臺灣網路認證股份有限公司

數位化申請作業之憑證管理中心

憑證實務作業基準

Certification Practice Statement

(第 2.0 版)

生效日期：中華民國 114 年 4 月 9 日

Effective Date：2025/4/9

本作業基準版本變更紀錄：

版本	生效日期	發行者	備註
V1.0	110/12/21	TWCA	初版發行
V2.0	114/4/9	TWCA	遵循新版電子簽章法之「數位簽章憑證實務作業基準應載明事項」進行修訂

目　錄

摘要

臺灣網路認證股份有限公司（TAIWAN-CA INC.，以下簡稱本公司或 TWCA）制定數位化申請作業之憑證管理中心之憑證實務作業基準（以下簡稱本作業基準或 CPS），係規範憑證申請以數位化申請為主、當面申請為輔之作業管理規範，包含簽發、廢止、管理暨更新憑證之服務，為依法設立之憑證機構（Certificates Service Provider，以下簡稱 CSP）。本公司憑證實務作業基準之重要事項說明如下：

1.主管機關核定

本作業基準係依據主管機關數位發展部頒布之「數位簽章憑證實務作業基準應載明事項」規範編撰，經審查後核定之文號為：

民國 114/4/9 數位發展部函 數授產經字第 1140001427 號

2.簽發之憑證

憑證種類及適用範圍：

憑 證 種 類	保 證 等 級	適 用 業 務 範 圍
商務 XML Plus 憑證	第一級	電子商務應用、身分識別服務。
	第二級	電子商務應用、網路報稅、電子發票、電子郵件應用、電子通訊投票、電子化政府應用、網路文件簽署、網路保險、身分識別服務。
	第三級	低風險電子銀行交易、低風險證券暨期貨網路下單交易、低風險電子金融交易、電子商務應用、網路報稅、電子發票、電子通訊投票、線上申請專利商標、短期票券發行交易應用、基金網路下單交易、電子支付、電子郵件應用、電子化政府應用、網路文件簽署、網路保險、身分識別服務。
	第四級	憑證管理中心使用（簽發下屬憑證或憑證廢止清冊）。
註：保證等級詳述於 1.4；憑證適用範圍及賠償責任詳述於 9.9		

3.法律責任重要事項

(1) 註冊：

用戶向註冊中心申請註冊時，必須提供詳細且正確的身分證明文件與資料、確實瞭解並同意申請書與合約書上的權利義務及憑證申請與使用的作業規範內容，並且於接受該規範的規定下始可確認表示。用戶因故意、過失或不正當意圖而提供不實資料致造成他人遭受損害時，應由該用戶負損害賠償責任。

(2) 憑證使用：

用戶必須妥善保管與憑證相對應的私密金鑰及保護密碼，不得洩漏或交付予他人使用。當有被冒用、曝露及遺失等不安全的顧慮或不擬使用該憑證時，用戶必須即刻向註冊中心辦理申告及處理。如因故意或過失，致造成他人遭受損害時，應由該用戶負損害賠償責任。

用戶必須依本作業基準與業務應用系統規範的規定，合法且正確的使用私密金鑰與憑證於相關的業務系統，不得使用於 1.本作業基準規範內容之外；2.會造成人體身心與精神的傷害、死亡、或對社會秩序與社會環境有重大危害的應用或業務系統；3.電子簽章法相關法令暨主管機關明訂禁止的應用或業務。因私密金鑰與憑證使用於前述禁止範圍內而所致之損害，由用戶承擔之。

(3) 賠償責任：

本公司如因作業人員之過失，使其未遵照本作業基準、憑證政策及相關作業規範的規定辦理用戶註冊、憑證的簽發、暫禁與廢止作業，或違反相關法律規範而造成用戶的損害時，本公司應依本作業基準之規定賠償用戶之損害。有關用戶單一憑證之最高賠償金額訂於 9.9 節；但上述損害事由係因本公司作業人員故意或重大過失所造成者，本公司賠償該用戶之實際所受損害。

如因網際網路傳輸的中斷或故障，或其他不可抗力的天災事故（例如戰爭或地震等），非為本公司的故意或過失致所簽發之憑證造成用戶損害時，本公司不負損害賠償責任。

本公司憑證用戶或其他有權者提出廢止憑證要求後，至本公司實際完成廢止該用戶憑證之期間內，當該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，本公司如依據本作業基準與相關之作業規範執行處理作業，則不負任何損害賠償責任。

4.其他重要事項

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

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

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

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

(5) 本公司每年自行委託會計師事務所定期進行外部稽核，以確保遵照憑證實務作業基準與憑證政策之規定運作。

1.簡介

1.1 概述

臺灣網路認證股份有限公司（TAIWAN-CA INC.，以下簡稱本公司或 TWCA）係由臺灣證券交易所股份有限公司、財金資訊股份有限公司、臺灣集中保管結算所股份有限公司、網際威信股份有限公司共同集資設立，為一值得信賴的憑證機構。

為建立安全及可信賴的網路環境，確保資訊在網路傳輸過程中不易遭致偽造、竄改或竊取，且能鑑別交易雙方的身分及防止事後否認已完成交易的事實，TWCA 除了提供傳統的紙本證明資料及當面身分識別申請方式外，另基於數位身分驗證機制建立數位化申請公開金鑰基礎建設（TWCA Digital Identity Public Key Infrastructure; TWCA DI PKI，以下簡稱本基礎建設），提供身分識別及交易認證的服務，以建立使用者的信心，確保參與交易雙方的權益。

為提供用戶於從事網際網路交易時所迫切需要之認證服務，本公司特規劃建置認證相關安全機制的網際網路認證服務系統，其中使用公開金鑰密碼學 (Public Key Cryptography) 機制，符合各項國際標準（如 Public Key Cryptography Standards, PKCS），具備網路交易訊息的不可否認 (Non-repudiation)、完整性 (Integrity) 以及隱密性 (Confidentiality)，並可達到身分的鑑別 (Authentication)、訊息的驗證 (Verification)、訊息加密 (Encryption) 等相關安全機制。可用於網際網路電子銀行、網路下單交易，亦可用於網路報稅、保險、票債券、企業詢價報價、採購與付款交易、電子通訊投票、電子化政府應用等網際網路電子商務的應用交易系統。

1.2 文件名稱及識別

本作業基準依據之商務 XML Plus 憑證（簡稱 IXML Plus 憑證）憑證政策 (CP)，物件識別碼如下：

OID=1.3.6.1.4.1.40869.1.2.1。

依憑證政策 (CP) 之定義，不同憑證保證等級之物件識別碼如下：

憑證保證等級	物件識別碼
第一級 (Class 1)	1.3.6.1.4.1.40869.1.2.1.1
第二級 (Class 2)	1.3.6.1.4.1.40869.1.2.1.2
第三級 (Class 3)	1.3.6.1.4.1.40869.1.2.1.3
第四級 (Class 4)	1.3.6.1.4.1.40869.1.2.1.4

1.3 成員及適用範圍

本章節就 IXML Plus 憑證公開金鑰基礎建設所包含之各成員做說明。本基礎建設相關成員包括：

(1) 憑證管理中心 (Certification Authorities)。

依階層及用途分為：

- 最高層憑證管理中心（Root CA，簡稱 RCA）。
- 政策憑證管理中心（Policy CA，簡稱 PCA）。
- 用戶憑證管理中心（User CA，簡稱 UCA）。

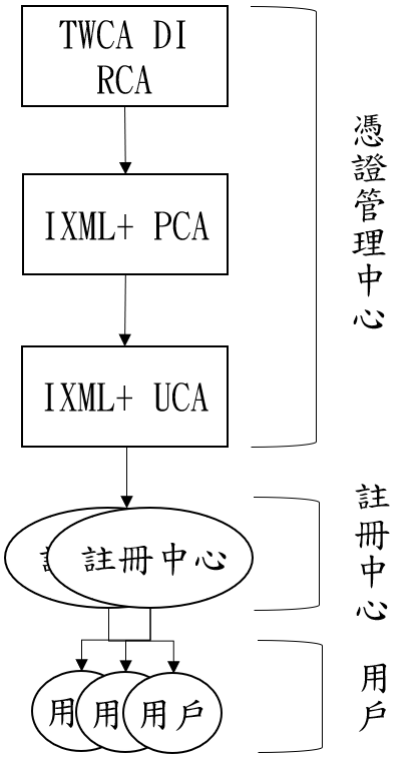
統稱本憑證管理中心。

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

(3) 用戶(Subscribers)。

(4) 信賴憑證者 (Relying Parties)。

成員關係圖如下：



1.3.1 憑證管理中心

1.3.1.1 最高層憑證管理中心

最高層憑證管理中心 (RCA) 為本憑證管理中心之最高層憑證管理機構，擔任本基礎建設之信賴起始源，由本公司負責營運及管理，主要負責以下工作：

- 管理與公告 PCA 之註冊、憑證、憑證廢止清冊 (Certificate Revocation List; CRL) 的作業程序與驗證的作業規範。
- 簽發、管理與遞送 PCA 的憑證、憑證廢止清冊。
- 建置於獨立、安全控管的作業環境下，經合法授權才可由二位以上的執行人員進行公開金鑰的產生、建置與簽發 PCA 憑證的作業。
- RCA 的憑證為自簽憑證，當新產生或變更憑證時，必須以最迅速的方式遞送予使用者或通知使用者至 RCA 索取。

1.3.1.2 政策憑證管理中心

政策憑證管理中心 (PCA) 由本公司負責營運及管理，主要負責以下工作：

- 遵循 RCA 訂定的規範。
- 管理與公告 UCA 之註冊、憑證、憑證廢止清冊的作業程序與驗證的作業規範。
- 簽發、管理與遞送 UCA 的憑證、憑證廢止清冊。

1.3.1.3 用戶憑證管理中心

用戶憑證管理中心 (UCA) 由本公司負責營運及管理，主要負責以下工作：

- 用戶憑證之簽發與管理。
- 用戶憑證廢止清冊之簽發與管理。
- 管理與公告用戶憑證、用戶憑證廢止清冊於儲存庫，並維持儲存庫的穩定與運作。
- 接受 RA 傳遞之憑證相關作業請求訊息，並確認 RA 的合法性以及請求訊息的正確性，並於作業完成後將回覆訊息安全地傳回 RA。
- 管理 RA 之註冊名稱、RA 憑證與相關聯絡資訊。

1.3.2 註冊中心

註冊中心 (RA) 由本公司遴選合於規範之機構擔任，並與本公司簽立合約後負責註冊業務，主要負責以下工作：

- 內部設有專屬部門負責註冊業務。
- 管理與公告用戶註冊申請的作業程序與身分識別的作業規範。

- 驗證用戶身分以及憑證相關作業請求訊息，以確保用戶身分合法性與訊息的正確性。
- 遞送用戶的憑證相關作業請求至用戶憑證管理中心辦理，並驗證回覆訊息的正確性。

1.3.3 用戶

用戶即為用戶憑證管理中心所簽發之憑證的擁有者，包含自然人、營利或非營利事業單位之法人、政府組織之相關單位、財團法人、教育公益或其他相關機構組織、電腦系統、機器設備等。

1.3.4 信賴憑證者

信賴憑證者係指在信任本憑證管理中心的前提下，相信用戶憑證與用戶身分間連結關係的第三方。基於此信任基礎下，信賴憑證者可進行：

- 使用本憑證管理中心之憑證鏈資訊（包含用戶憑證、用戶憑證管理中心憑證、政策憑證管理中心憑證與最高層憑證管理中心憑證），驗證用戶簽章訊息之完整性與不可否認性。
- 使用用戶憑證對訊息做加密，並將加密的訊息傳送至接收者（用戶），以達到通訊雙方訊息的隱密性。

1.3.5 其他參與者

其他與本憑證管理中心間接相關之可能成員，例如對本憑證中心進行跨簽 (Cross Sign) 之其他憑證中心。

1.4 憑證用途

1.4.1 憑證適用範圍

1.4.1.1 保證等級

本憑證管理中心依用戶於註冊（登錄）階段時所使用之身分識別方式的強度，區分不同的憑證保證等級。各憑證保證等級意義如下：

保證等級	保證意義
第一級 (Class 1)	用戶憑證管理中心及註冊中心僅保證用戶識別資訊於本公司資料庫內之唯一性，所有與用戶相關之資訊均視為未經證實。
第二級 (Class 2)	用戶憑證管理中心及註冊中心保證用戶識別資訊於本公司資料庫內之唯一性，而對於用戶相關資訊，僅提供完成查證而非絕對正確無誤之保證。
第三級 (Class 3)	用戶憑證管理中心及註冊中心除保證用戶識別資訊於本公司資料庫內之唯一性外，用戶相關資訊經由多重嚴謹之作業程序，提供趨近臨櫃核身之身分識別保證。

第四級 (Class 4)	用戶憑證管理中心及註冊中心除保證用戶識別資訊於本公司資料庫內之唯一性外，用戶相關資訊經由與用戶面對面互動之作業驗證程序，提供高於第三級之身分識別保證。

針對不同的保證等級，其註冊（登錄）階段針對身分識別方式之要求也會有所不同，具體說明於 3.2 節描述。

1.4.1.2 使用範圍

本憑證管理中心定義之各項使用憑證之業務如下：

業務種類	業務涵蓋範圍
身分識別應用	• 身分識別服務
電子商務暨政府應用業務	• 網路報稅 • 電子發票 • 電子郵件應用 • 電子通訊投票 • 電子化政府應用 • 網路文件簽署 • 網路保險 • 線上申請專利商標 • 其他電子商務應用
金融交易業務	• 低風險電子銀行交易 • 低風險電子金融交易 • 低風險證券暨期貨網路下單交易 • 短期票券發行交易應用 • 基金網路下單交易 • 電子支付 • 其他電子金融交易
憑證管理中心業務	• 憑證管理中心使用（簽發下屬憑證或憑證廢止清冊）

本憑證管理中心之憑證使用範圍由「使用範圍代碼」定義之。該代碼由四段子代碼組成，分別表示憑證「保證等級」、「用途別」、「用戶身分」以及「適用業務範圍」，各段子代碼之定義詳述如下：

憑證使用範圍代碼格式：

第一段代碼・第二段代碼・第三段代碼・第四段代碼

第一段代碼 [保證等級] (Assurance Level)	第二段代碼 [用途別] (Usage)	第三段代碼 [用戶身分] (Identity)	第四段代碼 [適用業務範圍] (Business Category)
1：第一級 2：第二級	1：單一用途 2：限定範圍內多用途	1：法人 2：自然人	1：身分識別應用 2：身分識別應用、電子商務暨

3：第三級 4：第四級 *註 1	*註 2	3：其他	政府應用業務 3：身分識別應用、金融交易業務 4：身分識別應用、電子商務暨政府應用業務、金融交易業務 5：憑證管理中心使用（簽發下屬憑證或憑證廢止清冊）
註 1.「保證等級」請參閱 1.4.1.1 節之規範。 註 2.「單一用途」係指專供某一特殊用途或限制特定交易對象使用，如財產申報專用或網路下單專用或網路銀行專用。此外，憑證內憑證政策 (CertificatePolicy) 之憑證簽發者的簡要聲明 (TerseStatement) 欄位會記載憑證專屬之用途及限制之交易對象。「限定範圍內多用途」係指非專供某一特殊用途或限制特定交易對象使用。若憑證中憑證政策之憑證簽發者的簡要聲明欄位有記載代碼者，其限定範圍多用途依其代碼而定；若無記載者，應依本公司簽署之合約或本公司網站之公告為主。			

例如：憑證之使用範圍代碼為 3.1.1.1 解讀如下：

第三級保證等級(3)・單一用途(1)・法人用戶(1)・金融交易使用(1)

1.4.2 憑證之禁止使用情形

本公司所簽署之憑證除使用於 1.4.1 節規定之範圍，禁止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，且禁止使用於電子簽章法或其他相關法令或各事業目的主管機關明訂禁止或排除之應用或業務。

1.5 政策管理

1.5.1 管理單位

本作業基準的訂定、修改、及發布等事宜，其權責單位為「臺灣網路認證股份有限公司」政策管理中心 (Policy Management Authority; PMA)。

1.5.2 聯絡窗口

用戶對憑證實務作業基準有任何修改建議時，請將詳細的建議、說明文件與聯絡資訊，E-mail 或郵寄至下述的聯絡窗口；

用戶有關憑證的註冊、申請、更新、查詢，與金鑰有遺失、不安全顧慮的申告處理作業，於本公司的聯絡及處理窗口如下述：

公司名稱	臺灣網路認證股份有限公司 (TAIWAN-CA INC.; TWCA)
聯絡單位	客服中心
地址	(100011) 台北市中正區延平南路 85 號 10 樓 10F., No. 85,Yan-Ping S. Rd., Zhongzheng Dist., Taipei 100011, Taiwan, R.O.C.
電話	886-2-23708886
傳真	886-2-23700728
電子郵箱	ca@twca.com.tw
網址	https://www.twca.com.tw

