金融用戶憑證管理中心
憑證實務作業基準
Certification Practice Statement

(第 2.1 版)

Version 2.1

生效日期：中華民國 100 年 5 月 6 日

Effective Date： 2011/05/06

本作業基準版本變更紀錄：

版 本	生效日期	發 行 者	備 註
1.0	92/01/01	TaiCA PMA	初版擬訂
2.0	97/03/10	TWCA PMA	1. 配合 94 年 3 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」。
2.1	100/05/06	TWCA PMA	1. 修訂 CPS 用字。 2. 修訂憑證「交易限額」與「賠償限額」。

目 錄

金融用戶憑證管理中心（FUCA）憑證實務作業基準

(Certification Practice 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：

100/05/06 經濟部函 經商字第 10002053740 號。

1.2 憑證之保證等級及適用範圍(Certificate's Applicability)

金融用戶憑證管理中心(Financial User Certification Authority，以下簡稱 FUCA)之用戶為一般自然人或法人憑證用戶(Subscriber，以下簡稱憑證用戶)，憑證用戶之憑證可使用範圍如下表所示，若有其他約定，則從其約定。

憑證適用對象	憑證適用範圍
法人	網路銀行、網路報稅、電子發票
自然人	

FUCA 憑證用戶之身分鑑別依據「4.1.8 憑證用戶身分之鑑別(Authentication of Subscribers Identity)」之規範執行，並無不同層級之身分鑑別程序，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)

FUCA 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：

憑證用戶向註冊中心申請憑證時，必須臨櫃提供詳細且正確之身分證明文件與資料，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；憑證用戶因故意、過失或不正當意圖而提供不實資料，致造成他人遭受損害時，應由該憑證用戶負損害賠償責任。

憑證之使用：

憑證用戶必須自行產生金鑰並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、曝露或遺失等不安全之顧慮時，或不再使用該憑證時，必須即刻向註冊中心辦理申告及處理；如因故意或過失，致造成他人遭受損害時，應由該憑證用戶負損害賠償責任。

憑證用戶必須依照本作業基準與業務應用系統規範之規定，合法且正確的使用私密金鑰與憑證於相關之業務，不得使用於 1.本作業基準規範之外、2.會造成人身傷亡與精神侵害，或對社會秩序與公共利益有重大危害之應用或業務系統、3.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；如將憑證使用於非本作業基準規範之業務範圍，或違反相關法令規範時，應由該憑證用戶負損害賠償責任。

憑證用戶及信賴憑證者皆應依本作業基準 1.2 節記載之適用範圍使用於適用之業務範圍內，並須遵循用途及交易對象之限制，且交易之金額不得超過「3.2.4 交易及賠償限額(Transaction and Loss Limitation)」表列之交易限額。

賠償責任：

FUCA 如因作業人員之故意或過失，使其未遵照本作業基準、憑證政策及相關作業規範之規定辦理憑證用戶憑證之簽發、更新、暫時停用與廢止作業，或違反相關法律規範而造成憑證用戶之損失時，FUCA 應依本作業基準之規定賠償憑證用戶之損失。

註冊中心如因作業人員之故意或過失，使其未遵照本作業基準、憑證政策及相關作業規範之規定辦理憑證用戶之註冊與身分鑑別之作業，或違反相關法律規範而造成憑證用戶之損失時，應由該註冊中心負責賠償憑證用戶之損失。

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，或其他不可抗力的事故（例如戰爭或地震等），致所簽發之憑證造成憑證用戶損失時，FUCA 不負損害賠償責任。

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) 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。

本公司負責維運 FUCA。FUCA 為銀行公會 PKI 階層架構下之金融用戶憑證管理中心，本公司依據 X.509（Public Key Infrastructure Certificate Policy and Certification Practice Statement Framework）國際標準、金融 XML 憑證共通性技術規範及主管機關(如：經濟部)之規範，制訂本作業基準。

FUCA 之憑證用戶為一般自然人及法人憑證使用者，FUCA 提供憑證用戶憑證簽發、更新、廢止、暫時停用等相關憑證作業。本作業基準遵循對應之 FRCA 憑證政策（Certificate Policy，CP）說明 FUCA 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 日所發行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所公布之「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。

憑證用戶在了解本作業基準規範前，建議已熟悉如下所列基本公開金鑰基礎建設(Public Key Infrastracture，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) 交易訊息機密性(Confidentiality)的密碼系統，例如對稱性或非對稱性的密碼系統。

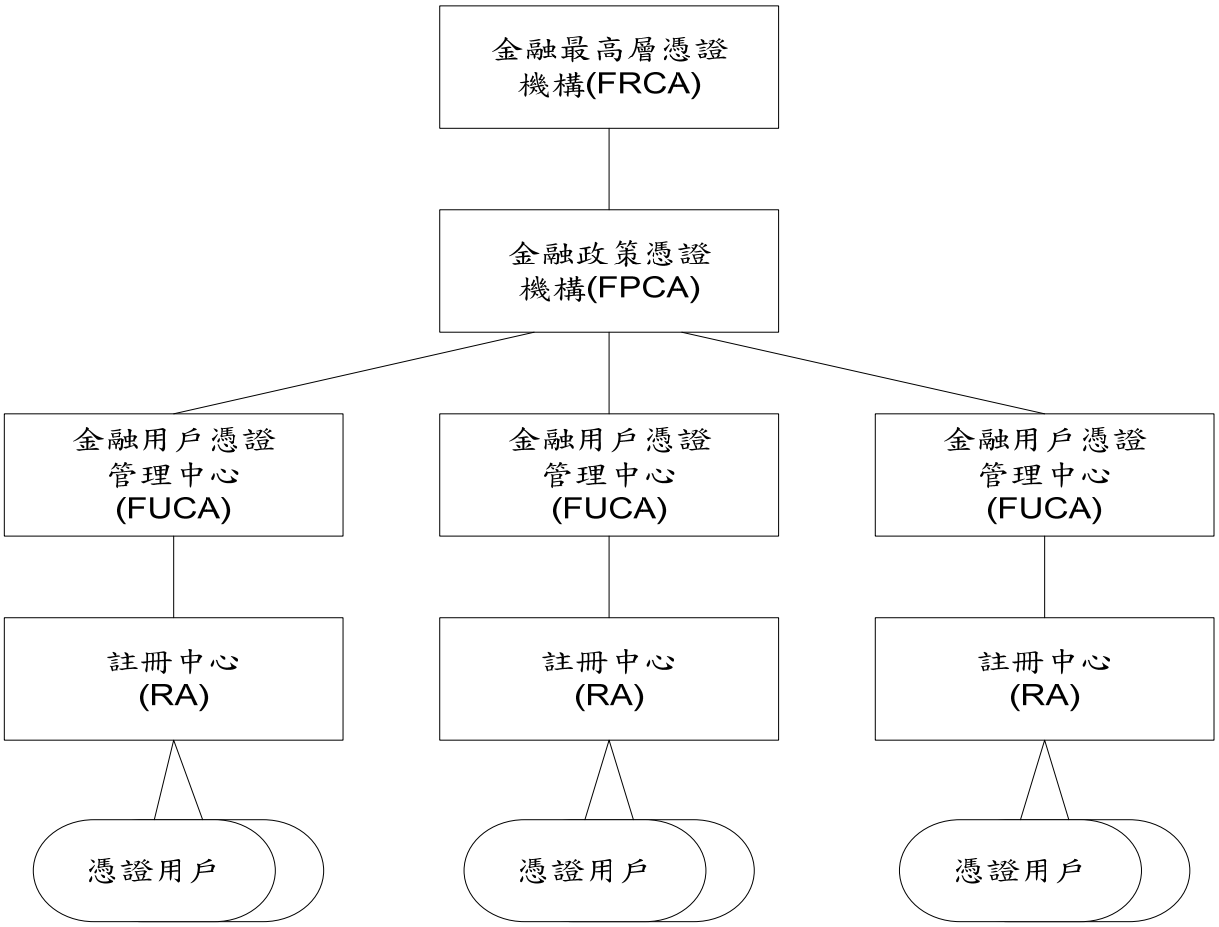
(3) 非對稱性的密碼系統，公開金鑰對(Public Key Pairs)，公開金鑰憑證(Public Key Certificate)，例如數位簽章與數位信封(Digital Envelope)的機制。

(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 FUCA 之實際營運架構並未包含下列所有單元。



2.3.2 金融最高層憑證機構(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、憑證廢止清冊(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、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 金融政策憑證機構(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 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、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。

2.3.4 金融用戶憑證管理中心(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鑑別方式，傳輸之交易訊息之完整性與機密性之安控措施），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至回註冊中心。

(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、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) 管理、公告，並遵循 FUCA 規範之憑證用戶（自然人或法人）註冊申請及身分鑑別作業程序（例如：憑證用戶註冊之身分鑑別之安控措施，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簽發、更新、暫時停用、廢止及查詢申請訊息，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。

