金融政策憑證管理中心
憑證實務作業基準
Certification Practices Statement

(第 3.0 版)
Version 3.0

TWCA
臺灣網路認證股份有限公司
TAIWAN-CA INC.

生效日期：中華民國一一〇年八月二十六日
Effective Date： 2021/08/26

本作業基準版本變更紀錄：

版本	生效日期	發行者	備註
1.0	2002/10/30	TaiCA PMA	初版擬訂
1.1	2003/1/7	TaiCA PMA	◎「金融最高層憑證機構」改為「台灣金融最高層憑證管理機構」,「金融政策憑證機構」改為「台灣金融政策憑證機構」。 ◎2.2.1 標準規範(Standards) [新增](3)。 ◎2.3.4 用戶憑證機構(User Certification Authority，UCA) [修改](1)(2)。 ◎2.3.5 註冊中心(Registration Authority，RA) [修改](2)(3)。 ◎7.1.4 TFCA 公開金鑰之遞送(TFCA Public Key Delivery to Users) [新增](2)。 ◎5.1.2 憑證展期策略(Certificate Extend Policy) [新增](2)。 ◎5.4.3 憑證廢止程序(Procedure for Revocation Request) [修改](4)改成(5)，[新增](4)。 ◎ 2.3.2(5)文字修正，新增 2.3.3(5) ◎ 政策管理機構改為政策管理單位
2.0	2008/02/04	TWCA PMA	1. 配合 94 年 8 月中華民國銀行商業同業公會全國聯合會所公布新版「金融公開金鑰基礎建設憑證政策」內容做修訂。 2. 依電子簽章法中名詞規則，將「憑證機構」修訂為「憑證管理中心」。
3.0	2021/08/26	TWCA PMA	配合 108 年 9 月 12 日中華民國銀行商業同業公會全國聯合會所公布新版「金融公開金鑰基礎建設憑證政策」內容做修訂。

目錄

1. 簡介

1.1 概述

臺灣網路認證股份有限公司（Taiwan-CA Inc.，以下簡稱本公司或 TWCA）係由臺灣證券交易所、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機構，本公司據此成立金融最高層憑證管理中心（簡稱 FRCA），並於九十一年十二月二十日銀行公會台灣金融最高層憑證管理機構建置建議書徵求暨資格評選裡載明，金融政策憑證管理中心（簡稱 FPCA）由金融最高層憑證管理中心 (FRCA) 兼任，且協助推動銀行公會 PKI 架構。FPCA 為銀行公會 PKI 架構之金融政策憑證管理中心，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。

FPCA 之憑證用戶為金融用戶憑證管理中心（簡稱 FUCA），FPCA 提供 FUCA 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金融公開金鑰基礎建設憑證政策 (Certificate Policy; CP) 說明 FPCA 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。

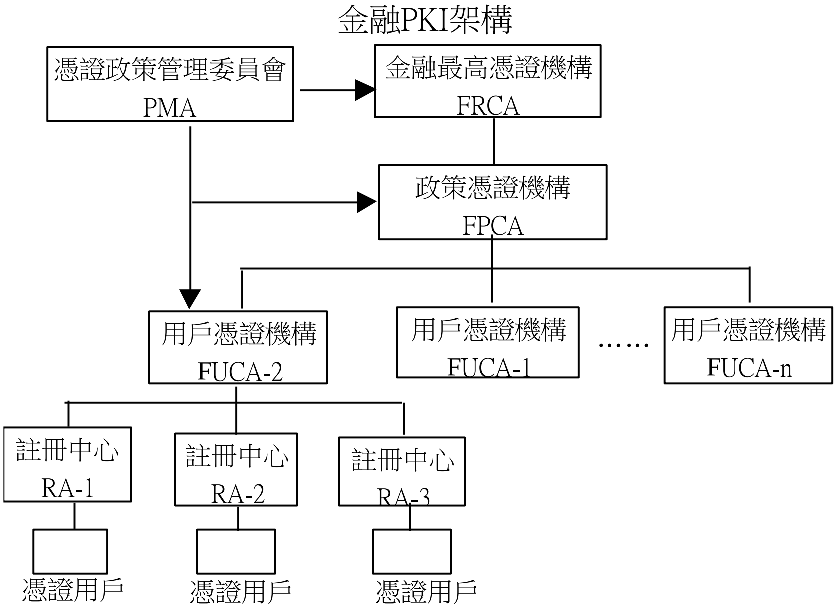
本憑證實務作業基準（以下簡稱本作業基準或 CPS）係依據主管機關經濟部頒布之「憑證實務作業基準應載明事項準則」規範編撰，經主管機關審查核定之文號如下：

110/08/26 經濟部函 經商字第 11002425100 號。

1.2 文件名稱與識別

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。

1.3 金融公開金鑰架構之成員



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 FPCA 之實際營運架構並未包含下列所有單元，FPCA 係指下圖中金融政策憑證管理中心 (FPCA)。

1.3.1 憑證機構 (CA)

1.3.1.1 金融最高層憑證機構 (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、憑證廢止清冊（Certificates Revocation List，以下簡稱 CRL）、線上憑證狀態查詢 (OCSP) 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、OCSP 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管理中心進行交互認證之事宜。

1.3.1.2 金融政策憑證機構 (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 FUCA 憑證、CRL 之作業程序與驗證之作業規範。

(3) 簽發、管理與遞送 FUCA 憑證、CRL 及 FUCA 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 FUCA 系統互通驗證規範,執行 FUCA 系統互通驗證作業。

1.3.1.3 用戶憑證機構 (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。

(5) 管理 RA 註冊名稱、RA 憑證、電子郵箱 (E-mail) 與聯絡之相關資訊。

1.3.2 註冊中心 (RA)

RA 負責:

註冊中心 (Registration Authority; RA) 主要負責鑑別下屬憑證~~機構~~管理中心的身分及簽發憑證所需之相關資訊,供本憑證管理中心簽發下屬憑證~~機構~~管理中心憑證。本憑證管理中心自行擔任註冊中心,不設置其他註冊中心。

1.3.3 憑證用戶 (Subscriber)

本憑證管理中心之用戶為 FUCA。

1.3.4 信賴憑證者 (Relying Party)

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。

1.3.5 其他相關成員

無其他相關成員。

1.4 憑證用途

1.4.1 適用範圍

FPCA 依據本作業基準所規範及簽發的 FUCA 憑證，FUCA 只可使用於簽發憑證予用戶（個人或法人）及 FUCA 之註冊中心之憑證，FUCA 憑證不可使用於其他具商業交易用途之應用。

1.4.2 憑證禁用範圍

FUCA 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。

1.5 政策管理

1.5.1 憑證政策之制定及管理機關

本作業基準之訂定、更新、及發布等事宜，其權責單位為本憑證管理中心。

1.5.2 聯絡資料

FUCA 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。

FUCA 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)
聯絡人	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)	rootca@twca.com.tw

1.5.3 憑證實務作業基準與憑證政策相符之審定

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，須經由本憑證管理中心之評估與審核後始可變更；變更後之作業基準，須送交銀行公會與主管機關審核，經核可後，始可對外公告新版之作業基準。

