中華電信安全電子郵件憑證管理中心憑證實務作業基準

(CHT SMIME Certification Authority Certification Practice Statement, CHT SMIME CA CPS)

第 1.05 版

中華電信股份有限公司

中華民國 110 年 5 月 28 日

目　　錄

中華電信安全電子郵件憑證管理中心憑證實務作業基準摘要

中華電信股份有限公司(以下簡稱本公司)依據電子簽章法第 11 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，制定中華電信安全電子郵件憑證管理中心(CHT SMIME Certification Authority，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，並公布於本公司網站，始得提供簽發憑證服務。

一、主管機關核定文號：經商字第 10902374410 號

二、所簽發的憑證種類：

自然人或組織所需的安全電子郵件憑證。

三、憑證等級：

本管理中心依據中華電信公開金鑰基礎建設憑證政策(以下簡稱憑證政策)之相關規定運作，簽發憑證政策所定義的身分識別保證等級第 1 級至第 3 級由自然人、組織所使用的安全電子郵件憑證(參見第 1.4.1 節)。

四、應用範圍：

本管理中心所簽發的憑證，適用於電子郵件收發所需的身分識別及資料保護。

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、相關法律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. 本管理中心及註冊中心損害賠償責任

本管理中心或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註冊中心負賠償責任。用戶得依與本管理中心或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、相關法律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. 除外條款

如因不可抗力及其他非可歸責於本管理中心及註冊中心之事由，所導致之損害，本管理中心及註冊中心不負任何法律責任。本管理中心及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，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。

4. 財務責任

本管理中心以本公司為財務擔保；本管理中心財務依相關法律規定辦理財務稽核。

5. 用戶責任

用戶應妥善保管及使用其私密金鑰。用戶之憑證如須暫停使用、廢止或辦理展期或重發，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. 本管理中心所屬註冊中心之註冊工作，皆經本管理中心授權許可。
2. 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。
3. 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。
4. 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。稽核採用的標準為 WebTrust Principles and Criteria for Certification Authorities。
5. 稽核結果以 WebTrust for Certification Authorities 及 WebTrust for Certification Authorities – SSL Baseline Requirements 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。

憑證實務作業基準修訂履歷表

版次	實施日期	修訂內容摘要
0.95	109/10/21	初版發行。
1.0	109/12 /30	經濟部核定版本(涵蓋中華電信憑證政策管理委員會通過之第 0.95 版)
1.05	110/05/28	修訂摘要、第 1.2 節、第 1.6.2 節、第 3.2.1 節、第 3.2.2 節、第 3.2.3 節、第 3.2.5 節、第 4.9.1 節、第 4.9.12 節、第 5.5.2 節、第 6.1.1.1 節、第 6.1.2 節、第 6.1.3 節、第 6.7 節、第 7.1.4.2.1 節、第 8.1 節、第 8.2 節、第 8.4 節、第 8.6 節、第 9.1.5 節、第 9.3.3 節、第 9.4.4 節。

1 序論

1.1 概要

依據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)憑證政策的規定，中華電信憑證總管理中心(ePKI Root Certification Authority, eCA)為本基礎建設之最頂層憑證管理中心與信賴根源(Trust Anchor)，具備最高的公信度，信賴憑證者(Relying Party)可直接信賴 eCA 的憑證。本管理中心是 eCA 的第 1 層下屬憑證機構(Level 1 Subordinate CA)，由 eCA 簽發憑證予本管理中心，在本基礎建設中負責簽發與管理自然人與組織所需的安全電子郵件憑證(S/MIME Certificiates)。

1.1.1 憑證實務作業基準

本憑證實務作業基準(Certification Practice Statement，以下簡稱為本作業基準)，係依據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，以下簡稱憑證政策)所訂定，並遵循與參考：

(1) 電子簽章法

(2) 及其子法「憑證實務作業基準應載明事項準則」

之相關規定及國際標準、政策、指引如：

(1) 網際網路工程任務小組(Internet Engineering Task Force, IETF)之徵求修正意見書(Request for Comments, RFC) 3647、RFC 5280、RFC 6960、RFC 5019 及 RFC8550

(2) ITU-T X.509

(3) Microsoft Trusted Root Program Requirements

(4) Apple Root Store Program

(5) Mozilla Root Store Policy

(6) Chromium Project Root Store Certificate Policy

(7) Google S/MIME certificate profiles

(8) 憑證機構與瀏覽器論壇 (CA/Browser Forum, http://www.cabforum.org) 發行的 Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates(以下簡稱 Baseline Requirements)及 Network and Certificate System Security Requirements

所訂定之政策文件，以做為本管理中心訂定憑證實務作業基準之依循。

1.1.2 憑證實務作業基準之適用範圍

本作業基準所載明之實務作業規範適用於本管理中心、註冊中心(Registration Authority)、用戶(Subscribers)、信賴憑證者、儲存庫(Repository)及其他相關成員等。

1.2 文件名稱與識別

本文件的名稱為中華電信安全電子郵件憑證管理中心憑證實務作業基準(CHT SMIME Certification Authority Certification Practice Statement)，本作業基準為第 1.05 版，版本發行日期為中華民國 110 年 5 月 28 日。本作業基準之最新版本可在以下網頁取得：

https://smimeca.hinet.net

本作業基準對應之身分識別保證等級(Identity Assurance Level，以下簡稱保證等級)與憑證政策物件識別碼如下表所示：

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
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}

1.3 主要成員

本管理中心之相關成員包括：

(1) 本管理中心

(2) 註冊中心

(3) 用戶

(4) 信賴憑證者

1.3.1 憑證機構

本管理中心由本公司負責建置及營運，依照憑證政策之規定運作，簽發自然人及組織所需之安全電子郵件憑證。

1.3.2 註冊中心

註冊中心負責蒐集和驗證用戶的身分及憑證相關資訊之註冊工作。註冊中心由 1 個或多個註冊窗口(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)，負責受理本管理中心不同群組與類別之憑證申請、廢止、憑證之更換金鑰等作業，包含負責電子郵件帳號之經授權網域名稱部分的審驗。

1.3.3 用戶

用戶係指已申請並取得本管理中心核發憑證之個體，其與憑證主體之關係如下表所示：

憑證主體	用戶
自然人	本人
組織	組織授權之委任人
應用軟體	應用軟體之擁有者

用戶金鑰對的產製應符合本作業基準第 6.1.1 節之規定，並且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，用戶本身不簽發憑證給其他方。

1.3.4 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關係的個體。信賴憑證者必須依照相對的憑證機構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) 驗證電子郵件數位簽章產生者的身分。
(2) 驗證具有數位簽章的電子郵件之完整性。
(3) 加密電子郵件訊息。

1.3.5 其他相關成員

若本管理中心有選擇其他相關提供信賴服務機構做為協同運作的夥伴，會於網站揭露並於本作業基準中訂定相互運作機制及彼此的權利與義務關係，以確保本管理中心服務品質的有效及可靠。

1.4 憑證用途

1.4.1 憑證適用範圍

本管理中心簽發憑證政策所定義保證等級第 1 級、第 2 級與第 3 級之憑證(含簽章及加密用的憑證)。

各憑證保證等級之適用範圍說明如下：

保證等級	適用範圍
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，適合應用於惡意篡改之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用於保護電子郵件機密性的對稱式金鑰；不適合應用於需要鑑別身分及不可否認(Non-Repudiation)/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)；不適合做為重要郵件(與生命及高金額相關的交易之文件)的簽署或加密。
第 3 級	適合應用於有惡意使用者會截取或篡改資訊、較第 2 級危險之網路環境，傳送簽章並能確認為其本人之簽署。可用於不可否認/內容承諾的線上交易。

使用及信賴本管理中心所提供的認證服務前，用戶及信賴憑證者都應詳細閱讀、遵守本作業基準，並且應注意本作業基準的更新。

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。

信賴憑證者在使用本管理中心所簽發之憑證前，應確認憑證之類

別、保證等級及金鑰用途(keyUsage)等是否符合應用需求。

信賴憑證者應依第 6.1.7 節所述記載於憑證中的 keyUsage，以適當地使用個別的金鑰，並且應正確處理在憑證擴充欄位中被標示為關鍵性(critical)欄位的憑證屬性資料。

1.4.2 憑證禁止事項

本管理中心所簽發的憑證禁止使用於下列的情況：

(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

1.5 聯絡方式

1.5.1 憑證實務作業基準之制訂與管理機構

中華電信股份有限公司。

1.5.2 聯絡資料

1.5.2.1 憑證實務作業基準建議

對本作業基準有疑義需要諮詢，或有修訂建議，請利用以下資訊與本管理中心聯繫：

電子郵件信箱：caservice@cht.com.tw

電話：886-2-2344-4820

郵遞地址:10048 台北市信義路一段 21 號數據通信大樓 4F
中華電信安全電子郵件憑證管理中心

也可至 https://smimeca.hinet.net 查詢聯絡資料。

1.5.2.2 憑證問題報告

用戶、信賴憑證者、應用軟體供應商以及其他第三方組織於發現私密金鑰遺失、疑似私密金鑰遭破解、憑證遭誤用、或是憑證被偽造、破解、濫用或不當使用等情況(包含工作日以外時間)時，可寄送電子郵件至 report_abuse@cht.com.tw 向本管理中心提出憑證問題報告(Certificate Problem Report)。本管理中心是否廢止該憑證，參見第 4.9.3 與 4.9.5 節。

1.5.3 憑證實務作業基準之審定

本管理中心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)進行審查及核定。在核定後本管理中心正式引用本基礎建設的憑證政策(參見 eCA 儲存庫 https://eca.hinet.net/repository_a.htm)。

另依據我國電子簽章法規定，憑證機構訂定之憑證實務作業基準，必須經主管機關經濟部核定後，始得對外提供簽發憑證服務。

本管理中心定期自行稽核，以證明遵照引用於本基礎建設憑證政策的保證等級進行營運。為使本管理中心所發之憑證順暢運作於電子郵件軟體，本基礎建設已經申請參與各作業系統、瀏覽器與軟體平台等應用軟體供應商之根憑證計畫(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，每年併同中華電信憑證總管理中心執行外部稽核並將最新之憑證實務作業基準與外部稽核的結果提供給各大根憑證計畫，並維護稽核標章公告於本管理中心網站。

1.5.4 憑證實務作業基準變更程序

本作業基準經政策管理委員會及電子簽章法主管機關經濟部核定後，由本管理中心公布。如憑證政策的修訂公告後，本作業基準將配合修訂，先送政策管理委員會審查後，再送交電子簽章法主管機關經濟部核定。

本作業基準修訂生效後，除另有規定外，如修訂之版本與原本作業基準有所牴觸時，以修訂之版本為準。

1.6 名詞定義與縮寫

1.6.1 縮寫

縮寫	全稱	中文名詞或定義
AIA	Authority Information Access	憑證機構資訊存取，參見第 1.6.2 節。
CA	Certification Authority	憑證機構，參見第 1.6.2 節。
CMMI	Capability Maturity Model Integration	能力成熟度模型，參見第 1.6.2 節。
CP	Certificate Policy	憑證政策，參見第 1.6.2 節。
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，參見第 1.6.2 節。
CRL	Certificate Revocation List	憑證廢止清冊，參見第 1.6.2 節。
DN	Distinguished Name	唯一識別名稱。
DNS	Domain Name System	網域名稱系統，參見第 1.6.2 節。

縮寫	全稱	中文名詞或定義
eCA	ePKI Root Certification Authority	中華電信憑證總管理中心，參見第 1.6.2 節。
EE	End Entities	終端個體。
ePKI	Chunghwa Telecom ecommerce Public Key Infrastructure	中華電信公開金鑰基礎建設，參見第 1.6.2 節。
FIPS	(US Government) Federal Information Processing Standard	(美國)聯邦資訊處理標準，參見第 1.6.2 節。
FQDN	Fully Qualified Domain Name	完全吻合網域名稱，參見第 1.6.2 節。
IANA	Internet Assigned Numbers Authority, IANA	網際網路號碼分配機構，參見第 1.6.2 節。
IETF	Internet Engineering Task Force	網際網路工程任務小組，參見第 1.6.2 節。
NIST	(US Government) National Institute of Standards and Technology	(美國)國家標準和技術研究院，參見第 1.6.2 節。
OCSP	Online Certificate Status Protocol	線上憑證狀態協定，參見第 1.6.2 節。
OID	Object Identifier	物件識別碼，參見第 1.6.2 節。
PIN	Personal Identification Number	個人識別碼。
PKCS	Public-Key Cryptography Standard	公開金鑰密碼學標準，參見第 1.6.2 節。
PKI	Public Key Infrastructure	公開金鑰基礎建設，參見第 1.6.2 節。
QGIS	Qualified Government Information Source	合格的政府資訊來源，參見第 1.6.2 節。
QTIS	Qualified Government Tax Information Source	合格的政府稅收資訊來源，參見第 1.6.2 節。
RA	Registration Authority	註冊中心，參見第 1.6.2

