銀行公會

金融 XML 憑證共通性技術規範

Version 1.2

電子銀行組

中華民國一０一年六月日

目 錄

圖表目錄

表格目錄

文件製/修訂履歷

日期 (yy/mm/dd)	修訂簡述	作者	備註
90/09/07	初版	XML 訊息安控分組	
98/1/14	增訂 4.4 使用者憑證申請訊息 修訂 6.3 跨 RA 時與跨 UCA 時憑證驗證 修訂 7.2.1.3~4 Browser Base 客戶憑證登記作業流程圖與說明 修訂 7.2.2.3~4 Server Base 客戶憑證登記作業流程圖與說明 增訂 7.2.4 索取與驗證登記憑證 修訂 7.3 憑証到期可展期期間 修訂 8.1 憑證各狀態查詢作業 修訂 8.3 憑證(金鑰)儲存媒體保護機制 修訂 9.1 使用者端安控系統 增訂 10.1 金融 XML 憑證載具 API 介面應用規範 增訂 10.2 金融 XML 憑證載具規格書 增訂 10.3 金融 XML 憑證載具安全規範	電子銀行組安控分組	金融業務電子化委員會第 114 次委員會會議通過
102/6/3	依據 102 年 6 月 3 日金管銀國字第 10200120550 號函備查之「金融機構辦理電子銀行業務安全控管作業基準」修正。 修訂 4,6 SHA1 雜湊演算法提為 SHA256 增訂 8.2 增加 RA 人員採用 2FA 認證 增訂 8.3 增加客戶採用載具規格 增訂 9.1 增加支援中介軟體之載具 增訂 9.2 增加銀行採用載具規格		

1. 前言

銀行公會於 2000 年 7 月成立金融 XML(eXtensible Markup Language)訊息訂定小組，負責金融 XML 訊息標準訂定，開發適用於網際網路之金融標準訊息，XML 訊息小組於訊息訂定方向討論時，即已確定金融 XML 訊息需符合安控基準要求之原則，換言之即高風險性交易必須帶有數位簽章。

目前國內各金融機構光是在網際網路上使用之電子憑證就有六種以上，且互不相通，而憑證互不相通情況不僅在不同金融機構間會發生，同一金融機構不同作業也常因該作業原規劃單位選定之認證機構(Certification Authority ，簡稱 CA)有所不同，導致客戶必須使用不同憑證。因為憑證不同相對憑證管理軟體也不同，使用者必須安裝多套憑證管理軟體，同時攜帶多個憑證，客戶使用時需辨識是哪一項作業，該使用哪一張憑證，造成很多困擾與不便。對金融機構而言因各憑證之申請、管理流程不同，金融機構相對應之作業流程也必須配合調整，因此必須同時維護多套憑證交易處理及憑證管理之電腦系統，增加作業成本。

金融機構面臨的另一個問題是跨國業務憑證使用問題，目前在國際上，除了憑證相關的技術規範均不盡相同外(雖均採用 X.509 之標準，但如憑證識別名稱內容及 CA 架構等在標準上仍留有極大的彈性，因而造成未能共通之差異性)，憑證生命週期之管理與使用範圍等亦有極大之差異。

目前各金融機構網路銀行交易，仍採用現行跨行通路進行跨行交易，跨行交易並未使用電子憑證，因此目前多憑證、多系統的狀況只會造成使用者及金融機構的不方便。但在金融 XML 訊息訂定時就面臨各家金融機構的網路銀行作業採用之電子憑證不盡相同，XML 跨行系統之安控憑證無所遵循的困境。憑證規格若未能及早標準化，憑證種類可能會日益增多，金融機構需負擔多憑證、多系統之高建置成本，而系統及業務無法整合，會衍生複雜之使用及管理問題。為解決以上的問題，銀行公會電子化委員會在 2000 年 9 月成立金融 XML 安控分組，負責檢討、整合並訂定金融 XML 憑證共通性技術規範，讓國內金融機構在建置相關安控系統時，有可遵循之依據，以達到電子商務金流國內憑證共通目標。

安控分組係由銀行公會電子化委員會所屬之電子銀行專案工作小組選派代表組成，從 2000 年 9 月開始，每週一到二次在銀行公會持續開會研議，從國內現行憑證規格及相關作業了解開始，期間內歷經下列步驟，

- 金融憑證共通性技術規範需求討論，整合金融機構共識
- 金融憑證共通性技術規範意見徵求，聽取參與金融相關憑證作業之認證機構及安控業者(以下簡稱廠商)建議
- 金融憑證共通性技術規範 RFP 撰寫，提出憑證共通性技術規範需求大綱

- 請廠商提出憑證共通性技術規範建議書
- 針對廠商建議書進行 Review 與問題澄清
- Identrus 相關規範研討
- 金融憑證共通性技術規範初稿撰寫
- 對廠商進行金融憑證共通性技術規範初稿重點說明及意見徵求
- 廠商意見彙整、討論
- 金融憑證共通性技術規範初稿修改
- 銀行公會電子銀行專案工作小組審查
- 銀行公會金融電子化委員會審查

經過將近一年的時間才得以完成憑證共通性技術規範初版。這段期間荷蒙各參與金融機構主管鼎力支持指派代表熱誠持續參與，並荷蒙網路消費協會徐博士瑞卿義務指導以及台灣網路認證公司、台網國際公司、異康公司、影像公司、網際威信公司、關貿公司等提供現行作業資訊，派員參與公會舉辦之意見徵求討論並依公會訂定之金融憑證共通性技術規範 RFP(Request For Proposal)提供建議書，讓金融憑證共通性技術規範初稿得以順利完成，特藉此敬致萬分的感謝，同時也要感謝普華資安公司提供 Identrus 導讀，加速工作小組對 Identrus 相關國際規範的了解。

金融 XML 憑證共通性技術規範初版只是憑證共通性技術規範的第一步，下一階段將是安控憑證與金融 XML 訊息之整合，配合相關國際規範之發展，本分組邇後將陸續修訂本規範之版本，我們希望憑證共通性技術規範不僅能配合 XML 訊息使用，也能適用在所有電子商務金流相關交易，讓國內民眾一證在手，就可行遍天下，。

XML安控分組成員如下(依單位名稱筆劃順序排列):

中國信託商業銀行	沈慧瑛(召集人)
	成家瑜
	李嘉銘
中國國際商業銀行	舒惠荃
合作金庫	王屏玉
台灣中小企業銀行	陳桂枝
台灣銀行	盧建志
世華商業銀行	王芳綺
財金資訊股份有限公司	蘇偉慶
第一商業銀行	王致平
彰化商業銀行	曾煒智

2. 憑證共通性技術規範說明

2.1 憑證共通性技術規範目的

憑證共通性技術規範訂定目的有二：

- 制定金融憑證共通性技術規範，由各金融機構共同遵循，以達到憑證共通目標。
  國內各金融機構跨行系統及新開發系統皆遵循本規範，建置安控系統，以達到國內憑證共通目標。至於跨國業務之憑證使用問題，國際金融憑證目前以 Identrus 最通用，至 2001 年五月止全世界已有五十家大型金融機構加入 Identrus，故跨國業務之憑證擬採用 Identrus 之規範。惟因 Identrus 規章規範現階段僅限企業戶使用，且用途與國內使用情況不同，國內憑證現階段無法全面以 Identrus 憑證取代。然考慮國內金融機構日後加入 Identrus 之可能性與必要性，在訂定國內金融憑證規範時也參考了 Identrus 規格，雖無法達到憑證共通之理想，但希望能縮小差異，以提高建置時系統之整合性。

- 請認證機構及安控業者依憑證共通性技術規範開發金融相關系統。
  銀行公會只是訂定共同規範提供業界系統建置依據，並不是要自建一個 CA，也不會指定使用那一家 CA，也就是說只要 CA 及安控系統能符合銀行公會訂定之憑證共通性技術規範，就可以為金融機構採用。但在不同 Root CA 間之憑證交互認證規範未訂定前，不同 Root CA 間尚無法達到憑證共通的目標，因此目前除了要持續關切國際上憑證交互認證機制發展進度與相關規範外，要達到憑證共通目標，唯有各金融機構皆採用同一個 CA，或將各金融機構使用之 CA 整合到同一個 Root CA。最終目的希望能以國家或金融機構整體名義加入國際認證組織，讓國內金融機構使用之憑證能獲得國際組織承認，以確保電子商務金流能跨出台灣，正式與國際接軌。

2.2 憑證共通性技術規範範圍

憑證共通性技術規範係以公鑰基礎建設(Public Key Infrastructure，簡稱 PKI)為基礎進行憑證共通性技術規範訂定，公鑰基礎建設(PKI)係依據[IETF PKIX roadmap]（請參閱附錄10.2）之定義為「一整套包括硬體、軟體、人員、規章與程序，用以產製、管理、儲存、遞送與註銷以公開金鑰密碼學為基礎之憑證」，可以得知整體公鑰基礎建設所涵蓋的範圍很廣，但考慮作業需求急迫性，本次憑證共通性技術規範涵蓋的範圍包括：