(5) 提供線上憑證更新服務機制。

(6) 應通知憑證即將到期之用戶辦理憑證更新作業。

2.3.6 使用者(End Entities)

2.3.6.1 憑證用戶(Subscribers，SC)

憑證用戶（自然人或法人），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 之憑證政策及本作業基準之規範，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) 之憑證做訊息之加密後，將加密之訊息傳送至接收者，以達到通訊雙方訊息之機密性。

2.3.7 應用(Applicability)

本作業基準適用於所有由 FUCA 所簽發之憑證，並說明簽發、使用、更新、暫時停用及廢止憑證用戶憑證之作業實務。FUCA 所簽發之憑證，具備身分識別、不可否認性、訊息完整性及訊息機密性之安全機制。

FUCA 憑證適用範圍載明於憑證內之「憑證政策(Certificate Policy : CP)憑證簽發者的簡要聲明(TerseStatement)」欄位：

(1) 憑證之使用範圍：依據「1.2 憑證之保證等級及適用範圍」所述。

(2) 憑證之適用範圍限制：憑證用戶及信賴憑證者皆應依本作業基準 1.2 節記載之適用範圍使用於適用之業務範圍內，並須遵循用途及交易對象之限制，且交易之金額不得超過「3.2.4 交易及賠償限額(Transaction and Loss Limitation)」表列之交易限額。

(3) 憑證禁止使用之狀況：憑證用戶之憑證除使用於上述規定之範圍外，絕不可使用於會造成人身傷亡與精神侵害，或對社會秩序與公共利益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)

本作業基準之制訂、修訂、發布等事宜，其權責單位為 FUCA 之憑證政策管理委員會。

2.4.2 聯絡窗口(Contact Person)

憑證用戶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。

憑證用戶有關憑證的申請、更新、暫時停用、廢止、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	台北市中正區(100)延平南路 85 號 10 樓 10TH Floor,85,Yen-Ping South Road,Taipei,Taiwan, R.O.C
電話	886-2-23708886
傳真	886-2-23700728
電子郵箱(E-mail)	ca@twca.com.tw

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須修改變更時，須經由 FUCA 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 義務(Obligations)

3.1.1 金融用戶憑證管理中心之義務(FUCA Obligations)

FUCA 於執行憑證用戶憑證之簽發、更新、暫時停用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準則、・・等）規劃建置憑證系統，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。

FUCA 之義務包含：

(1) 訂定、公告及管理 FUCA 業務範圍內之憑證政策及憑證實務作業基準規範。

(2) FUCA 憑證管理作業之運作，必須依據主管機關之作業規範與 FUCA 憑證政策之規範。

(3) 確認 FUCA 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) FUCA 與其作業人員必須善盡保管憑證用戶之憑證資料及相關訊息之義務，避免相關資訊洩漏、被冒用、竄改及任意使用。

(5) FUCA 應依照憑證政策及本作業基準之規範，接受註冊中心傳遞之憑證用戶憑證之申請、更新、暫時停用及廢止憑證之申請等有關訊息，確認註冊中心發送至 FUCA 之相關交易訊息之正確性與安全性，並執行憑證簽發、更新、暫時停用與廢止之相關作業，及將相關回覆訊息正確及安全地遞送至註冊中心。

(6) FUCA 若更新憑證，必須以最迅速安全之方式遞送予憑證用戶或通知憑證用戶至 FUCA 索取。

(7) FUCA 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，立即向銀行公會及上屬憑證機構（FPCA）辦理申告與處理。

(8) 憑證用戶申請或廢止憑證時，FUCA 依照憑證政策及本作業基準之規範，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。

(9) FUCA 與憑證用戶之合約或相關作業文件，應詳細說明憑證申請、更新、廢止、暫時停用與使用之作業規範，及相關之權利與義務關係。

(10) FUCA 簽發憑證用戶憑證與 CRL 之私密金鑰必須獨立使用，絕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。

3.1.2 註冊中心之義務(Registration Authority Obligations)

FUCA 之註冊中心由金融機構擔任，惟金融機構得委託其他單位代為處理註冊中心之事務，但應就該單位之行為與自己之行為負同一義務，註冊中心之義務包括：

(1) 依本作業基準、憑證政策及註冊中心的作業規範，確認註冊中心與用戶的權責關係，執行憑證用戶註冊身分鑑別及憑證相關作業的運作。

(2) 確認註冊中心註冊管理系統作業人員〈含合約委外人員〉的選用與系統運作符合本作業基準、與註冊中心的作業規範。

(3) 註冊中心必須確認憑證用戶於註冊申請時，確實了解且同意申請書與合約書上的權利與義務，及業務相關作業規範的內容，並由用戶簽名確認（或法人用戶的合法授權代理人員之簽名確認）。

(4) 接受憑證用戶註冊、憑證申請、更新、暫時停用及廢止、查詢之作業，並提供憑證管理中心之憑證鏈。

(5) 註冊中心於憑證用戶註冊申請時，鑑別用戶身分的合法性與訊息的完整性，完成後通知 FUCA 簽發憑證予憑證用戶。

(6) 註冊中心於憑證用戶申請暫時停用或廢止憑證時，鑑別用戶身分的合法性與訊息的完整性，完成後通知 FUCA 暫時停用或廢止憑證予憑證用戶。

(7) 註冊中心經手憑證相關作業，並留存相關資料，註冊中心與其作業人員必須善盡保管憑證用戶註冊資料及相關訊息之義務、避免相關資訊洩漏、被冒用、竄改及任意使用。

(8) 註冊中心與憑證用戶的合約或相關作業文件，詳細說明憑證申請、更新、暫時停用廢止、查詢、註冊與使用的作業規範，及相關的權利與義務關係。

(9) 註冊中心負責憑證用戶註冊管理作業相關的權責義務，註冊中心必須提供本節所述權責義務關係之資訊予憑證用戶及信賴憑證者。

(10) 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資訊有異動時，必須依相關作業的規定，即刻向 FUCA 辦理申告與處理。

3.1.3 用戶之義務(Subscriber Obligations)

FUCA 之憑證用戶為自然人或法人，憑證用戶之義務包含：

(1) 憑證用戶向註冊中心申請憑證時，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：本作業基準）之內容，並且於同意接受該規範之規定下始可簽名確認。

(2) 憑證用戶必須依據 FUCA 憑證實務作業基準之規定，確實且妥善安全地產製與保護其私密金鑰。

(3) 憑證用戶必須了解且同意 FUCA 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) 憑證用戶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，或憑證內憑證用戶相關之資訊有異動時，憑證用戶必須依相關作業之規定，即刻向註冊中心辦理申告與處理。

(5) 憑證用戶憑證申請時必須提供詳實且正確之資訊，接受 FUCA 簽發之憑證用戶憑證時，必須確認憑證資訊之內容為憑證用戶註冊申請之資訊，且公開金鑰與憑證用戶之私密金鑰為相關之一對金鑰。

(6) 憑證用戶憑證之使用，必須依 FUCA 憑證政策及憑證實務作業基準之規定、應用業務系統之作業規定、X.509 憑證標準之規範，由憑證鏈(Certificates

Chain)逐一驗證該憑證之正確性及有效性，當有憑證廢止清冊(CRL)機制時，尚須檢核此憑證是否為廢止憑證。

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

FUCA 之信賴憑證者為其他 FUCA 之憑證用戶，信賴憑證者之義務包括：

(1) 信賴憑證者使用或接受他人（憑證機構、憑證用戶）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所規定的業務範圍，確認該憑證之合法用途，並於該憑證使用目的範圍內，信賴該憑證。

(2) 該憑證使用於相關的業務系統，無任何違反相關法律的規定與侵害第三者的權利。

(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。

(5) 信賴憑證者查詢憑證狀態時，若該憑證非 FUCA 所簽發時，信賴憑證者應向該憑證之簽發機構查詢。

3.1.5 儲存庫之義務(Repository Obligations)

FUCA 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) 確認儲存庫管理系統作業人員（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) 當有新簽發憑證用戶憑證或公布 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 24 小時提供正常服務。

(3) 鑑別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) 儲存庫之作業人員必須善盡保管憑證用戶註冊憑證及相關訊息之義務，避免相關資訊洩漏、被冒用、竄改或任意使用。

(5) 儲存庫使用的私密金鑰有被冒用、曝露或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，辦理申告與處理。

3.2 賠償責任(Liability)

FUCA 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)」，非本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 金融用戶憑證管理中心之賠償責任(FUCA Liability)