1.5.4 憑證實務作業基準之審定程序

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，且須經主管機關之核定。

2. 資訊公布及儲存庫責任

2.1 儲存庫

FPCA 之儲存庫提供 FUCA，憑證作業實務與憑證相關作業文件、FUCA 憑證與 FPCA 憑證、廢止憑證清單 (CRL)、FUCA 與 FPCA 資訊之查詢及下載，FPCA 訂定適當之存取管控措施確保儲存庫內資訊之安全性。

儲存庫網址為：https://www.twca.com.tw

2.2 憑證資訊公布

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 FPCA 之網站供用戶下載使用；網址：https://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)
聯絡人	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)	rootca@twca.com.tw

經由 FPCA 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 FPCA 之網站。

儲存庫暫停服務時間之上限，依 5.2.7 節規定辦理。

2.3 公布頻率或時間

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，FPCA 應於接到核定公文一個月內公告於網站 (https://www.twca.com.tw)。

憑證廢止清冊 (CRL)，依據「4.9.7 憑證廢止清冊發布頻率」，每 24 小時產生及公布一次。

2.4 存取控制

FPCA 之儲存庫存取權限的安全管控為公開唯讀，憑證用戶及信賴憑證者可以依需求至 FPCA 的網站下載儲存庫發布之資訊；為防止惡意竄改於更新儲存庫時須進行存取控制。

3. 識別及驗證

3.1 命名

3.1.1 命名種類

FPCA 憑證系統產生或處理 X.509 V3 (ISO 9594-8) 憑證之 FUCA 主要識別名稱(SubjectName)（例如：FUCA 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

3.1.2 命名須有意義

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。

3.1.3 用戶匿名或假名

本作業基準不允許 FUCA 使用匿名或假名。

3.1.4 識別名稱之命名規則

下為一般識別名稱之說明：

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 = TWCA
3.OrganizationUnit (OU)	憑證管理中心所屬性質	OU = User CA
4.CommonName (CN)	憑證管理中心英文名稱	CN = Taiwan Financial User CA

3.1.5 識別名稱之唯一性

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

3.1.6 辨識，驗證與註冊商標的角色

FPCA 尊重 FUCA 識別名稱有關註冊公司中、英文名稱之註冊商標權，並接受 FUCA 之使

用，但不保證 FUCA 註冊商標之認可、驗證與唯一性，相關之糾紛處理非為 FPCA 之管轄權責範圍，FUCA 必須向相關之業務主管機關提出申請。

3.2 初始註冊

FPCA 於 FUCA 註冊時，應依據「3.2.2 法人用戶身分之驗證」作業規範，驗證 FUCA 申請之證明文件，正確之驗證 FUCA 之資格。FUCA 向 FPCA 申請憑證簽發時，必須依據本作業基準規範「4.1 憑證申請」處理，即為 FUCA 必須先完成註冊作業程序。

3.2.1 私密金鑰之驗證方法

FPCA 必須驗證 FUCA 私密金鑰擁有之合法性與正確性，須以下述之方法驗證 FUCA 所擁有之私密金鑰：

於 FUCA 申請憑證，以 FUCA 私密金鑰執行 FUCA 憑證申請訊息之簽章時，FPCA 必須驗證 FUCA 憑證申請訊息內，經保護之 FUCA 身分資訊、公開金鑰與私密金鑰之正確性、唯一性及合法性。

3.2.2 法人用戶身分之驗證

FPCA 處理 FUCA 註冊身分與識別名稱之驗證時，FUCA 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，並須驗證該授權代理人之相關身分證明文件。

3.2.3 個人用戶身分的驗證

不接受自然人擔任 FUCA。

3.2.4 未經驗證之用戶資訊

FPCA 對所有 FUCA 資訊皆須驗證。

3.2.5 權責之確認

個人、法人代理人及法人之身分證明文件，應確認為官方核發之證明文件；註冊中心須確認法人代理人授權文件之真偽。

3.2.6 交互運作標準

除非取得憑證政策管理委員會之同意，不得對其他憑證管理中心洽商交互認證等協議。

3.3 金鑰更新請求之識別及驗證

3.3.1 例行性金鑰更新之識別及驗證

FUCA 金鑰之生命週期為五年，FUCA 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 FPCA 申請憑證簽發，此為私密金鑰之更新 (Rekey)。FUCA 憑證申請程序依據「4.1 憑證申請」之規範處理。

FUCA 至少每九年將重新進行註冊，當 FUCA 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、產生新金鑰對，並向 FPCA 申請新憑證之簽發。為風險管理與安

全考量，FUCA 向 FPCA 申請新憑證簽發時，不可使用舊金鑰對。

3.3.2 憑證廢止後金鑰更新之識別及驗證

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

3.4 憑證廢止請求之識別及驗證

憑證廢止作業依「4.9 憑證暫時停用與廢止」內容辦理。

4. 憑證生命週期作業規範

4.1 憑證申請

4.1.1 憑證的申請者

FUCA 之法人代表人或經代表人授權之代理人為 FUCA 憑證之憑證申請者。

本公司自行擔任 FUCA 者，由該 FUCA 之憑證主管人員擔任憑證申請者。

4.1.2 註冊程序與責任

FUCA 應事先閱讀憑證使用者約定事項，了解使用憑證之權利及義務，如同意則撰寫憑證申請書並備妥相關身分證明文件正本或影本，至 FPCA 辦理憑證申請。

4.2 憑證申請的程序

4.2.1 執行識別及驗證功能

憑證申請程序如下：

(1) 申請人出具法人登記證明文件、經公司大小章用印之憑證申請書、經代表人簽署之授權書或其他可茲證明之授權資訊、PKCS#10 格式憑證申請檔向FPCA辦理憑證申請。

(2) 政策管理中心審查憑證申請書內容以及憑證實務作業基準是否符合憑證政策之規定。

(3) 政策管理中心通過審查後即進入憑證簽發程序。

4.2.2 憑證申請的核准或拒絕

完成「4.2.1 執行識別及驗證功能」後，視為憑證申請通過，如未能完成識別與鑑別程序，應拒絕憑證申請。

4.2.3 處理憑證申請的時間

FPCA 於政策管理中心通過憑證申請審查後，最遲應不超過 30 日曆天進行憑證簽發。

4.3 簽發憑證的程序

4.3.1 憑證機構的作業

FPCA 之憑證簽發程序如下：

(1) FUCA自行產製PKCS#10 格式之憑證申請檔，連同憑證申請書以書函方式交付FPCA。

(2) FPCA確認FUCA交付之憑證申請檔，確實來自FUCA。

(3) 以驗證數位簽章之方式，確認PKCS#10 格式之憑證申請檔之完整性；檢查憑證申請檔記載之憑證主旨識別名稱，符合憑證申請書所記載之主旨識別名稱及申請使用之擴充欄位。

