄檔之保護

目前和已歸檔之自動事件日誌以安全之方式保存，以數位簽章方式確保稽核紀錄檔之完整性，只有授權者才可調閱。

本管理中心之稽核系統具有資源控管與身分識別安全機制，由經授權之稽核員執行備份(Backup)及記錄檢視存取，並留存存取稽核紀錄的記錄檔，以偵測與防止不當的存取與竄改。

儲存稽核紀錄之媒體至少一份存放至具有妥善安全管控措施的異地儲存場

所。

4.5.5 稽核紀錄檔備份程序

電子式稽核紀錄至少每月備份 1 次，並訂定於本管理中心作業程序中。

(1)本管理中心週期性地將事件日誌歸檔。

(2)本管理中心將事件日誌檔案存放於具安全管控措施之場所。

4.5.6 安全稽核系統

所有本管理中心安全相關的事件，均做安全稽核紀錄(audit log)。安全稽核紀錄採自動產生、工作紀錄本、紙張等其他實體機制。所有安全稽核紀錄都被保存，且可供稽核時取得。

本管理中心稽核系統於憑證管理系統開始執行時即啟動記錄功能，於憑證管理系統關閉後才停止紀錄的功能。

當稽核系統發生異常或故障時，憑證管理系統將停止相關受影響之服務，直到稽核系統回復正常運作。如果憑證作業管理系統必須持續運作而無法停止，則必須啟動手動紀錄蒐集或其他可行的紀錄蒐集方式。

4.5.7 引起事件者之公告

當事件發生而被稽核系統記錄時，稽核系統並不需要告知引起該事件的個體。

4.5.8 弱點評估

本管理中心每年至少 1 次對憑證管理系統進行弱點掃描，並進行相關的補強措施。對於異常事件的稽核紀錄處理，本管理中心對於異常事件可能造成的威脅(Threat)與風險進行評估，調整與修改安全管控措施，每年至少執行 1 次。

4.6 紀錄歸檔

本管理中心採取可靠的機制，以電腦資料或書面資料精確完整地保存與憑證作業相關之紀錄，包括：

(1)本管理中心本身金鑰對產製、儲存、存取、備援及更換等之重要追蹤紀錄。

(2)憑證申請、簽發、廢止及重發等重要追蹤紀錄。

此等紀錄除提供追蹤或稽核外，必要時得作為解決爭議之佐證資料，為遵守前述規定，憑證註冊中心必要時，得要求申請者或其代理人提出相關證明文件。

4.6.1 紀錄事件之類型

本管理中心記錄的歸檔資料有：

(1)本管理中心的被稽核認證(accreditation)資料(假設適用)

(2)憑證政策與憑證實務作業基準

(3)與用戶合約、相關作業手冊與申請表單文件

(4)系統與設備組態設定

(5)系統或組態設定的修改與更新的內容

(6)憑證申請、更新、暫時停用、廢止等憑證作業管理生命週期的申請、用戶身分識別資料與處理訊息。

(7)本管理中心之憑證

(8)所有已簽發或公告的憑證

(9)本管理中心金鑰更換的紀錄

(10)所有被簽發或公告的憑證廢止清冊

(11)其他作業系統與憑證管理系統檔案資訊，與稽核紀錄等。

(12)用來驗證及佐證歸檔內容的其它資料或應用程式。

(13)稽核者所要求的文件。

4.6.2 歸檔之保留期限

本管理中心憑證管理系統運作相關紀錄保存期限除符合權責主管機關與司法管轄機關的法律管理規範外，最少要保留歸檔資料的時間為 10 年。用來處理歸檔資料的應用程式也被維護 10 年。

4.6.3 歸檔之保護

(1)任何使用者不被允許新增、修改或刪除歸檔的資料。

(2)經過本管理中心授權程序可以將歸檔資料移到另一個儲存媒體上。

(3)歸檔的資料存放於具安全管控措施且具有防潮溼的保護環境下，非經由合法的授權人員皆無法存取。

(4)本管理中心另保存一份資料於具安全管控措施且具有防潮溼的保護環境的異地儲存場所。

歸檔紀錄非經主管機關或司法管轄機關經合法申請的需求，及用戶自己授權且符合作業管理規範的申請，絕不任意予第三者知悉。

4.6.4 歸檔備份程序

本管理中心之電子式紀錄將依照所訂之備份程序，以複製方式定期備份至儲存媒體存放，紙本紀錄將由本管理中心所授權之人員定期整理歸檔。

4.6.5 時戳紀錄之要求

本管理中心的所有電腦系統都會定期進行校時，以確保電子式紀錄中日期與時間資訊的準確性與可信度。歸檔之電子式紀錄(例如憑證申請、展期、停用、復用與廢止之處理紀錄、憑證廢止清冊、金鑰更新及異動及稽核紀錄等)每一紀錄之時戳資訊包含日期與時間資訊，並採用系統經校時後的標準時間，而且這些紀錄皆經過適當的數位簽章保護，可用以檢核紀錄中的日期與時間資訊是否遭到篡改。

4.6.6 歸檔資料彙整系統

憑證管理系統作業相關的保存紀錄文件與資訊，如無法由電腦系統處理及

產出，則由本管理中心所授權之人員定期整理蒐集與處理。

4.6.7 取得及驗證歸檔資料之程序

依本管理中心之作業程序，在獲取憑證管理中心歸檔資訊時，相關人員必須得到正式的授權，才可以取出已歸檔的資訊。

在驗證歸檔資訊時，由經授權之稽核員進行驗證的程序，書面文件應驗證文件簽署者及日期的真偽。

4.7 金鑰更換

本管理中心之私密金鑰依照 6.3.2 節規定定期更換，本管理中心依據上層憑證管理中心之規定更換用來簽發憑證的金鑰對後，將向上層憑證管理中心申請新的憑證，以新私密金鑰簽發用戶之憑證、註冊中心憑證、線上憑證狀態協定回應伺服器(OCSP Responder)憑證及憑證廢止清冊，新的憑證將公布於儲存庫，提供用戶下載。