(1) FUCA 如因作業人員之故意或過失，使其未遵照本作業基準、憑證政策及相

關作業規範之規定辦理憑證用戶憑證之簽發、更新、暫時停用與廢止作業，或違反相關法律規範而造成憑證用戶之損失時，FUCA 應依本作業基準之規定賠償憑證用戶之損失；有關用戶單一憑證之最高賠償金額規範訂於「3.2.4 交易及賠償限額」。

(2) 如非因本憑證管理中心之故意或過失，造成網際網路傳輸之中斷或故障，或其他不可抗力之事故（例如戰爭或地震等），致所簽發之憑證造成憑證用戶損失時，FUCA 不負損害賠償責任。

(3) 憑證用戶或其他有權者提出廢止憑證用戶憑證之要求後，至 FUCA 實際完成廢止該憑證用戶憑證為止之期間內，當該憑證用戶憑證被用以進行非法交易，或進行交易後產生法律糾紛時，FUCA 如依據本作業基準與相關之作業規範執行處理作業時，則不負損害賠償責任。

(4) 憑證用戶或其他有權者提出暫時停用憑證用戶之憑證要求後，至 FUCA 實際完成暫時停用該憑證用戶憑證為止之期間內，當該憑證用戶憑證被用以進行非法交易，或進行交易後產生法律糾紛時，FUCA 如依據本作業基準與相關之作業規範執行處理作業時，則不負損害賠償責任。

(5) 憑證用戶之賠償請求權時效期間，依主管機關與相關法律之規範辦理。

(6) 憑證用戶或信賴憑證者透過 FUCA 查詢其他 UCA 所簽發憑證之憑證狀態時，若該 UCA 因作業緣故未及時更新 CRL 或 OCSP 資料，致 FUCA 傳遞予憑證用戶或信賴憑證者之資訊錯誤，而導致憑證用戶或信賴憑證者損失時，FUCA 不負損害賠償責任。

3.2.2 註冊中心之賠償責任(RA Liability)

(1) 註冊中心與其作業人員未善盡保管憑證用戶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憑證用戶或第三者遭受損害時，註冊中心與該作業人員應依與憑證用戶合約之規定負損害賠償責任。

(2) 註冊中心如因作業人員之故意或過失，未遵照本作業基準、憑證政策及註冊中心相關作業規範的規定辦理註冊作業，或違反相關法律規範而造成用戶的損失，或致善意第三人受有損失者，由註冊中心負損害賠償責任。

(3) 註冊中心因應用系統或軟體之錯誤，未能於本作業基準及註冊中心作業規範所規定之作業時間內，將憑證用戶憑證申請、更新、暫時停用及廢止之請求訊息傳送至 FUCA 處理，而導致憑證用戶或信賴憑證者之損失時，註冊中心應負損害賠償責任。

3.2.3 用戶之賠償責任(Subscriber Liability)

(1) 憑證用戶向註冊中心申請註冊時，因故意、過失或不正當意圖而提供不實資料，致造成 FUCA 或第三者遭受損害時，應由該憑證用戶負損害賠償責任。

(2) 憑證用戶應妥善保管其私密金鑰與密碼，不得洩漏或交付予他人使用，如因故意或過失，致造成 FUCA、註冊中心或第三者遭受損害時，應由該憑證用戶負損害賠償責任。

(3) 憑證用戶使用憑證或使用信賴憑證者憑證，有違反 FUCA 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，憑證用戶應自行負損害賠償責任。

(4) 憑證用戶使用憑證時之檢核，未依 FUCA 憑證政策、本作業基準、應用業務系統之作業規定、X.509 憑證標準之規範逐一檢核，致造成 FUCA 或第三者遭受損害時，應由該憑證用戶負損害賠償責任。

(5) 憑證用戶或其他有權者提出廢止憑證用戶憑證之要求後，至 FUCA 實際完成廢止該憑證用戶憑證為止之期間內，當該憑證用戶憑證被用以進行非法交易，或進行交易後產生法律糾紛時，如 FUCA 執行處理作業時，符合本作業基準與相關之作業規範，則憑證用戶必須負損害賠償責任。

(6) 憑證用戶或其他有權者提出暫停使用憑證用戶憑證之要求後，至 FUCA 實際完成暫停使用該憑證用戶憑證為止之期間內，當該憑證用戶憑證被用以進行非法交易，或進行交易後產生法律糾紛時，如 FUCA 執行處理作業時，符合本作業基準與相關之作業規範，則憑證用戶必須負損害賠償責任。

(7) 其他與業務相關之償責，訂定於業務相關之作業規範與憑證用戶之業務合約規範。

3.2.4 交易及賠償限額(Transaction and Loss Limitation)

(1) 交易限額：依安全性、用途別、客戶身分及適用業務範圍等分別訂定不同之交易限額；用戶進行交易時，其交易金額不可超出該使用範圍代碼所對應之交易限額。

(2) 賠償限額：依安全性、用途別、用戶身分等分別訂定不同之賠償限額；該賠償限額係指對用戶單一憑證之賠償上限，亦即不論交易次數多寡，單一憑證之累積賠償金額均不得超過賠償限額。

(3) FUCA 及註冊中心對測試憑證均未執行任何鑑別用戶身分之程序，且僅供測試使用，不可使用於測試以外之任何應用或業務，FUCA 及註冊中心對測試憑證不做任何形式之保證及負擔任何形式之責任。

(4) 若用戶與 FUCA 訂有合約，另行載明憑證使用範圍、交易限額及賠償限額者，從其約定。

各級憑證之交易限額及賠償限額說明如下：

適用對象	適用範圍	交易限額（NT$）	賠償限額（NT$）
法人	網路銀行、網路報稅、電子發票	不限定	2,500,000
自然人	網路銀行、網路報稅、電子發票	不限定	1,000,000

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)

因信賴憑證者或憑證用戶之故意或過失，而非為 FUCA 或註冊中心之過失，所造成第三者財務、信譽及其他各方面之損失時，FUCA 或註冊中心擁有賠償責任豁免權。

如因信賴憑證者或憑證用戶之故意或過失且可歸責於信賴憑證者或憑證用戶，而造成 FUCA 或其他第三者財務、信譽及其他各方面之損失時，信賴憑證者或憑證用戶必須負損害賠償責任，FUCA 或註冊中心可依照相關法律之規定向信賴憑證者或憑證用戶請求賠償。

3.3.2 代理(Fiduciary Relationships)

依據本作業基準所簽發之憑證，FUCA 與註冊中心、或 FUCA 與憑證用戶、或註冊中心與憑證用戶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)

FUCA 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，且被正式授與簽發憑證用戶憑證之資格。

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，如有跨國或跨區域的業務整合需求時，除配合業務整合規範所需之外，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、義務存續性、權利義務之整合及訊息公布(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。

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

依本作業基準與相關業務之規範，FUCA 與憑證用戶或註冊中心間資訊通知之

往來，可以下列傳遞方式：

(1) 電子訊息 ─ 傳送者將已簽章之訊息傳送至接收者，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 3 天前（國外航空郵寄至少於 1 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。

3.4.3 爭議處理程序(Dispute Resolution Procedures)

憑證用戶與 FUCA 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 FUCA 與憑證用戶之合約內說明。

爭議之雙方如無法於 14 天內合理之協商解決爭議，則得經雙方同意由金融最高層憑證機構之憑證政策管理委員會擔任公正第三協調者，以進行協調並解決爭議，且雙方必須同意協調者的協商與裁決。

爭議之雙方如無法於 30 天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。

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

註冊中心與 FUCA 遇有爭議時，雙方應本誠信原則協商解決之；如涉訴訟時，雙方同意以臺北地方法院為第一審管轄法院。

於爭議協商、訴訟處理過程所發生之費用分擔，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 憑證申請或更新收費(Certificate Issuance or Renewal Fees)

FUCA 與註冊中心或憑證用戶間之註冊、憑證申請、更新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)

FUCA 與註冊中心或憑證用戶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)

FUCA 與註冊中心或憑證用戶間之憑證狀態查詢(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)

憑證用戶經由網際網路至 FUCA 下載本作業基準或相關業務之憑證政策，FUCA 不計收任何服務費用，但如向 FUCA 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，FUCA 須向憑證用戶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)

FUCA 對註冊中心所有憑證服務項目之收費，包含但不限於憑證費用、憑證查詢費用、憑證廢止與憑證狀態資訊查詢費用、建置費用、參加年費等，FUCA 均不退還註冊中心任何費用。

FUCA 對憑證用戶所有憑證服務項目之收費，除憑證費用之外，包含但不限於憑證查詢費用、憑證廢止與憑證狀態資訊查詢費用等，FUCA 均不退還憑證用戶任何費用。

憑證用戶在憑證簽發後 7 天內廢止憑證者，FUCA 將扣除手續費後將剩餘費用退還憑證用戶，憑證簽發超過 7 天者，FUCA 將不退還憑證用戶任何費用。

憑證用戶退費作業規範於合約，退費詳細運作程序另訂定於相關憑證業務之作業規範。

3.6 公布與儲存 (Publication and Repository)

