

金融最高層憑證管理中心  
憑證實務作業基準  
Certification Practices Statement

(第 2.0 版)

Version 2.0



生效日期：中華民國九十七年一月四日

Effective Date : 2008/01/04



## 目 錄

|   |           |
|---|-----------|
| <b>1.使用憑證之重要聲明(IMPORTANT STATEMENTS OF USING CERTIFICATES)</b> .....    | <b>9</b>  |
| 1.1 主管機關核定(APPROVED BY MINISTRY OF ECONOMIC AFFAIRS) .....              | 9         |
| 1.2 憑證之保證等級與適用範圍(CERTIFICATE'S APPLICABILITY) .....                     | 9         |
| 1.3 使用憑證之重要聲明(IMPORTANT STATEMENTS OF USING CERTIFICATES) .....         | 9         |
| <b>2.簡介(INTRODUCTION)</b> .....   | <b>11</b> |
| 2.1 概述(OVERVIEW).....   | 11        |
| 2.2 識別(IDENTIFICATION).....   | 11        |
| 2.3 公開金鑰基礎建設及適用性(COMMUNITY AND APPLICABILITY) .....                     | 12        |
| 2.3.1 金融公開金鑰基礎建設 .....  | 12        |
| 2.3.2 金融最高層憑證管理中心(Financial Root Certification Authority , FRCA) .....  | 12        |
| 2.3.3 金融政策憑證中心(Financial Policy Certification Authority , FPCA ).....   | 13        |
| 2.3.4 金融用戶憑證中心(Financial User Certification Authority , FUCA) .....     | 13        |
| 2.3.5 註冊中心(Registration Authority , RA).....                            | 13        |
| 2.3.6 使用者(End Entities).....  | 14        |
| 2.3.7 應用(Applicability).....  | 14        |
| 2.4 聯絡事宜(CONTACT DETAILS) .....   | 14        |
| 2.4.1 管理單位(Specification Administration Organization).....              | 14        |
| 2.4.2 聯絡窗口(Contact Person).....   | 14        |
| 2.4.3 CPS 修改與訂定(Person Determining CPS Suitability for the Policy)..... | 15        |
| <b>3. 一般規範(GENERAL PROVISIONS)</b> .....                                | <b>16</b> |
| 3.1 責任(OBLIGATIONS).....  | 16        |
| 3.1.1 金融最高層憑證管理中心之責任(FRCA Obligations) .....                            | 16        |
| 3.1.2 註冊中心之責任(Registration Authority Obligations).....                  | 16        |
| 3.1.3 用戶之責任(Subscriber Obligations).....                                | 17        |
| 3.1.4 信賴憑證者之責任(Relying Party Obligations).....                          | 17        |
| 3.1.5 儲存庫之責任(Repository Obligations) .....                              | 17        |
| 3.2 賠償責任(LIABILITY).....  | 18        |
| 3.2.1 金融最高層憑證管理中心之賠償責任(FRCA Liability) .....                            | 18        |
| 3.2.2 用戶之賠償責任(Subscriber Liability).....                                | 19        |
| 3.3 財務責任 ( FINANCIAL RESPONSIBILITY ).....                              | 19        |
| 3.3.1 第三者賠償責任( Indemnification by Relying Parties and Subscriber )..... | 19        |
| 3.3.2 代理(Fiduciary Relationships).....                                  | 19        |
| 3.3.3 管理之執行( Administrative Processes).....                             | 19        |
| 3.4 釋義與施行( INTERPRETATION AND ENFORCEMENT ).....                        | 20        |
| 3.4.1 準據法(Governing Law).....   | 20        |
| 3.4.2 CPS 之適用性、義務續存性、權利義務之整合及訊息公佈(Severability of Provisions,           |           |

|   |           |
|---|-----------|
| Survival, Merger, and Notice).....  | 20        |
| 3.4.3 爭議處理程序(Dispute Resolution Procedures).....                          | 20        |
| 3.5 服務費(FEES).....  | 21        |
| 3.5.1 憑證申請收費(Certificate Issuance Fees ).....                             | 21        |
| 3.5.2 憑證查詢收費(Certificate Access Fees).....                                | 21        |
| 3.5.3 憑證廢止與憑證狀態查詢收費(Revocation or Status Information Access Fees) ....    | 21        |
| 3.5.4 其他收費( Fees for Other Services such as Policy Information).....      | 21        |
| 3.5.5 退費(Refund policy).....  | 21        |
| 3.6 公布與儲存 (PUBLICATION AND REPOSITORY ).....                              | 21        |
| 3.6.1 FRCA 資訊公布(Publication of FRCA Information ).....                    | 21        |
| 3.6.2 公布頻率(Frequency of Publication).....                                 | 22        |
| 3.6.3 存取管控(Access Control).....   | 22        |
| 3.6.4 儲存庫(Repositories).....  | 22        |
| 3.7 稽核(COMPLIANCE AUDIT).....   | 22        |
| 3.7.1 稽核頻率(Frequency of Compliance Audit for Each Entity).....            | 22        |
| 3.7.2 稽核人員適任條件(Identity/Qualifications of Auditor ).....                  | 22        |
| 3.7.3 稽核人員之獨立性(Auditor's Relationship to Audited Party ).....             | 22        |
| 3.7.4 稽核內容(Topics Cover by Audit).....                                    | 23        |
| 3.7.5 稽核缺失之處理(Action Taken as a Result of Deficiency ).....               | 23        |
| 3.7.6 稽核結果之查詢(Communication of Results ).....                             | 24        |
| 3.8 隱密性(CONFIDENTIALITY).....   | 24        |
| 3.8.1 應保護之資料種類(Type of Information to be keep Confidential).....          | 24        |
| 3.8.2 可公開之資訊種類(Type of Information Not considered Confidential).....      | 24        |
| 3.8.3 憑證廢止資訊之揭露(Disclosure of Certificate Revocation Information).....    | 24        |
| 3.8.4 依據法令要求之資料提供( Release to Law Enforcement Officials ).....            | 24        |
| 3.8.5 民事訴訟之資料提供(Release as Part of Civil Discovery ).....                 | 25        |
| 3.8.6 憑證用戶之資料提供( Disclosure upon Owner's Request ).....                   | 25        |
| 3.8.7 其他資訊公告條件(Other Information Release Circumstances ).....             | 25        |
| 3.9 智慧財產權( INTELLECTUAL PROPERTY RIGHTS ).....                            | 25        |
| <b>4. 識別與驗證(IDENTIFICATION AND AUTHENTICATION).....</b>                   | <b>26</b> |
| 4.1 註冊(INITIAL REGISTRATION).....   | 26        |
| 4.1.1 識別名稱之種類(Type of Names).....   | 26        |
| 4.1.2 識別名稱之意義( Need for Names to be Meaningful ).....                     | 26        |
| 4.1.3 各種識別名稱之規範 (Rules for Interpreting Various Name Forms).....          | 26        |
| 4.1.4 識別名稱之唯一性(Uniqueness of Names).....                                  | 26        |
| 4.1.5 識別名稱糾紛之處理(Name Claim Dispute Resolution Procedures ).....           | 27        |
| 4.1.6 註冊商標之認可與驗證(Recognition, Authentication and role of Trademarks)..... | 27        |
| 4.1.7 私密金鑰之驗證方法(Method to Prove Possession of Private Key).....           | 27        |
| 4.1.8 公司組織身分之驗證(Authentication of Organisation Identity).....             | 27        |

|  |           |
|--|-----------|
| 4.2 憑證及私密金鑰之更新(ROUTINE REKEY).....   | 27        |
| 4.3 廢止憑證之私密金鑰之更新(REKEY AFTER REVOCATION ) .....  | 28        |
| 4.4 憑證廢止需求(REVOCATION REQUEST ) .....  | 28        |
| <b>5. 憑證系統管理(OPERATION REQUIREMENTS).....</b>  | <b>29</b> |
| 5.1 憑證之申請(CERTIFICATES APPLICATION) .....  | 29        |
| 5.1.1 憑證申請政策(Certificate Application Policy) .....   | 29        |
| 5.1.2 憑證展期策略(Certificate Extend Policy) .....  | 29        |
| 5.1.3 FPCA 憑證暫時停用政策(Certificate Suspension Policy) .....   | 29        |
| 5.2 憑證之簽發(CERTIFICATES ISSUANCE).....  | 29        |
| 5.3 憑證之啟用 (CERTIFICATES ACCEPTANCE AND USING) .....  | 30        |
| 5.3.1 憑證之啟用(Certificates Acceptance) .....   | 30        |
| 5.3.2 憑證之使用(Certificates Using).....   | 30        |
| 5.4 憑證之廢止(REVOCATION OF CERTIFICATE) .....   | 30        |
| 5.4.1 憑證廢止時機(Circumstances for Revocation).....  | 30        |
| 5.4.2 有權廢止憑證者(Who can Request Revocation) .....  | 31        |
| 5.4.3 憑證廢止程序(Procedure for Revocation Request) .....   | 31        |
| 5.4.4 憑證請求廢止之寬限期(Revocation Request Grace Period).....   | 32        |
| 5.4.5 憑證廢止清單產生頻率(CRL Issuance Frequency).....  | 32        |
| 5.4.6 憑證廢止清單查證要求(CRL Checking Requirements).....   | 32        |
| 5.4.7 線上憑證與廢止憑證狀態查證功能(On-line Revocation/Status Checking Availability)                           | 32        |
| 5.4.8 線上廢止憑證查證要求(On-line Revocation Checking Requirement) .....                                  | 32        |
| 5.4.9 其他格式廢止憑證通知之功能(Other Forms of Revocation Advertisements Available) .....                    | 32        |
| 5.4.10 其他格式廢止憑證通知之查核需求(Checking Requirements for Other Forms of Revocation Advertisements) ..... | 33        |
| 5.4.11 金鑰危害之特殊要求(Special Requirements Re Key Compromise) .....                                   | 33        |
| 5.5 安全稽核(SEcurity AUDIT PROCEDURES).....   | 33        |
| 5.5.1 稽核紀錄種類(Types of Events Recorded) .....   | 33        |
| 5.5.2 稽核紀錄之檢視頻率(Frequency of Processing Log) .....   | 33        |
| 5.5.3 稽核紀錄之保存期限(Retention Period for Audit Log).....   | 33        |
| 5.5.4 稽核紀錄之保護(Protection of Audit Log).....  | 34        |
| 5.5.5 稽核紀錄備援程序(Audit log backup procedures).....   | 34        |
| 5.5.6 稽核紀錄蒐集系統(Audit Collection System) .....  | 34        |
| 5.5.7 異常狀況之通知(Notification to Event-Causing Subject).....  | 35        |
| 5.5.8 弱點評估(Vulnerability Assessments).....   | 35        |
| 5.6 紀錄留存(RECORDS ARCHIVAL).....  | 35        |
| 5.6.1 事件紀錄之種類(Types of Event Records).....   | 35        |
| 5.6.2 紀錄留存期限(Retention Period for Archive ).....   | 35        |

|  |           |
|--|-----------|
| 5.6.3 留存記錄之保護(Protection of Archive).....  | 35        |
| 5.6.4 留存記錄之備援程序(Archive Backup Procedures) .....                                       | 35        |
| 5.6.5 紀錄之時戳要求(Requirements for Time-Stamping of Records) .....                         | 36        |
| 5.6.6 留存紀錄蒐集系統(Archive Collection System).....   | 36        |
| 5.6.7 留存記錄之取得與驗證程序(Procedure to Obtain and Verify Archive Information) 36              |           |
| 5.7 金鑰變更(KEY CHANGEOVER).....  | 36        |
| 5.7.1 FPCA 金鑰變更(Key Changeover of FPCA).....   | 36        |
| 5.7.2 FRCA 金鑰變更(Key Changeover of FRCA) .....  | 36        |
| 5.8 危害及災害復原(COMPROMISE AND DISASTER RECOVERY) .....                                    | 37        |
| 5.8.1 電腦資源、軟體與資料之毀損(Computing Resources, Software, and/or Data are Corrupted ).....    | 37        |
| 5.8.2 金融政策憑證管理中心公開金鑰廢止之復原程序(FPCA Public Key is Revoked)...                             | 37        |
| 5.8.3 FRCA & FPCA 私密金鑰之破解處理程序(FPCA & FRCA Private Key is Compromised) .....            | 37        |
| 5.8.4 設備之安全維護(Secure Facility after a Natural or Other Type Disaster ).....            | 38        |
| 5.8.5 業務永續及災害復原計劃(Contingency and Disaster Recovery Plan) .....                        | 38        |
| 5.9 FRCA 結束營運(FRCA TERMINATION) .....  | 38        |
| <b>6. 實體、作業流程及人員安全控管(PHYSICAL、PROCEDURAL AND PERSONNEL SECURITY CONTROL) .....</b>     | <b>40</b> |
| 6.1 實體控管(PHYSICAL CONTROL).....  | 40        |
| 6.1.1 建築物與位置(Site Location and Construction).....                                      | 40        |
| 6.1.2 門禁管制(Physical Access).....   | 40        |
| 6.1.3 電力與空調(Power and Air-Condition) .....   | 40        |
| 6.1.4 水災之防範(Water Exposures) .....   | 40        |
| 6.1.5 火災之防範(Fire Prevention and Protection) .....                                      | 40        |
| 6.1.6 媒體儲存(Media Storage) .....  | 40        |
| 6.1.7 廢棄處理(Waste disposal) .....   | 41        |
| 6.1.8 異地備份(Off-Site Backup) .....  | 41        |
| 6.2 作業程序控管(PROCEDURE CONTROL) .....  | 41        |
| 6.2.1 可信賴角色(Trusted Role) .....  | 41        |
| 6.2.2 作業人員需求人數(Number of Persons Required per Role) .....                              | 42        |
| 6.2.3 角色之識別與驗證(Identification and Authentication for Each Role).....                   | 42        |
| 6.3 人員控管(PERSONNEL CONTROL) .....  | 42        |
| 6.3.1 適任條件與經歷(Background, Qualifications ,Experience ,and clearance requirements)..... | 42        |
| 6.3.2 資格審查程序(Background Check Procedures).....   | 42        |
| 6.3.3 教育訓練(Training Requirements) .....  | 43        |
| 6.3.4 再教育之頻率與需求(Retraining Frequency and Requirement ).....                            | 43        |
| 6.3.5 職務之輪調(Job Rotation Frequency and Sequence ).....                                 | 43        |