1.5.3 憑證實務作業基準之核定

本作業基準的修改與訂定事宜，權責管理單位為政策管理中心 (PMA)。

1.5.4 憑證實務作業基準核定程序

本作業基準由本憑證管理中心訂定，並由政策管理中心審查通過。

依據電子簽章法規定，本憑證管理中心訂定之憑證實務作業基準，必須經主管機關數位發展部核定後，始得對外公布並提供憑證簽發服務。

1.6 名詞定義及縮寫

請參閱附錄一附錄二。

2.公布及儲存庫

2.1 儲存庫

本憑證管理中心負責管理及維護儲存庫，公開並揭露憑證政策(CP)、憑證實務作業基準(CPS)、憑證相關資訊以及稽核報告於儲存庫中。本憑證管理中心確保儲存庫資訊 7 x 24 可取用，

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

2.2 憑證資訊之公布

本憑證管理中心公布之資訊包含但不限於以下項目：

(1) 憑證政策
(2) 憑證實務作業基準(即本作業基準)。
(3) 憑證管理中心憑證鏈。
(4) 憑證管理中心憑證相關資訊，包含憑證屬性欄位值以及憑證廢止清冊(CRL)下載點。
(5) 稽核報告。

2.3 公布頻率

新版憑證政策 (CP)，經修改完成且經政策管理中心 (PMA) 核定生效後之，7 個工作天內公告於本儲存庫。

新版憑證實務作業基準 (CPS)，依需求經修改完成且經政策管理中心 (PMA) 核定後，將送經主管機關核定，本公司於收到核定公文後 7 個工作天內即刻公布於儲存庫。

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

本憑證管理中心每年至少公布 1 次稽核報告於儲存庫。

2.4 儲存庫之存取控制

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

3.識別與鑑別

3.1 命名

3.1.1 名稱種類

本憑證管理中心之憑證主體 (Subject) 之 Distinguished Name (DN) 命名定義如下：

最高層憑證管理中心 (RCA)：

識別名稱 (DN)	說　　明	識 別 名 稱 內 容 範 例
1.Country (C)	憑證簽發所在地國別碼	C = TW
2.Organization (O)	CA 公司政策的資訊	O = TaiCA
3.OrganizationUnit (OU)	CA（簽發單位）的資訊	OU = Root CA
4.CommonName (CN)	憑證申請者的識別名稱	CN = TWCA Information XML Plus Root CA

政策憑證管理中心 (PCA)：

識別名稱 (DN)	說　　明	識 別 名 稱 內 容 範 例
1.Country (C)	憑證簽發所在地國別碼	C = TW
2.Organization (O)	CA 公司政策的資訊	O = TaiCA
3.OrganizationUnit (OU)	CA（簽發單位）的資訊	OU = Policy CA
4.CommonName (CN)	憑證申請者的識別名稱	CN = TWCA Information XML Plus Policy CA

用戶憑證管理中心 (UCA)：

識別名稱 (DN)	說　　明	識 別 名 稱 內 容 範 例
1.Country (C)	憑證簽發所在地國別碼	C = TW
2.Organization (O)	CA 公司政策的資訊	O = TaiCA
3.OrganizationUnit (OU)	CA（簽發單位）的資訊	OU = User CA
4.CommonName (CN)	憑證申請者的識別名稱	CN = TWCA Information XML Plus User CA

本憑證管理中心產生或處理 X.509 V3 (ISO 9594-8) 憑證的用戶主要識別名稱<SubjectName>（例如：個人的身分證統一編號或企業的營利事業統一編號，或財金公司跨行系統之銀行網際網路帳號）及擴充的次要識別名稱<SubjectAltName>（例如：銀行帳號、公司及個人中文名稱）採用 X.501 (ISO 9594-2) Distinguished Name (DN) 的命名方式，其格式如下：

識別名稱(DN)	說明	必要性	識別名稱內容範例
1.Country (C)	憑證簽發所在地國別碼	必要	C = TW
2.Organization (O)	CA 公司政策的資訊或憑證申請者組織資訊	選填	O = Information
3.OrganizationUnit (OU)	CA（簽發單位）的資訊或憑證申請者組織單位資訊(1)	選填	OU = TWCA Information XML Plus User CA
4.OrganizationUnit (OU)	註冊中心英文識別名稱或憑證申請者組織單位資訊(2)	選填	OU = 12345678-RA-Trade
5.OrganizationUnit (OU)	註冊中心應用或服務識別名稱或憑證申請者組織單位資訊(3)	選填	OU = IXMLP
6.CommonName (CN)	憑證申請者的識別名稱或其他可識別之名稱或其他經確認之資訊，例如企業的營利事業統一編號	必要	CN = 12345678-01-0001

3.1.2 識別名稱之意義

用戶憑證所記載之主體識別名稱，須符合相關法令及規範對於命名之規定，必須足以識別特定之法人單位及自然人，且必須可為信賴憑證者所識別。個人的身分證統一編號識別名稱，為依內政部訂定的規範處理；企業的營利事業統一編號識別名稱依主管機關訂定的規範處理。

若因業務需求而有非屬個人身分證統一編號或營利事業統一編號的主體識別名稱者，除應事先取得本公司同意外，用戶與信賴憑證者於使用憑證前，應事先約定用戶識別名稱，並於驗證憑證時確認用戶識別名稱之正確性。

3.1.3 用戶之匿名與假名

本作業基準不允許用戶使用匿名或假名。

3.1.4 各種名稱的解釋規則

憑證所記載之名稱，其名稱形式之解釋規則依 ITU-T X.520 名稱屬性定義。

3.1.5 名稱的唯一性

於憑證內使用的各種用戶識別名稱，於憑證系統內皆具有可辨識之唯一性，但當用戶有相同的註冊名稱或識別名稱時，以先申請註冊的用戶優先使用，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。

當用戶使用的識別名稱有相同時，用戶憑證管理中心或註冊中心以先申請註冊的用戶優先使用，相關的糾紛仲裁處理非為本公司或註冊中心的管轄權責，用戶必須向相關的業務主管機關提出申請，例如：個人的身分證統一編號識別名稱有相同情況時，則由用戶向內政部提出申請。

當用戶使用的識別名稱，經有權主管機關合法文件證實為其他申請者所擁有時，用戶憑證管理中心即刻註銷該用戶的用戶識別名稱使用權，且該用戶必須負擔相關的法律權責；驗證該用戶註冊識別名稱使用的合法性，非為本公司或註冊中心的業務權責範圍。

3.1.6 商標之辨識、鑑別及角色

用戶憑證管理中心或註冊中心尊重用戶識別名稱有關註冊公司中、英文名稱的註冊商標權，並接受用戶的使用，但不保證用戶註冊商標的認可、驗證與唯一性，相關的糾紛仲裁處理非為本公司或註冊中心的管轄權責範圍，用戶必須向相關的業務主管機關提出申請。

3.2 初始驗證

初始驗證目的在於防止偽冒申請，並且申請者提供之身分資料真實性經過確認。為此，註冊中心進行身分驗證時應秉持以下原則：

1. 對所收集的身分證明資料完成真偽 (Verification)、有效性 (Validation)，以及與申請者之連結性 (Linkage) 驗證，其驗證強度應與憑證保證等級相匹配。
2. 若申請者委託代理人辦理，須具備可驗證之授權機制以完成代理人之身分及授權驗證。
3. 最後登錄之身分資料須由申請者進行確認，以確保擬登錄之資料與申請人提交時的一致，且為申請人之正確資訊。

3.2.1 證明擁有私密金鑰的方式

用戶憑證管理中心或註冊中心必須驗證用戶私密金鑰擁有的正確性、完整性與有效性，須以如下所述之方法驗證用戶所擁有的私密金鑰：

✓ 用戶於申請憑證過程中，以用戶私密金鑰執行簽章並產生 PKCS#10 格式之憑證請求檔(Certificate Signing Request; CSR)，用戶憑證管理中心或註冊中心必須以該憑證請求檔中載明之公開金鑰對憑證請求檔執行驗章，以證明用戶擁有該公開金鑰對應之私密金鑰。

3.2.2 法人身分的鑑別

法人身分的鑑別方式依其所申請之憑證保證等級（定義於 1.4.1.1 節）而有所不同，具體驗證方式描述如下：

保證等級	法人身分識別方式
第一級 (Class 1)	1. 申請者遞交申請識別資訊（如公司註冊名稱及電子郵件信箱資訊），由註冊中心進行識別資訊唯一性及法人身分具備客觀存在的事實之確認（參閱「3.1.5 節）。 2. 申請者可透過數位或書面方式遞交上述識別資訊。 3. 相關資訊一旦遞交，即表示申請者確認並同意所提供之資訊，註冊中心將依此進行驗證用戶身分證明之正確性。
第二級 (Class 2)	4. 除了第一級相關資訊的檢核外，申請者須遞交法人之名稱、營利事業統一編號或足以識別法人身分之資料，由註冊中心透過電話或其他途徑（如第三方之資料庫）查驗法人身分的存在性及有效性。 5. 申請者初始註冊身分識別與認證程序，須遞交一項由可靠資料來源核發之身分資料*註1，經可信任第三方驗證，由註冊中心依該信物之驗證規範進行查驗*註2。 6. 申請者可透過數位或書面方式遞交上述識別資訊。 7. 相關資訊一旦遞交，即表示申請者確認並同意所提供之資訊，註冊中心將依此進行驗證用戶身分證明之正確性。 8. 藉由本保證等級之簽章用憑證，驗證數位簽章無誤後，可推定為用戶本人所產生之數位簽章。
第三級 (Class 3)	當面辦理： 1. 除了第二級相關資訊的檢核外，申請者(法人代表人)須遞交申請書，其中申請書內容應包含法人名稱、營利事業統一編號等法人相關資訊，且應蓋有法人及法人代表人之印鑑，由註冊中心進行資訊查驗。申請者亦須提供足以識別申請者身分的證明文件(例如具有相片的身分證或護照)。 2. 若申請者委託代理人辦理，則代理人須加附相關之授權文件及足以識別代理人身分的證明文件。 3. 相關資訊一旦遞交，即表示申請者確認並同意所提供之資訊，註冊中心將依此進行驗證用戶身分證明之正確性。 非當面辦理： 1. 除了第二級相關資訊的檢核外，申請者須遞交申請書影本，其中申請書內容應包含法人名稱、營利事業統一編號等法人相關資訊。

	2. 申請者初始註冊身分識別與認證程序，須遞交兩項由可靠資料來源核發之身分資料*註3，經可信任第三方驗證，由註冊中心依該信物之驗證規範進行查驗*註4。 3. 申請者可透過數位或書面方式遞交上述驗證資訊。 4. 相關資訊一旦遞交，即表示申請者確認並同意所提供之資訊，註冊中心將依此進行驗證用戶身分證明之正確性。 5. 藉由本保證等級之簽章用憑證，驗證數位簽章無誤後，可推定為用戶本人所產生之數位簽章。
第四級 (Class 4)	1. 除了第三級相關資訊的檢核外，必須由法人代表或其授權之代理人親自辦理。 2. 若非法人代表人親自辦理，則代理人須持相關之授權文件，且代理人必須提供證明文件足以識別代理人身分。 3. 相關資訊一旦遞交，即表示申請者確認並同意所提供之資訊，註冊中心將依此進行驗證用戶身分證明之正確性。 4. 藉由本保證等級之簽章用憑證，驗證數位簽章無誤後，可推定為用戶本人所產生之數位簽章。
註 1.初始註冊身分識別與認證程序之身分資料須為符合 ISO/IEC 29115 高保證等級以上之信物。 註 2.滿足保證等級二之初始註冊身分識別與認證程序，如：工商憑證驗證、法人存款帳戶驗證、公司變更登記申請書查驗等機制。 註 3.初始註冊身分識別與認證程序之兩項身分資料中至少一項須符合 ISO/IEC 29115 高保證等級以上之信物。 註 4.滿足保證等級三之初始註冊身分識別與認證程序，如：工商憑證驗證搭配公司變更登記申請書驗證、法人存款帳戶驗證搭配開戶約定之設備驗證、經法人授權之代理人以自然人保證等級三之機制進行驗證等。	

3.2.3 個人用戶身分的鑑別

個人用戶身分的鑑別方式依其所申請之憑證保證等級(定義於 1.4.1.1 節)而有所不同，具體驗證方式描述如下：

保證等級	個人身分識別方式
第一級 (Class 1)	1. 申請者遞交申請識別資訊，由註冊中心進行識別資訊唯一性及身分具備客觀存在的事實之確認。(參閱 3.1.5 節)。 2. 申請者可透過數位或書面方式遞交上述識別資訊。 3. 相關資訊一旦遞交，即表示申請者確認並同意所提供之資訊，註冊中心將依此進行驗證用戶身分證明之正確性。
第二級 (Class 2)	1. 滿足保證等級一之要求。 2. 申請者初始註冊身分識別與認證程序，須遞交一項由可靠資料來源核發之身分資料*註1，經可信任第三方驗證，由註冊中心依該信物之驗證規範進行查驗*註2。 3. 申請者可透過數位或書面方式遞交上述識別資訊。

	4. 相關資訊一旦遞交，即表示申請者確認並同意所提供之資訊，註冊中心將依此進行驗證用戶身分證明之正確性。 5. 藉由本保證等級之簽章用憑證，驗證數位簽章無誤後，可推定為用戶本人所產生之數位簽章。
第三級 (Class 3)	當面辦理： 1. 除了第二級相關資訊的檢核外，必須由申請者本人親自辦理，且申請者提供的證明文件足以識別申請者之身分（例如具有相片的身分證或護照）。 2. 若申請者委託代理人辦理，則代理人須加附相關之授權文件及足以識別代理人身分的證明文件。 3. 相關資訊一旦遞交，即表示申請者確認並同意所提供之資訊，註冊中心將依此進行驗證用戶身分證明之正確性。 非當面辦理： 1. 滿足保證等級二之要求。 2. 申請者初始註冊身分識別與認證程序，須遞交兩項由可靠資料來源核發之身分資料*註 3，經可信任第三方驗證，由註冊中心依該信物之驗證規範進行查驗*註 4。 3. 申請者可透過數位或書面方式遞交上述驗證資訊。 4. 相關資訊一旦遞交，即表示申請者確認並同意所提供之資訊，註冊中心將依此進行驗證用戶身分證明之正確性。 藉由本保證等級之簽章用憑證，驗證數位簽章無誤後，可推定為用戶本人所產生之數位簽章。
註 1.初始註冊身分識別與認證程序之身分資料須為符合 ISO/IEC 29115 高保證等級以上之信物。 註 2.滿足保證等級二之初始註冊身分識別與認證程序，如：存款帳戶驗證、金融機構原留門號驗證、電信門號認證輔以經其他權威單位驗證身分資料真偽等機制。 註 3.初始註冊身分識別與認證程序之兩項身分資料中至少一項須符合 ISO/IEC 29115 高保證等級以上之信物。 註 4.滿足保證等級三之初始註冊身分識別與認證程序，如：網銀帳密驗證搭配原留門號驗證、電信門號認證搭配存款帳戶驗證、自然人憑證驗證搭配人工查驗等機制。 註 5.本憑證管理中心無發放保證等級為第四級之個人憑證。	

3.2.4 未驗證之用戶資訊

本憑證管理中心所簽發憑證記載之用戶資訊皆經過驗證。

3.2.5 權責之確認

當個人代理人或法人代理人欲代表原申請者進行憑證作業時，除了出示身分證明文件之外，應出示授權文件，其中授權文件內容應包含代理人身分、原申請者與代理人之關係、欲

申請憑證作業之內容以及原申請者之證明印鑑或本憑證管理中心認可足之代表原申請者之信物(如工商憑證)。註冊中心須確認授權文件之真偽，必要時須聯繫原申請者，以確認代理人有權進行憑證之申請。

3.2.6 交互運作標準

無規定。

3.3 金鑰更新之識別與鑑別

3.3.1 憑證例行性金鑰更新

假若用戶金鑰的生命週期訂定為一年，於一年後到期時必須更新，即表示用戶憑證的有效期限為一年。在有效期限屆滿前的憑證更新期內（例如：屆滿前一個月），用戶必須自己重新產生一組公開金鑰及私密金鑰對，並向用戶憑證中心或註冊中心申請新憑證的簽發，此為憑證及私密金鑰的更新 (Rekey)。

本憑證管理中心之用戶憑證（私密金鑰的有效期限亦訂定為與憑證相同）有效期限最長為三年。

若用戶於憑證有效期限屆滿前執行憑證及私密金鑰的更新，須以使用中有效的私密金鑰對新產生的公開金鑰進行數位簽章，並將產生之 PKCS#10 格式憑證請求檔 (Certificate Signing Request; CSR)傳遞至註冊中心申請新憑證簽發，待用戶憑證管理中心或註冊中心驗證簽章訊息的正確性、完整性及有效性後，始得執行憑證申請作業。