(4) FPCA檢查無誤後，即簽發憑證予FUCA。簽發完成之憑證將以離線或連線的方式，交

付FUCA。

4.3.2 憑證機構對申請者的通知

FPCA於憑證簽發完成後，以電話或電子郵件方式通知FUCA，經由雙方人員確認後以離線或連線的方式傳遞憑證檔案予憑證申請者。

FPCA若不同意憑證簽發，須以書面或電子郵件方式通知憑證申請者。

4.4 接受憑證的程序

4.4.1 接受憑證的要件

FUCA申請憑證簽發完成且向FPCA取得憑證時，應依下列規定處理：

(1) 確認憑證內容之FUCA相關資訊與FUCA註冊時之一致性，且為FUCA之正確資訊。

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

(3) 必須驗證FUCA憑證中FPCA數位簽章之有效性，如：該FPCA憑證是否已廢止、該FPCA憑證有效期限是否已結束、是否為合法且由正確之FPCA所簽發、FPCA憑證是否有效。

(4) FUCA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為未依憑證實務作業基準核發時，憑證申請者得以拒絕，憑證管理中心應廢止該憑證。

(6) 憑證申請者確認上述 (1) ~ (5) 無誤並接受後，本憑證管理中心依此做為憑證接受之依據。

(7) 有關拒絕接受憑證衍生之法律糾紛與賠償，依9.1.5及9.13節規定辦理。

4.4.2 憑證機構的憑證發布

FPCA於FUCA完成憑證接受程序後，立即將簽發予FUCA之憑證公布於儲存庫。

4.4.3 憑證機構對其他個體的憑證簽發通知

無規定。

4.5 金鑰對及憑證之用途

4.5.1 用戶私密金鑰及憑證使用

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

(1) FUCA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FPCA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) FUCA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) FUCA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。

4.5.2 信賴憑證者公開金鑰及憑證使用

信賴憑證者於信賴 FPCA 簽發之 FUCA 憑證前，至少應進行以下必要之程序，方可使用於驗證 FUCA 所簽發之數位簽章：

(1) 透過適當及安全之管道，取得FRCA自簽憑證及FPCA憑證。

(2) 以FRCA自簽憑證內之公開金鑰，檢驗FRCA自簽憑證內之數位簽章是否有效，並檢查FRCA自簽憑證是否有效且並未被廢止。

(3) 以FRCA自簽憑證內之公開金鑰，檢驗FPCA憑證內之數位簽章是否有效，並檢查FPCA憑證是否有效且並未被廢止。

(4) 以FPCA憑證內之公開金鑰，檢驗FUCA憑證內之數位簽章是否有效，並檢查FUCA憑證是否有效且並未被廢止。

如未能通過前述檢驗，表示信賴憑證者取得之 FUCA 憑證非 FPCA 所簽發，或憑證已失效，信賴憑證者不應信賴該 FUCA 憑證。

4.6 憑證展期

(1) 為風險及安全管理考量， FPCA不提供憑證展期之功能。

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

4.7 憑證的金鑰更新

4.7.1 憑證金鑰更新的事由

如「3.3.1 例行性金鑰更新之識別及驗證」之規定。

4.7.2 憑證金鑰更新的申請者

FUCA 有權向 FPCA 申請更新憑證金鑰。

4.7.3 憑證金鑰更新的程序

(1) 依照「3.3 金鑰更新請求之識別及驗證」之規定對用戶進行身分識別與驗證。

(2) 依照「4.3 簽發憑證的程序」之規定簽發憑證。

4.7.4 憑證金鑰更新的簽發通知

依「4.3.2 憑證機構對申請者的通知」之規定。

4.7.5 接受金鑰更新後憑證的要件

依「4.4 接受憑證的程序」之規定。

4.7.6 金鑰更新後憑證的發布

依「4.4.2 憑證機構的憑證發布」之規定。

4.7.7 金鑰更新後憑證機構對其他個體的憑證簽發通知

依「4.4.3 憑證機構對其他個體的憑證簽發通知」之規定。

4.8 憑證變更

FPCA 不提供憑證變更之功能。

4.9 憑證暫時停用與廢止

4.9.1 憑證廢止的因素

FPCA 於 FUCA 憑證仍然有效期間內，當有下述情況時，得逕行憑證之廢止：

(1) FPCA因憑證管理系統之不適用或憑證系統之整合需求。

(2) FUCA使用憑證而為有權第三者（例如：FPCA）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FUCA之憑證。

FUCA 於憑證仍然有效期間內，當有下述情況時，必須提出憑證廢止申請：

(1) 憑證內容之FUCA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FUCA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：FUCA憑證內容與註冊資料不符，或因註冊資料輸入之疏忽。

(4) FUCA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。

4.9.2 憑證廢止的申請者

(1) 憑證用戶 (FUCA)。

(2) 本憑證管理中心 (FPCA)。

(3) 憑證政策管理委員會。

(4) 主管機關或法院。

憑證若由本憑證管理中心逕行廢止，其相關條件及衍生之費用、權利義務依照用戶合約規定辦理。

4.9.3 憑證廢止的程序

(1) FUCA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FPCA之合約規範，親自填寫申請表單並簽名確認，或以具有FUCA簽章之廢止憑證申請訊息，經由郵寄（限時掛號）或親自向FPCA申請廢止該憑證。

(2) FPCA、主管機關、法院與訴訟單位及其他有權責者，亦必須依據FPCA之作業規範，填具廢止申請單向FPCA申請廢止該憑證。

(3) FPCA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) FUCA進行憑證廢止時，須填具憑證廢止申請表，並須在憑證廢止申請表加註憑證廢止之理由，FPCA會在廢止憑證後產生的CRL，加註該憑證廢止之原因理由。

(5) FPCA完成FUCA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FUCA並告知憑證廢止處理作業已完成。