|   |           |
|---|-----------|
| 6.3.6 非授權作業之懲處(Sanctions for Unauthorized Actions) .....                | 43        |
| 6.3.7 委外人員需求(Contacting Personnel Requirements).....                    | 43        |
| 6.3.8 作業手冊之提供(Document Supplied to Personnel) .....                     | 43        |
| <b>7. 技術安全控管(TECHNICAL SECURITY CONTROL) .....</b>                      | <b>45</b> |
| 7.1 金鑰對之產生與建置(KEY PAIR GENERATION AND INSTALLATION) .....               | 45        |
| 7.1.1 金鑰對之產製(Key Pair Generation) .....                                 | 45        |
| 7.1.2 私密金鑰之遞送(Private Key Delivery to Entity).....                      | 45        |
| 7.1.3 公開金鑰遞送至憑證簽發者(Public Key Delivery to Certificate Issuer) .....     | 45        |
| 7.1.4 FRCA 公開金鑰之遞送(FRCA Public Key Delivery to Users).....              | 45        |
| 7.1.5 金鑰長度(Key Sizes) .....   | 45        |
| 7.1.6 公開金鑰參數之產生(Public Key Parameters Generation) .....                 | 45        |
| 7.1.7 參數品質之檢核(Parameter Quality Checking ) .....                        | 46        |
| 7.1.8 金鑰之產生設備(Hardware/Software Key Generation) .....                   | 46        |
| 7.1.9 金鑰之使用(Key Usage Purposes) .....                                   | 46        |
| 7.2 私密金鑰之保護(PRIVATE KEY PROTECTION).....                                | 46        |
| 7.2.1 密碼模組之標準(Standards for Cryptographic Module) .....                 | 46        |
| 7.2.2 私密金鑰之分持控管(Private Key (n out of m) Multi-Person Control ) .....   | 46        |
| 7.2.3 私密金鑰之託管、回復及保存(Private Key Escrow) .....                           | 46        |
| 7.2.4 私密金鑰之備份(Private Key Backup) .....                                 | 46        |
| 7.2.5 私密金鑰之留存(Private Key Archival).....                                | 46        |
| 7.2.6 私密金鑰之建置(Private Key Entry into Cryptographic Module) .....        | 47        |
| 7.2.7 私密金鑰之開啟(Method of Activating Private Key) .....                   | 47        |
| 7.2.8 私密金鑰之關閉(Method of Deactivating Private Key).....                  | 47        |
| 7.2.9 私密金鑰之銷毀(Method of Destroying Private Key) .....                   | 47        |
| 7.3 金鑰對管理之其他事項(OTHER ASPECTS OF KEY PAIR MANAGEMENT).....               | 47        |
| 7.3.1 公開金鑰之留存(Public Key Archival) .....                                | 47        |
| 7.3.2 公開金鑰與私密金鑰之有效期限(Usage Periods for Public Keys and Private Key)     |           |
| .....   | 47        |
| 7.4 啟動資訊(ACTIVATION DATA).....  | 48        |
| 7.5 電腦安全控管(COMPUTER SECURITY CONTROLS).....                             | 48        |
| 7.5.1 電腦安全技術需求(Specific Computer Security Technical Requirements) ..... | 48        |
| 7.5.2 電腦系統安全等級(Computer Security Rating) .....                          | 48        |
| 7.6 生命週期技術控管(LIFE CYCLE TECHNICAL CONTROLS ) .....                      | 48        |
| 7.6.1 系統開發控管(System Development Controls).....                          | 48        |
| 7.6.2 安全管理控管(Security Management Controls ) .....                       | 48        |
| 7.7 網路安全控管(NETWORK SECURITY CONTROL) .....                              | 49        |
| 7.8 密碼模組工程控管(CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS) .....           | 49        |
| <b>8. 憑證與憑證廢止清冊格式(CERTIFICATES AND CERTIFICATES REVOCATION LIST</b>     |           |
| <b>(CRL) PROFILES) .....</b>  | <b>50</b> |

|  |           |
|--|-----------|
| 8.1 憑證格式(CERTIFICATES PROFILE) .....   | 50        |
| 8.1.1 版本( Version Number(s) ).....   | 50        |
| 8.1.2 憑證擴充欄位(Certificate Extension) .....  | 50        |
| 8.1.3 演算法物件識別代碼(Algorithm Object Identifiers).....                                   | 50        |
| 8.1.4 命名格式(Name Forms).....  | 50        |
| 8.1.5 命名限制(Name Constraint).....   | 50        |
| 8.1.6 憑證政策物件識別代碼(Certificate Policy Object Identifiers) .....                        | 50        |
| 8.1.7 憑證政策限制擴充欄位之使用(Usage of Policy Constraints Extension).....                      | 51        |
| 8.1.8 憑證政策限制語法與語意(Policy Qualifiers Syntax and Semantics) .....                      | 51        |
| 8.1.9 憑證政策擴充欄位必要之處理(Processing Semantics for the Critical Policy<br>Extension) ..... | 51        |
| 8.2 憑證廢止清冊格式(CRL PROFILE).....   | 51        |
| 8.2.1 版本(Version number(s)) .....  | 51        |
| 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) .....                          | 51        |
| <b>9. 規範管理(SPECIFICATION ADMINISTRATION).....</b>                                    | <b>52</b> |
| 9.1 規範變更程序(SPECIFICATION CHANGE PROCEDURE) .....                                     | 52        |
| 9.2 公告與通知策略(PUBLICATION AND NOTIFICATION POLICIES) .....                             | 52        |
| 9.3 憑證實務作業基準核准程序(CPS APPROVAL PROCEDURES) .....                                      | 52        |
| <b>附錄一(APPENDIX 1) 詞彙(GLOSSARY).....</b>   | <b>53</b> |
| <b>附錄二(APPENDIX 2) 字首與縮寫語(ACRONYMS AND ABBREVIATIONS).....</b>                       | <b>56</b> |



# 金融最高層憑證管理中心 (FRCA) 憑證實務作業基準 (Certification Practices Statement ; CPS)

## 1.使用憑證之重要聲明(Important Statements of Using Certificates)

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

本憑證實務作業基準(以下簡稱本作業基準或 CPS)係依據主管機關經濟部頒布之「憑證實務作業基準應載明事項準則」規範編撰,經主管機關審查核定之文號如下:

**97/01/04 經濟部函 經商字第 09602169780 號。**

### 1.2 憑證之保證等級與適用範圍(Certificate's Applicability)

金融最高層憑證管理中心 (Financial Root Certification Authority, 以下簡稱 FRCA) 之用戶為金融政策憑證管理中心(Financial Policy Certification Authority, 以下簡稱 FPCA, 法人機構), FRCA 只簽發 FPCA 之憑證; FPCA 憑證只可使用於簽發其下屬憑證管理中心, 即用戶憑證管理中心(Financial User Certification Authority, 以下簡稱 FUCA, 法人機構)之憑證。

FRCA 憑證用戶之身分驗證及鑑別依據「4.1.8 公司組織身分之驗證(Authentication of Organisation Identity)之規範執行,並無不同層級身分驗證及鑑別程序,故憑證無保證等級之分別。

### 1.3 使用憑證之重要聲明(Important Statements of Using Certificates)

FRCA 自行委託律師事務所或會計師事務所進行稽核,再將稽核報告經由金融最高層憑證管理中心審核後送政策管理委員會,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:

FPCA 向 FRCA 申請憑證時,必須提供詳細且正確之公司組織證明文件與資料,確實了解並同意申請書與合約書上之權利與義務,及憑證申請與使用之作業規範內容,並且於接受該規範之規定下始可簽名確認;FPCA 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 FPCA 負損害賠償責任。

憑證之使用:

FPCA 必須妥善保管與憑證相對應之私密金鑰及保護密碼,當有被冒用、曝露及遺失等不安全之顧慮時,或不擬使用該憑證時,必須即刻向 FRCA 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 FPCA 負損害賠償責任。

FPCA 必須依照本作業基準與業務應用系統規範之規定,合法且正確之使用私密金鑰與憑證於相關之業務,絕不得使用於 1.本作業基準規範之外、2.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所危害之應用或業務系統、電子簽章法暨各項應用之主管機關明訂禁止之應用或業務,否則因而所致之損害,應由該 FPCA 負損

害賠償責任。

賠償責任：

FRCA 如因作業人員惡意或疏失，未遵照本作業基準及相關作業規範之規定辦理 FPCA 註冊、憑證之簽發與廢止作業，或違反相關法律規範而造成 FPCA 之損失時，FRCA 應依規定賠償 FPCA 之直接損失。

如因非作業人員之故意或過失，造成網際網路傳輸的中斷或故障，或其他不可抗拒的天災事故（例如戰爭或地震等），致所簽發之憑證造成 FPCA 損失時，FRCA 不負損害賠償責任。

FPCA 或其他有權者提出廢止 FPCA 之憑證要求後，至 FRCA 實際完成廢止該 FPCA 憑證之期間內，當該 FPCA 憑證被用以進行非法交易，或進行交易後產生法律糾紛時，FRCA 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)

臺灣網路認證股份有限公司(Taiwan-CA Inc.，以下簡稱本公司或 TWCA 或 TaiCA)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之資訊公司共同集資設立，為一值得信賴之憑證機構。

銀行公會於九十一年四月十八日發函(全電字第 0918 號)授權本公司擔任金融最高層憑證管理中心，行使 FRCA 職權，協助推動銀行公會 PKI 架構。FRCA 為銀行公會 PKI 架構內最高層憑證管理中心，本公司依據 X.509 (Public Key Infrastructure Certificate Policy and Certification Practice Statement Framework) 國際標準及經濟部及銀行公會之規範，制訂本作業基準。

FRCA 之憑證用戶為金融政策憑證管理中心(FPCA)，FRCA 提供 FPCA 憑證申請、核發、廢止等相關憑證作業。本作業基準遵循對應之 FRCA 憑證政策(Certificate Policy, CP) 說明 FRCA 憑證簽發作業之實務及程序，建立安全及可信賴之憑證作業環境。

### 2.2 識別(Identification)

本作業基準依據參考與對應之 CP 物件識別碼(Object Identifier, OID) 為 FRCA CP OID = 2.16.158.3.1.3.5。

#### 2.2.1 標準規範(Standards)

本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 日所發布之憑證實務作業基準應載明事項準則。
- (3) 中華民國銀行公會於九十四年八月二十五日公布之「金融公開金鑰基礎建設憑證政策(CP)V1.0」。

#### 2.2.2 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。

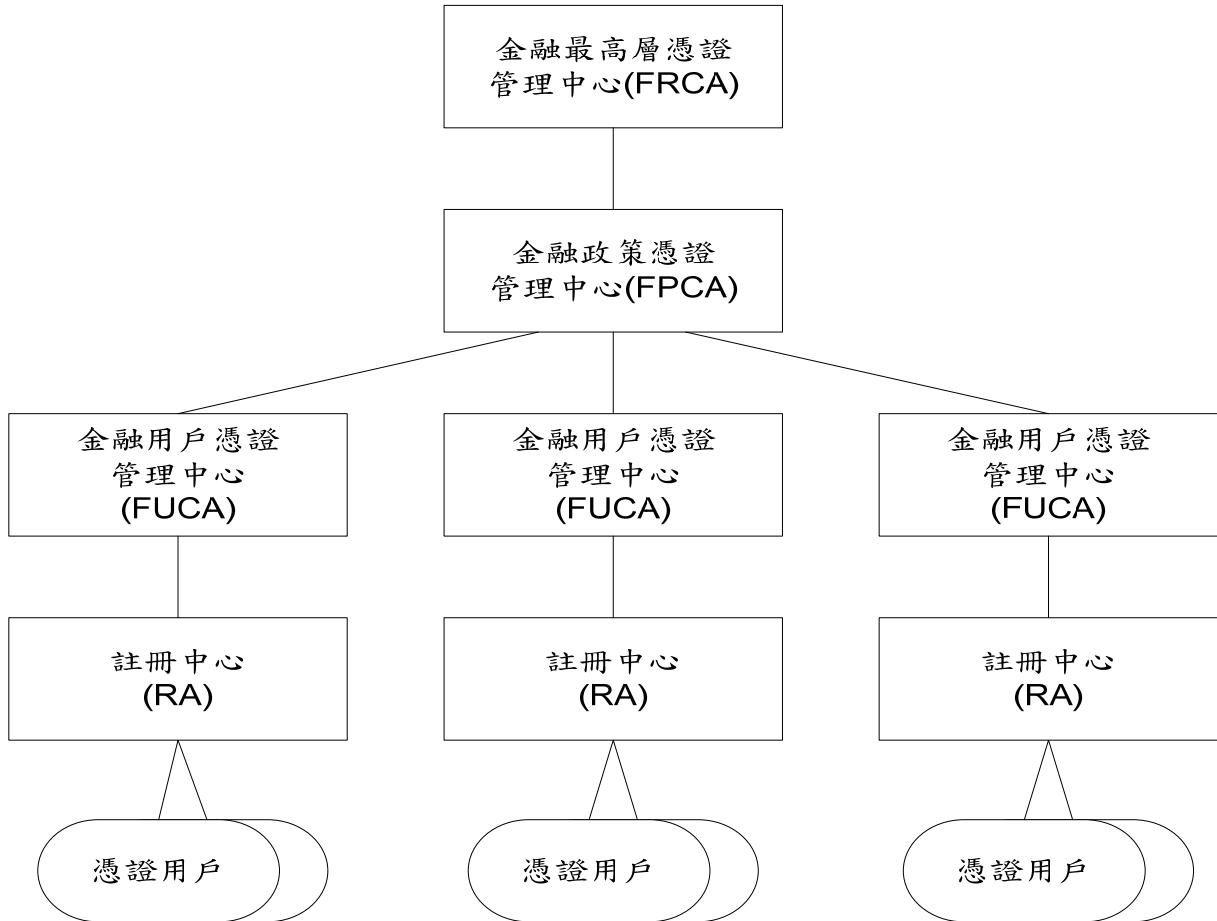
FPCA 在了解本作業基準規範前，建議應先行熟悉如下所列基本公開金鑰基礎建設(Public Key Infrastructure, PKI)運作的觀念：

- (1) 數位簽章(Digital Signature)使用於身分與交易訊息的驗證性(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) 交易訊息隱密性(Confidentiality)的密碼加密機制，例如對稱性或非對稱性的密碼加密機制。
- (3) 非對稱性的密碼加密機制，公開金鑰對(Public 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) 公開金鑰基礎建設階層架構下，憑證管理中心、註冊中心的運作功能。