縮寫	全稱	中文名詞或定義
		節。
RFC	Request for Comments	徵求修正意見書，參見第 1.6.2 節。
SSL	Secure Sockets Layer	安全插座層，參見第 1.6.2 節。
TLS	Transport Layer Security	傳輸層安全，參見第 1.6.2 節。
UPS	Uninterrupted Power System	不斷電系統，參見第 1.6.2 節。

1.6.2 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)，除金鑰外所需及應受保護之隱密資料。
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。
應用軟體供應商 (Application Software Suppliers)	顯示或使用憑證與根憑證的網際網路瀏覽器軟體或其他倚賴方的應用程式的供應商。
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 2 條第 1 款]
保證等級	具相對性保證層級中之某 1 級數。[憑證實務

(Assurance Level)	作業基準應載明事項準則第 2 條第 2 款]
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)	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：線上憑證狀態協定(OCSP)回應伺服器的服務位址，以及憑證簽發機構之憑證驗證路徑的下載位址等。
經授權網域名稱 (Authorization Domain Name)	用於取得對某一個特定完全吻合網域名稱(FQDN)之憑證簽發的授權之網域名稱。 憑證機構可使用網域名稱服務別名紀錄查詢服務(DNS CNAME lookup)所回覆之 FQDN 當作 FQDN，用來達到網域驗證的目的。如果 FQDN 包含萬用字元，則憑證機構必須從被請求之 FQDN 的最左邊移除所有萬用字元。憑證機構可從左至右刪除零個或多個標籤 (label) 直到遇到基礎網域名稱 (Base Domain Name)，也可使用任何在這個過程中的值來達到網域驗證的目的。
備份(Backup)	將資料或程式複製，必要時可供復原之用。
基礎網域名稱(Base Domain Name)	申請的 FQDN 之一部分，是除了第一個網域名稱節點外，剩下的註冊表控制(registry-

	controlled)或公開字尾(public suffix)左邊第一個網域名稱節點加上註冊表控制或公開字尾(例如「example.co.uk」或「example.com」)。FQDN 最右邊之網域名稱節點(domain name node)，在其註冊協議(registry agreement)有 ICANN 規格 13(ICANN Specification 13)的通用頂級網域名稱(gTLD)，則通用頂級網域名稱本身可以當做基礎網域名稱。
基本要求 (Baseline Requirements)	由 CA/Browser Forum 所發行的「The Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates」以及對這份文件所作的任何修訂。
連結、繫結(Binding)	將兩個相關的資訊元素做連結(結合)的過程。
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，內容至少包括： 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。 在本作業基準中所提及的「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 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 2 條第 3 款] (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(敘明於憑證政策或其他服務契約中)之聲明。
憑證問題報告 (Certificate Problem Reports)	疑似金鑰遭破解、憑證遭誤用(misuse)或其他種類的詐騙、破解、濫用或與憑證相關的不當行為之投訴。
憑證金鑰更換 (Certificate Re-key)	改變在密碼系統應用程式中所使用之金鑰對。通常必須藉由對新的公開金鑰簽發新的憑證來達成新的金鑰對替換的目的。
憑證廢止 (Certificate Revocation)	在憑證的有效期間內，提前終止憑證的運作。

憑證廢止清冊 (Certificate Revocation List, CRL)	由憑證機構以數位方式簽署且會定期更新之已廢止憑證清冊，清冊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。
中華電信憑證政策管理委員會(Chunghwa Telecom Certificate Policy Managemet Authority，簡稱政策管理委員會)	1 組織，其設立目的為：研議中華電信所經營之公開金鑰基礎建設其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。
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)	保證資料從發文者產製完到被收文者接受都未遭竄改。
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]
網域名稱聯絡人 (Domain Contact)	於網域名稱服務 Start of Authority 紀錄(DNS SOA record)或是基礎網域名稱之 WHOIS 紀錄所列，或透過直接聯絡網域名稱受理註冊機構所得的網域名稱註冊者(Domain Name Registrant)、技術聯絡人(technical contact)、或管理聯絡人(administrative contact)(或是在國碼頂級網域名稱(ccTLD)下對等的人員)。
網域名稱 (Domain Name)	在網域名稱系統分配給 1 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。
網域名稱註冊者 (Domain Name	有時被稱為網域名稱的擁有者(owner)，但更

Registrant)	恰當的是表示某人或某實體被網域名稱受理註冊機構(Domain Name Registrar)註冊為具有權利使用該網域名稱，亦即被網域名稱受理註冊機構或 WHOIS 列為「Registrant」之自然人或法人。
網域名稱受理註冊機構(Domain Name Registrar)	接受以下三類團體贊助、支持或簽署協議： (1)網際網路名稱和編號註冊中心(the Internet Corporation for Assigned Names and Numbers , ICANN), (2) 國家級網域名稱註冊中心(a national Domain Name authority/registry), 或 (3) 網路資訊中心(Network Information Center)及其加盟人、承包商、代表、繼承人或受讓人)，受理網域名稱註冊的實體(Entity)或自然人。
網域名稱系統(Domain Name System, DNS)	用來自動轉換 IP 位址與網域名稱的分散式資料庫。
憑證效期(Duration)	由「有效期限起始時間」(notBefore)及「有效期限截止時間」(notAfter)兩個子欄位所組成之憑證欄位。
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。
終端個體憑證(End-Entity Certificate)	簽發給終端個體的憑證。
中華電信公開金鑰基礎建設(Chunghwa Telecom ecommerce Public Key Infrastructure, ePKI)	本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,	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

FIPS)	140 號標準(簡稱 FIPS 140)，到 2016 年 12 月為止此標準的最新版本為 FIPS 140-2。FIPS 140 將密碼模組區分為 11 類需求範圍，而 FIPS 140-2 則定義了 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。FQDN 包含主機名稱(服務名稱)與網域名稱兩部分。以 ourserver.ourdomain.com.tw 為例，ourserver 是主機名稱，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)。FQDN 的開頭一定是主機名稱。 另以 www.ourdomain.com 為例，www 是主機名稱，ourdomain 是次級網域名稱，com 則是通用頂級網域名稱(Generic Top-Level Domain, gTLD)。
識別(Identification)	識別是某使用者是誰(廣為周知)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。
網際網路號碼分配機構 (Internet Assigned Numbers Authority, IANA)	負責管理國際網際網路中使用的 IP 位址、網域名稱及許多其他參數之組織。
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/。
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。簽發憑證機構可為根憑證機構或下屬憑證機構。

管轄區域(Jurisdiction of Incorporation)	針對私人組織而言，為國家和州或省(如適用)或地方的組織，組織合法存在是經由向適當的政府機關或實體(例如：設立地點)申請。 針對政府機關而言，國家和州或省(如適用)的合法實體為依法設立。
金鑰託管 (Key Escrow)	依據用戶必須遵守的託管協議(或類似的契約)所規定，將用戶的私密金鑰進行存放。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，擁有用戶加密用的私密金鑰。
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配對關係的另 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。
(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。其所制定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)	公開金鑰機制所提供的技術性證據以支援不可否認之安全服務。 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 2 條第 4 款] (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。
線上憑證狀態協定裝訂 (OCSP Stapling)	一種 TLS/SSL 憑證狀態請求擴展欄位(TLS Certificate Status Request extension)，可替代線上憑證狀態協定(OCSP)成為另一種檢查 X.509 憑證狀態的方法。 本方法在運作上，網站會事先向 OCSP 回應伺服器取得有「時間限制(例如兩小時)」的 OCSP Response 並暫存；接下來，在每一次的 TLS Handshake 的初始過程中，網站會將此暫存的 OCSP Response 傳送給用戶(通常為瀏覽器)，用戶只需驗證該 OCSP Response 的有效性而不用再向 CA 發送 OCSP 請求，如此可避免用戶每次連結高流量 TLS 網站都需要向 CA 詢問其 TLS/SSL 憑證狀態，因此減輕 CA 的負擔。 此種機制藉由 TLS 網站轉發 CA OCSP 回應伺服器定期簽發之 TLS/SSL 憑證有效性訊息，也避免 OCSP 回應伺服器可能得知有哪些用戶嘗試瀏覽該 TLS 網站的隱私疑慮。
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、稽核和服務所組成之集合，可用於管理憑證及金鑰對。
合格稽核業者(Qualified Auditor)	符合基本要求(Baseline Requirements)第 8.2 節規定之稽核資格要求，且與受稽方獨立的會計師事務所、法人或個人。
合格的政府資訊來源 (Qualified Government Information Source, QGIS)	定期更新且現行公眾可取得、為了準確提供可被諮詢且一般被公認為可信賴的資料庫而設計且由政府機關維護，例如經濟部全國商工登記資料庫。資料的報告是根據法律規定，且虛假或誤導性的報告將被處以刑事或民事處罰。CA/Browser Forum 之 Guidelines For The Issuance and Management of Extended Validation Certificates 不禁止使用第三方供應商從政府機關取得的資訊，如果這些第三方供應商是從政府機關直接取得資訊。
合格的政府稅收資訊來源(Qualified Government Tax Information Source, QTIS)	合格的政府資訊來源，須具體包含與私人組織、其他商業團體或個人相關的稅收資訊。例如我國的財稅資料中心、美國的國稅局(IRS)。
隨機值(Random Value)	由憑證機構所指定提供給申請者具備至少

	112 位元之亂度(熵，Entropy)的數值。
註冊機關 (Registration Agency)	負責登記個體營業設立或核准執照之營業資訊的政府機關，可能包含(但不限於)(1)公司申登機關(2)目的事業主管機關(例如：交通部)，或(3)監管機關(例如：金融監督管理委員會、國家通訊傳播委員會)。
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。
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 2 條第 6 款]
儲存庫(Repository)	(1) 指用以儲存及供檢索憑證與其他相關憑證資訊之系統。[憑證實務作業基準應載明事項準則第 2 條第 7 款] (2) 包含憑證政策、憑證實務作業基準及憑證相關資訊的資料庫。
徵求修正意見書 (Request for Comments, RFC)	由 IETF 發行的一系列備忘錄，包含網際網路、UNIX 和網際網路社群之標準、協定及程序等，並以編號排定。
安全插座層(Secure Sockets 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。
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：

	(a)憑證中所載明之主體 (b)擁有與憑證上所列公開金鑰相對應之私密金鑰。 (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，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 協定制定為 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。
可信賴系統(Trustworthy System)	具有下列性質之電腦硬體、軟體及程序： (1) 對於入侵及誤用有相當的保護功能。 (2) 提供合理的可用性、可靠度及正確操作。 (3) 適當地執行預定功能。 (4) 與一般為人所接受的安全程序一致。
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。
WHOIS	透過 RFC 3912 的 WHOIS、RFC 7482 的 RDAP(Registry Data Access Protocol) 或 HTTPS 網站，向網域名稱受理註冊機構或註冊管理機構(Registry)直接擷取的資訊。
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。[FIPS 140-2]

2 公布與儲存庫之責任

2.1 儲存庫

本管理中心儲存庫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及本作業基準，提供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://smimeca.hinet.net。如因故無法正常運作，將於 2 個日曆天內恢復正常運作。

2.2 憑證機構之資訊公布

本管理中心的責任在於將以下之資訊於儲存庫公布：

(1) 憑證政策及本作業基準。

(2) 憑證廢止資訊。

(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) 簽發之憑證。

(5) 隱私權保護政策。

(6) 本管理中心相關最新訊息。

(7) 最近 1 次之外部稽核結果(如第 8.6 節所述)。

2.3 公布之頻率或時間

(1) 本管理中心每年檢視更新本作業基準，於收到主管機關核准公文後 7 個日曆天內於儲存庫公布本作業基準。

(2) 本管理中心所遵循的憑證政策，於政策管理委員會核定後 7 個日曆天內公布於儲存庫。

(3) 本管理中心每天至少簽發兩次憑證廢止清冊,公布於儲存庫。

(4) 本管理中心本身之憑證，於接受上層之憑證管理中心簽發後7個日曆天內公布於儲存庫。

2.4 儲存庫之存取控制

本管理中心主機建置於防火牆內部，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。

有關第 2.2 節本管理中心公布的資訊為公開之資訊，主要提供用戶與信賴憑證者使用瀏覽器查詢之用，因此開放提供唯讀的閱覽存取，但為保障儲存庫之安全,實施邏輯和實體的控制防止未經授權的寫入儲存庫。

3 識別與鑑別

3.1 命名

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 及 rfc822Name 唯一識別名稱(Distinguished Name, DN)。

3.1.2 命名須有意義

本管理中心所簽發的憑證，其憑證主體名稱(Subject)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。