憑證用戶之私密金鑰必須依照 6.3.2 節有關憑證用戶私密金鑰使用期限之規定定期更換。

4.8 金鑰遭破解或災變時之復原程序

4.8.1 本管理中心電腦資源、軟體或資料遭破壞之復原程序

本管理中心訂定電腦資源、軟體及資料遭破壞之復原程序，同時每年進行演練。

如本管理中心的電腦設備遭破壞或無法運作，但本管理中心的簽章金鑰並未被損毀，則優先回復本管理中心儲存庫之運作，並迅速重建憑證簽發及管理的能力。

4.8.2 本管理中心簽章金鑰憑證被廢止之復原程序

如本管理中心之簽章金鑰憑證被廢止，將公告於儲存庫，通知信賴憑證者，並依照 4.7 節之程序產生新的金鑰對，將新的憑證公告於儲存庫，供用戶及信賴憑證者下載。

用戶依照 4.1 節之程序重新申請憑證。

4.8.3 本管理中心簽章金鑰遭破解之復原程序

如本管理中心簽章金鑰遭破解，採取以下復原程序：

(1)公告於儲存庫，通知上層憑證管理中心、用戶及信賴憑證者

(2)申請廢止本管理中心簽章金鑰憑證及所簽發之用戶憑證。

(3)依照 4.7 節之程序產生新的金鑰對，將新的憑證公告於儲存庫，供用戶及信賴憑證者下載。

(4)用戶依照 4.1 節之程序重新申請憑證。

4.8.4 本管理中心安全設施之災害復原工作

本管理中心訂定災害復原之程序，同時每年進行演練，當發生災害時，將由緊急應變小組啟動災害復原程序，優先回復本管理中心儲存庫之運作，並迅速重建憑證簽發及管理的能力。

4.9 本管理中心之終止服務

本管理中心終止服務時，應依我國電子簽章法相關規定進行憑證管理中心終止服務的程序。為確保用戶與信賴憑證者之權益，本管理中心應遵守以下事項：

(1)本管理中心於預定終止服務 30 日前，通知主管機關(經濟部)與用戶；

(2)本管理中心終止服務時將採如下措施：

- 對終止當時仍具效力之憑證，安排其他憑證管理中心承接此業務。並將終止服務及由其他憑證管理中心承接其業務之事實公告於儲存庫及通知仍具效力之憑證用戶。但無法通知者，不在此限。
- 將所有營業期間之紀錄檔案，移交給承接此業務之其他憑證管

理中心。

- 若無憑證管理中心願承接本管理中心之業務，將陳報主管機關安排其他憑證管理中心承接。
- 若經主管機關安排其他憑證管理中心承接，仍無其他憑證管理中心承接時，本管理中心將於終止服務 30 日前，於儲存庫公告廢止當時仍具效力之憑證憑證，並通知憑證之所有人。本管理中心將依憑證有效期限比例，退還憑證簽發或展期費用。
- 主管機關於必要時，得公告廢止當時仍具效力之憑證。

5 實體、程序及人員安全的控管

5.1 實體控管

本管理中心系統建置於具實體安全管控措施的安全環境,只有經授權人員才可依照相關作業規範執行憑證管理作業，避免系統遭破壞或未經授權使用。

5.1.1 實體所在及結構

本管理中心機房位於中華電信數據通信分公司,符合儲存高重要性及敏感性資訊的機房設施水準，並具備門禁、保全、入侵偵測及 24 小時監視錄影等實體安全機制，以防止未經授權存取本管理中心之相關設備。

5.1.2 實體存取

本管理中心建置採適當之措施管制連接提供本管理中心服務的硬體、軟體和硬體密碼模組，24 小時隨時執行監控錄影與紀錄。所有含敏感明文資料之可攜式儲存媒體及文件均存放於安全處所,需 2 人以上方可對系統及硬體密碼模組進行實體存取，並留存稽核軌跡。

本管理中心機房總共有四層門禁,第一層和第二層分別為全年無休的大門及大樓警衛，第三層為樓層讀卡機進出管制系統，第四層為機房人員指紋辨識器(Finger-printed)進出管制系統,指紋辨識器採用三度空間指紋取樣,可以判別被辨識物的紋深、色澤以及是否為活體，執行門禁認證。

除門禁系統可限制不相干人員接近機房外,機箱之監控系統可控制機箱之開啟，以防止未經授權存取硬體、軟體和硬體密碼模組等相關設備。

任何可攜式儲存媒體帶進機房,需檢查並確認沒有電腦病毒及任何可能危害本管理中心系統的惡意軟體。

非本管理中心人員進出機房，需填寫進出紀錄,並由本管理中心相關人員全程陪同。

本管理中心相關人員離開機房時,將進行以下之檢核工作並記錄,以防止未授權人員進入機房：

(1)確認設備是否正常運作。

(2)確認機箱門是否關閉。

(3)確認門禁系統是否正常運作。

5.1.3 電源和空調

本管理中心的電力系統，除了市電外，另設有發電機(滿載油料，可連續運轉 6 天）及不中斷電源系統（UPS）並及提供市電及發電機的電源自動切換。提供至少 6 小時以上備用電力供儲存庫備援資料。

本管理中心裝有恆溫恆濕的空調系統，用以控制環境的溫度及濕度，以確保機房具最佳運作環境，並定期維護及測試。

5.1.4 水災防範及保護

本管理中心機房設置在基地墊高建築物的第 3 樓層以上，該建築物具備防水閘門和抽水機，且沒有因為水災造成重大損害紀錄。

5.1.5 火災防範及保護

本管理中心具備有自動偵測火災預警功能，系統自動啟動滅火設備，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來操作。