若用戶於憑證有效期限屆滿後執行憑證及私密金鑰的更新，將視為憑證新申請，用戶必須重新執行 3.2 節之程序或其他能有效確認身分的方式，包含證明擁有私密金鑰以及身分之鑑別，待用戶憑證管理中心或註冊中心審驗通過後，始得執行憑證申請作業。

3.3.2 憑證廢止後之金鑰更新

當用戶憑證廢止後，不允許用戶向用戶憑證管理中心或註冊中心申請憑證及私密金鑰更新，若須申請憑證，將視為憑證新申請，用戶必須重新執行 3.2 節之程序，包含證明擁有私密金鑰以及身分之鑑別，待用戶憑證管理中心或註冊中心審驗通過後，始得執行憑證申請作業。

3.4 憑證廢止請求之識別與鑑別

當用戶提出憑證廢止請求時，應以數位或是書面方式提出請求。用戶憑證管理中心或註冊

中心除應檢核用戶身分識別無誤外，應檢驗請求資料之真偽，符合 3.2.2 節或 3.2.3 節對應之身分識別要求，必要時需聯繫原憑證申請者，以確認憑證欲廢止之具體事實。若透過代理人辦理，須滿足 3.2.5 節。詳細廢止作業依 4.9 節規定辦理。

4.憑證生命週期管理

4.1 憑證申請

4.1.1 憑證申請者

欲申請憑證之法人機構，其代表人或其代理人為憑證申請者。

欲申請憑證之自然人，以本人或其代理人為憑證申請者。

4.1.2 註冊程序與責任

用戶應依業務應用系統安控措施的需求，向註冊中心申請憑證的簽發，申請憑證前必須向註冊中心完成用戶註冊申請。

註冊中心必須向用戶詳細說明業務應用系統憑證使用範圍、申請單與合約書上之權利與義務規範以及相關業務運作的作業流程，並提供使用說明與操作文件予用戶。用戶必須同意並確認後方可執行註冊申請之作業。

根據 3.2 節，用戶遞交相關驗證文件，註冊中心依不同保證等級之身分識別作業規範，驗證用戶身分與證明文件無誤後，完成用戶註冊申請作業。

(1) 註冊中心依據用戶憑證管理中心的作業管理規範，向用戶憑證管理中心辦理註冊與申請註冊中心之憑證（簡稱為 RA 憑證），該憑證用於與用戶憑證管理中心間用戶憑證作業訊息收送之安全保護。

4.2 憑證申請程序

4.2.1 識別與鑑別程序

受理所有保證等級之 IXML Plus 憑證申請時，皆依下列程序辦理：

(1) 用戶完成 4.1.2 之註冊程序。

(2) 用戶產生金鑰對並使用私密金鑰 PKCS#10 格式之憑證請求檔 (Certificate Signing Request; CSR) 後，將之傳送至註冊中心。

(3) 註冊中心檢核用戶憑證申請訊息的正確性、完整性與有效性正確無誤後，將用戶憑證申請訊息以註冊中心的私密金鑰簽章後傳送至用戶憑證管理中心。

(4) 用戶憑證管理中心檢核註冊中心身分、註冊中心所傳送之用戶憑證申請訊息，與用戶身分的訊息的正確性、完整性與有效性正確無誤後，簽發用戶憑證並傳送至註冊中心。

(5) 註冊中心檢核用戶憑證管理中心回覆訊息的正確性、完整性與有效性，並確認用戶憑證記載之資訊正確無誤後，將用戶憑證傳送予申請人。

註冊中心或用戶憑證管理中心為安控措施的考量，可將憑證申請與私密金鑰產生的介面軟體，以可信賴且具安控措施的方式遞送予用戶，且該介面軟體必須經由註冊中心或用戶憑證管理中心適當的安全評估與驗證。

4.2.2 接受或拒絕憑證申請

完成 4.2.1 節後，視為憑證申請通過，憑證申請者即成為本憑證管理中心之用戶；如未能完成識別與鑑別程序，應拒絕憑證申請。

4.2.3 憑證申請處理時間

無規定。

4.3 憑證簽發

4.3.1 憑證機構簽發憑證

憑證的簽發作業規範詳述於 4.2 節。

用戶憑證管理中心於產生用戶憑證後，除遞送予申請的用戶外，並即刻更新資料庫的憑證資訊供用戶查詢使用。

4.3.2 憑證機構簽發憑證通知用戶

用戶憑證簽發完成後，用戶憑證管理中心與註冊中心必須立刻通知用戶進行憑證下載。

當用戶憑證申請訊息為用戶憑證管理中心拒絕時，用戶憑證管理中心與註冊中心必須立刻通知用戶該失敗訊息。

4.4 憑證接受

4.4.1 憑證接受之程序

申請憑證簽發完成且由用戶憑證管理中心取得憑證時用戶應依下列規定處理：

(1) 確認憑證內容的用戶相關資訊與用戶註冊時的一致，且為用戶本人之正確資訊。

(2) 每張憑證的公開金鑰與所對應的私密金鑰為相關的一組且為用戶所擁有，憑證內容的憑證有效期限欄位之值是否為有效且正確。

(3) 用戶必須驗證該憑證之憑證鏈，檢驗其每張憑證的正確性、完整性與有效性，以確認該憑證是否已廢止、憑證有效期限是否已結束、是否為合法且正確的用戶憑證管理中心所簽發。

(4) 用戶於確認憑證內容時，如發生上述之問題或其他經憑證管理中心認可之問題時，可於簽發後 7 日內，向用戶憑證管理中心或註冊中心辦理憑證重發。

(5) 用戶啟用所申請的憑證後，即是接受本作業基準、憑證政策與合約上的權利與義務的關係。

4.4.2 憑證機構公布憑證

憑證簽發完成後，即將簽發之用戶憑證公布於儲存庫。

4.4.3 憑證機構通知其他機構憑證簽發

無規定。

4.5 金鑰對及憑證用途

4.5.1 用戶私密金鑰及憑證使用

憑證使用的範圍依本作業基準，及使用者與本公司合約規定的憑證使用範圍之限制規定，用戶使用憑證時：

(1) 用戶必須妥善的保管及儲存與憑證相關的私密金鑰，避免遺失、曝露、被篡改或為第三者任意使用或竊用。

(2) 除必須驗證該憑證之憑證鏈，檢驗其每張憑證及該憑證的正確性、完整性與有效性外（該憑證是否已廢止、憑證有效期限是否已結束、是否為合法且正確的用戶憑證管理中心所簽發、是否為合法且正確的憑證擁有者），且須依各使用業務相關安控的規範檢核憑證相關欄位的正確性，及此張憑證擁有者是否為合法且正確的交易者。

(3) 用戶憑證以公開金鑰的方式儲存於業務應用系統中，使用時除存取授權的身分核驗外，必須檢核該憑證的正確性、完整性與有效性。

(4) 用戶使用憑證執行交易訊息的簽章與加密時，必須確實瞭解並接受使用該憑證於相關業務系統之憑證使用業務限制範圍、交易限額、賠償限額的權利與義務規範，且合法使用於

憑證政策、本作業基準與相關業務規範所訂定的範圍。

4.5.2 信賴憑證者公開金鑰及憑證使用

信賴憑證者於信賴本憑證管理中心簽署之用戶憑證前，至少應進行以下必要之程序以決定是否信賴該憑證：

(1) 透過適當及安全之管道，取得最高層憑證管理中心自簽憑證。
(2) 檢查最高層憑證管理中心自簽憑證、政策憑證管理中心憑證、用戶憑證管理中心憑證及用戶憑證是否已過期。
(3) 檢查最高層憑證管理中心自簽憑證、政策憑證管理中心憑證及用戶憑證管理中心憑證之數位簽章是否有效且並未被廢止。
(4) 以用戶憑證管理中心憑證內之公開金鑰，檢驗用戶憑證內之數位簽章是否有效。
(5) 檢查用戶憑證未遭用戶憑證管理中心廢止或暫禁。

如未能通過前述檢驗，表示信賴憑證者取得之用戶憑證非本憑證管理中心所簽發，或憑證已失效，信賴憑證者不應信賴該用戶憑證。

4.6 憑證展期

憑證展期 (Renewal) 係指用戶識別資訊不變之情況下，重新簽發一張與原有憑證具相同金鑰、不同序號、以及效期延長之憑證。

4.6.1 憑證展期之事由

不提供憑證展期。

4.6.2 有權展期憑證者

不適用。

4.6.3 憑證展期程序

不適用。

4.6.4 通知用戶展期憑證之簽發

不適用。

4.6.5 展期憑證接受程序

不適用。

4.6.6 憑證機構公布展期憑證

不適用。

4.6.7 憑證機構通知其他機構展期憑證之簽發

不適用。

4.7 憑證及私密金鑰更新

憑證進行金鑰更新係指用戶重新產生一組公開金鑰及私密金鑰對，並以原有的註冊資訊向憑證機構申請憑證簽發。金鑰更新後之新憑證與舊有憑證具有相同的特徵及保證等級。

4.7.1 憑證金鑰更新之事由

憑證金鑰更新的事由請參見 3.3 節。

4.7.2 有權更新憑證金鑰者

用戶或其授權之代理人。

4.7.3 憑證金鑰更新程序

- 依 3.3 節之規定進行識別與鑑別。
- 依 4.3 節之規定簽發憑證。

4.7.4 通知用戶更新金鑰憑證之簽發

依 4.3.2 節之規定。

4.7.5 更新金鑰憑證接受程序

依 4.4 節之規定。

4.7.6 憑證機構公布更新金鑰憑證

依 4.4.2 節之規定。

4.7.7 憑證機構通知其他機構更新金鑰憑證之簽發

依 4.4.3 節之規定。

4.8 憑證變更

憑證變更係指憑證之公開金鑰不變，但其所記載之用戶名稱識別資訊須變更時，重新簽發憑證予用戶。

4.8.1 憑證變更之事由

本憑證管理中心不接受用戶進行憑證變更，如用戶之識別資訊或其他記載於憑證之資訊須變更時應依 4.9 之規定廢止憑證後，依 4.1、4.2、4.3、4.4 節規定重新申請憑證簽發。

4.8.2 有權變更憑證者

不適用。

4.8.3 憑證變更程序

不適用。

4.8.4 通知用戶變更憑證之簽發

不適用。

4.8.5 變更金鑰憑證接受程序

不適用。

4.8.6 憑證機構公布變更憑證

不適用。

4.8.7 憑證機構通知其他機構變更憑證之簽發

不適用。

4.9 憑證廢止及暫禁

4.9.1 憑證廢止之事由

於憑證仍然為有效期間內，當有下述情況時必須執行憑證廢止：

(1) 用戶執行：
- 用戶欲廢止該憑證的使用時，例如：公司員工的職務異動或離職時，為控管措施的安全考量，或用戶擬不繼續使用憑證而廢止。
- 憑證內容及用戶註冊相關資訊有更動時，例如：公司的整合與合併，或因特殊原因而更新公司的註冊名稱及註冊相關資料。
- 與憑證相關的私密金鑰有毀損、遺失、曝露、被篡改，或有為第三者竊用之慮時。

(2) 本公司逕行廢止用戶憑證：
- 因憑證系統的金鑰異動變更、或不適用、或憑證系統的整合需求。
- 憑證機構的業務結束營運管理而必須移轉至其他憑證機構的需求。
- 用戶使用憑證而為註冊中心或用戶憑證管理中心宣告未依據合約或作業規範履行應盡義務（如費用），或不當使用憑證而違反政府法令、規章、或業務使用規範時。
- 憑證內容的用戶相關資訊，不符合憑證政策、本作業基準或業務使用規範時，例如：用戶憑證內容與註冊資料不符，或因註冊資料輸入的疏忽。

(3) 權責單位：
- 主管機關或法院，因業務之需求依正式合法作業程序申請。

4.9.2 有權請求廢止憑證者

用戶（或其授權之代理人）、註冊中心、本公司、主管機關或合法授權的第三者皆有權申請憑證的廢止。

(1) 用戶執行：
- 用戶可依其需求，依註冊中心作業規範申請廢止用戶憑證。

(2) 註冊中心（本公司）：
- 註冊中心（本公司）申請廢止用戶憑證時，必須依「4.9.3 憑證廢止程序」處理，且必須依註冊中心與用戶間的合約與相關作業規範辦理。

(3) 有權責的第三者：
- 公司授權人員於公司合法授權下，廢止用戶憑證。
- 用戶財產合法繼承人的申請，註冊中心必須依相關作業規範，驗證用戶的死亡與合法繼承人的身分。
- 因法院訴訟或仲裁經註冊中心依正式合法作業程序申請。
- 主管機關依正式合法作業程序申請。

4.9.3 憑證廢止程序

IXML Plus 憑證廢止程序：

(1) 依據註冊中心或用戶憑證管理中心的安控措施登錄註冊管理系統，經註冊中心檢核用戶身分識別無誤後，或填寫憑證廢止申請單，經由註冊中心的身分識別無誤後，執行憑證廢止作業。註冊中心將用戶憑證廢止請求訊息以註冊中心的簽章保護後，傳遞至用戶憑證管理中心申請用戶憑證廢止。
(2) 用戶憑證管理中心收妥註冊中心的用戶憑證廢止申請訊息時，檢核申請訊息註冊中心與用戶身分及訊息的合法性與完整性，正確無誤後，依據憑證廢止作業規範執行用戶憑證廢止作業，並將廢止憑證回覆訊息通知註冊中心。
(3) 註冊中心收妥用戶憑證管理中心的用戶廢止憑證回覆訊息時，檢核回覆訊息的合法性與完整性正確無誤後，回覆予申請的用戶。

主管機關、法院訴訟或仲裁機構及其他有權責者，亦必須依據註冊中心的作業規範，填具廢止申請單向註冊中心申請廢止該憑證。

憑證機構的業務因故結束營運管理時，必須依據主管機關電子簽章法的作業規範及與註冊中心的合約規範，廢止用戶憑證。

用戶於憑證仍為有效期內，因有安全的顧慮或擬不使用該憑證時，除向註冊中心（或用戶憑證管理中心）申請廢止憑證，亦必須立刻通知相關業務使用單位停止該憑證的使用。於用戶憑證管理中心完成廢止憑證的寬限期內，因使用該張憑證所衍生的糾紛，如非為用戶憑證管理中心/註冊中心業務處理上的過失，本公司/註冊中心不負賠償責任。

4.9.4 憑證廢止請求提出期限

用戶有廢止憑證的需求時，必須立刻向註冊中心（或用戶憑證管理中心）申請憑證的廢止。如懷疑或證實金鑰遭破解或有其他安全事項須廢止憑證，用戶應於 24 小時內提出。

4.9.5 憑證機構處理憑證廢止請求時限

註冊中心（或用戶憑證管理中心）收到用戶憑證廢止請求訊息時應於 24 小時內完成，但於營運或上班時間必須立刻處理。

IXML Plus 憑證，依據用戶憑證管理中心憑證系統的作業規範，應於 24 小時內產生憑證廢止清冊，故憑證請求廢止的寬限期間為 24 小時。

4.9.6 信賴憑證者憑證廢止檢驗規定

用戶或信賴憑證者於業務應用系統有使用憑證時，除驗證憑證的有效性外，尚須檢核該

憑證是否為廢止憑證。考量業務風險因素，相關業務應用系統可依據系統安全度的需求，在一定的時間內主動至用戶憑證管理中心索取或查詢憑證廢止清冊狀態。

4.9.7 憑證廢止清冊簽發頻率

至少於 24 小時內簽發憑證廢止清冊，故憑證廢止清冊的簽發頻率為 24 小時。

4.9.8 憑證廢止清冊最大潛在因素

不做規範。

4.9.9 線上憑證廢止/狀態查詢服務

不提供線上憑證狀態協定查詢服務(OCSP)，故用戶必須使用憑證廢止清冊(CRL)進行憑證狀態查核。

4.9.10 線上廢止/狀態查詢檢驗規定

不適用。

4.9.11 其他形式之廢止公告

無規定。

4.9.12 金鑰遭破解之特殊規定

憑證管理中心之簽章金鑰遭破解時，應依以下程序辦理：

(1) 產生新的簽章用金鑰對及相對應的新憑證。
(2) 廢止所有已簽發之憑證，使用新的簽章金鑰簽發憑證廢止清冊，憑證廢止清冊包含所有已簽發之未到期憑證資訊（含金鑰遭破解前簽發之已廢止憑證）。
(3) 告知用戶。
(4) 使用新的簽章用金鑰來簽發新憑證予用戶。
(5) 安全地遞送新憑證予用戶。

用戶之金鑰已證實或有足夠理由相信遭到破解時，應於 24 小時內告知本憑證管理中心廢止憑證。

4.9.13 憑證暫禁之事由

「暫禁」即為暫時停用，「解禁」即為恢復使用，用戶憑證暫禁的作業方式悉遵照用戶憑證管理中心與註冊中心的業務需求與作業規範辦理。用戶於憑證仍然有效期間內，當有下述

情況時可執行憑證的暫禁：

(1) 用戶：
- 憑證的私密金鑰有可能遺失、洩露的不安全疑慮時，為保留用戶的憑證使用權利而不申請廢止憑證時，用戶欲暫禁該憑證的使用。
- 用戶欲暫時停止使用該憑證一段時間。