本管理中心和註冊中心可縮寫組織名稱的字首或字尾，例如：將官方機構所記載的組織名稱「Company Name Incorporated」改為「Company Name, Inc.」，且該縮寫內容必須使憑證主體於其設立或註冊的管轄區域易於辨識。假若組織名稱長度超過 64 個字元(Characters)時，可縮寫組織名稱或是刪除組織名稱中不重要的文字。

3.1.3 用戶之匿名或假名

本管理中心沒有簽發匿名憑證(anonymous certificate)給終端用戶，原則上也不簽發假名憑證(pseudonymous Certificate)。

3.1.4 不同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。

3.1.5 命名獨特性

本管理中心的憑證機構憑證其X.500唯一識別名稱為：

C=TW，

O=Chunghwa Telecom Co., Ltd.，

CN=CHT SMIME CA - Gn，其中 n = 1, 2, 3, 4…

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)
- stateOrProvinceName(縮寫為 S)
- localityName(縮寫為 L)
- organizationName(縮寫為 O)
- organizationalUnitName(縮寫為 OU)
- commonName(縮寫為 CN)
- serialNumber

3.1.6 商標之辨識、鑑別及角色

用戶提供之憑證主體名稱包含商標或任何受法律保護之姓名、商業或公司名稱、表徵時，本管理中心雖不負審查之責任，但其命名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憑證主體名稱若含商標之認可、驗證、合法及唯一性，相關糾紛或仲裁處理非本管理中心權責範圍，由用戶向主管機關或法院依據一般行政或司法救濟途徑處理之。

3.1.7 命名爭議之解決程序

當用戶之識別名稱相同時，以先申請之用戶優先使用，相關之糾紛或仲裁處理，非本管理中心之權責範圍，由用戶向相關權責機關(構)

或法院提出申請。

當用戶使用之識別名稱，經相關權責機關(構)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(可參考第 4.9.1 節)。

3.2 初始身分驗證

3.2.1 證明擁有私密金鑰之方式

本管理中心會驗證個體持有之私密金鑰與將記載於憑證上的公鑰成對，分為兩種方式。

(1) 由用戶自行產製金鑰對，然後產生 PKCS#10 憑證申請檔並以私密金鑰加以簽章，並於申請憑證時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簽章，以證明用戶擁有相對應的私密金鑰。

(2) 由卡管中心於晶片內部安全產製用戶之金鑰對，簽發憑證時由註冊中心透過安全管道將用戶之公開金鑰傳送至本管理中心，所以用戶在申請憑證時就不必證明持有私密金鑰。

3.2.2 組織身分之鑑別

保證等級 1 至 3 的安全電子郵件憑證申請，組織必須展現其電子郵件地址的控制權，參見第 3.2.5 節。對於組織(Organization)身分鑑別所需之證件、鑑別確認程序及是否需臨櫃辦理等，依照不同保證等級而有不同之規定，如下表 3-1 所列：

表 3-1

保證等級	組織身分鑑別之程序
第 1 級	無需識別申請者之身分是否為真實存在，只要申請人具有自己的電子郵件地址即可申請憑證，且申請者提供的識別資訊均視為自我提供的識別資訊。 (1) 不做證件核對。 (2) 不需臨櫃辦理。
第 2 級	須識別申請者是實際存在的個體，並能連結到真實世界的真實身分。 (1) 可不做證件核對。 (2) 不需臨櫃辦理。 (3) 提交組織資料例如組織識別碼(如扣繳單位稅籍統一編號)、組織名稱等，本管理中心有權與政府提供之資料庫或可信賴之第三者資料庫的登記資料進行比對，以確認申請人之身分。
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

保證等級	組織身分鑑別之程序
	(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。

3.2.3 個人身分之鑑別

保證等級 1 至 3 的安全電子郵件憑證申請，個人必須展現其電子郵件地址的控制權，參見第 3.2.5 節。對於個人(Individual)身分鑑別之證件、確認程序及是否需臨櫃辦理等，依照不同保證等級而有不同之規定，如下表所列：

保證等級	個人身分鑑別之程序
第 1 級	無需識別申請者之身分是否為真實存在，只要申請人具有自己的電子郵件地址即可申請憑證，且申請者提供的識別資訊均視為自我提供的識別資訊。 (1) 不做證件核對。 (2) 不需臨櫃辦理。
第 2 級	須識別申請者是實際存在的個體，並能連結到真實世界的真實身分。 (1) 可不做證件核對。 (2) 申請者提交個人資料，例如個人識別碼(如身分證字號、護照號碼)、姓名等，本管理中心有權與政府提供之資料庫或可信賴之第三者資料庫的登記資料進行比對，以確認申請者之身分。 (3) 不需臨櫃辦理。
第 3 級	個人身分鑑別方式可分為臨櫃辦理與非臨櫃辦理： (1) 臨櫃辦理： 申請者必須親臨辦理並檢具政府機關單位核發且附照片之相關身分證明文件(如國民身分證、護照或健

保證等級	個人身分鑑別之程序
	保卡)供憑證機構或註冊中心查驗，若申請者無法親自臨櫃辦理，得以委託書委任代理人代為臨櫃申請，非本國國民依照相關業務規範辦理，詳細作業程序於各註冊中心內控制度中制訂。 如申請者(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(例如戶口名薄)取代，並由 1 位完全行為能力人以書面保證申請者之身分；出具保證之成年人之身分必須經過上述之鑑別。 (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) 透過自然人憑證 IC 卡申請。 (b) 委由申請公司之代表人確認用戶身分。 (c) 用戶檢附律師、會計師之證明文件正本，經函證確認。 (d) 其他經憑證信賴者的主管機關所認可之非臨櫃開戶的身分識別機制。 (e) 使用本基礎建設簽發之保證等級第 3 級個人憑證。 (f) 經由本管理中心所信賴人員訪視確認，並比對申請者檢具之政府機關單位核發且附照片之相關身分證明文件。

3.2.4 未經驗證之用戶資訊

保證等級第 1 級之憑證不需要驗證憑證申請者的法定名稱，因此憑證主體唯一識別名稱僅放電子郵件地址於通用名稱(CommonName)欄位。

3.2.5 授權之確認

當某個個人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，本管理中心或註冊中心應進行授權之確認

(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、簡訊、傳真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。

驗證申請人有辦法控制其將記載於憑證主體別名之電子郵件地址可採以下方式：

(1) 註冊中心寄送包含隨機值之電子郵件至將包含於憑證主體別名欄位之電子郵件地址，並透過收到使用該隨機值的確認回應，確認申請人對電子郵件地址之擁有權或控制權。或

(2) 依照 Baseline Requirements 第 3.2.2.4 節網域驗證之規定，驗證申請人具備電子郵件地址之經授權網域名稱的擁有權或控制權。再透過組織之人事資料庫、目錄服務或 LDAP 服務取得將記載於憑證主體的資訊與其電子郵件地址。或由組織之初審註冊窗口提交電子郵件地址及申請者之身分識別資訊。

3.2.6 互運之準則

本管理中心非根憑證機構，故不適用。

3.2.7 資料正確性

在使用任何資料來源作為可靠資料來源之前，本管理中心應評估此來源的可靠性、正確性和對變更或偽造的抵抗性。本管理中心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) 資料提供者和資料收集的目的。

(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。

3.3 金鑰更換請求之識別與鑑別

當用戶私密金鑰使用期限到期需要更換金鑰時，可進行憑證更換金鑰作業，由用戶重新申請憑證，依照第 3.2 節規定進行識別及鑑別。

3.3.1 例行性金鑰更換之識別與鑑別

用戶申請憑證即將到期前兩個月，系統將寄送電子郵件提醒用戶重新申請憑證，註冊中心依照第 3.2 節規定，對於憑證將到期重新申請憑證之用戶進行識別及鑑別。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。

3.3.2 憑證廢止之金鑰更換

如用戶之私密金鑰因憑證廢止必須更換金鑰時，應向本管理中心重新申請憑證，註冊中心將依照第 3.2 節規定，對於重新申請憑證之用戶進行識別及鑑別。

3.4 憑證廢止請求之識別與鑑別

本管理中心或註冊中心必須對於憑證廢止申請進行鑑別，以確認申請者為有權提出憑證廢止之申請者，憑證廢止申請之鑑別程序與第 3.2 節規定相同。

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

組織或個人可提出憑證之申請。

4.1.2 註冊程序與責任

本管理中心與註冊中心負責確保憑證申請者的身分在憑證簽發前依據憑證政策與本作業基準之規定確認，憑證申請者要負責提供足夠充分與正確的資訊(如依據申請的憑證類別填寫組織之法定名稱與代碼、憑證申請者之姓名或擁有的電子郵件位地址)與身分證明文件給註冊中心與本管理中心在憑證簽發前執行必要的身分識別與鑑別工作。用戶應負以下之責任：

(1) 用戶應遵守本作業基準憑證申請之相關規定，並確認所提供申請資料之正確性。

(2) 本管理中心同意憑證申請並簽發憑證後，用戶應依照第4.4節規定接受憑證。

(3) 用戶在取得本管理中心所簽發之憑證後，應確認憑證內容資訊之正確性，並依照第1.4.1節規定使用憑證，如憑證內容資訊有誤，用戶應通知註冊中心，並不得使用該憑證。

(4) 用戶應妥善保管及使用其私密金鑰。

(5) 用戶之憑證如須廢止或重發，應依照第4章規定辦理。如發生私密金鑰資料外洩或遺失等情形，必須廢止憑證時，應儘速通知註冊中心，但用戶仍應承擔異動前所有使用該憑證之法律責任。

(6) 用戶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，用戶應自行承擔責任。

(7) 本管理中心如因故無法正常運作時，用戶應儘速尋求其他途徑完成與他人應為之法律行為，不得以本管理中心無法正常運作，作為抗辯他人之事由。

4.2 憑證申請之程序

憑證申請步驟如下：

(1) 憑證申請者填寫憑證申請資料並同意用戶約定條款。

(2) 憑證申請者將憑證申請資料及相關證明資料傳送給註冊中心。

(3) 如憑證申請者自行產製金鑰，須產生PKCS#10憑證申請檔並以私密金鑰加以簽章，於申請憑證時將該憑證申請檔交給註冊中心。

4.2.1 執行識別與鑑別

本管理中心及註冊中心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的規定。初始註冊程序依照憑證實務作業基準第 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。由憑證申請者提供之資訊及於申請過程中之聯繫紀錄由本管理中心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。

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，本管理中心及註冊中心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，本管理中心及註冊中心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，本管理中心及註冊中心得因其他原因不同意簽發憑證。本管理中心及註冊中心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

本管理中心及註冊中心將在合理時間內完成憑證申請之受理。註冊中心在申請者提交的資料齊全且符合憑證政策、憑證實務作業基準及各項查核要求下，註冊審驗窗口會儘速完成憑證申請之審核。註冊中心處理憑證申請的時間及管理中心簽發憑證的時間視不同憑證群組與類別，可能於用戶約定條款、契約或註冊中心網站揭露。

S/MIME 憑證之申請件在收件且符合相關規定下，2 個工作天內由憑證註冊窗口人員完成審核程序，請用戶進行憑證接受，憑證接受後，本管理中心將於 1 個工作天內完成憑證簽發之作業。

4.3 憑證簽發

4.3.1 憑證簽發時憑證機構之作業

本管理中心及其註冊中心在接到憑證申請資料後，即依本作業基準第 3 章之規定，進行相關的審核程序，以作為判定是否同意簽發憑證之依據。

簽發憑證步驟如下：

(1) 註冊中心將審核通過之憑證申請資料傳送至本管理中心。

(2) 本管理中心接獲註冊中心送來之憑證申請資料時，先查驗相

關註冊中心之授權狀態，確認其被授權之保證等級與範圍，再依據註冊中心所送之憑證申請資料簽發憑證。

(3) 若註冊中心被授權之保證等級與範圍與憑證申請不符時，本管理中心將回傳相關錯誤信息給註冊中心，並拒絕後續相關作業；若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。

(4) 為確保本管理中心及註冊中心間傳輸資料之安全、完整及不可否認性，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協定加密傳送。

(5) 本管理中心保有拒絕簽發憑證給任何個體之權利，本管理中心拒絕簽發憑證對憑證申請者不負任何損害賠償責任。

4.3.2 對用戶之通告

本管理中心完成憑證簽發後，將通知用戶領取憑證或是透過註冊中心通知用戶領取憑證。

本管理中心或註冊中心如不同意簽發憑證，會以電子郵件或電話通知憑證申請者，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，得因其他原因不同意簽發憑證。

4.4 憑證接受

本管理中心所簽發憑證其接受憑證之程序分為兩類：

(1) 憑證申請者預先審視將簽發之憑證內容，憑證申請者審視憑證將註記之資訊是否正確且與申請時提供之資料一致，若憑證申請者審視將簽發之憑證內容後，拒絕接受將註記於憑證之資訊，則憑證不予簽發。另依照第 4.2 節重新提出憑證申