4.9.4 憑證廢止申請的寬限期

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

4.9.5 憑證機構處理憑證廢止申請的時效

FPCA 處理廢止廢止 FUCA 憑證，應於 24 小時內完成，其憑證廢止資訊之異動，應留存適當稽核軌跡。

4.9.6 信賴憑證者檢查憑證廢止的要求

(1) 信賴憑證者應根據其風險、責任及可能導致之後果，自行判斷查詢（或下載）廢止資料（憑證廢止清冊）的間隔時間。

(2) 信賴憑證者在使用FPCA簽發之FUCA憑證，驗證FUCA之數位簽章時，應檢查該FUCA憑證是否為廢止狀態。

4.9.7 憑證廢止清冊發布頻率

FPCA 憑證廢止清冊 (CRL) 之產生頻率為每 24 小時產生一次。

4.9.8 憑證廢止清冊產生與發布間的時間差

憑證廢止清冊產生時間（有效日期欄位）與發布間的時間差不得超過 4 小時。

4.9.9 線上憑證狀態查詢 (OCSP) 服務

FPCA 提供線上憑證狀態查詢服務 (OCSP)。

4.9.10 線上憑證狀態查詢 (OCSP) 的規定

信賴憑證者於決定信賴 FPCA 簽發之憑證前，必須檢查其憑證狀態；若信賴憑證者未使用

FRCA 簽發之憑證廢止清冊 (CRL) 來檢查憑證狀態，則信賴憑證者必須以「4.9.9 線上憑證狀態查詢」規定之方式，透過 OCSP 來檢查憑證狀態。

4.9.11 其他形式的廢止公告

FPCA 除 X.509 V2 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。

4.9.12 金鑰遭破解時的其他特殊規定

金鑰更新有安全顧慮時之作業規範，皆依照 「5.6 金鑰更換」之規範處理。

4.9.13 憑證暫時停用的因素

FPCA 不提供 FUCA 憑證暫時停用服務。

4.9.14 憑證暫時停用的申請者

無相關規定。

4.9.15 憑證暫時停用的程序

無相關規定。

4.9.16 暫時停用時間之限制

無相關規定。

4.10 憑證狀態服務

4.10.1 服務特性

請參見 4.9.9 線上憑證狀態查詢 (OCSP) 服務、4.9.10 線上憑證狀態查詢 (OCSP) 的規定。

4.10.2 服務可用性

FPCA 提供 7 x 24 小時憑證狀態查詢的服務。

4.10.3 其他服務項目

請參見 4.9.9 線上憑證狀態查詢 (OCSP) 服務、4.9.10 線上憑證狀態查詢 (OCSP) 的規定。

4.11 終止所申請的憑證服務

當下屬憑證管理中心不再使用 FPCA 的服務時，FPCA 在下屬憑證管理中心依其憑證實務作業基準「5.8 憑證機構終止服務」所載，完成有效憑證之移轉後，同意並妥善辦理終止程序。

4.12 私密金鑰託管與回復

FPCA 不提供 FUCA 私密金鑰之託管、回復及保存服務。

5. 設施面、管理面與作業面的安全控管

5.1 實體控管

FPCA 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。

5.1.1 建築物與位置

FPCA 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。

5.1.2 實際進出管制

作業人員進入 FPCA 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（單獨一人員無法開啟進出），並有 24 小時 CCTV 位移監控錄影設備、及紅外線防入侵警報系統。

FPCA 運作之相關私密金鑰、備份資料皆妥善、安全之存放於此 FPCA 設有監控錄影系統保護之保險櫃內，FPCA 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。

FPCA 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。

5.1.3 電力與空調

FPCA 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。

FPCA 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。

5.1.4 防水處理

FPCA 憑證系統之房屋為密閉式建築物，除內部可進出之出入門外，外部皆為混凝土建築物，雨水無法進入，且樓層地板裝置高架地板無進水之顧慮。

5.1.5 防火處理

FPCA 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。

5.1.6 媒體儲存

媒體儲存環境，具有對磁性媒體防磁、防靜電干擾之設備與環境，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。

5.1.7 廢棄處理

FPCA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。

5.1.8 異地備份

FPCA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，與人員進出存取須經過合法授權之高度安全管控之異地備援環境。

FPCA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。

5.2 作業程序控管

5.2.1 可信賴角色

FPCA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FPCA扮演之可信賴且具公信力之機構，公正與嚴謹之執行。

因此FPCA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員，於具有安全控管機制之憑證系統下，依照FPCA內部憑證作業規範及作業手冊，確實執行業務。

FPCA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) 系統管理人員 (Administrator)：負責系統安裝、管理作業及環境參數之設定。

(2) 憑證管理人員 (Officer) ：負責憑證及憑證廢止之請求、簽發。

(3) 稽核人員 (Auditor) ：負責進行內部稽核、檢視並維護稽核紀錄。

(4) 操作人員 (Operator) ：負責系統例行性維護作業，如備份、還原、網站資料維護。

5.2.2 作業人員需求人數

FPCA執行各種業務之作業人員，其權責為獨立且不重疊，依照系統管理人員、憑證管理人員、稽核人員操作人員，不同業務之特性指派適當數目之人員擔任，例如FPCA金鑰之建置或變更、FUCA 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，至少須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。

5.2.3 角色的識別與驗證

FPCA執行各種業務之系統管理人員、憑證管理人員、稽核人員與操作人員，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。

5.2.4 角色的權責劃分

角色	系統管理人員	憑證管理人員	稽核人員	操作人員
系統管理人員	O	X	X	X
憑證管理人員	X	O	X	X
稽核人員	X	X	O	X
操作人員	X	X	X	O

O：可兼任

X：不可兼任

5.3 人員控管

5.3.1 適任條件與經歷

(1) FPCA 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。

5.3.2 審核

FPCA 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。

5.3.3 教育訓練

FPCA 系統運作之人員，皆依照其職務，施予 FPCA 系統運作所應具備之軟硬體功能、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，亦須給予適當之教育訓練。

FPCA 須訂定一套 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。

5.3.4 再教育的頻率與需求

FPCA 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。

FPCA 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，皆須對系統運作之相關人員執行教育訓練。

5.3.5 職務的輪調

配合 FPCA 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，但調派前必須施以適當知識與技能之教育訓練。

5.3.6 非授權作業的懲罰

FPCA 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。

5.3.7 委外人員需求

FPCA 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，必須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。

5.3.8 作業文件需求

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) FPCA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) FPCA憑證系統內部作業文件，例如：系統備援與回復作業文件、異地災變備援與回復作業文件、例行工作作業文件。

5.4 稽核紀錄程序

FPCA 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 FPCA 之稽核作業規範，確實執行憑證系統運作之稽核作業。

5.4.1 處理事件的紀錄種類

FPCA 稽核紀錄至少應保存如下之資訊：

(1) FUCA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) 或其他基碼之產生、建置、變更之成功

與失敗之記錄。

(3) FPCA金鑰與憑證之產生、建置、變更之成功與失敗之記錄。

(4) FUCA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FPCA 機房之紀錄報表，FPCA 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FPCA 機房監控攝錄影機之媒體紀錄。

(8) FPCA 主機系統硬、軟體、應用系統，及FPCA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。

5.4.2 稽核紀錄處理頻率

新系統開始加入營運時，每日執行憑證系統運作相關紀錄之查核，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，須由 FPCA 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。

5.4.3 稽核紀錄的保存期限

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 FPCA 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。

5.4.4 稽核紀錄的保護

FPCA 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。

5.4.5 稽核紀錄備援程序

FPCA 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。

5.4.6 稽核紀錄蒐集系統

各種稽核紀錄之蒐集由憑證系統開啟至系統關閉為止，FPCA 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 FPCA 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. FPCA 系統建置與變更	自動	FPCA 憑證系統
6.金鑰與憑證之產生、簽發與廢止	自動	FPCA 憑證系統
7.憑證用戶資訊之建置、修改與刪除	自動	FPCA 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

5.4.7 對引起事件者之告知

作業人員於執行 FPCA 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。

5.4.8 弱點的風險評估

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。

5.5 紀錄歸檔方法

5.5.1 保存紀錄的種類

FPCA 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 FUCA 相關合約條款、FUCA 註冊資料之相關資訊、FUCA 憑證及廢止憑證資料檔、交易資料檔、稽核資料檔、FPCA 金鑰與憑證變更資訊、憑證實務作業基準、憑證政策、FPCA 憑證應用系統及其他稽核人於要求等之資料執行備份保存。

