臺灣網路認證股份有限公司
憑證實務作業基準
Certification Practice Statement

(第 2.~~34~~ 版)

Version 2.~~34~~

臺灣網路認證股份有限公司
TAIWAN-CA INC.

生效日期：中華民國~~九十九~~XX 年~~七~~XX 月~~二十三~~XX 日

Effective Date：~~2010~~XXXX/~~07~~XX/~~23~~XX

本作業基準版本變更紀錄：

版 本	生效日期	發 行 者	備 註
Version. 1.0	89/03/20	TaiCA	初 版公告
Version. 1.1	91/03/01	TaiCA	配合 TaiCA CA PKI 系統文件(CPS,CP,・・・)的整合，與關貿網路公司 EDI 跨亞洲交易系統(PAA CP) 的整合。
Version 1.2	91/11/04	TaiCA	1.配合主管機關經濟部訂定電子簽章法、電子簽章法施行細則及憑證實務作業基準(CPS)應載明事項之規範而修訂。 2.TaiCA〈1.網際 NB 憑證機構、2.企業 EC 憑證機構、3.商務 EC 憑證機構、4.金融 XML 憑證機構〉憑證機構送審。 3.91/11/04 經濟部核定，經商字第 09102245130 號函。
Ver.1.3	94/02/18	TWCA	1.配合增加電子股務憑證作業、網路保險憑證作業、與憑證多用途作業而修訂。 2.修訂憑證使用的適用範圍與交易限額。 3.原 CPS 之「憑證機構」一詞因過於廣泛，無法明確描述，現依具體狀況以「用戶憑證中心」或「憑證系統」來替代。
Ver.2.0	97/03/04	TWCA	1. 配合企業 EC 憑證停止服務，修訂刪除企業 EC 憑證部份。 2. 將「憑證中心」，修訂為「憑證管理中心」。 3. 為避免「金融 XML 憑證」與銀行公會所屬 XML 憑證混淆，將「金融 XML 憑證」修訂為「商務 XML 憑證」。
Ver.2.1	97/11/12	TWCA	1. 新增『電子通訊投票』適用範圍。 2. 調整識別名稱說明。 3. 加強金鑰長度要求之描述。
Ver 2.2	98/07/14	TWCA	1. 新增『線上申請專利商標』適用範圍。 2. 文句修飾。
Ver 2.3	99/07/23	TWCA	1. 修正 CPS 英文用字。 2. 增加憑證適用範圍。 3. 於商務 XML 憑證系統下，新增 S/MIME UCA。 4. 將 SSL 自 EC+ UCA 分割成立 SSL UCA。 5. 修訂退費機制說明。
Ver 2.4	XX/XX/XX	TWCA	1. 補充說明 SSL 伺服器憑證申請流程。 2. 補充說明商務 XML 憑證申請流程。

目 錄

臺灣網路認證股份有限公司　憑證實務作業基準

(Certification Practice Statement；CPS)

1.使用憑證的重要聲明(Important Statements of Using Certificates)

1.1 主管機關核定(Approved by Ministry of Economic Affairs)

臺灣網路認證股份有限公司〈以下簡稱本公司或 TWCA〉憑證實務作業基準〈以下簡稱本作業基準或 CPS〉，係規範所屬 1.網際 NB 憑證〈以下簡稱 NBCA〉、2.商務 EC 憑證〈以下簡稱 EC+〉、3.商務 XML 憑證等憑證之作業管理規範，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)。

本作業基準係依據主管機關經濟部頒布的「憑證實務作業基準應載明事項準則」規範編撰，經審查核定的文號如下：

~~99XX~~/~~07XX~~/~~23XX~~ 經濟部函 經商字第 ~~09902081770~~XXXXXXXXXXX 號。

1.2 憑證的保證等級及適用範圍(Certificates Level of Assurance and Applicability)

憑證種類：

	憑 證 種 類	保 證 等 級	適 用 業 務 範 圍	備　註
1	網際 NB 憑證	第三級 第二級	網路銀行轉帳、網路下單交易、網路電子資訊安控、網路報稅、電子發票、電子通訊投票。 電子商務應用。	
2	商務 EC 憑證	第三級 第二級	網路下單交易、金融交易、電子商務應用、網路報稅、電子發票、電子通訊投票。 SSL 伺服器憑證、資訊安控。	
3	商務 XML 憑證	第三級 第二級 第一級	金融交易、有價證券交易、電子商務應用、線上身分確認、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。 電子商務應用、線上身分確認、電子郵件應用。 電子商務應用、線上身分確認。	
註：保證等級詳述於「2.2 憑證的適用性」 憑證適用範圍及賠償責任詳述於「2.2.1.2 之 表〈一〉」				

1.3 使用憑證的重要聲明(Important Statements of Using Certificates)

本公司已於 96 年 9 月取得 ISO27001:2005 證書，並持續運作。另自行委託律師事務所或會計師事務所進行外部稽核，以確保遵照憑證實務作業基準與憑證政策之規定運作。

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，確實了

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簽名確認；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。

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，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。

用戶必須依照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；否則因而所致之損害，由用戶承擔之。

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、暫時停用與廢止作業，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「2.2.1.2 憑證適用範圍與償責」；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非為本公司的故意或過失，或其他不可抗拒的天災事故〈例如戰爭或地震等〉，致所簽發之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時，則不負任何損害賠償責任。

2.簡介(Introduction)

2.1 概述(Overview)

政府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，特推動建置憑證機構，提供身分認證及交易認證的服務，以建立使用者的信心，確保參與交易雙方的權益。

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、財金資訊股份有限公司、關貿網路股份有限公司、臺灣證券集中保管股份有限公司、網際威信股份有限公司及多家優良的資訊公司共同集資設立，為一值得信賴的憑證機構。

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，使用公開金鑰亂碼機制(public- key cryptography)，其安控機制的安全標準符合金融監督管理委員會「金融機構辦理電子銀行業務安全控管作業基準」，具備網路交易訊息的不可否認(non-repudiation)、用戶身分的鑑別(authentication)、訊息完整的驗證(verification)、訊息加密的保護(encryption) 及其他機制的安全控管(security control)，可用於網際網路電子銀行、網路下單交易，亦可用於網路報稅、保險、票債券、企業詢價報價、採購與付款交易等網際網路電子商務的應用交易系統。

2.2 憑證的適用範圍(Certificate's Applicability)

2.2.1 憑證的適用範圍與償責(Certificate's Applicability and Liability)

2.2.1.1 憑證身分認證安全等級(Level of Assurance)

本公司認證服務系統於用戶註冊時，依身分認證方式區分安全及保證等級如下：

(1) 第一級(Class 1)：

1. 身分認證方式：

   用戶憑證管理中心或註冊中心僅透過電子郵件，以簡單的程序對用戶名稱(如個人姓名或公司註冊名稱或網域名稱<URL>)及電子郵件信箱資訊進行有限之查證。

2. 保證等級：

   用戶憑證管理中心及註冊中心僅保證用戶名稱及電子郵件信箱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。

3. 適用範圍：

   供憑證用戶 E-mail 電子文件或保護自己的電子文件時使用，但不可使用於須經身分確認之商業交易。

(2) 第二級(Class 2)：

1. 身分認證方式：

   用戶註冊時除了個人姓名或公司註冊名稱或網域名稱(URL)及一般相關資訊的檢核外，必須提供合法且正確的證明文件〈例如個人身分證或公司的營利事業登記證影本〉，但不需本人親自辦理；用戶憑證管理中心或註冊中心將透過電話或其他途徑(如第三者之資料庫)確認申請者之身分。

2. 保證等級：

   用戶憑證管理中心及註冊中心保證用戶名稱及電子郵件信箱於本公司資料

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。

3. 適用範圍：

建議使用於企業內部或非金融、非有價證券之小額電子商務交易或傳輸加密時使用。

(3) 第三級(Class 3)：

1. 身分認證方式：

除了第二級相關資訊的檢核外，必須由本人親自辦理，法人或企業用戶必須由持有授權文件之代理人親自辦理，且提供的證明文件足以識別申請者〈例如具有相片的身分證或護照〉。

2. 保證等級：

經由多重嚴謹之作業程序，提供高於第二級憑證之身分認證保證，高度提升用戶及信賴憑證者對憑證之信賴。

3. 適用範圍：

建議使用於金融或有價證券交易。

(4) 測試憑證：

1. 身分認證方式：

用戶憑證管理中心及註冊中心均未執行任何驗證用戶身分之程序，且僅供測試使用，不可使用於測試以外之任何應用或業務。

2. 保證等級：

用戶憑證管理中心及註冊中心均不做任何形式之保證。

3. 適用範圍：

僅供用戶憑證管理中心授權之用戶使用，且僅供測試使用，不可使用於測試以外之任何應用或業務。

2.2.1.2 憑證適用範圍與償責(Scope of Using and Liability)

本公司憑證的使用範圍、交易限額及賠償限額，詳列如表一，憑證安全等級及使用範圍代碼說明如下，本公司憑證使用範圍之代碼共分四段，各段依下列原則區分及編碼之：

☆ 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

範例：3.1.2.1 代表第三級身分認證、單一用途、之自然人持有、使用於金融交易的憑證

第 一 段 [身分認證安全等級]	第 二 段 [用途別]	第 三 段 [用戶身分]	第 四 段 [適用業務範圍]
1.第一級 2.第二級 3.第三級 0. 測試用憑證	1.單一用途 2.限定範圍內多用途	1.法人 2.自然人 3.其他	1.金融交易、電子商務應用、網路報稅、電子發票、電子通訊投票、短期票券發行交易應用

			2.有價證券交易、電子商務應用、網路報稅、電子發票、電子通訊投票 3.電子商務應用、線上身分確認、網路報稅、電子發票、電子通訊投票、線上申請專利商標、電子郵件應用

1. 第一段為身分認證安全等級：

區分為 (1)第一級、(2)第二級、(3)第三級、 (0)測試憑證，安全性係依用戶註冊時身分認證的方式區分等級，請參閱「2.2.1.1 憑證身分認證安全等級」之規範。

2. 第二段為用途別(Usage)：

區分為(1)單一用途、(2)限定範圍內多用途(例如金控公司範圍內)，說明：

(1). 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。

(2). 限定範圍內多用途：若於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。下列 FXML、EC、MARKET 為限定使用範圍之代碼，將記載於憑證中憑證政策之憑證簽發者的簡要聲明欄位：

a. FXML：供憑證持有者與本公司認可之註冊中心間交易使用，惟憑證持有者須先至交易對方辦理註冊或登記；該憑證之原始註冊中心為銀行。

b. EC：供憑證持有者與本公司認可之註冊中心間交易使用，惟憑證持有者須先至交易對方辦理註冊或登記，且該交易為資訊流電子商務交易。

c. MARKET：供憑證持有者與本公司認可之註冊中心提供之交易平台中使用，惟憑證持有者須先至該註冊中心辦理註冊或登記。

3.第三段為用戶身分：

區分為(1)法人、(2)自然人、(3)其他。

4.第四段為適用業務範圍(Business Category)：

區分為(1)金融交易、電子商務應用、網路報稅、電子發票、電子通訊投票、短期票券發行交易應用、(2)有價證券交易、電子商務應用、網路報稅、電子發票、電子通訊投票、(3)電子商務應用、線上身分確認、網路報稅、電子發票、電子通訊投票、線上申請專利商標、電子郵件應用；其中金融交易用憑證亦得於符合使用範圍限制之規範或本公司同意下，使用於有價證券交易及電子商務應用、線上身分確認。

例如:網路銀行現行企業憑證之使用範圍代碼為 3.1.1.1 解讀如下：

(3)安全性第三級・(1)單一用途・(1)法人用戶・(1)金融交易使用。

✪ 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：依安全性、用途別、客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：依安全性、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。

*憑證適用範圍及賠償責任表如下所示：

〈表一〉 單位：新台幣元

使用範圍代碼(Class)	安全等級	用途別	用戶身分	適用業務範圍	交易限額	賠償限額
1.1.1.3	第一級	單一用途	法人	電子商務應用、線上身分確認	3,000	3,000
1.1.2.3	第一級	單一用途	自然人	電子商務應用、線上身分確認	3,000	3,000
1.1.3.3	第一級	單一用途	其他	電子商務應用、線上身分確認	3,000	3,000
2.1.1.3	第二級	單一用途	法人	電子商務應用、線上身分確認、電子郵件應用	900,000	300,000
2.1.2.3	第二級	單一用途	自然人	電子商務應用、線上身分確認、電子郵件應用	300,000	100,000
2.1.3.3	第二級	單一用途	其他	電子商務應用、線上身分確認、電子郵件應用	900,000	300,000
3.1.1.1	第三級	單一用途	法人	金融交易	不限定	2,000,000
3.2.1.1	第三級	限定範圍內多用途	法人	金融交易、電子商務應用、網路報稅、電子發票、電子通訊投票、短期票券發行交易應用	不限定	2,000,000
3.1.2.1	第三級	單一用途	自然人	金融交易	不限定	300,000