## 2.3 公開金鑰基礎建設及適用性(Community and Applicability)

### 2.3.1 金融公開金鑰基礎建設

本章節就金融公開金鑰基礎建設所包含之各單元做說明，但 FRCA 之實際營運架構並未包含下列所有單元，FRCA 係指下圖中金融最高層憑證管理中心 (FRCA)。



### 2.3.2 金融最高層憑證管理中心(Financial Root Certification Authority, FRCA)

FRCA 負責：

- (1) 依據法律、政策及銀行公會規範，訂定、管理 FRCA 作業及憑證實務作業基準、憑證及廢止憑證之內容(例如：依法律、政策與業務之需求訂定憑證申請之規範標準、作業程序)。
- (2) 管理與公告 FPCA 憑證、憑證廢止清單(Certificates Revocation List，以下簡稱 CRL)之作業程序與驗證之作業規範。
- (3) 簽發、管理與遞送 FPCA 之憑證、CRL 及 FPCA 資訊(如：註冊名稱、電子郵箱、聯絡地址、電話等)，並規範查詢作業之功能。
- (4) 公告、管理與維護 FRCA 之憑證政策及憑證實務作業基準、相關作業規範、憑證、CRL、註冊名稱、網址(URL)、郵箱(E-Mail)與聯絡之相關資訊。
- (5) FRCA 負責執行 FUCA 技術資格審查、制定 FUCA 系統互通驗證規範。

(6) FRCA 負責處理與其他國內外憑證機構進行交互認證之事宜。

### 2.3.3 金融政策憑證中心(Financial Policy Certification Authority, FPCA)

FPCA 負責：

- (1) 依據法律、政策及銀行公會規範訂定、管理 FPCA 作業、憑證政策及憑證實務作業基準、憑證及廢止憑證之內容(例如：依法律、政策與業務之需求訂定憑證申請之規範標準、作業程序)。
- (2) 管理與公告及維護 FPCA 憑證、CRL 之作業程序與驗證之作業規範。
- (3) 簽發、管理與遞送 FPCA 憑證、CRL 及 FPCA 資訊(如：註冊名稱、電子郵箱、聯絡地址、電話等)，並規範查詢作業之功能。
- (4) 公告、管理 FPCA 之憑證政策及憑證實務作業基準、相關作業規範、憑證、CRL、註冊名稱、網址(URL)、電子郵箱(E-mail)與聯絡之相關資訊。
- (5) FPCA 依照 FRCA 所制定之 FPCA 系統互通驗證規範，執行 FPCA 系統互通驗證作業。

### 2.3.4 金融用戶憑證中心(Financial User Certification Authority, FUCA)

FUCA 負責：

- (1) 公告及管理憑證用戶（自然人或法人）及註冊中心憑證簽發、更新、暫時停用及廢止之作業程序與驗證之作業規範（例如：憑證申請時之憑證用戶與註冊中心之身分驗證方式，傳輸之交易訊息之完整性與隱密性之安控措施），並訂定查詢作業功能之規範。
- (2) 驗證註冊中心傳遞之憑證用戶註冊申請訊息，與憑證申請訊息之身分合法性與交易訊息之有效性，並將回覆訊息安全地傳回註冊中心。
- (3) 簽發、管理與維護、遞送註冊中心與憑證用戶之憑證、廢止憑證及用戶資訊。
- (4) 公告及管理與維護 FUCA 之憑證政策及憑證實務作業基準、相關作業規範、憑證、註冊名稱、網址(URL)、電子郵箱(E-Mail) 與聯絡之相關資訊。

### 2.3.5 註冊中心(Registration Authority, RA)

RA 負責：

- (1) 遵循 FUCA 規範之憑證用戶（個人或法人）註冊申請之作業程序與身分驗證之作業規範（例如：憑證用戶註冊之身分驗證之安控措施，傳輸之交易訊息之加密與完整性之安控措施）。
- (2) 驗證憑證用戶註冊、憑證之簽發、更新、暫時停用與廢止及查詢之申請訊息，身分合法性與訊息完整性之驗證。
- (3) 遞送憑證用戶之註冊申請訊息與憑證、廢止憑證、查詢申請訊息，至 FUCA 申請憑證、更新、暫時停用及廢止憑證，並驗證回覆訊息之正確性後傳回予申請之用戶。
- (4) 公告、管理 RA 註冊名稱、網址(URL)、電子郵箱(E-Mail) 與聯絡之相關資訊。

## 2.3.6 使用者(End Entities)

### 2.3.6.1 憑證用戶(Subscribers, SC)

憑證用戶(個人或法人)，其憑證與憑證對應之私密金鑰(private key)使用之業務範圍，皆依 FUCA 之憑證政策及憑證實務作業基準之規範，運用於銀行公會規範之業務上。用戶可使用自我憑證對應之私密金鑰，執行交易訊息之簽章。

### 2.3.6.2 信賴憑證者(Relying Parties, RP)

信賴憑證者即為使用他人(憑證用戶)之憑證、FUCA、FPCA 與 FRCA 之憑證鏈(Certificates Chain)資訊，用以驗證接收之簽章訊息之完整性，或使用他人(接收者)之憑證中所記載之公開金鑰作訊息之加密後、將加密之訊息傳送至接收者，以達到通訊雙方訊息之隱密性。

## 2.3.7 應用(Applicability)

本作業基準適用於所有由 FRCA 所簽發之憑證，並說明簽發、使用及廢止 FPCA 憑證之作業實務。FRCA 所簽發之憑證，具備身分識別、不可否認性、訊息完整性及訊息隱密性之安全機制。

### 2.3.7.1 憑證之使用範圍

FRCA 依據本作業基準所規範及簽發的 FPCA 憑證，FPCA 只可使用於簽發金融用戶憑證管理中心(FUCA)之憑證。

### 2.3.7.2 憑證禁止使用之狀況

FPCA 憑證除使用於上述規定之範圍外，絕不可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，且絕不可使用於電子簽章法與相關法令規範、主管機關及銀行公會明訂禁止之應用或業務。

## 2.4 聯絡事宜(Contact Details)

### 2.4.1 管理單位(Specification Administration Organization)

本作業基準之訂定、更新、及發布等事宜，其權責單位為 FRCA 憑證政策管理委員會。

### 2.4.2 聯絡窗口(Contact Person)

FPCA 或其他相關單位對本作業基準有任何修改建議時，請將詳細之建議、說明文件與聯絡資訊，E-mail 或郵寄至下述之聯絡窗口。

FPCA 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 or TaiCA)  |
| 聯絡人              | 客服中心   |
| 地址               | (100) 台北市中正區延平南路 85 號 10 樓<br>10 <sup>TH</sup> 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<br>(E-mail) | rootca@twca.com.tw   |

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

本作業基準因國際標準之變動、安全機制之提昇、業務系統之需求、或作業環境與系統異動而需修改變更時，須經由 FRCA 憑證政策管理委員會之評估與審核後始可變更；變更後之作業基準，須送交主管機關審核，經主管機關核可後，始可對外公告新版之作業基準。

### 3. 一般規範(General Provisions)

#### 3.1 責任(Obligations)

##### 3.1.1 金融最高層憑證管理中心之責任(FRCA Obligations)

FRCA 於執行 FPCA 憑證之簽發與廢止之憑證管理作業前，應依據權責主管機關之作業規範（例如電子簽章法、電子簽章法施行細則、憑證實務作業基準應載明事項）規劃建置憑證管理系統，受主管機關與作業相關法律規範之管轄與監督，並由主管機關審核本作業基準。

FRCA 之責任包含：

- (1) 訂定、公告及管理 FRCA 業務範圍內之憑證實務作業基準規範。
- (2) FRCA 憑證管理作業之運作，必須依據主管機關之作業規範與 FRCA 憑證政策之規範。
- (3) 確認 FRCA 憑證系統作業人員（含合約委外人員）之選用與系統運作符合憑證政策及憑證實務作業基準之規範。
- (4) FRCA 與其作業人員必須善盡保管 FPCA 註冊資料、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。
- (5) FRCA 應依照憑證政策及憑證實務作業基準之規範，接受 FPCA 憑證之申請、廢止憑證之申請等有關訊息，確認 FPCA 發送至 FRCA 之相關交易訊息之正確性與安全性，並執行憑證簽發與憑證廢止之相關作業，及將相關回覆訊息正確及安全地遞送至 FPCA。
- (6) FRCA 執行 FPCA 憑證簽發時，必須確認 FPCA 已確實了解且同意申請書與合約書上之權利與義務，及業務相關作業規範之內容，並驗證 FPCA 申請文件與身分之正確性及合法性。
- (7) FRCA 若更新自簽憑證，必須以最迅速安全之方式遞送予 FPCA 或通知 FPCA 至 FRCA 索取。
- (8) FRCA 憑證相對應之私密金鑰有安全之顧慮時，必須依憑證實務作業基準之相關作業規定，立即向銀行公會辦理申告與處理。
- (9) FPCA 申請或廢止憑證時，依照憑證政策及憑證實務作業基準之規範，應及時產生憑證或 CRL，並立刻安全之遞送至目錄伺服器(Directory Server)或憑證查詢資料庫。
- (10) FRCA 與 FPCA 之合約或相關作業文件，應詳細說明憑證申請、更新、廢止、註冊與使用之作業規範，及相關之權利與義務關係。
- (11) FRCA 簽發 FPCA 憑證與 CRL 之私密金鑰必須獨立使用，決不可與其他功能共用，如有訊息之簽章與加密之需求時，必須使用不同且獨立之私密金鑰。
- (12) 若權責機關有規定，FRCA 應於憑證實務作業基準與相關作業規範內，訂定憑證廢止處理時效。

##### 3.1.2 註冊中心之責任(Registration Authority Obligations)

FPCA 之憑證註冊及申請需求，由 FRCA 直接處理，不另外成立註冊中心。FPCA 之身分驗證程序於簽約程序中執行。



### 3.1.3 用戶之責任(Subscriber Obligations)

FRCA 之憑證用戶為 FPCA(法人機構)，FPCA 之責任包含：

- (1) FPCA 向 FRCA 申請憑證時，必須確實了解並同意申請書與合約書上之權利與義務，及業務相關作業規範（例如：憑證實務作業基準）之內容，並且於同意接受該規範之規定下始可簽名確認。
- (2) FPCA 必須依據 FRCA 憑證實務作業基準之規定，確實且妥善安全地產製及保護其私密金鑰。
- (3) FPCA 必須了解且同意 FRCA 憑證政策及憑證實務作業基準相關作業規範之規定，合法且正確之使用私密金鑰與憑證於相關之業務系統，無任何違反相關法律之規定與侵害第三者之權利。
- (4) FPCA 與憑證相對應之私密金鑰有被冒用、曝露及遺失等不安全之顧慮時，或憑證內 FPCA 相關之資訊有異動時，FPCA 必須依本憑證實務作業基準之規定，即刻向 FRCA 辦理申告與處理。FPCA 憑證申請時必須提供詳實且正確之資訊，接受 FRCA 簽發之 FPCA 憑證時，必須確認憑證資訊之內容為 FPCA 註冊申請之資訊，且公開金鑰與 FPCA 之私密金鑰為相關之一對金鑰。
- (5) FPCA 憑證之使用，必須依 FRCA 憑證政策及憑證實務作業基準之規定，由憑證鏈(Certificates Chain)逐一驗證該憑證之正確性及有效性，當有憑證廢止清單(CRL)之安全機制時，亦需檢核此憑證是否為廢止憑證。
- (6) FPCA 應參考 FRCA 之憑證政策及憑證實務作業基準之規範，適當制訂相對應之憑證政策及憑證實務作業基準，並要求 FUCA 遵循。
- (7) FPCA 應與 FUCA 簽署服務合約，詳細說明憑證申請、更新、廢止、註冊與使用之作業規範，及相關之權利與義務關係。

### 3.1.4 信賴憑證者之責任(Relying Party Obligations)

FRCA 之信賴憑證者為其他 FPCA、向 FPCA 申請憑證簽發之 FUCA 或向 FUCA 申請憑證簽發之一般用戶（個人或組織），信賴憑證者之責任包括：

- (1) 信賴憑證者使用或接受他人（FPCA、FUCA 或一般使用者）之憑證前，應依據簽發該憑證之憑證機構之憑證實務作業基準及憑證內容所規定的業務範圍，確認該憑證之合法用途及了解該憑證機構法律責任條款，並於該憑證使用目的範圍內，信賴該憑證。
- (2) 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。
- (3) 信賴憑證者使用或接受他人之憑證時，應依據憑證實務作業基準、應用業務系統作業規範的規定及 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。
- (4) 信賴憑證者使用或接受他人之憑證時，應從 CRL 或利用線上憑證狀態查詢(OCSP) 方式檢查憑證之狀態，確認憑證是否為廢止或暫時停用。

### 3.1.5 儲存庫之責任(Repository Obligations)

FRCA 應存放憑證、CRL 及 OCSP 之資料於安全的儲存庫內，確保儲存庫存

取之有效性，提供信賴憑證者隨時查詢：

- (1) 確認儲存庫憑證系統作業人員（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、與儲存庫的作業規範。
- (2) 當有新簽發 FPCA 憑證或公佈 CRL 時，必須能立刻更新資料庫，提供用戶查詢最新的資訊，除系統維護的需求當有新簽發憑證用戶憑證或公佈 CRL 時，必須能立刻更新資料庫，提供用戶查詢最新的資訊，除系統維護的需求得暫時停止服務(上限 24 小時)外，每天二十四小時提供正常服務。
- (3) 驗證信賴憑證者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信賴憑證者。
- (4) 儲存庫與其作業人員必須善盡保管 FPCA 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。
- (5) 儲存庫使用的私密金鑰有被冒用、曝露及遺失等不安全的顧慮時，或憑證內相關的儲存庫資訊有異動時，必須依相關作業的規定，即刻向 FRCA 辦理申告與處理。

### 3.2 賠償責任(Liability)

本公司所提供的憑證服務作業項目與內容，皆訂定於本作業基準「1.2 憑證之適用範圍(Certificates's Applicability)」，非前述作業基準所訂定的內容，例如用戶與信賴憑證者使用的服務，皆排除於賠償責任之外。

#### 3.2.1 金融最高層憑證管理中心之賠償責任(FRCA Liability)

- (1) FRCA 處理 FPCA 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而造成 FPCA 之損失，且可歸責於 FRCA 之過失外，FRCA 概不負任何損害賠償責任。
- (2) 如非為 FRCA 惡意或疏失，造成網際網路傳輸之中斷或設備之故障或其他不可抗拒之天災事故（例如戰爭或地震等），致所簽發之憑證造成 FPCA 損失時，FRCA 不負任何損害賠償責任。
- (3) FRCA 與其作業人員未善盡保管 FPCA 之註冊及憑證相關資料，而造成相關資訊洩漏、被冒用、篡改及任意使用致造成 FPCA 遭受損害時，FRCA 與該作業人員應依 FRCA 與 FPCA 之合約規定負損害賠償責任。
- (4) FRCA 如因作業人員惡意或疏失，未遵照本作業基準之規定辦理註冊、憑證之簽發與廢止作業，而造成 FPCA 之損失時，FRCA 應依 FRCA 與 FPCA 之合約規定賠償 FPCA 損失。
- (5) FPCA 或其他有權者提出廢止 FPCA 之憑證要求後，至 FRCA 實際完成廢止該 FPCA 憑證之期間內，當該 FPCA 憑證被用以進行非法交易，或進行交易後產生法律糾紛時，FRCA 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。
- (6) FPCA 之賠償追究有效期限，依業務主管機關與相關法律之規範辦理。