5.1.6 媒體儲存

記錄稽核、歸檔和備援資料的儲存媒體儲存一份在 5.1.1 節所述具有防火、防水、防磁、防靜電干擾的場所，另一份存在具安全管控措施的異地備援場所。

備份及保存資訊的儲存媒體與文件，定期執行測試與驗證資訊的有效性及可用性。

5.1.7 廢料處理

2.8.1 節所記載本管理中心的文件資料，不需要使用時，都要經過碎紙機處

裡。任何磁帶、硬碟、磁碟、磁光碟(MO)和任何形式的記憶體，在報廢前，都要經過格式化程序清除所儲存的資料。光碟將被實體銷毀，經稽核員驗證，並留存查核紀錄。

5.1.8 異地備援

異地備援的地點與本管理中心機房距離 30 公里以上，備援的內容包括資料、系統程式及回復系統運作所需之復原程序。

5.2 程序控制

本管理中心經由作業程序控管(procedural controls)，以規定可以操作本管理中心系統的各個可信賴角色(trusted role)，每個工作的人員需求數，和每個角色的識別與鑑別(identification and authentication)，以確保系統的作業程序安全有合理的保證度。

5.2.1 信賴角色

本管理中心必須確保從事關鍵性本管理中心功能的責任，能做適當的區隔分派，以防止某人惡意使用本管理中心系統而不被察覺。每個使用者必須依照其被指定之任務執行該任務所需之系統存取。

本管理中心指派 5 個不同的 PKI 人員角色，分別為管理員、簽發員、稽核員、維運員和實體安全控管員，以抵擋可能的內部攻擊。1 個角色的工作可以多個人來擔任，但是每個群組只設有 1 個主管(Chief Role)來領導該群組的工作，而 5 種角色的工作責任區分如下：

管理員主要負責：

- 安裝、設定和維護本管理中心系統。
- 建立和維護系統之使用者帳號。
- 產製和備份本管理中心之金鑰。

簽發員主要負責：

- 啟動/停止憑證簽發服務。

■ 啟動/停止憑證廢止服務。

■ 啟動/停止憑證廢止清冊簽發服務

稽核員主要負責：

■ 對稽核紀錄的檢核、維護和歸檔。

■ 執行或監督內部的稽核，以確認本管理中心維運是否遵照本作業基準的規定。

維運員主要負責：

■ 系統設備的日常運作維護。

■ 系統的備援及復原作業。

■ 儲存媒體的更新。

■ 系統軟硬體的更新。

■ 網路及網站的維護：建置系統安全與病毒防護機制及網路安全事件的偵測與通報等。

實體安全控管員主要負責：

■ 系統的實體安全控管(機房的門禁管理、防火、防水、空調系統等）。

5.2.2 角色分派

本管理中心角色分依照5.2.1節定義的5種信賴角色，對人員及角色分配必須符合以下規定：

■ 管理員、簽發員、稽核員和維運員不得相互兼任

■ 實體安全控管員不得兼任其他4種角色工作。

■ 無論在任何條件下，任何一個角色，都不可以執行自我稽核功能，不允許自己稽核自己。

5.2.3 每個任務所需之人數

■ 管理員(Administrator)

共需要有至少 3 位合格的人員來擔任。

■ 簽發員(Officer)

共需要有至少 2 位合格的人員來擔任。

■ 稽核員(Auditor)

共需要有 2 位合格的人員來擔任。

■ 維運員(Operator)

需要有 2 位合格的人員來擔任。

■ 實體安全控管員 (Controller)

需要有 2 位合格的人員來擔任。

每個任務項目所需要的人員數在以下表格所述：

任務項目	管理員	簽發員	稽核員	維運員	實體安全控管員
安裝、設定和維護本管理中心系統	2				1
建立和維護系統之使用者帳號	2				1
產製和備份本管理中心之金鑰	2		1		1
啟動/停止憑證簽發服務		2			1

任務項目	管理員	簽發員	稽核員	維運員	實體安全控管員
啟動/停止憑證廢止服務		2			1
啟動/停止憑證廢止清冊簽發服務		2			1
對稽核紀錄的檢核、維護和歸檔			1		1
系統設備的日常運作維護				1	1
系統的備援及復原作業				1	1
儲存媒體的更新				1	1
除本管理中心憑證管理系統以外軟硬體的更新				1	1
網路及網站的維護				1	1

5.2.4 識別及鑑別每一個角色

使用 IC 卡識別和鑑別管理員、簽發員、稽核員和維運員角色，利用中央門禁系統設定權限識別和鑑別實體安全控管員角色。

本管理中心主機的作業系統帳號管理，使用登入者帳號、密碼和群組，提供識別和鑑別管理員、簽發員、稽核員和維運員角色。

5.3 人員控管

5.3.1 身家背景、資格、經驗及安全需求

1.人員晉用之安全評估

工作人員的甄選及晉用包含下列項目：

(1)個人性格之評估。

(2)申請者經歷之評估。

(3)學術及專業能力及資格之評估。

(4)人員身分之確認。

(5)人員操守之評估。

2.人員考核管理

本管理中心對於執行憑證業務之員工，在初任時予以資格審查，以確認其具可信度及工作能力，就任後予以適當之教育訓練，並以書面約定並註明負責的責任，並每年進行資格複查，以確認其可信度及工作能力是否維持，若無法通過資格複查則調離其職，改派其他符合資格人選擔任。