3.2.2.1	第三級	限定範圍內多用途	自然人	金融交易、電子商務應用、網路報稅、電子通訊投票、短期票券發行交易應用	不限定	300,000
3.1.1.2	第三級	單一用途	法人	有價證券交易	100,000,000	2,000,000
3.2.1.2	第三級	限定範圍內多用途	法人	有價證券交易、電子商務應用、網路報稅、電子發票、電子通訊投票	100,000,000	2,000,000
3.1.2.2	第三級	單一用途	自然人	有價證券交易	15,000,000	300,000
3.2.2.2	第三級	限定範圍內多用途	自然人	有價證券交易、電子商務應用、網路報稅、電子通訊投票	15,000,000	300,000
3.1.1.3	第三級	單一用途	法人	電子商務應用、線上身分確認、線上申請專利商標	20,000,000	2,000,000
3.2.1.3	第三級	限定範圍內多用途	法人	電子商務應用、線上身分確認、網路報稅、電子發票、電子通訊投票	20,000,000	2,000,000
3.1.2.3	第三級	單一用途	自然人	電子商務應用、線上身分確認、線上申請專利商標	2,000,000	300,000
3.2.2.3	第三級	限定範圍內多用途	自然人	電子商務應用、線上身分確認、網路報稅、電子通訊投票	2,000,000	300,000

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

2.2.1.3 憑證適用範圍與限制 (Using and Prohibition)

1.當憑證內容未將本公司使用範圍代碼載明於「憑證政策之憑證簽發者的簡要聲明(TerseStatement)欄位」時：

因本公司原有之 CA 系統，受限於已發行之用戶憑證，無法將本公司使用範圍代碼增訂於「憑證政策之憑證簽發者的簡要聲明」欄位註記，本公司另於此定義說明，未於以下定義者，該憑證即不得使用於測試以外之任何應用或業務，且本公司對此憑證不負賠償責任:

〈一〉、網際 NB 憑證系統 (NBCA)

本公司簽發之憑證中，其憑證簽發者 DN(Issuer Distinguished Name)下之 CN 欄位資料載明有「TEST」者，即為測試用憑證，本公司對此憑證不負賠償責任。

本公司簽發之憑證中，其憑證簽發者 DN(Issuer Distinguished Name)下之 CN 欄位資料以「NBS」或「NSS」或「ERS」或「VOT」或「INS」或「ECB」或「TCA」開頭者，即為網際 NB 憑證。

〈O 為 OrganizationName 之前面第一個英文字母的簡稱，OU 為 OrganizationUnitName 的簡稱，CN 為 CommonName 的簡稱〉

(1).本公司簽發之網際 NB 憑證內容，於用戶替代名稱(SubjectAltName)下之第三子欄位用戶類別載明非為「B1」〈解讀為 Binary 10000000〉，此憑證即為法人用戶持有使用，範例如「SubjectType = B1」。

(2).本公司簽發之網際 NB 憑證內容，於用戶替代名稱(SubjectAltName)下之第三子欄位用戶類別載明為「B1」〈解讀為 Binary 10000000〉，此憑證即為自然人用戶持有使用。

(3).本公司簽發之網際 NB 憑證內容，其憑證簽發者 DN 下之 CN 欄載明「NBS」開頭者，其憑證使用範圍及賠償責任為「Class 3.1.1.1 ,或 Class 3.1.2.1, 或 Class 3.2.1.1, 或 Class 3.2.2.1」。

(4).本公司簽發之網際 NB 憑證內容，其憑證簽發者 DN 下之 CN 欄載明「NSS」開頭者，其憑證使用範圍及賠償責任為「Class 3.1.1.2 ,或 Class 3.1.2.2, 或 Class 3.2.1.2, 或 Class 3.2.2.2」。

(5).本公司簽發之網際 NB 憑證內容，其憑證簽發者 DN 下之 CN 欄載明「ERS」開頭者，其憑證使用範圍及賠償責任為「Class 3.1.1.3,或 Class 3.1.2.3，或 Class 3.2.1.3 ,或 Class 3.2.2.3」。

(6).本公司簽發之網際 NB 憑證內容，其憑證簽發者 DN 下之 CN 欄載明「VOT 」開頭者，其憑證使用範圍及賠償責任為「Class 3.2.1.3 ,或 Class 3.2.2.3」。

(7).本公司簽發之網際 NB 憑證內容，其憑證簽發者 DN 下之 CN 欄載明「INS」開頭者，其憑證使用範圍及賠償責任為「Class 3.2.1.3 ,或 Class 3.2.2.3」。

(8).本公司簽發之網際 NB 憑證內容，其憑證簽發者 DN 下之 CN 欄載明「ECB」開頭者，其憑證使用範圍及賠償責任為「Class 3.2.1.3 ,或 Class 3.2.2.3」。

(9).本公司簽發之網際 NB 憑證內容，其憑證簽發者 DN 下之 CN 欄載明「TCA」開頭者，其憑證使用範圍及賠償責任為「Class 3.2.1.3 ,或 Class 3.2.2.3」。

〈二〉、商務 EC 憑證系統 (EC+)

本公司簽發之憑證中，其憑證簽發者 DN(Issuer Distinguished Name)欄位載明為「CN=TaiCA Secure CA,OU=Certification Service Provider,O=TAIWAN-CA.COM Inc.,C=TW」者，即為商務 EC 憑證。本公司簽發之商務 EC 憑證內容，於憑證申請者 DN 下之 CN 欄位內容資料載明有「公司企業統一編號」者，此憑證即為法人用戶持有者使用，範例如「CN= TW1674277416742774」；於憑證申請者 DN 下之 CN 欄位內容資料載明有「自然人身分證字號」者，此憑證即為自然人用戶持有者使用，範例如「CN= TWH14520147801」。

(1).本公司簽發之商務 EC 憑證內容，其憑證申請者 DN 下之 OU 欄位內容載明有「銀行英文名稱」者，範例如「OU=Cathay United Bank」， 其憑證使用範圍及賠償責任為「Class 3.1.1.1, 或 Class 3.1.2.1 或 3.2.1.1,或 3.2.2.1」。

(2).本公司簽發之商務 EC 憑證內容，其憑證申請者 DN 下之 OU 欄位內容載明有「證券商英文名稱」者，範例如「OU=DASHIN SECURITIES CO. LTD.」， 其憑證使用範圍及賠償責任為「Class 3.1.1.2, 或 Class 3.1.2.2 或 3.2.1.2,或 3.2.2.2」。

(3).本公司簽發之商務 EC 憑證內容，其憑證申請者 DN 下之 OU 欄位內容載明有「電子商務單位英文名稱，且非銀行或證券商英文名稱」者，範例如「OU=TAIWAN-CA.COM Inc. (FORMOSA RA)」,其憑證使用範圍及賠償責任為「Class 3.1.1.3 或 3.1.2.3 或 3.2.1.3 或 3.2.2.3」。

本公司簽發之憑證中，其憑證簽發者 DN(Issuer Distinguished Name)欄位載明為「CN=TaiCA Secure CA,OU=SSL Certification Service Provider,O=TAIWAN-CA.COM Inc.,C=TW」者，即為 SSL 伺服器憑證。

本公司簽發之 SSL 伺服器憑證內容，其憑證申請者 DN 下之 CN 欄位載明為網站名稱(URL)，即為 SSL 伺服器憑證，範例如「CN=WWW.TAICA.COM.TW」。

其憑證使用範圍僅供網站間傳輸加密使用，其交易限額為新台幣壹仟萬元，賠償限額為新台幣貳佰萬元。

〈三〉、商務 XML 憑證系統

(1).本公司簽發之憑證中，其憑證簽發者 DN(Issuer Distinguished Name)欄位載明為「CN=TaiCA Information User CA,OU=User CA,O=TaiCA,C=TW」者，即為商務 XML 憑證。

本公司簽發之商務 XML 憑證內容，於憑證申請者 DN 下之 CN 欄位內容資料載明有「公司企業統一編號」者，此憑證即為法人用戶持有使用，範例如「CN= 16742774-16-A742774」;於憑證申請者 DN 下之 CN 欄位內容資料載明有「自然人身分證字號」者，此憑證即為自然人用戶持有使用，範例如「CN= H145201478-01-001」，其憑證使用範圍及賠償責任為「Class 3.2.1.3,或 Class 3.2.2.3,或 Class 3.2.1.1,或 Class3.2.2.1」。

(2).本公司簽發之憑證中，其憑證簽發者 DN 欄位載明為「CN=TaiCA Finance User CA,OU=User CA,O=TaiCA,C=TW」者，即為通關稅費憑證。

本公司簽發之通關稅費憑證內容，於憑證申請者 DN 下之 CN 欄位內容資料載明有「公司企業統一編號」者，此憑證即為法人用戶持有使用，範例如「CN= 16742774-16-A742774」;於憑證申請者 DN 下之 CN 欄位內容資料載明有「自然人身分證字號」者，此憑證即為自然人用戶持有使用，範例如「CN= H145201478-01-001」，其憑證使用範圍及賠償責任為「Class 3.1.1.1,或 Class 3.1.2.1,或 Class 3.2.1.1,或 Class3.2.2.1」。

(3).本公司簽發之憑證中，其憑證簽發者 DN 欄位載明為「CN=TWCA SMIME User CA,OU=User CA,O=TAIWAN-CA Inc.,C=TW」者，即為 S/MIME 憑證。

本公司簽發之 S/MIME 憑證內容，於憑證申請者 DN 下之 CN 欄位內容資料載明有「應用別+編號後四碼+流水號」者，範例如「CN=

SMIME5678-00-000001」，其憑證使用範圍及賠償責任為「Class 2.1.1.3,或 Class 2.1.2.3,或 Class 2.1.3.3」。

2.當憑證內容已將本公司適用範圍代碼載明於憑證內之「憑證政策(Certificate Policy:CP)憑證簽發者的簡要聲明(TerseStatement)」欄位註記時：

(1).憑證適合之應用:請參閱上述「2.2 憑證的適用性」之內容。

(2).憑證適用範圍限制:憑證用戶及信賴憑證者皆應依憑證內記載之適用範圍代碼使用於適用之業務範圍內，並須遵循用途及交易對象之限制，且交易之金額不得超過表列之交易限額。

(3).憑證用戶及信賴憑證者於交易時，應確認憑證內容憑證政策(CP)之憑證簽發者的簡要聲明(TerseStatement)欄位，確認交易係於規範之使用範圍內才可後續處理及完成交易。

(4).提供簽驗章或加解密安控軟硬體系統之廠商應將憑證使用範圍顯示於明顯處供客戶確認，或以程式檢核憑證確實於訂定的使用範圍內使用。

憑證簽發者簡要聲明(TerseStatement) 範例：

〈 有關憑證使用的交易限額與賠償限額，詳述於 2.2.1.2 之 表〈一〉 〉

<1>.Restriction = 3.1.1.1,Financial,only for the authorized relying party :refer to the 1st OU of this certificate's Subject DN.

(DN 為 Distinguished Name 前面的第一個英文字母簡稱，OU 為 Organization Unit Name 前面的第一個英文字母簡稱) 表示本憑證為第三級單一用途憑證，信賴憑證者限制為本憑證申請者識別名稱(Subject DN)欄位內存放的第一個組織名稱(OU)欄位內所描述授權的信賴單位，憑證持有者為企業(法人)用戶，供金融交易使用。

<2>.Restriction = 3.1.2.2,Securities,only for the authorized relying party :refer to the 1st OU of this certificate's Subject DN.

表示本憑證為第三級單一用途憑證，信賴憑證者限制為本憑證申請者識別名稱(Subject DN)欄位內存放的第一個組織名稱(OU)欄位內所描述授權的信賴單位，憑證持有者為個人(自然人)用戶，供有價證券交易使用。

<3>.Restriction = 3.2.1.1,Financial,FXML.

表示本憑證為第三級限定範圍內多用途憑證，供憑證持有者與本公司認可之註冊管理單位間交易使用，惟憑證持有者須先至交易對方辦理註冊或登記；該憑證之持有者為企業(法人)用戶，適用之業務範圍為金融交易。

<4>.Restriction = 1.1.1.3,Non-financial and non-securities,only for the authorized relying party:refer to the 2nd OU of this certificate's Subject DN.