3.6.1 FUCA資訊公布(Publication of TFUCA 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 FUCA 之網站供用戶下載使用；網址：http://www.twca.com.tw/cps.asp。

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

3.6.2 公布頻率(Frequency of Publication)

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，FUCA 應於接到核定公文 1 個月內公告於網站(http://www.twca.com.tw/cps.asp)。

FUCA 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 24 小時產生及公布 1 次。

3.6.3 存取管控(Access Control)

FUCA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(http://www.twca.com.tw/cps.asp)。

3.6.4 儲存庫(Repositories)

FUCA 以目錄伺服器之作業方式提供憑證用戶，憑證作業實務與憑證相關作業文件、憑證用戶憑證與 FUCA 憑證、廢止憑證清冊(CRL)、憑證用戶與 FUCA 資訊之查詢及使用，FUCA 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)

FUCA 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)

FUCA 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 Infor-mation Security Management 編撰)每年至少定期執行 1 次內部自行查核作業與外部例行性查核，必要時得接受金融最高層憑證機構之憑證政策管理委員會派員執行專案查核。

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

FUCA 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 2 年以上之稽核相關經驗，且須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)

FUCA 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。

FUCA 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)

稽核人員查核：

(1) 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) 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) 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) 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) 業務執行之公告：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：私密金鑰與相關憑證之生命週期（產生、建置、使用、廢止、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) 環境之安全控管：符合 FUCA 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)

FUCA 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。

FUCA 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 FUCA 的營運；在發現重大缺失時，金融最高層憑證機構之憑證政策管理委員會得撤銷 FUCA 擔任憑證管理中心之資格。

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，與信賴憑證者信賴用戶憑證的相關資訊均公開提供。FUCA 將公布最近一次的稽核結果於公司網站上。

3.8 機密性(Confidentiality)

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

FUCA/註冊中心對於憑證用戶資訊機密性之保護，必須於憑證用戶資訊保密策略規範中訂定，對於憑證用戶資訊之保護，必須依照「個人資料保護法」或其他政府單位相關之規範運作，且符合 OECD 隱私權與個人資料保護之規範(OECD; Organization for Economic Co-operation and Development,Guidelines on the

Protection of Privacy and Transborder Flows of Personal Data) 。

FUCA/註冊中心於管理及使用憑證用戶註冊、憑證申請之相關資訊時，除憑證用戶憑證內容可公開外，憑證用戶之註冊基本資料與身分認證資料，非經由憑證用戶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下列資訊必須嚴謹且機密的保護：

(1) 憑證用戶身分鑑別資訊（例如：憑證用戶名稱、聯絡資訊等）。
(2) 憑證用戶註冊或憑證申請、更新、暫停使用與廢止時交易的相關機密性訊息。
(3) 憑證用戶註冊時填寫於註冊相關申請單、合約上的憑證用戶資訊，與身分證明文件（或影印本）上的機密性資訊。

FUCA/註冊中心為憑證管理作業之需求而使用與存取憑證用戶資訊時，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。FUCA/註冊中心管理與使用憑證用戶資訊時，憑證用戶之註冊基本資料與身分認證資料，非經由憑證用戶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)

FUCA 公告於目錄伺服器之憑證用戶憑證資訊，憑證狀態（提供憑證有效性狀態查詢功能時），及 FUCA 之憑證資訊、憑證政策、憑證作業實務基準，為可公開之非機密性資訊。

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

FUCA 依據作業規範處理憑證用戶憑證之廢止時，依據「5.4.9 憑證廢止清冊產生頻率（CRL Issuance Frequency）」之規範，公告於憑證資料庫或目錄伺服器憑證廢止清冊(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，否則憑證用戶之註冊基本資料與身分認證相關資料絕不任意提供予權責管理單位，或其他任何人知悉使用：

(1) 政府法律、規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)

FUCA/註冊中心絕不任意提供憑證用戶之註冊基本資料與身分認證資料，當因憑證之交易產生民事訴訟而必須存取憑證用戶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) 憑證用戶以數位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)

FUCA 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、或憑證用戶自己之授權需求、或 FUCA 合法用途且正式申請外，FUCA 目前尚無公告憑證用戶資訊之其他公告條件。

3.9 智慧財產權(Intellectual Property Rights)

本公司於 FUCA 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，則其智慧財產權為本公司所有。

FUCA 憑證政策、本作業基準、與執行憑證管理作業相關文件，其智慧財產權皆為本公司所有。

憑證用戶產生之私密金鑰與公開金鑰，為憑證用戶所擁有之財產權，但公開金鑰經 FUCA 簽發成憑證格式，該憑證為 FUCA 之智慧財產權，FUCA 只提供憑證用戶與信賴憑證者公開金鑰憑證之使用權限。

FUCA 產生之 FUCA 憑證，為 FUCA 所擁有之智慧財產權，FUCA 只提供憑證用戶與信賴憑證者使用之權限。

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

4. 識別與鑑別(Identification and Authentication)

4.1 註冊(Initial Registration)

註冊中心於憑證用戶註冊時，應依據「4.1.8 憑證用戶身分之鑑別(Authentication of Subscribers Identity)」作業規範，驗證憑證用戶申請之證明文件，正確之驗證憑證用戶之資格。憑證用戶向 FUCA 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，即為憑證用戶必須先完成註冊作業程序。

4.1.1 識別名稱之種類(Type of Names)

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

下為發行者之一般識別名稱之說明：

識別名稱(DN)	說　　明	內　容
1.Country(C)	CA 公司所在地之國碼	C = TW
2.Organization(O)	CA 公司英文名稱	O = TWCA
3.OrganizationUnit(OU)	CA 所屬性質資訊	OU = User CA
4.CommonName(CN)	CA 應用或服務英文名稱	CN=TWCA Financial User CA

4.1.4 識別名稱之唯一性(Uniqueness of Names)

FUCA 憑證使用之憑證用戶中、英文名稱及識別名稱於憑證系統中必須為唯一，但當憑證用戶有相同之註冊名稱或識別名稱時，以先申請註冊之憑證用戶優先使用，後申請者於註冊名稱後加重號編號（2 碼）、或另由憑證用戶使用自選編號，以資區別與識別不同之憑證用戶。

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

當憑證用戶使用之識別名稱有相同時，FUCA 以先申請註冊之憑證用戶優先使用，相關之糾紛仲裁處理非為 FUCA 之管轄權責，憑證用戶必須向金融最高層憑證機構之憑證政策管理委員會提出申請。

當憑證用戶使用之識別名稱，經有權主管機關合法文件證實為其他申請者所擁

有時，FUCA 即刻廢止先前使用者之憑證用戶識別名稱使用權，該使用者必須負擔相關之法律權責；且鑑別該憑證用戶註冊識別名稱使用之合法性，非為 FUCA 之業務權責範圍。

4.1.6 註冊商標之認可與鑑別(Recognition, Authentication and role of Trademarks)

FUCA 尊重憑證用戶識別名稱有關註冊公司中、英文名稱之註冊商標權，並接受憑證用戶之使用，但不保證憑證用戶註冊商標之認可、鑑別與唯一性，相關之糾紛仲裁處理非為 FUCA 之管轄權責範圍，憑證用戶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)

憑證用戶於自行產生公開金鑰及私密金鑰後，以公開金鑰向 FUCA 申請用戶憑證的簽發時，申請訊息應以用戶私密金鑰進行簽章，並傳送至 FUCA，當 FUCA 驗證申請訊息無誤完成憑證簽發，即確定用戶擁有此私密金鑰。

註冊中心必須驗證憑證用戶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憑證用戶所擁有之私密金鑰：

(1) 於憑證用戶申請憑證，以憑證用戶私密金鑰執行憑證用戶憑證申請訊息之簽章時，註冊中心必須驗證憑證用戶憑證申請訊息內，經保護之憑證用戶身分資訊、公開金鑰與私密金鑰之正確性與唯一性及合法性。

(2) 憑證用戶除以簽章方式驗證私密金鑰擁有之合法性與正確性外，亦可由註冊中心以憑證用戶之公開金鑰將訊息亂碼加密後，經數位信封之方式傳遞至憑證用戶，憑證用戶驗證無誤後，再將該訊息以私密金鑰簽章後，回覆確認訊息傳回註冊中心，且經註冊中心驗證無誤。

4.1.8 憑證用戶身分之鑑別(Authentication of Subscribers Identity)

註冊中心應依據下列程序，執行憑證用戶註冊身分與識別名稱之鑑別程序：

適用對象	**身分鑑別程序**
法人	憑證申請者應臨櫃親自辦理，或委任代理人代為臨櫃辦理。 憑證申請者若委託他人代為辦理，應出具委託書及委託人之身分證明文件。 註冊中心須鑑別組織名稱、所在地及代表人名稱之真實性，且須鑑別該憑證申請者是否有權以該組織之名義申請憑證。