3.人員任免遷調管理

當人員任用及約聘僱條件或契約有所變更，尤其是人員離退或是約聘僱用契約終止時，必定要遵守機密維護責任約定。

4.機密維護之責任約定

工作人員，依相關規定課予機密維護責任，並簽署本管理中心所規定之維護營業秘密契約書，員工不得以口頭、影印、借閱、交付、文章發表或其他方法取得、使用、洩漏營業秘密。

5.3.2 身家背景檢核程序

本管理中心對於5.2節之各信賴角色人員在初任時予以資格審查，以確認身分資格證明相關文件是否屬實。相關人員亦接受定期審核；經審查有不適任

該可信賴角色時，不可繼續執行該職務。

5.3.3 教育訓練需求

角色	教育訓練需求
管理員	1、公開金鑰基礎建設安全原理和機制。 2、安裝、設定和維護本管理中心系統操作程序。 3、建立和維護系統之用戶帳號操作程序。 4、設定稽核參數操作程序。 5、產製和備份本管理中心之金鑰操作程序。 6、災後復原以及營運持續管理之程序。
簽發員	1、公開金鑰基礎建設安全原理和機制。 2、本管理中心系統軟硬體的使用及操作程序。 3、啟動/停止憑證簽發服務之操作程序。 4、啟動/停止憑證廢止服務之操作程序。 5、啟動/停止憑證廢止清冊簽發服務之操作程序。 6、災後復原以及營運持續管理之程序。
稽核員	1、公開金鑰基礎建設安全原理和機制。 2、本管理中心系統軟硬體的使用及操作程序。 3、產製和備份本管理中心之金鑰操作程序。 4、對稽核紀錄的檢核、維護和歸檔程序。 5、災後復原以及營運持續管理之程序。
維運員	1、系統設備的日常運作維護程序。

角色	教育訓練需求
	2、系統的備援及復原作業程序。 3、儲存媒體的更新程序。 4、災後復原以及營運持續管理之程序。 5、網路和網站的維護程序。
實體安全控管員	1、 設定實體門禁權限程序。 2、 災後復原以及營運持續管理之程序。

5.3.4 再教育訓練需求及頻率

本管理中心的每1位相關工作人員，要熟悉本管理中心及其相關工作程序或法規的改變。有任何重大變動時(如憑證管理系統功能更新，或加入新系統，或進用新進人員)，於變動後1個月內要安排適當的教育訓練時間實施再訓練並做紀錄，以適應新的工作程序及法規的運作，對於執行憑證管理作業需求而訂之教育訓練時程，每年至少檢討1次。

5.3.5 工作調換頻率及順序

1、不得互兼的角色，不可工作調換。

2、維運員經過受訓之後，且經由審核通過，2年後可轉任管理員、簽發員、稽核員等工作。

3、管理員、簽發員及稽核員，可以於轉任維運員工作1年後，再轉任管理員、簽發員或稽核員等工作。

人員進行工作輪調前將提供適當之知識與技能之教育訓練，使其勝任該職務。

5.3.6 未授權行動之制裁

本管理中心之相關人員，如違反憑證政策與本作業基準或其他本管理中心公布之程序，將接受適當的管理與懲處，如情節重大而造成損害者，將採取法

律行動追究其責任。

5.3.7 聘雇人員之規定

本管理中心委外聘僱人員安全要求除依照聘僱工作內容簽訂相關合約外，相關作業安全管理措施與正式人員相同。

5.3.8 提供給人員之文件資料

本管理中心提供憑證政策、本作業基準、本管理中心系統操作及相關作業手冊及我國電子簽章法及其施行細則等文件給本管理中心之相關人員。

6 技術安全控管

本章描述由本管理中心所執行的技術安全控管。

6.1 金鑰對產製與安裝

6.1.1 金鑰對產製

6.1.1.1本管理中心金鑰對產製

本管理中心依照 6.2.1 節規定，於密碼模組內產製金鑰對，採虛擬亂數產生器(Pseudo Random Number Generator)及 RSA 金鑰演算法，私密金鑰在密碼模組內產製後一直儲存在其中而不外洩。

本管理中心之金鑰產製由相關人員見證下進行，經 2 位(含)以上之授權人員啟動密碼模組產生。

6.1.1.2金融憑證用戶金鑰對產製

由 FPKI 金融憑證使用者自行產生。

6.1.2 將私密金鑰傳送給金融憑證用戶

FPKI 金融憑證使用者之金鑰對皆需自行產生，因此無傳送私密金鑰之需求。

6.1.3 將憑證用戶之公開金鑰傳送給憑證管理中心

憑證用戶必須以 PKCS# 10 憑證申請檔的格式將公開金鑰送給憑證註冊中心，憑證註冊中心依照 3.1.7 節規定檢核用戶確實擁有相對應的私密金鑰後，以安全管道將憑證用戶的公開金鑰傳送至本管理中心。

6.1.4 將憑證管理中心之公開金鑰傳送給信賴憑證者

本管理中心本身之公開金鑰憑證，公布在本管理中心的儲存庫上，並提供識別資訊與驗證完整性資料，讓用戶及信賴憑證者直接做下載及安裝。

信賴憑證者在使用本管理中心本身之公開金鑰憑證前必須由安全管道取得上層憑證管理中心之公開金鑰或自簽憑證，然後檢核上層憑證管理中心對本管理中心本身之公開金鑰憑證的簽章，以確保公開金鑰憑證中之公開金鑰是可信賴