表示本憑證為第一級單一用途憑證，信賴憑證者限制為本憑證申請者識別名稱(Subject DN)欄位內存放的第二個組織名稱(OU)欄位內所描述授權的信賴

單位，憑證持有者為企業(法人)用戶，供憑證用戶使用於電子商務應用或線上身分確認。

<5>.Restriction = 3.2.2.2,Securities,EC

表示本憑證為第三級限定範圍內多用途憑證，供憑證持有者與本公司認可之註冊中心間交易使用，惟憑證持有者須先至交易對方辦理註冊或登記；該憑證之持有者為自然人用戶，適用之業務範圍為有價證券交易。

☆ **禁止使用之狀況:憑證除依照上述規定使用於相關的範圍，絕不可使用於：**

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。

2.3 識別(Identification)

本憑證實務作業基準所詳述之各種憑證分類，其所對應的憑證政策之物件識別碼(Object Identifier; OID)分別說明如后：

〈一〉、網際 NB 憑證 (NBCA)

OID=2.16.886.3.1.1.5

〈二〉、商務 EC 憑證 (EC+)

OID=2.16.886.3.1.3.1

〈三〉、商務 XML 憑證

OID=2.16.158.3.1.8.5

2.3.1 標準規範(Standards)

本「憑證實務作業基準」參考下列標準規範編撰：

1. RFC 3647, *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*, IETF PKIX RFC 3647 November 2003.
2. 經濟部於 2004 年 7 月 7 日所訂定發布之憑證實務作業基準應載明事項準則。
3. 臺灣網路認證股份有限公司公開金鑰基礎建設憑證政策(CP)V1.5。

2.3.2 定義(Definition)

有關本憑證實務作業基準所使用到的名詞與字義，請參考附錄一的詞彙解釋。

用戶在了解本憑證實務作業基準作業規範前，建議已熟悉如下所列基本 PKI(Public Key Infrastracture)運作的觀念：

1.數位簽章(Digital Signature)使用於身分與交易訊息的鑑別(Authentication)、訊息的完整性(Integrity)，與交易訊息傳送或接收的不可否認性(non-Repudiation)。

2.交易訊息機密性(Confidentiality)的密碼系統，例如對稱性或非對稱性的密碼系統。

3.非對稱性的密碼系統，公開/私密金鑰對(Public/Private Key Pairs)，公開金鑰憑證(Public Key Certificate)，例如數位簽章與數位信封(Digital Envelope)的機制。

4.公開金鑰基礎建設 PKI 階層架構下，憑證管理中心(CA)、註冊中心(RA)的運作功能。

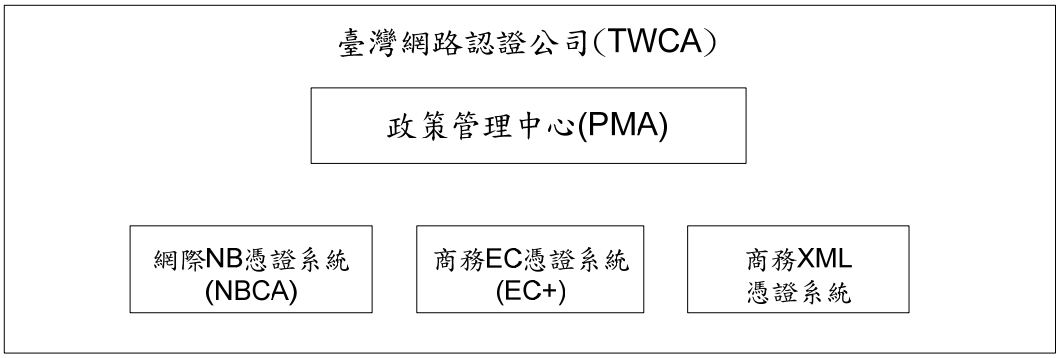
2.4 公開金鑰基礎建設與應用(Community and Applicability)

2.4.1 TWCA憑證機構(TWCA Certificates Service Provider)

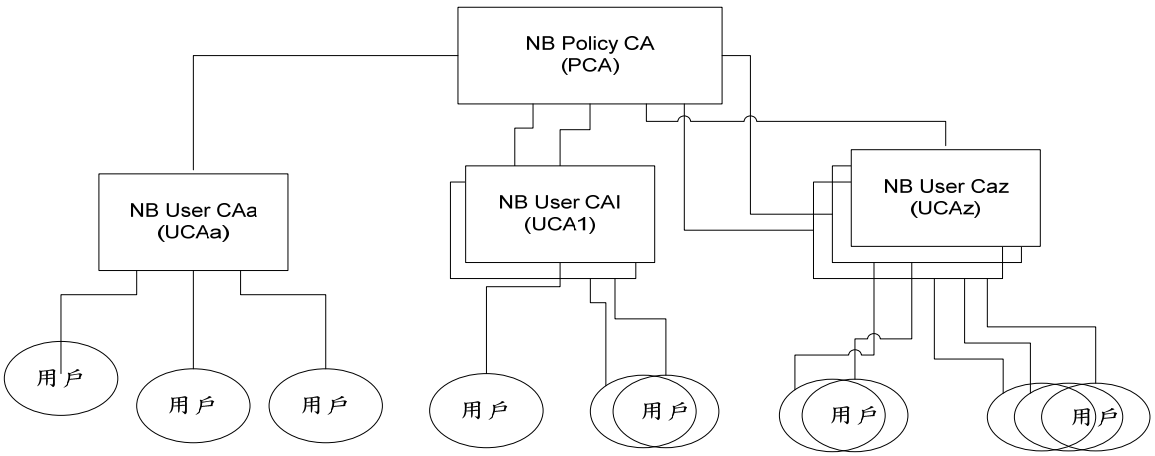
本公司為簽發 1.網際 NB 憑證(NBCA)、2.商務 EC 憑證(EC+) 及 3.商務 XML 憑證等各憑證之執行與管理單位。

本公司係配合法律、政策、主管機關訂定之電子簽章法與相關施行細則及憑證機構管理規範與業務需求，訂定、公告及管理下列事項完成身分及憑證之識別與驗證：

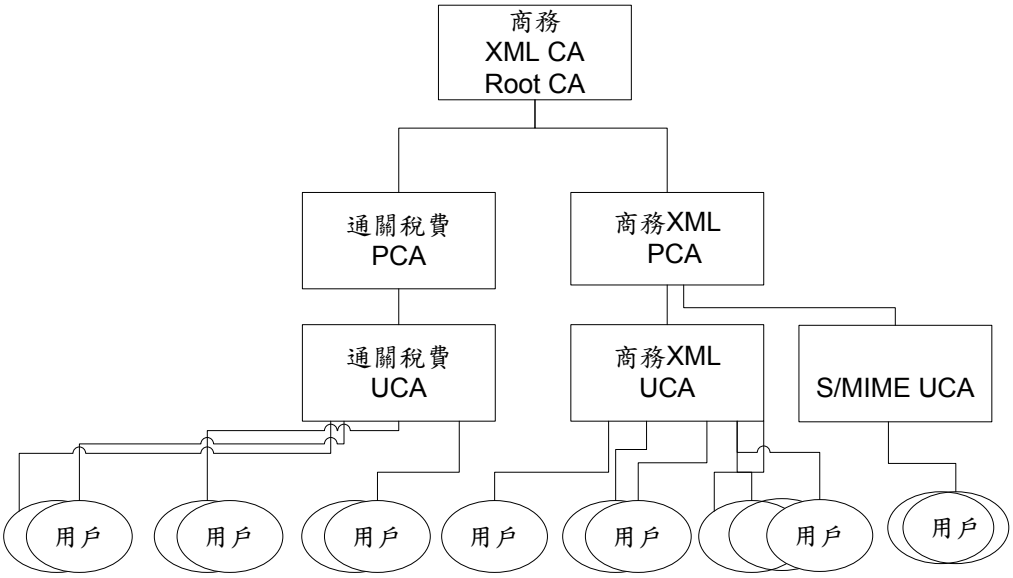
1. 最高層憑證管理中心(RCA)、政策憑證管理中心(PCA)、用戶憑證管理中心(UCA)之 PKI 架構與規範。
2. 憑證政策(CP)及憑證實務作業基準(CPS)。
3. 憑證及廢止憑證之內容。
4. 跨國憑證 PKI 間相互認證(Cross Certification)的作業規範與程序。



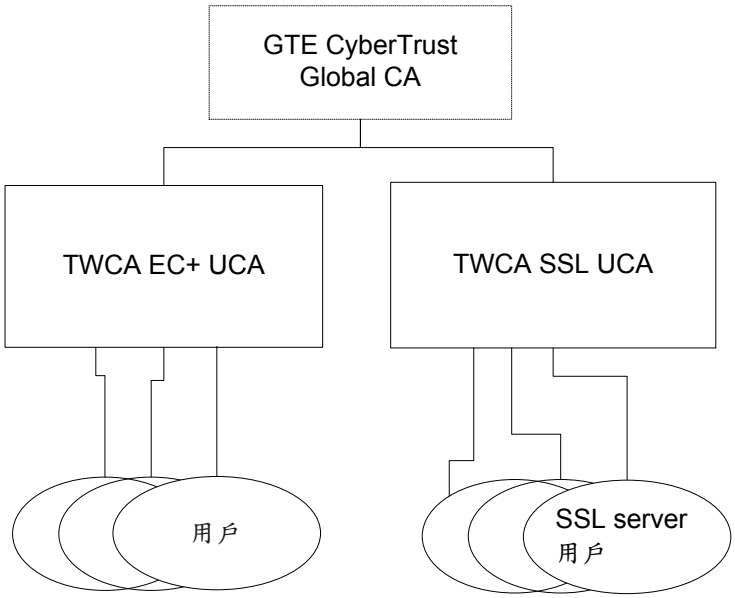
〈一〉、網際 NB 憑證系統 (NBCA)



〈二〉、商務 XML 憑證系統



〈三〉、商務 EC 憑證系統 (EC+)



2.4.2 最高層憑證管理中心(Root Certification Authority；RCA)

- 管理與公告政策憑證管理中心之註冊、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、管理與遞送政策憑證管理中心(PCA)的憑證、憑證廢止清冊。
- 建置於獨立、安全管控的作業環境下，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、建置與簽發政策憑證管理中心憑證的作業，Root CA 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最高層憑證管理中心索取。

2.4.3 政策憑證管理中心 (Policy Certification Authority；PCA)

- 遵循最高層憑證管理中心訂定的規範。
- 管理與公告用戶憑證管理中心之註冊、憑證、憑證廢止清冊的作業程序與驗證的作業規範。
- 簽發、管理與遞送用戶憑證管理中心的憑證、憑證廢止清冊。

2.4.4 用戶憑證管理中心 (User Certification Authority；UCA)

- 遵循政策憑證管理中心訂定的規範。
- 公告及管理用戶註冊、憑證、憑證廢止清冊的作業程序與驗證的作業規範。
- 接受用戶憑證的申請、更新、暫時停用、廢止、查詢及有關註冊申請作業。
- 簽發、管理與遞送註冊中心與用戶的憑證、憑證廢止清冊及用戶資訊。

2.4.5 註冊中心(Registration Authority；RA)

註冊中心負責用戶憑證管理中心註冊管理作業：

- 遴選優良金融機構或相關單位擔任註冊中心，註冊中心與本公司簽立合約後負責註冊業務。
- 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驗證的作業規範。
- 驗證用戶註冊，憑證簽發與廢止及查詢之申請訊息，身分合法性與訊息的正確性。
- 遞送用戶的註冊申請訊息與憑證、廢止憑證、查詢申請訊息，至用戶憑證管理中心辦理。
- 註冊、申請憑證、廢止憑證，並驗證回覆訊息的正確性後傳回申請之用戶。
- 公告、管理註冊中心之註冊名稱、網址、電子郵箱與聯絡的相關資訊。
- 處理費用作業。

2.4.6 儲存庫(Repository Authority; RA or Directory Authority; DA)

- 以目錄伺服器(Directory Server)或資料庫的作業方式，管理、公告並提供使用者查詢用戶憑證、廢止憑證及憑證管理中心的憑證鏈(Certificate Chain)。
- 管理與公告目錄伺服器查詢資訊時的作業程序與身分驗證及訊息安控措施的作業規範。
- 管理與公告線上憑證狀態協定(Online Certificate Status Protocol:OCSP)查詢資訊時的作業程序與身分驗證及訊息安控措施的作業規範。
- 驗證用戶查詢資訊時，身分的合法性與查詢訊息的有效性，並將正確的訊息傳回查詢之用戶。
- 公告、管理儲存庫的註冊名稱、網址、電子郵箱與聯絡的相關資訊。

2.4.7 使用者(End Entities)

2.4.7.1 用戶(Users or Subscribers)

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，其憑證與憑證對應的私密金鑰使用的業務範圍，皆依本作業基準之規範，運用於相關業務上，包括網路銀行系統、網路下單系統、網路保險系統、網路票債券系統、網路企業系統等的個人或法人企業之電子商務交易；用戶可以自我憑證對應的私密金鑰執行交易訊息的簽章。

2.4.7.2 信賴憑證者(Relying Parties)

信賴憑證者即為使用他人(用戶)的憑證、用戶憑證管理中心、政策憑證管理中心與最高層憑證管理中心的憑證鏈(Certificate Chain)資訊，用以驗證接收的簽章訊息之完整性與不可否認性，或使用他人(接收者) 的憑證做訊息的加密後、將加密的訊息傳送至接收者，以達到通訊雙方訊息的隱密性。

2.4.8 政策管理中心 (Policy Management Authority;PMA)

設於本公司內之組織並負責制定下列事項：

1.憑證政策(CP)。

2.憑證實務作業基準(CPS)。

3.營運等規範。

2.4.9 應用(Applicability)

本作業基準所規範及簽發的憑證，用戶必須依照本作業基準與業務應用系統規範之規定，合法且正確使用私密金鑰與憑證於相關之業務系統，不得使用於 1.本作業基準規範內容之外、2.對社會秩序與社會環境有重大危害之應用或業務系統、3.電子簽章法相關法令暨主管機關明訂禁止之應用或業務；否則因而所致之損害，由用戶承擔之。

2.4.9.1 風險與安全

公開金鑰系統的憑證之可信度，繫於憑證簽發管理系統之公開金鑰與私密金鑰的唯一性、身分的驗證性、實體設施〈包括硬軟體〉設備的安全性、人員作業程序安全管控的嚴謹性，及訊息於網際網路上傳遞時的安全性。

應用系統選用公開金鑰系統時，除考量憑證所提供安全度的因素外，尚需考慮內部與外在環境人為的破壞因素與天然災變之威脅風險等級，設定適合應用系統安全等級的安全措施，本作業基準以下各章節，將詳細敘述本公司公開金鑰認證服務系統相關的作業規範及安全措施。

2.5 聯絡事宜(Contact Details)

2.5.1 管理單位(Specification Administration Organization)

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

2.5.2 聯絡窗口(Contact Person)

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	(100) 台北市中正區延平南路 85 號 10 樓 10TH Floor,85,Yen-Ping South Road,Taipei,Taiwan, R.O.C
電話	886-2-23708886
傳真	886-2-23700728
電子郵箱(E-mail)	ca@twca.com.tw
網址(URL)	http:// www.twca.com.tw