(2) 註冊中心或本公司：
- 用戶使用憑證而為註冊中心或本公司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的疑慮時。

(3) 權責單位：
- 主管機關或法院，因業務之需求依正式合法作業程序申請。
- 若金鑰遭破解不得使用憑證暫禁之程序，應依 4.9.12 節辦理。

4.9.14 有權請求憑證暫禁者

用戶（或其授權之代理人）、註冊中心、本公司、主管機關或合法授權的第三者皆有權執行憑證的暫禁。

(1) 用戶執行：
- 用戶可依其需求，依註冊中心作業規範申請暫禁用戶憑證。

(2) 註冊中心（本公司）：
- 註冊中心（本公司）申請暫禁用戶憑證時，必須依 4.9.13 節處理，且必須依註冊中心與用戶間的合約與相關作業規範辦理。

(3) 有權責的第三者：
- 公司授權人員於公司合法授權下，申請暫禁用戶憑證。
- 因法院訴訟或仲裁經註冊中心依正式合法作業程序申請。
- 主管機關依正式合法作業程序申請。

4.9.15 憑證暫禁程序

(1) 依據註冊中心或用戶憑證管理中心的安控措施登錄註冊管理系統，經註冊中心檢核用戶身分識別無誤後，或填寫憑證暫禁申請單，經由註冊中心的身分識別無誤後，執行憑證暫禁。註冊中心將用戶憑證暫禁請求訊息以註冊中心的簽章保護後，傳遞至用戶憑證管理中心申請用戶憑證暫禁。

(2) 用戶憑證管理中心收妥註冊中心的用戶憑證暫禁申請訊息時，檢核申請訊息註冊中心與用戶身分及訊息的合法性與完整性，正確無誤後，依據憑證暫禁作業規範執行用戶憑證暫禁作業，並將回覆訊息通知註冊中心。

(3) 註冊中心收妥用戶憑證管理中心的用戶暫禁憑證回覆訊息時，檢核回覆訊息的合法性與完整性正確無誤後，回覆予申請的用戶。

用戶或其他有權者提出暫禁用戶的憑證要求後，至用戶憑證管理中心於 24 小時內實際公布暫禁該用戶憑證為止之期間內，用戶必須即刻依據業務系統的規範，暫禁憑證的使用，並即刻通知相關信賴憑證者停止該憑證的使用。當該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，如用戶憑證管理中心與註冊中心執行處理作業時，符合本作業基準與相關的作業規範，且用戶已即刻通知相關信賴憑證者停止該憑證的使用，則信賴憑證者必須負損害賠償責任；於提出暫禁用戶憑證之期間內，如用戶未依據業務系統的規範暫禁該憑證的使用，及即刻通知相關信賴憑證者停止該憑證的使用，則用戶必須負損害賠償責任。

暫禁憑證於限制之原因解除後，憑證用戶擬繼續使用該張憑證，且憑證之有效期限尚未到期時，憑證用戶可向註冊中心申請憑證之解禁，經由註冊中心身分識別無誤後，註冊中心將用戶憑證解禁請求訊息以註冊中心的簽章保護後，傳遞至用戶憑證管理中心申請用戶憑證解禁，使憑證成為有效且可以使用。

4.9.16 憑證暫禁期間限制

用戶執行憑證暫禁完成後，於憑證有效期間終止前，如未執行憑證的解禁，則此張憑證皆存在憑證廢止清冊中，為無法使用的憑證。

IXML Plus 憑證暫禁的時效為，當用戶憑證經完成暫禁後存放至憑證廢止清冊中，至用戶申請憑證解禁完成，而憑證從憑證廢止清冊中移轉成有效憑證為止的期間。

憑證暫禁的時效最長為用戶憑證管理中心簽發用戶憑證的有效期限。

4.10 憑證狀態服務

4.10.1 服務特性

- 本憑證管理中心提供憑證廢止清冊(CRL)下載服務供用戶或憑證信賴者查詢憑證狀態。
- 憑證廢止清冊之下載點註記於憑證 cRLDistributionPoints 延伸欄位中。
- 本憑證管理中心不提供線上憑證狀態協定(OCSP)查詢服務。

4.10.2 服務之可用性

本憑證管理中心提供 7 x 24 憑證廢止清冊(CRL)下載服務，CRL 簽發頻率參考 4.9.7 節之說明。

4.10.3 附加功能

無規定。

4.11 憑證終止

當本憑證管理中心簽發之憑證效期屆滿、憑證廢止或本憑證管理中心結束營運時，已簽發之憑證即告失效。

4.12 金鑰託管及復原

4.12.1 私密金鑰託管及復原政策與施行

本憑證管理中心之私密金鑰不允許託管。用戶之私密金鑰不禁止被託管。

4.12.2 加密金鑰封裝及復原政策與施行

不做規範。

5.實體、管理及作業流程控管

5.1 實體控管

5.1.1 建築物與位置

憑證管理中心所在機房，具備防震、防水、防火、門禁保全系統、防入侵門禁監視與防破壞警報系統，符合儲存高重要性及敏感性資訊的機房設施水準，以防止未經授權者存取本憑證管理中心之相關設備。

5.1.2 實體進出管制

作業人員欲進入憑證中心機房必須通過三道 IC 卡門禁管制，其中至少一道門禁具備生物特徵鑑別裝置（包含但不限於指紋、臉部或掌形）；憑證中心電腦主機所在位置至少具備須兩人以上經身分驗證之實體控管措施；具備 24 小時 CCTV 位移監控錄影設備及紅外線防入侵警報系統，以記錄進出機房之狀況及預防未經授權者進入機房。

憑證管理中心運作的相關私密金鑰與備份資料皆妥善、安全的存放於本中心設有監控錄影系統保護的保險櫃內，憑證系統運作的相關作業人員，執行憑證管理作業時，皆有監控錄影設備的監測。

憑證管理中心運作的硬軟體及硬體密碼模組 (HSM) 皆置於有監控錄影系統保護的環境下，憑證系統安全控管人員，執行金鑰管理相關作業時，皆有監控錄影設備的監測。

5.1.3 電力與空調

憑證管理中心機房設有柴油發電機及不斷電系統 (Uninterruptible Power Supply; UPS)，當一般供電系統異常時，會自動切換至柴油發電機供電，切換過程由 UPS 提供穩定之電力。

憑證管理中心機房具備獨立之空調系統，確保系統運作的穩定與提供最佳之工作環境，並定期執行維護與測試。

5.1.4 防水處理

憑證管理中心機房的房屋為密閉式建築物，除內部可進出的出入門外，外部皆為混凝土建築物，雨水無法進入，且樓層地板裝置高架地板無進水之顧慮。

5.1.5 防火

憑證管理中心之機房建築物的材質為防火材質並配置具有中央監控系統的滅火設備，於

偵測到發生火災時，能自動啟動滅火功能，並設置手動開關於各主要出入口處，以供現場人員於緊急情況時以手動方式操作。

5.1.6 媒體儲存

媒體儲存環境，具有對磁性媒體防磁、防靜電干擾的設備與環境，重要資料媒體則儲存具高度防火功能的保險櫃，其中一份備份資訊的媒體儲存於具有安控措施的異地處所，備份及保存資訊的儲存媒體，定期執行測試與驗證資訊的有效性與可使用性。

5.1.7 廢棄處理

憑證管理中心於憑證系統所使用的硬體設備、磁碟機與硬體密碼模組 (HSM) 等，於廢棄不使用時，商業敏感性及機密性資訊必須經過安全的清除與銷毀，且經由稽核單位的驗證，並留存查核文件。

文件與媒體資訊儲存有商業敏感性及機密性資訊時，於廢棄處理時必須經安全的銷毀，該資訊皆無法回復與存取使用，且經由稽核單位的驗證，並留存查核文件。

5.1.8 異地備援

憑證系統運作所須的相關媒體資訊、文件規範，備份後儲存於具備中央恆溫、恆濕空調系統、防磁、防靜電干擾，且具有中央監控攝影機監控錄影，與人員進出存取須經過合法授權之高度安全控管的異地備援環境。

憑證系統每日的交易備份紀錄檔，每週完整的系統備份紀錄檔，皆備份後儲存於高度安全控管的異地。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與可使用性。

5.2 作業程序控管

5.2.1 信賴角色

本公司於公開金鑰基礎建設的架構下，簽發的憑證必須在具備嚴密性與安全性的作業流程下之憑證系統，由本公司扮演的可信賴且具公信力的機構，公正與嚴謹的執行。

本公司作業人員的工作指派，均依作業規範選用適任且職責獨立的可信賴人員，於具有安全控管機制的憑證系統下，依本公司內部憑證作業規範及作業手冊，以及註冊中心的內部作業規範及作業手冊確實執行業務。

本公司於憑證系統的運作上，為使職務與權責的區分，及職務的備援功能不危及整體系

統的安全性與營運的完整性，各業務可信賴的執行人員與職務詳述如下。

5.2.1.1 憑證管理中心

- 經理負責管理、監督整個憑證系統業務的營運。
- 稽核人員（本公司非屬憑證管理中心之作業人員），負責稽核、監督本公司憑證系統業務的運作工作內容詳 8.4 節。
- 憑證系統業務營運的監督人員，至少二員以上互為業務上的備援，負責系統運作資源的管理與授權（例如：作業人員的授權與建置，系統資源的異動與調整，但不可執行憑證簽發的相關業務運作）。
- 憑證系統業務營運的管理人員，至少二員以上互為業務上的備援，負責系統運作時相關系統規範、環境參數的設定及管理性功能的作業（例如：CA 金鑰及憑證的變更，但不可以執行用戶憑證簽發、用戶資料建置等作業）。
- 憑證系統業務營運的操作人員，負責系統運作時用戶資料建置、執行憑證簽發等相關作業及報表與批次作業。
- 其他硬軟體系統的維護人員、硬體密碼模組 (HSM) 作業人員及系統資源控管人員，負責其授權的相關作業。

5.2.1.2 註冊中心

- 註冊中心負責人，負責管理、監督用戶註冊業務的運作。
- 管理人員，至少二員以上互為業務上的備援，負責系統運作時相關系統規範、環境參數的設定及管理性功能的作業（例如：註冊中心金鑰及憑證的變更，註冊中心作業人員的建置等作業）。
- 作業人員負責用戶註冊資料的建置，註冊文件合約、身分證明文件及註冊申請人身分的審核驗證，及發送用戶註冊資料至用戶憑證管理中心。如須執行雙重驗證時，則須加入管理人員的用戶註冊資料確認，始可發送用戶註冊資料至用戶憑證管理中心。
- 其他註冊中心硬軟體系統的維護人員、硬體密碼模組 (HSM) 作業人員、監督人員及稽核人員，各自負責其所授權的相關作業。

5.2.2 作業人員需求人數

本公司執行各種業務的作業人員，其權責為獨立且不重疊，依監督人員、管理人員、作業人員、稽核人員、硬軟體系統的維護人員與硬體密碼模組 (HSM) 作業人員不同業務的特性指派適當數目的人員擔任。例如：CA 金鑰的建置或變更、用戶資訊的異動等相關作業皆有二位以上的作業人員才可以執行；金鑰基碼建置的作業人員則必須依金鑰作業安全控管程序的規定，至少須二位以上的金鑰安全管理人員同時進行才可以變更與建置，且有相互備援的功能。

5.2.3 角色的識別與鑑別

執行各種業務的監督人員、管理人員、操作人員、系統維護人員與系統資源控管人員，於系統資源的使用上皆有一組依業務區分且唯一的身分識別碼、IC 卡及相關的身分識別驗證密碼（或是指紋辨識驗證），以達到系統資源使用者的身分識別與驗證。相關作業人員依業務需求執行的作業功能，每筆皆有詳細的紀錄，確保系統資源使用的可稽核性，與系統安全威脅及風險評估的管控。

5.2.4 角色隔離

如 5.2.2 規定。

5.3 人員控管

5.3.1 背景、適任條件與經歷

本公司執行各種業務的作業人員，必須具備忠實、可信賴及工作的熱誠度，無影響本公司作業的其他兼職工作，無本公司作業上因工作的疏失、不盡責的缺失紀錄，無違法犯紀的不良紀錄。

- 作業人員，至少具備憑證機構作業的實務經驗，或經過憑證機構相關作業的訓練而通過測驗者。此職務本公司因人力資源不足時，可以委由外包人員擔任。
- 管理人員與監督人員，至少具備憑證機構作業的實務經驗，具有電腦系統規劃、開發、營運管理的經驗更佳，且必須由公司選派適當人員擔任，不可以委由外包人員擔任。

5.3.2 背景審核程序

憑證系統運作的人員，由人事管理相關部門依監督人員、管理人員、作業人員所訂定的審核規範，執行身分背景安全的審查，以及本公司部門相關作業的實務與經歷的審查通過後，始可任職，且每年必須依各種作業人員的職務特性，執行安全、實務與經歷的審查，該員是否適任相關的工作以做為執行工作調整或調派的依據。

5.3.3 教育訓練

憑證系統運作的人員，皆依其職務，施予憑證系統運作所應具備的軟硬體功能、作業程序、安控程序、災變備援作業規範、PKI 公開金鑰作業及憑證政策與憑證實務作業基準與其他資訊安全相關作業規範的訓練，認證系統有異動或有新系統的加入時，亦須給予適當的教育訓練。

本公司須訂定一套憑證系統有關硬軟體、應用系統與安全管理系統之完整的教育訓練規

範，於新進人員及認證系統或有異動時，施行相關技能的教育訓練。教育訓練完成後有詳實的成果紀錄，做為相關作業人員工作委任的參考。

5.3.4 教育訓練的頻率與需求

憑證系統運作的相關人員，其執行憑證系統運作的相關知識與技能，每年至少檢討一次，並給予適當的再教育的訓練。

憑證系統功能的更新、新系統的加入，或相關知識與技術的進步與更新，皆須對系統運作的相關人員執行教育訓練。

5.3.5 職務的輪調

配合系統運作的需求與相關作業人員工作的適任性，本公司會選派適任的人選輪調至適合的工作歷練，但調派前必須施以適當知識與技能的教育訓練。

- 系統管理人員調離原職務滿 1 年後，才可轉任憑證主管人員或稽核人員。
- 憑證主管人員調離原職務滿 1 年後，才可轉任系統管理人員或稽核人員。
- 稽核人員調離原職務滿 1 年後，才可轉任系統管理人員或憑證主管人員。
- 擔任操作人員滿 2 年，且已接受相關教育訓練並通過審核後，才可轉任系統管理人員、憑證主管人員及稽核人員。

5.3.6 非授權作業的處罰

憑證系統運作的相關作業人員，因故意或疏失而執行非自己職務上的作業時，無論造成或未造成憑證系統安全的問題，皆應即刻呈報監督管理者，依相關作業之規範處理。

5.3.7 委外人員需求

因人力資源不足而委由外包人員擔任操作人員時，除必須依業務的工作內容簽訂相關的保密合約外，該委外人員的權利與義務與本公司之內部操作人員相同，必須施以職務上知識與技能的教育訓練，且遵守相關作業規範與法律規範。

5.3.8 作業文件需求

為使憑證系統的運作正常及順暢，必須提供相關作業人員執行系統運轉的作業文件，至少包含如下：

(1) 硬體、軟體作業平台的操作文件、網路系統與網站相關的操作文件、硬體密碼模組 (HSM) 的操作文件。
(2) 憑證管理中心與註冊中心憑證系統的相關操作文件、用戶端憑證系統的相關操作文件。

(3) 憑證實務作業基準、憑證政策及相關作業規範文件。
(4) 憑證系統內部作業文件，例如：系統備援與回復作業文件、異地災變備援與回復作業文件、例行工作作業文件。

5.4 稽核記錄程序

5.4.1 事件紀錄類型

稽核紀錄至少應保存如下之資訊：

(1) 用戶註冊或註銷資訊的保存，包含合約、註冊文件、申請表單與註冊交易相關訊息。
(2) 憑證系統運作使用到的相關公開金鑰與基碼，其產生、建置、變更之成功與失敗的紀錄。
(3) 憑證管理中心之金鑰與憑證的產生、建置、變更之成功與失敗的紀錄。
(4) 用戶憑證申請交易處理與回覆之成功與失敗相關的紀錄。
(5) 憑證系統運作之稽核的相關紀錄，與憑證系統運作相關的通訊 (E-mail) 紀錄。
(6) 憑證廢止申請交易處理與回覆、憑證廢止清冊處理的相關訊息紀錄。
(7) 進出入憑證管理中心機房之申請表單、作業人員身分識別 IC 卡進/出 CA 機房的紀錄報表、CA 機房工作日誌紀錄簿、作業人員執行業務功能的簽名紀錄，及作業人員進/出 CA 機房監控攝錄影機的媒體紀錄。
(8) CA 主機系統硬、軟體、應用系統，及 CA 憑證系統的作業異動申請單與系統異動變更的紀錄，作業人員執行系統參數變更作業的紀錄。
(9) 經由網際網路至憑證系統，執行憑證作業與存取系統資源有關的交易紀錄。