自然人	憑證申請者應臨櫃親自辦理，或委任代理人代為臨櫃辦理。 憑證申請者若委託他人代為辦理，應出具委託書及委託人之身分證明文件。 註冊中心須比對身分證明文件，證明為其本人，如為委託代理人辦理，也須鑑別委託書之真偽及比對委託人之身分證明文件。

4.2 憑證及私密金鑰之更新(Routine Rekey)

憑證用戶金鑰之生命週期最長為 2 年，憑證用戶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 FUCA 申請新憑證簽發，此為私密金鑰之更新（Rekey）。憑證申請程序應依據「5.1 憑證申請(Certificates Application)」之規範。

當憑證用戶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，並向註冊中心申請新憑證之簽發。為風險管理與安全考量，憑證用戶向註冊中心申請新憑證簽發時，不可使用舊公開金鑰對。

註冊中心須於憑證有效期限屆滿前，通知用戶進行憑證更新。用戶憑證已廢止或有效期限已過期時，不可執行憑證及私密金鑰的更新作業。

憑證用戶每 9 年必須重新註冊一次。

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

FUCA 不提供憑證用戶廢止憑證之私密金鑰之更新，憑證用戶必須重新執行註冊之身分確認，並重新產生新公開金鑰對，向註冊中心申請新憑證之簽發。憑證申請程序應依據「5.1 憑證申請(Certificates Application)」之規範。

4.4 憑證廢止需求(Revocation Request)

廢止作業依「5.4 憑證之廢止及暫時停用」憑證作業系統的廢止規範辦理。

5. 憑證系統管理(Operation Requirements)

5.1 憑證申請(Certificates Application)

憑證用戶向註冊中心提出註冊及憑證申請：

(1) 註冊中心必須確實說明申請單與合約書上之權利與義務規範，相關業務運作之作業流程，憑證用戶同意後確認。

(2) 憑證用戶應正確且詳實之填寫相關申請單並提供相關證明文件。憑證用戶依據申請之憑證等級，提供註冊中心適當之身分證明文件（例如身分證或公司之營利事業登記證）及相關資訊。

(3) 註冊中心依據「4.1.8 憑證用戶身分之鑑別(Authentication of Subscribers Identity)」之作業規範，鑑別憑證用戶之身分；身分鑑別程序完成後，註冊中心提供憑證用戶身分識別代碼及保護密碼，完成憑證用戶註冊及憑證申請作業。

(4) 憑證用戶自行產生公開金鑰對及 PKCS#10 憑證申請檔，透過註冊中心驗證無誤後，由註冊中心向 FUCA 申請憑證用戶憑證之簽發。

(5) 憑證用戶若提出憑證更新申請，可不必填寫申請單，註冊中心透過電話或電子郵件方式確認申請者身分。

5.1.1 憑證申請政策(Certificate Application Policy)

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

(2) 憑證更新：憑證用戶憑證之使用有效期限將屆滿時，依據「5.1 憑證申請(Certificates Application)」之作業規範，向 FUCA 申請憑證之更新。

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

(4) 憑證暫時停用：憑證用戶之憑證暫時停用後，未解除暫時停用或確實廢止該憑證前或憑證效期結束時，憑證用戶不允許向 FUCA 申請新憑證之簽發。

5.1.2 憑證更新政策(Certificate renewal(Extend) Policy)

憑證用戶憑證更新作業方式悉遵照 FUCA 與註冊中心的業務需求與作業規範辦理，憑證系統如有配合業務系統安全性管控的需求時，則不提供憑證更新之功能，憑證用戶必須重新產生新公開金鑰對，才可向 FUCA 申請憑證簽發。

業務系統允許憑證用戶更新憑證時，為了安全的風險考量，憑證最多只能更新 1 次。

憑證用戶之憑證若已過期，或為無效之憑證時，絕不可執行憑證的更新。

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

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

(2) 憑證用戶執行憑證暫時停用完成後，於憑證有效期間終止前，如未執行憑證的解禁（解除暫時停用），則此張憑證皆存在廢止憑證清冊中為無法使用的憑證；如於該張憑證有效期間終止前，憑證用戶向註冊中心申請解禁完成時，則此張憑證自憑證廢止清冊中移除而成為有效憑證，直到憑證的有效期限結束而成為過期無效之憑證。

(3) 憑證用戶之憑證若已過期或為無效之憑證時，絕不可執行憑證的暫時停用與解禁。

5.2 憑證之簽發(Certificates Issuance)

FUCA 簽發憑證之作業規範如下：

(1) 註冊中心完成憑證用戶註冊及憑證申請作業後，依 FUCA 之作業規範將憑證用戶之身分識別及申請資料安全的傳遞至 FUCA。

(2) FUCA 於接收到憑證用戶之憑證申請訊息時，鑑別憑證用戶身分之合法性，及憑證申請訊息之完整性及有效性（例如：憑證用戶簽章），正確無誤後載入資料庫，並簽發憑證予憑證用戶。

(3) FUCA 於產生憑證用戶憑證後，即刻更新資料庫或目錄伺服器之憑證資訊供憑證用戶查詢使用。

(4) 當憑證用戶憑證申請訊息為 FUCA 拒絕時，此失敗交易 FUCA 必須立刻通知註冊中心；惟交易失敗之原因，FUCA 或註冊中心應以電子郵件方式、電話或其他適當方式告知憑證申請者不同意簽發的理由；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)

憑證用戶申請憑證簽發完成且由 FUCA 取得憑證時，憑證用戶應依下列規定處理：

(1) 確認憑證內容之憑證用戶相關資訊與憑證用戶註冊時之一致性，且為憑證用戶之正確資訊。

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

(3) 憑證用戶必須驗證 FUCA 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 FUCA 所簽發。

(4) 憑證用戶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，FUCA 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、憑證用戶與 FUCA 之合約規定，憑證用戶使用

憑證時：

(1) 憑證用戶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、被竄改或為第三者任意使用或竊用。

(2) 除必須驗證 FUCA 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），且須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) 憑證用戶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) 憑證用戶使用憑證時，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、交易限額、賠償限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 憑證之廢止及暫時停用(Certificate Revocation and Suspension)

5.4.1 憑證廢止時機(Circumstances for Revocation)

FUCA 於憑證用戶之憑證仍於有效期間內，當有下述情況時，得逕行憑證之廢止：

(1) FUCA 因憑證系統之不適用或憑證系統之整合需求。

(2) 憑證用戶使用憑證而為有權第三者（例如：FUCA）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。

憑證用戶於其憑證仍於有效期間內，當有下述情況時，必須提出憑證廢止申請：

(1) 憑證內容之憑證用戶相關資訊有更動時，例如：憑證用戶名稱或公司之註冊名稱變更。

(2) 與憑證相關之私密金鑰有毀損、遺失、曝露、被竄改，或有為第三者竊用之疑慮時。

(3) 憑證內容之憑證用戶相關資訊，不符合本作業基準、憑證政策或業務使用規範時，例如：憑證用戶憑證內容與註冊資料不符，或因註冊資料輸入之疏忽。

FUCA 於其憑證仍於有效期間內，當有下述情況時，必須向 FPCA 提出憑證廢止申請：

(1) FUCA 憑證之相關資訊有更動時，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、被竄改，或有為第三者竊用之疑慮時。

(3) FUCA 憑證之相關資訊，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) 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)

與憑證用戶有關之註冊中心、FUCA、主管機關或合法授權之第三者與憑證用

戶皆有權執行憑證之廢止。

(1) FUCA 廢止憑證用戶憑證時，必須依照「5.4.1 憑證廢止時機(Circumstances for Revocation)」與相關作業規範辦理。

(2) 憑證用戶可依照其需求，依註冊中心作業規範申請廢止憑證用戶憑證。

(3) 有權責之第三者申請廢止憑證用戶之憑證：

■法院因訴訟與仲裁向註冊中心提出廢止憑證用戶憑證之申請，註冊中心必須鑑別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) 憑證用戶親自填寫申請表單述明理由並簽名確認，或以具有憑證用戶簽章之廢止憑證申請訊息，依照註冊中心之作業規範，向註冊中心申請。

(2) FUCA、主管機關、法院與訴訟仲裁單位及其他有權責者，亦必須依據註冊中心之作業規範，填具廢止申請單向註冊中心申請廢止該憑證。

(3) FUCA 因業務緣故結束營運管理時，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，向 FPCA 申請廢止該憑證。

(4) 註冊中心接到憑證廢止申請後，應確實鑑別申請者之身分及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），並歸檔相關查核紀錄（如：核准人姓名、簽章、核准日期....等）。註冊中心應於憑證廢止申請訊息說明憑證用戶廢止憑證之理由，FUCA 於 CRL 加註說明憑證廢止之理由。