2.5.3 CPS修改與訂定(Person Determining CPS Suitability for the Policy)

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)。

3.一般規範(General Provisions)

3.1 義務(Obligations)

3.1.1 本公司之義務(CSP Obligations)

- 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與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。
- 依照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、暫時停用、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，詳細說明憑證申請、更新、暫時停用、廢止、註冊與使用的作業規範，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。

3.1.2 註冊中心之義務(RA Obligations)

- 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，執行用戶註冊身分認證及憑證申請、更新、暫時停用、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，確實了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，並於用戶親自辦理下簽名確認〈或法人戶的合法授權代理人員之親自辦理下簽名確認〉，或於依據用戶註冊時身分認證安全等級的作業規範，由用戶簽名確認。
- 接受用戶註冊、註銷、憑證申請、更新、暫時停用、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，詳細說明憑證申請、更新、暫時停用、廢止、查詢、註冊與使用的作業規範，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。

3.1.3 儲存庫之義務(Repository Obligations)

- 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全管控措施的運作。
- 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，每天二十四小時提供正常服務。
- 驗證用戶至目錄伺服器或資料庫查詢資訊時，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決無法查詢。
- 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。

3.1.4 用戶之義務(Subscriber Obligations)

- 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，必須確實了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、暫時停用、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。
- 用戶必須了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。

3.1.5 信賴憑證者之義務(Relying Party Obligations)

- 憑證的使用，信賴憑證者必須了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權利與義務的規定，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，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，尚需檢核此憑證是否為廢止或暫時停用憑證。

- 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。

3.2 賠償責任(Liability)

本公司所提供的認證服務作業項目與內容，皆訂定於本作業基準「2.2 憑證的適用性」，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。

3.2.1 本公司之憑證賠償責任(TWCA CA Liability)

- 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而非為本公司的故意或過失，或其他不可抗拒的天災事故〈例如戰爭或地震等〉，致所簽發之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「2.2.1.2 憑證適用範圍與償責」；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時停用用戶的憑證要求後，至用戶憑證管理中心實際公布廢止或暫時停用該用戶憑證〈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時，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律的規範辦理。

3.2.2 註冊中心賠償責任(RA Liability)

- 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時停用用戶的憑證要求後，至簽發該憑證之用戶憑證管

理中心實際公布廢止或暫時停用該用戶憑證〈憑證廢止清冊〉為止之期間內，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，如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，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。

3.2.3 用戶賠償責任(Subscriber Liability)

- 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時停用用戶的憑證要求後，至簽發該憑證之用戶憑證管理中心實際公布廢止或暫時停用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，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；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，如本公司與註冊中心執行處理作業時，符合憑證實務作業基準與相關的作業規範，則信賴憑證者必須負損害賠償責任；於提出廢止或暫時停用用戶的憑證之期間內，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。
- 用戶申請使用憑證或使用信賴憑證者憑證，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。

3.3 財務責任 (Financial Responsibility)

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。

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，為分散業務的營運風險，目前積極洽詢國內外相關的保險公司投保認證業務責任險；本公司為保障用戶的權益，於完成保險作業之前，先行提撥新台幣參仟萬元作為執行憑證業務時產生賠償責任風險的財務保證基金。

3.3.1 第三者免責權(Indemnification by Relying Parties and Subscriber)

因信賴憑證者或用戶的故意或過失，而非為本公司或註冊中心的疏失，所造成第三者財務、信譽及其他各方面的損害時，本公司或註冊中心擁有賠償責任豁免權。

如因信賴憑證者或用戶的過失且可歸責於信賴憑證者或用戶，而造成本公司或註冊中心、或其他第三者財務、信譽及其他各方面的損害時，信賴憑證者或用戶必須負損害賠償責任，本公司或註冊中心可依照相關法律的規定向信賴憑證者或用戶請求賠償。

3.3.2 代理(Fiduciary Relationships)

本公司、註冊中心與用戶三者間絕無互為代理之關係存在。

3.4 釋義與執行(Interpretation and Enforcement)

3.4.1 政府管理之法規(Governing Law)

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、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。

3.4.2 適用性(Severability of Provisions, Survival, Merger, and Notice)

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「2.5 聯絡事宜」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，必需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。

3.4.3 爭議處理程序(Dispute Resolution Procedures)

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，無法以上面的處理方式解決時，則必須依照相關的跨國或跨區域的糾紛仲裁規範處理。

3.5 服務費(Fees)

3.5.1 憑證申請或更新收費(Certificate Issuance or Renewal Fees)

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。

3.5.2 憑證查詢收費(Certificate Access Fees)

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。

3.5.3 憑證廢止與憑證狀態查詢收費(Revocation or Status Information Access Fees)

用戶憑證管理中心提供用戶憑證廢止功能與線上憑證狀態協定(OCSP)查詢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。

3.5.4 其他收費

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 或 CP 或其他相關作業文件時，本公司需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。

3.5.5 退費

網際 NB 憑證、商務 XML 憑證、商務 EC 憑證，用戶於完成憑證簽發後，七日內向本公司或註冊中心申請退費並廢止憑證者，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。

商務 EC 憑證之 SSL 伺服器憑證，用戶於完成憑證申請，但憑證尚未簽發前，向本公司申請退費者，扣除參仟元的處理工本費後，餘無息退還予用戶，於完成憑證簽發後，用戶始申請退費時，按比例扣除使用月份之費用後，再扣除參仟元的處理工本費，餘無息退費。

3.6 公布與儲存 (Publication and Repository)

3.6.1 本公司憑證資訊公布(Publication of CA Information)

本憑證實務作業基準以電子檔案 PDF(.pdf)格式，於正式生效前一個月公告於本公司網站供用戶下載及查詢使用；網址：http://www.twca.com.tw。

用戶有憑證實務作業基準紙本文件的需求，或有與認證作業有關的問題時，請洽下列聯絡窗口：

公司名稱	臺灣網路認證股份有限公司 (TAIWAN-CA INC.；TWCA)
聯絡單位	客服中心
地址	(100) 台北市中正區延平南路 85 號 10 樓 10TH Floor,85,Yen-Ping South Road,Taipei,Taiwan, R.O.C
電話	886-2-23708886
傳真	886-2-23700728
電子郵箱(E-mail)	ca@twca.com.tw

3.6.2 公布頻率(Frequency of Publication)

經修改完成且經政策管理中心(PMA)核定生效後之新版憑證政策(CP)，即刻公告於本公司網站。

依照需求經修改完成且經主管機關核定生效後之新版憑證實務作業基準(CPS)，即刻公告於本公司網站。

用戶憑證、用戶憑證管理中心憑證與憑證廢止清冊，一經產生後即刻公告於儲存庫供用戶查詢使用；網際 NB 憑證的用戶憑證經申請廢止後，即刻產生並公告憑證廢止清冊，商務 EC 憑證、與商務 XML 憑證經申請廢止後，依據「5.4.9 憑證廢止清冊產生頻率」每二十四小時產生及公布一次。

3.6.3 存取管控(Access Control)

本作業基準沒有存取權限的安全管控，用戶可以依需求至網站下載。

目錄伺服器或資料庫的憑證、廢止憑證資訊，僅開放用戶查詢使用，但不提供修改的功能，用戶必須依照用戶憑證管理中心儲存庫的安全管控措施執行存取。

3.6.4 儲存庫(Repositories)

用戶憑證管理中心儲存庫係以本公司資料庫及目錄伺服器的作業方式提供用戶，用戶憑證與用戶憑證管理中心憑證、憑證廢止清冊的查詢及使用，儲存庫內資訊的存取，除憑證與憑證廢止清冊的資訊查詢外，其他儲存庫資訊非經授權的用戶絕無法查詢。

3.7 稽核(Compliance Audit)

3.7.1 稽核頻率(Frequency of Compliance Audit for Each Entity)

本公司憑證系統業務營運安全管控的稽核作業，以本公司訂定的內部自行查核規範〈依據 ANS X9.79-2001 Certification Authority Control Object(CACO)的查核標準，與參考 ISO 27001:2005 Information Technology – Code of Practice for Infor-mation Security Management 編撰)，每年至少定期執行一次內部自行查核作業。

3.7.2 稽核人員適任條件(Identity/Qualifications of Auditor)

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者並具有稽核的相關實務經驗。

3.7.3 稽核人員客觀性(Auditor's Relationship to Audited Party)

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，可以委由專業且公正、客觀的專責稽核機構，代為執行稽核相關作業。

3.7.4 稽核內容(Topics Cover by Audit)

稽核人員查核：

1. 是否訂定憑證實務作業基準及相關作業規範。
2. 是否依憑證實務作業基準及相關作業規範執行相關業務。
3. 註冊中心是否依憑證實務作業基準訂定註冊相關作業規範。
4. 註冊中心是否依憑證實務作業基準的規範及註冊中心作業規範的規定執行相關業務。

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。

3.7.5 稽核缺失的處理(Action Taken as a Result of Deficiency)

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。

3.7.6 稽核結果的處理(Communication of Results)

稽核結果經與受檢單位的相關業務人員討論確定後，視為重要隱密資訊處理，只有受檢單位與相關稽核人員可知悉，非經受檢單位的授權稽核單位絕不洩露與其他人員取得或知悉。

3.8 機密性(Confidentiality)

3.8.1 資訊的保護種類(Type of Information to be keep Confidential)

本公司對於用戶資訊的保護，皆依照「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 個人資料隱密性的保護規範(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/註冊中心於管理及使用用戶的相關資訊時，除用戶憑證內容可公開外，用戶的註冊基本資料與身分認證資料，非經由用戶的同意或主管機關的核可，絕不

任意對外公開〈例如：身分證統一編號為隱密保護的資訊，但當作為憑證內容的用戶身分識別資訊時為可公開資訊〉，其他於註冊或憑證申請時相關作業所使用的

1. 身分驗證的用戶資訊〈例如：用戶名稱、出生年月日、身分驗證識別碼、用戶密碼或密語、帳號、聯絡資訊等〉。
2. 用戶註冊或憑證申請、更新、暫時停用與廢止憑證時交易的相關隱密性訊息。
3. 用戶註冊時填寫於註冊相關申請單、合約上的用戶資訊，與身分證明文件〈或影印本〉上的隱密性資訊，必須嚴謹且隱密的保護。

憑證管理中心使用於憑證系統的任何私密金鑰，皆妥善且隱密的保護，使用時決不以明碼顯現於亂碼化設備之外。

憑證管理中心/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管控，由業務有權存取的作業人員執行。

憑證管理中心/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認證資料，非經由用戶之允許絕不任意對外公開、銷售、租借。

3.8.2 可公開資訊的種類(Type of Information Not considered Confidential)

公告於目錄伺服器或資料庫的用戶憑證資訊，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，為可公開的非隱密性資訊。

3.8.3 憑證廢止與暫時停用資訊的公告(Disclosure of Certificate Revocation/ Suspension Information)

用戶憑證管理中心依據作業規範處理用戶憑證的廢止與暫時停用時，依據「5.4.9 憑證廢止清冊產生頻率」的產生頻率規範，即時產生且完整的公告於憑證資料庫或目錄伺服器之憑證廢止清冊，供用戶存取使用。

3.8.4 權責管理單位的存取(Release to Law Enforcement Officials)

除非符合下列之一的條件，否則用戶的註冊基本資料與身分認證相關資料絕不任意提供予權責管理單位，或其他任何人知悉使用：

1. 政府法律、規範的規定並經由權責主管機關合法的授權。
2. 法院因處理糾紛與仲裁而正式合法的申請需求。

3.8.5 民事訴訟的存取(Release as Part of Civil Discovery)

用戶的註冊基本資料與身分認證資料絕不任意提供，當因使用憑證的交易產生民事訴訟而必須存取用戶的註冊與憑證相關資訊時，必須符合

1. 具有合法司法管轄權的訴訟仲裁機構之正式申請。
2. 用戶以電子簽章方式或親筆簽名的文件證明方式授權。

3.8.6 用戶提出需求的存取(Disclosure upon Owner's Request)

用戶的註冊與憑證相關資訊，除憑證內容可公開資訊外，必須用戶自己以電子簽章方式或親筆簽名的證明文件提出申請，才能提供予第三者，非用戶本人的授權，任何第三者的需求索取，本公司/註冊中心絕不任意提供。

3.8.7 其他資訊公告條件(Other Information Release Circumstances)

除了符合政府法令規章的需求，或用戶自己的授權需求、或合法用途且正式申請外，目前尚無公告用戶資訊的其他公告條件。

3.9 智慧財產權(Intellectual Property Rights)

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。

4.識別與鑑別(Identification and Authentication)

4.1 註冊(Initial Registration)

用戶憑證管理中心與註冊中心於用戶註冊時，除驗證用戶申請時身分證明文件，亦須依據本章下述的作業規範與「2.2.1.1 憑證身分認證安全等級」的作業規範，正確的驗證用戶的身分。

用戶向用戶憑證管理中心與註冊中心申請憑證簽發時，必須依據憑證實務作業基準規範「5.1 憑證申請」處理，即為用戶必須先完成註冊作業程序。

4.1.1 識別名稱之格式(Type of Names)

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：

〈一〉、網際 NB 憑證系統(NBCA)

網際 NB 憑證

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)	憑證簽發機構	O = TAIWAN-CA.COM Inc.
3.OrganizationUnit(OU)	註冊中心識別名稱	OU = Taiwan Bank
4.CommonName(CN)	憑證申請者的識別名稱，例如用戶身分證統一編號	CN = A123456789-00