### 3.2.2 用戶之賠償責任(Subscriber Liability)

FRCA 之憑證用戶為 FPCA：

- (1) FPCA 向 FRCA 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 FRCA、FUCA 或第三者遭受損害時，應由該 FPCA 負損害賠償責任。
- (2) FPCA 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 FRCA、FUCA 或第三者遭受損害時，應由該 FPCA 負損害賠償責任。
- (3) FPCA 申請使用憑證或使用信賴憑證者憑證，有違反 FRCA 憑證政策與本作業基準及相關作業之規範，或憑證使用於非本作業基準規定之其他業務範圍時，FPCA 應自行負一切損害賠償責任。
- (4) FPCA 使用憑證時之檢核，未依 FRCA 憑證政策、本作業基準之規範逐一檢核，致造成 FRCA、FUCA 或第三者遭受損害時，應由該 FPCA 負損害賠償責任。
- (5) FPCA 或其他有權者提出廢止 FPCA 之憑證要求後，至 FRCA 實際完成廢止該 FPCA 憑證之期間內，當該 FPCA 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 FRCA 執行處理作業時，符合本作業基準與相關之作業規範，則 FPCA 必須負所有損害賠償責任。
- (6) 其他與業務相關之償責，訂定於業務相關之作業規範與 FPCA 之業務合約規範。

### 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。

本公司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，於完成保險作業前提撥新台幣三千萬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 第三者賠償責任( Indemnification by Relying Parties and Subscriber )

因信賴憑證者或 FPCA 之惡意或過失，而非為 FRCA 之疏失，所造成第三者財務、信譽及其他各方面之損失時，FRCA 擁有賠償責任豁免權。

如因信賴憑證者或 FPCA 之過失且可歸責於信賴憑證者或 FPCA，而造成 FRCA 或其他第三者財務、信譽及其他各方面之損失時，信賴憑證者或 FPCA 必須負損害賠償責任，FRCA 可依照相關法律之規定向信賴憑證者或 FPCA 請求賠償。

#### 3.3.2 代理(Fiduciary Relationships)

依據本作業基準所簽發之憑證，FRCA 與 FPCA 之權責關係均屬直接關係，絕無代理之關係存在。

#### 3.3.3 管理之執行( Administrative Processes)

FRCA 依據本作業基準執行於憑證管理作業，本作業基準須經主管機關審核

通過，且被正式授與簽發 FPCA 憑證之資格。

### 3.4 釋義與施行( Interpretation and Enforcement )

#### 3.4.1 準據法(Governing Law)

本作業基準依據政府相關法律之規範而訂定，且受中華民國相關法律規範之管轄與督導，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準則之管理與監督，不論合約或其他準據法之條款為何，且不限於中華民國境內，本作業基準的執行、詮釋及效力皆以中華民國法律為準據法。

#### 3.4.2 CPS 之適用性、義務續存性、權利義務之整合及訊息公佈(Severability of Provisions, Survival, Merger, and Notice)

本作業基準之某些章節規定有不適用而必須修正時，其他條文之規定仍屬有效，不受該項不適用規定影響，直到新版之憑證實務作業基準之更新完成並公告使用，該項不適用規定之更新悉依本作業基準「2.4 聯絡事宜(Contact Details)」之規定辦理。

當 FPCA 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。

依本作業基準與相關業務之規範，FRCA 與 FPCA 間資訊通知之往來，可依下列傳遞方式：

- (1) 電子訊息 — 訊息經過傳送者，將發送訊息簽章後傳送，於接收者收妥訊息並完成訊息之簽章驗證。
- (2) 紙本文件— 文件表單具有傳送者與接收者之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；以傳真之方式傳送訊息時，除傳送者與接收者之詳細資訊外，必須具有詳細之傳真機識別號碼與傳送者業務相關人員之親筆簽名需求。

#### 3.4.3 爭議處理程序(Dispute Resolution Procedures)

FPCA 與 FRCA 因使用憑證所引起之爭議處理程序或糾紛仲裁處理，以本作業基準為基礎，詳細處理步驟於業務作業規範及 FRCA 與 FPCA 之合約內說明。

爭議之雙方如無法於 14 天內合理之協商解決爭議，得經雙方同意由憑證政策管理委員會協助解決雙方之爭議。

爭議之雙方如無法於 1 個月內同意協調者之協商與裁決，與合理的解決該問題爭議時，則由雙方將爭議提至臺北地方法院進行糾紛之訴訟與處理。

FPCA 與 FRCA 遇有爭議時，FPCA 與 FRCA 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。

於爭議協商、訴訟處理過程所發生之費用分擔，依據協商或相關之法律規範處理。

如為跨國或跨區域之爭議處理，無法以上述之處理方式解決時，則必須依照

相關之跨國或跨區域之糾紛仲裁規範處理。

### 3.5 服務費(Fees)

#### 3.5.1 憑證申請收費(Certificate Issuance Fees )

FRCA 與 FPCA 間之註冊、憑證申請等計費架構及收費之費率，訂定於相關業務之計費作業規範或於合約之條款中。

#### 3.5.2 憑證查詢收費(Certificate Access Fees)

FRCA 與 FPCA 間之憑證查詢收費等計費架構及收費之費率，訂定於相關業務之計費作業規範或於合約之條款中。

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

FRCA 與 FPCA 間之憑證狀態查詢(OCSP)功能之收費架構及收費之費率，訂定於相關業務之計費作業規範或於合約之條款中。

#### 3.5.4 其他收費( Fees for Other Services such as Policy Information)

FPCA 經由網際網路至 FRCA 下載本作業基準或相關業務之憑證政策，FRCA 不計收任何服務費用，但如向 FRCA 索取紙本文件之憑證實務作業基準或憑證政策或其他相關作業文件時，FRCA 需向 FPCA 收取郵寄及處理之工本費，收費之費率另訂定於相關業務之計費作業規範。

#### 3.5.5 退費(Refund policy)

FRCA 對 FPCA 所有憑證服務項目之收費，包含但不限於憑證費用、憑證讀取費用、憑證廢止與憑證狀態資訊讀取費用、建置費用、參加年費等，FRCA 均不退還 FPCA 任何費用。

### 3.6 公布與儲存 (Publication and Repository )

#### 3.6.1 FRCA 資訊公布(Publication of FRCA Information )

本作業基準以電子檔案 PDF(.pdf)格式，於主管機關核准正式生效後公告於 FRCA 之網站供用戶下載使用；網址：<http://www.twca.com.tw>。

憑證用戶有本作業基準紙本文件之需求時，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 or TaiCA)  |
| 聯絡人              | 客服中心   |
| 地址               | (100) 台北市中正區延平南路 85 號 10 樓<br>10 <sup>TH</sup> 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<br>(E-mail) | rootca@twca.com.tw   |

### 3.6.2 公布頻率(Frequency of Publication)

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，FRCA 應於接到核定公文一個月內公告於網站(<http://www.twca.com.tw/cps.asp>)。

FRCA 的用戶憑證經申請廢止後，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佈一次。

### 3.6.3 存取管控(Access Control)

FRCA 之憑證實務作業基準沒有存取權限的安全管控，任何憑證用戶可以依需求至本公司的網站下載。

### 3.6.4 儲存庫(Repositories)

FRCA 以目錄伺服器之作業方式提供 FPCA，憑證作業實務與憑證相關作業文件、FPCA 憑證與 FRCA 憑證、廢止憑證清單(CRL)、FPCA 與 FRCA 資訊之查詢及使用，FRCA 訂定適當之存取管控措施確保儲存庫內資訊之安全性。

## 3.7 稽核(Compliance Audit)

FRCA 自行委託律師事務所或會計師事務所進行稽核，再將稽核報告經由金融最高層憑證管理中心審核後送政策管理委員會核備，以確保遵照憑證實務作業基準與憑證政策之規定運作。

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

本公司憑證作業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 Objectives(CACO) 的查核標準，與參考 ISO 27001:2005 Information Technology – Code of Practice for Information 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 )

FRCA 執行稽核作業之稽核人員至少必須具備憑證機構、資訊系統安全稽核之知識，有二年以上之稽核相關經驗，且需熟悉本作業基準之運作規範，以及具有應用系統之業務及電腦硬軟體系統之相關知識與系統規劃、設計開發之相關經驗；國家相關管理單位（例如：經濟部）有規範稽核人員之適任條件時，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之相關實務經驗。

外部稽核人員應具備 CISA 及 CIA 資格之律師事務所或會計師事務所人員。

### 3.7.3 稽核人員之獨立性(Auditor's Relationship to Audited Party )

FRCA 執行稽核作業之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之客觀

性，並以獨立、公正、客觀之態度執行查核評估。

FRCA 當適任之稽核人力不足時，可以委由專業且公正、客觀之專業稽核機構，代為執行稽核相關作業。

### 3.7.4 稽核內容(Topics Cover by Audit)

FRCA 稽核人員查核：

- (1) FRCA 是否訂定與公告符合憑證政策之憑證實務作業基準及相關作業規範。
- (2) FRCA 是否依憑證實務作業基準及相關作業規範執行憑證相關業務。
- (3) FRCA 是否依憑證實務作業基準訂定與公告註冊相關作業規範。
- (4) FRCA 是否依憑證實務作業基準之規範及註冊作業規範之規定執行相關業務。

稽核人員主要稽核項目如下：

- (1) FRCA 業務執行之公告：FRCA 是否依憑證實務作業基準及相關作業規範公告與執行憑證管理作業。
- (2) 服務之完整性：FRCA、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）之安全管理，憑證與廢止憑證之生命週期作業之安全管理。
- (3) FRCA 環境之安全控管：符合 FRCA 資訊安全政策、憑證政策與憑證實務作業基準之資訊安全管理，資產之風險評估與安全控管，作業人員之安全控管，實體環境安全設施之安全控管，硬軟體設備、媒體之安全控管，系統或網路存取之安全控管，系統開發與維護之安全控管，系統開發與運作委外之安全控管，系統災變異地備援管理，符合相關法令規範與國際標準之管理，稽核事件與紀錄之安全管理。

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 稽核缺失之處理(Action Taken as a Result of Deficiency )

FRCA 之運作經詳細查核評估後，有不符合作業基準之規範時，稽核人員應依問題檢查缺失嚴重性之等級詳細條列，由稽核單位與受稽核單位共同討論稽核之缺失點，並將結果通知稽核單位與受稽核有關之單位，進行後續處理。

受稽核單位必須依檢查缺失，提矯正與預防措施及其改善規劃說明書，稽核單位之相關業務人員負責審查矯正措施與預防措施之合理性，並追蹤稽核後之改善情形。

FRCA 接受外部稽核報告後，依據稽核報告在限定時間內改善缺失，如未改善，憑證政策管理委員會得暫停 FRCA 的營運；在發現重大缺失時，憑證政策管理委員會得撤銷該機構擔任 FRCA 之資格。

### 3.7.6 稽核結果之查詢(Communication of Results )

除可能危害系統安全之資訊外，與信賴憑證者信賴該憑證的相關資訊，均應公開提供。FRCA 將公佈最近一次的稽核結果於公司網站上。

## 3.8 隱密性(Confidentiality)

### 3.8.1 應保護之資料種類(Type of Information to be keep Confidential)

FRCA 對於 FPCA 資訊隱密性之保護，必須於 FPCA 資訊保密策略規範中訂定，對於 FPCA 資訊之保護，必須依照行政院公告之「電腦處理個人資料保護法」之規範運作，或其他政府單位相關之規範運作，且符合 OECD 個人資料隱密性之保護規範 (OECD; Organization for Economic Co-operation and Development, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data ) 。

FRCA 於管理及使用 FPCA 註冊、憑證申請之相關資訊時，除 FPCA 憑證內容可公開外，FPCA 之註冊基本資料與身分驗證資料，非經由 FPCA 同意或主管機關的核可，絕不任意對外公開，於註冊或憑證申請時相關作業所使用之：

- (1) FPCA 身分驗證資訊 (例如：FPCA 名稱、聯絡資訊等)。
- (2) FPCA 註冊或憑證申請與註銷 (廢止) 時交易的相關隱密性訊息。
- (3) FPCA 註冊時填寫於註冊相關申請單、合約上的 FPCA 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。
- (4) FRCA 為憑證管理作業之需求而使用與存取 FPCA 資訊時，必須合於業務之需求與嚴謹之安全管控，由業務有權存取之作業人員執行。
- (5) FRCA 管理與使用 FPCA 資訊時，FPCA 之註冊基本資料與身分驗證資料，非經由 FPCA 之允許絕不任意對外銷售、租借與公開。

### 3.8.2 可公開之資訊種類(Type of Information Not considered Confidential)

FRCA 公告於目錄伺服器之 FPCA 憑證資訊，憑證狀態 (提供憑證有效性狀態查詢功能時)，及 FRCA 之憑證資訊、憑證政策、憑證實務作業基準，為可公開之非隱密性資訊。

### 3.8.3 憑證廢止資訊之揭露(Disclosure of Certificate Revocation Information)

FRCA 依據作業規範處理 FPCA 憑證之廢止時，依據「5.4.5 憑證廢止清單產生頻率」之規範，公告於憑證資料庫或目錄伺服器憑證廢止清單(CRL)，供憑證用戶存取使用。

### 3.8.4 依據法令要求之資料提供( Release to Law Enforcement Officials )

除非符合下列之一之條件，否則 FPCA 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，或其他任何人知悉使用：

- (1) 政府法律、規章之規定並經由權責管理單位合法之授權。
- (2) 法院處理因使用憑證產生的糾紛與仲裁而合法之申請需求。



### 3.8.5 民事訴訟之資料提供(Release as Part of Civil Discovery )

FRCA 絕不任意提供 FPCA 之註冊基本資料與身分驗證資料，當因憑證之交易產生民事訴訟而必須存取 FPCA 之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) FPCA 以電子簽章方式或親筆簽名之文件證明方式授權。

### 3.8.6 憑證用戶之資料提供( Disclosure upon Owner's Request )

FRCA 所保存及保護之憑證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之需要而經合法之申請，絕不任意予第三者知悉。