5.5.2 保存期限

除配合主管機關訂定之資訊保存期限規範，FPCA 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FUCA註冊申請表單相關合約條款、FUCA之廢止憑證或過期憑證，或過期憑證，至少保留至憑證有效期限結束後十年。

(2) FUCA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) FUCA金鑰與憑證相關之異動資料至少保留十年。

(4) FPCA金鑰與憑證等相關之異動資料至少保留十年。

5.5.3 保存紀錄的保護

金鑰、憑證、交易資料、稽核資訊、憑證實務作業基準與註冊文件等相關保存資料之保護，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。

5.5.4 保存紀錄的備援程序

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 FPCA 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。

5.5.5 紀錄的時序需求

FPCA 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。

FUCA 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。

5.5.6 保存紀錄蒐集系統

FPCA 憑證系統作業相關之保存紀錄資訊，皆由 FPCA 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。

5.5.7 取得與驗證保存紀錄程序

FPCA 憑證系統作業相關之保存紀錄資訊之驗證，依 FPCA 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。

5.6 金鑰更換

(1) FUCA憑證有效期限為五年，FUCA簽發下層用戶之憑證效期最長為二年，為使FUCA能發出具完整效期之用戶憑證，且簽發時FUCA之剩餘效期有完整覆蓋期，FUCA須於FUCA憑證生效第三年時完成金鑰更新程序，FUCA須產生下一組新金鑰對及相對之憑證申請檔，並向FPCA申請新憑證的簽發。FUCA依據「4.1 憑證申請」，向FPCA申請新憑證之簽發。

(2) FPCA憑證有效期限為十一年，FPCA簽發下層FUCA之憑證效期最長為五年，為使FPCA能發出具完整效期之FUCA憑證，且簽發時FPCA之剩餘效期有完整覆蓋期，FPCA須於FPCA憑證生效第六年時完成金鑰更新程序，FPCA須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。

5.7 金鑰遭破解及災難之復原

5.7.1 緊急事件及系統遭破解之處理程序

本公司為使 FPCA 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。

5.7.2 電腦資源、軟體或資料庫之復原程序

FPCA 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系統之復原作業，使系統能繼續且正常營運。

當 FPCA 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。

FPCA 內部復原程序應於 6 個小時內完成，若無法於 6 小時之內恢復正常作業，FPCA 應啟動異地備援機制，並於 24 小時內完成災難復原程序。

5.7.3 憑證機構簽章金鑰遭破解之復原程序

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，應立即向 FRCA 申告，並廢止所有由 FPCA 簽發之 FUCA 憑證及更新 CRL 資料，供憑證用戶或信賴憑證者查詢。同時 FPCA 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 取得新憑證後，依據「4. 憑證生命週期作業規範」，重新簽發 FUCA 之憑證。

FPCA 新產生之公開金鑰，依據「6.1.4 憑證公開金鑰遞送至信賴憑證者」之規範，遞送給 FUCA。

FUCA 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「4.9 憑證暫時停用與廢止」之程序，立即向 FPCA 申告，並產生下一組新金鑰對及相對之憑證申請檔，並向 FPCA 申請新憑證的簽發。

5.7.4 憑證機構災後持續營運措施

為避免因天災與地變而造成 FPCA 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 FPCA 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，FPCA 憑證系統之運作至少能於 24 小時內立刻回復且繼續營運，而將對業務系統運作之影響風險減少至最低。

5.8 憑證機構之終止服務

FPCA 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、銀行公會及FRCA。

(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管理中心承接。

(4) 於高度安全且無安全顧慮之作業環境下，廢止FPCA與全部用戶之憑證，將結束之FPCA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FPCA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FPCA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。

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

必須執行如業務正常結束時的作業程序，將對FUCA業務系統運作的影響減少至最低程度。

6. 技術性安全控管

6.1 金鑰對產生與安裝

6.1.1 金鑰對產生

(1) FPCA不提供代替FUCA產生金鑰對之服務，FUCA金鑰對應由二位以上獨立之授權人員，同時登入 (Log-in) 至硬體密碼模組，由硬體密碼模組直接產生，不允許單獨一人執行金鑰對之產生作業，且私密金鑰於硬體密碼模組內產生後，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，須經由硬體密碼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密碼模組外。

(2) FPCA金鑰對產製之方式亦如 (1) 所述。

6.1.2 私密金鑰遞送

FPCA 不提供代替 FUCA 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。

6.1.3 公開金鑰遞送

FUCA 以公開金鑰向 FPCA 申請憑證時，該請求訊息內之 FUCA 公開金鑰 (Public Key) 具有 FUCA 簽章及 FUCA 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 FPCA 之簽章與訊息完整性之保護。當 FUCA 之公開金鑰遞送至 FPCA 時應有正式的收發程序並保留憑據。

6.1.4 憑證機構公開金鑰遞送至信賴憑證者

(1) FPCA公開金鑰有異動或因FUCA查詢而需遞送至FUCA時，FPCA公開金鑰憑證皆有FPCA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) FPCA需在FPCA網站上公布FPCA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。

6.1.5 金鑰長度

FPCA 之 RSA 金鑰長度至少為 4096 位元，FUCA 之 RSA 金鑰長度至少為 4096 位元金鑰長度將視銀行公會之規範而調整。

6.1.6 公開金鑰參數產製與品質的檢核

FPCA RSA 公開金鑰參數之產生與選取，由通過 FIPS 140-2 Level 3 安全等級之亂數產生器 (Random Number Generator) 產生最佳之質數參數。

FPCA 之 RSA 公開金鑰參數品質，由通過 FIPS 140-2 驗證標準，安全等級為 Level 3 之硬體密碼模組檢核。

6.1.7 金鑰用途

FPCA 簽發給憑證用戶作為簽章或加密用途之憑證，其用途記載於 X.509 V3 憑證的標準擴充欄位的金鑰用途欄位 (KeyUsage)，憑證用戶與信賴憑證者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。

FPCA 與 FUCA 之憑證，其金鑰用途為簽發憑證廢止清冊用 (cRLSign) 及簽發憑證用 (keyCertSign)。

6.2 私密金鑰保護與密碼模組安全控管措施

6.2.1 密碼模組標準與控管

FPCA 之硬體密碼模組，通過 FIPS 140-2 驗證標準，安全等級為 Level 3。

6.2.2 金鑰分持之多人管控

(1) FPCA私密金鑰之產生、建置及變更，皆由至少二位以上之授權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，則需由不同授權人員個別獨立備份儲存於具安全管控措施之媒體。

6.2.3 私密金鑰託管

FPCA 不提供 FUCA 私密金鑰之託管、回復及保存服務。

6.2.4 私密金鑰備份

(1) FPCA私密金鑰加密後儲存於之硬體密碼模組內，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。

6.2.5 私密金鑰歸檔

FPCA 之私密金鑰於使用期限過後不進行歸檔。

6.2.6 私密金鑰於密碼模組的收送傳輸

FPCA 之私密金鑰是在硬體密碼模組中產生及儲存，並且只有在進行金鑰備份回復時，才能將私密金鑰輸入至另一個硬體密碼模組中；自密碼模組輸出時，依「6.2.4 私密金鑰備份」之規定辦理。