〈二〉、商務 EC 憑證系統 (EC+)

甲、商務 EC 憑證

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)	憑證機構一般識別名稱	O = TaiCA Secure CA
3.Organization(O)	憑證機構政策分類名稱	O = Certificate Service Provider
4.OrganizationUnit(OU)	註冊中心英文識別名稱	OU = President Securities Corp.
5.OrganizationUnit(OU)	註冊中心分支機構或服務分類	OU = PSCNET
6.CommonName(CN)	憑證申請者的識別名稱，例如用戶身分證統一編號	CN = TWA123456789-00
7.Email(E)	憑證申請者的電子郵件信箱	E= user@sec.com

乙、SSL 伺服器憑證

識別名稱(DN)	說　　明	識 別 名 稱 內 容 範 例
1.Country(C)	憑證申請者所在地國別碼	C = TW
2.State(S)	憑證申請者所在地	S = TAIWAN
3.Locality(L)	憑證申請者所在地	L = TAIPEI
4.Organization (O)	憑證申請者英文識別名稱	O = TAIWAN-CA.COM Inc.
5.OrganizationUnit(OU)	憑證申請者英文識別名稱或服務分類	OU = IT
6.CommonName(CN)	憑證申請者的識別名稱，例如網址(URL)	CN = www.twca.com.tw

〈三〉、商務 XML 憑證系統

甲、通關稅費憑證

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 = Finance
3.OrganizationUnit(OU)	CA(簽發單位)的資訊	OU = TaiCA Finance User CA
4.OrganizationUnit(OU)	註冊中心英文識別名稱	OU = 12345678-RA-FINANCE
5.OrganizationUnit(OU)	註冊中心應用或服務識別名稱	OU = TAX
6.CommonName(CN)	憑證申請者的識別名稱例如企業的營利事業統一編號	CN = 12345678-01-000

乙、商務 XML 憑證

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 = Information
3.OrganizationUnit(OU)	CA(簽發單位)的資訊	OU = TaiCA Information User CA
4.OrganizationUnit(OU)	註冊中心英文識別名稱	OU = 12345678-RA-Trade
5.OrganizationUnit(OU)	註冊中心應用或服務識別名稱	OU = Trade
6.CommonName(CN)	憑證申請者的識別名稱例如企業的營利事業統一編號	CN = 12345678-01-000

丙、S/MIME 憑證

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 公司的資訊	O = TAIWAN-CA Inc.
3.OrganizationUnit(OU)	CA(簽發單位)的資訊	OU = TWCA SMIME User CA
4.OrganizationUnit(OU)	註冊中心英文識別名稱	OU = 12345678-RA-SMIME
5.OrganizationUnit(OU)	註冊中心應用或服務識別名稱	OU = SMIME
6.CommonName(CN)	憑證申請者的識別名稱例如 應用別+編號後四碼+流水號	CN = SMIME5678-00-000001

主體別名擴充欄位中應記載 Email 識別名稱。

4.1.2 名稱意義(Need for Names to be Meaningful)

識別名稱欄位中所存放的用戶識別資訊，皆存放具有意義的資訊〈例如：身分證統一編號、營利事業統一編號、應用系統識別名稱、・・〉，於每一憑證系統下每一用戶的識別名稱皆為可辨別且具有唯一性，決無存放匿名或不可辨識的用戶識別名稱。

4.1.3 各種識別名稱的規範 (Rules for Interpreting Various Name Forms)

各業務系統使用的用戶識別名稱的規範，依照各相關主管機關訂定的規範處理，個人的身分證統一編號識別名稱，為依照內政部訂定的規範處理，企業的營利事業統一編號識別名稱，為依照主管機關訂定的規範處理，其他非本國的用戶識別名稱，則依照各國護照的統一編碼規定或財稅資料中心識別外國人的統一編碼規範，伺服器的網域註冊名稱，台灣為依據台灣網路資訊中心的網域管理規範，跨國則依據國際的網域管理規範處理。

若因業務需求而有其他編碼方式者，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。

4.1.4 名稱的唯一性(Uniqueness of Names)

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。

4.1.5 識別名稱糾紛的處理(Name Claim Dispute Resolution Procedures)

當用戶使用的識別名稱有相同時，用戶憑證管理中心/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/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先前使用者的用戶識別名稱使用權，該使用者必須負擔相關的法律權責；且驗證該用戶註冊識別名稱使用的合法性，非為本公司/註冊中心的業務權責範圍。

4.1.6 註冊商標的認可與驗證(Recognition, verification and role of Trademarks)

用戶憑證管理中心/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/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。

4.1.7 私密金鑰擁有的驗證方法(Method to Prove Possession of Private Key)

用戶憑證管理中心/註冊中心必須驗證用戶私密金鑰擁有的合法性與正確性，至少須以如下所述之任一方法驗證用戶所擁有的私密金鑰：

1. 於用戶申請憑證，以用戶私密金鑰執行用戶憑證申請訊息的簽章時，用戶憑證管理中心/註冊中心必須驗證用戶憑證申請訊息內，經保護的用戶身分資訊、公開金鑰與私密金鑰的正確性與唯一性及合法性，且公開金鑰非為目前使用中的憑證。
2. 用戶除以簽章方式驗證私密金鑰擁有的合法性與正確性外，亦可由用戶憑證管理中心/註冊中心，以用戶的公開金鑰將訊息亂碼加密後，經數位信封的方式傳遞至用戶，用戶驗證無誤後，再將該訊息以私密金鑰簽章後，回覆確認訊息傳回用戶憑證管理中心/註冊中心，且經用戶憑證管理中心/註冊中心驗證無誤。

4.1.8 公司組織身分的鑑別(Authentication of Organization Identity)

公司組織之用戶註冊的身分驗證安全等級為第三級時，本公司與註冊中心處理用戶註冊身分與識別名稱的驗證時，公司必須提供主管機關或合法授權單位核發的相關證明文件〈影本必須加蓋公司章與負責人的簽名〉，或外國公司合法的相關證明文件，如為公司授權代理人辦理，並需授權代理人親自辦理且驗證該授權代理人的相關身分證明文件，其他註冊時的身分驗證安全等級規範詳訂於「2.2.1.1 憑證身分認證安全等級」。

4.1.9 個人用戶身分的鑑別(Authentication of Individual Identity)

個人用戶註冊的身分驗證安全等級為第三級時，個人申請註冊時必須由用戶本人親自辦理並檢具相關身分證明文件〈有相片可識別的身分證、護照等〉經註冊中心查核驗證，絕不允許委由他人辦理；非本國之用戶時，依照相關業務規範的驗證程序辦理〈例如具有相片可識別的護照<passport>〉，其他註冊時的身分驗證安全等級相關規範詳訂於「2.2.1.1 憑證身分認證安全等級」。

4.2 憑證及私密金鑰的更新(Routine Rekey)

當用戶金鑰〈即憑證〉的生命效期訂定為一年，於一年後到期時必須更新，即是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/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〉。

網際 NB 憑證、商務 EC 憑證、商務 XML 憑證的用戶憑證〈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。

SSL 伺服器憑證有效期限最長為四年，惟如有特別需要，可經 PMA 審核通過後，延長其效期。

商務 EC 憑證、商務 XML 憑證的用戶，於憑證有效期限屆滿前，將新產生的公開金鑰憑

證申請訊息以使用中有效的私密金鑰簽章後，傳遞至註冊中心申請新憑證簽發；網際 NB 憑證的用戶，於憑證有效期限屆滿前執行私密金鑰的更新時，必須以臨櫃或郵遞方式向註冊中心申請新憑證簽發或以新產生的公開金鑰憑證申請訊息以使用中有效的私密金鑰簽章後，傳遞至註冊中心申請新憑證簽發。

於憑證有效期限屆滿後用戶執行憑證及私密金鑰的更新時，用戶必須以臨櫃、郵遞或其他能有效確認用戶身份的方式向註冊中心申請憑證更新，待取得註冊中心的憑證更新申請時之身分認證識別資料後，用戶將帶有新私密金鑰簽章的憑證申請訊息與用戶身分認證識別資訊，依註冊中心作業規範至用戶憑證管理中心/註冊中心申請新憑證簽發；註冊中心於收妥用戶憑證申請訊息時，除驗證私密金鑰擁有的合法性外，並驗證用戶憑證申請訊息的合法性與完整性。

4.3 廢止憑證之私密金鑰的更新(Rekey after Revocation)

用戶憑證廢止(revoke)後，不允許繼續向用戶憑證管理中心/註冊中心申請憑證簽發，必須重新執行註冊的身分確認，待取得註冊中心的憑證更新申請時之身分認證識別資料後，重新產生新公開金鑰對，用戶將帶有新私密金鑰簽章的憑證申請訊息與用戶身分認證識別資訊，依註冊中心作業規範至用戶憑證管理中心/註冊中心申請新憑證簽發；註冊中心於收妥用戶憑證申請訊息時，除驗證私密金鑰擁有的合法性外，並驗證用戶憑證申請訊息的合法性與完整性。

4.4 憑證廢止需求(Revocation Request)

廢止作業依「5.4 憑證的廢止」憑證作業系統的廢止規範處理。

5.憑證系統管理 (Operation Requirements)

5.1 憑證申請(Certificates Application)

用戶應依照業務應用系統安全控管措施的需求，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。

1. 註冊中心必須向用戶詳細說明業務應用系統憑證使用，及申請單與合約書上之權利與義務規範，相關業務運作的作業流程與提供使用說明與操作文件，用戶同意並確認。
2. 用戶正確且詳實的填寫相關申請單與提供相關證明文件，註冊中心依身分認證安全等級的作業規範，驗證用戶身分與證明文件無誤後，提供用戶身分識別代碼與保護密碼，完成用戶註冊申請作業。
3. 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，該憑證用於與用戶憑證管理中心間安全收送用戶憑證作業之訊息。

〈一〉、網際 NB 憑證申請 (NBCA)

1. 用戶經向註冊中心完成註冊作業程序，取得註冊中心發給的用戶憑證申請時之身分認證識別資料，完成後產生公開金鑰對及依據作業規範產生憑證申請訊息，用戶憑證申請訊息經用戶私密金鑰簽章完成後遞送至註冊中心申請憑證簽發。
2. 註冊中心於用戶憑證申請之前，將用戶憑證申請時之身分認證識別資料依據作業規範安全且隱密的傳遞至用戶憑證管理中心。
3. 用戶憑證申請訊息遞送至註冊中心申請憑證簽發，註冊中心檢核用戶憑證申請訊息的合法性與完整性，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，並執行訊息完整性的亂碼保護後傳送至用戶憑證管理中心。
4. 用戶憑證管理中心驗證註冊中心傳遞之用戶憑證申請訊息的合法性與完整性，正確無誤後簽發憑證予用戶。

〈二〉、商務 EC 憑證申請 (EC+)

壹、 商務 EC 憑證

1. 用戶經向註冊中心完成註冊作業程序，取得註冊中心發給的用戶憑證申請時之身分認證識別資料，完成後產生公開金鑰對及依據作業規範產生憑證申請訊息，用戶憑證申請訊息經用戶私密金鑰簽章完成後遞送至註冊中心申請憑證簽發。
2. 註冊中心檢核用戶憑證申請訊息的合法性與完整性，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，經伺服器憑證亂碼保護後傳送至用戶憑證管理中心。
3. 用戶憑證管理中心檢核註冊中心所傳送之用戶憑證申請訊息，註冊中心與用戶身分的合法性與訊息的完整性，正確無誤後，簽發用戶憑證並傳送至註冊中心。
4. 註冊中心檢核用戶憑證管理中心傳回之用戶憑證回覆訊息的合法性與完整性，正確無誤後，將用戶憑證傳送予申請人。

貳、SSL 伺服器憑證申請

1. 受理所有保證等級之 SSL 伺服器憑證申請時，皆依照下列程序辦理。
2. 用戶備妥“公司營利事業登記證影本”、“網域名稱使用授權書”、“SSL 伺服器數位憑證憑證申請單”、及服務費用之支票或匯款收據，一併~~郵寄~~遞送至註冊中心辦理憑證申請。
3. 經由網際網路進入 SSL 伺服器憑證申請的網頁，用戶依據 SSL 伺服器憑證申請註冊規範，產生用戶憑證申請檔完成後，依“SSL 伺服器數位憑證憑證申請單”內設定的資訊，填入技術聯絡人、業務聯絡人、帳務聯絡人的資訊，與通行密碼而完成憑證的申請。
4. 若申請者欲申請之伺服器名稱係於臺灣註冊(例如: *.com.tw)，註冊中心必須查詢 TWNIC WHOIS 或其他公開資料庫，檢核其網域名稱所有權確實屬於該申請者；若伺服器名稱非於臺灣註冊，則必須查詢全球網域管理服務組織之資料庫(例如: Network Solutions 或其他組織)，以檢核網域名稱所有權。
5. 作業人員檢核用戶申請文件及憑證申請資訊無誤後，簽發用戶憑證，並以電子郵件通知用戶至本公司網站下載。