5.4.2 紀錄處理頻率

新系統開始加入營運時，每日執行憑證系統運作相關紀錄的查核，當系統調整與修改至正常運作狀況時，每日只執行憑證系統運作異常紀錄的查核，且應定期（至少每週）依業務需求隨時執行正常紀錄的詳細查核。

可能影響系統安全的異常事件稽核紀錄，須由本公司相關的系統與文件紀錄依稽核作業規範詳細查核，且記錄事件的查核、處理過程，及追蹤改善措施的執行。

執行憑證系統運作紀錄的查核時，亦查核稽核紀錄是否為非授權作業人員修改，並記錄事件的查核、處理過程，及追蹤改善措施的執行。

5.4.3 稽核紀錄保留期限

相關稽核紀錄報表與媒體資料至少應保留七年；異常狀況的系統紀錄及報表至少應保留九年；錄影媒體紀錄除特殊異常狀況必須保留外，以每三個月為一週期循環使用。

5.4.4 稽核紀錄的保護

本公司各憑證系統的稽核紀錄資訊之保護措施，依各憑證系統所提供的安控措施保護稽核紀錄，具有資源控管與身分識別的安全機制。

稽核紀錄由權責獨立的授權備份作業人員，只具有可執行稽核紀錄的讀取功能，至少每週執行備份一次，且一份備份資訊儲存於具安全控管的異地備援中心。

憑證系統的稽核紀錄資訊之保護，為只可讀取且無法寫入與清除的安全控管系統所保護，且只有與業務有關的稽核人員才可以讀取。

文件稽核紀錄保存的執行，亦具有安控措施的保護，且一份保存資訊儲存於具安控措施的異地備援中心。

5.4.5 稽核紀錄備份程序

各憑證系統的稽核紀錄資訊檔與文件檔，每週皆依據稽核紀錄備援作業程序執行系統的整理與備份，保存於稽核紀錄資訊檔備份的媒體，並運送一份至具安控措施的異地備援中心儲存備援。

5.4.6 稽核紀錄彙整系統

各種稽核紀錄的蒐集由憑證系統開啟至系統關閉為止，各憑證系統稽核紀錄的蒐集，為經由作業系統、憑證系統與憑證管理作業人員，以電腦自動或人員手動的方式記錄之，當自動稽核紀錄功能無法正常運作且 CA 認證系統必須繼續提供服務時，則採人工稽核紀錄功能，相關事件種類至少如下：

事件種類	紀錄蒐集 （電腦自動或人員手動）	紀錄者
1.作業系統安全參數的變更	自動	作業系統
2.憑證系統的開啟與關閉	自動	作業系統
3.登錄 (Log-in) 與登出 (Log-off) 系統	自動	作業系統
4.系統用戶 (User) 的建置、修改與刪除	自動	作業系統
5.用戶 CA 系統建置與變更	自動	CA, RA 憑證系統
6.金鑰與憑證的產生、簽發與廢止	自動	CA, RA 憑證系統
7.憑證用戶資訊的建置、修改與刪除	自動	CA, RA 憑證系統
8.經網際網路的交易資訊	自動	網際網路系統
9.備份與復原	自動與人工	系統與人員
10.系統環境參數檔的變更	人工	作業人員
11.硬體與軟體系統的更新	人工	作業人員
12.系統維護	人工	作業人員

13.人員的異動	人工	作業人員
14.其他憑證系統運作的相關表單	人工	作業人員

5.4.7 對引發事件者之告知

作業人員於執行憑證系統，出現影響安控措施的異常事件時，必須通知系統安全管理人員，依系統異常作業處理規範採取適當的處理措施。

5.4.8 脆弱性評估

每年至少進行一次以下所列的各種弱點評估：

(1) 作業系統的脆弱性評估。

(2) 實體設施的脆弱性評估。

(3) 憑證管理系統的脆弱性評估。

(4) 網路的脆弱性評估。

5.5 紀錄歸檔

5.5.1 歸檔紀錄類型

本公司為使憑證系統能穩定的運作，必須將系統環境建置檔、與用戶相關的合約條款、用戶註冊資料的相關資訊、用戶憑證及廢止憑證資料檔、交易資料檔、稽核資料檔、憑證管理中心金鑰與憑證變更資訊、憑證實務作業基準、憑證政策、憑證管理中心系統等之資料執行備份保存。

5.5.2 歸檔紀錄保留期限

除配合主管機關訂定的資訊保存期限規範，本公司訂定公開金鑰系統運作有關資訊的保存期限至少如下：

- 憑證實務作業基準、憑證政策與相關作業手冊、及用戶的註冊申請表單相關合約條款、身分證明文件等資料至少保留至有效期限結束後十年。
- 用戶申請、更新、展期、廢止的憑證，或過期憑證，至少保留至憑證有效期限結束後十年。
- 用戶憑證申請、查詢與廢止的交易訊息紀錄，至少保留至憑證有效期限結束後十年。
- 政策憑證管理中心 (PCA) 與用戶憑證管理中心 (UCA) 之金鑰與憑證等相關的異動資料至少保留至憑證有效期限結束後十年。
- 最高層憑證管理中心 (RCA) 之金鑰與憑證等相關的異動資料至少保留至憑證有效期限

結束後十五年。

5.5.3 歸檔紀錄的保護

金鑰、憑證、交易資料、稽核資訊、憑證實務作業基準與註冊文件等相關保存資料的保護，皆儲存於具安控措施且有防潮濕的中央空調的保護環境下，非授權人員無法存取，非合乎相關法律與作業規範的需求，任何人皆無法任意取得。

另一份保存資料儲存於具安控措施、防潮濕的中央空調環境下之異地備援中心。

本公司所保存及保護的用戶基本資料與身分識別資料，非經主管機關或法院因處理交易糾紛的需求而經合法的申請，絕不任意予第三者知悉。

5.5.4 歸檔紀錄的備份程序

金鑰、憑證、交易資料等相關資料，依備份與備援回復的作業程序，每日、週、月的整理歸檔及備份，一份儲存於本公司具安控措施的環境下，且一份保存資料儲存於具安控措施的異地備援環境。當憑證系統異常無法開啟時，依系統備份與回復作業手冊，以保存的備份資料執行憑證系統的異常回復作業。

5.5.5 歸檔紀錄之時戳要求

本公司於憑證系統運作時，有關的硬軟體設施與系統，或系統參數系統資源的變更異動，皆有時序的註記，如由電腦作業系統或憑證系統自動產生時，時戳 (Time-stamp) 由電腦的時鐘讀取而自動加入紀錄資訊內；如是由作業人員產生的紀錄資訊，則由作業人員手寫加入作業表單紀錄資訊內，以做為日後追蹤時的時間參考依據。

用戶於執行註冊以及憑證申請、更新、廢止、暫禁與查詢等有關的作業時，交易的訊息內容具有時戳的註記，是經由電腦作業系統或憑證系統自動產生，時戳 (Time-stamp) 由電腦的時鐘讀取而自動加入紀錄資訊內。

5.5.6 歸檔紀錄彙整系統

本公司憑證系統作業相關的保存紀錄資訊，皆由本公司內部的作業人員執行，內部的相關系統於具有資源權責獨立及安全的管控措施下產生；稽核紀錄蒐集的保存資訊亦是由內部的管控系統所產生；憑證系統運作的相關文件保存紀錄，由權責的業務相關人員蒐集與管理。

5.5.7 取得及驗證歸檔紀錄之程序

本公司憑證系統作業相關的保存紀錄資訊的驗證，依本公司的內部管理作業規範，至少一年一次或依據業務的需求不定期抽查驗證；或執行保存紀錄資訊的驗證稽核作業時，由權

責的稽核人員依內部稽核作業規範抽查驗證；或於執行異地災變備援測試時，執行保存紀錄的驗證。

5.6 金鑰更新

5.6.1 用戶金鑰變更

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

用戶金鑰使用有效期限結束前，填具憑證更新申請單向註冊中心辦理用戶金鑰變更申請作業完成後，用戶可以產生新金鑰對向用戶憑證管理中心或註冊中心申請新憑證的簽發，相關作業參考 3.3.1 節之規定。

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

5.6.2 用戶憑證管理中心金鑰變更

(1) 用戶憑證管理中心金鑰使用有效期限結束時，可以產生新金鑰對向政策憑證管理中心申請新憑證的簽發，完成後以新私密金鑰簽發用戶的新憑證申請，且以舊金鑰繼續簽發該金鑰簽發的憑證之用戶憑證廢止作業，至該舊金鑰的生命有效期限結束，並即刻通知註冊中心。
(2) 當用戶憑證管理中心舊金鑰有不安全顧慮且有效期限尚未結束時，必須先向政策憑證管理中心申請廢止舊憑證，才可以產生新金鑰對申請新憑證的簽發。完成後以新私密金鑰簽發用戶新憑證的申請，與廢止憑證的簽發，且必須即刻以最迅速的方式通知用戶與註冊中心，舊私密金鑰所簽發的用戶憑證與憑證廢止清冊皆為無效，用戶必須重新產生新金鑰對向用戶憑證管理中心申請新憑證的簽發。

5.6.3 政策憑證管理中心金鑰變更

(1) 政策憑證管理中心金鑰使用有效期限結束時，依憑證鏈產生下一組新金鑰對，並向 RCA 申請新憑證的簽發，以新私密金鑰簽發用戶憑證管理中心新憑證與廢止憑證簽發的申請，且以舊金鑰繼續簽發該舊金鑰簽發的用戶憑證管理中心憑證之憑證廢止清冊，至該舊金鑰的生命週期結束，並即刻通知用戶憑證管理中心。
(2) 當政策憑證管理中心舊金鑰有不安全顧慮且有效期限尚未結束時，必須先廢止舊憑證，才可以依憑證鏈產生新金鑰對，及向最高層憑證管理中心申請新憑證的簽發。完成後才可以新私密金鑰簽發用戶憑證管理中心新憑證的申請與廢止憑證的簽發，且必須即刻以

最迅速的方式通知用戶憑證管理中心，舊私密金鑰所簽發的用戶憑證管理中心憑證與憑證廢止清冊皆為無效，用戶憑證管理中心必須重新產生新金鑰對向政策憑證管理中心申請新憑證的簽發。

5.6.4 最高層憑證管理中心金鑰變更

(1) 最高層憑證管理中心金鑰使用有效期限結束前，產製一對新金鑰對及自簽憑證，與此張憑證的指紋辨識碼 (Fingerprint)，且以舊金鑰繼續簽發該金鑰簽發的政策憑證管理中心憑證之憑證廢止作業，至該舊金鑰的生命週期結束，並立即公告此新自簽憑證的指紋辨識碼，並即刻通知政策憑證管理中心。
(2) 當最高層憑證管理中心舊金鑰有不安全顧慮且有效期限尚未結束時，必須先廢止舊憑證，才可以產生新金鑰對及自簽憑證，與此張憑證的指紋辨識碼 (Fingerprint)；且以最迅速的方式通知政策憑證管理中心，舊有的憑證皆無效，必須重新產生新金鑰對向最高層憑證管理中心申請新憑證的簽發。

當最高層憑證管理中心私密金鑰遭破解時，立刻廢止全部政策憑證管理中心的憑證，並依憑證鏈的作業規範通知用戶憑證管理中心，即刻廢止全部用戶的憑證，且通知業務應用系統停止使用憑證系統所簽發的憑證。

5.7 金鑰遭破解及災變復原程序

5.7.1 金鑰遭破解及緊急應變處理程序

本憑證管理中心訂定有緊急應變處理程序和災難復原計畫，以書面記載業務持續計畫與災變復原程序，內容包含當發生災難、安全性遭破解以及營運中斷事件時，對用戶及信賴憑證者之告知程序；以上程序本憑證管理中心將每年定期檢視或修訂。

5.7.2 電腦資源、軟體及資料損毀之處理程序

憑證系統使用的電腦軟體資源、或憑證系統運作相關的資料有異常毀損時，依系統備份與回復作業手冊，可以由內部備份媒體資料、或移送異地的備份媒體資料執行憑證系統的復原作業，使系統能繼續且正常營運。

當憑證系統使用的電腦硬體資源異常毀損時，可以由內部的硬體備援設備，與相關的備份電腦軟體資源及憑證系統運作備份資料，依系統備份與回復作業手冊，重新安裝、建置與復原憑證系統，而使系統正常營運。

5.7.3 憑證機構金鑰遭破解之處理程序

若憑證管理中心金鑰疑遭破解或遺失（雖尚未確定是否遭破解），則須進行下列程序：

(1) 必須儘快透過註冊中心以電子郵件、書面或其他方式，通知所有用戶。
(2) 依 6.1 節的規定產生新的金鑰對並交由上層憑證管理中心簽發新憑證。
(3) 廢止所有有效憑證，使用新的簽章金鑰簽發憑證廢止清冊，憑證廢止清冊包含所有未到期憑證。
(4) 依 4.3 節的程序，簽發新的憑證給各用戶。

憑證管理中心必須調查，並向政策管理中心報告金鑰遭破解或遺失之原因，以及採取何種措施以避免發生相同狀況。

5.7.4 災變後之營運持續能力

憑證系統運作所使用的相關安全設施，於天災與地變時毀損時：

(1) 如果在回復使用的相關安全設施至正常運轉之前，不會影響憑證系統的運作，則儘速修護或更新至正常運轉狀態，不至於影響憑證系統的正常運作。
(2) 當足以造成憑證系統運作的危害時，必須立刻緊急關閉憑證系統的運作，且儘速修護或更新相關安全設施至正常運轉狀態後，才開啟憑證系統的運作。如果於作業規範的時間內無法修護或更新相關的安全設施時，則必須執行異地災變復原計劃，於異地正式開啟憑證系統的營運作業。
(3) 如發生的災變已嚴重損害憑證系統運作使用的相關安全設施時，則必須立即執行異地災變復原計劃，回復憑證系統的運作功能。

為避免因天災與地變而造成憑證系統運作的停頓，TWCA 已規劃與建置一套於異地的業務回復作業計劃，及異地災變備援的復原系統，將憑證系統運作所需要硬軟體系統與設施、憑證資訊相關的媒體與文件、及作業規範與業務系統回復文件，於離開本公司營運系統適當距離處的異地備援中心，建置系統與儲存媒體與文件。

異地災變備援的業務復原系統，依業務需求每年至少執行一次災變復原計劃的人員訓練與測試演練，並配合實際作業環境隨時更新作業規範與業務系統回復文件，與留存測試紀錄文件以備稽核作業的查核，以期達成當有異常天災或地變時，憑證系統的運作至少能於 24 小時內立刻回復且繼續營運，而將對業務系統運作的影響風險減少至最低。

5.8 憑證機構終止服務

本公司因故結束任一系統營運時，須對業務系統運作的影響減少至最低程度，而將相關認證業務穩定的轉移至安全且公正客觀的其他憑證機構繼續運作。

於業務正常結束、或合約終止、或公司重整而無安全的考量因素時：

- 於終止服務日之三十日前通報主管機關。

- 於終止服務日之三十日前，將終止服務及由其他憑證機構承接相關業務之事實通知用戶。
- 將終止服務當時仍具效力之用戶憑證的權利，安排由承接相關業務之其他憑證機構承接。
- 於高度安全且無安全顧慮的作業環境下，廢止結束系統營運之憑證中心與全部用戶的憑證，將結束的憑證管理中心相關私密金鑰與憑證、全部用戶憑證與憑證廢止清冊，移轉至承接的憑證機構。
- 將憑證政策、本作業基準、本公司相關作業手冊文件、用戶合約與註冊資料、稽核紀錄、歸檔資料、憑證狀態資料及其他業務承接所必須的相關文件，移轉至承接的憑證機構，至少妥善安全的保存七年。
- 將結束系統營運憑證管理中心之相關私密金鑰完全清除乾淨，並向用戶正式宣告，認證業務已移轉至承接的憑證機構繼續營運，且儘可能的協助接任者執行認證業務憑證的簽發。
- 於業務異常結束（法院宣告破產、或不合法）時，本公司必須儘早向用戶公告事實，且必須執行如業務正常結束時的作業程序，將對用戶業務系統運作的影響減少至最低程度。

6.技術安全控管

6.1 金鑰對的產製及安裝

6.1.1 金鑰對的產生

憑證管理中心金鑰對由二位以上金鑰管理人員，同時登入 (Log-in) 至硬體密碼模組(HSM)，由硬體密碼模組 (HSM) 直接產生，任何人絕無法單獨一人執行金鑰對的產生作業，且私密金鑰於硬體密碼模組 (HSM) 內產生後，直接經加密保護後儲存在設備內。