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

除了政府法令規章之需求、或 FPCA 自己之授權需求、或 FRCA 合法用途且正式申請外，FRCA 目前尚無公告 FPCA 資訊之其他公告條件。

## 3.9 智慧財產權( Intellectual Property Rights )

本公司於 FRCA 憑證系統所使用之硬、軟體系統與相關設備及相關作業手冊，其智慧財產權為各提供廠商所有，但本公司保證皆為合法且擁有使用權，絕無侵害第三者之權利，但如為本公司自行開發之系統與相關作業手冊，則其所有權為本公司所有。

FRCA 憑證政策、憑證實務作業基準、與其他執行憑證管理作業，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。

FPCA 產生之私密金鑰與公開金鑰之智慧財產權屬於 FPCA，但公開金鑰經 FRCA 簽發成憑證格式，該憑證之智慧財產權屬於 FRCA。FRCA 只提供 FPCA 與信賴憑證者公開金鑰憑證之使用權限。

FRCA 產生之 FRCA 憑證之智慧財產權屬於 FRCA。FRCA 只提供 FPCA 與信賴憑證者使用之權限。

FRCA 尊重置於 X.509 V3 憑證內憑證用戶識別名稱欄位所存放之 FPCA 註冊名稱之註冊商標，但不保證 FPCA 註冊名稱之智慧財產權之歸屬，FPCA 之註冊商標如果於註冊時已為先前申請者佔用時，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 FRCA 之管轄權責，FPCA 必須向相關之業務主管機關提出申請。

## 4. 識別與驗證(Identification and Authentication)

### 4.1 註冊(Initial Registration)

FRCA 於 FPCA 註冊時，應依據「4.1.8 公司組織身分之驗證(Authentication of Organisation Identity)」作業規範，驗證 FPCA 申請之證明文件，正確之驗證 FPCA 之資格。FPCA 向 FRCA 申請憑證簽發時，必須依據本作業基準規範「5.1 憑證之申請(Certificates Application)」處理，即為 FPCA 必須先完成註冊作業程序。

#### 4.1.1 識別名稱之種類(Type of Names)

FRCA 憑證系統產生或處理 X.509 V3(ISO 9594-8)憑證之 FPCA 主要識別名稱 (SubjectName) (例如：FPCA 之營利事業統一編號) 採用 X.501(ISO 9594-2) Distinguished Name(DN)之命名方式，其參考格式如下：

|                      |
|----------------------|
| 識別名稱(DN)             |
| X.501 DN             |
| X.501 用戶主要識別名稱 (必要性) |
| SubjectName          |

#### 4.1.2 識別名稱之意義( Need for Names to be Meaningful )

識別名稱欄位中所存放之用戶識別資訊，皆存放具有意義之資訊，絕無存放匿名之名稱。

#### 4.1.3 各種識別名稱之規範 (Rules for Interpreting Various Name Forms)

下為自簽 Root 憑證之識別名稱之說明：

| 識別名稱(DN)               | 說 明      | 內 容(範例)                      |
|------------------------|----------|------------------------------|
| 1.Country(C)           | 公司所在國家   | C = TW                       |
| 2.Organization(O)      | 公司英文名稱   | O = TaiCA                    |
| 3.OrganizationUnit(OU) | 憑證機構所屬性質 | OU = Root CA                 |
| 4.CommonName(CN)       | 憑證機構英文名稱 | CN = TaiCA Financial Root CA |

下為簽發 Policy CA 識別名稱之說明：

| 識別名稱(DN)               | 說 明      | 內 容(範例)                        |
|------------------------|----------|--------------------------------|
| 1.Country(C)           | 公司所在國家   | C = TW                         |
| 2.Organization(O)      | 公司英文名稱   | O = TaiCA                      |
| 3.OrganizationUnit(OU) | 憑證機構所屬性質 | OU = Policy CA                 |
| 4.CommonName(CN)       | 憑證機構英文名稱 | CN = TaiCA Financial Policy CA |

#### 4.1.4 識別名稱之唯一性(Uniqueness of Names)

FRCA 憑證使用之公司註冊中、英文名稱、FPCA 中、英文名稱及識別名稱於憑證系統中必須為唯一，但當 FPCA 有相同之註冊名稱或識別名稱時，以先申請註

冊之 FPCA 優先使用，後申請者於註冊名稱後加區分欄位碼以資區別與識別不同之 FPCA。

#### 4.1.5 識別名稱糾紛之處理(Name Claim Dispute Resolution Procedures)

當 FPCA 使用之識別名稱有相同時，FRCA 以先申請註冊之 FPCA 優先使用，相關之糾紛仲裁處理非為 FRCA 之管轄權責，FPCA 必須向憑證政策管理委員會提出申請。

當 FPCA 使用之識別名稱，經有權主管機關合法文件證實為其他申請者所擁有時，FRCA 即刻註銷先前使用者之 FPCA 識別名稱使用權，該使用者必須負擔相關之法律權責；且驗證該 FPCA 註冊識別名稱使用之合法性，非為 FRCA 之業務權責範圍。

#### 4.1.6 註冊商標之認可與驗證(Recognition, Authentication and role of Trademarks)

FRCA 尊重 FPCA 識別名稱有關註冊公司中、英文名稱之註冊商標權，並接受 FPCA 之使用，但不保證 FPCA 註冊商標之認可、驗證與唯一性，相關之糾紛仲裁處理非為 FRCA 之管轄權責範圍，FPCA 必須向相關之業務主管機關提出申請。

#### 4.1.7 私密金鑰之驗證方法(Method to Prove Possession of Private Key)

FRCA 必須驗證 FPCA 私密金鑰擁有之合法性與正確性，至少須以如下所述之任一方法驗證 FPCA 所擁有之私密金鑰：

- (1) 於 FPCA 申請憑證，以 FPCA 私密金鑰執行 FPCA 憑證申請訊息之簽章時，FRCA 必須驗證 FPCA 憑證申請訊息內，經保護之 FPCA 身分資訊、公開金鑰與私密金鑰之正確性與唯一性及合法性。
- (2) FPCA 除以簽章方式驗證私密金鑰擁有之合法性與正確性外，亦可由 FRCA 以 FPCA 之公開金鑰將訊息亂碼加密後，經數位信封之方式傳遞至 FPCA，FPCA 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 FRCA，且經 FRCA 驗證無誤。

#### 4.1.8 公司組織身分之驗證(Authentication of Organisation Identity)

FRCA 處理 FPCA 註冊身分與識別名稱之驗證時，FPCA 必須提供主管機關或合法授權單位核發之相關證明文件（影本必須加蓋公司章與負責人之簽名），如為公司授權代理人辦理，並需驗證該授權代理人之相關身分證明文件。

### 4.2 憑證及私密金鑰之更新(Routine Rekey)

FPCA 金鑰之生命週期為十一年，FPCA 金鑰到期後必須更新(重新產生一組公開金鑰及私密金鑰對)，並向 FRCA 申請憑證簽發，此為私密金鑰之更新 (Rekey)。FPCA 憑證申請程序依據「5.1 憑證申請(Certificates Application)」之規範處理。

當 FPCA 與憑證有關之註冊訊息有異動或私密金鑰有安全顧慮時，必須重新註冊、產生新公開金鑰對，並向 FRCA 申請新憑證之簽發。為風險管理與安全考量，FPCA 向 FRCA 申請新憑證簽發時，不可使用舊公開金鑰對。

#### 4.3 廢止憑證之私密金鑰之更新(Rekey after Revocation )

FRCA 不提供 FPCA 廢止憑證之私密金鑰之更新，FPCA 必須重新執行註冊之身分確認，與重新產生新公開金鑰對，並向 FRCA 申請新憑證之簽發。

#### 4.4 憑證廢止需求(Revocation Request )

憑證廢止作業依「5.4 憑證之廢止」內容辦理。

## 5. 憑證系統管理(Operation Requirements)

### 5.1 憑證之申請(Certificates Application)

(1) 起始申請：FPCA 檢具相關證明文件及填寫申請表，向 FRCA 提出申請。

FPCA 應確實瞭解申請單與合約書上之權利與義務規範，FPCA 相關業務運作之作業流程，並於同意後確認。

FPCA 應正確且詳實之填寫相關申請單並提供相關證明文件。FPCA 必須提供公司合法且正確之證明文件（例如公司之營利事業登記證）、一般相關資訊之檢核，同時須由公司代表人或持有授權文件之代理人親自辦理。

(2) 身分識別與驗證程序：FRCA 依據「4.1.8 公司組織身分之驗證(Authentication of Organisation Identity)」進行 FPCA 之身分識別與驗證。

(3) 申請註冊作業處理程序：

FPCA 產生公開金鑰對及 PKCS#10 憑證申請檔，向 FRCA 申請憑證之簽發。

FRCA 驗證 FPCA 身分與證明文件無誤後，即完成 FPCA 註冊申請作業。

#### 5.1.1 憑證申請政策(Certificate Application Policy)

(1) 新憑證申請：FPCA 依據「5.1 憑證申請(Certificates Application)」之作業規範，向 FRCA 申請新憑證之簽發。

(2) 憑證展期：FRCA 不提供 FPCA 憑證展期作業，FPCA 憑證之使用有效期限將屆滿或已過期時，FPCA 必須重新產生新公開金鑰對向 FRCA 申請憑證簽發。

(3) 憑證廢止：FPCA 憑證廢止後，不允許繼續向 FRCA 申請憑證簽發，必須重新執行 FPCA 註冊之身分確認，與重新產生新公開金鑰對，才可向 FRCA 申請新憑證之簽發。

#### 5.1.2 憑證展期策略(Certificate Extend Policy)

(1) 為風險及安全管理考量，FRCA 不提供憑證展期之功能。

(2) FPCA 憑證之使用有效期限將屆滿或已過期時，FPCA 必須重新產生新公開金鑰對向 FRCA 申請憑證簽發，以代替憑證更新之功能。

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

FRCA 不提供 FPCA 憑證暫時停用服務。

### 5.2 憑證之簽發(Certificates Issuance)

FRCA 簽發憑證之作業規範如下：

(1) FRCA 於接收到 FPCA 之憑證申請訊息時，驗證憑證申請訊息之完整性及有效性（例如：FPCA 簽章），正確無誤後，簽發憑證予 FPCA。

(2) FRCA 憑證管理系統為離線作業，作業人員依循「6.2 作業程序控管(Procedure Control)」之安控規範，以人工作業方式簽發 FPCA 憑證。

(3) FRCA 於產生 FPCA 憑證後，即刻更新資料庫與目錄伺服器之憑證資訊

供 FPCA 查詢使用。

- (4) 當 FPCA 憑證申請訊息為 FRCA 拒絕時，此失敗交易 FRCA 必須立刻通知 FPCA；惟交易失敗之原因，FRCA 應以電子郵件方式或電話或其他適當方式告知 FPCA；若主管機關或相關法律有特別規範則不在此限。

### 5.3 憑證之啟用 (Certificates Acceptance and Using)

#### 5.3.1 憑證之啟用(Certificates Acceptance)

FPCA 申請憑證簽發完成且向 FRCA 取得憑證時，FPCA 應依下列規定處理：

- (1) 確認憑證內容之 FPCA 相關資訊與 FPCA 註冊時之一致性，且為 FPCA 之正確資訊。
- (2) FPCA 憑證之公開金鑰與所對應之私密金鑰為相關之一組且為 FPCA 所擁有。
- (3) FPCA 必須驗證 FRCA 憑證鏈中每張憑證之有效性及合法性，如：該憑證是否已廢止、憑證有效期限是否已結束、是否為合法且正確之 FRCA 所簽發。
- (4) FPCA 於接受所申請之憑證後，即是接受本作業基準、憑證政策與合約上之權利與義務之關係。
- (5) 當憑證之公開金鑰與申請者憑證請求不一致或憑證之欄位未依憑證實務作業基準核發時，憑證申請者得以拒絕，憑證管理中心應廢除該憑證。

#### 5.3.2 憑證之使用(Certificates Using)

憑證使用之範圍依本作業基準、FPCA 與 FRCA 之合約規定，FPCA 使用憑證時：

- (1) FPCA 必須妥善保管及儲存與憑證相關之私密金鑰，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 FRCA 憑證鏈中每張憑證及該憑證之有效性及合法性外（該憑證是否已廢止、憑證有效期限是否已結束、是否為合法且正確之憑證擁有者），且需依各憑證使用業務相關安控之規範檢核憑證相關欄位之正確性。
- (3) FPCA 憑證以公開金鑰之方式儲存於業務應用系統中，使用時除存取授權之身分核驗外，必須檢核該憑證之有效性。
- (4) FPCA 使用憑證時，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、賠償額之權利與義務規範，且合法使用於本作業基準、憑證政策與相關業務規範所訂定之範圍。

### 5.4 憑證之廢止(Revocation of Certificate)

#### 5.4.1 憑證廢止時機(Circumstances for Revocation)

FRCA 於 FPCA 之憑證仍為有效期間內，當有下述情況時，得逕行憑證之廢止：

- (1) FRCA 因憑證系統之不適用或憑證系統之整合需求。
- (2) FPCA 使用憑證而為有權第三者(例如:FRCA)宣告未履行應盡義務(例如:費用),或不當使用憑證而違反政府法律、規章、本作業基準或業務使用規範時。
- (3) 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廢止 FPCA 之憑證。

FPCA 於憑證仍為有效期間內,當有下述情況時,必須提出憑證廢止申請:

- (1) 憑證內容之 FPCA 相關資訊有更動時,例如:公司之整合與合併,或因特殊原因而更新公司之註冊名稱。
- (2) 與憑證相關之私密金鑰有毀損、遺失、曝露、被篡改,或有為第三者竊用之疑慮時。
- (3) 憑證內容之 FPCA 相關資訊,不符合本作業基準、憑證政策或業務使用規範時,例如:FPCA 憑證內容與註冊資料不符,或因註冊資料輸入之疏忽。
- (4) FPCA 因業務、財務或其他不可抗拒之因素,而須終止憑證服務結束營運時。

#### 5.4.2 有權廢止憑證者(Who can Request Revocation)

與 FPCA 有關之 FRCA、主管機關或合法授權之第三者與 FPCA 皆有權執行憑證之廢止。

- (1) FRCA 廢止 FPCA 憑證時,必須依照「5.4.1 憑證廢止時機」與相關作業規範辦理。
- (2) FPCA 可依照其需求,依 FRCA 作業規範申請廢止 FPCA 憑證。
- (3) 有權責之第三者申請之廢止 FPCA 憑證:
  - 法院因訴訟與仲裁向 FRCA 提出廢止 FPCA 憑證之申請,FRCA 必須驗證法院正式申請文件之合法性,才接受申請。
  - 其他第三者或主管機關,符合相關法令與規範之申請。