- CA 架構及各單位權責
- 憑證格式
- 憑證管理與週期
- 交易驗證及憑證作業程序

憑證共通性技術規範後續預定將持續增加之內容如下：

- XML 訊息整合
- RA 與 CA、銀行之界面
- 憑證儲存媒體
- DB 格式或 API
- 其他

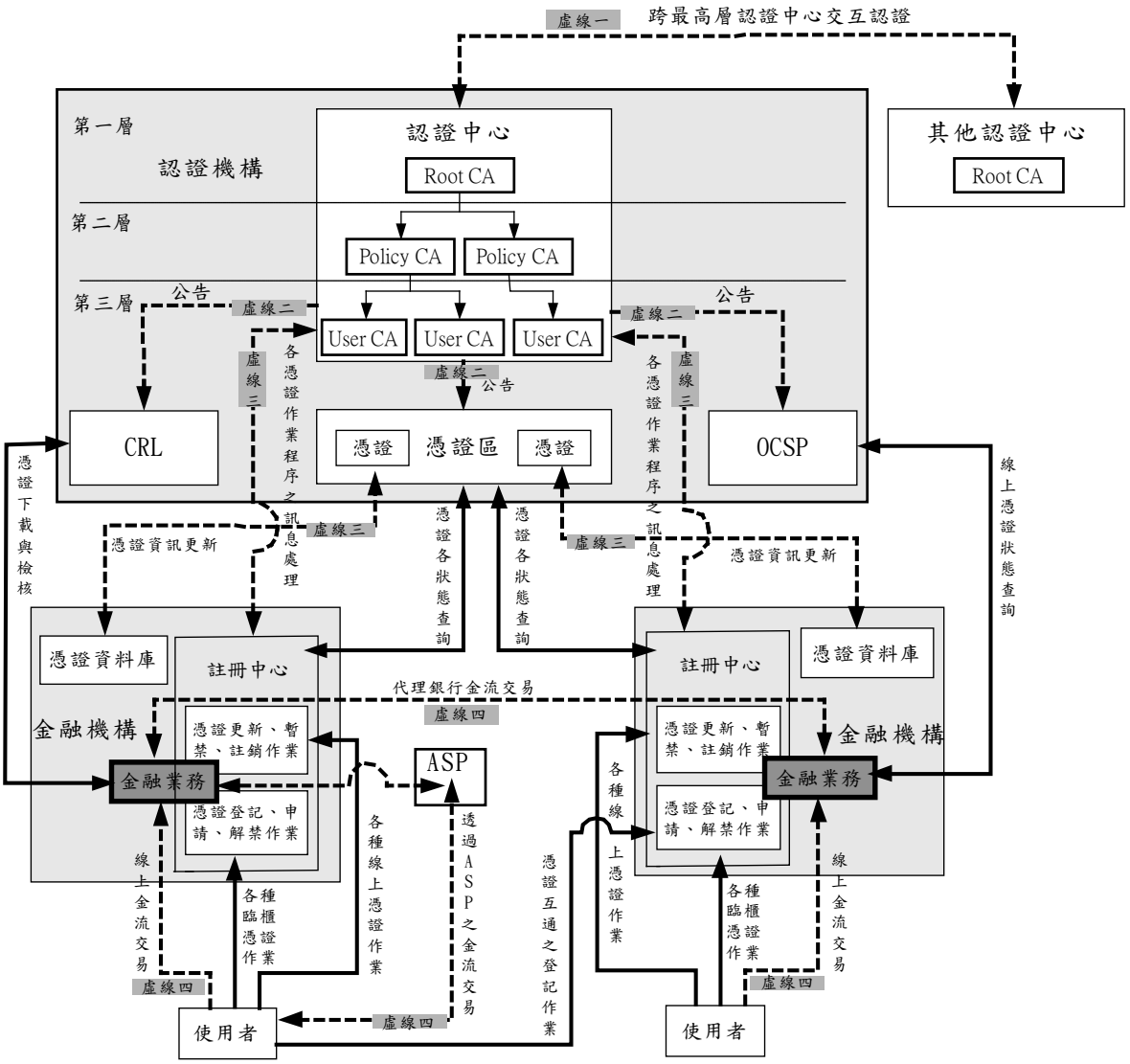
本規範目前僅涵蓋客戶與金融機構間交易，暫未將客戶與客戶間之交易納入。

本規範以 RSA 數位簽章相關技術為限，唯諸如生物科技等各類電子鑑別技術發展迅速，當其他電子鑑別技術運用成熟時，將依金融機構需要，進行憑證共通性技術規範修正。

3. 憑證共通性技術規範內容

3.1 整體架構

本規範之整體架構如下圖所示



圖表 3-1 憑證共通性技術規範整體架構圖

針對此整體架構圖之說明如下：

- 圖中共有三大塊灰色方框，圖上方之灰色方框代表認證機構之作業環境，圖左、右兩邊之灰色方框代表金融機構之作業環境
- Root CA 代表最高認證中心，其權責詳見本規範3.3節
- Policy CA 代表策略認證中心，其權責詳見本規範3.4節
- User CA 代表使用者認證中心，其權責詳見本規範3.5節
- 註冊中心 (Registration Authority, RA)，其權責詳見本規範3.6節，由於註冊中心肩負確認使用者身份之第一線把關工作，考慮整體作業之安全性故目前只允許由金融機構擔任註冊中心

- 目前本規範所考量之交易模式僅涵蓋客戶與金融機構間及金融機構與金融機構之模式，暫未將客戶與客戶間之交易模式納入，但不論何種交易模式，當具安控訊息之交易進行時(如圖中之線上金流交易)，一方即為憑證使用者，而另一方即為交易夥伴，其權責詳見本規範3.7與3.8節，但當客戶擔任交易夥伴時，由於目前其所應對之憑證使用者為金融機構，風險相對而言很低，考量建置成本與系統複雜度，故客戶端可不具備憑證廢止清單及憑證狀態線上查詢機制
- 圖中實線部份代表本規範目前已涵蓋之作業，如使用者與金融機構註冊中心間之各種線上憑證作業、金融機構與認證機構間之線上憑證狀態查詢等等，詳見本規範第六、七、八章及其他相關章節之說明
- 圖中虛線部份作業說明如下：
  - 虛線一(跨最高層認證中心交互認證)
    目前本作業不論在標準與實務上均缺乏引用依據，故本規範目前只能提出針對單一階層式認證中心(Single Root CA)之相關規範，跨最高層認證中心交互認證作業將依循目前正在規劃討論中之 Asia PKI Forum 或 APEC 等國際組織之建議方案提出後另行訂定之
  - 虛線二(認證中心相關公告事宜)
    此為認證中心之內部作業範圍，由各認證機構自行處理，故不擬納入本規範中
  - 虛線三(各憑證作業程序之訊息處理及憑證資訊更新等，為認證中心與註冊中心間之作業界面)
    將納入憑證共通性技術規範後續預定增加之內容
  - 虛線四(代理銀行金流交易等)
    請參見「金融 XML 系統建置指引」

3.2 制定原則

分類	原則	參見章節
PKI 架構	暫以 Single Root CA 進行相關規劃	3.3
	三階層式 CA 架構，包括 Root CA、Policy CA 和 User CA	3.3
	CA 應同時提供 OCSP 及 CRL 二種憑證檢核服務	3.3
憑證和憑證註銷清單	憑證格式採用 X.509v3	4.1.1
	憑證註銷清單(CRL) 格式採用 X.509v2	4.3
	使用者憑證申請訊息	4.4
	基於安全考量，使用者憑證中不放戶名	4
	Email 資訊為選用欄位且置於憑證擴充欄位 RFC822name 內	4.1.7.2
	使用者憑證應與瀏覽器環境相容	9.1
	個人或企業可申請多張憑證	4.2.3
	簽章和加密不同用途應使用不同金鑰(Dual Key System/Two Key System)	4
	憑證暫禁資訊應於 CRL 及 OCSP 中公告	4.3 7.6.1.2
	憑證內容中應可區分出是否為註冊中心(RA)所使用之憑證；至於是否為金融機構或 ASP 之憑證，則由應用系統面自行記錄與管制	4.2.2
	臺灣國碼採用 158	4.1.1
憑證管理與週期	於使用者端自行產製金鑰	5
	使用者憑證效期為一年或二年	5.2
	由於法人戶交易金額龐大，憑證互通後為確保整體作業安全等級之一致性，法人戶必須使用硬體裝置儲存金鑰	8.3
交易驗證	跨 RA 或跨 CA 之憑證驗證時可透過 OCSP 機制	6.2.7
	應用服務統一選定使用 OCSP 或 CRL 驗證憑證	6.3
憑證作業	線上執行申請憑證作業時除需網路銀行的密碼之外，若再增加其他資料以供驗證申請者的身分，所增加驗證之資料由各行庫自行決定	7.1.1.2
	金融機構即使擔任註冊中心，其本身所需使用之憑證應直接透過認證中心所提供之註冊中心機制進行申請	8.2
	可執行憑證更新的期間為憑證到期前一至二個月至到期日，應由 RA 主動通知使用者	7.4.1.2

	憑證更新時憑證識別名稱不變,可線上以仍有效之舊憑證來申請新憑證	7.4.1.2
	憑證更新時，應重新產生金鑰	7.4.1.2
	辦理憑證更新後，新憑證之有效期間為原憑證到期日再加一憑證週期	5.1.4
	憑證跨 RA 使用前需要先完成登記作業，憑證更新後亦須重新登記	7.2
	憑證跨 UCA 使用前先索取登記憑證	7.2.4
	應考量無統一編號單位之作業處理方式	7.2.1.2
其他作業	CA 應以 LDAP 或 Http 方式，透過存取控管，開放給 RA 存取其所經手之相關憑證完整資訊	8.1
	CA 應以 Http 方式，透過存取控管，開放給 RA 存取其他 RA 所經手之相關憑證基本資訊	8.1
	使用者憑證(金鑰)之儲存媒體應具備保護機制(如密碼)，且應具備錯誤次數之管制機制(如密碼連續輸入錯誤超過三次則不得繼續使用)	8.3
安控系統軟體	使用者端軟體以 Thin Client 為設計原則，且各功能須以模組化設計，以便使用者決定安裝選項	9.1

3.3 最高層認證中心(RCA)權責

XML 金融憑證共通性技術規範目前定義金融機構公鑰基礎建設的最高層認證中心(Root CA)為單一的最高層認證中心（Single Root CA），此單位必須負責下列事項：

- 配合法律、政策與業務的需求，訂定、管理最高層認證中心 PKI 的架構與規範、憑證策略(Certificate Policy，CP)及憑證實務作業基準(Certificate Practice Statement，CPS)包含憑證申請、登記、註銷、暫禁等憑證的內容（例如：依法律、政策與業務的需求訂定策略認證中心的種類、申請的規範標準、程序、流程等)。
- 管理與公告下層使用者憑證註銷、暫禁等 CRL，OCSP 的作業程序與驗證的作業規範。
- 簽發、管理與遞送下層策略認證中心的憑證、憑證註銷等。
- 管理與公告憑證狀態線上查詢資訊時的作業程序與身分驗證及訊息安控措施的作業規範。
- 訂定、管理下層註冊中心(RA)的作業規範與程序，完成身分及憑證的識別與驗證。
- Root CA 建置於獨立、安全管控的作業環境下，經合法授權才可由二位以上的執行人員進行公開金鑰的產生、建置與簽發註冊中心憑證的作業，其他相關作業規範則訂定於註冊中心與認證中心之憑證管理相關作業手冊。
- 確認憑證管理系統作業人員〈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憑證策略的規範。
- 作業人員必須善盡保管憑證資料及相關訊息之責任、避免相關資訊洩漏、被冒用、篡改及任意使用。
- 依照憑證實務作業基準與憑證策略的規範，接受註冊中心憑證的申請、註銷等憑證狀態的申請及確認註冊中心發送至認證中心之相關交易訊息的正確性與安全性，並執行憑證簽發與憑證註銷的相關作業，及將相關回覆訊息正確與安全的遞送註冊中心。
- 產生 Self-Signed 憑證或更新 Self-Signed 憑證後，必須以安全的方式遞送予註冊中心，由註冊中心遞送予使用者。
- 申請或註銷憑證時，產生憑證或憑證註銷清單，需公告至憑證區和憑證廢止清單區供查詢使用，並將憑證註銷資訊立刻通知 OCSP 伺服器。