請。

(2) 本管理中心完成憑證簽發後，將通知憑證申請者領取憑證，憑證申請者審視憑證註記之資訊是否正確且與申請時提供之資料一致，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。若憑證申請者審視已經簽發之憑證內容後，拒絕接受所簽發的憑證，本管理中心將廢止該憑證。

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及憑證主體別名欄位所註記之電子郵件地址與申請時提供之資料一致。

接受憑證視為憑證申請者同意遵守本作業基準或相關合約上之權利與義務。

憑證申請者拒絕接受憑證，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所訂定之契約辦理。

4.4.1 構成接受憑證之事由

憑證申請者預先審視將簽發之憑證內容或審視憑證內容無誤，憑證經本管理中心公布於儲存庫或傳遞給憑證申請者。

4.4.2 本管理中心之憑證發布

本管理中心的儲存庫服務定期公布所簽發之憑證或是藉由將憑證傳遞給憑證申請者達成憑證之發布。註冊中心得與本管理中心協議將憑證透過註冊中心傳遞給憑證申請者。

4.4.3 本管理中心對其他個體之簽發通知

不做規定。

4.5 金鑰對與憑證之用途

4.5.1 用戶私密金鑰與憑證之用途

用戶係指已申請並取得本管理中心核發憑證之個體，其與憑證主體之關係如本作業基準第 1.3.3 節表格所示，不同保證等級憑證之應用範圍如本作業基準第 1.4.1 節所示，用戶金鑰對的產製應符合本作業基準第 6.1.1 節之規定，並且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，用戶本身不簽發憑證給其他方。用戶應保護其私密金鑰不被他人未經授權的使用或揭露，且只使用其私密金鑰於正確的金鑰用途(於憑證之擴充欄位有註記金鑰用途)，如 digitalSignature 或 keyEncipherment。用戶必須依據憑證所記載的憑證政策(certificatePolicies)正確地應用憑證。

4.5.2 信賴憑證者公開金鑰與憑證之用途

信賴憑證者係指相信憑證主體名稱與公開金鑰間連結關係之第三人。信賴憑證者應使用符合 ITU-T X.509、IETF RFCs 及 S/MIME certificate profile requirements of Google 相關標準或規範的軟體。

信賴憑證者必須依照相對的憑證機構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) 驗證電子郵件數位簽章產生者的身分

(2) 驗證具有數位簽章的電子郵件之完整性

(3) 加密電子郵件訊息

前述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，憑證廢止清冊發布點(cRLDistributionPoints)的位置可在憑證的詳細資訊取得。此外，信賴憑證者也應檢驗簽發憑證機構與用

戶憑證之 certificatePolicies 欄位內容，確認憑證之保證等級。

例如信賴憑證者只有以下條件符合下才能相信數位簽章：

(1) 數位簽章是透過相對應有效的憑證產生，且能透過憑證串鏈驗證憑證之正確性。

(2) 憑證並未被廢止且信賴憑證者在使用憑證前透過相關的憑證廢止清冊或線上憑證狀態協定回應訊息(OCSP Response)進行檢查。

(3) 憑證依據其憑證實務作業基準之規定及其憑證用途使用。

4.6 憑證展期

憑證展期(renewal)是指在用戶識別資訊不變下重新簽發 1 張與原有憑證具有相同公開金鑰、相同憑證主體資訊、不同序號但效期展延的憑證。

本管理中心不提供憑證展期之服務，請比照初始註冊另行產製金鑰對提出憑證申請。

4.6.1 憑證展期之情況

不適用。

4.6.2 憑證展期之申請者

不適用。

4.6.3 憑證展期之程序

不適用。

4.6.4 對用戶憑證展期之簽發通知

不適用。

4.6.5 構成接受展期之憑證的事由

不適用。

4.6.6 憑證機構對展期之憑證的發布

不適用。

4.6.7 憑證機構對其他個體之憑證簽發通知

不適用。

4.7 用戶憑證之金鑰更換

4.7.1 憑證金鑰更換之情況

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

持有保證等級第 1、第 2 及第 3 級之用戶，如其憑證沒有被廢止，本管理中心或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第 4.2 節規定辦理。

當用戶的憑證被廢止後，其私密金鑰應停止使用，並於更換金鑰對後，依照第 4.2 節規定向憑證機構或註冊中心申請新憑證。

4.7.2 更換憑證金鑰之申請者

用戶或合法授權之第三人(如組織授權之代理人)。

4.7.3 憑證金鑰更換之程序

用戶之憑證更換金鑰，請向本管理中心重新申請憑證，參見本作業基準第 3.1、3.2、3.3、4.1 及 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

依照第 4.3.2 節規定辦理。

4.7.5 構成接受金鑰更換之憑證的事由

依照第 4.4.1 節規定辦理。

4.7.6 憑證機構對金鑰更換之憑證的發布

依照第 4.4.2 節規定辦理。

4.7.7 憑證機構對其他個體之憑證簽發通知

依照第 4.4.3 節規定辦理。

4.8 憑證變更

4.8.1 憑證變更之情況

用戶如有變更組織名稱、個人的姓名、身分證字號或電子郵件地址等重要的身分資料時，則原憑證必須廢止，用戶須以變更後的組織名稱、姓名或身分證字號進行憑證的重新申請以取得有效的憑證。申請憑證時，依第 4.1 與 4.2 節規定的程序做辦理。本管理中心不提供憑證變更之服務。

4.8.2 憑證變更之申請者

不適用。

4.8.3 憑證變更之程序

不適用。

4.8.4 對用戶憑證變更之簽發通知

不適用。

4.8.5 構成接受變更之憑證的事由

不適用。

4.8.6 憑證機構對變更之憑證的發布

不適用。

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 憑證廢止與停用

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。

4.9.1 廢止憑證之情況

以下幾種情況發生時，本管理中心應於 24 小時內廢止憑證：

(1) 用戶以書面提交本管理中心同意廢止憑證

(2) 用戶告知本管理中心原有之憑證請求未經授權

(3) 本管理中心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) 得知一種經過驗證或證明的方法，可以根據憑證中的公鑰輕鬆計算用戶的私鑰

(5) 本管理中心證實憑證中所記載之電子郵件地址在擁有權或控制權之驗證上是不可信賴的

以下幾種情況發生時，本管理中心最遲於 5 天內廢止憑證：

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

(2) 本管理中心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) 安全電子郵件憑證中所記載之經授權網域名稱已被禁用(可能原因如網域名稱遭司法機關註銷或與網域名稱受理註冊機構(Domain Name Registrar)之間的授權或合約到期)

(5) 安全電子郵件憑證被用於詐欺或釣魚郵件用途

(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) 憑證未依憑證政策或本作業基準之規定程序簽發時

(8) 憑證中所記載之資訊不準確(inaccurate)

(9) 本管理中心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) 憑證政策或本作業基準所規定應廢止項目

(11) 獲悉已證明或經過驗證的方法會暴露用戶的私鑰，或者有明確的證據表明用於生成私鑰的特定方法存在缺陷。

(12) 超過繳費期限並經催繳後，用戶仍未繳納憑證費用

(13) 對於安全電子郵件憑證，憑證機構收到通知或以其他方式得知有任何情況表明不再合法使用憑證所記載的電子郵件地址

本管理中心依照上述應廢止憑證之情況，得逕行廢止用戶憑證。

4.9.2 憑證廢止之申請者

用戶、本管理中心、註冊中心或合法授權之第三人(如司法或檢調機關、組織授權之代理人、自然人之法定繼承人)。

此外，用戶、信賴憑證者、應用軟體廠商或其他第三方可提交憑證問題報告知會本管理中心合理之原因以廢止憑證。

4.9.3 憑證廢止之程序

(1)憑證廢止申請者依據註冊中心制定之作業規範提出憑證廢止請求，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。

(2)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)本管理中心接獲註冊中心送來之憑證廢止申請資料時，先查驗註冊中心之授權狀態，確認其被授權之保證等級與範圍，再依據註冊中心所送之憑證廢止請求廢止該憑證。

(4)如以上之查驗不通過時，本管理中心將回傳相關錯誤信息給註冊中心，並拒絕後續相關作業；若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。

(5)為確保本管理中心及註冊中心間傳輸資料之安全、完整及不可否認性，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協定加密傳送。

(6)本管理中心使用與簽發憑證時相同的管理中心私密金鑰將廢止憑證序號與憑證廢止理由等資訊經由數位簽章後記載於憑證廢止清冊。

(7)提供更即時的線上憑證狀態協定查詢服務(亦即除了已廢止外也有申請中或正常之狀態)。

(8)本管理中心提供 7 天 x 24 小時之憑證問題通報受理以及憑證問題回應機制如第 4.9.3.1 節所述。

4.9.3.1 憑證問題回應機制

本管理中心於網站儲存庫之「憑證實務作業基準公告事項」項目下，提供憑證問題回報之指引說明，供用戶、應用軟體廠商、信賴憑證者以及其他第三方組織於發現疑似私密金鑰遭破解、憑證被誤用、或是憑證被偽造、破解、濫用或不當使用等情形時，可透過第 1.5.2.2 節之聯絡資訊向本管理中心提出憑證問題報告。

4.9.4 憑證廢止請求之寬限期

憑證廢止請求的寬限期是指用戶在憑證廢止事由已經確認而必須提出憑證廢止申請的時間。註冊中心必須在 1 小時內通報本管理中心其註冊中心私密金鑰疑似遭破解的事由。用戶在其私密金鑰遺失或疑似遭破解或已被破解或是憑證所記載之資訊已經過時不正確時，應儘速向註冊中心提出憑證廢止之申請，憑證廢止請求之寬限期為 2 個工作天，本管理中心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

在接收到憑證問題報告的 24 小時內，應調查有關的事實及情況，並提供 1 份初步的調查報告給用戶及報告回報者。

在審視有關的事實及情況後，本管理中心應與用戶及憑證問題報告(或其他憑證廢止通知)之回報者共同確認該憑證廢止請求是否成立。若憑證廢止請求經確認後成立，應於第 4.9.1 節規範之處理期限內完

成憑證廢止作業。憑證廢止之處理期限應考量下述準則：

(1) 聲稱問題的內容(包括範圍、過程、嚴重程度、重要性及危害的風險等)。

(2) 憑證廢止的後果(對用戶或信賴憑證者直接或間接的影響)

(3) 該憑證或用戶的憑證問題報告數量。

(4) 提出憑證問題報告的單位。

(5) 相關的法律條文。

4.9.6 信賴憑證者檢查憑證廢止之規定

信賴憑證者使用本管理中心所簽發之憑證前，應先檢驗本管理中心公布之憑證廢止清冊或線上憑證狀態協定回應訊息，以確定該憑證是否有效。信賴憑證者應檢驗憑證廢止時間、憑證廢止清冊或線上憑證狀態協定回應訊息之簽章有效性、憑證串鏈及其有效性等資訊。

本管理中心於儲存庫公開暫停使用及廢止之憑證資料，以供查核，對於信賴憑證者查驗憑證廢止清冊無任何限制，網址如下：

http://smimeca.hinet.net

4.9.7 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至少每天 2 次，所簽發的憑證廢止清冊之有效期限不超過 36 小時。在憑證廢止清冊尚未過期前，本管理中心即可能簽發新的憑證廢止清冊，因此新憑證廢止清冊的效期與舊的憑證廢止清冊的效期會可能有所重疊，在效期重疊期間，即使舊的憑證廢止清冊尚未過期，信賴憑證者仍可至本管理中心儲存庫取得新的憑證廢止清冊，以獲得更即時的憑證廢止資訊。

4.9.8 憑證廢止清冊發布之最大延遲時間

本管理中心產製憑證廢止清冊後立即發佈，系統無預簽行為。

4.9.9 線上憑證廢止與狀態查驗之可用性

本管理中心以憑證廢止清冊、網頁式之憑證查詢與下載及線上憑證狀態協定回應訊息等方式提供憑證之廢止/狀態查詢。

本管理中心由線上憑證狀態協定回應伺服器(OCSP Responder)提供符合 RFC 6960 及 RFC 5019 標準規範的線上憑證狀態協定(OCSP)回應訊息，本管理中心簽章用私密金鑰使用 RSA-4096 或其以上 w/SHA-256 雜湊函數演算法簽發線上憑證狀態協定回應伺服器之憑證以供信賴憑證者驗證 OCSP 回應訊息的數位簽章，確認資料來源之完整性。

4.9.10 線上憑證廢止查驗之規定

信賴憑證者應依照第 4.9.6 節之規定查詢憑證廢止清冊或依照第 4.9.9 節使用線上憑證狀態協定服務，檢驗所使用的憑證是否有效。

線上憑證狀態協定回應伺服器採 RSA-2048 併同 SHA-256 演算法簽發線上憑證狀態協定回應訊息。

本管理中心提供線上憑證狀態協定查詢服務，其可支援符合 RFC 6960 及 RFC 5019 標準規範所述之 HTTP-based 的 POST 與 GET 方法。