6.2.7 私密金鑰儲存於密碼模組

FPCA 之私密金鑰的建置，至少由二位以上的授權人員由硬體密碼模組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，且私密金鑰經密碼保護後儲存在設備內，私密金鑰無法以明碼方式輸出至密碼模組外。

當有使用該私密金鑰執行運算的需求時，須經由密碼模組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密碼模組外。

6.2.8 私密金鑰之啟動方式

FPCA 儲存於硬體密碼模組內之私密金鑰，必須由二位以上之授權人員開啟（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。

6.2.9 私密金鑰之解除使用方式

儲存於硬體密碼模組內之私密金鑰，必須由二位以上授權人員簽入 (Log-in) 系統啟動，使用後必須立即在稽核人員的監看下解除使用以避免未經授權存取。

硬體密碼模組或私密金鑰關閉不使用時，皆須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。

6.2.10 私密金鑰之銷毀方式

私密金鑰不再使用時，如相對應之公開金鑰憑證過期、廢止時，硬體密碼模組或 IC 卡必須以零值化 (Zeroize) 之覆蓋方式清除不再使用之私密金鑰。

硬體密碼模組於廢棄不使用時，亦以上述方式清除全部私密金鑰。

6.2.11 密碼模組的等級

FPCA 與 FUCA 使用之硬體密碼模組等級，必須為 CNS 15135、ISO 19790 或 FIPS 140-2 等級 3。

6.3 金鑰對管理的其他規範

6.3.1 公開金鑰的歸檔

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，期限至少留存十年，若主管機關規範的保存期限較長時，則以主管機關的管理規範為準據。

6.3.2 公開金鑰及私密金鑰的使用期限

FPCA 公開金鑰與私密金鑰之有效期限為相同效期。

FPCA 金鑰之有效期限為十一年，FUCA 金鑰之有效期限為五年。

6.4 啟動資料

FPCA 所簽發之 FUCA 憑證，FUCA 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 FPCA 不產生 FUCA 之啟動資訊，FPCA 亦無其他啟動資訊。

6.4.1 啟動資料的產生及設定

啟動簽章用私密金鑰的啟動資料由多張智慧卡個別產生，並使用多人控管的權限分離 (Duty Separation) 機制，通過智慧卡的個人識別碼（以下簡稱 PIN 碼）檢核後，以智慧卡中的啟動資料做為身分鑑別。

6.4.2 啟動資料的保護

啟動資料由控管智慧卡組保護，智慧卡的 PIN 碼由保管人員負責保存，不得記錄於任何媒體上，如登入的失敗次數超過 3 次，則鎖住此智慧卡；智慧卡移交時，新的保管人員必須重新設定新的 PIN 碼。

6.4.3 其他啟動資料的規定

無規定。

6.5 電腦安全控管

6.5.1 電腦安全技術需求

FPCA 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。FPCA 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。

6.5.2 電腦系統安全等級

FPCA 使用之憑證管理系統，其電腦軟體系統安全等級，至少符合 ITSEC E2、TCSEC C2、ISO 15408-EAL3 或同等級之國際安全標準。

6.6 生命週期技術控管

6.6.1 系統開發控管

FPCA 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。

6.6.2 安全管理控管

執行 FPCA 憑證系統之資訊安全管理系統環境，遵循 WebTrust Principles and Criteria for Certification Authorities 及 ISO27001 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。

6.6.3 生命週期的安全等級

無規定。

6.7 網路安全控管

FPCA 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 FPCA 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。

FPCA 憑證系統為離線 (Off-line)、獨立之作業管理系統，且須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。

6.8 時戳

無規定。

7. 憑證及憑證廢止清冊格式

7.1 憑證格式剖繪

FPCA 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。

7.1.1 版本

FPCA 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。

7.1.2 憑證擴充欄位

FPCA 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。

7.1.3 演算法物件識別碼

FPCA 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)
金鑰產製	RSAEncryption	1.2.840.113549.1.1.1
簽章	sha256WithRSAEncryption	1.2.840.113549.1.1.11

7.1.4 識別名稱格式

FPCA 憑證系統所簽發之 FUCA 憑證，其識別名稱格式內容皆符合 X.500 Distinguished Name (DN)之命名方式以及中華民國銀行公會公布之「金融 XML 憑證共通性技術規範」。

7.1.5 識別名稱限制

FPCA 憑證系統所簽發之 FUCA 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布之「金融 XML 憑證共通性技術規範」。

7.1.6 憑證政策物件識別碼

FPCA 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。

7.1.7 憑證政策限制擴充欄位的使用

FPCA 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。

7.1.8 憑證政策限制語法與語意

FPCA 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。

7.1.9 憑證政策擴充欄位必要的處理

FPCA 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。

7.2 憑證廢止清冊格式剖繪

7.2.1 版本

FPCA 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。

7.2.2 憑證廢止清冊擴充欄位

FPCA 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。

7.3 線上憑證狀態協定格式剖繪

7.3.1 版本

符合 RFC 6960 之規定。

7.3.2 線上憑證狀態協定擴充欄位

符合 RFC 6960 之規定。

8. 稽核方法

FPCA 自行委託會計師事務所進行稽核，再將稽核報告經由 FRCA 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。

8.1 稽核之頻率

FPCA 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 27001:2013 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與外部例行性查核。

8.2 稽核人員之身份及資格

FPCA 執行稽核作業之稽核人員至少必須具備憑證管理中心、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 資格之會計師事務所人員。

8.3 稽核人員及被稽核方之關係

FPCA 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。

FPCA 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。

8.4 稽核之範圍

FPCA 稽核人員查核：

(1) FPCA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) FPCA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) FPCA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) FPCA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) FPCA業務執行之公告：FPCA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：FPCA、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) FPCA環境之安全控管：符合FPCA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。

8.5 稽核缺失之處理

FPCA 之運作經詳細查核評估後，有不符合本作業基準之規範時，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。

FPCA 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 FPCA 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 FPCA 之資格。

8.6 稽核結果公開之範圍

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。FPCA 將公布最近一次的稽核結果於公司網站上。

9. 其他業務與法律事項

9.1 費用

FPCA 對於 FUCA 收取費用或收費機制之規定，由憑證政策管理委員會同意後方得施行。

9.1.1 憑證簽發、更新費用

FPCA 與 FUCA 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。

9.1.2 憑證查詢費用

FPCA 與 FUCA 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。

9.1.3 憑證廢止、狀態查詢費用

FPCA 與 FUCA 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。

9.1.4 其他服務費用

FUCA 經由網際網路至 FPCA 下載本作業基準或相關業務之憑證政策，FPCA 不計收任何服務費用，但如向 FPCA 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，FPCA 需向 FUCA 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。

其他收費項目之費率，如建置費用、參加年費等，FPCA 將另訂定於相關業務之計費作業規範。

9.1.5 請求退費之程序

FPCA 對 FUCA 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，FPCA 均不退還 FUCA 任何費用。