的。

6.1.5 金鑰長度

本管理中心使用金鑰長度為4096位元的RSA金鑰及SHA256雜湊函數演算法簽發憑證。

用戶使用金鑰長度為2048位元的RSA金鑰。

6.1.6 公開金鑰參數產製

RSA 演算法公開金鑰參數為空的(Null)。

6.1.7 金鑰參數品質檢核

本管理中心簽章用金鑰對採ANSI X9.31演算法產生RSA演算法中所需的質數，該法可保證該質數為強質數(Strong Prime)。

用戶金鑰可於IC卡內部或其他軟硬體密碼模組產生RSA演算法中所需的質數，但不保證該質數為強質數。

6.1.8 金鑰經軟體或硬體產製

本管理中心及其用戶使用 6.2.1 節規定之安全密碼模組產製虛擬隨機亂數、公開/私密金鑰對和對稱金鑰。

用戶的金鑰對可由硬體或軟體產生，產生後的金鑰對應做適當之機密性保護，嚴禁將金鑰對以明碼的形式儲存於一般媒體中(如硬碟、磁片等)。

6.1.9 金鑰之使用目的

本管理中心簽章用私密金鑰用於簽發憑證、憑證廢止清冊。

本管理中心簽發給用戶之簽章用或加密用憑證，其用途將記載於X.509 憑證金鑰用途欄位(keyUsage)。

用戶憑證允許可兼具有簽章用及加密用的金鑰用途設定。

6.2 私密金鑰保護

6.2.1 密碼模組標準

本管理中心使用通過FIPS 140-2 Level 3認證之硬體密碼模組儲存簽章用私密金鑰。

FPKI憑證用戶金鑰對之儲存媒體符合銀行公會所訂之「金融XML憑證共通性技術規範」。

6.2.2 金鑰分持之多人控管

對本管理中心私密金鑰備份的持份之安全控管，將以m-out-of-n金鑰分持方式來做本管理中心私密金鑰的備份及回復，依5.2.3節多人控管規範，至少由2位以上授權人員同時進行作業。

用戶私密金鑰之多人控管不另做規定。

6.2.3 私密金鑰託管

本管理中心簽章用私密金鑰不被託管，本管理中心也不負責保管用戶的私密金鑰。

6.2.4 金鑰備份

依照6.2.2節的金鑰分持之多人控管方法備份本管理中心私密金鑰，並使用通過CNS 15135、ISO 19790或FIPS 140-2 Level 2以上之驗證的IC卡做為秘密分持的儲存媒體。

用戶為確保交易之持續進行，可自行決定是否做私密簽章金鑰之備份，惟用戶應妥善保管其私密金鑰之備份，惟用戶端之私密金鑰備份應以不影響交易簽章之唯一性及不可否認性為原則。

6.2.5 金鑰歸檔

本管理中心簽章用私密金鑰不被歸檔，但會依照4.6節執行相對應公開金鑰憑證的歸檔。

6.2.6 私密金鑰輸入密碼模組

本管理中心在兩種情況時做私密金鑰輸入密碼模組中：

(1)金鑰產製時。

(2)金鑰持份備援的回復時。在此情況是以秘密持份(m-out-of-n control)的方式來做本管理中心私密金鑰的回復，經由私密金鑰秘密持份IC卡的回復後，便即時將完整的私密金鑰寫入到硬體密碼模組中。

6.2.7 私密金鑰啟動方式

本管理中心之私密金鑰之啟動是由m-out-of-n控管IC卡來控制，不同用途的控管IC卡由管理員、簽發員所保管，依5.2.3節多人控管規範，至少由2位以上授權人員同時進行作業。

憑證用戶私密金鑰啟動方式符合銀行公會所訂之「金融XML憑證共通性技術規範」。

6.2.8 私密金鑰停用方式

本管理中心之私密金鑰採6.2.2節多人控管方法方式將私密金鑰停用。

本管理中心不提供用戶之私密金鑰停用。

6.2.9 私密金鑰銷毀方式

為避免本管理中心舊的私密金鑰被盜用，妨害整個憑證之真確性，本管理中心金鑰不再需要使用時其私密金鑰必須加以銷毀，將會把存在硬體密碼模組內本管理中心舊的私密金鑰做零值化(Zeroization)處理，以便確保銷毀硬體密碼模組中本管理中心舊的私密金鑰。

而除了銷毀硬體密碼模組中本管理中心舊的私密金鑰外，該私密金鑰的金鑰備援的秘密持份IC卡也會在本管理中心金鑰更新的同時進行實體銷毀。

如果一個金鑰儲存模組已經將被永久的不再提供服務，但還是可以被取得時(accessible)，則儲存在這個安全模組中的所有私密金鑰(含已經有使用過或是

可能要被使用的)，都將要被銷毀。銷毀該密碼模組中的金鑰後，必須再使用該密碼模組所提供的金鑰管理工具加以檢視，以確認是否上述所有的金鑰都已經不存在。

如果一個金鑰儲存密碼模組已經將被永久的不再提供服務，則儲存在這個安全模組中已經有使用過的所有私密金鑰，都將要被自此安全模組中刪除(erased)。

用戶之私密金鑰銷毀方式，不另做規定。

6.3 金鑰對管理之其他要點

用戶必須自行管理金鑰對，本管理中心不負責保管用戶的私密金鑰。

6.3.1 公開金鑰之歸檔

本管理中心將進行用戶憑證之歸檔，且依照4.6節規定執行歸檔系統之安全控管，不再另外進行用戶公開金鑰的歸檔。

6.3.2 公開金鑰及私密金鑰之使用期限

6.3.2.1本管理中心公開金鑰及私密金鑰之使用期限

本管理中心之公開金鑰及私密金鑰長度為RSA 4096 位元(bits)。公開金鑰憑證經金融政策憑證管理中心簽發給本管理中心有效期限為5年。本管理中心之私密金鑰使用期限與公開金鑰憑證有效期限相同，其中私密金鑰簽發用戶憑證與註冊中心憑證之使用期限最長為3年，但簽發憑證廢止清冊、線上憑證狀態協定回應伺服器憑證之用途則必須至所簽發之用戶憑證、註冊中心憑證與線上憑證狀態協定回應伺服器憑證其效期到期為止，故本管理中心之私密金鑰使用期限至多5年。整理如下表:

種類	私密金鑰使用期限	憑證效期
本管理中心之公開金鑰憑證對應之私密金鑰用於簽發用戶憑證	3年	5年

本管理中心之公開金鑰憑證對應之私密金鑰用於簽發註冊中心憑證	3年	5年
本管理中心之公開金鑰憑證對應之私密金鑰用於簽發憑證廢止清冊、線上憑證狀態協定回應伺服器憑證	5年	5年