3.4 策略認證中心(PCA)權責

策略認證中心負責下列事項：

- 簽發、管理與遞送註冊中心的憑證申請、憑證註銷等資訊。
- 配合法律、政策與業務的需求，及遵循最高層認證中心訂定的規範，訂定、管理策略認證中心 PKI 的架構與規範，憑證策略及憑證實務作業基準，憑證及廢止憑證的內容。
- 管理與公告下層認證中心憑證申請、憑證註銷的作業程序與驗證的作業規範。
- 簽發、管理與遞送下層認證中心的憑證、憑證註銷清單資訊。
- 公告、管理認證中心的憑證策略與憑證實務作業基準相關資訊。

3.5 使用者認證中心(UCA)權責

使用者認證中心負責下列事項：

- 公告及管理使用者〈註冊中心、個人、企業……〉憑證、註銷憑證等相關作業程序與驗證的作業規範。
- 簽發、管理與遞送註冊中心與使用者的憑證申請、憑證註銷等資訊。
- 公告及管理 CA 的憑證策略與憑證實務作業基準。
- 管理與公告憑證註銷清單與憑證狀態線上查詢資訊時的作業程序與身分驗證及訊息安控措施的作業規範。

3.6 註冊中心(RA)權責

註冊中心負責下列事項：

- 管理與公告使用者〈個人、企業.....〉註冊申請的作業程序與身分驗證的作業規範。
- 驗證使用者憑證之簽發與註銷及查詢等申請訊息，身分合法性與訊息正確性的驗證。
- 遞送使用者的申請憑證、註銷憑證、查詢申請訊息，至認證中心辦理、申請憑證、註銷憑證，並驗證回覆訊息的正確性後傳回申請之使用者。
- 公告、管理 RA 註冊名稱相關資訊。
- 管理、公告並提供使用者查詢使用者憑證、註銷憑證及認證中心的憑證鏈。
- 使用者申請或註銷、暫禁等憑證作業時必須驗證使用者身分的安全性與正確性，使用者憑證相關申請訊息轉送至認證中心時，必須驗證訊息的安全性與正確性。
- 註冊中心與其作業人員必須善盡保管使用者資料及相關訊息之責任、避免相關資訊洩漏、被冒用、篡改及任意使用。
- 註冊中心與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，即刻向認證中心辦理申告與處理。
- 認證中心遞送的使用者憑證，必須能立刻更新，提供使用者最新的資訊。
- 考量整體作業安全性，本規範目前僅允許金融機構擔任 RA。
- 為使金融機構能提供客戶完整的客戶服務，憑證相關作業一律需經過 RA 並留存相關資料於 RA。
- RA 需通知憑證即將到期的使用者辦理更新憑證作業。

3.7 使用者權責

使用者即為憑證的擁有者，負責下列事項：

- 在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。
- 其憑證與憑證對應的私密金鑰(Private Key)使用的業務範圍，皆依認證中心「憑證實務作業基準」與相關「憑證策略」之規範，運用於相關業務上。
- 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。
- 使用者需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。
- 憑證內使用者相關的資訊有異動時，使用者必須依相關作業的規定，即刻向註冊中心辦理申告與處理。

3.8 交易夥伴權責

交易夥伴即為使用他人(使用者)的憑證、認證中心、策略認證中心與最高層認證中心的憑證鏈(Certificates Chain)資訊，用以驗證接收的簽章訊息之完整性，或使用他人(接收者)的憑證作訊息的加密後、將加密的訊息傳送至接收者，以達到通訊雙方訊息的隱密性。

交易夥伴負責下列事項：

- 必須了解且同意憑證實務作業基準與憑證策略相關作業規範的規定，且依規範所訂定的業務範圍使用於相關的業務，無任何違反相關法律的規定與侵害第三者的權利。
- 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，也需利用憑證廢止清單及憑證狀態線上查詢機制，檢核此憑證是否為註銷或暫禁憑證；由於目前本規範所考量之交易模式僅涵蓋客戶與金融機構間及金融機構與金融機構之模式，暫未將客戶與客戶間之交易模式納入，故當客戶擔任交易夥伴時，由於目前其所應對之憑證使用者為金融機構，風險相對而言很低，考量建置成本與系統複雜度，故客戶端可不具備憑證廢止清單及憑證狀態線上查詢機制。

4. 憑證和憑證註銷清單

憑證內容格式與憑證註銷清單格式遵循[X509V3]和[RFC 2459]相關標準。

憑證種類依 PKI 階層式架構由上而下可分為 Root CA 憑證、Policy CA 憑證、User CA 憑證和使用者憑證，Root CA 憑證為 Self-Signed 憑證，上層 CA 憑證簽發下層憑證。

憑證種類依使用者可分為使用者憑證、RA 憑證與 CA 憑證三種，使用者憑證使用於一般交易，客戶需向 RA 申請憑證，RA 憑證需向 CA 申請而使用於 CA 與 RA 間，RA 送至 CA 的任何憑證作業訊息皆需 RA 簽章，CA 以此 RA 憑證判別是否為合法的RA與憑證作業訊息的資料完整性,CA憑證則用於簽發憑證。

而憑證種類依其用途可分為簽章憑證與加密憑證兩種(Two Key System/Dual Key System)，簽章憑證使用於簽章與不可否認性，加密憑證使用於保護資料，確保加密資料不被非加密憑證擁有者所解密，使用者憑證與 RA 憑證皆是 Dual Key System，憑證欄位格式也相同，唯識別名稱(Subject)的命名方式不同，且基於安全考量，使用者憑證中不存放戶名資料。

4.1 憑證說明

4.1.1 憑證欄位說明

以下針對本規範可能使用到的憑證欄位做說明，不包含憑證結構中的認證中心簽章演算法欄位(SignatureAlgorithm)和簽體欄位(SignatureValue)。

表格 4-1 憑證欄位說明表

欄 位	說 明
1. X.509v1 Field	**憑證基本欄位**
1.1. Version	憑證版本，使用 X509 Version 3
1.2. Serial Number	**憑證序號，最大長度為 32 BYTES，由 CA 指定**
1.3. Signature Algorithm	簽章演算法，使用 SHA-1 with RSA Encryption (PKCS#1-5) (1.2.840.113549.1.1.5)或 SHA256 with RSA Encryption (PKCS#1-5) (1.2.840.113549.1.1.11)，自 2017/1/1 起須使用 SHA256 with RSA Encryption (PKCS#1-5) (1.2.840.113549.1.1.11)
1.4. Issuer	**憑證簽發者識別名稱，命名規則於4.2章節說明**
1.4.1. Country (C)	認證公司所在國家
1.4.2. Organization (O)	認證公司英文名稱
1.4.3. Organizational Unit (OU)	認證中心所屬性質
1.4.4. Common Name (CN)	認證中心英文名稱
1.5. Validity	憑證有效日期時間
1.5.1. Not Before	憑證生效日期時間
1.5.2. Not After	憑證終止日期時間
1.6. Subject	憑證擁有者識別名稱，命名規則於4.2章節說明
1.6.1. Country (C)	認證公司所在國家
1.6.2. Organization (O)	認證公司策略
1.6.3. Organizational Unit (OU)	認證中心資訊
1.6.4. Organizational Unit (OU)	註冊中心名稱
1.6.5. Organizational Unit (OU)	註冊中心應用或服務名稱
1.6.6. Common Name (CN)	使用者識別碼
1.7. Subject Public Key Info	憑證擁有者公開金鑰，使用 RSA 演算法
2. X.509v3 Extensions	X509 V3 Extensions
2.1. Authority Key Identifier	
2.1.1. Key Identifier	憑證簽發者公開金鑰的 160-bits SHA-1 值或 256 bits SHA256 值，自 2017/1/1 起須使用 256 bits SHA256
2.2. Subject Key Identifier	憑證擁有者公開金鑰的 160-bits SHA-1 值或 256 bits SHA256 值，自 2017/1/1 起須使用 256 bits SHA256
2.3. Key Usage	
2.3.1. Digital Signature	用於簽章
2.3.2. Non Repudiation	用於不可否認
2.3.3. Key Encipherment	用於加密 Session Key
2.3.4. Data Encipherment	用於加密資料
2.3.5. Key Agreement	用於交換 Session Key
2.3.6. Key Certificate Signature	用於簽發憑證
2.3.7. CRL Signature	用於簽發 CRL
2.4. Extended Key Usage	
2.4.1. Client Authentication	用於 SSL 客戶端認證(1.3.6.1.5.5.7.3.2)
2.4.2. Email Protection	用於保護電子郵件 (1.3.6.1.5.5.7.3.4)
2.5. Certificate Policies	憑證策略

2.5.1 Policy Information	策略資訊
2.5.1.1 Policy Identifier	由 CA 指定的憑證政策 ID，**臺灣使用之國碼為 158**
2.5.1.2. Policy Qualifier ID	1.3.6.1.5.5.7.2.1 為聯結至 CPS 的 URL 方式
2.5.1.3. Qualifier	聯結至 CPS 的 URL
2.5.1.4. Policy Qualifier ID	1.3.6.1.5.5.7.2.2 為使用者聲明(User Notice)
2.5.1.5. Qualifier	使用者聲明
2.6. Subject Alternate Names	
2.6.1. rfc822Name	使用者電子郵箱
2.7. Basic Constraints	**憑證基本限制**
2.7.1. CA	區分憑證為 CA 類(True)和非 CA 類(False)
2.7.2 Path Length Contraints	限制 CA 層級
2.8. CRL Distribution Point	CRL 資料存取
2.8.1. CRL DP Name	
2.8.1.1 Full Name	
2.8.1.1.1 URI	CRL URL 位址
***** 2.9. Authority Information Access	**認證中心資訊存取**
2.9.1 Access Description	
2.9.1.1. Access Method	以 OCSP(1.3.6.1.5.5.7.48.1)方式存取
2.9.1.2. Access Location	OCSP URL 位址

*註：RFC2459 定義之欄位

以下將針對 RCA、PCA、UCA、RA 與使用者憑證使用之欄位分別說明。

4.1.2 憑證欄位處理應注意事項

考量憑證間之互通性,所列欄位皆是本規範可能使用之 X509 v3 和 RFC2459 憑證欄位，凡符合此規範之安控系統都需要能正確處理這些欄位，若憑證內容使用到所列以外之欄位，則不保證符合此規範之安控系統可以正確處理此憑證。