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

- (1) FPCA 因故結束營運管理時,必須依據主管機關電子簽章法、銀行公會之作業規範、及與 FRCA 之合約規範,親自填寫申請表單並簽名確認,或以具有 FPCA 簽章之廢止憑證申請訊息,經由郵寄(限時掛號)或親自向 FRCA 申請廢止該憑證。
- (2) FRCA、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 FRCA 之作業規範,填具廢止申請單向 FRCA 申請廢止該憑證。
- (3) FRCA 接到憑證廢止申請後,應確實驗證申請者之身分、權限及憑證廢止申請之正確性(使用電子郵件、電話或傳真等方式驗證),並留存相關查核紀錄(如:核准人姓名、簽章、核准日期....等)。
- (4) FPCA 進行憑證廢止時,需填具憑證廢止申請表,並需在憑證廢止申請表加註憑證廢止之理由,FRCA 會在廢止憑證後產生的 CRL,加註該憑證

廢止之原因理由。

(5) FRCA 完成 FPCA 憑證廢止作業後，立即更新資料庫或目錄伺服器之憑證資訊，並即刻發函予 FPCA 並告知憑證廢止處理作業已完成。

FRCA 處理廢止 FPCA 憑證之時效性，應至少於二十四小時內完成，其憑證廢止清冊及線上憑證狀態查詢資訊(OCSP)之異動，應留存適當稽核軌跡。

#### 5.4.4 憑證請求廢止之寬限期(Revocation Request Grace Period)

憑證請求廢止之寬限期為 FPCA 向 FRCA 提出憑證廢止申請，至 FRCA 完成廢止憑證作業期間。FRCA 完成 FPCA 憑證廢止請求之驗證後，立即執行廢止憑證之作業。

#### 5.4.5 憑證廢止清單產生頻率(CRL Issuance Frequency)

FRCA 憑證廢止清單(CRL)之產生頻率為每二十四小時產生一次。

#### 5.4.6 憑證廢止清冊查證要求(CRL Checking Requirements)

憑證廢止清冊(CRL)為公開資訊，沒有存取權限的安全管控，FPCA 或信賴憑證者皆可依需求自由存取。

FPCA 或信賴憑證者於業務應用系統有使用憑證時，除驗證雙方憑證之有效性外，尚須檢核該憑證是否為廢止憑證。惟考量業務風險因素，相關業務應用系統可依系統安全度之需求，在一定之時間內主動至 FRCA 索取 CRL。

FPCA 或信賴憑證者之業務應用系統之安全機制如使用線上憑證狀態查詢(Online Certificates Status Protocol, OCSP)之功能時，則無需使用憑證廢止清冊(CRL) 檢核之安全機制。

#### 5.4.7 線上憑證與廢止憑證狀態查證功能(On-line Revocation/Status Checking Availability)

FRCA 統籌管理 FPCA 及 FUCA 最新即時註銷資訊。

FRCA 提供 FPCA 及 FUCA 線上即時憑證狀態查詢服務(OCSP)。

#### 5.4.8 線上廢止憑證查證要求(On-line Revocation Checking Requirement)

如「5.4.6 憑證廢止清冊查證要求」與「5.4.7 線上憑證與廢止憑證狀態查證功能」之說明。

#### 5.4.9 其他格式廢止憑證通知之功能(Other Forms of Revocation Advertisements Available)

FRCA 除 X.509 V3 CRL 格式之憑證廢止清冊外，目前不提供其他格式之廢止憑證通知功能。



#### 5.4.10 其他格式廢止憑證通知之查核需求(Checking Requirements for Other Forms of Revocation Advertisements)

FRCA 目前不提供其他格式廢止憑證之查核。

#### 5.4.11 金鑰危害之特殊要求(Special Requirements Re Key Compromise)

金鑰更新有安全顧慮時之作業規範，皆依照「5.7 金鑰變更」之規範處理。

### 5.5 安全稽核(Security Audit Procedures)

FRCA 憑證作業營運，由實體設備之操作到憑證作業系統之執行，皆須確實留存相關作業文件及交易或操作稽核紀錄，作為執行稽核憑證系統安全控管之文件資訊依據，並且依 FRCA 之稽核作業規範，確實執行憑證系統運作之稽核作業。

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

FRCA 稽核紀錄至少應保存如下之資訊：

- (1) FPCA 註冊或註銷資訊之保存，包含合約、註冊文件、申請表單與註冊交易相關訊息。
- (2) 憑證系統運作使用之相關公開金鑰(RSA key)與基碼(3DES key)或其他基碼之產生、建置、變更之成功與失敗之記錄。
- (3) FRCA 金鑰與憑證之產生、建置、變更之成功與失敗之記錄。
- (4) FPCA 憑證申請交易處理與回覆之成功與失敗記錄。
- (5) 憑證系統運作之稽核之相關紀錄，與憑證系統運作相關之通訊(E-mail)紀錄。
- (6) 憑證廢止申請交易處理與回覆、憑證廢止清冊處理之相關訊息記錄。
- (7) 進出入本公司申請表單，作業人員身分識別 IC 卡進/出 FRCA 機房之紀錄報表，FRCA 機房工作日誌紀錄簿，作業人員執行業務功能之簽名紀錄，作業人員進/出 FRCA 機房監控攝錄影機之媒體紀錄。
- (8) FRCA 主機系統硬、軟體、應用系統，及 FRCA 憑證作業系統之異動申請單與系統異動變更之紀錄，作業人員執行系統參數變更作業之紀錄。

#### 5.5.2 稽核紀錄之檢視頻率(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之查核，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之查核，且應定期依業務需求，由授權的稽核管理人員對稽核紀錄執行查核管理作業。

可能影響系統安全之異常事件稽核紀錄，需由 FRCA 相關之系統與文件紀錄依稽核作業規範詳細查核，且紀錄事件之查核、處理過程，及追蹤改善措施之執行。

執行憑證系統運作紀錄之查核時，亦查核稽核紀錄是否為非授權作業人員修改，並紀錄事件之查核、處理過程，及追蹤改善措施之執行。

#### 5.5.3 稽核紀錄之保存期限(Retention Period for Audit Log)

相關稽核紀錄報表與媒體資料至少應保留十年；異常狀況之系統紀錄及報表至

少應保留十二年，並於 FRCA 所在處所保留至少二個月資料；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 稽核紀錄之保護(Protection of Audit Log)

FRCA 憑證系統之稽核紀錄資訊之保護措施，依憑證系統所提供之安全控管措施保護稽核紀錄，具有資源控管與身分識別之安全機制。

稽核紀錄由權責獨立之授權人員執行備份作業，該人員只具有稽核紀錄之讀取功能，稽核紀錄至少每週執行備份一次，且另儲存一份備份資料於具安全管控之異地備援中心。

憑證系統之稽核紀錄資訊之保護，為只可讀取且無法寫入與清除之安全管控系統所保護，且只有與業務有關之稽核人員才可以讀取。

文件稽核紀錄留存之執行，亦具有安控措施之保護，且另儲存一份備份資料於具安全管控之異地備援中心。

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

FRCA 憑證系統之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之整理與備份，稽核紀錄資訊檔備份之媒體，並運送一份至具安全管控措施之異地備援中心。

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

各種稽核紀錄之蒐集由憑證系統開啟至系統關閉為止，FRCA 憑證系統稽核紀錄之蒐集，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之方式紀錄之，當自動稽核紀錄功能無法正常運作且 FRCA 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<br>(電腦自動或人員手動) | 紀錄者       |
|----------------------------|---------------------|-----------|
| 1.作業系統安全參數之變更              | 自動                  | 作業系統      |
| 2.憑證系統之開啟與關閉               | 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)之建置、修改與刪除      | 自動                  | 作業系統      |
| 5. FRCA 系統建置與變更            | 自動                  | FRCA 憑證系統 |
| 6.金鑰與憑證之產生、簽發與廢止           | 自動                  | FRCA 憑證系統 |
| 7.憑證用戶資訊之建置、修改與刪除          | 自動                  | FRCA 憑證系統 |
| 8.經網際網路之交易資訊               | 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.系統環境參數檔之變更              | 人工                  | 作業人員      |
| 11.硬體與軟體系統之更新              | 人工                  | 作業人員      |
| 12.系統維護                    | 人工                  | 作業人員      |
| 13.人員之異動                   | 人工                  | 作業人員      |
| 14.其他憑證系統運作之相關表單           | 人工                  | 作業人員      |

### 5.5.7 異常狀況之通知(Notification to Event-Causing Subject)

作業人員於執行 FRCA 憑證系統，出現影響安全控管措施之異常事件時，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之處理措施，但並不告知引發該事件之個體，該事件已被系統所紀錄。

### 5.5.8 弱點評估(Vulnerability Assessments)

對於執行憑證系統運作時，內部與外部可能造成之威脅與風險之評估，經由稽核紀錄之查核及監控追蹤，隨時調整與修改憑證系統運作之安全控管措施，以便將系統運作之風險降至最低，且每年至少應執行一次。

## 5.6 紀錄留存(Records Archival)

### 5.6.1 事件紀錄之種類(Types of Event Records)

FRCA 為使憑證作業系統能穩定之運作，必須將系統環境建置檔、與 FPCA 相關合約條款、FPCA 註冊資料之相關資訊、FPCA 憑證及廢止憑證資料檔、交易資料檔、稽核資料檔、FRCA 金鑰與憑證變更資訊、憑證實務作業基準、憑證政策、FRCA 憑證應用系統及其他稽核人員要求等之資料執行備份保存。

### 5.6.2 紀錄留存期限(Retention Period for Archive )

除配合主管機關訂定之資訊保存期限規範，FRCA 訂定公開金鑰系統運作有關資訊之保存期限至少如下：

- (1) 憑證實務作業基準、憑證政策與相關作業手冊、及 FPCA 註冊申請表單相關合約條款、FPCA 之廢止憑證或過期憑證，至少保留至憑證有效期限結束後十年。
- (2) FPCA 憑證申請、查詢與憑證廢止之交易訊息紀錄，至少保留至憑證有效期限結束後十年。
- (3) FPCA 金鑰與憑證相關之異動資料至少保留十年。
- (4) FRCA 金鑰與憑證等相關之異動資料至少保留十年。

### 5.6.3 留存記錄之保護(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之保護，皆儲存於具安全管控措施且有防潮濕、防靜電感應之中央空調之保護環境下，非授權人員無法存取，非合乎相關法律與作業規範之需求，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、防靜電感應之中央空調環境下之異地備援中心。

### 5.6.4 留存記錄之備援程序(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之作業程序，每日、週、月之整理歸檔及備份，一份儲存於 FRCA 具安全管控措施之環境下，且一份

保存資料儲存於具安全管控措施之異地備援環境，當憑證管理系統異常無法開啟時，依系統備份與回復作業手冊，及保存之備份資料，執行憑證系統之異常回復作業。

#### 5.6.5 紀錄之時戳要求(Requirements for Time-Stamping of Records)

FRCA 於憑證系統運作時，有關之硬軟體設施與系統，或系統參數與系統資源之變更異動，皆有時序之註記，如由電腦作業系統或憑證系統自動產生時，時戳(time-stamp)由電腦之時鐘讀取而自動加入紀錄資訊內，如是由作業人員產生之紀錄資訊，則由作業人員手寫加入作業表單紀錄資訊內，以作為日後追蹤時之時間參考依據。

FPCA 於執行註冊、憑證申請、憑證廢止與查詢等有關之作業時，交易之訊息內容具有時序之註記，是經由電腦作業系統或憑證系統自動產生，時戳(time-stamp)由電腦之時鐘讀取而自動加入紀錄資訊內。

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

FRCA 憑證系統作業相關之保存紀錄資訊，皆由 FRCA 內部之作業人員執行，內部之相關系統於具有資源權責獨立及安全之管控措施下產生；稽核紀錄蒐集之保存資訊亦是由內部之管控系統所產生，憑證系統運作之相關文件保存紀錄，由權責之業務相關人員蒐集與管理。

#### 5.6.7 留存記錄之取得與驗證程序(Procedure to Obtain and Verify Archive Information)

FRCA 憑證系統作業相關之保存紀錄資訊之驗證，依 FRCA 之內部管理作業規範，至少一年一次或依據業務之需求不定期抽查驗證，或執行保存紀錄資訊之驗證稽核作業時，由權責之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，執行保存紀錄之驗證。

### 5.7 金鑰變更(Key Changeover)

#### 5.7.1 FPCA 金鑰變更(Key Changeover of FPCA)

FPCA 憑證有效期限為十一年，因 FPCA 簽發下層 FUCA 之憑證效期最長為五年，FPCA 需於 FPCA 憑證生效第六年時進行金鑰更新程序，FPCA 需產生下一組新金鑰對及相對之憑證申請檔，並向 FRCA 申請新憑證的簽發。FPCA 依據「5.1 憑證申請(Certificates Application)」之作業規範，向 FRCA 申請新憑證之簽發。

#### 5.7.2 FRCA 金鑰變更(Key Changeover of FRCA)

FRCA 憑證有效期限為十七年，因 FRCA 簽發下層 FPCA 之憑證效期最長為十一年，FRCA 需於 FRCA 憑證生效第六年時進行金鑰更新程序，FRCA 需產生下一組新金鑰對及下一張的自簽憑證，並以此新憑證產生此張新憑證的指紋辨識碼(fingerprint)。

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

本公司為使 FRCA 憑證系統，於異常狀況或天災與地變時，能於最短之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之網路及軟、硬體備援系統、憑證系統異常狀況時之回復計劃外，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之功能。

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

FRCA 憑證系統使用之電腦軟體資源、或憑證系統運作相關之資料有異常毀損時，依照系統備份與回復作業手冊，可以由內部備份媒體資料、或移送異地之備份媒體資料執行憑證管理系統之復原作業，使系統能繼續且正常營運。

當 FRCA 憑證系統使用之電腦硬體資源異常毀損時，可以由內部之硬體備援設備，與相關之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。

FRCA 內部復原程序應於六個小時內完成，若無法於六小時之內恢復正常作業，FRCA 應啟動異地備援機制，並於二十四小時內完成災難復原程序。

### 5.8.2 金融政策憑證管理中心公開金鑰廢止之復原程序(FPCA Public Key is Revoked)

當 FPCA 符合「5.4.1 憑證廢止時機(Circumstances for Revocation) (4)(5)(6)(7)」所述之時機時，應向 FRCA 提出憑證廢止申請，同時廢止其公開及私密金鑰。FPCA 公開金鑰廢止之復原程序依照「5.8.3 FRCA & FPCA 私密金鑰之破解處理程序(FPCA & FRCA Private Key is Compromised) (2)」之作業規範辦理。