本管理中心之 OCSP 的更新頻率為每小時至少更新 1 次，OCSP 服務的回應訊息效期 8 小時以上且 16 小時以下。信賴憑證者透過本管理中心所提供之 OCSP 回應訊息查驗憑證前應先查看 nextUpdate 之資訊，並自行衡量是否信賴該資訊。

線上憑證狀態協定查詢封包內含之憑證序號可分為三種，分別為「已分配(Assigned)」、「已保留(Reserved)」及「未使用(Unused)」。「已分配」之憑證序號意即為本管理中心已簽發憑證之憑證序號，「已保留」之憑證序號為簽發 TLS/SSL 憑證所需之預簽憑證(Precertificate)的憑證序號，不符合前述條件之憑證序號皆屬於「未使用」之憑證序號。本管理中心不提供 TLS/SSL 憑證之簽發，故未簽發預簽憑證。換言之，本管理中心之線上憑證狀態協定回應伺服器可處理之線上憑證狀態協定查詢封包應僅包含「已分配」或「未使用」等兩種憑證序號。

若線上憑證狀態協定回應伺服器接收到查詢「已分配」之憑證序號的線上憑證狀態協定查詢封包時，應依該憑證序號所對應之憑證當時之狀態回覆。若線上憑證狀態協定回應伺服器接收到查詢「未使用」之憑證序號的線上憑證狀態協定查詢封包時，不可回覆其狀態為「正常(Good)」，並且本管理中心應監督線上憑證狀態協定回應伺服器對於這類請求的回覆是否符合上述安全回應程序。

4.9.11 廢止公告之其他發布形式

本管理中心根據 RFC 4366 支援線上憑證狀態協定裝訂(OCSP Stapling)。

4.9.12 金鑰被破解時之特殊規定

如果用戶確認私密金鑰遭破解，用戶必須立即通知本管理中心依照本作業基準第 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。

若本管理中心私密金鑰遭破解，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) 由本管理中心提供隨機值或文件，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 暫時停用憑證之情況

不提供停用憑證服務。

4.9.14 暫時停用憑證之申請者

不適用。

4.9.15 暫時停用憑證之程序

不適用。

4.9.16 憑證暫時停用期間之限制

不適用。

4.9.17 恢復使用憑證之程序

不適用。

4.10 憑證狀態服務

4.10.1 操作特性

本管理中心提供憑證廢止清冊服務，且憑證廢止清冊服務的 HTTP URL 註記於用戶憑證的 cRLDistributionPoints 擴充欄位，本管理中心並提供線上憑證狀態協定查詢服務。

CRL 或 OCSP 所回應之某張憑證廢止紀錄的訊息，直到該被廢止憑證的效期已到，才會被移除。

4.10.2 服務可用性

本管理中心提供 7 天 x 24 小時不中斷之憑證狀態服務，使應用軟體隨時可針對未過期憑證進行檢查。

本管理中心提供 7 天 x 24 小時對於高優先權的憑證問題報告之內部回應機制，並適時地轉交給執法機關或進行憑證廢止。

4.10.3 可選功能

不做規定。

4.11 訂購終止

訂購終止(End of Subscription)是指用戶終止使用本管理中心的服務。本管理中心允許用戶藉由廢止憑證、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 金鑰託管與回復之政策及實務

本管理中心不會對自身及用戶簽章用的私密金鑰託管(Key Escrowed)。

4.12.2 會議金鑰封裝與回復政策及實務

本管理中心並未支援會議金鑰(Session Key)封裝及回復(Encapsulation and Recovery) 。

5 憑證機構設施、管理及操作控管

5.1 實體控管

5.1.1 所在位置與結構

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。

本管理中心機房總共有 4 層門禁，第 1 層和第 2 層分別為全年無休的大門及大樓警衛，第 3 層為樓層讀卡機進出管制系統，第 4 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，須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，須填寫進出紀錄，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，將進行以下之查驗工作並記錄，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 電源與空調

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。

5.1.4 水災防範

本管理中心機房設置在基地墊高建築物的第 3 樓層(含)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 火災防範與保護

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除了儲存一份在第 5.1.1 節所述的場所，另將複製 1 份在安全場所。

5.1.7 廢料處理

第 9.3.1 節所記載本管理中心的文件資料不需要使用時，都要經過碎紙機處理。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。

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與系統程式。

5.2 程序控管

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 7 個不同的 PKI 人員角色，分別為管理員(Administrator)、簽發員(CA Officer)、稽核員(Internal Auditor)、維運員(System Operator)、實體安全控管員(Physical Security Controller)、網路安全專員(Cyber Security Coordinator)和防毒防駭專員(Anti-virus and Anti-hacking Coordinator)，以抵擋可能的內部攻擊。一個角色的工

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 7 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：

- 對稽核紀錄的查驗、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。
- 網站的維護
- 建置系統安全與病毒或惡意軟體等威脅之防護機制。

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)。

網路安全專員負責：

- 網路和網路設備的維護。
- 網路設備之弱點修補作業。
- 本管理中心之網路安全。
- 網路安全事件的偵測與通報。

防毒防駭專員負責：

- 研議、應用或提供防毒防駭、防惡意軟體等威脅之技術或措施，以確保系統和網路之安全。
- 將蒐集之電腦病毒之威脅或弱點通報管理員或網路安全專員進行修補。

5.2.2 每項任務所需之人數

根據各個工作角色的作業安全需求，訂定各個工作角色所需的人數如下：

- 管理員

  共需要有至少 3 位合格的人員來擔任。

- 簽發員

  共需要有至少 2 位合格的人員來擔任。

- 稽核員

  共需要有 2 位合格的人員來擔任。

- 維運員

  需要有 2 位合格的人員來擔任。

- 實體安全控管員

  需要有 2 位合格的人員來擔任。

- 網路安全專員

至少 1 位合格人員擔任。

■ 防毒防駭專員

至少 1 位合格人員擔任。

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	網路安全專員	防毒防駭專員
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		
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		
對稽核紀錄的查驗、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		
網站的維護				1	1		
網路和網路設備的日常運作維護				1	1	1	
網路設備之弱點修補作業	1				1	1	

任務項目	管理員	簽發員	稽核員	維運員	實體安全控管員	網路安全專員	防毒防駭專員
電腦病毒威脅與弱點之通報事項							1
系統病毒碼與弱點之修補作業				1	1		

5.2.3 識別與鑑別每個角色

使用 IC 卡識別及鑑別管理員、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。註冊審驗人員登入註冊中心系統及進行相關審驗動作，必須使用 IC 卡進行身分鑑別與數位簽章。

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。本管理中心利用使用者帳號、通行碼和群組之系統帳號管理功能或其他安全機制識別網路安全專員之角色。

5.2.4 需要職責分離之角色

本管理中心角色分依照第 5.2.1 節定義的 7 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、稽核員和網路安全專員 4 種信賴角色不得相互兼任，但管理員、簽發員、稽核員可兼任維運員。
- 實體安全控管員不得兼任管理員、簽發員、稽核員和維運員。

無論在任何條件下，任何 1 個角色，都不可以執行自我稽核功能，不允許自己稽核自己。

5.3 人員控管

5.3.1 資格、經驗及清白規定

(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：

(a) 個人性格之評估。

(b) 申請者經歷之評估。

(c) 學術及專業能力及資格之評估。

(d) 人員身分之確認。

(e) 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洩漏營業秘密。

5.3.2 背景調查程序

本管理中心對於第 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。

5.3.3 教育訓練規定

角色	教育訓練規定
管理員	(1) 本管理中心安全原理和機制。 (2) 本管理中心安裝、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) 災後復原以及業務永續經營之程序。
簽發員	(1) 本管理中心安全原理和機制。 (2) 本管理中心系統軟硬體的使用及操作程序。 (3) 啟動/停止憑證簽發之操作程序。 (4) 啟動/停止憑證廢止之操作程序。 (5) 啟動/停止憑證廢止清冊簽發服務之操作程序。 (6) 災後復原以及業務永續經營之程序。
稽核員	(1) 本管理中心安全原理和機制。 (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) 對稽核紀錄的查驗、維護和歸檔程序。 (5) 災後復原以及業務永續經營之程序。
維運員	(1) 系統設備的日常運作維護程序。 (2) 系統的備援及復原作業程序。 (3) 儲存媒體的更新程序。 (4) 災後復原以及業務永續經營之程序。 (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) 災後復原以及業務永續經營之程序。

角色	教育訓練規定
網路安全專員	(1) 網路和網路設備的維護程序。 (2) 網路安全機制。
防毒防駭專員	(1) 電腦病毒威脅與弱點及其防制。 (2) 作業系統與網路之安全機制。

5.3.4 再教育訓練頻率與規定

本管理中心的每一位相關工作人員，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，於 1 個月內要安排適當的教育訓練時間實施再訓練並做記錄，以適應新的工作程序及法規的運作。

5.3.5 工作輪調之頻率及順序

(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、簽發員及稽核員等工作人員等如果是未兼任維運員工作的人員，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。

(4) 擔任網路安全專員滿 2 年，且已接受相關教育訓練及通過審核，才可轉任管理員、簽發員及稽核員。

(5) 擔任防毒防駭專員滿 2 年，且已接受相關教育訓練及通過審核，才可轉任管理員、簽發員及稽核員。

5.3.6 未授權行為之裁罰

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 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。

5.3.8 提供給人員之文件

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。

5.4 稽核紀錄程序

可稽核事件之安全稽核紀錄遵循第 5.5.2 節所述之歸檔保留期間的維護方式進行。

5.4.1 被記錄事件種類

(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

- 憑證之註冊申請過程。

(4) 廢止憑證

- 憑證之廢止申請過程。

(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

- 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。

5.4.2 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。稽核檢視之結果以文件記錄。

本管理中心每 2 個月檢視稽核紀錄 1 次。

5.4.3 稽核紀錄檔保留期限

稽核資料現場保留兩個月，依第 5.4.4 節、5.4.5 節及 5.4.6 節所描述做為資料保留的管理機制。

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。

5.4.4 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。

5.4.5 稽核紀錄檔備份程序

電子式稽核紀錄至少每月備份 1 次。

(1) 本管理中心週期性的將事件日誌歸檔。

(2) 本管理中心將事件日誌檔案存放於安全保險場所。

5.4.6 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。

5.4.7 對引起事件者之通知

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。

5.4.8 弱點評估

憑證註冊中心系統每年應進行弱點掃描至少 1 次，並進行相關的補強措施。

本管理中心每季執行弱點評估至少 1 次，每年執行滲透測試至少 1 次。本管理中心於滲透測試與弱點評估後進行補強與矯正措施。本管理中心於認定應用程式或基礎設施(Infrastructure)重大更新或變更

後,也須執行滲透測試。本管理中心針對足以執行可信賴的弱點掃瞄、滲透測試、資安健診或安全監控之人員或團體，記錄其技能、工具、遵循之道德倫理規範、競業關係以及獨立性。

5.5 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、廢止及重發等之重要追蹤紀錄。

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，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。

5.5.1 歸檔紀錄之種類

本管理中心記錄的歸檔資料有：

(1) 本管理中心被主管機關認證(Accreditation)的資料

(2) 憑證實務作業基準

(3) 重要的契約

(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) 憑證申請的資料

(7) 廢止申請的資料

(8) 如第 3.2 節所訂定的用戶身分識別資料

(9) 所有已簽發或公告的憑證

(10)本管理中心金鑰更換的紀錄

(11)所有被簽發或公告的憑證廢止清冊

(12)所有的稽核紀錄

(13)用來驗證及佐證歸檔內容的其他資料或應用程式

(14)稽核者所要求的文件

5.5.2 歸檔資料保留期限

本管理中心最少要保留歸檔資料的時間為 2 年。用來處理歸檔資料的應用程式也被維護 10 年。

5.5.3 歸檔資料之保護

(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) 歸檔的資料存放於安全保險場所。

5.5.4 歸檔資料備份程序

本管理中心之電子式紀錄將依照備份程序，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。

5.5.5 紀錄之時戳規定

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、憑證廢止清冊及稽核紀錄等)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，可用以檢測紀錄中的日期與時間資訊是否遭到篡改。

5.5.6 歸檔資料彙整系統

目前沒有歸檔資料彙整系統。

5.5.7 取得與驗證歸檔資料之程序

在獲取憑證機構歸檔資訊時，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，由稽核員進行驗證的程序，如為書面文件必須驗證文件簽署者及日期等的真偽。

5.6 憑證機構之金鑰更換

本管理中心之私密金鑰依照第 6.3.2 節規定定期更換，最遲應於其私密金鑰簽發用戶憑證用途的使用期限到期前，更換用來簽發憑證的金鑰對。更換金鑰對後，以新金鑰對向上層憑證機構(中華電信憑證總管理中心)申請新的憑證機構憑證，並公布於儲存庫，提供用戶或信賴憑證者下載。