本章以下各表中選項別共有兩種：

- 『必』為必要使用欄位。
- 『選』為選用欄位。

4.1.3 RCA 憑證

表格 4-2 RCA 憑證欄位說明表

欄 位		內 容	說 明
1. X.509v1 Field	**必**		
1.1. Version	必	2	X509v3 版本
1.2. Serial Number	**必**		**由 CA 指定**
1.3. Signature Algorithm	必	1.2.840.113549.1.1.5 或 1.2.840.113549.1.1.11，自 2017/1/1 起須為 1.2.840.113549.1.1.11	SHA-1 with RSA Encryption 或 SHA256 with RSA Encryption，自 2017/1/1 起須使用 SHA256 with RSA Encryption
1.4. Issuer	**必**		**RCA 識別名稱，命名規則於4.2.1章節說明**
1.4.1. Country (C)	必	e.g., “TW”	由 CA 指定
1.4.2. Organization (O)	必	e.g., “CyberTrust Corporation”	由 CA 指定
1.4.3. Organizational Unit (OU)	必	e.g., “Root CA”	由 CA 指定
1.4.4. Common Name (CN)	必	e.g., “Root”	由 CA 指定
1.5. Validity	必		
1.5.1. Not Before	必	e.g.“00:00:01 01 September 1999”	由 CA 指定
1.5.2. Not After	必	e.g., “23:59:59 31 August 2020”	由 CA 指定
1.6. Subject	必		RCA 識別名稱,命名規則於 4.2.1章節說明
1.6.1. Country (C)	必	e.g., “TW”	由 CA 指定
1.6.2. Organization (O)	必	e.g., “CyberTrust Corporation”	由 CA 指定
1.6.3. Organizational Unit (OU)	必	e.g., “Root CA”	由 CA 指定
1.6.4. Common Name (CN)	必	e.g., “Root”	由 CA 指定
1.7. Subject Public Key Info	必		RCA 公開金鑰，長度 2048bits (含)以上，自 2017/1/1 起長度須為 4096bits (含)以上
2. X.509v3 Extensions	必		
2.1. Authority Key Identifier	必		
2.1.1. Key Identifier	必		RCA 公開金鑰代碼
2.2. Subject Key Identifier	必		RCA 公開金鑰代碼
2.3. Key Usage	必		
2.3.1. Digital Signature		不使用	
2.3.2. Non Repudation		不使用	
2.3.3. Key Encipherment		不使用	
2.3.4. Data Encipherment		不使用	
2.3.5. Key Agreement		不使用	
2.3.6. Key Certificate Signature		使用	
2.3.7. CRL Signature		使用	
2.4. Certificate Policies	必		
2.4.1 Policy Information	必		一個 Policy Information
2.4.1.1 Policy Identifier	必		由 CA 指定的 RCA 憑證政策 ID
2.4.1.2. Policy Qualifier ID	選	1.3.6.1.5.5.7.2.1	
2.4.1.3. Qualifier	選	e.g.,” http://ca.CyberTrust.com.tw/”	由 CA 指定
2.4.1.4. Policy Qualifier ID	選	1.3.6.1.5.5.7.2.2	

2.4.1.5. Qualifier	選	e.g.," This certificate is for the sole use of CyberTrust and its customers"	由 CA 指定
2.5. Basic Constraints	**必**		
2.5.1. CA	必	True	屬 CA 憑證
2.5.2. Path Length Constraint	必	2	下有 PCA 和 UCA

4.1.4 PCA 憑證

表格 4-3 PCA 憑證欄位說明表

欄 位		內 容	說 明
1. X.509v1 Field	**必**		
1.1. Version	必	2	X509v3 版本
1.2. Serial Number	**必**		**由 CA 指定**
1.3. Signature Algorithm	必	1.2.840.113549.1.1.5 或 1.2.840.113549.1.1.11，自 2017/1/1 起須為 1.2.840.113549.1.1.11	SHA-1 with RSA Encryption 或 SHA256 with RSA Encryption，自 2017/1/1 起須使用 SHA256 with RSA Encryption
1.4. Issuer	**必**		**RCA 識別名稱，命名規則於4.2.1章節說明**
1.4.1. Country (C)	必	e.g., “TW”	由 CA 指定
1.4.2. Organization (O)	必	e.g., “CyberTrust Corporation”	由 CA 指定
1.4.3. Organizational Unit (OU)	必	e.g., “Root CA”	由 CA 指定
1.4.4. Common Name (CN)	必	e.g., “Root”	由 CA 指定
1.5. Validity	必		
1.5.1. Not Before	必	e.g.,“00:00:01 01 September 1999”	由 CA 指定
1.5.2. Not After	必	e.g.,“23:59:59 31 August 2012”	由 CA 指定
1.6. Subject	必		PCA 識別名稱，命名規則於4.2.1章節說明
1.6.1. Country (C)	必	e.g., “TW”	由 CA 指定
1.6.2. Organization (O)	必	e.g., “CyberTrust Corporation”	由 CA 指定
1.6.3. Organizational Unit (OU)	必	e.g., “Policy CA”	由 CA 指定
1.6.4. Common Name (CN)	必	e.g., “Finance”	由 CA 指定
1.7. Subject Public Key Info	必		PCA 公開金鑰，長度 1024bits (含)以上，自 2017/1/1 起長度須為 4096bits (含)以上
2. X.509v3 Extensions	必		
2.1. Authority Key Identifier	必		
2.1.1. Key Identifier	必		RCA 公開金鑰代碼
2.2. Subject Key Identifier	必		PCA 公開金鑰代碼
2.3. Key Usage	必		
2.3.1. Digital Signature		不使用	
2.3.2. Non Repudation		不使用	
2.3.3. Key Encipherment		不使用	
2.3.4. Data Encipherment		不使用	
2.3.5. Key Agreement		不使用	
2.3.6. Key Certificate Signature		使用	
2.3.7. CRL Signature		使用	
2.4. Certificate Policies	必		
2.4.1 Policy Information	必		一個 Policy Information
2.4.1.1 Policy Identifier	必		由CA指定的PCA憑證政策ID
2.4.1.2. Policy Qualifier ID	選	1.3.6.1.5.5.7.2.1	
2.4.1.3. Qualifier	選	e.g.,” http://ca.CyberTrust.com.tw/”	由 CA 指定

2.4.1.4. Policy Qualifier ID	選	1.3.6.1.5.5.7.2.2	
2.4.1.5. Qualifier	選	e.g.," This certificate is for the sole use of CyberTrust and its customers"	由 CA 指定
2.5. Basic Constraints	**必**		
2.5.1. CA	必	True	屬 CA 憑證
2.5.2. Path Length Constraint	必	1	下有 UCA
2.6 CRL Distribution Point	必		一個 CRL DP
2.6.1. CRL DP Name	必		
2.6.1.1 Full Name	必		
2.6.1.1.1 URI	必	e.g.,"https://ca.CyberTrust.com.tw /user/FXML/revoke.crl"	由 CA 指定
2.7. Authority Information Access	**必**		
2.7.1 Access Description	**必**		**一個 ACCESS DESCRIPTION**
2.7.1.1. Access Method	必	1.3.6.1.5.5.7.48.1	
2.7.1.2. Access Location	必	e.g., "URL=https://OCSP. CyberTrust.com.tw:8000/"	由 CA 指定

4.1.5 UCA 憑證

表格 4-4 UCA 憑證欄位說明表

欄 位		內 容	說 明
1. X.509v1 Field	**必**		
1.1. Version	必	2	X509v3 版本
1.2. Serial Number	**必**		**由 CA 指定**
1.3. Signature Algorithm	必	1.2.840.113549.1.1.5 或 1.2.840.113549.1.1.11，自 2017/1/1 起須為 1.2.840.113549.1.1.11	SHA-1 with RSA Encryption 或 SHA256 with RSA Encryption，自 2017/1/1 起須使用 SHA256 with RSA Encryption
1.4. Issuer	**必**		**PCA 識別名稱，命名規則於4.2.1章節說明**
1.4.1. Country (C)	必	e.g., “TW”	由 CA 指定
1.4.2. Organization (O)	必	e.g., “CyberTrust Corporation”	由 CA 指定
1.4.3. Organizational Unit (OU)	必	e.g., “Policy CA”	由 CA 指定
1.4.4. Common Name (CN)	必	e.g., “Finance”	由 CA 指定
1.5. Validity	必		
1.5.1. Not Before	必	e.g., “00:00:01 01 September 1999”	由 CA 指定
1.5.2. Not After	必	e.g., “23:59:59 31 August 2004”	由 CA 指定
1.6. Subject	必		UCA 識別名稱，命名規則於4.2.1章節說明
1.6.1. Country (C)	必	e.g., “TW”	由 CA 指定
1.6.2. Organization (O)	必	e.g., “CyberTrust Corporation”	由 CA 指定
1.6.3. Organizational Unit (OU)	必	e.g., “User CA”	由 CA 指定
1.6.4. Common Name (CN)	必	e.g., “Banking”	由 CA 指定
1.7. Subject Public Key Info	必		UCA 公開金鑰，長度 1024bits (含)以上，自 2017/1/1 起長度須為 4096bits (含)以上
2. X.509v3 Extensions	必		
2.1. Authority Key Identifier	必		
2.1.1. Key Identifier	必		PCA 公開金鑰代碼
2.2. Subject Key Identifier	必		UCA 公開金鑰代碼
2.3. Key Usage	必		
2.3.1. Digital Signature		不使用	
2.3.2. Non Repudation		不使用	
2.3.3. Key Encipherment		不使用	
2.3.4. Data Encipherment		不使用	
2.3.5. Key Agreement		不使用	
2.3.6. Key Certificate Signature		使用	
2.3.7. CRL Signature		使用	
2.4. Certificate Policies	必		
2.4.1 Policy Information	必		一個 Policy Information
2.4.1.1 Policy Identifier	必		由 CA 指定的 UCA 憑證政策 ID
2.4.1.2. Policy Qualifier ID	選	1.3.6.1.5.5.7.2.1	
2.4.1.3. Qualifier	選	e.g.,” http://ca.CyberTrust.com.tw/”	由 CA 指定

2.4.1.4. Policy Qualifier ID	選	1.3.6.1.5.5.7.2.2	
2.4.1.5. Qualifier	選	e.g.," This certificate is for the sole use of CyberTrust and its customers"	由 CA 指定
2.5. Basic Constraints	**必**		
2.5.1. CA	必	True	
2.5.2. Path Length Constraint	必	0	
2.6 CRL Distribution Point	必		一個 CRL DP
2.6.1. CRL DP Name	必		
2.6.1.1 Full Name	必		
2.6.1.1.1 URI	必	e.g.,"https://ca.CyberTrust.com.tw /user/FXML/revoke.crl"	由 CA 指定
2.7. Authority Information Access	**必**		
2.7.1 Access Description	**必**		**一個 ACCESS DESCRIPTION**
2.7.1.1. Access Method	必	1.3.6.1.5.5.7.48.1	
2.7.1.2. Access Location	必	e.g., "URL=https://OCSP. CyberTrust.com.tw:8000/"	由 CA 指定