6.3.2.2用戶公開金鑰及私密金鑰之使用期限

憑證用戶私密金鑰使用期限至多2年，公開金鑰憑證有效期限至多為2年。

6.4 啟動資料

6.4.1 啟動資料的產生及安裝

本管理中心之私密金鑰啟動資料(Activation Data)以亂數產生後寫入密碼模組內，並分持至m-out-of-n控管IC卡中，存取IC卡中的啟動資料時必須輸入IC卡的個人識別碼(以下簡稱為PIN碼)。

憑證用戶金鑰啟動資料，由用戶自行產生及設定或由憑證註冊中心產生，由憑證註冊中心產生之啟動資料須經安全管道(如密封之密碼單)傳送給用戶。

6.4.2 啟動資料之保護

本管理中心之私密金鑰啟動資料由m-out-of-n控管IC卡保護，IC卡的PIN碼由保管人員自行記憶，不得記錄於任何媒體上，IC卡移交時由新的保管人員重新設定新的PIN碼。

若登入的失敗次數超過3次，即鎖住此控管IC卡。

憑證用戶金鑰啟動資料，憑證用戶應妥善保管或記憶後銷毀，以確保惟有憑證用戶可使用，由憑證註冊中心產生之啟動資料，憑證註冊中心之系統應有安全管控措施(如以亂碼化方式儲存)，以防止非授權人員取得用戶之啟動資料。

6.4.3 其他啟動資料之要點

本管理中心的私密金鑰的啟動資料不做歸檔。

6.5 電腦軟硬體安全管控措施

6.5.1 特定電腦安全技術需求

本管理中心和其相關輔助系統透過作業系統，或結合作業系統、軟體和實體的保護措施提供下列電腦安全功能。

(1)具備角色或身分識別的登入，於系統資源存取控管之角色與權責區分的獨立性與可稽核性，達到授權人員於系統資源存取控管時，身分識別驗證的唯一性與確實性。

(2)提供自行定義(discretionary)存取控制。

(3)提供安全稽核能力。

(4)對各種憑證服務和PKI信賴角色存取控制的限制

(5)傳遞訊息，符合機密性(Confidentiality)、完整性與不可否認性等安全控管。

(6)憑證相關交易的回復管理機制，與稽核作業的管理機制。

6.5.2 電腦安全評等

本管理中心憑證伺服器採用通過 Common Criteria EAL 3 認證的電腦作業系統。

6.6 生命週期技術控管

6.6.1 系統研發控管措施

本管理中心的系統研發遵循CMMI Level 3的規範進行品質控管。

系統開發環境與測試環境、上線環境應有所區隔。

系統研發單位應善盡良善管理責任，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、測試報告與管理手冊、版本控管給本管理中心。

6.6.2 安全管理控管措施

本管理中心之資訊安全管理系統遵循美國會計師公會與加拿大會計師公會(AICPA/CPA) 所制定的Trust Service Principles and Criteria for Certification Authorities標準規範運作。

本管理中心的軟體在首次安裝時,將確認是由供應商提供正確的版本且未被修改。

本管理中心之硬體和軟體是專用的，僅能使用獲得安全授權的元件，不安裝與運作無關的硬體裝置、網路連接或元件軟體。

本管理中心將記錄和控管系統的組態及任何修正與功能提升,同時偵測未經許可修改系統之軟體或組態。

6.6.3 生命週期安全評等

每年至少1次評估現行金鑰是否有被破解之風險。

6.7 網路安全管控措施

本管理中心之主機和儲存庫透過防火牆和外部網路連接,儲存庫置於防火牆之對外服務區(非軍事區DMZ)，連接到網際網路(Internet)，除必要之維護或備援外，提供不中斷之憑證與憑證廢止清冊查詢服務。

本管理中心之儲存庫透過系統修補程式的更新、系統弱點掃描、入侵偵測系統、防火牆系統等加以保護，以防範阻絕服務和入侵等攻擊。

非屬本管理中心之私密金鑰的控管活動，在緊急狀況下得允許啟用諸如SSL VPN之機制進行問題偵測及狀況排除。SSL VPN之使用將被自動記錄於稽核主機中，並遵守6.6.2節之規定，SSL VPN稽核紀錄之審查由內部稽核員負責。

6.8 密碼模組安全管控措施

參照 6.1、6.2 節

7 憑證及憑證廢止清冊之格式剖繪

7.1 憑證格式剖繪

本管理中心所簽發的憑證會遵循本作業基準的規定。

7.1.1 版本序號

本管理中心簽發 X.509 V3 版本的憑證。

7.1.2 憑證擴充欄位

本管理中心簽發的憑證之憑證擴充欄位會遵循 RFC5280 之規定。

7.1.3 演算法物件識別碼

本管理中心 簽發的憑證於簽章時，所使用的演算法物件識別碼為：

sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

(OID：1.2.840.113549.1.1.11)：

本管理中心簽發的憑證於識別產製主體金鑰時，所使用的演算法物件識別碼為：

RsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}

(OID:1.2.840.113549.1.1.1)