本管理中心以新私密金鑰簽發用戶之憑證及憑證廢止清冊時，舊私密金鑰仍須簽發憑證廢止清冊或線上憑證狀態協定回應訊息，維持與保護至以舊私密金鑰簽發的所有用戶憑證到期為止。

如本管理中心本身的憑證被廢止後，其私密金鑰應停止使用，並須更換金鑰對。

5.7 遭破解與災變之復原

5.7.1 緊急事件與系統遭破解之處理程序

本管理中心訂定緊急事件及系統遭破解之處理程序，同時每年進行演練。

5.7.2 電腦資源、軟體或資料遭破壞

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。

5.7.3 憑證機構私密金鑰遭破解之處理程序

如本管理中心簽章金鑰遭破解，應先通知政策管理委員會、總管理中心及應用軟體供應商，並採取以下處理程序：

(1) 公告於儲存庫，通知用戶及信賴憑證者。

(2) 廢止本管理中心簽章金鑰憑證及所簽發之用戶憑證。

(3) 依照第 5.6 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。

本管理中心每年至少進行 1 次本管理中心簽章金鑰遭破解之演練。

5.7.4 災變後業務持續營運能力

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。

5.8 憑證機構或註冊中心之終止服務

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機構終止服務的程序。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，安排其他憑證機構承接此業務。並將終止服務及由其他憑證機構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機構。
- 若無憑證機構願承接本管理中心之業務，將陳報主管機關安排其他憑證機構承接。
- 若經主管機關安排其他憑證機構承接，仍無其他憑證機構承接時，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，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。

註冊中心終止服務時，由本管理中心停止其審驗憑證之權利。

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 金鑰對之產製

本管理中心及其用戶使用第 6.2.1 節規定之安全密碼模組產製虛擬隨機亂數和公開金鑰對。

本管理中心依照第 6.2.1 節規定,於硬體密碼模組內產製金鑰對,採依照 NIST FIPS 140-2 規範之演算法與流程，私密金鑰之匯出與匯入應依照第 6.2.2 與 6.2.6 節規定辦理。

本管理中心之金鑰產製由相關人員見證及錄影留存,並簽署金鑰產製見證書(記載產製的金鑰對之公開金鑰)，相關人員應包含政策管理委員會之委員及本管理中心之稽核員。

6.1.1.1 用戶金鑰對之產製

由卡管中心代用戶產製金鑰對(符記為晶片)或用戶自行產製金鑰對(軟體或硬體密碼模組)。

6.1.2 將私密金鑰傳送給憑證用戶

本管理中心不應代用戶產製金鑰對,如用戶金鑰對由卡管中心代為產製時，註冊中心將於簽發憑證後，透過註冊窗口將含有用戶私密金鑰的符記(例如 IC 卡)交予用戶。

6.1.3 將用戶之公開金鑰傳送給憑證機構

如由卡管中心代用戶產製金鑰對時,則由註冊中心透過安全管道

將用戶之公開金鑰傳送至憑證中心。

如用戶自行產製金鑰對時，則用戶必須以 PKCS#10 憑證申請檔的格式將公開金鑰送給註冊中心，註冊中心依照第 3.2.1 節規定檢驗用戶確實擁有相對應的私密金鑰後，以安全管道將用戶的公開金鑰傳送至憑證中心。

本節所指安全管道為使用傳輸層安全協定或其他相同或更高級之資料加密傳送方式。

6.1.4 將憑證機構之公開金鑰傳送給信賴憑證者

本管理中心本身之公鑰憑證由中華電信憑證總管理中心簽發，公布在本管理中心的儲存庫上，而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鑰憑證前必須依照中華電信憑證總管理中心憑證實務作業基準規定，由安全管道取得中華電信憑證總管理中心之公開金鑰或自簽憑證，然後檢驗中華電信憑證總管理中心對本管理中心本身之公鑰憑證的簽章，以確保公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 4096 位元或其以上的 RSA 金鑰以及 SHA-256 雜湊函數演算法簽發憑證。

到民國 119 年 12 月 31 日(含)之前，用戶必須使用 RSA-2048 位元金鑰或安全強度相當的其他種類金鑰。

民國 119 年 12 月 31 日以後，用戶應使用 RSA-3072 位元金鑰或安全強度相當的其他種類金鑰。

若本管理中心使用橢圓曲線密碼演算法(Elliptic Curve

Cryptography, ECC)簽發憑證將使用符合 NIST P-256 或 P-384 的金鑰長度。

對於 ECDSA 金鑰，本管理中心應使用以下曲線-雜湊對其中之一：P-256 with SHA-256，P-384 with SHA-384。

6.1.6 公開金鑰參數之產製與品質檢驗

RSA 演算法公鑰參數為空的(Null)。

本管理中心簽章用金鑰對採用 NIST FIPS 186-4 之規範產生 RSA 演算法中所需的質數，並確保該質數為強質數(Strong Prime)。

用戶金鑰可於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。

根據 NIST SP 800-89 第 5.3.3 節，本管理中心確認公開指數(public exponent)的值為大於 3 的奇數，且其值介於 2^{16}+1 和 2^{256}-1 之間。此外，模數應具有奇數、非質數的指數次方且沒有小於 752 的因數的性質。

若使用橢圓曲線密碼演算法簽發之憑證，本管理中心將遵循 NIST SP 800-56A Revision 2 第 5.6.2.3.2 與 5.6.2.3.3 節確認所有使用 ECC Full Public Key Validation Routine 與 ECC Partial Public Key Validation Routine 的金鑰之效期。

6.1.7 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及憑證廢止清冊。本管理中心本身之公鑰憑證由中華電信憑證總管理中心簽發；其中 keyUsage 擴充欄位設定使用的 keyUsage 位元為 keyCertSign 及 cRLSign。若本管理中心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，則金鑰用途位元尚須包含 digitalSignature，其他位元不得設定。擴充金鑰用途(extKeyUsage)擴充欄位必須設定 emailProtection，但不得設定 serverAuth、codeSigning、timeStamping、與 anyExtendedKeyUsage。

S/MIME 憑證之 keyUsage 擴充欄位必須包含 digitalSignature 及/或 nonRepudiation，且可設定 dataEncipherment 及/或 keyEncipherment，其他位元不得設定。擴充金鑰用途擴充欄位必須設定 emailProtection，但不得設定 serverAuth、codeSigning、timeStamping、與 anyExtendedKeyUsage。

6.2 私密金鑰保護與密碼模組工程控管

6.2.1 密碼模組標準與控管

本管理中心使用通過FIPS 140-2 Level 3認證之硬體密碼模組。

用戶金鑰對之儲存媒體可為：

儲存媒體類型	通過之認證標準
晶片	FIPS 140-2 Level 2 或 Common Criteria EAL 4+以上等級
硬體密碼模組	FIPS 140-2 Level 3 以上等級
其它載具 (如：軟體)	無

6.2.2 私密金鑰分持之多人控管

本管理中心金鑰分持之多人控管，採 LaGrange 多項式內插法(LaGrange Polynomial Interpolation)的 n-out-of-m(以下簡稱 n-out-of-m)，他是一種完全秘密分享(Perfect Secret Sharing)的方式，可做為私密金鑰分持備份及回復方法；其中，n 與 m 皆須為大於或等於 2 的數值，

且 n 必須小於或等於 m。採用此方法可使本管理中心私密金鑰的多人控管具有最高的安全度，因此也用來做為私密金鑰之啟動方式(參閱第 6.2.8 節)。

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。

6.2.4 私密金鑰備份

依照第 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 FIPS 140-2 Level 2 以上之驗證的 IC 卡做為秘密分持的儲存媒體。

6.2.5 私密金鑰歸檔

本管理中心簽章用私密金鑰不被歸檔，但會以憑證資料的方式依照第 5.5 節執行相對公鑰的歸檔。

6.2.6 私密金鑰匯入、匯出密碼模組

本管理中心在下述情況時會將私密金鑰匯入至密碼模組中：

(1) 金鑰產製。

(2) 金鑰持份備援的回復時。在此情況是以秘密持份(n-out-of-m 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。

(3) 更換密碼模組時，私密金鑰輸入方式採加密方式以確保輸入過程中不得將金鑰明碼暴露於密碼模組之外，私密金鑰輸入完成後，須將輸入過程產製之相關機密參數完全銷毀。

6.2.7 私密金鑰儲存於密碼模組

依照 第 6.1.1 及 6.2.1 節規定辦理。

6.2.8 私密金鑰之啟動方式

本管理中心之私密金鑰之啟動是由多人控管 IC 卡來控制，不同用途的控管 IC 卡由管理員、簽發員所保管。

用戶應慎選安全的電腦環境及可信賴的應用系統，妥善保管及使用其私密金鑰。用戶之私密金鑰啟動方式依照私密金鑰儲存媒體分類如下：

(1) 若為 IC 卡，則私密金鑰之啟動必須(由經鑑別身分之)用戶設定與僅為用戶所知之個人識別碼(以下簡稱為 PIN 碼)啟動。

(2) 若為硬體密碼模組，則私密金鑰之啟動方式，是由多人控管 IC 卡組來控制，不同用途的控管 IC 卡組由不同的人員所保管。

(3) 若為代理郵件伺服器，由用戶自行信賴及託管私密金鑰於該代理郵件伺服器，私密金鑰之啟動方式由該代理郵件伺服器所控制。

(4) 其他私密金鑰載具，用戶應使用強效通行碼或相同等級的鑑別方式啟動私密金鑰以防止未經授權的存取或使用私密金鑰。

6.2.9 私密金鑰之停用方式

本管理中心之私密金鑰採第 6.2.2 節多人控管方法將私密金鑰停用。

本管理中心不提供用戶之私密金鑰停用。

6.2.10 私密金鑰之銷毀方式

為避免舊的本管理中心私密金鑰被盜用，妨害整個憑證之真確性，本管理中心金鑰生命週期到期時其私密金鑰必須加以銷毀，因此，當本管理中心完成金鑰更新及中華電信憑證總管理中心簽發新的本管理中心憑證，且不再簽發任何憑證與憑證廢止清冊之後(參照第 4.7 節)，將會把存在硬體密碼模組內舊的本管理中心私密金鑰做零值化處理(Zeroization)，以便確保銷毀硬體密碼模組中舊的本管理中心私密金鑰。

而除了銷毀硬體密碼模組中舊的本管理中心私密金鑰外，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 1 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 1 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。

6.2.11 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

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 公開金鑰歸檔

本管理中心將進行用戶憑證之歸檔，且依照第 5.5 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 憑證操作與金鑰對之效期

6.3.2.1 本管理中心憑證操作與金鑰對之效期

本管理中心憑證操作及金鑰對之效期為：

憑證類別	私密金鑰效期	憑證效期
本管理中心之憑證機構憑證	■ 簽發用戶憑證：10年 ■ 簽發憑證廢止清冊或線上憑證狀態協定回應伺服器憑證：20年	20年
線上憑證狀態協定回應伺服器憑證	■ 簽發線上憑證狀態協定回應訊息：36小時	36小時

本管理中心每天會公布新的線上憑證狀態協定回應伺服器憑證(透過新的私密金鑰簽署過的線上憑證狀態協定回應訊息包含該憑證給信賴憑證者)。

6.3.2.2 用戶憑證操作與金鑰對之效期

本管理中心用戶之公開金鑰及私密金鑰之金鑰長度為 RSA-2048

位元或其以上，或為 ECC-256 位元或其以上。用戶憑證操作及金鑰對之效期為：

憑證類別	金鑰效期	憑證效期
S/MIME憑證	■ 參照第6.1.7節：小於27個月	小於27個月

6.4 啟動資料

6.4.1 啟動資料之產生與安裝

啟動資料以亂數產生後寫入密碼模組內，並分持至 n-out-of-m 控管 IC 卡中，存取 IC 卡中的啟動資料時必須輸入 IC 卡的 PIN 碼。

6.4.2 啟動資料之保護

啟動資料由 n-out-of-m 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。

6.4.3 啟動資料之其他規範

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) 具備角色或身分鑑別的登入。

(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。

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

本管理中心的系統研發遵循能力成熟度模型整合(Capability Maturity Model Integration, CMMI)的規範進行品質控管。

對於註冊中心之硬體和軟體，必須在初次使用時檢查是否有惡意程式碼。並定期使用工具包括防毒軟體、惡意軟體移除工具掃瞄。

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、與原始程式碼掃瞄報告給本管理中心，並進行程式版本控管。

6.6.2 安全管理控管

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。

本管理中心在風險評鑑、風險處理與安全管理控管措施參考 ISO/IEC 27001、ISO/IEC 27002、ISO/IEC 27005、ISO/IEC 31000、WebTrust Principles and Criteria for Certification Authorities 及 Network and Certificate System Security Requirements 之方法論或規定。