### 5.8.3 FRCA & FPCA 私密金鑰之破解處理程序(FPCA & FRCA Private Key is Compromised)

FRCA 私密金鑰有毀損、遺失、曝露、被篡改，或有為第三者竊用之疑慮時，應立即向銀行公會申告，並廢止所有由 FRCA 簽發之 FPCA 憑證，更新 CRL 或 OCSP 資料，以供憑證用戶或信賴憑證者查詢。同時 FRCA 產生下一組新金鑰對及下一張的自簽憑證，並以此新憑證產生此張新憑證的指紋辨識碼(fingerprint)。

FRCA 產生新憑證後，依據「5.1 憑證申請(Certificates Application)」及「5.2 憑證之簽發(Certificates Issuance)」之作業規範，重新簽發 FPCA 之憑證。

FRCA 新產生之公開金鑰，依據「7.1.4 FRCA 公開金鑰之遞送(FPCA Public Key Delivery to Users)」之規範，遞送給 FPCA。

FPCA 私密金鑰有毀損、遺失、曝露、被篡改，或有為第三者竊用之疑慮時，應依據本作業基準「5.4 金鑰之廢止(Revocation of Certificate)」之程序，立即向 FRCA 申告，並產生下一組新金鑰對及相對之憑證申請檔，並依據「5.1 憑證申請(Certificates Application)」之作業規範向 FRCA 申請新憑證的簽發。

#### 5.8.4 設備之安全維護(Secure Facility after a Natural or Other Type Disaster )

FRCA 憑證系統運作所使用之相關安全設施，若於天災與地變時毀損：

- (1) 如果在回復使用之相關安全設施至正常運轉之前，不會影響憑證系統之運作，則儘速修護或更新至正常運轉狀態，不至於影響憑證系統之正常運作。
- (2) 當足以造成憑證系統運作之危害時，必須立刻緊急關閉憑證系統之運作，且儘速修護或更新相關安全設施至正常運轉狀態，才開啟憑證系統之運作，如果於作業規範之時間內無法修護或更新相關之安全設施時，則必須執行異地災變復原計劃，於異地正式開啟憑證系統之營運作業。
- (3) 如發生之災變已嚴重損害憑證系統運作使用之相關安全設施時，則必須立即執行異地災變復原計劃，回復憑證管理系統之運作功能。

#### 5.8.5 業務永續及災害復原計劃(Contingency and Disaster Recovery Plan)

為避免因天災與地變而造成 FRCA 憑證系統運作之停頓，本公司已規劃與建置一套於異地之業務回復作業計劃，及異地災變備援之復原系統，將憑證系統運作所需要硬軟體系統與設施、憑證資訊相關之媒體、文件及作業規範與業務系統回復文件，於離開 FRCA 營運系統適當距離處之異地備援中心，建置系統與儲存媒體與文件。

異地災變備援之業務復原系統，依業務需求每年至少一次以上，執行災變復原計劃之人員訓練與測試，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之查核，以期達成當有異常天災或地變時，FRCA 憑證系統之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之影響風險減少至最低。

#### 5.9 FRCA 結束營運(FRCA Termination)

FRCA 因故結束其系統營運時，需對業務系統運作之影響減少至最低程度。

於業務結束而無安全之考量因素時：

- (1) 於終止服務之日一個月前通報主管機關及銀行公會。
- (2) 於終止服務之日一個月前，將終止服務之事實通知用戶。
- (3) 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。
- (4) 於高度安全且無安全顧慮之作業環境下，廢止 FRCA 與全部用戶之憑證，將結束之 FRCA 相關私密金鑰與憑證及全部用戶憑證，移轉至接任之憑證管理中心。
- (5) 將憑證政策、憑證實務作業基準、憑證管理中心相關作業手冊文件、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，移轉至承接的憑證管理中心，至少妥善安全的保存七年。
- (6) 將 FRCA 之相關私密金鑰完全清除乾淨，並向用戶正式宣告，憑證業務已移轉至承接的憑證管理中心繼續營運，且儘可能的協助接任者執行憑證業務憑證的簽發。

於業務異常結束（法院宣告破產、或不合法）時，FRCA 必須儘早向 FPCA 公告事

實，且必須執行如業務正常結束時的作業程序，將對 FPCA 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)

FRCA 憑證作業系統建置於安全穩固之建築物及獨立之硬軟體作業環境。只有被授權之作業人員，才可以依照安全控管之作業規範進入執行憑證管理相關作業，密碼模組亦必須存放於有安全控管措施之環境下，避免被破壞或未經過授權之使用。

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

FRCA 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，詳述如下列章節。

##### 6.1.2 門禁管制(Physical Access)

作業人員進入 FRCA 機房必須有三道 IC 卡及指紋識別門禁之身分查核識別管制，且必須兩人以上才可進入(單獨一人無法開啟進出)，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。

FRCA 運作之相關私密金鑰、備份資料皆妥善、安全之存放於此 FRCA 設有監控錄影系統保護之保險櫃內，FRCA 憑證系統運作之相關作業人員，執行憑證管理作業時，皆有監控錄影設備之監測。

FRCA 運作之硬軟體及密碼模組皆置於有監控錄影系統保護之環境下，憑證系統安全控管人員，執行金鑰管理相關作業時，皆有監控錄影設備之監測。

##### 6.1.3 電力與空調(Power and Air-Condition)

FRCA 設有柴油發電機及不中斷電系統(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。

FRCA 具備獨立之空調系統，以確保系統運作之穩定與提供最佳之工作環境。

##### 6.1.4 水災之防範(Water Exposures)

FRCA 憑證系統之房屋為密閉式建築物，除內部可進出之出入口外，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 火災之防範(Fire Prevention and Protection)

FRCA 之機房具芮氏地震五級之防震功能，建築物之材質為防火材質並配置具有中央監控系統之 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、防靜電干擾之設備與環境，重要資料媒



體則儲存具高度防火功能之保險櫃，其中一份備份資訊之媒體儲存於具有安全管控措施之異地備援中心。備份及保存資訊的儲存媒體，必須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)

FRCA 於憑證系統所使用之硬體設備、磁碟機與密碼模組等，於廢棄不使用時，商業敏感性及隱密性資訊必須經過安全之清除與銷毀，且經由稽核單位之驗證，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之銷毀，該資訊皆無法回復與存取使用，且經由稽核單位之驗證，並留存查核文件。

### 6.1.8 異地備份(Off-Site Backup)

FRCA 憑證系統運作所須之相關媒體資訊、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之異地備援環境。

FRCA 憑證系統每日之交易備份紀錄檔，每週完整之系統備份紀錄檔，皆備份後儲存於高度安全管控之異地，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)

FRCA 於公開金鑰基礎建設之架構下，簽發之憑證必須在具備嚴密性、與安全性之作業流程下之憑證系統，由 FRCA 扮演之可信賴且具公信力之機構，公正與嚴謹之執行。

因此 FRCA 作業人員之工作指派，均依作業規範選用適任且職責獨立之可信賴人員，於具有安全控管機制之憑證系統下，依照 FRCA 內部憑證作業規範及作業手冊，確實執行業務。

FRCA 於憑證系統之運作上，為使職務與權責之區分，及職務之備援功能不危及整體系統之安全性與營運之完整性，各業務可信賴之執行人員與職務詳述如下。

- (1) 經理負責管理、監督 FRCA 整個憑證系統業務之營運。
- (2) 稽核人員(本公司非屬 FRCA 之作業人員)，負責稽核、監督 FRCA 憑證系統業務之運作工作內容詳「5.5 安全稽核」。
- (3) FRCA 憑證系統業務營運之監督人員，至少二名以上互為業務上之備援，負責系統運作資源之管理與授權（例如：作業人員之授權與建置，系統資源之異動與調整，但不可執行憑證簽發之相關業務運作）。
- (4) FRCA 憑證系統業務營運之管理人員，至少二名以上互為業務上之備援，負責系統運作時相關系統規範、環境參數之設定及管理性功能之作業（例如：FRCA 金鑰及憑證之變更，但不可以執行 FPCA 憑證簽發、FPCA 資料建

置等作業)。

- (5) FRCA 憑證系統業務營運之操作人員，負責系統運作時 FPCA 資料建置、執行憑證簽發等相關作業及報表與批次作業。
- (6) 其他 FRCA 硬軟體系統之維護人員，密碼模組系統作業人員，系統資源控管人員負責其授權之相關作業。

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

FRCA 執行各種業務之作業人員，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之維護人員，密碼模組系統作業人員不同業務之特性指派適當數目之人員擔任，例如 FRCA 金鑰之建置或變更、FPCA 資訊之異動等相關作業皆有二位以上之作業人員才可以執行，金鑰基碼建置之作業人員則必須依照金鑰作業安全控管程序之規定，至少需二位以上之金鑰安全管理人員，同時進行才可以變更與建置且有相互備援之功能。

### 6.2.3 角色之識別與驗證(Identification and Authentication for Each Role)

FRCA 執行各種業務之監督人員、管理人員、操作人員、系統維護人員與系統資源控管人員，於系統資源之使用上皆有一組依業務區分，而且是唯一之身分識別碼，與 IC 卡及相關之身分識別驗證密碼（或是指紋辨識驗證），以達到系統資源使用者之身分識別與驗證，且相關作業人員依業務需求執行之作業功能，每筆皆有詳細之紀錄，確保系統資源使用之可稽核性，與系統安全威脅及風險評估之管控。

## 6.3 人員控管(Personnel Control)

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

- (1) FRCA 憑證系統執行各種業務之作業人員，必須具備忠實、可信賴及工作之熱誠度，無影響憑證作業之其他兼職工作，無憑證作業上因工作之疏失、不盡責之缺失紀錄，無違法犯紀之不良紀錄。
- (2) 作業人員，至少具備憑證作業之實務經驗，或經過憑證相關作業之訓練而通過測驗者，必須由本公司選派適當人員擔任。
- (3) 管理人員與監督人員，至少具備憑證作業之實務經驗，具有電腦系統規劃、開發、營運管理之經驗更佳，且必須由本公司選派適當人員擔任。

### 6.3.2 資格審查程序(Background Check Procedures)

FRCA 系統運作之人員，由人事管理相關部門依監督人員、管理人員、作業人員所訂定之審核規範，執行身分背景安全之審查，以及部門相關作業之實務與經歷之審查通過後，始可任職，且每年必須依各種作業人員之職務特性，執行安全、實務與經歷之審查，為該員是否適任相關之工作以作為執行工作調整或調派之依據。

### 6.3.3 教育訓練(Training Requirements)

FRCA 系統運作之人員，皆依照其職務，施予 FRCA 系統運作所應具備之軟體功能、作業程序、安控程序、災變備援作業規範、公開金鑰作業及憑證政策與本作業基準與其他資訊安全相關作業規範之訓練，憑證系統有異動或有新系統之加入時，亦需給予適當之教育訓練。

FRCA 需訂定一套 CA 系統有關硬軟體、應用系統與安全管理系統之完整之教育訓練規範，於新進人員雇用或 FRCA 憑證系統有異動時，施行相關技能之教育訓練，教育訓練完成後有詳實之成果紀錄，作為相關作業人員工作委任之參考。

### 6.3.4 再教育之頻率與需求(Retraining Frequency and Requirement )

FRCA 憑證系統運作之相關人員，其執行憑證系統運作之相關知識與技能，每年至少檢討一次，並給予適當之再教育之訓練。

FRCA 憑證系統功能之更新、或新系統之加入、或公開金鑰基礎建設相關知識與技術之進步與更新，皆需對系統運作之相關人員執行教育訓練。

### 6.3.5 職務之輪調(Job Rotation Frequency and Sequence )

配合 FRCA 憑證系統運作之需求與相關作業人員工作之適任性，本公司會選派適任之人選輪調至適合之工作歷練，但調派前必需施以適當知識與技能之教育訓練。

### 6.3.6 非授權作業之懲處(Sanctions for Unauthorized Actions)

FRCA 憑證系統運作之相關作業人員，因故意或疏失而執行非自己職務上之作業時，無論造成或未造成憑證系統安全之問題，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(Contacting Personnel Requirements)

FRCA 因人力資源不足而委由外包人員擔任操作人員時，除必須依照業務之工作內容簽訂相關之保密合約外，該委外人員之權利與義務與 FRCA 之內部操作人員相同，必需施以職務上知識與技能之教育訓練，且遵守相關作業規範與法律規範。

### 6.3.8 作業手冊之提供(Document Supplied to Personnel)

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

- (1) 硬體、軟體作業平台之操作文件、網路系統與網站相關之操作文件、密碼模組系統之操作文件。
- (2) FRCA 憑證系統之相關操作文件。
- (3) 本憑證作業基準、憑證政策及相關作業規範文件，
- (4) FRCA 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 金鑰對之產生與建置(Key Pair Generation and Installation)

#### 7.1.1 金鑰對之產製(Key Pair Generation)

- (1) FRCA 不提供代替 FPCA 產生金鑰對之服務，FPCA 金鑰對應由二位以上獨立之金鑰管理人員，同時登入(log-in)至硬體加密模組，由硬體加密模組直接產生，不允許單獨一人執行金鑰對之產生作業，且私密金鑰於硬體加密模組內產生後，直接經亂碼保護後儲存在模組內。當有使用該私密金鑰執行運算之需求時，須經由硬體加密模組之功能介面直接在模組內執行運算，完成後將執行結果輸出，私密金鑰不可以明碼方式輸出至硬體加密模組外。
- (2) FRCA 金鑰對產製之方式亦如(1)所述。

#### 7.1.2 私密金鑰之遞送(Private Key Delivery to Entity)

FRCA 不提供代替 FPCA 產生金鑰對之服務，故無私密金鑰遞送上安全控管措施之需求。

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

FPCA 以公開金鑰向 FRCA 申請憑證時，該請求訊息內之 FPCA 公開金鑰(public key)具有 FPCA 簽章及 FPCA 身分驗證與訊息完整性之保護。  
憑證申請成功之回覆訊息內，均具有 FRCA 之簽章與訊息完整性之保護。  
FRCA 為最高憑證單位故應有簽證自身之能力，當 FPCA 之公開金鑰遞送至 FRCA 時應有正式的收發程序並保留憑據。

#### 7.1.4 FRCA 公開金鑰之遞送(FRCA Public Key Delivery to Users)

- (1) FRCA 公開金鑰有異動或因 FPCA 查詢而需遞送至 FPCA 時，FRCA 公開金鑰憑證皆有 FRCA 簽章與訊息完整性之保護，經由媒體之郵寄傳遞時亦具有完整之安全控管措施。
- (2) FRCA 需在 FRCA 網站上公布 FRCA 之公開金鑰憑證，且提供識別資訊與驗證完整性資料(如：憑證拇指紋)，並以安全保護方式傳遞公開金鑰憑證(如：SSL 網站識別加密方式)，供信賴憑證者索取。