用戶金鑰對由用戶驅動產製。

6.1.2 私密金鑰遞送至用戶

憑證管理中心不代替用戶產生金鑰對，故無私密金鑰遞送安控措施的需求。

6.1.3 公開金鑰遞送至憑證簽發者

用戶以公開金鑰經由註冊中心向用戶憑證管理中心申請憑證或直接到用戶憑證管理中心申請憑證時，該請求訊息內的用戶公開金鑰 (Public Key) 除具有用戶簽章的保護外，且具有訊息加密完整性的保護。

憑證申請成功的回覆訊息內，均具有用戶憑證管理中心的簽章與訊息完整性的保護。

6.1.4 憑證機構公開金鑰遞送至信賴憑證者

憑證管理中心公開金鑰有異動或因用戶查詢而須遞送至用戶時，公開金鑰憑證皆有憑證管理中心之簽章與訊息完整性的保護。

6.1.5 金鑰長度

最高層憑證管理中心(RCA)的 RSA 公開金鑰長度至少為 2048 位元，且位元長度必可整除 8；ECC 公開金鑰使用之曲線其安全強度至少為 P-256。

政策憑證管理中心(PCA)的 RSA 公開金鑰長度至少為 2048 位元，且位元長度必可整除 8；ECC 公開金鑰使用之曲線其安全強度至少為 P-256。

用戶憑證管理中心(UCA)的 RSA 公開金鑰長度至少為 2048 位元，且位元長度必可整除 8；ECC 公開金鑰使用之曲線其安全強度至少為 P-256。

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

6.1.6 公開金鑰參數的產生及參數品質檢驗

RSA：憑證管理中心採用 RSA 演算法，質數產生器是採用 ANSI X9.31 演算法產生 RSA 演算法所需的質數，此方法可保證該質數為強質數(Strong Prime)。其中指數(Exponent)應包含以下特性：大於等於 3 的奇數且介於 2^16 + 1 與 2^256 – 1 之間；模數(Modulus)應包含以下特性：奇數、不是質數乘冪且無小於 752 之因數。

ECC：本憑證管理中心使用 ECC 完整公開金鑰驗證程序(ECC Full Public Key Validation Routine)或 ECC 部分公開金鑰驗證程序(ECC Partial Public Key Validation Routine)來確保所有金鑰的有效性。

6.1.7 金鑰使用目的

本公司簽發給用戶作為簽章及加密或其他用途使用的憑證，該憑證使用於安控措施用途上的種類區分，用戶必須依本作業基準與業務應用系統的規範使用，且訂定於 X.509 V3 憑證的標準擴充欄位的金鑰用途欄位 (Key Usage)。用戶必須依憑證的用途使用於相關的業務系統。

除簽章及加密憑證的需求外，用戶如果有其他用途的憑證需求時，用戶憑證管理中心必須簽發該種用途的金鑰憑證予用戶使用。

6.1.8 用戶金鑰產製設備

用戶之金鑰對產製裝置，通常係使用作業系統內建之金鑰產製裝置。

6.2 私密金鑰保護措施及密碼模組工程控管

6.2.1 密碼模組標準

憑證管理中心使用通過 CNS15135、ISO19790 或 FIPS 140 有效版本 Level 3 規範的硬體密碼模組 (HSM)。

6.2.2 私密金鑰分持控管

憑證管理中心私密金鑰的產生、建置及變更，皆由至少二位以上的金鑰管理人員同時進行作業始可辦理，任何人絕不可能單獨進行上述私密金鑰的產生、建置及變更作業。私密金鑰的相關資訊（例如：IC 卡）與保護密碼 (PIN)，分別由職務獨立的不同管理人員管控，並

儲存於具安控措施的環境。

私密金鑰的備份與保存作業，如果是以部分基碼的方式儲存，則是由不同金鑰管理人員個別獨立備份儲存於具安控措施的媒體；如果是以明碼的方式備份與保存，則是由金鑰管理人員將私密金鑰經由硬體密碼模組 (HSM) 之主基碼進行加密後，備份保存於具安控措施的媒體，且須留存稽核紀錄。

6.2.3 私密金鑰託管、回復及保存

不適用。

6.2.4 私密金鑰的備份

憑證管理中心私密金鑰儲存於加密後的硬體密碼模組 (HSM) 內，備份時至少由二位以上授權人員，將加密後的私密金鑰備份儲存於媒體，或是私密金鑰的部分基碼 (m-out-of-n key parts) 儲存於 IC 卡，並存放於經雙重控管、安全的金庫環境內，其中一份備份媒體存放於具安全控管的異地備援環境。

6.2.5 私密金鑰歸檔

憑證管理中心的私密金鑰經加密後，或以部分基碼 (Key Component) 方式儲存於具安控措施的保護 IC 卡內，或經加密後儲存於介面媒體，並存放於經雙重控管、安全的金庫環境內。私密金鑰的有效期限結束後的保存作業，與使用中的私密金鑰安控措施相同，相關的私密金鑰保存作業與 5.5 節的保存作業相同。

6.2.6 私密金鑰自密碼模組輸入或輸出

憑證管理中心私密金鑰的建置，至少由二位以上的金鑰管理人員透過硬體密碼模組 (HSM) 直接產生與建置或變更，任何一人絕無法單獨進行建置或變更作業，且私密金鑰經加密保護後儲存在設備內。

當有使用該私密金鑰執行運算的需求時，須經由硬體密碼模組 (HSM) 的功能介面直接在設備內執行運算，完成後將執行結果輸出，私密金鑰無法以明碼方式輸出至硬體密碼模組 (HSM) 外。

6.2.7 私密金鑰儲存於密碼模組

本憑證管理中心之私密金鑰係以加密型態儲存於密碼模組。

6.2.8 私密金鑰啟動方式

憑證管理中心儲存於硬體密碼模組 (HSM) 內的私密金鑰，必須由授權的二位以上的金

鑰管理人員開啟（例如：身分 (IC 卡) 與指紋或密碼驗證通過）方可使用，且未經授權者絕不可以開啟或存取使用。

用戶私密金鑰的開啟，至少必須具有通行密碼 (Passwords) 或密語 (Pass-phases) 的保護，且只有用戶擁有，他人絕無法知悉。

6.2.9 私密金鑰停用方式

儲存於硬體密碼模組 (HSM) 內的私密金鑰由二位以上授權金鑰管理人員簽入 (Log-in) 系統（例如：身分 (IC 卡) 與密碼驗證通過）方可執行關閉，且未經授權者絕不可以任意存取使用。

硬體密碼模組 (HSM) 或私密金鑰關閉不使用時，皆須要儲存於具備安全控管的環境下，未經授權者絕不可以任意存取。

6.2.10 私密金鑰銷毀

憑證管理中心在私密金鑰效期屆滿後或相對應的公開金鑰失效、廢止時，其軟體亂碼化模組必須以資料覆蓋方式 (Overwrite) 清除私密金鑰；硬體密碼模組 (HSM) 或 IC 卡必須以零值化 (Zeroization) 的覆蓋方式清除私密金鑰。

硬體密碼模組 (HSM) 於廢棄不使用時，亦以上述方式清除全部私密金鑰。

6.2.11 密碼模組等級

憑證管理中心使用之硬體密碼模組等級，必須為 CNS15135、ISO19790 或 FIPS 140 有效版本等級 Level 3（含）以上。

6.3 金鑰對管理的其他事項

6.3.1 公開金鑰歸檔

公開金鑰的保存，其執行程序及安全措施的需求與憑證的保存相同，期限至少保留十年，若主管機關規範的保存期限較長時，則以主管機關的管理規範為準據。

6.3.2 公開金鑰與私密金鑰的有效期限

除憑證中心與註冊中心的業務規範需求外，用戶公開金鑰與私密金鑰的有效期限目前訂定為相同的效期。

用戶公開金鑰與私密金鑰的有效期限最長為三年。

6.4 啟動資料

6.4.1 啟動資料產製及安裝

憑證管理中心私密金鑰的啟動資料由多張智慧卡共同產生，並使用多人控管的權限分離 (Duty Separation) 機制；智慧卡中的啟動資料由讀卡機存取，並以智慧卡的個人識別碼（以下簡稱 PIN 碼）做為啟動資料存取身分驗證之用。

用戶私密金鑰啟動資訊（例如：IC 卡密碼 (Personal Identification Number; PIN)、通行密語 (Pass-phrase)）於安全控管的環境下，直接於硬體密碼模組 (HSM) 設備內產生，且是隨機產生的一組亂數（密碼建議至少六位文數字符號以上，通行密語建議至少八位文數字符號以上）。當有經由網路傳遞至用戶的需求時，具有適當的安全措施保護，如果以郵件方式傳遞時，必須是以密封的密碼單方式遞送，於建置使用時可依用戶安全需求而隨時變更。

6.4.2 啟動資料的保護

憑證管理中心啟動資料由一組智慧卡保護，智慧卡的 PIN 碼由保管人員負責保存，不得記錄於任何媒體上，如登入的失敗次數連續 3 次，則鎖住此智慧卡；智慧卡移交時，新的保管人員必須重新設定新的 PIN 碼。

用戶的啟動資訊必須妥善保管或記憶後銷毀，不可為其他人所知悉，如有書面文件保留的需求時，必須儲存於嚴密且有安全保護措施的環境下，不可洩露予他人，配合業務系統安全的需求得隨時變更啟動資訊。

6.4.3 啟動資料的其他考量

考量安全因素，對於申請憑證的用戶啟動資訊的生命週期之變更頻率訂定如下：

(1) 低保護性：啟動資訊長度 4-6 位的數字，儲存於系統的啟動資訊為明碼，可由用戶選取，以信封郵寄時無特殊安控措施。使用於非機密或普通資料的傳遞，或低交易金額時的啟動資訊。建議生命週期為一年，一年後必須執行啟動資訊的變更。
(2) 中保護性：啟動資訊長度 4-8 位的文數字，儲存於系統的啟動資訊為亂碼化，以信封郵寄時需特殊安控措施，可由用戶選取或系統產生。使用於一般重要資料的傳遞，或一般交易金額時的啟動資訊。建議生命週期為六個月，六個月後必須執行啟動資訊的變更。
(3) 高保護性：啟動資訊長度 6-8 位的文數字，儲存於系統的啟動資訊為亂碼化，以信封郵寄時需特殊安控措施，在安全的管控環境下由亂碼化設備內亂數產生系統直接產生。使用於較重要資料的傳遞，或一定交易金額以上時的啟動資訊。建議生命週期為一個月，一個月後必須執行啟動資訊的變更。

本公司產生給予用戶保護私密金鑰或 IC 卡的啟動資訊，為考量安全因素，建議用戶依

業務系統安全度的需求而隨時變更啟動資訊。

用戶於向本公司申請憑證時，使用的啟動資訊之生命週期規範，訂定於憑證相關作業規範。

註冊中心所產生提供用戶使用的啟動資訊（例如：IC 卡密碼、磁片密碼），用戶應依業務安全度的需求，考量變更啟動資訊頻率（例如：用戶連上註冊中心網際網路的啟動資訊至少三個月或六個月變更一次）。

6.5 電腦安全控管

6.5.1 電腦安全技術需求

憑證系統和相關輔助系統透過作業系統，或結合作業系統、軟體和實體的保護措施提供以下安全控管功能：

(1)具備身分鑑別的登入。

(2)提供自行定義存取控制。

(3)提供安全稽核能力。

(4)對於各種憑證服務和信賴角色存取控制的限制。

(5)具備信賴角色及身分的識別和鑑別。

(6)確保通訊和資料庫之安全。

(7)具備信賴角色和相關身分識別的安全及可信賴的管道。

(8)具備程序完整性及安全控管保護。

6.5.2 電腦系統安全等級

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

6.6 生命週期技術控管

6.6.1 系統開發控管

憑證管理中心的系統開發遵循 ISO 27001 的規範。

憑證管理中心之硬體和軟體是專用的，僅能使用符合安全政策的元件，不安裝與運作無關的硬體裝置、網路連接或元件軟體。

6.6.2 安全管理控管

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

憑證管理中心的軟體在安裝或更新時，將確認是由開發人員提供正確的版本且未被修改。系統安裝後，每次啟動時檢驗軟體的完整性。

6.6.3 生命週期安全控管

憑證管理中心每年定期審視現行演算法或金鑰是否有遭破解之風險。

6.7 網路安全控管

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

憑證系統須經授權後由業務相關之作業人員才可以執行管理作業，透過網路存取憑證系統須進行身分鑑別後方可與許存取。為防範網路入侵與破壞，安裝及建置有防火牆、入侵防禦與防毒系統等，以增進網路安全。

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

憑證系統的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、防火牆系統等加以保護，以防範阻絕服務及入侵等攻擊。

6.8 時戳

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

(1) 憑證簽發時間。

(2) 憑證廢止時間。

(3) CRL 簽發時間。

7.憑證、憑證廢止清冊及線上憑證狀態查詢剖繪

7.1 憑證剖繪

憑證管理中心各憑證系統使用的憑證詳細內容，訂定於各憑證相關的憑證格式剖繪作業規範。

7.1.1 版本

憑證管理中心各憑證系統目前簽發 X.509 V3 格式的憑證，此版本之值存放於憑證版本格式欄位之內。

7.1.2 憑證擴充欄位

憑證管理中心各憑證系統除使用基本欄位，與標準擴充欄位外，亦有使用 X.509 V3 私有擴充欄位之憑證系統，其憑證各欄位詳細內容參考各憑證相關的憑證格式剖繪文件。

7.1.3 演算法物件識別碼

憑證管理中心依 ISO 物件識別碼 (OID) 管理單位公告的規範，各憑證系統使用的演算法物件識別碼，如下：

演算法類型	演算法 (Algorithm)	物件識別碼 (OID)
金鑰	rsaEncryption	{iso(1)member-body(2)us{840}rsadsi(113549)pkcs(1)pkcs-1(1)1}
金鑰	ecPublicKey	{iso(1)member-body(2)us(840)ansi-X9-62(10045)keyType(2)ecPublicKey(1)}
簽章	sha256WithRSAEncryption	{iso(1)member-body(2)us{840}rsadsi(113549)pkcs(1)pkcs-1(1)11}
簽章	ECDSAWithSHA256	{iso(1)member-body(2)us(840)ansi-X9-62(10045)signatures(4)ecdsa-with-SHA2(3)2}
簽章	ECDSAWithSHA384	{iso(1)member-body(2)us(840)ansi-X9-62(10045)signatures(4)ecdsa-with-SHA2(3)3}

7.1.4 識別名稱格式

憑證系統所簽發用戶憑證，使用的識別名稱格式內容皆符合 X.500 Distinguished Name (DN) 的命名方式。

7.1.5 識別名稱限制

憑證管理中心簽發之憑證，可視需要使用「名稱限制」(nameConstraints) 擴充欄位。

7.1.6 憑證政策物件識別代碼

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

憑證系統依 X.509 V3 規範所簽發的用戶憑證，其憑證政策相關的物件識別碼 (OID)，存放於憑證內憑證政策相關的識別欄位，其物件識別碼之識別值訂定於憑證相關的憑證政策與憑證格式剖繪作業規範。

7.1.7 憑證政策限制擴充欄位的使用

憑證管理中心所簽發之憑證可視需要包含「政策限制 (policyConstraints)」擴充欄位。

7.1.8 憑證政策限定元語法與語意

憑證有使用憑證政策限制擴充欄位時，其語法與語意訂定於憑證相關的憑證格式剖繪作業規範；IXML Plus 憑證的憑證政策擴充欄位存放憑證政策 (CP) 的簡要聲明，憑證使用時的適用範圍限制的代碼，其限制語法與語意為：第一段為身分識別安全等級，第二段為用途別，第三段為用戶身分，第四段為適用業務範圍，詳述於 1.4 節。

7.1.9 憑證政策擴充欄位語意必要的處理

憑證有使用憑證政策限制擴充欄位時，其必要處理的作業規範訂定於業務系統相關的作業規範；IXML Plus 憑證的憑證政策擴充欄位存放憑證政策 (CP) 的簡要聲明，憑證使用時的適用範圍限制的代碼，於業務應用系統使用憑證時必須檢核與處理。

7.2 憑證廢止清冊剖繪

7.2.1 版本

各憑證系統目前簽發 X.509 V2 格式的憑證廢止清冊，此版本之值存放於廢止憑證版本格式欄位之內。

7.2.2 憑證廢止清冊與憑證廢止清冊擴充欄位

各憑證系統，於廢止憑證作業有使用憑證廢止清冊擴充欄位時，各欄位詳細內容參考憑證廢止清冊格式剖繪文件。

7.3 線上憑證狀態查詢剖繪

7.3.1 版本

無規定。

7.3.2 線上憑證狀態查詢擴充欄位

無規定。

8. 稽核及其他評估方法

8.1 稽核頻率或評估事項

本公司憑證系統業務營運安全控管的稽核作業，以本公司訂定的內部自行查核規範（參考 WebTrust Principles and Criteria for Certification Authorities 的查核標準與參考 ISO 27001 的規範標準），每年至少定期執行一次內部查核作業。