6.6.3 生命週期安全控管

每年至少 1 次評估現行金鑰是否有被破解之風險。

6.7 網路安全控管措施

本管理中心遵循 CA/Browser Forum 的 Network and Certificate System Security Requirements 實施網路安全控管措施。

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。

本管理中心主機所簽發的憑證與憑證廢止清冊以數位簽章保護，自動從本管理中心主機傳送到儲存庫。

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、入侵防禦系統/入侵偵測系統、防火牆系統及過濾路由器(Filtering Router)等加以保護，以防範阻絕服務和入侵等攻擊。

本管理中心監督存取控制權限，持續監督系統健康與安全事件並安排滲透測試。

6.8 時戳

本管理中心定期根據受信賴的時間源進行系統校時，以維持系統時間的正確性，並確保以下時間之正確性：

(1) 用戶憑證簽發時間。

(2) 用戶憑證廢止時間。

(3) 憑證廢止清冊之簽發時間。

(4) 系統事件之發生時間。

可能會使用自動與手動程序來進行系統時間調整，系統校時動作須可被稽核。

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

本管理中心所簽發的憑證會遵循 ITU-T X.509、S/MIME certificate profile requirements of Google、RFC 8550 及 RFC 5280 正式版的規定。

本管理中心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

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遵循 ITU-T X.509、S/MIME certificate profile requirements of Google、RFC 8550 及 RFC 5280 正式版之規定。

7.1.2.1 本管理中心之憑證機構憑證(Subordinate CA Certificate)

總管理中心簽發給本管理中心之下屬憑證機構憑證(Subordinate CA Certificate)的擴充欄位說明如下：

a.憑證政策(certificatePolicies)

此擴充欄位為必要欄位，其標示為非關鍵性(non-critical)欄位，其內容用於註記憑證政策識別碼(policyIdentifier)。可視憑證需求使用憑證政策限定元(policyQualifier)，用於標示總管理中心憑證實務作業基準公告之網址。

b.憑證廢止清冊發布點(cRLDistributionPoints)

此擴充欄位為必要欄位，其標示為非關鍵性(non-critical)欄位，其內容用於註記總管理中心之憑證廢止清冊服務的 HTTP URL。

c.憑證機構資訊存取(authorityInfoAccess)

此擴充欄位為必要欄位，其標示為非關鍵性(non-critical)欄位。其內容用於註記總管理中心 OCSP 回應伺服器的 HTTP URL，其內容也用於註記總管理中心之自簽憑證的 HTTP URL。

d.基本限制(basicConstraints)

此擴充欄位為必要欄位，其標示為關鍵性(critical)欄位。其內容用於註記 cA 欄位值為 true。因本管理中心不再往下簽署下層憑證機構憑證，故 pathLenConstraint 欄位設定為 0。

e.金鑰用途(keyUsage)

此擴充欄位為必要欄位，其標示為關鍵性(critical)欄位，其內容用於註記 keyUsage 位元為 keyCertSign 和 cRLSign。因並非由本管理中心簽章用私密金鑰簽 OCSP 回應訊息，而是經由本管理中心簽發 OCSP 回應伺服器憑證後，由 OCSP 回應伺服器簽發 OCSP 回應訊息，所以設定未使用 digitalSignature。

f.命名限制(nameConstraints)

總管理中心簽發給本管理中心之下屬憑證機構憑證無此選擇性欄位。

g.擴充金鑰用途

此擴充欄位為必要欄位，其標示為非關鍵性(non-critical)欄位，S/MIME 憑證之擴充金鑰用途參見第 6.1.7 節。

7.1.2.2 用戶憑證(Subscriber Certificate)

a.憑證政策(certificatePolicies)

此擴充欄位為必要欄位，其標示為非關鍵性(non-critical)欄位，其內容用於註記憑證政策識別碼(policyIdentifier)。可視憑證需求使用憑證政策限定元(policyQualifier)，用於標示本作業基準公告之網址。

b.憑證廢止清冊發布點(cRLDistributionPoints)

此擴充欄位為必要欄位，其標示為非關鍵性(non-critical)欄位，其內容用於註記本管理中心之憑證廢止清冊服務的 HTTP URL。

c.憑證機構資訊存取(authorityInfoAccess)

此擴充欄位為必要欄位，其標示為非關鍵性(non-critical)欄位。其內容用於註記本管理中心 OCSP 回應伺服器的 HTTP URL，其內容也用於註記本管理中心之憑證的 HTTP URL。

d.基本限制(basicConstraints)

此擴充欄位為選擇性欄位，若有的話，其標示為非關鍵性(non-critical)欄位。其內容用於註記 cA 欄位值為 false，但不得包含 pathLenConstraint 欄位。

e.金鑰用途(keyUsage)

此擴充欄位為必要欄位，其標示為關鍵性(critical)欄位。S/MIME 憑證之 keyUsage 參見第 6.1.7 節。

f.擴充金鑰用途

此擴充欄位為必要欄位，其標示為非關鍵性(non-critical)欄位，S/MIME 憑證之擴充金鑰用途參見第 6.1.7 節。

除非知道包含某些資料於憑證的理由，本管理中心不允許簽發下述兩種情境之憑證：

(1) 憑證的擴充欄位內含無法應用於公眾網路(Public Internet)的設定，例如：擴充金鑰用途擴充欄位包含僅適用於私有網路服務的設定值。

(2) 憑證內容包含可能誤導信賴憑證者相信該憑證資訊已經由本管理中心驗證。

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) sha256WithRSAEncryption(11)}

(OID：1.2.840.113549.1.1.11)

sha384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha384WithRSAEncryption(12)}

(OID：1.2.840.113549.1.1.12)

sha512WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha512WithRSAEncryption(13)}

(OID：1.2.840.113549.1.1.13)

ecdsaWithSHA256	{iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA256(2)}

(OID：1.2.840.10045.4.3.2)

ecdsaWithSHA384	{iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA384(3)}

(OID：1.2.840.10045.4.3.3)

ecdsaWithSHA512	{iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA512(4)}

(OID：1.2.840.10045.4.3.4)

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) rsaEncryption(1)}

(OID: 1.2.840.113549.1.1.1)

ecPublicKey	{iso(1) member-body(2) us(840) ansi-x962(10045) keyType(2) ecPublicKey(1)}

(OID: 1.2.840.10045.2.1)

對於 ECC 演算法，須同時註記下述橢圓曲線參數之物件識別碼：

secp256r1	{iso(1) member-body(2) us(840) ansi-x962(10045) curves(3) prime(1) prime256v1(7)}

(OID: 1.2.840.10045.3.1.7)

secp384r1	{iso(1) identified-organization(3) certicom(132) curve(0) ansip384r1(34)}

(OID: 1.3.132.0.34)

7.1.4 命名形式

憑證中的主體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 ITU-T X.509、S/MIME certificate profile requirements of Google、RFC 8550 及 RFC 5280 正式版的規定。

本管理中心的憑證機構憑證之主體資訊必須包含 countryName (OID 2.5.4.6)欄位，其值為本管理中心所在地之雙字母 ISO 3166-1 國家代碼。除此之外，必須包含 organizationName (OID 2.5.4.10)欄位，其值必須包含可識別本管理中心之名稱、商標或其他有意義的識別名

稱，以供能更準確地識別本管理中心，而不能僅包含通用名稱，例如：CA 1。本管理中心的憑證機構憑證其 X.500 唯一識別名稱參見第 3.1.5 節。

7.1.4.1 簽發者資訊(Issuer Information)

依據 RFC 5280 名稱串鍊(Name chaining)的規定，憑證簽發者之唯一識別名稱欄位(Issuer DN)的內容，必須與簽發該憑證之憑證管理中心的主體唯一識別名稱(Subject DN)相同。故本管理中心簽發的用戶憑證，其簽發者唯一識別名稱欄位內容必須與本管理中心主體的唯一識別名稱欄位內容相同。

7.1.4.2 用戶憑證之主體資訊(Subject Information–Subscriber Certificates)

藉由簽發用戶憑證，表示本管理中心與註冊中心在憑證的簽發日期前已遵循憑證政策和/或憑證實務作業基準所闡述的程序來作驗證，確保所有記載於憑證之主體資訊的值是準確的。此外，憑證主體屬性不得僅包含如「.」、「-」、及「 」(即空格)等詮釋字元，及/或任何其他標示來代表該值不存在、不完整、或不適用。

7.1.4.2.1 主體別名擴充欄位(Subject Alternative Name Extension)

S/MIME 憑證之主體別名擴充欄位如下：

憑證欄位	必要/選擇性擴充欄位
extension:subjectAltName	必要

憑證主體別名欄位必須為 rfc822Name，且不得為 dNSName、iPAddress、與 uniformResourceIdentifier。

主體別名擴充欄位將註記憑證申請案件之電子郵件帳號，應由註冊審驗人員依照第 3.2.5 節進行電子郵件帳號之驗證。

7.1.4.2.2 主體唯一識別名稱欄位(Subject Distinguished Name Fields)

本管理中心所簽發 S/MIME 憑證的主體唯一識別名稱欄位(Subject Distinguished Name Fields)說明如下表：

憑證欄位	第 2, 3 級組織 S/MIME 憑證	第 2, 3 級個人 S/MIME 憑證	第 1 級 S/MIME 憑證
subject:commonName (OID 2.5.4.3)	Δ	Δ	Δ
subject:organizationName (OID 2.5.4.10)	○	Δ	Δ
subject:givenName (OID 2.5.4.42)和 subject:surname (OID 2.5.4.4)	×	Δ	Δ
subject:streetAddress (OID 2.5.4.9)	Δ	Δ	Δ
subject:localityName (OID 2.5.4.7)	Δ	Δ	Δ
subject:stateOrProvinceName (OID 2.5.4.8)	Δ	Δ	Δ
subject:postalCode(OID 2.5.4.17)	Δ	Δ	Δ
subject:countryName(OID 2.5.4.6)	○	○	Δ
subject:organizationUnitName(OID2.5.4.11)	Δ	Δ	Δ

上表之符號說明：

選擇性：Δ　　必要：○　　禁止：×

7.1.4.3 憑證機構憑證之主體資訊(Subject Information–CA Certificates)

本管理中心之憑證機構憑證是由上層的總管理中心依循憑證政策和/或其憑證實務作業基準所闡述的程序來作驗證後簽發。其主體唯一識別名稱欄位(Subject Distinguished Name Field)如下表：

7.1.4.3.1 主體唯一識別名稱欄位(Subject Distinguished Name Field)

憑證欄位	必要/選擇性擴充欄位
subject:commonName (OID 2.5.4.3)	必要
subject:organizationName (OID 2.5.4.10)	必要
subject:countryName(OID 2.5.4.6)	必要

7.1.5 命名限制

不採用命名限制。

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，請參照第 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限制擴充欄位。

7.1.8 政策限定元之語法及語意

可視憑證需求使用憑證政策限定元(policyQualifier)，用於標示本作業基準公告之網址。

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 ITU-T X.509 V2 版本的憑證廢止清冊(CRL)。

7.2.2 憑證廢止清冊與憑證廢止清冊條目之擴充欄位

本管理中心簽發的憑證廢止清冊(CRL)，其憑證廢止清冊擴充欄位(crlExtensions)及憑證廢止清冊條目擴充欄位(crlEntryExtensions)會遵照 ITU-T X.509、S/MIME certificate profile requirements of Google、RFC 8550 及 RFC 5280 正式版之規定。

7.3 線上憑證狀態協定之格式剖繪

本管理中心提供符合 RFC 6960 及 RFC 5019 標準規範之線上憑證狀態協定(OCSP)查詢服務，並在憑證的憑證機構資訊存取(authorityInfoAccess)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
- 待查詢憑證識別碼(Target certificate identifier)

待查詢憑證識別碼包含：雜湊演算法、憑證簽發者名稱之雜湊值、憑證簽發者公開金鑰之雜湊值及待查詢憑證之憑證序號。

OCSP 回應伺服器簽發的線上憑證狀態協定回應封包含有以下基本欄位：

欄位	說明
狀態	回應狀態，包括成功、請求格式錯誤、內部錯誤、稍候重試、請求沒有簽章或請求憑證無授權，當狀態為成功時必須包括以下各項。
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
待查詢憑證識別碼(Target certificate 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	此回應封包建議的效期區間，包含：生效時間

(ThisUpdate/NextUpdate)	(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，為sha256WithRSAEncryption 或 ecdsaWithsha384
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

OCSP 回應伺服器簽發的線上憑證狀態協定回應封包包含有以下擴充欄位：

- OCSP 回應伺服器的憑證機構金鑰識別碼(Authority Key Identifier)
- 此外當 OCSP 請求封包含有隨機數(nonce)欄位時，OCSP 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(OCSP Request) 。