#### 7.1.5 金鑰長度(Key Sizes)

FRCA 之 RSA 金鑰長度為 2048 bits，FPCA 之 RSA 之金鑰長度為 1024bits，金鑰長度將視銀行公會之規範而調整。

#### 7.1.6 公開金鑰參數之產生(Public Key Parameters Generation)

FRCA RSA 公開金鑰參數之產生與選取，由通過 FIPS 140-1 Level 3 安全等級之亂數產生器(random number generator)產生最佳之質數參數。

### 7.1.7 參數品質之檢核(Parameter Quality Checking)

FRCA 之 RSA 公開金鑰參數品質，由通過 FIPS 140-1 驗證標準，安全等級為 Level 3 之硬體加密模組檢核。

### 7.1.8 金鑰之產生設備(Hardware/Software Key Generation)

FRCA 之金鑰於通過 FIPS 140-1 Level 3 安全等級之硬體加密模組內直接產生。

### 7.1.9 金鑰之使用(Key Usage Purposes)

FRCA 簽發給 FPCA 作為簽章或加密用途之憑證，其用途訂定於 X.509 V3 憑證的標準擴充欄位的金鑰用途欄位(key Usage)，FPCA 必須依照本作業基準與業務應用系統的規範使用於相關之業務上。

## 7.2 私密金鑰之保護(Private Key Protection)

### 7.2.1 密碼模組之標準(Standards for Cryptographic Module)

FRCA 之硬體加密模組，通過 FIPS 140-1 驗證標準，安全等級為 Level 3。

### 7.2.2 私密金鑰之分持控管(Private Key (n out of m) Multi-Person Control)

- (1) FRCA 私密金鑰之產生、建置及變更，皆由至少二位以上之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之產生、建置及變更作業。
- (2) 私密金鑰之相關資訊（例如：IC card）與保護密碼(PIN)，分別由職務獨立之不同管理人員管控，並儲存於具安全管控措施之環境。
- (3) 私密金鑰之備份與保存作業，如果是以部份基碼之方式儲存，則需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之媒體。

### 7.2.3 私密金鑰之託管、回復及保存(Private Key Escrow)

FRCA 不提供 FPCA 私密金鑰之託管、回復及保存服務。

### 7.2.4 私密金鑰之備份(Private Key Backup)

- (1) FRCA 私密金鑰加密後儲存於之硬體加密模組內，備份時至少由二位以上授權人員，將加密亂碼後之私密金鑰備份儲存於媒體。
- (2) 私密金鑰之部份基碼(m of n key parts) 儲存於 IC 卡，並存放於經雙重控管、安全之保險櫃內，由安全控管人員密封保管。
- (3) 私密金鑰之備份至少保留二份，一份存放於本公司保險櫃內，另一份存放於具安全管控之異地備援中心。

### 7.2.5 私密金鑰之留存(Private Key Archival)

FRCA 之私密金鑰經密碼加密機制加密後，或以部份基碼(key component)方

式儲存於具安控措施的保護 IC 卡內，或儲存於介面媒體，並存放於經雙重控管、安全之金庫環境內，私密金鑰之有效期限結束後之保存作業，與使用中之私密金鑰安全管控措施相同，相關之私密金鑰保存作業與「5.6 紀錄保存」之保存作業相同。

#### 7.2.6 私密金鑰之建置(Private Key Entry into Cryptographic Module)

FRCA 之私密金鑰的建置，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，且私密金鑰經亂碼化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預算，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 私密金鑰之開啟(Method of Activating Private Key)

FRCA 儲存於硬體加密模組內之私密金鑰，必須由授權之 2 位以上之金鑰管理人員開啟（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。

#### 7.2.8 私密金鑰之關閉(Method of Deactivating Private Key)

儲存於硬體加密模組內之私密金鑰，必須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。

硬體加密模組或私密金鑰關閉不使用時，皆需儲存於具備安全控管之環境下，未經授權者絕不可以任意存取。

#### 7.2.9 私密金鑰之銷毀(Method of Destroying Private Key)

私密金鑰不再使用時，或相對應之公開金鑰失效、廢止時，其軟體加密模組必須以資料覆蓋方式(Overwrite)清除，硬體加密模組或 IC 卡必須以零數位化(Zero)之覆蓋方式清除。

硬體加密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 金鑰對管理之其他事項(Other Aspects of Key Pair Management)

#### 7.3.1 公開金鑰之留存(Public Key Archival)

公開金鑰之留存，其執行程序及安全措施之需求與憑證之保存相同，期限至少留存七年，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之有效期限(Usage Periods for Public Keys and Private Key)

FRCA 公開金鑰與私密金鑰之有效期限為相同效期。

FRCA 金鑰之有效期限為十七年，FPCA 金鑰之有效期限為十一年。

## 7.4 啟動資訊(Activation Data)

FRCA 所簽發之 FPCA 憑證，FPCA 必須親自領取，不可使用啟動資訊透過網際網路取得憑證。因此 FRCA 不產生 FPCA 之啟動資訊，FRCA 亦無其他啟動資訊。

## 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)

FRCA 憑證系統運作之資訊安全管理系統環境，依據 ISO 27001 資訊安全管理系統標準之規範施行及運作。FRCA 憑證系統之安控措施包含下列作業：

- (1) 身分之識別及驗證管控機制。
- (2) 系統資源及資料庫存取權限控管。
- (3) 安控事件之稽核與紀錄。
- (4) 資料備份與保存之保護措施。
- (5) 人員權責區分。
- (6) 內部作業程序控管。
- (7) 業務永續經營回復機制。
- (8) 使用通過電腦作業系統安全等級認證之平台，及使用通過安全等級認證之憑證系統。

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

FRCA 使用之憑證管理系統，其電腦軟體系統安全等級，符合 ITSEC、TCSEC、CC 或同等級之國際安全標準。

## 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)

FRCA 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 FRCA 憑證系統之資訊安全管理系統環境，遵循 WebTrust program for CA(AICPA/CICA)之標準規範運作。

憑證系統之使用具有嚴謹之管控措施，系統皆經嚴謹之測試驗證後才安裝使用，修改或更新皆有版本之管控、功能測試與記錄，且不定期查核、測試驗證系統之完整性。

硬軟體設備由採購至接收時須有安全之保護措施，具有相關之可查核安全機制（例如：封條、密碼、簽章等安控措施），用來識別設備之未被侵入與異動之完整性，加密設備尤須於安全管控之作業機制下，執行設備之驗證、系統安裝與接收。



硬軟體設備更新提昇後，舊設備捨棄時，必須確認無安全之考量資訊存在。

### 7.7 網路安全控管(Network Security Control)

FRCA 建置防火牆、防入侵偵測系統、防病毒破壞系統與網路資源安全控管系統的保護，只開放與憑證相關的作業功能，其他非 FRCA 所提供的功能或通訊介面，一般使用者均無法使用，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。

FRCA 憑證系統為離線(Off-Line)、獨立之作業管理系統，且需經授權後由業務相關之作業人員才可以人工方式執行作業，單獨一位作業人員絕對無法進行。

### 7.8 密碼模組工程控管(Cryptographic Module Engineering Controls)

FRCA 密碼模組之安全控管機制，符合 FIPS 140-1 Level 3 之安全等級。

## 8. 憑證與憑證廢止清冊格式(Certificates and Certificates Revocation List (CRL) Profiles)

### 8.1 憑證格式(Certificates Profile)

FRCA 憑證系統使用之憑證詳細格式，訂定於各相關之憑證格式剖繪作業規範。

#### 8.1.1 版本( Version Number(s) )

FRCA 憑證系統目前簽發 X.509 V3 格式之憑證，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)

FRCA 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憑證相關之憑證格式剖繪作業規範。

#### 8.1.3 演算法物件識別代碼(Algorithm Object Identifiers)

FRCA 憑證系統使用之演算法物件識別代碼，為 ISO 物件識別代碼(OID)管理單位公告之規範，例如：

| 演算法安全機制 | 演算法(Algorithm)         | 物件識別代碼(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      | 3desEDE-CBC            | 1.2.840.113549.3.7   |
| 雜湊函數    | SHA-1                  | 1.3.14.3.2.26        |

#### 8.1.4 命名格式(Name Forms)

FRCA 憑證系統所簽發之 FPCA 憑證，其識別名稱格式內容皆符合 X.501 Distinguished Name(DN)之命名方式以及中華民國銀行公會公佈之「金融 XML 憑證共通性技術規範」。

#### 8.1.5 命名限制(Name Constraint)

FRCA 憑證系統所簽發之 FPCA 憑證，其識別名稱不允許為匿名或假名之識別名稱，符合中華民國銀行公會公佈之「金融 XML 憑證共通性技術規範」。

#### 8.1.6 憑證政策物件識別代碼(Certificate Policy Object Identifiers)

FRCA 憑證系統依 X.509 V3 規範所簽發之用戶憑證，其憑證政策相關之物件識別代碼(OID)，存放於憑證內憑證政策相關之識別欄位，其物件識別代碼之識別值訂於憑證相關之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之使用(Usage of Policy Constraints Extension)

FRCA 憑證系統有使用憑證政策限制擴充欄位，其作業規範參考憑證相關之憑證格式剖繪作業規範。

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

FRCA 憑證系統有使用憑證政策限制擴充欄位，除存放憑證政策可取得的網址外，尚存放憑證使用時權責說明的簡要聲明(TerseStatement)等資訊。

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

FRCA 憑證系統有使用憑證政策限制擴充欄位，為必要處理的擴充欄位，除存放憑證政策可取得的網址提供用戶能讀取外，使用憑證的簡要聲明必須顯示予憑證用戶讀取與了解。

## 8.2 憑證廢止清冊格式(CRL Profile)

### 8.2.1 版本(Version number(s))

FRCA 憑證系統目前簽發 X.509 V2 格式之廢止憑證，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)

FRCA 憑證系統，於廢止憑證作業有使用憑證廢止清冊擴充欄位，其作業規範參考憑證相關之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)

本作業基準規範之權責管理單位為 FRCA 憑證政策管理委員會，每年至少一次審查該作業規範，確保符合主管機關規範之要求；或因配合業務需求、憑證作業管理系統架構與功能之調整、國際標準規範更新、作業錯誤及憑證用戶適當之建議而適當修改本作業基準之內容，確保本作業基準文件之適用性。

當本作業基準有訂定相關之物件識別代碼(OID)，而本作業基準內容有更新版本時，相對應之物件識別代碼不跟隨異動，只變更版本之序號識別代碼。

本作業規範有建議更新時，必須將詳細之相關文件郵寄或 E-mail 至「2.4 聯絡窗口」，由 FRCA 客服中心處理。

### 9.2 公告與通知策略(Publication and Notification Policies)

經由 FRCA 憑證政策管理委員會審查通過之本作業基準規範，或更新版本之規範，須經主管機關審查通過後，始得公布於 FRCA 之網站。

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

本作業基準之主管機關為經濟部，並依據及受政府與主管機關訂定之電子簽章法、電子簽章法施行細則、憑證實務作業基準應載明事項準則之管轄與監督，且需經主管機關之核定。

## 附錄一(Appendix 1) 詞彙(Glossary)

### (1).網際網路(Internet)

許多不同之電腦網路相互連結，經過標準之通訊協定，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之特性產生之訊息，其依附在電子訊息上，具有與簽名同等之效力，可用以辨識及確認電子文件簽署人之身分，及辨識簽署訊息之完整性。

### (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，以確保資料傳輸之安全。

### (5).解密(decrypt/Decipher)

將經加密後形成人無法辨識其代表意義之訊息，以相關之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之訊息。

### (6).數位簽章(Digital Signature)

數位簽章為電子簽章之一種，係指採用非對稱型之密碼演算法(Asymmetric Cryptosystem)及雜湊函數(Hash Function)，對一定長度之數位訊息壓縮後再以簽署人之私密金鑰予以加密，其相對應之公開金鑰可以驗證此加密後之數位訊息，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之訊息資料之正確性，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之紀錄，內含申請者之註冊識別名稱、公開金鑰、該公開金鑰之有效期限、憑證機構之註冊識別名稱與簽章，及其他用以識別之相關訊息，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). 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)  
憑證機構向所服務之對象公告其執行憑證簽發、廢止、查詢等管理之作業規範及申請程序，內含憑證運作之公開金鑰架構與安全機制、作業規範與程序、憑證機構軟體施行之安全機制、權責之管理及相關之規範。
- (12). 非對稱型之密碼演算法(亂碼系統)(Asymmetric Cryptosystem )  
以電腦為媒介基礎之一種數學演算法，可以產生及使用一組數學運算上相關連之安全金鑰對。其中私密金鑰用以對訊息作簽章，對應之公開金鑰則用以對簽章後之訊息作驗證；公開金鑰亦可用以對訊息作加密，而對應之私密金鑰則用以對加密後之訊息作解密。
- (13). 雜湊函數(Hash Function)  
一種可以將一長串之位元訊息轉換成固定長度位元訊息之數學演算法。相同之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之結果推算出輸入之訊息。
- (14). 簽發憑證(電子認證)(Issue a Certificate) :  
係指憑證機構依 CPS，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). 金融公開金鑰基礎建設(Financial Public Key Infrastructure : FPKI)  
係配合行政院推動電子商務，建立安全之電子交易機制，達成金融憑證共通之目標而設立。
- (16). 金融最高層憑證管理中心(Financial Root Certificate Authority : FRCA)  
為金融公開金鑰基礎建設之最高層憑證管理中心，其簽發之自我簽章憑證乃本基礎建設唯一可信賴根源。

(17).憑證申請者(Certificate Applicant)

請求 CA 簽發憑證之自然人或法人。

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

|         |  |
|---------|--|
| ANS     | American National Standard   |
| CA      | Certification Authority  |
| CC      | Common Criteria  |
| 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 Standardisation/<br>The International Electrotechnical Commission |
| ITSEC   | Information Technology Security Evaluation Criteria  |
| LDAP    | Lightweight Directory Access Protocol  |
| OCSP    | Online Certificates Status Protocol  |
| OID     | Object Identifier  |
| OECD    | Organization for Economic Co-operation and Development   |
| PIN     | Personal Identification number   |
| PKCS    | Public Key Cryptography Standard   |
| PKI     | Public Key Infrastructure  |
| RA      | Registration Authority   |
| RA      | Repository Authority(Directory Authority)  |
| RSA     | Rivest,Shamir,Adleman(encryption algorithm)  |
| FRCA    | Financial Root Certification Authority   |
| FPCA    | Policy Certification Authority   |
| TCSEC   | Trusted Computer System Evaluation Criteria  |
| UCA     | User Certification Authority   |
| URL     | Universal Resource Location  |