8.2 稽核人員之識別及資格

執行稽核作業的稽核人員，至少必須具備憑證機構、資訊系統安全稽核的知識，有二年以上的稽核相關經驗，且必須熟悉本作業基準的運作規範，以及具有應用系統的業務及電腦硬軟體系統的相關知識與系統規劃、設計開發的相關經驗；國家相關管理單位有規範稽核人員的適任條件時，以該規範為準據，或具有國家稽核人員正式資格者、或具有國際上認可之稽核資歷並具有稽核的相關實務經驗者。

8.3 稽核者與受稽核者之關係

執行稽核作業的內部稽核人員或委外稽核人員與被稽核單位的業務權責為獨立分工，無任何業務、財務往來，或其他任何利害關係足以影響稽核的客觀性，並以獨立、公正、客觀的態度執行查核評估作業。

當適任的稽核人力不足時，可以委由專業、公正且客觀的專責稽核機構，代為執行稽核相關作業。

8.4 稽核項目

稽核人員主要稽核項目如下：

(1) 業務執行的公告：是否依本作業基準及相關作業規範執行憑證管理作業。
(2) 服務的完整性：憑證管理中心之私密金鑰與相關憑證之生命週期（產生、建置、使用、註銷保存與銷毀）的安全管理，憑證與廢止憑證及過期憑證之生命週期作業的安全管理，介面媒體（例如：IC 卡）生命週期的安全管理。
(3) 憑證管理中心環境的安全控管：符合資訊安全政策、憑證政策與憑證實務作業基準的資訊安全管理，資產的風險評估與安全控管，作業人員的安全控管，實體環境安全設施的安全控管，硬軟體設備、媒體的安全控管，系統或網路存取的安全控管，系統開發與維護的安

全控管，系統災變異地備援管理，符合相關法令規範與國際標準的管理，稽核事件與紀錄的安全管理。

主管機關另有訂定稽核的查核規範標準時，亦須符合且通過主管機關的查核驗證；當有配合跨國或跨區域的憑證系統整合時，亦須符合且通過跨國或跨區域的查核規範標準。

8.5 稽核結果之因應

本公司的運作經詳細查核評估後，有不符合憑證實務作業基準及運作安全有關的規範時，稽核人員應依問題檢查缺失嚴重性的等級詳細條列，並將結果通知稽核單位與受檢單位。

受檢單位必須依檢查缺失，提矯正與預防措施及其規劃說明書；稽核單位的相關稽核人員負責審查矯正措施與預防措施的合理性與適用性，並追蹤稽核後的改善情形。

8.6 稽核結果之公開

憑證管理中心將於儲存庫公布最近一次的外部稽核報告。

9. 其他業務及法律規定

9.1 收費

9.1.1 憑證簽發及更新費用

用戶憑證管理中心與註冊中心或與用戶之間的註冊、憑證申請、更新等計費架構及收費的費率，訂定於相關業務之計費作業規範或合約之條款中。

9.1.2 憑證查詢費用

用戶憑證管理中心與註冊中心或與用戶之間，憑證查詢收費等計費架構及收費的費率，訂定於相關業務之計費作業規範或合約之條款中。

9.1.3 憑證廢止及狀態查詢費用

用戶憑證管理中心提供用戶憑證廢止功能之收費架構及收費的費率，訂定於相關業務之計費作業規範或合約之條款中。

9.1.4 其他服務費用

用戶經由網際網路至網站下載憑證實務作業基準 (CPS) 或相關業務的憑證政策 (CP)，不計收任何服務費用，但如向本公司索取紙本文件的 CPS、CP 或其他相關作業文件時，本公司須向用戶收取郵寄及處理的工本費，收費的費率訂定於相關業務之計費作業規範或合約之條款中。

9.1.5 退費

本公司所簽發之所有憑證，在完成憑證簽發後七日內，用戶向本公司或註冊中心申請退費並廢止憑證時，扣除壹佰元的處理工本費後，餘無息退還予用戶；於完成憑證簽發七日後，用戶始申請退費時，恕不接受退費。

9.2 財務責任

9.2.1 保險範圍

於憑證管理作業有關的風險管理，除已投保建築物與硬體設施的地震及火險外，為保障用戶的權益與分散業務的營運風險，已投保 200 萬美元之一般責任險和 500 萬美元之專業責任險。

9.2.2 其他資產

本公司執行憑證業務有關財務運作的稽核作業，每年定期委由公正、客觀的第三機構執行財務運作的查核。

9.2.3 對用戶及信賴憑證者之賠償責任

9.2.3.1 本公司之憑證賠償責任

- 本公司所提供的~~認證~~驗證服務作業項目與內容，皆訂定於本作業基準「1.4.1.2 使用範圍」，非本作業基準所訂定的內容，例如用戶與信賴憑證者使用的交易系統，皆排除於賠償責任之外。
- 本公司處理用戶註冊資料及憑證簽發作業，除未遵照本作業基準、憑證政策及相關作業規範的規定辦理而造成用戶的損失，且可歸責於本公司之故意或過失外，本公司不負損害賠償責任。
- 如因網際網路傳輸的中斷或故障，或其他不可抗力的天災事故（例如戰爭或地震等），非為本公司的故意或過失致所簽發之憑證造成用戶損失時，本公司不負損害賠償責任。
- 本公司如因作業人員之過失，使其未遵照本作業基準、憑證政策及相關作業規範的規定辦理註冊、憑證的簽發與廢止作業，或違反相關法律規範而造成用戶的損害時，本公司應依本作業基準之規定賠償用戶之損害。有關用戶單一憑證之最高賠償金額訂定於 9.9 節；但上述損害事由係因本公司作業人員故意或重大過失所造成者，本公司賠償該用戶之實際所受損害。
- 用戶或其他有權者提出廢止或暫禁用戶的憑證要求後，至用戶憑證管理中心實際公布廢止或暫禁該用戶憑證（憑證廢止清冊）為止之期間內，如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，用戶憑證管理中心如依據本作業基準與相關的作業規範執行處理作業，則不負損害賠償責任。
- 用戶使用非法假造、錯誤的憑證而造成損害時，當不可歸責於本公司時，本公司不負損害賠償責任。
- 用戶的賠償追究有效期限，依業務主管機關與相關法令的規範辦理。

9.2.3.2 註冊中心賠償責任

- 註冊中心與其作業人員必須善盡保管用戶的註冊及相關資料之責任，避免相關資訊洩漏、被冒用、篡改及任意使用。註冊中心作業人員因處理用戶註冊及相關訊息，或向用戶憑證管理中心申請用戶憑證發生錯誤而造成用戶或他人損害時，應由該註冊中心與其作業人員負損害賠償責任。
- 註冊中心如因作業人員故意或過失，未遵照本作業基準及註冊中心相關作業規範的規定辦理註冊、憑證的簽發、更新、暫停使用與廢止作業，或違反相關法律規範而造成用戶的損害時，註冊中心應依規定賠償用戶的直接損害。
- 用戶使用非法假造、錯誤的憑證而造成損害時，當不可歸責於註冊中心時，註冊中心不負

損害賠償責任。

- 用戶或其他有權者提出廢止或暫禁用戶的憑證要求後，至用戶憑證管理中心實際公布廢止或暫禁該用戶憑證（憑證廢止清冊）為止之期間內，如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，註冊中心如依據本作業基準與相關的作業規範執行處理作業，則不負損害賠償責任。
- 任何因使用憑證而造成用戶的病痛、精神與情緒的困擾，非屬註冊中心損害賠償責任範圍。

9.2.3.3 用戶賠償責任

- 用戶向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，致造成他人遭受損害時，應由該用戶負損害賠償責任。
- 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，致造成註冊中心、本公司或第三者遭受損害時，應由該用戶負損害賠償責任。
- 用戶或其他有權者提出廢止或暫禁用戶的憑證要求後，至用戶憑證管理中心實際公布廢止或暫禁該用戶憑證（憑證廢止清冊）為止之期間內，用戶必須即刻依據業務系統的規範，廢止憑證的使用，並即刻通知相關信賴憑證者停止該憑證的使用。於提出廢止或暫禁用戶憑證之期間內，如用戶未依據業務系統的規範廢止該憑證的使用，及即刻通知相關信賴憑證者停止該憑證的使用，則用戶必須負損害賠償責任。
- 用戶申請使用憑證若有違反本作業基準及相關作業的規範，或憑證使用於非本作業基準規定的其他業務範圍，或主管機關明訂禁止的業務範圍，或違反相關法令規範時，用戶應負損害賠償責任。

9.2.3.4 信賴憑證者賠償責任

- 信賴憑證者若將用戶憑證用於非法交易而產生法律糾紛時，則信賴憑證者必須負損害賠償責任。
- 信賴憑證者若未依 4.5.2 節之要求進行憑證驗證，進而產生法律糾紛或財產損失時，則信賴憑證者必須負損害賠償責任。

信賴憑證者若因未符合憑證實務作業基準與相關的作業規範，進而產生法律糾紛或財產損失時，則信賴憑證者必須負損害賠償責任。

9.3 機密資訊

9.3.1 機密資訊的種類

機密資訊包括：

(1) 用於憑證管理中心營運的私密金鑰及通行密碼。

(2) 控管憑證管理中心私密金鑰之分持資料。

(3) 用戶申請憑證時，擔任憑證申請者代表人及代理人之個人資料。

(4) 憑證管理中心產生或保管之可供稽核及追蹤之紀錄。

(5) 稽核人員於稽核過程中產生之稽核紀錄及文件。

(6) 列為機密等級的營運相關文件。

9.3.2 非機密資訊種類

憑證政策、本作業基準、本憑證管理中心簽發之憑證、本憑證管理中心簽發之憑證廢止清冊、外部稽核結果等皆為可公開之資訊。

9.3.3 保護機密資訊之責任

除非符合下列條件之一，否則用戶之註冊基本資料與身分驗證相關資料絕不任意提供予權責管理單位，或其他任何人知悉：

(1) 政府法令之規定並經由權責管理單位依法定程序授權。

(2) 具有合法司法管轄權之訴訟或仲裁機構處理因憑證產生之糾紛或仲裁，而依法定程序申請之需求。

9.4 個人資訊隱私

9.4.1 隱私保護計畫

本公司對於用戶資訊的保護，皆依「個人資料保護法」及其他政府單位相關的規範運作，且符合 OECD 個人資料隱私的保護規範 (OECD; Organization for Economic Co-operation and Dvelopment, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data)。

憑證管理中心或註冊中心為憑證管理作業的需求而使用與存取用戶資訊時，必須合於業務的需求與具體嚴謹的安全控管，由業務有權存取的作業人員執行。

憑證管理中心或註冊中心管理與使用用戶資訊時，用戶的註冊基本資料與身分識別資料，非經用戶之允許絕不任意對外公開、銷售、租借。

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

9.4.2 個人隱私資訊種類

(1) 用戶的註冊基本資料與身分識別資料。

(2) 於註冊或憑證申請相關作業所使用的身分識別的用戶資訊。

(3) 用戶註冊或憑證申請、更新、暫禁與廢止時，交易的相關隱私訊息。

(4) 用戶註冊時填寫於註冊相關申請單與合約上的用戶資訊，與身分證明文件（或影印本）上的隱私資訊。

9.4.3 非個人隱私資訊種類

公告於儲存庫的用戶憑證資訊，憑證狀態（提供憑證有效性狀態查詢功能時），及用戶憑證管理中心的憑證資訊、憑證廢止清冊、憑證政策、憑證實務作業基準，為可公開的非機密性資訊。

9.4.4 個人隱私資訊保護責任

依相關法令規定辦理。

9.4.5 使用個人隱私資訊之告知與同意

依相關法令規定辦理。

9.4.6 因行政法令或司法要求之揭露

如 9.3.3 節之規定。

9.4.7 其他資訊公開情形

如 9.3.3 節之規定。

9.5 智慧財產權

本公司於憑證系統所使用的硬、軟體系統與相關設備及相關作業手冊，其智慧財產權如為各提供廠商所有，保證皆為合法且擁有使用權，絕無侵害第三者的權利；如為本公司自行開發

的系統與相關作業手冊，則其所有權為本公司所擁有。

本作業基準、憑證政策、與其他執行憑證管理作業，而為本公司開發撰寫的相關文件之智慧財產權皆為本公司所有。

用戶產生的私密金鑰與公開金鑰為用戶所擁有，但公開金鑰經用戶憑證管理中心簽發成憑證格式，儲存於目錄伺服器或資料庫時，該憑證為本公司的智慧財產權，只提供用戶與信賴憑證者公開金鑰憑證的使用權限。

本公司產生的 CA 憑證，CA 與用戶的憑證狀態，及憑證廢止清冊訊息皆為本公司的智慧財產權，本公司只提供用戶與信賴憑證者使用的權限。

本公司尊重置於 X.509 V3 憑證內用戶識別名稱欄位所存放的用戶註冊名稱，但不保證用戶註冊名稱的智慧財產權之歸屬。用戶的註冊商標如果於註冊時已為先前的用戶佔用時，註冊商標與註冊名稱智慧財產權相關的糾紛仲裁處理非為本公司的管轄權責，用戶必須向相關的業務主管機關提出申請。

9.6 職責及義務

9.6.1 憑證機構之職責

- 訂定、公告與管理憑證業務範圍內的憑證實務作業基準與憑證政策，及憑證運作的相關作業規範。
- 確認用戶憑證管理中心與註冊中心的權責關係，且註冊中心的實務作業必須依本作業基準、憑證政策及相關的規範運作。
- 確認憑證系統作業人員（含合約委外人員）的選用與系統運作符合憑證實務作業基準的規範。
- 作業人員必須善盡保管用戶註冊與憑證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。
- 依憑證實務作業基準的規範，接受用戶（註冊中心）憑證的申請、更新、暫禁、廢止、查詢及有關註冊申請訊息，確認註冊中心及用戶發送至用戶憑證管理中心之相關交易訊息的正確性與完整性，並執行憑證簽發作業及將相關回覆訊息正確且安全的遞送至用戶。
- 提供目錄伺服器的服務時，依據憑證作業規範將用戶與本公司的憑證及廢止憑證清冊正確且安全的遞送至儲存庫。
- 必須於與用戶的合約或相關作業文件，詳細說明用戶註冊、憑證申請、更新、暫禁、廢止、與使用的作業規範，及相關的權利與義務關係。
- 用戶憑證管理中心的私密簽章金鑰只可用於用戶憑證與廢止憑證的簽發，如有訊息加密或其他簽章的需求時，必須使用不同且獨立的私密金鑰。

9.6.2 註冊機構之職責

- 依本作業基準、憑證政策及註冊中心的作業規範，確認註冊中心與用戶的權責關係，執行用戶註冊身分識別及憑證申請、更新、暫禁、與廢止相關作業時，申請訊息合法性與完整性的驗證。
- 確認註冊中心憑證系統作業人員（含合約委外人員）的選用與系統運作符合憑證實務作業基準、與註冊中心的作業規範。
- 註冊中心必須確認用戶於註冊申請時，確實瞭解且同意申請書與合約書上的權利與義務，及業務相關作業規範的內容。
- 接受用戶註冊、註銷、憑證申請、更新、暫禁、查詢與憑證廢止申請之作業。
- 用戶申請註冊或註銷時必須驗證用戶身分的合法性與正確性，於用戶申請憑證時，驗證用戶身分的合法性與正確性，完成後通知用戶憑證管理中心簽發憑證予用戶，並將用戶憑證管理中心傳回的正確回復訊息安全的遞送予用戶。
- 註冊中心與其作業人員必須善盡保管用戶註冊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。
- 註冊中心與用戶的合約或相關作業文件，詳細說明用戶註冊、憑證申請、更新、暫禁、廢止、查詢與使用的作業規範，及相關的權利與義務關係。
- 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，即刻向簽發該憑證之用戶憑證管理中心辦理申告與處理。
- 註冊中心負責用戶註冊管理作業相關的權責義務，用戶憑證管理中心負責由註冊中心委託的憑證簽發管理作業相關的權責義務，註冊中心必須提供上述權責義務關係之資訊予用戶及信賴憑證者。

9.6.3 用戶之義務

- 用戶向註冊中心申請註冊時，必須提供詳細且正確的身分證明文件與資料。
- 用戶向註冊中心申請註冊時，必須確實瞭解並同意申請書與合約書上的權利與義務，及憑證申請、更新、暫禁、廢止、註冊與使用的作業規範內容，並且於接受該規範的規定下始可簽名確認。
- 用戶必須依本作業基準規範的規定，確實且妥善安全的產製與保護其私密金鑰及私密金鑰保護密碼，除本人或受託管者外絕無其他任何人知悉與使用。
- 用戶於接受本公司所簽發的用戶憑證時，必須驗證用戶及用戶憑證管理中心身分的合法性，及憑證訊息的完整性與有效性。
- 用戶必須瞭解且同意憑證實務作業基準相關作業規範的規定，合法且正確的使用私密金鑰與憑證於相關的業務系統，無任何違反相關法律的規定與侵害第三者的權利。
- 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，或憑證內用戶相關的資訊有異動時，或擬不使用該憑證時，用戶必須依相關作業的規定，即刻向註冊中心辦理申告與處理。