7.1.4 命名形式

憑證中的申請者及簽發者兩個欄位值，必須使用 X.500 的唯一識別名稱，且此名稱的屬性型態必須遵循 RFC 5280 的規定。

FPKI 金融憑證命名形式符合銀行公會所訂之「金融 XML 憑證共通性技術規範」。

7.1.5 命名限制

FPKI 金融憑證命名限制符合銀行公會所訂之「金融 XML 憑證共通性技術規範」。

7.1.6 憑證政策物件識別碼

本管理中心於簽發憑證內存放相對應之憑證政策物件識別碼，請參照 1.2 節。

7.1.7 政策限制擴充欄位之使用

本管理中心簽發憑證不含政策政策限制擴充欄位。

7.1.8 政策限定元的語法及語意

本管理中心簽發的憑證不含政策限定元(Policy qualifiers)。

7.1.9 關鍵憑證政策擴充欄位之語意處理

本管理中心簽發的憑證所含之憑證政策擴充欄位不註記為關鍵擴充欄位。

7.2 憑證廢止清冊之格式剖繪

7.2.1 版本序號

本管理中心簽發 X.509 v2 版本的憑證廢止清冊(CRL)。

7.2.2 憑證廢止清冊擴充欄位

本管理中心簽發的憑證廢止清冊(CRL) 會遵照 RFC 5280 之規定。

7.3 線上憑證狀態協定之格式剖繪

本管理中心提供符合 IETF PKIX Working Group 的 RFC 6960 及 RFC 5019 標準規範之線上憑證狀態協定(OCSP)服務，並在憑證的憑證機構資訊存取(Authority Info Access, AIA)擴充欄位中包含本管理中心 OCSP 的服務網址。

7.3.1 版本序號

本管理中心接受的線上憑證狀態協定查詢封包應包含以下資訊：

- 版本序號
- 待查詢憑證識別元(identifier)

待查詢憑證識別元包含：雜湊演算法、憑證簽發者(CA)名稱(Issuer Name)之雜湊值、憑證簽發者(CA)公開金鑰(Issuer Key)之雜湊值及待查詢憑證之憑證序號。

本管理中心簽發的線上憑證狀態協定(OCSP)查詢回應封包含有以下基本欄位：

欄位	說明
版本序號(Version)	v.1 (0x0)
OCSP 回應伺服器 ID(Responder ID)	OCSP 回應伺服器的主體名稱(Subject DN)
產製時間(Produced Time)	回應封包簽署時間
待查詢憑證識別元(identifier)	包含：雜湊演算法、憑證簽發者(CA)名稱(Issuer Name)之雜湊值、憑證簽發者公開金鑰(Issuer Key)之雜湊值及待查詢憑證之憑證序號
憑證狀態碼(Certificate Status)	憑證狀態對應碼(0:有效/1:廢止/2:未知)
效期 (ThisUpdate/NextUpdate)	此回應封包建議的效期區間，包含：生效時間(ThisUpdate)及下次更新時間(NextUpdate)
簽章演算法(Signature Algorithm)	回應封包的簽章演算法，可為 sha256WithRSAEncryption
簽章(Signature)	OCSP 回應伺服器的簽章
憑證(Certificates)	OCSP 回應伺服器的憑證

7.3.2 線上憑證狀態協定擴充欄位

本管理中心針對線上憑證狀態協定查詢的回應封包包含有以下擴充欄位：

- 線上憑證狀態協定回應伺服器的金鑰識別元(Authority Key Identifier)

此外，當線上憑證狀態協定查詢封包含有隨機數(nonce)欄位時，線上憑證狀

態協定查詢之回應封包也必須包含相同的隨機數欄位。

7.3.3 線上憑證狀態協定服務運轉規範

本管理中心線上憑證狀態協定(OCSP)服務運轉作業包含有以下：

- 可以處理與接受 HTTP Get/Post 管道或方法所傳送 OCSP 用戶端之查詢請求封包(OCSPRequest) 。

線上憑證狀態協定(OCSP)服務伺服端所使用的 OCSP 回應伺服器憑證為 CA 系統所簽發，且必須為短效期之有效憑證，需要由 CA 系統定期進行簽發與更新。

8 憑證實務作業基準之維護

8.1 變更程序

本作業基準每年定期評估是否需要修訂，以維持其保證度，本作業基準之修訂不會變更物件識別碼。修訂方式包括以附加文件方式修訂及直接修訂本作業基準的內容。

8.1.1 變更時不另作通知之變更項目

本作業基準重新排版時，不另作通知。

8.1.2 應通知之變更項目

8.1.2.1變更項目

評估變更項目對用戶或信賴憑證者之影響程度：

(1)影響程度大者，於本管理中心儲存庫公告 30 個日曆天，始得修訂。

(2)影響程度小者，於本管理中心儲存庫公告 15 個日曆天，始得修訂。

8.1.2.2通知機制

所有變更項目將公告於本管理中心儲存庫。

8.1.2.3意見之回覆期限

對於變更項目有意見者，其回覆期限：

(1)8.1.2.1 節之(1)影響程度大者，回覆期限為自公告日起 15 個日曆天內。

(2)8.1.2.1 節之(2)影響程度小者，回覆期限為自公告日起 7 個日曆天內。

8.1.2.4處理意見機制

對於變更項目有意見者，於意見回覆期限截止前，以本管理中心儲存庫公告之回覆方式傳送給本管理中心，本管理中心將考量相關意見，評估變更項目。

8.1.2.5最後公告期限

本作業基準公告之變更項目依照8.1.2.2及8.1.2.3節規定進行修訂，公告期限依照8.1.2.1節規定至少公告15個日曆天，直到本作業基準修訂生效。

8.2 公告及通知之規定

本作業基準修訂後7個日曆天內公告於本管理中心儲存庫，本作業基準之修訂生效日期，除另有規定外，於公告後生效。

8.3 憑證實務作業基準之審定程序

本作業基準將送交「銀行公會憑證政策管理委員會」審查，並經電子簽章法主管機關經濟部核定後，由本管理中心公布。

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

附錄 1：縮寫和定義

英文縮寫	英文全稱	中文名詞或定義
AIA	Authority Info Access	憑證機構存取資訊，參見附錄 2。
AICPA	American Institute of Certified Public Accountants	美國會計師公會，參見附錄 2。
CA	Certification Authority	憑證機構，參見附錄 2。
CMM	Capability Maturity Model	能力成熟度模型，參見附錄 2。
CP	Certificate Policy	憑證政策，參見附錄 2。
CPA	Chartered Professional Accountants Canada	加拿大會計師公會，參見附錄 2。
CP OID	CP Object Identifier	憑證政策物件識別碼。
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。
DN	Distinguished Name	唯一識別名稱。
FPKI	Financial Public Key Infrastructure	銀行公會金融公開金鑰基礎建設
FUCA	Financial User Certification Authority	用戶憑證管理中心
FIPS	(US Government) Federal Information Processing Standard	(美國)聯邦資訊處理標準，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。
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。
PIN	Personal Identification Number	個人識別碼。
PKCS	Public-Key Cryptography Standard	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	Security Socket 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	不中斷電源系統，參見附錄 2。