(5) FUCA 收到註冊中心之憑證用戶廢止憑證申請訊息時，鑑別註冊中心身分之合法性，與憑證用戶廢止憑證申請訊息之安全性，正確無誤後，依廢止憑證作業規範，即時處理憑證用戶憑證之廢止。

(6) FUCA 將憑證用戶憑證廢止回覆訊息，正確且安全之傳回註冊中心。註冊中心於收到回覆訊息後，即刻通知憑證用戶憑證廢止之作業完成。

(7) FUCA 定期產生憑證廢止清冊(CRL)後，即刻將憑證廢止清冊傳遞至憑證目錄伺服器與憑證資料庫，更新憑證廢止清冊以提供憑證用戶查詢及使用。

FUCA 處理廢止憑證用戶憑證之時效性，應至少於 24 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憑證用戶向註冊中心提出憑證廢止申請，至 FUCA 完成廢止憑證作業，並及時更新憑證目錄伺服器與憑證資料庫之期間。FUCA 憑證廢止之處理期間應至少於 24 小時內完成。

5.4.5 憑證暫時停用時機(Circumstances for Suspension)

憑證之暫時停用需求皆由該憑證之憑證用戶提出，FUCA 無其他得逕行憑證暫時停用之時機。憑證用戶暫時停用憑證之作業方式悉遵照 FUCA 與註冊中心的業務需求與作業規範辦理，憑證系統如有配合業務系統安全性管控的需求時，則不

提供憑證暫時停用之功能。

憑證用戶於憑證仍然有效期間內，為保留用戶的憑證使用權利而不申請廢止憑證時，當有下述情況時可執行憑證的暫時停用：

(1) 憑證之私密金鑰有可能遺失、洩露的不安全疑慮時，憑證用戶可暫時停用該憑證之使用；

(2) 憑證用戶欲暫時停止使用該憑證一段時間，例如用戶出國；

(3) 憑證用戶使用憑證而為有權第三者〈例如：FUCA 或註冊中心〉宣告未履行應盡義務〈例如：費用〉，或不當使用憑證而有可能違反政府法律、規章、 本作業基準或業務使用規範之疑慮時。

5.4.6 有權暫時停用憑證者(Who can Request Suspension)

(1) 憑證用戶之憑證只有憑證用戶可提出暫時停用之申請；

(2) 憑證用戶可依照其需求，依註冊中心作業規範申請暫時停用憑證用戶之憑證；

(3) FUCA 暫時停用憑證用戶憑證時，必須依照「5.4.7 憑證暫時停用程序(Procedure for Suspension Request)」處理，且必須依與憑證用戶間之合約與相關作業規範辦理。

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

(1) 憑證用戶親自以填寫申請表單並簽名確認，或依照註冊中心之憑證用戶身分鑑別規範，或以具有憑證用戶簽章之暫時停用憑證申請訊息，依照註冊中心之安全控管措施，經由郵寄或網際網路向註冊中心申請。

(2) 註冊中心收到憑證用戶之暫時停用憑證申請表單，檢核憑證用戶身分之合法性與訊息之安全性，且此憑證為憑證用戶之有效憑證，經檢核正確無誤後，及時將具有註冊中心簽章之憑證用戶暫時停用憑證申請訊息，依照 FUCA 之安全控管措施，經由網際網路線上向 FUCA 申請暫時停用憑證用戶憑證。

(3) 註冊中心為提供憑證用戶於緊急，或特殊之異常狀況下申請憑證暫時停用之作業程序〈例如：電話、傳真〉，則依照各業務之相關作業規範之規定辦理，但亦須具有完整之身分鑑別之安全管控措施。

(4) FUCA 收到註冊中心之憑證用戶暫時停用憑證申請訊息時，鑑別註冊中心身分之合法性，與憑證用戶暫時停用憑證申請訊息之安全性，正確無誤後，依暫時停用憑證作業規範，及時處理憑證用戶憑證之暫時停用 。

(5) FUCA 將憑證用戶憑證暫時停用回覆訊息，正確且安全之傳回註冊中心，並及時通報 OCSP 服務系統知悉，且定時產生憑證廢止清冊(CRL)。

(6) FUCA 即刻將憑證廢止清冊傳遞至憑證目錄伺服器與憑證資料庫，更新憑證廢止清冊以提供憑證用戶查詢及使用。

FUCA 處理暫時停用憑證用戶憑證之時效性，應至少於 24 小時內完成。

暫時停用憑證於限制之原因解除後，憑證用戶擬繼續使用該張憑證，且憑證之有效期限尚未到期時，憑證用戶可向註冊中心申請憑證之解禁，使憑證成為有效且可以使用。

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

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

憑證暫時停用之時效為，當憑證用戶憑證經完成暫時停用後存放至廢止憑證清冊，至憑證用戶申請憑證解禁完成，而憑證從廢止憑證清冊移轉成有效憑證為止之期間，是為憑證之暫時停用時效，此段期間如至超過憑證有效期限仍未執行憑證解禁時，則此張憑證即為廢止憑證。憑證暫時停用之時效最長為 FUCA 簽發憑證用戶憑證之有效期限。

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

FUCA 憑證廢止清冊(CRL)之產生頻率為每 24 小時產生 1 次。

5.4.10 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，憑證用戶或信賴憑證者皆可依需求自由存取。

憑證用戶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，尚須確認憑證是否存在目前的憑證廢止清冊中，所有已存在憑證廢止清冊中之憑證將不可被信賴。信賴憑證者參考憑證廢止清冊時須確認憑證廢止清冊來源的正確性與資料完整性，且該憑證廢止清冊尚未過期。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 FUCA 索取 CRL。

憑證用戶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。

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

FUCA 提供憑證用戶或信賴憑證者線上憑證與廢止憑證狀態查詢功能(OCSP)。

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

如「5.4.10 憑證廢止清冊查證要求(CRL Checking Requirements)」與「5.4.11 線上憑證與廢止憑證狀態查證功能(On-line Revocation/Status Checking Availability)」之說明。

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

FUCA 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。

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

FUCA 目前不提供其他格式廢止憑證之查核。

5.4.15 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(Key Changeover)」之規範處理。

5.5 安全稽核(Security Audit Procedures)

FUCA 憑證作業營運，由實體設備之操作到憑證作業系統之執行，皆須確實歸檔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 FUCA 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)

FUCA 稽核紀錄至少應保存如下之資訊：

(1) 憑證用戶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紀錄。

(3) FUCA 金鑰與憑證之產生、建置、變更之成功與失敗之紀錄。

(4) 憑證用戶憑證申請交易處理與回覆之成功與失敗紀錄。

(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紀錄。

(7) 進出入本公司申請表單，作業人員身分識別 IC 卡進/出 FUCA 機房之紀錄報表，FUCA 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 FUCA 機房監控攝錄影機之媒體紀錄。

(8) FUCA 主機系統硬、軟體、應用系統，及 FUCA 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。

(9) 註冊中心經由網際網路至憑證系統，執行憑證作業與存取系統資源有關之交易紀錄。

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 3 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上述紀錄執行稽核管理作業。

可能影響系統安全之異常事件稽核紀錄，須由授權的稽核管理人員依相關之系統與文件紀錄詳細查核，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)

相關稽核紀錄相關報表與媒體資料至少應保留 10 年；異常狀況之系統紀錄及報表至少應保留 12 年，並於 FUCA 所在處所保留至少 2 個月資料；錄影媒體紀錄除特殊異常狀況必須保留外，以每 3 個月為一週期循環使用。

5.5.4 稽核紀錄之保護(Protection of Audit Log)

FUCA 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，安全控管措施應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 1 次，且另儲存 1 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，並留存存取稽核紀錄的紀錄檔，以偵測與防止非法及不當的存取及竄改。

文件稽核紀錄歸檔之執行，亦具有安控措施之保護，且另儲存 1 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)

FUCA 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 1 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從憑證系統開啟至系統關閉為止，FUCA 憑證系統稽核紀錄之蒐集，係經由作業系統、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 FUCA 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.FUCA 系統建置與變更	自 動	FUCA 憑證系統
6.金鑰與憑證之產生、簽發與廢止	自 動	FUCA 憑證系統
7.憑證用戶資訊之建置、修改與刪除	自 動	FUCA 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 FUCA 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 脆弱性評鑑(Vulnerability Assessments)

對於執行憑證系統運作時，內部與外部可能造成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 1 次。

5.6 紀錄保存(Records Archival)

5.6.1 事件紀錄之種類(Types of Event Records)