〈三〉、商務 XML 憑證申請

1. 受理所有保證等級之商務 XML 憑證申請時，皆依照下列程序辦理。
2. 用戶經過至少為身分識別碼及密碼的檢核驗證完成後，登錄至註冊中心，將產生的憑證申請訊息經由用戶私密金鑰簽章後傳送至註冊中心。
3. 註冊中心驗證用戶身分識別碼及密碼正確無誤後，檢核用戶憑證申請訊息的完整性，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，經伺服器憑證亂碼保護後傳送至用戶憑證管理中心。
4. 註冊中心於驗證 S/MIME 憑證申請者之電子郵件地址時，應先驗證電子郵件地址確實為該申請者所有，確認後，由註冊中心傳遞確認電子郵件至憑證申請者申請註冊之電子郵件地址，要求回覆電子郵件，以確認憑證申請者有申請憑證與註冊之電子郵件地址之有效性。
5. 用戶憑證管理中心檢核註冊中心所傳送之用戶憑證申請訊息，註冊中心與用戶身分的合法性與訊息的完整性，正確無誤後，簽發用戶憑證並傳送至註冊中心。
6. 註冊中心檢核用戶憑證管理中心傳回之用戶憑證回覆訊息的合法性與完整性，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全管控措施的考量，可將憑證申請與私密金鑰產生的介面軟體，以可信賴且具安全管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。

5.1.1 憑證申請政策(Certificate Application Policy)

- 新憑證申請：用戶辦理註冊完成後，才可以向註冊中心申請新憑證的簽發。
- 憑證展期：參閱下節「5.1.2 憑證展期政策」說明。
- 憑證更新：用戶憑證的使用有效期限將屆滿前，可用舊憑證進行更新，若已過期時，用戶必須以臨櫃、郵遞或其他能有效確認用戶身分的方式向註冊中心申請憑證更新。
- 用戶憑證暫時停用(Suspension)後，不允許繼續向用戶憑證管理中心申請憑證簽發。

- 用戶憑證廢止後：必須填寫憑證申請單，重新執行用戶身分認證，向註冊中心申請新憑證簽發。
- 用戶註銷完成後：用戶註銷即為終止與註冊中心合約的權責關係，必須向註冊中心重新辦理註冊，才可以向註冊中心申請憑證的簽發。

5.1.2 憑證展期政策(Certificate renewal(Extend) Policy)

商務 EC 憑證、商務 XML 憑證不提供憑證展期的作業機制，網際 NB 憑證最多只能展期一次。

用戶於憑證有效期結束時，使用舊有的用戶註冊資料及公開金鑰向註冊中心/用戶憑證管理中心申請新憑證的簽發，是為憑證展期，即為用戶的憑證識別資料及公開金鑰不變，但憑證有效期限延長及憑證序號不同。

用戶憑證已過期，或無有效憑證時，絕不可執行憑證的展期。

5.1.3 憑證暫時停用政策(Certificate Suspension Policy)

網際 NB 憑證、商務 EC 憑證不提供用戶憑證暫時停用的作業機制。

用戶於憑證有效期間欲暫時停止憑證的使用，或與憑證相關的私密金鑰有被竊取、盜用之安全上的疑慮時，用戶必須依業務系統與註冊中心的作業規範，即刻向註冊中心申請暫時停用憑證。

用戶執行憑證暫時停用完成後，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；如於該張憑證有效期間終止前，用戶向註冊中心申請解禁完成時，則此張憑證自憑證廢止清冊中移除而成為有效憑證，直到憑證的有效期限結束而成為無效憑證。

用戶憑證已過期或無有效憑證時，絕不可執行憑證的暫時停用與解禁。

5.2 憑證的簽發(Certificates Issuance)

憑證的簽發作業規範詳述於「5.1 憑證申請」的作業程序。

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，並即刻更新資料庫或目錄伺服器的憑證資訊供用戶查詢使用。

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；惟此交易失敗的原因，用戶憑證管理中心有權無需通知用戶，但符合本作業基準、憑證政策、或主管機關相關法律的規範則不在此限。

註冊中心與用戶只可以執行訊息的簽章與加密，不可以簽發任何種類的憑證。

5.3 憑證的啟用與使用(Certificates Acceptance and Using)

5.3.1 憑證的啟用(Certificates Acceptance)

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：

- 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。
- 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。
- 用戶必須驗證該憑證之憑證鏈，檢驗其每張憑證的有效性及合法性，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。

- 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。
- 用戶於接受所申請的憑證後，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。

5.3.2 憑證的使用(Certificates Using)

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：

- 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。
- 除必須驗證該憑證之憑證鏈，檢驗其每張憑證及該憑證的有效性及合法性外〈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〉，且需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。
- 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，必須檢核該憑證的有效性與完整性。
- 用戶使用憑證執行交易訊息的簽章與加密時，必須確實了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，且合法使用於憑證策略、本作業基準與相關業務規範所訂定的範圍。

5.4 憑證的暫時停用與廢止(Certificate Suspension and Revocation)

5.4.1 憑證廢止時機(Circumstances for Revocation)

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，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. 本公司得逕行廢止用戶憑證：
   - 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〈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，因業務之需求依照正式合法作業程序申請。

5.4.2 有權申請廢止憑證者(Who can Request Revocation)

與用戶有關的註冊中心或本公司、主管機關或合法授權的第三者及用戶皆有權申請

憑證的廢止。

1. 用戶執行：
   - 用戶可依照其需求，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，必須依照「5.4.1 憑證廢止時機」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。
   - 法院因訴訟與仲裁經註冊中心的申請，但必須符合本公司的相關作業規範。
   - 主管機關，符合相關法令與規範的申請。

5.4.3 憑證廢止程序(Procedure for Revocation Request)

〈一〉、網際 NB 憑證廢止 (NBCA)

1. 用戶依據註冊中心/本公司的作業規範填寫憑證廢止申請單，或是經由註冊中心的身分驗證後，將以用戶私密金鑰簽章保護的憑證廢止申請訊息，傳遞至註冊中心申請廢止用戶憑證。
2. 用戶憑證廢止訊息遞送至註冊中心申請憑證廢止時，註冊中心檢核用戶憑證廢止訊息的合法性與完整性，正確無誤後，將用戶憑證廢止訊息以註冊中心的私密金鑰簽章，並執行訊息完整性的亂碼保護後傳送至用戶憑證管理中心申請憑證廢止。
3. 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，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，及即刻更新憑證廢止清冊。
4. 註冊中心收妥用戶憑證管理中心的用戶廢止憑證回復訊息時，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。

依據註冊中心的憑證廢止作業規範，當允許用戶直接向用戶憑證管理中心申請憑證廢止時：

1. 用戶憑證廢止訊息經用戶簽章完成後遞送至用戶憑證管理中心申請憑證廢止。
2. 用戶憑證管理中心收妥用戶憑證廢止申請訊息時，檢核申請訊息的合法性與完整性，正確無誤後，執行用戶憑證廢止作業，並將廢止憑證回覆訊息通知用戶，及即刻更新憑證廢止清冊。

〈二〉、商務 EC 憑證廢止 (EC+)

壹、 商務 EC 憑證

1. 依據註冊中心/本公司的安控措施〈身分識別碼、保護密碼、・・〉登錄註冊管理系統，經註冊中心檢核用戶身分驗證無誤後，或填寫憑證廢止申請單，經由註冊中心的身分驗證無誤後，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。

貳、 SSL 伺服器憑證廢止

1. 郵寄申請：

用戶填寫“SSL 伺服器數位憑證用戶註銷憑證申請單”蓋章簽名確認後，經由郵寄至本公司申請憑證廢止，本公司檢核用戶身分無誤後，由作業人員執行憑證廢止作業。

2. 經由網際網路申請：

用戶登錄本公司 SSL 伺服器憑證系統的網頁，經本公司檢核用戶身分無誤後，用戶點選憑證註銷，經本公司憑證系統立即執行憑證廢止作業，且用戶必須郵寄蓋章簽名確認後的“SSL 伺服器數位憑證用戶註銷憑證申請單”至本公司存查。

〈三〉、商務 XML 憑證廢止

1. 依據註冊中心/用戶憑證管理中心的安控措施〈身分識別碼、保護密碼、・・〉登錄註冊管理系統，經註冊中心檢核用戶身分驗證無誤後，或填寫憑證廢止申請單，經由註冊中心的身分驗證無誤後，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、法院與訴訟仲裁單位及其他有權責者，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。

5.4.4 憑證請求廢止的寬限期(Revocation Request Grace Period)

用戶有廢止憑證的需求時，必須立刻向註冊中心〈用戶憑證管理中心〉申請憑證的廢止。

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，於營運或上班時間必需立刻處理，且至少於二十四小時內完成。

商務 EC 憑證、與商務 XML 憑證，依據用戶憑證管理中心憑證系統的作業規範，至少於二十四小時內產生憑證廢止清冊，故憑證請求廢止的寬限期間為二十四小時。

網際 NB 憑證於用戶申請廢止憑證時，立刻執行憑證廢止作業並且產生憑證廢止清冊，故無憑證請求廢止的寬限期限。

5.4.5 暫時停用時機(Circumstances for Suspension)

用戶憑證暫時停用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時停用：

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，用戶欲暫時停用該憑證的使用。
   - 用戶欲暫時停止使用該憑證一段時間。
2. 註冊中心/本公司：
   - 用戶使用憑證而為註冊中心/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，因業務之需求依照正式合法作業程序申請。

5.4.6 有權暫時停用者(Who can Request Suspension)

與用戶有關的註冊中心或本公司、主管機關或合法授權的第三者及用戶皆有權執行憑證的暫時停用。

1. 用戶執行：
   - 用戶可依照其需求，依註冊中心作業規範申請暫時停用用戶憑證。
2. 註冊中心〈本公司〉：
   - 註冊中心〈本公司〉申請暫時停用用戶憑證時，必須依照「5.4.5 憑證暫時停用時機」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，申請暫時停用用戶憑證。
   - 法院因訴訟與仲裁經註冊中心的申請，但必須符合本公司的相關作業規範。
   - 主管機關，符合相關法令與規範的申請。

5.4.7 暫時停用程序(Procedure for Suspension Request)

網際 NB 憑證、商務 EC 憑證之用戶憑證管理中心無憑證暫時停用的作業機制。

1. 依據註冊中心/用戶憑證管理中心的安控措施〈身分識別碼、保護密碼、・・〉登錄註冊管理系統，經註冊中心檢核用戶身分驗證無誤後，或填寫憑證暫時停用申請單，經由註冊中心的身分驗證無誤後，執行憑證暫時停用，註冊中心將用戶憑證暫時停用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時停用。
2. 用戶憑證管理中心收妥註冊中心的用戶憑證暫時停用申請訊息時，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，依據憑證暫時停用作業規範執行用戶憑證暫時停用作業，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時停用憑證回覆訊息時，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時停用用戶的憑證要求後，至用戶憑證管理中心於二十四小時內實際公布暫時停用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，暫時停用憑證的使用，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，則信賴憑證者必須負損害賠償責任；於提出暫時停用用戶的憑證之期間內，如用戶未依據業務系統的規範暫時停用該憑證的使用，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。

暫時停用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，使憑證成為有效且可以使用。

5.4.8 暫時停用時效(Limits on Suspension Period)

網際 NB 憑證與商務 EC 憑證之用戶憑證管理中心不提供用戶憑證暫時停用的作業機制，故無暫時停用時效。

用戶執行憑證暫時停用完成後，於憑證有效期間終止前，如未執行憑證的解禁，則此張憑證皆存在廢止憑證清冊中，為無法使用的憑證。

商務 XML 憑證暫時停用時效為，當用戶憑證經完成暫時停用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，是為憑證的暫時停用時效，此段期間如至超過憑證有效期限仍未執行憑證解禁時，則此張憑證即為過期憑證〈與廢止憑證同為無法使用的憑證〉。

憑證暫時停用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。

5.4.9 憑證廢止清冊產生頻率(CRL Issuance Frequency)

企業 EC 憑證與商務 XML 憑證用戶憑證管理中心，依據憑證系統的作業規範，至少於二十四小時內產生憑證廢止清冊，故憑證廢止清冊的產生頻率為二十四小時。

網際 NB 用戶憑證管理中心於用戶申請廢止憑證時，立刻執行憑證廢止作業並且產生憑證廢止清冊。

5.4.10 憑證廢止清冊查核(CRL Checking Requirements)

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，因只有在有用戶申請憑證廢止時，用戶憑證管理中心才會依憑證廢止清冊產生的頻率產生憑證廢止清冊，商務 EC 憑證與商務 XML 憑證的憑證廢止清冊產生頻率為每二十四小時執行一次，網際 NB 憑證於用戶申請廢止憑證時，立刻執行憑證廢止作業並且產生憑證廢止清冊，故考量業務風險因素，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。

用戶或信賴憑證者之業務應用系統的安全機制如使用線上憑證狀態協定(OCSP)查核的功能時，則可不必使用憑證廢止清冊檢核的安全機制。

5.4.11 線上憑證與廢止憑證狀態查核功能(On-line Revocation/Status Checking Availability)

網際 NB 憑證、商務 EC 憑證不提供線上憑證與廢止憑證狀態查核的功能，故用戶必須使用憑證廢止清冊查核功能。

商務 XML 憑證的安全機制，提供線上憑證與廢止憑證狀態查核的功能，如果用戶選用此種安全機制則可以不使用憑證廢止清冊查核功能。

5.4.12 線上廢止憑證查核需求(On-line Revocation Checking Requirement)

如「5.4.10 憑證廢止清冊查核」與「 5.4.11 線上憑證與廢止憑證狀態查核功能」的說明。

5.4.13 其他格式廢止憑證通知的功能(Other Forms of Revocation Advertisements Available)

本公司之憑證系統，提供憑證狀態查詢的功能，除了 X.509 V2 CRL 格式的憑證廢止清冊外，目前不提供其他格式的廢止憑證通知功能。

5.4.14 其他格式廢止憑證通知的查核需求(Checking Requirements for Other Forms of Revocation Advertisements)