9.2 財務責任

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

9.2.1 保險範圍

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，已投保認證業務責任險。

9.2.2 其他資產

無其他資產。

9.2.3 對用戶及信賴憑證者之賠償責任

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

如因信賴憑證者或 FUCA 之過失且可歸責於信賴憑證者或 FUCA，而造成 FPCA 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 FUCA 必須負損害賠償責任，FPCA 可依照相關法律之規定向信賴憑證者或 FUCA 請求賠償。

9.3 業務資訊保密

9.3.1 機敏性資料的範圍

FPCA 對於 FUCA 資訊隱密性之保護，必須於 FUCA 資訊保密策略規範中訂定，對於 FUCA 資訊之保護，必須依照行政院公告之「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)。

FPCA 於管理及使用 FUCA 註冊、憑證申請之相關資訊時，除 FUCA 憑證內容可公開外，FUCA 之註冊基本資料與身分認證資料，非經由 FUCA 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) FUCA身分驗證資訊（例如：FUCA名稱、聯絡資訊等）。

(2) FUCA註冊或憑證申請與註銷（廢止）時交易的相關隱密性訊息。

(3) FUCA註冊時填寫於註冊相關申請單、合約上的FUCA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) FPCA為憑證管理作業之需求而使用與存取FUCA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) FPCA管理與使用FUCA資訊時，FUCA之註冊基本資料與身分認證資料，非經由FUCA之允許絕不任意對外銷售、租借與公開。

9.3.2 非機敏性資料的範圍

FPCA 公告於儲存庫之 FUCA 憑證資訊，憑證狀態（提供憑證有效性狀態查詢功能時），及 FPCA 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。

9.3.3 保護機敏性資料的責任

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

(1) 依法令之規定並經由權責管理單位依法定程序授權。

(2) 具管轄權之法院或~~仲裁~~機構處理因憑證產生之糾紛~~與仲裁~~，而依法定程序申請之要求或申請者。

9.4 個人資料的隱密私性

9.4.1 保護計畫

FPCA 依據我國個人資料保護法相關規範運作。

9.4.2 隱私資料

依「9.4.1 保護計畫」之規定。

FUCA 應保密之資訊種類，必須於其憑證實務作業基準或隱私權保密政策中訂定。

9.4.3 非隱私資料

無規定。

9.4.4 保護隱私資料的責任

依相關法令規定辦理。

9.4.5 使用隱私資料的告知與同意

FPCA 於使用個人隱私資訊時，須告知並經過隱私資訊所有人同意，方可使用。

9.4.6 因應法規與管理程序的應揭露事項

依相關法令規定辦理。

9.4.7 其他應揭露事項

如「9.3.3 保護機敏資料的責任」之規定。

9.5 智慧財產權

本公司於 FPCA 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。

FPCA 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。

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

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

FPCA 尊重置於 X.509 V3 憑證內憑證用戶識別名稱欄位所存放之 FUCA 註冊名稱之註冊商標，但不保證 FUCA 註冊名稱之智慧財產權之歸屬，FUCA 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處理非為 FPCA 之管轄權責，FUCA 必須向相關之業務主管機關提出申請。

9.6 職責與義務

9.6.1 憑證機構職責與義務

(1) 未依憑證實務作業基準及相關之規範，處理相關作業，致下屬憑證管理中心、用戶或信賴憑證者遭受之損害，本憑證管理中心應負賠償責任。

(2) 未依憑證實務作業基準履行相關之責任及擔保，致下屬憑證管理中心、用戶或信賴憑證者所受之損害，本憑證管理中心應負賠償責任。

(3) 因網際網路傳輸的中斷或設備的故障或其他不可抗拒的天災事故(例如戰爭或地震等)，而非可歸責之事由，所致下屬（用戶或信賴憑證者）機構的損失，本憑證管理中心不負賠償責任。

(4) 憑證管理中心對因其經營或提供認證服務之相關作業程序，致當事人受有損害，或致善意第三人因信賴該憑證而受有損害者，應負賠償責任。但能證明其行為無過失者，不在此限。憑證管理中心就憑證之使用範圍設有明確限制時，對逾越該使用範圍所生之損害，不負賠償責任。(電子簽章法第 14 條)

(5) 其他依電子簽章法規定應負之賠償責任。

(6) 對憑證內容與核發之正確性負擔保責任。

(7) 憑證管理中心應於憑證實務作業基準中載明註冊中心之責任。

(8) 訂定並公告憑證實務作業基準。

(9) 公告憑證廢止清冊 (CRL) 的內容。

(10) 簽發、管理、遞送與廢止下屬憑證管理中心/用戶之憑證。

(11) 公告、管理憑證作業程序與驗證的作業規範。

(12) 依據憑證實務作業基準之規範，執行相關之作業程序。

(13) 憑證管理中心應管理與公告憑證廢止清冊與憑證狀態線上查詢（Online Certificate Status Protocol，以下簡稱OCSP）資訊時的作業程序與身份驗證及訊息安控措施的作業規範。

(14) 依據憑證政策各項規定提供相關控制。

9.6.2 註冊中心職責與義務

由於註冊中心係代理憑證機構管理中心執行身分識別工作所引發的所有責任，註冊中心之責任應依其與憑證機構管理中心間約定之權利義務而定。本憑證機構管理中心之註冊中心由本中心自行擔任。

(1) 負責確認憑證申請人之身分，但不負責簽發及管理憑證。

(2) 管理與公告用戶註冊申請的作業程序與身分驗證的作業規範。

(3) 驗證用戶憑證之簽發與廢止及查詢等申請訊息、身分合法性與訊息正確性。

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

(5) 管理、公告並提供用戶憑證查詢、廢止及憑證管理中心的憑證鏈。

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

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

(8) 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，即刻向憑證管理中心辦理申告與處理。

(9) 憑證管理中心遞送的用戶憑證，必須提供用戶憑證適時更新的機制。

(10) 為能提供客戶完整的客戶服務，憑證相關作業一律須經過註冊中心並留存相關資料於註冊中心。

(11) 註冊中心應通知憑證即將到期的用戶辦理更新憑證作業。

9.6.3 用戶的職責與義務

接受憑證機構管理中心簽發憑證的用戶應負以下義務：

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

(2) 其憑證與憑證對應的私密金鑰使用的業務範圍，皆依憑證管理中心「憑證實務作業基準」與「憑證政策」之規範，運用於相關業務上。

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

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

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

9.6.4 信賴憑證者的職責與義務

使用憑證機構管理中心簽發憑證的信賴憑證者應負以下義務：

(1) 必須了解且同意憑證實務作業基準與憑證政策相關作業規範的規定，且依規範所訂定的業務範圍應用於相關的業務，無任何違反相關法律的規定與侵害第三者的權利。

(2) 驗證憑證時必須由憑證鏈逐一驗證該憑證的正確性及有效性，也須利用憑證廢止清冊或OCSP機制，檢核此憑證是否為廢止或暫時停用憑證。

9.6.5 其他參與者的職責與義務

無規定。

9.7 免責聲明

(1) FPCA處理FUCA註冊資料及憑證簽發作業，除可歸責於FPCA之故意或過失外，FPCA不負損害賠償責任。

(2) FPCA如因不可抗力之天災事故（例如地震等），或其他非可歸責於FPCA之事由（例如戰爭等），造成FUCA損失時，FPCA不負損害賠償責任。

(3) FPCA未善盡保管FUCA之註冊及憑證相關資料，而造成相關資訊洩漏、被冒用、竄改及任意使用致造成第三者遭受損害時，FPCA應負損害賠償責任。

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

9.8 責任限制

FPCA 與 FUCA，因簽發憑證或使用憑證而發生損害賠償事件時，雙方應承擔之損害賠償責任，以相關法令規定及合約所定之範圍為責任上限。

9.9 賠償

FUCA 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 FPCA 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 FUCA 負損害賠償責任。