FUCA 為使憑證作業系統能穩定之運作，必須將系統環境建置檔、與憑證用戶相關合約條款、憑證用戶註冊資料之相關資訊、憑證用戶憑證及廢止憑證資料檔、交易資料檔、稽核資料檔、FUCA 金鑰與憑證變更資訊、憑證實務作業基準、憑證政策、FUCA 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 紀錄歸檔期限(Retention Period for Archive)

除配合主管機關訂定之資訊保存期限規範，FUCA 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、及憑證用戶註冊申請表單、相關合約條款、憑證用戶憑證申請、更新、暫停使用、廢止之憑證，或過期憑證，至少保留至憑證有效期限結束後 10 年。

(2) 憑證用戶憑證申請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 10 年。

(3) FUCA 金鑰與憑證等相關之異動資料至少保留 10 年。

5.6.3 歸檔紀錄之保護(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 歸檔紀錄之備援程序(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，1 份儲存於 FUCA 具安全管控措施之環境下，且 1 份保存資料儲存於具安全管控措施之異地備援環境，當憑證系統異常無法開啟時，依系統備份與回復作業手冊，以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)

FUCA 於憑證管理作業系統運作時，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。

憑證用戶於執行註冊、憑證申請與更新、暫時停用、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 歸檔紀錄蒐集系統(Archive Collection System)

FUCA 憑證系統作業相關之保存紀錄資訊，皆由 FUCA 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 歸檔紀錄之取得與驗證程序(Procedure to Obtain and Verify Archive Information)

FUCA 憑證系統作業相關之保存紀錄資訊之驗證，依 FUCA 之內部管理作業規範，至少 1 年 1 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 憑證用戶金鑰變更(Key Changeover of Subscriber)

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

FUCA 憑證用戶之憑證有效期限最長為 2 年。用戶金鑰使用有效期限結束時，填具憑證更新申請單向註冊中心辦理用戶金鑰變更申請作業完成後，用戶可以產生新金鑰對向註冊中心申請新憑證的簽發。

5.7.2 FUCA金鑰變更(Key Changeover of FUCA)

FUCA 憑證有效期限為 5 年，因 FUCA 簽發憑證用戶之憑證效期最長為 2 年，FUCA 須於 FUCA 憑證生效第 3 年時進行金鑰更新程序，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。

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

本公司為使 FUCA 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)

FUCA 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 FUCA 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。

FUCA 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，FUCA 應啟動異地備援機制，並於 24 小時內完成災難復原程序。

5.8.2 金融用戶憑證管理中心公開金鑰廢止之復原程序(FUCA Public Key is Revoked)

當 FUCA 符合「5.4.1 憑證廢止時機(Circumstances for Revocation)(7)(8)(9)(10)」所述之時機時，須向 FPCA 提出憑證廢止申請，同時廢止其公開及私密金鑰。

FUCA 公開金鑰廢止之復原程序依照「5.8.3 金融用戶憑證管理中心及憑證用戶私密金鑰之破解處理程序(FUCA & SC Private Key is Compromised)(1)(2)(3)(4)」之作業規範辦理。

5.8.3 金融用戶憑證管理中心及憑證用戶私密金鑰之破解處理程序(FUCA & SC Private Key is Compromised)

FUCA 私密金鑰有毀損、遺失、曝露、被竄改，或有為第三者竊用之疑慮時，

(1) 應立即向 FPCA 申告，並產生下一組新金鑰對及相對之憑證申請檔，向 FPCA 申請新憑證的簽發。

(2) FUCA 應立刻廢止所有由 FUCA 簽發之憑證（憑證用戶、註冊中心），並更新 CRL 或 OCSP 資料，供憑證用戶或信賴憑證者查詢。

(3) FUCA 取得新憑證後，應依據「5.1 憑證申請(Certificates Application)」及「5.2 憑證之簽發(Certificates Issuance)」之規範，重新簽發憑證用戶及註冊中心之憑證。

(4) FUCA 新產生之公開金鑰，依據「7.1.4 FUCA 公開金鑰之遞送(FUCA Public Key Delivery to Users)」之規範，遞送給憑證用戶。

憑證用戶私密金鑰有毀損、遺失、曝露、被竄改，或有為第三者竊用之疑慮時，

可依據本作業基準「5.4.3 憑證廢止程序(Procedure for Revocation Request)」，先向註冊中心申請廢止舊憑證的使用，然後再產生新金鑰對，向註冊中心申請新憑證之簽發。

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

FUCA 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，回復憑證系統之運作功能。

5.8.5 業務持續及災害復原計劃(Contingency and Disaster Recovery Plan)

為避免因天災與地變而造成 FUCA 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 FUCA 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 1 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，與歸檔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，FUCA 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。

5.9 FUCA結束營運(FUCA Termination)

FUCA 因故結束其系統營運時，須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 1 個月前通報主管機關、銀行公會及 FPCA。

(2) 於終止服務之日 1 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 FUCA 與全部用戶之憑證，將結束之 FUCA 相關私密金鑰與憑證及全部用戶憑證，移轉至承接之憑證管理中心。

(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 7 年。

(6) 於作業(4)完成後，將 FUCA 儲存於硬體密碼模組內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，且儘可能的協助承接者執行憑證的簽發業務。

於業務異常結束（法院宣告破產、或不合法）時，FUCA 必須儘早向憑證用戶公告事實，且必須執行如業務正常結束時的作業程序，將對憑證用戶業務系統運作的影響減少至最低程度。

6. 實體、作業流程及人員安全控管(Physical、Procedural and Personnel Security Control)

6.1 實體控管(Physical Control)

FUCA 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)

FUCA 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 FUCA 機房必須有 3 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。

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

FUCA 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)

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

FUCA 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，並定期執行維護與測試。

6.1.4 水災之防範(Water Exposures)

FUCA 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。

6.1.5 火災之防範(Fire Prevention and Protection)

FUCA 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於具高度防火功能之保險櫃，其中 1 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)

FUCA 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，商業敏感性及機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，並歸檔查核文件。

文件與媒體資訊儲存有商業敏感性及機密性資訊時，於廢棄處理時必須經安全之銷毀，該資訊皆無法回復與存取使用，且經由稽核單位之驗證，並歸檔查核文件。

6.1.8 異地備份(Off-Site Backup)

FUCA 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。

FUCA 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)

FUCA 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 FUCA 扮演之可信賴且具公信力之機構，公正與嚴謹之執行。

因此 FUCA 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 FUCA 內部憑證作業規範及作業手冊，確實執行業務。

FUCA 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 FUCA 整個憑證系統業務之營運。

(2) 稽核人員(本公司非屬 FUCA 之作業人員)，負責稽核、監督 FUCA 憑證系統業務之運作工作內容詳「5.5 安全稽核(Security Audit Procedures)」。

(3) FUCA 憑證系統業務營運之監督人員，至少 2 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) FUCA 憑證系統業務營運之管理人員，至少 2 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：FUCA 金鑰及憑證之變更， 但不可以執行憑證用戶憑證之簽發、憑證用戶資料之建置等作業）。

(5) FUCA 憑證系統業務營運之操作人員，負責系統運作時憑證用戶資料建置、執行憑證簽發等相關作業及報表與批次作業。

(6) 其他 FUCA 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)

FUCA 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 FUCA 金鑰之建置或變更、憑證用戶資訊之異動等相關作業皆有 2 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 2 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 角色之識別與鑑別(Identification and Authentication for Each Role)

FUCA 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鑑別，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) FUCA 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)

FUCA 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)

FUCA 系統運作之人員，皆依照其職務，施予 FUCA 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。

FUCA 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 FUCA 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)

FUCA 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 1 次，並給予適當之再教育之訓練。

FUCA 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。

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

配合 FUCA 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。

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

FUCA 憑證系統運作之相關作業人員，因故意或過失而執行非自己職務上之作業時，無論是否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)

FUCA 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 FUCA 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。

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) FUCA 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) FUCA 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 金鑰對之產生(Key Pair Generation)

(1) FUCA 不提供代替憑證用戶產生金鑰對之服務，憑證用戶之金鑰對須憑證用戶自行產製。

(2) FUCA 金鑰對由 2 位以上獨立之金鑰管理人員，同時登入(log-in)至硬體密碼模組，由硬體密碼模組直接產生，任何人絕無法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，直接經密碼加密機制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，私密金鑰無法以明碼方式輸出至硬體密碼模組外。

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

私密金鑰由憑證用戶自行產生金鑰對。

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

憑證用戶以公開金鑰向註冊中心申請憑證時，該請求訊息內之憑證用戶公開金鑰(public key)具有憑證用戶簽章及憑證用戶身分鑑別與訊息完整性之保護。

憑證申請成功之回覆訊息內，均具有 FUCA 之簽章與訊息完整性之保護。當憑證用戶之公開金鑰遞送至 FUCA 時應有正式的收發程序並保留憑據。

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

FUCA 於網站上(http://www.twca.com.tw/)公布 FUCA 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（如：SSL 網站識別加密方式）傳遞公開金鑰憑證，供憑證用戶或信賴憑證者查詢。