本公司目前不提供其他格式的廢止憑證通知功能，故無其他格式廢止憑證的查核規範。

5.4.15 金鑰更新有安全顧慮的特別需求(Special Requirements ReKey Compromise)

金鑰更新有安全顧慮時的作業規範，皆依照 「5.7 金鑰變更」的規範處理，無特別需求的規定。

5.5 安全稽核(Security Audit Procedures)

由實體設備的操作到憑證系統的執行，本公司與註冊中心皆須確實留存相關作業文件及交易與操作稽核紀錄，做為執行稽核憑證系統安全控管的資訊依據，並且依本公司與註冊中心的稽核作業規範，確實執行憑證系統運作的稽核作業。

5.5.1 稽核紀錄種類(Types of Events Recorded)

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(RSA key)與基碼(3DES key)或其他基碼，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，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。

5.5.2 稽核紀錄查詢頻率(Frequency of Processing Log)

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，經三個月後，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，需由本公司與註冊中心相關的系統與文件紀錄依稽核作業規範詳細查核，且紀錄事件的查核、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，並紀錄事件的查核、處理過程，及追蹤改善措施的執行。

5.5.3 稽核紀錄的保存期限(Retention Period for Audit Log)

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。

5.5.4 稽核紀錄的保護(Protection of Audit Log)

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全控管措施保護稽核紀錄，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管控的異地備援中心。

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管控系統所保護，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。

5.5.5 稽核紀錄備援程序(Audit log backup procedures)

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，稽核紀錄資訊檔備份的媒體，並運送一份至具安全管控措施的異地備援中心儲存備援。

5.5.6 稽核紀錄蒐集系統(Audit Collection System)

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紀錄之，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

5.5.7 異常狀況的通知(Notification to Event-Causing Subject)

作業人員於執行憑證系統，出現影響安全控管措施的異常事件時，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。

5.5.8 脆弱性評鑑(Vulnerability Assessments)

對於執行憑證系統運作時，內部與外部可能造成的威脅與風險的評估，經由稽核紀錄的查核及監控追蹤，隨時調整與修改憑證系統運作的安全控管措施，以便將系統運作的風險降至最低，且每年至少應執行一次。

5.6 紀錄保存(Records Archival)

5.6.1 保存紀錄的種類(Types of Event Records)

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、與用戶的相關合約條款、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。

5.6.2 保存期限(Retention Period for Archive)

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。
- 用戶憑證申請、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、查詢與憑證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。
- Root CA 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。

5.6.3 保存資料的保護(Protection of Archive)

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，皆儲存於具安全管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全管控措施、防潮濕的中央空調環境下之異地備援中心。

本公司/註冊中心所保存及保護的用戶基本資料與身分認證資料，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。

5.6.4 保存資料的備援程序(Archive Backup Procedures)

金鑰、憑證、交易資料等相關資料，依照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全管控措施的環境下，且一份保存資料儲存於具安全管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。

5.6.5 紀錄的時戳需求(Requirements for Time-Stamping of Records)

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，時序(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、憑證申請與更新、憑證廢止、憑證暫時停用與查詢等有關的作業時，交易的訊息內容具有時序的註記，是經由電腦作業系統或憑證系統自動產生，時序(time-stamp)由電腦的時鐘讀取而自動加入紀錄資訊內。

5.6.6 保存紀錄蒐集系統(Archive Collection System)

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。

5.6.7 驗證保存紀錄程序(Procedure to Obtain and Verify Archive Information)

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。

5.7 金鑰變更(Key Changeover)

5.7.1 用戶金鑰變更(Key Changeover of User)

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時，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/註冊中心申請新憑證的簽發；或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/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。

5.7.2 用戶憑證管理中心金鑰變更((Key Changeover of UCA<or sub-CA>)

〈一〉、網際 NB 憑證系統

1. 用戶憑證管理中心金鑰生命週期有效期限結束時，可以產生新金鑰對向政策憑證中心申請新憑證的簽發，完成後以新私密金鑰簽發用戶新憑證的申請，並以新私密金鑰重新簽發用戶憑證管理中心的憑證廢止清冊，並即刻以最迅速的方式通知用戶與註冊中心。
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，於用戶憑證管理中心之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。

〈二〉、商務 EC 憑證系統、商務 XML 憑證系統

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，於用戶憑證管理中心之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。

5.7.3 政策憑證管理中心金鑰變更(Key Changeover of PCA)

〈一〉、網際 NB 憑證系統

1. 網際 NB 政策憑證管理中心兼具根憑證功能。
2. 政策憑證管理中心金鑰使用有效期限結束時，可以依憑證鏈產生下下一組新金鑰對及下下一張的政策憑證中心自簽憑證；以下一組新私密金鑰簽發用戶憑證管理中心新憑證與廢止憑證的簽發申請，以下一張新私密金鑰重新簽發政策憑證管理中心的用戶憑證管理中心之憑證廢止清冊，並即刻通知用戶憑證管理中心。
3. 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下下一組新金鑰對及下下一張的自簽憑證，再以下一張的私密金鑰，簽發用戶憑證管理中心的憑證與廢止憑證申請，且以最迅速的方式通知用戶憑證管理中心，於政策憑證管理中心舊私密金鑰所簽發的憑證與憑證廢止清冊皆為無效，且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。

〈二〉、商務 XML 憑證系統

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 Root CA 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皆為無效，必須重新產生新金鑰對向政策憑證管理中心申請用戶憑證管理中心新憑證的簽發。

5.7.4 最高層憑證管理中心金鑰變更(Key Changeover of RCA)

商務 XML 憑證系統

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。

5.8 危害及災害復原(Compromise and Disaster Recovery)

TWCA 為使憑證系統，於異常狀況或天災與地變時，能於最短的時間內重新建置與開啟憑證系統繼續營運，目前除了有一套完整的網路及軟、硬體備援系統、憑證系統異常狀況時的回復計劃外，尚規劃系統於發生災變異常狀況時，異地憑證系統之復原與開啟繼續營運的功能。

5.8.1 電腦資源、軟體與資料的毀損(Computing Resources, Software, and/or Data are Corrupted)

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，依照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，依照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。

5.8.2 用戶公開金鑰的廢止(Entity Public Key is Revoked)

用戶公開金鑰的廢止相關作業，依照本作業基準「5.4 憑證的暫時停用與廢止」作業規範辦理。

5.8.3 用戶私密金鑰的危害(Entity Private Key is Compromised)

用戶私密金鑰有毀損、遺失、曝露、被篡改，或有為第三者竊用之慮時，用戶必須立刻向註冊中心辦理申告與廢止，並向私密金鑰相關之憑證使用的業務應用系統，申請註銷該私密金鑰〈憑證〉的使用，其他處理的作業規範，依照本作業基準「5.4 憑證的暫時停用與廢止」作業規範辦理。

5.8.4 安全設施的毀損(Secure Facility after a Natural or Other Type Disaster)

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：

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，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。

5.8.5 災害復原計劃(Contingency and Disaster Recovery Plan)

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二十四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。

5.9 CA 結束營運(CA Termination)

本公司因故結束任一系統營運時，需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：

- 於終止服務之日三十日前通報主管機關。
- 於終止服務之日三十日前，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。
- 於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.實體、作業流程及人員安全控管(Physical、Procedural and Personnel Security Control)

6.1 實體控管(Physical Control)

憑證系統建置於安全穩固的建築物及獨立的硬軟體作業環境，只有被授權的作業人員，才可以依照安全控管的作業規範進入執行憑證管理相關作業，亂碼化設備亦存放於有安全控管措施的環境下，避免被破壞或未經過授權的使用。

6.1.1 建築物與位置(Site Location and Construction)

憑證管理中心為獨立機房，具備防震、防水、防火溫控系統、獨立電力、獨立不斷電系統、門禁保全系統、防入侵門禁監視與防破壞警報系統，詳述如下：

6.1.2 實際進出管制(Physical Access)

作業人員進入憑證中心機房必須有三道 IC 卡及指紋識別門禁的身分查核識別管制，且必須兩人以上才可進入(單獨一人員無法開啟進出)，並有二十四小時 CCTV 位移監控錄影設備、及紅外線防入侵警報系統。

憑證管理中心運作的相關私密金鑰、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亂碼化設備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。

6.1.3 電力與空調(Power and Air-Condition)

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。

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。

6.1.4 防水處理(Water Exposures)

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。

6.1.5 防火處理(Fire Prevention and Protection)

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 FM200 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。

6.1.6 媒體儲存(Media Storage)

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全管控措施的異

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。

6.1.7 廢棄處理(Waste disposal)

憑證管理中心於憑證系統所使用的硬體設備、磁碟機與亂碼化設備等，於廢棄不使用時，商業敏感性及隱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隱密性資訊時，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。

6.1.8 異地備份(Off-Site Backup)

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，與人員進出存取需經過合法授權之高度安全管控的異地備援環境。

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管控的異地，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。

6.2 作業程序控管(Procedure Control)

6.2.1 可信賴角色(Trusted Role)

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、註冊中心扮演的可信賴且具公信力的機構，公正與嚴謹的執行。

本公司及註冊中心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，依照本公司內部憑證作業規範及作業手冊，註冊中心的內部作業規範及作業手冊確實執行業務。

本公司與註冊中心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。

6.2.1.1 憑證管理中心(CA)

- 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「5.5 安全稽核」。
- 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，亂碼化系統作業人員，系統資源控管人員負責其授權

的相關作業。

6.2.1.2 註冊中心(RA)

- 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，如需執行雙重驗證時，則需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，亂碼化系統作業人員，監督人員，稽核人員各自負責其所授權的相關作業。

6.2.2 作業人員需求人數(Number of Persons Required per Role)

本公司及註冊中心執行各種業務的作業人員，其權責為獨立且不重疊，依照監督人員、管理人員、作業人員、稽核人員與硬軟體系統的維護人員，亂碼化系統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照金鑰作業安全控管程序的規定，至少需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。

6.2.3 角色的識別與鑑別(Identification and Authentication for Each Role)

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，而且是唯一的身分識別碼，與 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，且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。

6.3 人員控管(Personnel Control)

6.3.1 適任條件與經歷(Background, Qualifications ,Experience ,and clearance requirements))

本公司及註冊中心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。

6.3.2 審核(Background Check Procedures)

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。

6.3.3 教育訓練(Training Requirements)

憑證系統運作的人員，皆依照其職務，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，亦需給予適當的教育訓練。

本公司需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。

6.3.4 再教育的頻率與需求(Retraining Frequency and Requirement)

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，或新系統的加入，或相關知識與技術的進步與更新，皆需對系統運作的相關人員執行教育訓練。

6.3.5 職務的輪調(Job Rotation Frequency and Sequence)

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，但調派前必需施以適當知識與技能的教育訓練。

6.3.6 非授權作業的懲罰(Sanctions for Unauthorized Actions)

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，依照相關作業之規範處理。

6.3.7 委外人員需求(Contracting Personnel Requirements)

因人力資源不足而委由外包人員擔任操作人員時，除必須依照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，必需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。

6.3.8 作業文件需求(Document Supplied to Personnel)

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、亂碼化系統的操作文件。
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。

7.技術安全控管(Technical Security Control)

7.1 金鑰對的產生與建置(Key Pair Generation and Installation)

7.1.1 金鑰對的產生(Key Pair Generation)

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)至硬體亂碼化設備，由硬體亂碼化設備直接產生，任何人決無法單獨一人執行金鑰對的產生作業，且私密金鑰於硬體亂碼化設備內產生後，直接經亂碼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，須經由亂碼化設備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亂碼化設備外。

7.1.2 私密金鑰的遞送(Private Key Delivery to Entity)

本公司不提供代替用戶產生金鑰對的功能，故無私密金鑰遞送上安全控管措施的需求。

7.1.3 公開金鑰遞送至憑證簽發者(Public Key Delivery to Certificate Issuer)

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。

7.1.4 憑證管理中心公開金鑰的遞送(CA Public Key Delivery to Users)

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

7.1.5 金鑰長度(Key Sizes)

憑證管理中心簽章與加密的RSA 金鑰長度(Key Sizes)，最高層憑證管理中心(RCA)的金鑰長度為 2048 位元（含）以上，政策憑證管理中心(PCA)的金鑰長度為 1024 位元（含）以上，用戶憑證管理中心(UCA)為 1024 位元（含）以上，及用戶的金鑰長度為 1024 位元（含）以上，爾後將視業務系統安全度的需求、與密碼學分析技術及電腦硬體技術的進步而調整金鑰長度。

7.1.6 公開金鑰參數的產生(Public Key Parameters Generation)

本公司 RSA 公開金鑰參數的產生與選取：

商務 EC 憑證系統、商務 XML 憑證系統，由通過 CNS15135、ISO19790 或 FIPS 140-2 規範的亂數產生器產生最佳的金鑰參數。

7.1.7 參數品質的檢核(Parameter Quality Checking)

本公司 RSA 公開金鑰參數的品質的檢核：

商務 EC 憑證系統、商務 XML 憑證系統，由通過 CNS15135、ISO19790 或 FIPS 140-2 規範的硬體亂碼化設備檢核。

7.1.8 金鑰的產生設備(Hardware/Software Key Generation)

商務 EC 憑證系統、商務 XML 憑證系統，使用通過 CNS15135、ISO19790 或 FIPS 140-2 規範的硬體亂碼化設備。

7.1.9 金鑰的使用(Key Usage Purposes)

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，用戶必須依照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。

7.2 私密金鑰的保護(Private Key Protection)