4.1.6 RA 憑證

表格 4-5 RA 憑證欄位說明表

欄 位		內 容	說 明
1. X.509v1 Field	**必**		
1.1. Version	必	2	X509v3 版本
1.2. Serial Number	**必**		**由 CA 指定**
1.3. Signature Algorithm	必	1.2.840.113549.1.1.5 或 1.2.840.113549.1.1.11，自 2017/1/1 起須為 1.2.840.113549.1.1.11	SHA-1 with RSA Encryption 或 SHA256 with RSA Encryption，自 2017/1/1 起須使用 SHA256 with RSA Encryption
1.4. Issuer	**必**		**UCA 識別名稱，命名規則於 4.2.1章節說明**
1.4.1. Country (C)	必	e.g., “TW”	由 CA 指定
1.4.2. Organization (O)	必	e.g., “CyberTrust Corporation”	由 CA 指定
1.4.3. Organizational Unit (OU)	必	e.g., “User CA”	由 CA 指定
1.4.4. Common Name (CN)	必	e.g., “Banking”	由 CA 指定
1.5. Validity	必		
1.5.1. Not Before	必	e.g.“00:00:01 01 September 1999”	由 CA 指定
1.5.2. Not After	必	e.g., “23:59:59 31 August 2003”	由 CA 指定
1.6. Subject	必		RA 識別名稱，命名規則於 4.2.2章節說明
1.6.1. Country (C)	必	e.g., “TW”	由 CA 指定
1.6.2. Organization (O)	必	e.g., “CyberTrust Finance”	由 CA 指定
1.6.3. Organizational Unit (OU)	必	e.g., “CyberTrust Banking”	由 CA 指定
1.6.4. Organizational Unit (OU)	必	e.g., “12345678-CyberTrust”	由 CA 指定
1.6.5. Organizational Unit (OU)	必	e.g., “FXML”	由 CA 指定
1.6.6. Common Name (CN)	必	e.g., “0040000-RA-001”	由 CA 依 RA 申請資料指定
1.7. Subject Public Key Info	必		RA 公開金鑰，長度 1024 bits(含)以上，自 2017/1/1 起長度須為 2048bits (含)以上
2. X.509v3 Extensions	必		
2.1. Authority Key Identifier	必		UCA 之憑證資訊
2.1.1. Key Identifier	必		UCA 公開金鑰代碼
2.2. Subject Key Identifier	必		RA 公開金鑰代碼
2.3. Key Usage	必		
2.3.1. Digital Signature		使用	
2.3.2. Non Repudation		使用	
2.3.3. Key Encipherment		不使用	
2.3.4. Data Encipherment		不使用	
2.3.5. Key Agreement		不使用	
2.3.6. Key Certificate Signature		不使用	
2.3.7. CRL Signature		不使用	
2.4. Certificate Policies	必		
2.4.1 Policy Information	必		一個 Policy Information
2.4.1.1 Policy Identifier	必		由 CA 指定的 RA 憑證政策 ID
2.4.1.2. Policy Qualifier ID	選	1.3.6.1.5.5.7.2.1	

2.4.1.3. Qualifier	選	e.g.," http://ca.CyberTrust.com.tw/"	由 CA 指定
2.4.1.4. Policy Qualifier ID	選	1.3.6.1.5.5.7.2.2	
2.4.1.5. Qualifier	選	e.g.," This certificate is for the sole use of CyberTrust and its customers"	由 CA 指定
2.5. Basic Constraints	選		
2.5.1. CA	選	False	
2.6. Subject Alternate Names	選		
2.6.1. Rfc822Name	選	e.g., "john.doe@XYZCorp.com"	RA 電子郵箱
2.7. CRL Distribution Point	必		一個 CRL DP
2.7.1. CRL DP Name	必		
2.7.1.1 Full Name	必		
2.7.1.1.1 URI	必	e.g.,"https://ca.CyberTrust.com.tw/user/FXML/revoke.crl"	由 CA 指定
2.8. Authority Information Access	必		
2.8.1 Access Description	必		一個 ACCESS DESCRIPTION
2.8.1.1. Access Method	必	1.3.6.1.5.5.7.48.1	
2.8.1.2. Access Location	必	e.g., "URL=https://OCSP.CyberTrust.com.tw:8000/"	由 CA 指定

4.1.7 使用者憑證

4.1.7.1 使用者簽章憑證

表格 4-6 使用者簽章憑證欄位說明表

欄 位		內 容	說 明
1. X.509v1 Field	**必**		
1.1. Version	必	2	X509v3 版本
1.2. Serial Number	**必**		**由 CA 指定**
1.3. Signature Algorithm	必	1.2.840.113549.1.1.5 或 1.2.840.113549.1.1.11，自 2017/1/1 起須為 1.2.840.113549.1.1.11	SHA-1 with RSA Encryption 或 SHA256 with RSA Encryption，自 2017/1/1 起須使用 SHA256 with RSA Encryption
1.4. Issuer	**必**		**UCA 識別名稱，命名規則於4.2.1章節說明**
1.4.1. Country (C)	必	e.g., “TW”	由 CA 指定
1.4.2. Organization (O)	必	e.g., “CyberTrust Corporation”	由 CA 指定
1.4.3. Organizational Unit (OU)	必	e.g., “User CA”	由 CA 指定
1.4.4. Common Name (CN)	必	e.g., “Banking”	由 CA 指定
1.5. Validity	必		
1.5.1. Not Before	必	e.g., “00:00:01 01 September 1999”	由 CA 指定
1.5.2. Not After	必	e.g., “23:59:59 31 August 2000”	由 CA 指定
1.6. Subject	必		使用者識別名稱，命名規則於4.2.3章節說明
1.6.1. Country (C)	必	e.g., “TW”	由 CA 指定
1.6.2. Organization (O)	必	e.g., “CyberTrust Finance”	由 CA 指定
1.6.3. Organizational Unit (OU)	必	e.g., “CyberTrust Banking”	由 CA 指定
1.6.4. Organizational Unit (OU)	必	**E.G., “0040000-BOT”**	由 CA 指定
1.6.5. Organizational Unit (OU)	必	e.g., “FXML”	由 CA 指定
1.6.6. Common Name (CN)	必	e.g., “A123456789”	由 CA 依使用者申請資料指定
1.7. Subject Public Key Info	必		使用者公開金鑰，長度 1024bits(含)以上，自 2017/1/1 起長度須為 2048bits (含)以上
2. X.509v3 Extensions	必		
2.1. Authority Key Identifier	必		UCA 之憑證資訊
2.1.1. Key Identifier	必		UCA 公開金鑰代碼
2.2. Subject Key Identifier	必		使用者公開金鑰代碼
2.3. Key Usage	必		
2.3.1. Digital Signature		使用	
2.3.2. Non Repudation		使用	
2.3.3. Key Encipherment		不使用	
2.3.4. Data Encipherment		不使用	
2.3.5. Key Agreement		不使用	
2.3.6. Key Certificate Signature		不使用	
2.3.7. CRL Signature		不使用	
2.4. Certificate Policies	必		

2.4.1 Policy Information	必		一個 Policy Information
2.4.1.1 Policy Identifier	必		由 CA 指定的使用者憑證政策 ID
2.4.1.2. Policy Qualifier ID	選	1.3.6.1.5.5.7.2.1	
2.4.1.3. Qualifier	選	e.g.," http://ca.CyberTrust.com.tw/"	由 CA 指定
2.4.1.4. Policy Qualifier ID	選	1.3.6.1.5.5.7.2.2	
2.4.1.5. Qualifier	選	e.g.," This certificate is for the sole use of CyberTrust and its customers"	由 CA 指定
2.5. Basic Constraints	選		
2.5.1. CA	選	False	
2.6. Subject Alternate Names	選		
2.6.1. rfc822Name	選	e.g., "john.doe@XYZCorp.com"	使用者電子郵箱
2.7. CRL Distribution Point	必		一個 CRL DP
2.7.1. CRL DP Name	必		
2.7.1.1 Full Name	必		
2.7.1.1.1 URI	必	e.g.,"https://caCyberTrust.com.tw/user/FXML/revoke.crl"	由 CA 指定
2.8. Authority Information Access	**必**		
2.8.1 Access Description	**必**		**一個 ACCESS DESCRIPTION**
2.8.1.1. Access Method	必	1.3.6.1.5.5.7.48.1	
2.8.1.2. Access Location	必	e.g., "URL=https://OCSP.CyberTrust.com.tw:8000/"	由 CA 指定

4.1.7.2 使用者加密憑證

表格 4-7 使用者加密憑證欄位說明表

欄 位		內 容	說 明
1. X.509v1 Field	**必**		
1.1. Version	必	2	X509V3 版本
1.2. Serial Number	**必**		**由 CA 指定**
1.3. Signature Algorithm	必	1.2.840.113549.1.1.5 或 1.2.840.113549.1.1.11，自 2017/1/1 起須為 1.2.840.113549.1.1.11	SHA-1 with RSA Encryption 或 SHA256 with RSA Encryption，自 2017/1/1 起須使用 SHA256 with RSA Encryption
1.4. Issuer	**必**		**UCA 識別名稱，命名規則於4.2.1章節說明**
1.4.1. Country (C)	必	e.g., “TW”	由 CA 指定
1.4.2. Organization (O)	必	e.g., “CyberTrust Corporation”	由 CA 指定
1.4.3. Organizational Unit (OU)	必	e.g., “User CA”	由 CA 指定
1.4.4. Common Name (CN)	必	e.g., “Banking”	由 CA 指定
1.5. Validity	必		
1.5.1. Not Before	必	e.g., “00:00:01 01 September 1999”	由 CA 指定
1.5.2. Not After	必	e.g., “23:59:59 31 August 2000”	由 CA 指定
1.6. Subject	必		使用者識別名稱,命名規則於4.2.3章節說明
1.6.1. Country (C)	必	e.g., “TW”	由 CA 指定
1.6.2. Organization (O)	必	e.g., “CyberTrust Finance”	由 CA 指定
1.6.3. Organizational Unit (OU)	必	e.g., “CyberTrust Banking”	由 CA 指定
1.6.4. Organizational Unit (OU)	必	**E.G., “0040000-BOT”**	由 CA 指定
1.6.5. Organizational Unit (OU)	必	e.g., “FXML”	由 CA 指定
1.6.6. Common Name (CN)	必	e.g., “A123456789”	由CA依使用者申請資料指定
1.7. Subject Public Key Info	必		使用者公開金鑰，長度 1024bits(含)以上，自 2017/1/1 起長度須為 2048bits (含)以上
2. X.509v3 Extensions	必		
2.1. Authority Key Identifier	必		UCA 之憑證資訊
2.1.1. Key Identifier	必		UCA 公開金鑰代碼
2.2. Subject Key Identifier	必		使用者公開金鑰代碼
2.3. Key Usage	必		
2.3.1. Digital Signature		使用	
2.3.2. Non Repudation		不使用	
2.3.3. Key Encipherment		使用	
2.3.4. Data Encipherment		使用	
2.3.5. Key Agreement		使用	
2.3.6. Key Certificate Signature		不使用	
2.3.7. CRL Signature		不使用	
2.4. Extended Key Usage	必		
2.4.1. Client Authentication	必		