FUCA 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 FUCA 負損害賠償責任。

FPCA 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 FUCA 註冊、憑證之簽發與廢止作業，或違反相關法律規範而造成 FUCA 之損失時， FPCA 應依規定賠償 FUCA 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 FUCA 損失時，FPCA 不負損害賠償責任。

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

9.10 有效期限與終止

9.10.1 有效期限

本作業基準於主管機關依電子簽章法核定通過後，於 FPCA 儲存庫公布後即生效。

9.10.2 終止

本作業基準新版本經 PMA 同意且主管機關核定後公布，現有版本即告終止。

9.10.3 終止與存續之效力

本作業基準之效力，維持至遵循本作業基準所簽發之最後一張憑證到期或廢止為止。

9.11 對參與者的個別通知與溝通

FPCA 將以適當的方式，與 FUCA 建立聯絡管道，包括但不限以下方式：電話、傳真或 E-mail。

9.12 修訂

9.12.1 修訂程序

本作業基準規範之權責管理單位為 FPCA 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「1.5.2 聯絡資料」，由 FPCA 客服中心處理。

9.12.2 通知機制與期限

(1) 對本作業基準有建議更新時，請將詳細的建議文件郵寄或E-mail至 1.5.2 節的聯絡窗口，交由FPCA憑證政策管理委員會審議。

(2) 本作業基準之修訂經主管機關審查核定後，於 10 個日曆天內公布於本憑證管理中心之儲存庫供下載。

(3) 除另有規定外，本憑證管理中心以 9.11 節規定之方式，做為與下屬憑證~~機構~~管理中心

(4) 間之變更聯絡機制。

9.12.3 修改憑證政策物件識別碼的事由

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

9.13 紛爭之處理程序

FUCA 與 FPCA 因使用憑證所引起之爭議處理程序或糾紛處理，以本作業基準為基礎，詳細處理步驟於業務作業規範及 FPCA 與 FUCA 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。

FUCA與FPCA遇有爭議時，FUCA與FPCA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規範處理。

FUCA與其他FUCA之爭議處理方式應以本處理程序為基礎。

9.14 管轄法律

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。

9.15 適用法律

本作業基準及FPCA應符合電子簽章法及其相關子法之規定。個人資料保護適用法律參考9.4.1節。

9.16 雜項條款

9.16.1 完整協議

無規定。

9.16.2 轉讓

本作業基準所敘述的主要成員之間的權利，不能在未通知FPCA之情況下，以任何形式轉讓給其他方。

9.16.3 可分割性

本作業基準的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，不受該項不適用之規定影響，直到新版之本作業基準更新完成並公告。

本作業基準之更新，依「9.12修訂」規定辦理。

9.16.4 契約履行

無規定。

9.16.5 不可抗力

如因不可抗力或其他不可歸責於FPCA之事由（例如戰爭或地震等），FPCA不負損害賠償責任。

9.17 其他條款

無規定。

附錄一　參考文件

1. 參考文件金融 XML 憑證共通性技術規範 (Version 1.2)，銀行公會，2012 年 6 月
2. 政府機關公開金鑰基礎建設憑證政策（第 2.0 版），國家發展委員會，2018 年 8 月
3. 金融機構辦理電子銀行業務安全控管作業基準，銀行公會，2018 年 3 月
4. 憑證實務作業基準應載明事項（報部定稿）
5. 中華民國銀行商業同業公會全國聯合會憑證政策管理委員會設置要點（104 年 2 月 26 日 PMA 第十次委員會議修正通過）
6. 金融憑證機構管理準則（93 年 8 月 26 日 PMA 第一次委員會議修正通過）
7. [RFC 5280] S. Farrell, S. Boeyen, R. Housley, W. Polk., “Internet X.509 Public Key Infrastructure Certificate and CRL Profile”, RFC 5280,May 2008.
8. [FIPS PUB 140-2]Federal Information Processing Standards Publication 140-2, Security Requirements For Cryptographic Modules, 25 May 2001.
9. [X.509] ITU-T Recommendation X.509 (1997 E): Information Technology - Open Systems Interconnection – The Directory: Authentication Framework, June 1997.
10. WebTrust Program for Certification Authorities (Version2.1)
11. EuroPKI Certificate Policy VERSION 1.1 (DRAFT 4)
12. X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA), June 14, 2001
13. [RFC 2256] M. Wahl, “A Summary of the X.500(96) User Schema for use with LDAPv3”, RFC 2256, December 1997.
14. [RFC 3647] Internet X.509 Public key Infrastructure Certificate Policy and Certification Practices Framework
15. [RFC 6960] A. Malpani, S. Galperin, C. Adams, “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP”, RFC 6960, June 2013.

附錄二　詞彙

(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、圖片、影像、符號或其他資料，以電子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)

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)

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)

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 (Certification Authority or Certificates Authority; CA)

指簽發憑證之機關、法人，為憑證上所載之簽發名義人。

(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; RCA)

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。

(18) 金融政策憑證管理中心 (Financial Policy Certificate Authority; FPCA)

為金融公開金鑰基礎建設之政策憑證管理中心，專責簽發用戶憑證管理中心之憑證；金融政策憑證管理中心之自身憑證係由金融最高層憑證管理中心簽發。

(19) 金融用戶憑證管理中心 (Financial User Certificate Authority; FUCA)

為金融公開金鑰基礎建設之用戶憑證管理中心，簽發之用戶憑證供用戶及信賴憑證者使用於銀行公會所規範之業務範圍；金融用戶憑證管理中心之自身憑證係由金融政策憑證管理中心簽發。

(20) 註冊中心 (Registration Authority; RA)

為主要負責鑑別憑證申請者的身分及簽發憑證所需之相關資訊供憑證管理中心簽發憑證。

(21) 憑證用戶 (Subscriber)

為使用憑證於銀行公會所規範之業務範圍進行交易之個人或法人。

(22) 信賴憑證者 (Relying Party)

為使用他人（憑證用戶）之憑證、憑證鏈資訊，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。

附錄三 字首與縮寫

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
FPCA	Financial Policy Certification Authority
FRCA	Financial Root Certification Authority
ISO/IEC	The International Organization for Standardisation/ The International Electrotechnical Commission
ITSEC	Information Technology Security Evaluation Criteria
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificates Status Protocol
OECD	Organization for Economic Co-operation and Development
OID	Object Identifier
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)
TCSEC	Trusted Computer System Evaluation Criteria
UCA	User Certification Authority
URL	Universal Resource Location