線上憑證狀態協定服務伺服端所使用的 OCSP 回應伺服器憑證為本管理中心所簽發，且必須為短效期之有效憑證，由本管理中心定期簽發與更新。

8 稽核及其他評核

8.1 稽核頻率或評核時機

本管理中心接受 1 年 1 次的外部稽核(且查核期間不可超過 12 個月)與不定期的內部稽核，以確認本管理中心的運作確實遵循憑證政策及本作業基準所訂的安全規定與程序。

8.2 稽核人員身分與資格

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 WebTrust Principles and Criteria for Certification Authorities 標準之合格稽核業者，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 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，本管理中心於稽核時應對稽核人員進行身分識別。

8.3 稽核人員與被稽核方之關係

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。

8.4 稽核範圍

稽核採用的標準為 WebTrust Principles and Criteria for Certification Authorities。

稽核範圍如下所述：

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

(2) 確認註冊中心是否遵照本作業基準及相關程序運作。

(3) 本作業基準所揭露之內容是否與對應之憑證政策相符，且對本管理中心之實務作業而言是否允當。

若有負責審驗保證等級 1 與 2 之憑證之申請或廢止審核的註冊中心，可接受每 2 年 1 次之外部稽核，記錄任何和憑證政策或憑證實務作業基準不符合或例外之事項，並採取行動矯正缺失。

若有負責審驗保證等級 3 之憑證的申請或廢止審核的註冊中心應接受每 1 年 1 次之外部稽核，記錄任何和憑證政策或憑證實務作業基準不符合或例外之事項，並採取行動矯正缺失。

外部註冊中心設立並於本管理中心介接前，由本管理中心派員執行現場調查(Site Survey)以確認相關安控措施執行情形。

若有外部註冊中心因所屬組織或業主之規定或其他因素而未接受前述之外部稽核，可於稽核報告與管理聲明書中說明當年度排除外部稽核之範圍，但本公司保留對於前述外部註冊中心是否遵循憑證政策及本作業基準的符合性查核(compliance audit)權力，以降低任何有不符合憑證政策或憑證實務作業基準衍生的風險。本公司有權執行其他包含但不限於以下項目的查核或調查，以確保本管理中心之公信力：

(1) 若有事件造成本公司合理懷疑外部註冊中心由於電腦緊急事件或金鑰遭破解而無法符合憑證政策與本作業基準。

(2) 在符合性查核有不完整或特殊發現下，本公司有權執行風險管理之查核。

(3) 由於註冊中心的行動或不採取行動造成實際或潛在對於本基礎建設之安全性與完整性之威脅，本公司必須執行相關之查

核或調查。

本公司有權將稽核調查的功能委託第三方稽核業者執行，受稽之外部註冊中心應提供本公司和執行稽核或調查的人員充分而合理之合作。

8.5 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。有關註冊中心之缺失將通知註冊中心改善。

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，本管理中心將公布合格稽核業者所提供之應公開說明資訊。稽核結果以 WebTrust for Certification Authorities 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亦於查核區間結束後 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。

9 其他業務及法律事項

9.1 費用

9.1.1 憑證簽發或展期費用

本管理中心與用戶之間的憑證申請及簽發等計費架構，於相關業務契約條款中訂定，且相關之條款用戶可直接連結至儲存庫查詢。

9.1.2 憑證查詢費用

若有收費，應於相關業務契約條款中訂定。

9.1.3 憑證廢止或狀態查詢費用

若有收費，應於相關業務契約條款中訂定。

9.1.4 其他服務費用

暫不收費。

9.1.5 退費規定

本管理中心所收取之憑證簽發費用，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，本管理中心應退還用戶本項費用。除前述情形及第 4.9 節之情形外，其他費用均不退費。

9.2 財務責任

9.2.1 保險範圍

本管理中心由本公司營運，其財務責任由本公司負責。

9.2.2 其他資產

本管理中心之財務，係屬本公司整體財務之一部分。本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。本公司財務健全，流動資產與流動負債比符合 CA/ Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates 要求不低於 1.0 的要求。

9.2.3 對終端個體之保險或保固責任

對終端個體(用戶及信賴憑證者)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

以下由本管理中心或註冊中心產生、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報告。

(6) 列為機密等級的營運相關文件。

本管理中心及註冊中心之現職及退職人員與各類稽核人員對於機密資訊均嚴守秘密。

9.3.2 非機密之資訊

(1) 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) 本管理中心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不視為機密資訊。

9.3.3 保護機密資訊之責任

本管理中心依照電子簽章法、WebTrust Principles and Criteria for Certification Authorities 稽核標準及個人資料保護法處理本管理中心之用戶申請資料。

9.4 個人資訊之隱私

9.4.1 隱私保護計畫

本管理中心於網站公告個人資料保護與隱私權聲明。本管理中心實施隱私衝擊分析、個資風險評鑑等措施並訂定隱私保護計畫。

9.4.2 隱私之資訊

(1) 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。

(2) 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。

(3) 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特徵與指紋特徵。

(4) 保密協定或契約之個人資訊。

本管理中心及註冊中心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

辨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

配合本管理中心運作所需之個人資料，無論紙本或是電子之形式，必須依照於網站公告的個人資料保護暨隱私權聲明以及個人資料蒐集告知條款，安全存放與受到保護，符合電子簽章法、WebTrust Principles and Criteria for Certification Authorities 稽核標準及個人資料保護法相關規定。本管理中心並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作業基準另有規範，不會將個人資料用於其他地方。用戶得查詢第 9.3.1 節第(3)款用戶本身之申請資料；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。

9.4.6 應法定程序要求釋出資訊

司法機關、監察機關、治安機關或各主管機關如因調查或蒐集證據需要，必須查詢第 9.4.2 節隱私資訊，依法定程序辦理；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。

9.4.7 其他資訊釋出之情況

本管理中心將遵守相關法律規範，不對外揭露以確保用戶個人資料。但法律另有規定時，不在此限。

9.5 智慧財產權

下列項目為本管理中心之智慧財產：

(1) 本管理中心及註冊中心的金鑰對及金鑰分持。

(2) 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。

(3) 本管理中心所簽發的憑證及憑證廢止清冊。

(4) 本作業基準。

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，並註明著作權為本公司所擁有。若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。

9.6 聲明及擔保

9.6.1 憑證機構之聲明與擔保

本管理中心依照本作業基準第 4 章規定之程序執行相關之憑證管理作業。本管理中心聲明及擔保以下之責任：

(1) 遵循憑證政策及本作業基準運作。

(2) 對憑證申請進行識別及鑑別。

(3) 提供簽發及公布憑證服務。

(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協定回應訊息。

(7) 安全產製本管理中心與註冊中心之私密金鑰。

(8) 私密金鑰安全管理。

(9) 依第 6.1.7 節規定使用私密金鑰。

(10) 支援註冊中心進行憑證註冊相關作業。

(11) 對憑證機構與註冊中心人員作識別與鑑別。

9.6.2 註冊中心之聲明與擔保

本管理中心所核發之憑證僅對憑證主體身分做確認，惟其確認程度係當時註冊中心審驗人員之審驗結果，不對用戶之金融信用、財務能力、技術能力、可靠性等作任何擔保。

註冊中心應聲明及擔保：

(1) 對於憑證管理，係遵照憑證政策及本作業基準之規定

(2) 提供給本管理中心之資訊皆為正確且無誤之資訊

(3) 提出之憑證請求符合本作業基準之規定

(4) 實施憑證註冊審驗人員之識別與鑑別程序

(5) 安全地管理註冊中心之私密金鑰

9.6.3 用戶之聲明與擔保

為了本管理中心及憑證受益人之明確利益，申請人應擔保憑證核發前，本管理中心會收到申請人對用戶約定條款的確認。

申請人應向本管理中心聲明及擔保下列事項：

(1) 安全地產製其私密金鑰並避免遭受破解

(2) 提供本管理中心及註冊中心正確及完整之資訊

(3) 遵守第 3 及第 4 章之規定及程序

(4) 於使用憑證前確認憑證中資料之正確性

(5) 立即通知本管理中心並要求廢止憑證，包括：

(i) 記載於憑證中的資訊已經變更或可能誤導；

(ii) 有任何實際或懷疑憑證所記載之公開金鑰其相對應的用戶私密金鑰遭誤用或破解 (並停用私密金鑰)

(6) 憑證只用於符合憑證政策、本作業基準及用戶協議之合法及經授權的使用目的

(7) 於憑證到期後，立即停止使用憑證及其對應之私密金鑰

9.6.4 信賴憑證者之聲明與擔保

信賴憑證者應聲明與擔保以下之責任：

(1) 使用憑證或查詢本管理中心儲存庫時，必須遵守本作業基準之相關規定

(2) 使用憑證時，應先查驗該憑證之保證等級

(3) 使用憑證時，應確認該憑證所記載之金鑰用途

(4) 使用本管理中心簽發之憑證廢止清冊或線上憑證狀態協定查驗本管理中心簽發之憑證，以確認該憑證之有效性

(5) 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或用戶權益受損時，信賴憑證者應自行承擔責任

(6) 本管理中心如因故無法正常運作時，信賴憑證者應儘速尋求其他途徑完成與他人應為之法律行為，不得以本管理中心無

法正常運作，作為抗辯他人之事由

(7) 接受本管理中心簽發之憑證時，即視為已了解並同意有關本管理中心法律責任之條款，並依照第 1.4.1 節規定範圍使用憑證

如有違反，應依照民法及相關法規之規定負擔對他人的損害賠償責任

9.6.5 其他參與者之聲明與擔保

不做規定。

9.7 免責聲明

除法律或本作業基準另有規範禁止之範圍外，本管理中心在此特別對商品使用及合用性之明示及默示的保證作免責聲明。

9.8 責任限制

用戶或信賴憑證者如未依照本作業基準之適用範圍使用憑證所引發之損失，本管理中心不負任何賠償責任。若屬可歸咎於本管理中心之責任，其賠償金額上限依照本作業基準第 9.9 節規範。

9.9 賠償

9.9.1 本管理中心之賠償責任

本管理中心處理用戶憑證相關作業，若未遵照憑證政策、本作業基準、相關法律規定及本管理中心與用戶及相關信賴憑證者之契約約定，致用戶或信賴憑證者受有損害時，由本管理中心負賠償責任。用戶得依與本管理中心或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。

9.9.2 註冊中心之賠償責任

註冊中心處理用戶憑證註冊作業，若未遵照本作業基準、相關法律規定及註冊中心與用戶及相關信賴憑證者之契約約定，致用戶或信賴憑證者受有損害時，由註冊中心負賠償責任。用戶得依與註冊中心所訂契約之相關約定，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。

9.10 本文件之生效與終止

9.10.1 生效

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

9.10.2 終止

本作業基準新版本經主管機關核定後公布，現有版本即告終止。

9.10.3 終止及保留之效力

本作業基準之效力，維持至遵循本作業基準所簽發之最後一張憑證到期或廢止為止。

9.11 主要成員間之個別告知與溝通

本管理中心、註冊中心、用戶、信賴憑證者彼此間得採適當的方式，建立通告與聯絡管道，包括但不限於：公文、書信、電話、傳真、電子郵件或安全電子郵件。

9.12 修訂

9.12.1 修訂程序

本作業基準每年定期評估是否需要修訂，以維持其保證度。如憑證政策修訂或物件識別碼變更時，本作業基準將配合修訂，且以適當之版本編號代表本作業基準有進行修訂。

9.12.2 通知之機制與期限

重大變更項目將公告於本管理中心儲存庫。用戶或信賴憑證者對於變更項目有意見者，可於公告之意見回覆期限截止前提出，由本管理中心考量相關意見，評估變更項目與回覆。

本作業基準重新排版時，不另作通知。

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

用戶或註冊中心與本管理中心如有爭議時，雙方應本誠信原則協商解決之。如有訴訟之必要時，雙方同意以台灣台北地方法院為第一審管轄法院。

9.14 管轄法律

牽涉本管理中心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

依據本作業基準所簽署的任何協議之解釋，悉依中華民國相關法律之規定。

9.16 雜項條款

9.16.1 完整協議

本作業基準所約定者，係主要成員(本管理中心、註冊中心、用戶、信賴憑證者)間最終且完整之約定。

9.16.2 轉讓

本作業基準所敘述的主要成員之間的權利或責任，不能在未通知本管理中心下以任何形式轉讓給其他方。

9.16.3 可分割性

本作業基準的任一條款不正確或無效時，其他條款仍然有效，直到本作業基準修改為止。

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作業基準相關規定，致本管理中心受有損害時，本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。

本管理中心未向違反本憑證作業基準相關規定者主張權利，不代表本管理中心對於其繼續或未來違反本憑證作業基準情事，有拋棄權利主張之意思。

9.16.5 不可抗力

因不可抗力或其他不可歸責於本管理中心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，本管理中心不負任何法律責任。本管理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。

9.17 其他條款

不做規定。