2.4.2. Email Protection	必		
2.4. Certificate Policies	必		
2.4.1 Policy Information	必		一個 Policy Information
2.4.1.1 Policy Identifier	必		由CA指定的使用者憑證政策 ID
2.4.1.2. Policy Qualifier ID	選	1.3.6.1.5.5.7.2.1	
2.4.1.3. Qualifier	選	e.g.," http://ca.CyberTrust.com.tw/"	由 CA 指定
2.4.1.4. Policy Qualifier ID	選	1.3.6.1.5.5.7.2.2	
2.4.1.5. Qualifier	選	e.g.," This certificate is for the sole use of CyberTrust and its customers"	由 CA 指定
2.5. Basic Constraints	選		
2.5.1. CA	選	False	
2.6. Subject Alternate Names			
2.6.1. rfc822Name	選	e.g., "john.doe@XYZCorp.com"	使用者電子郵箱
2.7. CRL Distribution Point	必		一個 CRL DP
2.7.1. CRL DP Name	必		
2.7.1.1 Full Name	必		
2.7.1.1.1 URI	必	e.g.,"https://CyberTrust.com.tw /user/FXML/revoke.crl"	由 CA 指定
2.8. Authority Information Access	**必**		
2.8.1 Access Description	**必**		**一個 ACCESS DESCRIPTION**
2.8.1.1. Access Method	必	1.3.6.1.5.5.7.48.1	
2.8.1.2. Access Location	必	e.g., "URL=https://OCSP. CyberTrust.com.tw:8000/"	由 CA 指定

4.2 憑證的識別名稱命名規則

4.2.1 RCA/PCA/UCA 憑證識別名稱

RCA/PCA/UCA 憑證識別名稱規則是相同的，內含四個英文欄位，欄位意義如下表：

表格 4-8 RCA/PCA/UCA 憑證識別名稱規則表

欄　位	說　明	長度
Country (C)	CA 公司所在地之國碼	2
Organization (O)	CA 公司英文名稱	1~64
Organizational Unit (OU)	CA 所屬性質資訊	1~64
Common Name (CN)	CA 應用或服務英文名稱	1~64

舉例資料：

表格 4-9 RCA/PCA/UCA 憑證識別名稱範例表

欄位	RCA	PCA	UCA
Country (C)	TW	TW	TW
Organization (O)	CyberTrust Corporation	CyberTrust Corporation	CyberTrust Corporation
Organizational Unit (OU)	Root CA	Policy CA	User CA
Common Name (CN)	Root	Finance	Banking

4.2.2 RA 識別名稱

RA 憑證之識別名稱內含六個英文欄位，欄位意義如下表：

表格 4-10 RA 憑證識別名稱規則表

欄　位	說　明	長度
Country (C)	申請憑證所在地之國碼	2
Organization (O)	CA 公司政策的資訊	1~64
Organizational Unit (OU)	CA(簽發單位)的資訊	1~64
Organizational Unit (OU)	RA 憑證的註冊中心英文名稱	1~64
Organizational Unit (OU)	RA 憑證的註冊中心應用或服務英文名稱	1~64
Common Name (CN)	RA 識別碼 (1)金融機構代碼：金融機構代碼(3)+分行代碼(4)，若不使用金融機構分行代碼則金融機構分行代碼用“0000”取代 (2)“RA” (3)自選編號(optional)：提供 RA 單位自選的 ID 輔助申請者 ID 的資訊，最長 11 碼。 若應用到第(2)或第(3)的要素，則每個要素之間以「－」符號區隔。 其語法規則如下： ● 金融機構代碼－RA－自選編號 ● 長度 10 到 22 碼	10~22

舉例資料：

表格 4-11 RA 憑證識別名稱範例表

欄　位	RA 識別名稱
Country (C)	TW
Organization (O)	CyberTrust Finance
Organizational Unit (OU)	CyberTrust Banking
Organizational Unit (OU)	12345678-CyberTrust
Organizational Unit (OU)	FXML
Common Name (CN)	0040000-RA-01

4.2.3 使用者識別名稱

使用者憑證之識別名稱，內含六個英文欄位，欄位意義如下表：

表格 4-12 使用者憑證識別名稱規則表

欄　位	說　明	長度
Country (C)	申請憑證所在地之國碼	2
Organization (O)	CA 公司政策的資訊	1~64
OrganizationalUnit (OU)	CA(簽發單位)的資訊	1~64
Organizational Unit (OU)	註冊中心英文名稱	1~64
Organizational Unit (OU)	註冊中心應用或服務英文名稱	1~64
Common Name (CN)	憑證申請人的使用者識別碼	8~25

註冊中心英文名稱規則如下：

金融機構總行代碼＋金融機構分行代碼＋區隔符號「-」＋金融機構英文簡稱，

e.g. 台灣銀行城中分行即可為 0044045-BOT。

若不使用金融機構分行代碼則金融機構分行代碼用'0000'取代，

e.g. 台灣銀行即可為 0040000-BOT。

憑證申請人的使用者識別碼由以下三個要素組成：

(1)申請者 ID

(2)重號編號(optional)：提供 RA 遇到不同實體使用者但其申請者 ID 相同時的區別資訊。

(3)自選編號(optional)：提供使用者自選的 ID 輔助申請者 ID 的資訊。

若應用到第(2)或第(3)的要素，則每個要素之間以「－」符號區隔。

其語法規則建議如下：

- 申請者 ID－重號編號－自選編號。
- 長度 8 到 25 碼

使用者種類在此共分為二類：個人、法人

一、 個人

(1)申請者 ID = PID（本國公民為身份證字號；外國人採用稅籍編號 10 位）10 碼

(2)重號編號 = 2 碼

(3)自選編號 = 最長 11 碼

二、 法人

(1)申請者 ID = BAN（在本國經濟部登錄之公司統一編號）8 碼

(2)重號編號 = 2 碼

(3)自選編號 = 最長 11 碼

註：

1. 不允許 Null DN，且每個欄位都必須有內容。
2. 重號編號、自選編號之型態限定為數字字元 0 至 9、小寫英文字元 a 至 z、與大寫英文字元 A 至 Z 組成。
3. 外國人採用稅籍編號 10 位，依據「財稅中心-所得人基本資料維護」規定之「所得人基本資料維護－身份證統一編號－所得人身分證統一編號編號方式附註說明」，所得人如為外僑，其統一編號前八位採護照內之西元出生年、月、日，後兩位則採護照內英文姓名第一個字之前兩位字母。參照10.2資料。

舉例資料：

表格 4-13 使用者憑證識別名稱範例表

欄　位	使用者識別名稱
Issuer	
Country (C)	TW
Organization (O)	CyberTrust Finance
Organizational Unit (OU)	CyberTrust Banking
Organizational Unit (OU)	0040000-BOT
Organizational Unit (OU)	FXML
Common Name (CN)	本國個人 (1) 不重號，且不提供使用者自選的 ID：“A123456789”。 (2) 重號，且不提供使用者自選的 ID：“A123456789-01”。 (3) 不重號，提供使用者自選的 ID：“A123456789--001”。 (4) 重號，提供使用者自選的 ID：“A123456789-01-001”。 外國個人 (1) 不重號，且不提供使用者自選的 ID：“19570228MJ” (2) 重號，且不提供使用者自選的 ID：“19570228MJ-01”。 (3) 不重號，提供使用者自選的 ID：“19570228MJ--001”。 (4) 重號，提供使用者自選的 ID：“19570228MJ-01-001”。 法人 (1) 不重號，且不提供使用者自選的 ID：“12345678”。 (2) 重號，且不提供使用者自選的 ID：“12345678-01”。 (3) 不重號，提供使用者自選的 ID：“12345678--001”。 (4) 重號，提供使用者自選的 ID：“12345678-01-001”。

4.3 憑證註銷清單說明

表格 4-14 憑證註銷清單欄位說明表

欄　位		內　容	說　明
1. CRL Field	**必**		**基本欄位**
1.1. Version	必	1	X509 V2 CRL 版本
1.2. Signature Algorithm	必	1.2.840.113549.1.1.5 或 1.2.840.113549.1.1.11，自 2017/1/1 起須為 1.2.840.113549.1.1.11	SHA-1 with RSA Signature 簽章代碼 PKCS#1-5 或 SHA256 with RSA Encryption，自 2017/1/1 起須使用 SHA256 with RSA Encryption
1.3. Issuer	必		簽發 CRL 之 CA 識別名稱，請參考4.2章節
1.3.1. Country (C)	必	e.g., “TW”	
1.3.2. Organization (O)	必	e.g., “CyberTrust Corporation”	
1.3.3. Organizational Unit (OU)	必	e.g., “User CA”	
1.3.4. Common Name (CN)	必	e.g., “Banking”	
1.4. This Update	必	e.g.,“00:00:01 01 September 2001”	發行日期時間
1.5. Next Update	必	e.g.,“00:00:01 02 September 2001”	下次發行日期時間
1.6. Revoked Certificates	必		被註銷憑證(一或多張)
1.6.1. Certificate Serial Number	必	e.g., “123456789”	憑證序號
1.6.2. Revocation Date	必	e.g., “00:00:01 01 June 2001”	註銷日期
1.6.3. CRL Entry Extensions	必		被註銷憑證的擴充欄位
1.6.3.1. CRL Reason	必		註銷原因(七種選一種)
1.6.3.1.1. Unspecified		0	不指定
1.6.3.1.2. Key Compromise		1	金鑰遭破解
1.6.3.1.3. CA Compromise		2	CA 金鑰遭破解
1.6.3.1.4. Affiliation Changed		3	憑證資料有改變
1.6.3.1.5. Superseded		4	憑證已被新憑證取代
1.6.3.1.6. Cessation Of Operation		5	不繼續使用憑證
1.6.3.1.7. Certificate Hold		6	憑證暫禁
1.6.3.1.8. Remove From CRL		8	(目前不使用)
2. CRL Field Extensions	必		標準擴充欄位
2.1. Authority Key Identifier	必		簽章之 CA 憑證資訊
2.1.1. Key Identifier	必		簽章之 CA 公開金鑰代碼
2.2. CRL Number	必	e.g., “987654321”	CRL 序號

依 X509 v2 標準，註銷原因有以下幾種，而註銷原因應記載於 CRL 內：

unspecified(0)　　：不指定
keyCompromise(1)　　：金鑰被破解或懷疑被破解
cACompromise(2)　　：CA 金鑰被破解或懷疑被破解
affiliationChanged(3)　　：憑證內所記錄資訊已改變
superseded(4)　　：憑證已被新憑證取代
cessationOfOperation(5)　：不再使用憑證

certificateHold(6)　　：憑證暫停使用，即暫禁
removeFromCRL(8)　　：使用於 Delta CRL 機制(不使用)