7.2.1 亂碼化模組的標準(Standards for Cryptographic Module)

商務 EC 憑證系統、商務 XML 憑證系統，使用通過 *FIPS 140-1 Level 3* 規範的硬體亂碼化設備。

7.2.2 私密金鑰的分持控管(Private Key (n out of m) Multi-Person Control)

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，且私密金鑰的相關資訊〈例如：IC card〉與保護密碼(PIN)，分別由職務獨立的不同管理人員管控，並儲存於具安全管控措施的環境。

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全管控措施的媒體；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亂碼化設備之主基碼進行亂碼後，備份保存於具安全管控措施的媒體，且需留存稽核紀錄。

7.2.3 私密金鑰的託管、回復及保存(Private Key Escrow)

網際 NB 憑證系統、商務 EC 憑證系統、商務 XML 憑證系統不提供私密金鑰的託管、回復及保存服務。

7.2.4 私密金鑰的備份(Private Key Backup)

憑證管理中心私密金鑰儲存於加密後的硬體亂碼化設備內，備份時至少由二位以上授權人員，將加密亂碼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 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管控的異地備援環境。

7.2.5 私密金鑰的保存(Private Key Archival)

憑證管理中心的私密金鑰經加密亂碼後，或以部分基碼(key component)方式儲存於具安控措施的保護 IC 卡內，或經加密亂碼後儲存於介面媒體，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全

管控措施相同，相關的私密金鑰保存作業與 「5.6 紀錄保存」的保存作業相同。

7.2.6 私密金鑰的建置(Private Key Entry into Cryptographic Module)

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由硬體亂碼化設備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，且私密金鑰經亂碼保護後儲存在設備內，私密金鑰無法以明碼方式輸出至亂碼化設備外。

當有使用該私密金鑰執行運算的需求時，須經由亂碼化設備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亂碼化設備外。

7.2.7 私密金鑰的開啟(Method of Activating Private Key))

憑證管理中心儲存於亂碼化設備內的私密金鑰，必須由授權的 2 位以上的金鑰管理人員開啟〈例如：身分(IC card) 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。

7.2.8 私密金鑰的關閉(Method of Deactivating Private Key)

儲存於亂碼化設備內的私密金鑰由二位以上授權金鑰管理人員簽入(log-in)系統執行〈例如：身分(IC card) 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。

亂碼化設備或私密金鑰關閉不使用時，皆需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。

7.2.9 私密金鑰的清除(Method of Destroying Private Key)

私密金鑰不使用，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，硬體亂碼化設備或 IC 卡必須以零值化(Zeroization)的覆蓋方式清除。

硬體亂碼化設備於廢棄不使用時，亦以上述方式清除全部私密金鑰。

7.3 金鑰對管理的其他事項(Other Aspects of Key Pair Management)

7.3.1 公開金鑰的保存(Public Key Archival)

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。

7.3.2 公開金鑰與私密金鑰的有效期限(Usage Periods for Public Keys and Private Key)

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。

網際 NB 憑證、商務 EC 憑證、商務 XML 憑證之用戶公開金鑰與私密金鑰的有效期限最長為三年。

SSL 伺服器憑證之公開金鑰與私密金鑰有效期限最長為四年，惟如有特別需要，可經 PMA 審核通過後，延長其效期。

7.4 啟動資訊(Activation Data)

7.4.1 啟動資訊產生及建置(Activation Data Generation and Installation)

用戶私密金鑰啟動資訊〈例如：IC card 密碼(PIN:personal identification number), 通行密語(pass-phrase)〉於安全控管的環境下，直接由硬體亂碼化設備內產生，且是隨機產生的一組亂數〈密碼建議至少六位，通行密語建議至少八位以上〉，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。

7.4.2 啟動資訊的保護(Activation Data Protection)

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。

7.4.3 啟動資訊的其他考量(Other Aspects of Activation Data)

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，使用於非隱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，一年後必需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，建議其生命週期為六個月，六個月後必需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，建議其生命週期為 一個月，一個月或至少三個月後必需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 card 的啟動資訊，為考量安全因素，建議用戶依照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〉。

7.5 電腦安全控管(Computer Security Controls)

7.5.1 電腦安全技術需求(Specific Computer Security Technical Requirements)

憑證系統於具備安控措施的保護作業系統環境下執行，具有用戶身分的識別及驗證，系統資源存取權限的區分與控管，及安控事件的稽核與紀錄，資料庫具備安控措施的保護。

交易訊息的傳遞具有嚴謹的隱密性、完整性與不可否認性的安全管控措施，備份與保存的資料具有嚴謹的保護措施，人員與內部作業程序的管理具有嚴謹的權責區分與作

業控管，及建置完善的業務永續經營回復機制，並使用通過電腦作業系統安全等級認證的平台，與使用通過安全等級認證的憑證系統，憑證系統運作之資訊安全管理系統環境，依據 ISO 27001:2005 資訊安全管理系統標準的規範施行及運作，且符合主管機關的憑證機構安全管理規範標準。

7.5.2 電腦系統安全等級(Computer Security Rating)

執行認證作業使用的相關軟體系統，重要的憑證系統，其電腦軟體系統安全等級至少須符合 ISO/IEC 15408 CC 的安全標準，或類似此規範的標準。

商務 EC 憑證系統、商務 XML 憑證系統之憑證系統，使用通過 ITSEC E3 安全認證標準的憑證系統。

7.6 生命週期技術控管(Life Cycle Technical Controls)

7.6.1 系統開發控管(System Development Controls)

使用憑證系統的軟體開發作業控管規範，依據 ISO 15408 共通標準(Common Criteria)等級的規範執行，或類似此 ISO 共通標準等級的軟體開發控管規範，執行相關系統規劃與開發的作業控管。

7.6.2 安全管理控管(Security Management Controls)

執行憑證系統的資訊安全管理系統環境，為遵循 WebTrust program for CA(AICPA/CICA)的標準規範運作。

憑證系統的使用具有嚴謹的管控措施，系統取得皆經嚴謹的測試驗證後才安裝使用，修改或更新皆有版本的管控、功能測試與記錄，且不定期查核、測試驗證系統的完整性。

硬軟體設備由採購至接收時須有安全的保護措施，具有相關的可查核安全機制〈例如：封條、密碼、簽章等安控措施〉，用來識別設備的未被侵入與異動之完整性，亂碼化設備尤須於安全管控的作業機制下，執行設備的驗證、系統安裝與接收。

硬軟體設備更新提昇後，舊設備捨棄時，必須確認無安全的考量資訊存在。

7.6.3 生命週期的安全等級(Life Cycle Security Ratings)

生命週期的安全控管等級作業規範，目前暫無訂定。

7.7 網路安全控管(Network Security Control)

最高層憑證管理中心、政策憑證管理中心憑證系統為離線(Off-Line) 、獨立的作業管理系統，且需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。

用戶憑證管理中心經由防火牆與網路資源安全控管系統的保護，只開放 CA 系統相關的作業功能，供用戶經由網際網路(Internet)至用戶憑證管理中心執行憑證相關的作業功能，其他非用戶憑證管理中心提供的功能或通訊介面，用戶皆無法執行，為提昇網路防入侵與防破壞的安全功能，而安裝及建置防入侵偵測與防病毒管理系統，以增進網路管理系統的安全控管措施，且隨時提昇更新網路防火牆、防入侵偵測、防病毒與網路資源安全控管系統的版本，以期能將網路系統的威脅風險減至最低。

7.8 亂碼化模組工程控管(Cryptographic Module Engineering Controls)

商務 EC 憑證系統、商務 XML 憑證系統，使用通過 *FIPS 140-1 Level 3* 規範的硬體亂碼化設備。

8.憑證與憑證廢止清冊格式剖繪(Certificate and Certificate Revocation List(CRL) Profiles)

8.1 憑證格式剖繪(Certificates Profile)

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。

8.1.1 版本(Version Number(s))

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。

8.1.2 憑證擴充欄位(Certificate Extension)

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作業規範。

8.1.3 演算法物件識別碼(Algorithm Object Identifiers)

憑證管理中心依照 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：

演算法安全機制	演算法(Algorithm)	物件識別碼(OID)
亂碼	RSAEncryption	1.2.840.113549.1.1.1
亂碼〈簽章〉	sha-1WithRSAEncryption	1.2.840.113549.1.1.5
亂碼	desCBC	1.3.14.3.2.7
亂碼	3desEDE-CBC	1.2.840.113549.3.7
雜湊函數	MD5	1.2.840.113549.2.5
雜湊函數	SHA-1	1.3.14.3.2.26

8.1.4 識別名稱格式(Name Forms)

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。

8.1.5 識別名稱限制(Name Constraint)

憑證系統所簽發用戶憑證，其識別名稱不允許為匿名、或假名之識別名稱，皆存放具有可唯一識別的有意義之用戶識別名稱。

8.1.6 憑證政策物件識別碼(Certificate Policy Object Identifiers)

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。

8.1.7 憑證政策限制擴充欄位的使用(Usage of Policy Constraints Extension)

憑證有使用憑證政策限制擴充欄位時，其作業規範訂定於憑證相關的憑證格式剖繪作業規範；商務 XML 憑證的憑證政策擴充欄位，除存放通知使用者取得憑證政策資訊的網址等資訊外，且存放憑證政策(CP)的簡要聲明，為憑證使用時的適用範圍限制。

8.1.8 憑證政策限制語法與語意(Policy Qualifiers Syntax and Semantics)

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；商務 XML 憑證的憑證政策擴充欄位存放憑證政策(CP)的簡要聲明，為憑證使用時的適用範圍限制的代碼，其限制語法與語意為：第一段為身分認證安全等級，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「2.2 憑證的適用性」。

8.1.9 憑證政策擴充欄位必要的處理(Processing Semantics for the Critical Policy Extension)

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；商務 XML 憑證的憑證政策擴充欄位存放憑證政策(CP)的簡要聲明，為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。

8.2 憑證廢止清冊格式剖繪(CRL Profile)

8.2.1 版本(Version number(s))

憑證政策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。

8.2.2 憑證廢止清冊與憑證廢止清冊擴充欄位(CRL and CRL Entry Extensions)

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，其作業規範訂定於憑證相關的憑證格式剖繪作業規範。

9.規範管理(Specification Administration)

9.1 規範變更程序(Specification Change Procedure)

本作業基準規範的權責管理單位為 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。

當本作業基準有訂定相關的物件識別碼(OID)，而憑證實務作業基準內容有更新版本時，相對應的物件識別代碼不跟隨異動，只變更版本的序號識別代碼。

本作業規範有建議更新時，必須將詳細的相關文件郵寄或 E-mail 至「2.5 聯絡窗口」，經 TWCA 政策管理中心的審查。

9.2 公告與通知政策(Publication and Notification Policies)

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： http:// www.twca.com.tw〉下載。

9.3 憑證實務作業基準核准程序(CPS Approval Procedures)

本作業基準的核准單位為 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、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，且需通過主管機關的核定。

附錄一(Appendix 1) 詞彙(Glossary)

(1).網際網路(Internet)

許多不同的電腦網路相互連結，經過標準的通訊協定，得以相互交換資訊。

(2).電子文件(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)

指依附於電子文件並與其相關連，用以辨識及確認電子文件簽署人身分、資格及電子文件真偽者。

(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。

(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)

指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。

(7).私密金鑰(Private Key)

係指具有配對關係之數位資料中，由簽署人保有，用以製作數位簽章者。

(8).公開金鑰(Public Key)

係指具有配對關係之數位資料中，對外公開，用以驗證數位簽章者。

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

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。

(10).憑證機構(Cerificate Service Provider;CSP)

指簽發憑證之機關、法人。

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

指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。

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

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

(13).雜湊函數(Hash Function)

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

(14).簽發憑證(電子認證)(Issue a Certificate)：

係指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。

附錄二(Appendix 2) 字首與縮寫語((Acronyms and Abbreviations)

AICPA	American Institute of Certified Public Accountants, Inc.
ANS	American National Standard
BCA	Brand Certification Authority
CA	Certification Authority
CC	Common Criteria
CCA	Cardholder Certification Authority
CCITSE	Common Criteria for Information Technology Security Evaluation
CMA	Certification Management Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CSP	Cerificate Service Provider
CRL	Certificate Revocation List
DA	Directory Authority
DN	Distinguished Name
EAL	Evaluation Assurance Level
EB	Electronic Banking
EC	Electronic Commerce
FEDI	Financial Electronic Data Exchange
FIPS	Federal Information Processing Standard
HMAC-SHA1	Hash Message Authentication Code – Security Hash Algorithm 1
ISO/IEC	the International Organization for Standardisation, The International Electrotechnical Commission
ITSEC	Information Technology Security Evaluation Criteria
LDAP	Lightweight Directory Access Protocol
MCA	Merchant Certification Authority
NB	Network Banking
OCSP	Online Certificates Status Protocol
OID	Object Identifier
OECD	Organization for Economic Co-operation and Development
PAA	Pan-Asian e-Commerce Alliance
PMA	Policy Management Authority
PCA	Policy Certification Authority
PIN	Personal Identification number
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
RA	Registration Authority
RA	Repository Authority(Directory Authority)
RCA	Root Certification Authority

RSA	Rivest,Shamir,Adleman(encryption algorithm)
SET	Secure Electronic Transactions
SSL	Secure Socket Layer
TCSEC	Trusted Computer System Evaluation Criteria
TSA	Time Stamp Authority
TTP	Trusted Third Party
UCA	User Certification Authority
URL	Universal Resource Location