附錄 2：名詞解釋

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。
美國會計師公會(American Institute of Certified Public Accountants, AICPA)	與加拿大會計師公會共同訂頒 The Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy 系列標準之單位，並為 WebTrust for CA、SSL Baseline Requirement & Network Security 標章之管理單位。
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。
鑑別(Authenticate)	(1)驗證某個聲稱的身分是合法的且屬於提出此聲稱者的程序。(A Guide to Understanding Identification and Authentication in Trusted Systems, National Computer Security Center) (2)當某個體出示身分時，確認其身分之正確性。
鑑別程序(Authentication)	(1)建立使用者或資訊系統身分信賴程度的程序。 （NIST.SP.800-63-2 Electronic Authentication Guideline）。 (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) 鑑別是識別的證明。(A Guide to Understanding Identification and Authentication in Trusted Systems) 而所謂的相互鑑別(Mutual Authentication, National Computer Security Center)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 Info Access, AIA)	記載有關存取憑證機構資訊的擴充欄位，內容可包含：線上憑證狀態協定(OCSP)的服務位址，以及憑證簽發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。
能力成熟度模型 (Capability Maturity Model, CMM)	由美國卡內基美隆大學(Carnegie Mellon University, CMU)的軟體工程研究所(Software Engineering Institute, SEI)以軟體流程評鑑(Software Process Assessment, SPA)與軟體能力評估(Software Capability Evaluation, SCE)為基礎的框架，協助軟體開發業者找出軟體開發流程需要改善之處。
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。 C.用戶的公開金鑰。 D.憑證之有效期間。 E.憑證機構數位簽章。 在本憑證政策中所提及的“憑證”特別指其格式為 ITU-T 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。
憑證政策 (Certificate	(1)某 1 憑證所適用之對象或情況所列舉之 1 套

Policy, CP)	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、展期及存取等)符合特定需求(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)憑證機構以數位方式簽章，並可供信賴憑證者使用之已廢止憑證表列。(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。
加拿大會計師公會 (Chartered Professional Accountants Canda, CPA)	與美國會計師公會共同訂頒 The Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy 系列標準之單位，並為 WebTrust for CA、SSL Baseline Requirement & Network Security 標章之管理單位。加拿大會計師公會之前英文名稱為 Canadian Institute of Chartered Accountants，縮寫為 CICA。
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。
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)	資料未遭受未經授權或意外的更改、破壞或遺失的性質。
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)
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。
識別(Identification)	識別是某使用者是誰（廣為週知）的陳述方式或表達方式。(A Guide to Understanding Identification and Authentication in Trusted Systems) 。 識別是指描述或宣稱某個當事人或個體的方式，例如透過使用者帳號、姓名、電子郵件。
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。官方網站位於 https://www.ietf.org/，其願景是藉由產製高品質之技術文件影響人類設計、使用與管理網際網路，使得網際網路運作更順暢。
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。
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任者(信任之一方)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	(1)1 種以字母或數字組成之唯一識別碼，該識別碼必須

Identifier, OID)	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。
線上憑證狀態協定(Online Certificate Status Protocol, OCSP)	線上憑證狀態協定(Online Certificate Status Protocol)是 1 種線上憑證檢查協定，使信賴憑證者應用軟體可決定某張憑證之狀態(例如已廢止、有效等)。
線上憑證狀態協定回應伺服器(OCSP Responder)	由憑證管理中心所授權維運的線上伺服器，並連接至其儲存庫以處理憑證狀態查詢請求。
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 Standard, 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。
憑證註冊中心(Registration Authority, RA)	(1)負責確認憑證申請人之身分或其他屬性，但不簽發憑證亦不管理憑證。註冊中心是否需為其行為負責及其應負責任之範圍，依所適用之憑證政策或協議訂之。 (2)1 個體，負責對憑證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)	(1)信賴所收受之憑證及可用憑證中所載之公開金鑰加以驗證之數位簽章者，或信賴憑證中所命名主體之身

	份(或其他屬性)及憑證所載公開金鑰之對應關係者。(憑證實務作業基準應載明事項準則第 1 章第 2 條第 6 項) (2)個人或機構收到包含憑證及數位簽章(此數位簽章可藉由憑證上所列之公開金鑰做驗證)之資訊，並且可能信賴這些資訊。
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。
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。
安全插座層(Secure Socket Layer)	由網景公司(Netscape)推出 Web 瀏覽器時所提出的協定，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。
用戶(Subscriber)	(1)指憑證中所命名或識別之主體，且其持有與憑證中所載公開金鑰相對應之私密金鑰者。(憑證實務作業基準應載明事項準則第 1 章第 2 條第 5 項) (2)具下列特性之個體，包括(但不限於)個人、機構、伺服器軟體或網路裝置： (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(Inside Threat) 與外部威脅(Outside 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。
傳輸層安全(Transport Layer Security, TLS)	由網際網路工程任務小組(IETF)將 SSL 協定制訂為 RFC 2246，並將其稱為 TLS (Transport Layer Security)，其最新版本是 RFC 5246，亦即 TLS 1.2 協定。
不中斷電源系統 (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，是指建立憑證申請者的身分背景之識別。(RFC 3647)
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。