4.4 使用者憑證申請訊息

表格 4-15 使用者憑證申請訊息欄位說明

欄　位		說　明
1. Version	**必**	**憑證請求資訊格式使用 PKCS#10 V1 格式（注意 V1 的值是 0 而不是 1）**
2. Signature Algorithm	必	簽章演算法，使用 SHA-1 with RSA Encryption (PKCS#1-5) (1.2.840.113549.1.1.5) 或 SHA256 with RSA Encryption (PKCS#1-5) (1.2.840.113549.1.1.11)，自 2017/1/1 起須使用 SHA256 with RSA Encryption (PKCS#1-5) (1.2.840.113549.1.1.11)
3. Subject	必	使用者識別名稱
3.1 Common Name (CN)	必	使用者識別碼，命名規則於「4.2.3 使用者識別名稱」之憑證申請人的用戶識別碼說明
4. Subject Public Key Info	必	使用者公開金鑰，使用 RSA 演算法

本申請標準為 PKCS #10 [RFC 2314]: Certification Request Syntax Standard。不包含憑證申請訊息結構中的簽章演算法欄位(SignatureAlgorithm)和簽體欄位(SignatureValue)。

5. 憑證管理與週期

使用者的金鑰對須由客戶自行產生,不由 RA 作業人員替使用者產生以減少糾紛。

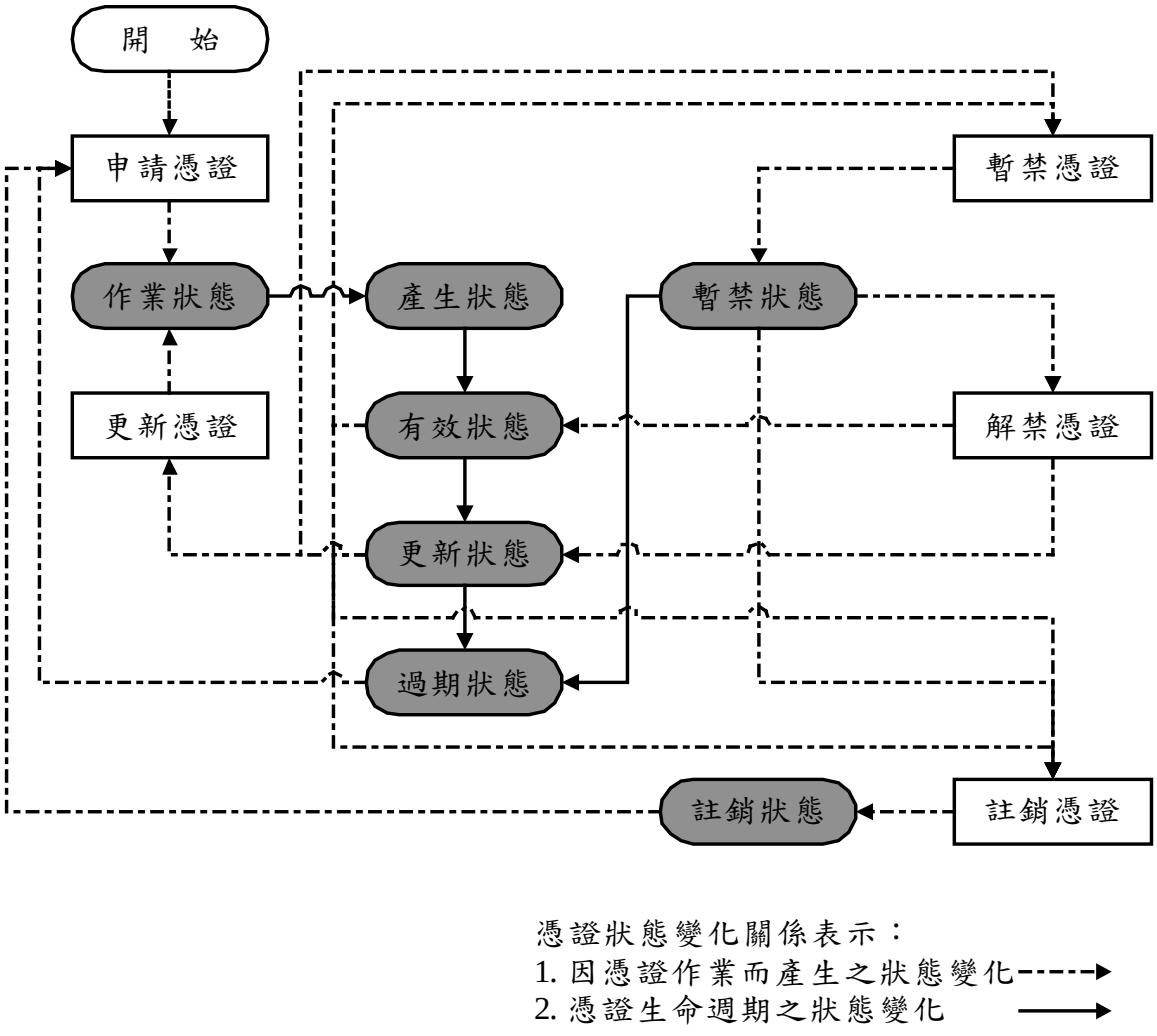
使用者金鑰的週期與使用者憑證的週期是一致的，以下對使用者憑證週期的解釋即涵蓋使用者金鑰週期。

5.1 憑證狀態

憑證狀態是起始於憑證申請、憑證被產生，結束於憑證被註銷或過期，區分為七種狀態：

- 作業狀態
- 產生狀態
- 有效狀態
- 更新狀態
- 暫禁狀態
- 註銷狀態
- 過期狀態

各狀態間關係如下圖：



圖表 5-1 憑證狀態圖

5.1.1 作業狀態

憑證申請者需要攜帶相關文件親至註冊中心辦理申請與身份確認事項，所有的憑證開始於此狀態。

- 在此狀態內，確認使用者身份。
- 在此狀態內，確認使用者資料。
- 在此狀態內，使用者產生一組公開金鑰與私密金鑰。
- 在此狀態內，使用者的憑證申請訊息透過註冊中心傳送至認證中心。

完成以上作業，憑證的作業狀態改變為產生狀態。

5.1.2 產生狀態

在認證中心接受註冊中心憑證申請訊息後進入憑證產生狀態。

- 在此狀態內，認證中心產生一個憑證。
- 在此狀態內，認證中心公告一個憑證至目錄伺服。
- 在此狀態內，認證中心回傳憑證鏈至至註冊中心。
- 在此狀態內，使用者至註冊中心下載憑證鏈。

完成以上作業，憑證的產生狀態改變為有效狀態。

5.1.3 有效狀態

客戶下載憑證後就進入了憑證有效狀態，客戶可以開始使用這憑證與金鑰，除了因憑證註銷、暫禁的情況外，憑證內的開始日期時間與終止日期時間之間皆算是有效狀態。

憑證的有效狀態有可能：

- 因日期為終止日前一至二個月而改變為更新狀態。
- 因註銷憑證而改變為註銷狀態。
- 因暫禁憑證而改變為暫禁狀態。

5.1.4 更新狀態

指憑證的終止日期前一至二個月開始到終止日期為止，憑證更新的通知由註冊中心負責，憑證擁有者不需臨櫃而可以線上來申請另外一張新的憑證，此新憑證內的使用者資料須與舊憑證使用者資料一致，憑證更新時需重新產生金鑰，不可使用原有金鑰，新憑證生效日期為新憑證簽發日，而新憑證終止日期為舊憑證終止日期加上一個憑證週期(請參考5.2章節)，憑證更新後客戶會有兩張有效的憑證。

憑證的更新狀態有可能：

- 因客戶再次的申請憑證後而改變為作業狀態。
- 因註銷憑證而改變為註銷狀態。
- 因暫禁憑證而改變為暫禁狀態。
- 因過了憑證終止日而改變為過期狀態。

5.1.5 過期狀態

當日期時間過了憑證的終止日期時間，憑證會進入憑證過期狀態，當憑證進入過期狀態，憑證即不能辦理憑證更新，客戶就需要再次的臨櫃辦理憑證申請，不能線上更新憑證，而設定憑證有效期限的主要原因是為防止金鑰遭遇長時間攻擊而引起的安全顧慮。

5.1.6 暫禁狀態

暫禁憑證有以下二個目的：

- 懷疑憑證的不安全性，如不確定是否遺失金鑰。
- 暫停使用憑證一段期間。

如客戶有需要暫禁憑證時，需登錄原申請憑證之註冊中心憑證註冊應用系統辦理或親至原申請憑證之註冊中心辦理。

在憑證暫禁請求被認證中心接受後，憑證即進入暫禁狀態，而憑證的暫禁狀態有可能：

- 因解禁憑證而改變為有效狀態或更新狀態。
- 因註銷憑證而改變為註銷狀態。
- 因超過憑證終止日而改變為過期狀態。

如客戶暫禁憑證的原因消失，有需要解禁憑證時，亦需親至原申請憑證之註冊中心辦理。

5.1.7 註銷狀態

註銷憑證有以下二個目的：

- 憑證的不安全性，如洩露金鑰密碼。
- 永久停止使用憑證與其關聯的金鑰。

如客戶有需要註銷憑證時，需親至原申請憑證之註冊中心辦理。

在憑證註銷請求被認證中心接受後，憑證即進入註銷狀態，憑證一旦註銷後，就不可以回復成任何狀態，而憑證註銷的原因也會被記錄於憑證註銷清單內。

5.2 憑證週期

使用者憑證的週期為：

- 1 年：金鑰儲存媒體使用非硬體裝置，如磁碟片。
  或
- 2 年：金鑰儲存媒體使用硬體裝置，如 IC 卡。

認證中心與註冊中心所使用之憑證週期與更新程序，認證機構應自行做妥善的規劃與管理，本規範不擬統一制定

在憑證更新的過程中，會有二個有效憑證同時存在的情況。

憑證週期即將到期前會進入至憑證更新狀態，憑證使用者可根據需要而申請新的憑證，此憑證更新的過程必須避免中斷或終止任何相關憑證的正常運作。

5.3 憑證作業記錄保存

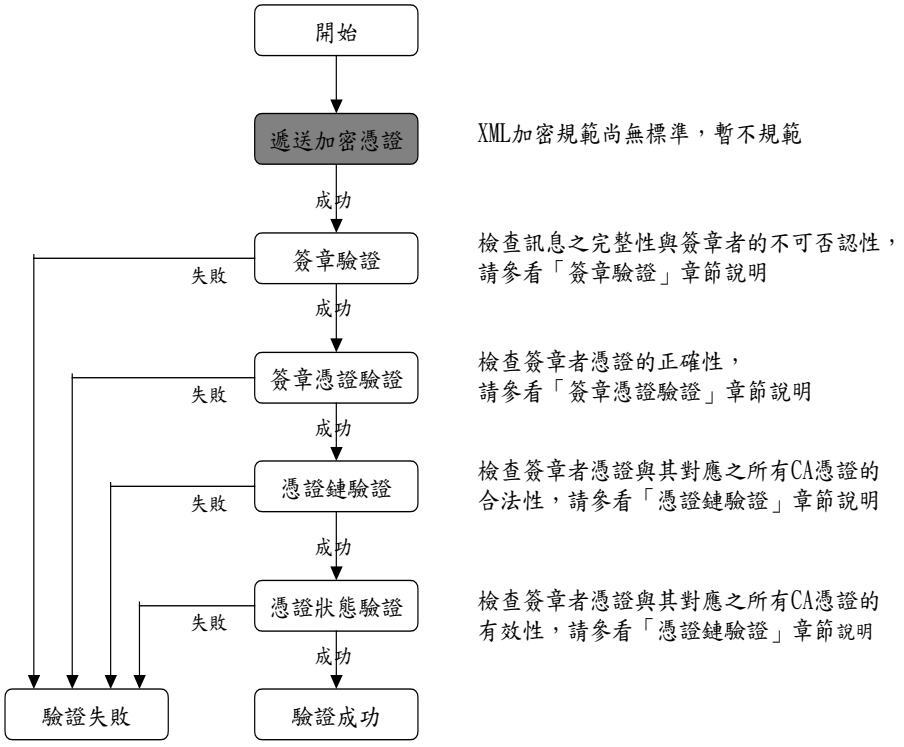
PKI 系統內必須針對憑證的相關使用紀錄與審核資料加以儲存。
所有的文件與資料必須安全的保護在實體的架構中。
以下是必須儲存的憑證作業資料：