FUCA 公開金鑰有異動或因憑證用戶查詢而須遞送至憑證用戶時，FUCA 公開金鑰憑證皆有 FUCA 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。

7.1.5 金鑰長度(Key Sizes)

FUCA、憑證用戶及註冊中心之 RSA 金鑰長度至少為 1024 位元，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)

FUCA 之 RSA 公開金鑰參數之產生與選取，由通過 CNS15135、ISO19790 或 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。

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

FUCA 之 RSA 公開金鑰參數品質，由通過 CNS15135、ISO19790 或 FIPS 140-2 Level 3 規範之硬體密碼模組檢核。

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

FUCA 之金鑰於通過 CNS15135、ISO19790 或 FIPS 140-2 Level 3 規範之硬體密碼模組內直接產生。

憑證用戶的金鑰對可由硬體或軟體產生，產生後的金鑰對應有適當之機密性機制保護，且不以明碼的形式儲存於一般媒體中(如硬碟、磁片等)。

7.1.9 金鑰之使用(Key Usage Purposes)

FUCA 簽發給憑證用戶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)，憑證用戶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)

FUCA 之硬體密碼模組，通過 CNS15135、ISO19790 或 FIPS 140-2 Level 3 規範。

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

(1) FUCA 私密金鑰之產生、建置及變更，皆由至少 2 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，如果是以部分基碼之方式儲存，則須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 (Private Key Escrow)

本憑證管理中心之私密金鑰不可被託管，亦不提供用戶私密金鑰託管服務。

7.2.4 私密金鑰之備份(Private Key Backup)

(1) FUCA 私密金鑰加密後儲存於硬體密碼模組內，備份時至少由 2 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) FUCA 私密金鑰之部分基碼(m of n key parts) 儲存於 IC 卡，並存放於經雙重控管、安全之保險櫃內，由安全控管人員密封保管。

(3) FUCA 私密金鑰之備份至少保留 2 份，1 份存放於本公司保險櫃內，另 1 份存放於具安全管控之異地備援中心。

(4) FUCA 不提供代替憑證用戶產生金鑰對之功能，故無憑證用戶之私密金鑰備份之作業。

7.2.5 私密金鑰之歸檔(Private Key Archival)

本憑證管理中心私密金鑰不進行歸檔。

7.2.6 私密金鑰輸入至密碼模組

FUCA 之私密金鑰的建置，至少由 2 位以上的金鑰管理人員由硬體密碼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設備外。

當有使用該私密金鑰執行運算的需求時，須經由密碼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密碼設備外。

7.2.7 私密金鑰之開啟(Method of Activating Private Key)

FUCA 儲存於硬體密碼模組內之私密金鑰，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。

憑證使用者私密金鑰之開啟，必須由使用者出示相關的啟動資料(如密碼、通行密語等)，始得啟動使用私密金鑰。

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

儲存於硬體密碼模組內之私密金鑰，必須由 2 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。

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，其軟體密碼模組必須以資料覆蓋方式(Overwrite)清除，硬體密碼模組或 IC 卡必須以零值化(Zeroization)之覆蓋方式清除。

硬體密碼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 公開金鑰之歸檔(Public Key Archival)

公開金鑰之歸檔，其執行程序及安全措施之需求與憑證之保存相同，期限至少歸檔 7 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)

公開金鑰與私密金鑰之有效期限為相同效期，FUCA 金鑰之有效期限為 5 年，憑證用戶金鑰之有效期限最長為 2 年。

7.4 啟動資訊(Activation Data)

7.4.1 產生及建置(Activation Data Generation and Installation)

FUCA 產生憑證用戶啟動資訊(例如：IC card 密碼),通行密語(pass-phrase))於安全控管的環境下，直接由硬體密碼模組內產生，且是隨機產生的一組亂數(密碼建議至少 6 位，通行密語建議至少 8 位以上)，當有經由網路傳遞至用戶的需求時，必須有適當的安全措施保護，如果以郵件方式傳遞時，必須以密封的密碼單方式遞送，於建置使用時可依用戶安全需求而隨時變更。

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

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

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

考量安全因素，對於申請憑證的用戶啟動資訊的生命週期之變更頻率訂定如下：

(1) 低保護性：啟動資訊長度 4-6 位的數字，儲存於系統的啟動資訊為明碼，可由用戶選取，以信封郵寄時無特殊安控措施，使用於非機密或普通資料的傳遞，或低交易金額時的啟動資訊，建議生命週期為 1 年，1 年後必須執行啟動資訊的變更。

(2) 中保護性：啟動資訊長度 4-8 位的文數字，儲存於系統的啟動資訊為亂碼化，以信封郵寄時須特殊安控措施，可由用戶選取或系統產生，使用於一般重要資料的傳遞，或一般交易金額時的啟動資訊，建議其生命週期為 6 個月，6 個月後必須執行啟動資訊的變更。

(3) 高保護性：啟動資訊長度 6-8 位的文數字，儲存於系統的啟動資訊為亂碼化，以信封郵寄時須特殊安控措施，在安全的管控環境下由亂碼化設備內亂數產生系統直接產生，使用於較重要資料的傳遞，或一定交易金額以上時的啟動資訊，建議其生命週期為 1 個月，1 個月或至少 3 個月後必須執行啟動資訊的變更。

FUCA 產生給予憑證用戶保護私密金鑰或 IC card 的啟動資訊，為考量安全因素，建議用戶依照業務系統安全度的需求而隨時變更啟動資訊。

註冊中心所產生供用戶使用的啟動資訊(例如：IC 卡密碼、磁片密碼)，憑證用戶應依業務需求的安全度，考量變更啟動資訊頻率(例如用戶連上註冊中心網際網路的啟動資訊至少 3 個月或 6 個月變更一次)。

7.5 電腦安全控管(Computer Security Controls)

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

FUCA 憑證系統運作之資訊安全管理系統環境，依據 ISO 27001:2005 資訊安全管理系統標準之規範施行及運作。FUCA 憑證系統之安控措施包含下列作業：

(1) 身分之識別及鑑別管控機制。
(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) 業務持續經營回復機制。
(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)

FUCA 使用之憑證系統，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)

FUCA 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 FUCA 憑證系統之資訊安全管理系統環境，遵循中華民國銀行公會所規定之標準規範運作。

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、功能測試與紀錄，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)

建置防火牆、入侵偵測與防毒管理系統，確保系統安全，防止網路入侵破壞，以提

昇網路管理系統之安全控管，且隨時更新網路防火牆、防入侵偵測、防病毒與網路資源安全控管系統之版本，以期能將網路系統之威脅風險減至最低。

FUCA 憑證系統經由防火牆與網路資源安全控管系統的保護，只開放憑證系統相關的作業功能，供憑證用戶經由網際網路(Internet)至 FUCA 執行憑證相關的作業功能，其他非憑證機構提供的功能或通訊介面，憑證用戶皆無法執行。

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

FUCA 密碼模組之安全控管機制，符合 CNS15135、ISO19790 或 FIPS 140-2 Level 3 規範。

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

8.1 憑證剖繪(Certificate Profile)

FUCA 憑證系統使用之憑證詳細格式，訂定於各相關之憑證剖繪作業規範。

8.1.1 版本(Version Number(s))

FUCA 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)

FUCA 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剖繪作業規範。

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

FUCA 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	desCBC	1.3.14.3.2.7
亂碼	3desEDE-CBC	1.2.840.113549.3.7
雜湊函數	SHA-1	1.3.14.3.2.26
雜湊函數	MD5	1.2.840.113549.2.5

8.1.4 命名格式(Name Forms)

FUCA 憑證系統所簽發之憑證，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布之「金融 XML 憑證共通性技術規範」。

8.1.5 命名限制(Name Constraint)

FUCA 憑證系統所簽發之憑證，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」。

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

FUCA 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)

FUCA 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)

FUCA 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)

FUCA 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 憑證廢止清冊剖繪(CRL Profile)

8.2.1 版本(Version number(s))

FUCA 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剖繪欄位之內。

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)

FUCA 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 FUCA 憑證政策管理委員會，每年至少 1 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(Contact Details)」，由 FUCA 客服中心處理。

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

經由 FUCA 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 FUCA 之網站。

9.3 憑證實務作業基準核定程序(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，且須經主管機關之核定。

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，於執行訊息機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、憑證機構軟硬體施行之安全機制、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).金融最高層憑證機構(Financial Root Certificate Authority：FRCA)

為金融公開金鑰基礎建設之最高層憑證機構，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/ 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	Financial Policy Certification Authority
TCSEC	Trusted Computer System Evaluation Criteria
UCA	User Certification Authority
URL	Universal Resource Location