9.6.4 信賴憑證者之義務

- 信賴憑證者必須瞭解且同意憑證實務作業基準，與使用之業務系統相關作業規範的權利與義務規定，且依憑證內容所規定的業務範圍及本作業基準的規範使用於相關的業務系統使用憑證，無任何違反相關法律的規定與侵害第三者的權利。
- 憑證的使用，必須依憑證實務作業基準、應用業務系統作業規範的規定、X.509 憑證標準的規範，由憑證鏈逐一驗證該憑證的正確性及有效性，當有憑證廢止清冊的安全機制時，尚須檢核此憑證是否為廢止或暫禁憑證。
- 驗證交易訊息的有效性時，除驗證用戶憑證的有效性與合法性外，必須依憑證實務作業基準與業務系統相關規範的規定，驗證交易限額、賠償限額、使用業務範圍、及法律的權責關係。

9.6.5 儲存庫之義務

- 依本作業基準及儲存庫的作業規範，確認儲存庫與用戶及本公司的權責關係，執行用戶憑證相關資訊查詢作業與安控措施的運作。
- 用戶憑證管理中心及時遞送的用戶憑證與憑證廢止清冊，必須能立刻更新資料庫，提供與通知用戶查詢最新的資訊，除系統維護的需求外，每天 24 小時提供正常服務。
- 至目錄伺服器或資料庫查詢資訊時，驗證用戶身分的合法性與查詢訊息的有效性，並將正確的訊息安全且有效的傳回至查詢之用戶；除憑證與憑證廢止清冊的資訊開放使用者查詢外，其他儲存庫資訊非儲存庫合法與經過授權的用戶絕無法查詢。
- 儲存庫與其作業人員必須善盡保管用戶註冊憑證及相關訊息之責任，避免相關資訊洩漏、被冒用、篡改及任意使用。
- 儲存庫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，或憑證內儲存庫相關的資訊有異動時，必須依相關作業的規定，即刻向簽發該憑證之用戶憑證管理中心辦理申告與處理。

9.7 除外責任

(1) 本公司處理用戶註冊資料及憑證簽發作業，除未遵照本作業基準之規定辦理，或違反相關法律規章之規定，或可歸責於本公司之過失外，本公司不負損害賠償責任。

(2) 本公司如因網際網路傳輸之中斷或設備之故障或其他不可抗力之天災事故（例如戰爭或地震等），或其他不可歸責於本公司之事由，造成用戶及信賴憑證者損失時，本公司不負損害賠償責任。

(3) 本公司未善盡保管用戶之註冊及憑證相關機密資料，而造成相關資訊洩漏、被冒用、篡改及任意使用致造成第三者遭受損害時，本公司應負損害賠償責任。

(4) 本公司在收到憑證廢止申請後，應於 1 個工作天內完成憑證廢止作業，並於憑證廢止作業完成後 1 天內簽發憑證廢止清冊及公告於儲存庫。用戶於憑證廢止狀態未被公布之前，應採取適當之行動，以減少對信賴憑證者之影響，並承擔所有因使用該憑證所引發之責任。

9.8 責任限制

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

9.9 賠償

本公司如因作業人員之過失，使其未遵照本作業基準、憑證政策及相關作業規範的規定辦理用戶註冊、憑證的簽發、暫禁與廢止作業，或違反相關法律規範而造成用戶的損害時，本公司應依本作業基準之規定賠償用戶之損害；但上述損害事由係因本公司作業人員故意或重大過失所造成者，本公司賠償該用戶之實際所受損害。

如因網際網路傳輸的中斷或故障，或其他不可抗力的天災事故（例如戰爭或地震等），非為本公司的故意或過失致所簽發之憑證造成用戶損害時，本公司不負損害賠償責任。

本公司憑證用戶或其他有權者提出廢止憑證要求後，至本公司實際完成廢止該用戶憑證之期間內，當該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，本公司如依據本作業基準與相關之作業規範執行處理作業，則不負任何損害賠償責任。

各類憑證之交易限額、賠償限額及使用範圍說明如下：

(1) 交易限額：依保證等級、用途別、用戶身分及適用業務範圍等分別訂定不同之交易限額；用戶進行交易時，其交易金額不可超出該使用範圍代碼所對應之交易限額。
(2) 賠償限額：依保證等級、用途別、用戶身分等分別訂定不同之賠償限額；該賠償限額係指對用戶單一憑證之賠償上限，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。
(3) 若用戶與本公司訂有合約，另行載明憑證使用範圍、交易限額及賠償限額者，從其約定。
(4) 限定範圍內多用途：用戶憑證的使用範圍，應依本公司簽署之合約或本公司訂定相關的作業管理規範並公告於本公司網站。

憑證使用範圍及其對應之交易限額、賠償限額如下表所示(使用範圍代碼參閱 1.4.1.2 節)：

單位：新台幣元

使用範圍代碼	保證等級	用途別	用戶身分	交易限額	賠償限額
1.1.1.3	第一級	單一用途	法人	3,000	3,000
1.1.2.3	第一級	單一用途	自然人	3,000	3,000
2.1.1.1 2.1.1.2 2.1.1.3	第二級	單一用途	法人	900,000	300,000
2.1.2.1 2.1.2.2 2.1.2.3	第二級	單一用途	自然人	300,000	100,000
2.2.1.1 2.2.1.2 2.2.1.3	第二級	限定範圍內 多用途	法人	900,000	300,000
2.2.2.1 2.2.2.2 2.2.2.3	第二級	限定範圍內 多用途	自然人	300,000	100,000
3.1.1.1 3.1.1.2 3.1.1.3 3.1.1.4	第三級	單一用途	法人	不限定	2,000,000 2,000,000 2,000,000 2,000,000
3.1.2.1 3.1.2.2 3.1.2.3 3.1.2.4	第三級	單一用途	自然人	不限定	300,000 300,000 300,000 300,000
3.2.1.1 3.2.1.2 3.2.1.3 3.2.1.4	第三級	限定範圍內 多用途	法人	不限定	2,000,000 2,000,000 2,000,000 2,000,000
3.2.2.1 3.2.2.2 3.2.2.3 3.2.2.4	第三級	限定範圍內 多用途	自然人	不限定	300,000 300,000 300,000 300,000

註：若憑證內載明之使用範圍代碼不在上述表列中，此憑證即不得使用於任何應用或業務，且本公司對此憑證不負賠償責任。

9.10 本文件生效與終止

9.10.1 生效

本作業基準於主管機關依電子簽章法核定通過後，於本公司儲存庫公布後即生效。

9.10.2 終止

本作業基準新版本經主管機關核定後公布，現有版本即告終止。

9.10.3 終止及存續之效力

本作業基準之效力，維持至遵循本作業基準所簽發之最後一張憑證到期或廢止為止。

9.11 通知與聯絡方式

本公司將以適當的方式，與用戶建立聯絡管道，包括但不限以下方式：電話、傳真或 E-mail。

9.12 變更及公告

9.12.1 變更程序

本作業基準規範的權責管理單位為 TWCA 政策管理中心 (PMA)，並依據及受政府與主管機關訂定的電子簽章法、電子簽章法施行細則、數位簽章憑證實務作業基準應載明事項及憑證機構相關的管理規範管轄，且須通過主管機關的核定。

TWCA 政策管理中心 (PMA)，每年至少一次審查該作業規範，是否符合國際標準的安全規範、主管機關的作業規範、憑證作業管理系統架構與功能的調整、業務系統需求的適用性，或因配合業務需求與符合國際標準規範、錯誤、用戶適當的建議而隨時修改與更新調整。

經由 TWCA 政策管理中心 (PMA) 審查通過的憑證實務作業基準，或更新版本的規範，經收到主管機關審查核定通過後，除另有規定外，本作業基準於本公司網站公告時生效，用戶可至網站（網址：https://www.twca.com.tw）下載。

9.12.2 變更聯絡機制

本作業基準有建議更新時，必須將詳細的相關文件郵寄或 E-mail 至 1.5.2 節載明之聯絡窗口，經 TWCA 政策管理中心的審查。

9.12.3 物件識別碼變更條件

本作業基準引用之憑證政策物件識別碼，於本作業基準內容變更時不會更動，僅增加本作業基準之版本識別代碼。

9.13 爭議處理程序

本作業基準敘述，因公開金鑰憑證或私密金鑰所引起問題之爭議處理程序或糾紛仲裁處理，為一般原則性，與各業務有關的問題，必須另參考業務相關的作業規範。

爭議之雙方應本誠信原則，於合理的方式下雙方盡力協商解決之。

爭議之雙方如無法於十四天內合理的協商解決爭議，則必須共同協商並指派具適任能力的公正第三協調者，以進行協調並解決爭議，且雙方必須同意協調者的協商與裁決。

爭議之雙方如無法於一個月內同意協調者的協商與裁決，與合理的解決該問題爭議時，則將爭議提至臺北地方法院進行糾紛的訴訟處理。

用戶與註冊中心或本公司遇有爭議時，用戶與註冊中心或用戶與本公司間雙方應本誠信原則協商解決之；如涉訴訟時，雙方同意以臺北地方法院為第一審管轄法院。

註冊中心與本公司遇有爭議時，雙方應本誠信原則協商解決之；如涉訴訟時，雙方同意以臺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的費用分擔，依據協商或相關的法律規範處理。

如為跨國或跨區域的爭議處理，無法以上述的處理方式解決時，則必須依相關的跨國或跨區域的糾紛仲裁規範處理。

9.14 政府管理法規

本作業基準依據政府相關法律的規範而訂定，受中華民國相關法律規範的管轄與督導，接受主管機關相關法律規範，例如電子簽章法與相關施行細則、數位簽章憑證實務作業基準應載明事項之管理與監督，如有跨國或跨區域的業務整合需求時，除配合業務整合規範所需之外，仍以中華民國相關法律規範為管轄依據。

9.15 法規之符合性

本作業基準及本憑證管理中心應符合本國電子簽章法及其施行細則之規定。

9.16 各項條款

9.16.1 完整合約

無規定。

9.16.2 轉讓

無規定。

9.16.3 存續性

本作業基準的某些章節規定有不適用而必須修正時，其他條文的規定仍屬有效，不受該項不適用規定影響，直到新版基準的更新完成並公告使用，該項不適用規定的更新悉依本作業基準 1.5 節及 9.12 節的規定辦理。

當用戶與信賴憑證者的關係已過期或因其他因素而中止，本作業基準的規範內，相關的用戶權利與責任仍然有效，不會因此關係的結束而失效（例如：銀行用戶使用憑證於網路銀行轉帳系統，完成後向銀行註銷相關業務關係，則該用戶與銀行的相關權責，因此交易而發生者仍屬有效，不會因此關係的結束而失效）。

依本作業基準與相關業務的規範，用戶憑證管理中心與用戶或註冊中心間資訊通知的往來，可以下列方式傳遞：

(1) 電子訊息 － 訊息經由傳送者將發送訊息簽章後傳送，於接收者收妥訊息並完成訊息的驗章。
(2) 紙本文件 － 文件表單具有傳送者與接收者的詳細相關作業人員名稱與聯絡地址，郵寄至少於三天前（國外航空郵寄至少於一週前）完成投遞；以傳真的方式傳送訊息時，除傳送者與接收者的詳細資訊外，必須具有詳細的傳真機識別號碼，與傳送者業務相關人員的親筆簽名。

9.16.4 施行

無規定。

9.16.5 不可抗力

如因不可抗力或其他不可歸責於本憑證管理中心之事由（例如戰爭或地震等），本憑證管理中心不負損害賠償責任。

9.17 其他條款

無規定。

附錄一 詞彙

(1) 網際網路 (Internet)

許多不同的電腦網路相互連結，經過標準的通訊協定，得以相互交換資訊。

(2)（電子）訊息 ((Electronic) Message)

指文字、聲音、影像、符號或其他資料，以電子、磁性或人之知覺無法直接認識之方式，所製成足以表示其用意之紀錄，而供電子處理之用者。

(3) 電子簽章 (Electronic Signature)

指以電子型式存在之資料訊息，依附在電子文件可用以辨識及確認電子文件簽署人身分及簽署人以數位、聲音、指紋、或其他生物光學技術的特性產生的訊息，其依附在電子訊息上，具有與簽名同等的效力，可用以辨識及確認電子文件簽署人的身分，及辨識簽署訊息的完整性。

(4) 加密 (Encrypt/Encipher)

指利用數學演算法或其他方法，將電子文件以亂碼方式處理，以確保資料傳輸的安全。

(5) 解密 (Decrypt/Decipher)

將經加密後形成人無法辨識其代表意義的訊息，以相關的數學演算法或其他方法將該訊息還原為人可以辨識其代表意義的訊息。

(6) 數位簽章 (Digital Signature)

數位簽章為電子簽章的一種，係指採用非對稱型的密碼演算法 (Asymmetric Cryptosystem) 及雜湊函數 (Hash Function)，對一定長度的數位訊息壓縮後再以簽署人的私密金鑰予以加密，其相對應的公開金鑰可以驗證此加密後的數位訊息，形成一可供辨識簽署人身分及電子文件真偽之資料訊息。

(7) 私密金鑰 (Private Key)

指用以製作及驗證數位簽章具有配對關係之一組數位資料而由簽署人保有者，該數位資料除作為製作數位簽章之用外，尚可用作電子訊息解密之用。

(8) 公開金鑰 (Public Key)

於非對稱型密碼演算法之數位簽章，指用以製作及驗證數位簽章之一組具有配對關係之數位資

料中對外公開者；其可用以執行驗證簽署人簽章過的訊息資料的正確性，於執行訊息隱密性功能時可以將傳遞訊息加密。

(9) <公開金鑰>憑證或電子憑證 (<Public Key>Certification or Certificate)

一筆以電腦為媒介基礎由憑證機構簽發之數位式的紀錄，內含申請者的註冊識別名稱、公開金鑰、該公開金鑰的有效期限、憑證機構的註冊識別名稱與簽章，及其他用以識別的相關訊息，用以確認簽署人之身分，並證明其擁有相配對之公開金鑰及私密金鑰。

(10) 認證中心/憑證機構 (Certification Authority or Certificates Authority; CA)

指提供數位簽章製作及電子認證服務之機構，亦即係指居於公正客觀地位，查驗憑證申請人身分資料之正確性，及其與待驗證公開金鑰及私密金鑰間之關連性與合法性，並據以簽發公開金鑰憑證之單位。

(11) 憑證實務作業基準 (Certification Practice Statement; CPS)

憑證機構向所服務的對象公告其執行憑證簽發、廢止、查詢等管理的作業規範及申請程序，內含憑證運作的公開金鑰架構與安全機制、作業規範與程序、憑證機構軟硬體施行的安全機制、權責的管理及相關的規範。

(12) 非對稱型的密碼演算法（亂碼系統）(Asymmetric Cryptosystem)

以電腦為媒介基礎的一種數學演算法，可以產生及使用一組數學運算上相關連的安全金鑰對。其中私密金鑰用以對訊息作簽章，對應的公開金鑰則用以對簽章後的訊息作驗證；公開金鑰亦可用以對訊息作加密，而對應的私密金鑰則用以對加密後的訊息作解密。

(13) 雜湊函數 (Hash Function)

一種可以將一長串的位元訊息轉換成固定長度位元訊息的數學演算法。相同的訊息輸入經由壓縮函數運算產生輸出結果必定相同，且絕無法由輸出產生的結果推算出輸入的訊息。

(14) 簽發憑證（電子認證）(Issue a Certificate)：

係指認證中心（憑證機構）依憑證實務作業基準，審驗公開金鑰憑證申請人之身分資格、相關文件，並驗證其公開金鑰及私密金鑰之配對關係後，簽發公開金鑰憑證或其他憑證。

(15) 硬體安全模組(Hardware Security Module; HSM)

是一種硬體運算設備，主要用於保護和管理數位金鑰、執行加解密及數位簽章等密碼學作業，一般具備防竄改(tamper resistance)並符合嚴格的安全性需求。

附錄二 名詞與簡稱

AICPA	American Institute of Certified Public Accountants, Inc.
ANS	American National Standard
CA	Certification Authority
CC	Common Criteria
CICA	Canadian Institute of Chartered Accountants
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
FIPS	Federal Information Processing Standard
ISO/IEC	the International Organization for Standardization, The International Electrotechnical Commission
ITSEC	Information Technology Security Evaluation Criteria
OCSP	Online Certificates Status Protocol
OECD	Organization for Economic Co-operation and Development
OID	Object Identifier
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PMA	Policy Management Authority
RA	Registration Authority

RCA Root Certification Authority

RSA Rivest, Shamir, Adleman (encryption algorithm)