- 憑證申請作業紀錄
- 憑證申請的相關文件
- 相關合約文件
- 所有在憑證週期中所產生的需求紀錄與相關作業紀錄

資料保存規範請參照主管機關相關規定辦理。

6. 交易驗證

交易驗證主要在保障交易雙方的權益，驗章目的在於確保簽章者的不可否認性和簽章資料的完整性，而憑證鏈驗證的過程是為了檢查此憑證的狀態與相關資訊，此過程根據憑證鏈上所有憑證的內容，利用繁複的檢查與驗證機制，以取得此憑證可靠的狀態與相關資訊，利用簽章和憑證驗證機制以維持 PKI 架構的安全環境。



圖表 6-1 交易驗證流程圖

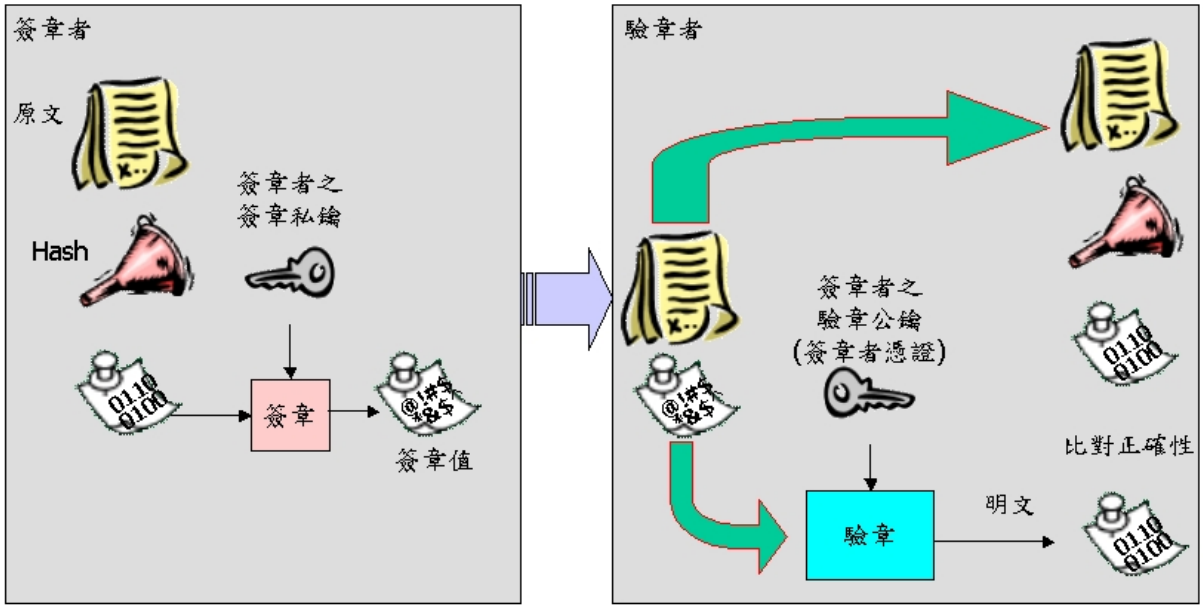
加密憑證遞送

因國際 XML 標準在加密部份尚未公布，暫不規範加密部份，待 XML 加密國際標準公布後再行規範。

6.1 簽章驗證

6.1.1 簽章驗證

接收者在收到送方簽章過的訊息時，第一個檢驗動作是先對此訊息做驗章的動作，以確定簽章者的不可否認性，與原文在傳輸過程中未遭篡改的資料完整性，故需利用簽章者憑證針對原文和簽體作一比對，若發現錯誤則需回覆給予送方錯誤訊息，若比對正確則進行下一檢驗動作，檢查簽章者憑證。



圖表 6-2 簽章驗證示意圖

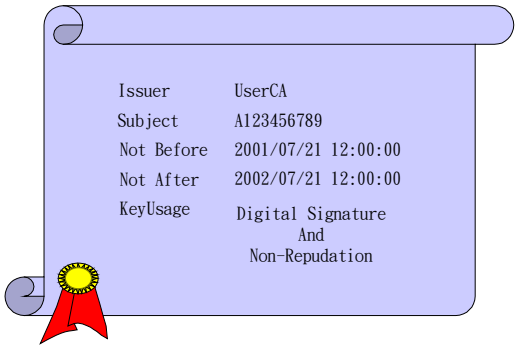
6.1.2 簽章憑證驗證

接收者為了確認簽章者為一合法使用者，且應用正確之憑證進行交易作業，必須對憑證進行檢驗，以達安控管制。

檢查憑證的項目如下：

1. 簽章者憑證中的使用者識別名稱(Subject)，必須符合交易系統的合法使用者。
2. 簽章者憑證的生效日期時間：必須是已開始。
3. 簽章者憑證的終止日期時間：必須是未過期。
4. KeyUsage 擴充欄位內的金鑰用途設定：必須是簽章憑證。

若檢查憑證的項目有任何一項有錯誤，則需回覆錯誤訊息，若所有項目都通過則進行下一檢驗動作，憑證鏈驗證。

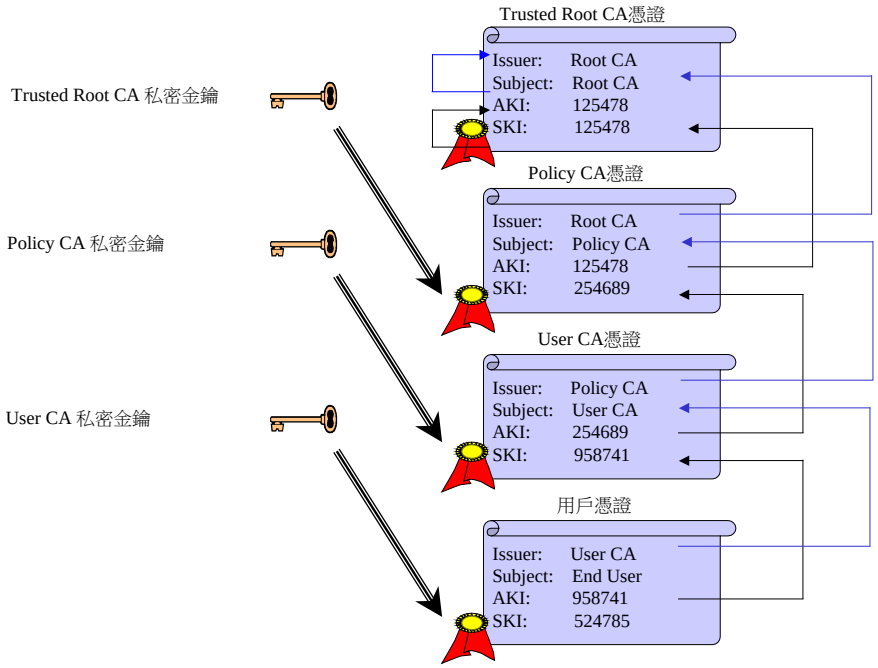


圖表 6-3 使用者憑證

6.2 憑證鏈驗證

6.2.1 憑證鏈的關係

憑證是以 CA 之簽章來保證憑證內容之正確性與完整性,所以要驗證此一個憑證之正確性與完整性，需使用 CA 之公開金鑰來做驗證，CA 之公開金鑰可由 CA 之憑證中獲得，而此 CA 憑證或許也是被其所屬之上層 CA 簽章保證，因此要驗證此 CA 憑證，同理需取得其上層 CA 之憑證來做驗證，依此類推直到最高層之 CA，此一連鎖現象，稱為憑證鏈。



圖表 6-4 憑證鏈關係圖

交易對象透過階層式之憑證信任架構來驗證使用者的憑證。每一個憑證都可串聯到其上層 CA 的簽章憑證。驗證憑證鏈時，可依階層順序由下而上為：使用者憑證，UCA 憑證，PCA 憑證，最後為 RCA 憑證，同時必須檢驗憑證內的 CA 簽章,另需確定憑證的效期需涵蓋於上層 CA 憑證的效期內。

6.2.2 使用者憑證有效性驗證

以下原則需完全滿足：

(1)使用者憑證的憑證效期必須涵蓋住驗章者所選定的驗章時間。
（使用者憑證的生效日 ≦ 驗章時間 ≦ 使用者憑證到期日）

(2)使用使用者憑證的「Authority Key Identifier」欄位，以取得正確 UCA 憑證，再使用 UCA 公開金鑰(Public Key)檢驗使用者憑證的完整性必須是正確。

(3)UCA 憑證中之「Subject」必須與使用者憑證中的「Issuer」相符。

(4)UCA 憑證的憑證效期必須涵蓋住使用者憑證的憑證效期。
（UCA 憑證的生效日 ≦ 使用者憑證的生效日，且
UCA 憑證的到期日 ≧ 使用者憑證的到期日）

(5)使用 OCSP 或 CRL 機制檢驗時，使用者憑證於驗章時間必須未被註銷或暫禁。

[註 1]使用 OCSP 機制檢驗時，使用者憑證的「Authority Information Access Location」內容即為使用者憑證所屬 UCA 的 OCSP 伺服器位址，可利用此訊息使用 OCSP 查尋此使用者憑證最新狀態，OCSP 查詢作業又可分跨 RA 與跨 UCA 兩種模式，於6.2.7章節說明。

[註 2]使用 CRL 機制檢驗時，須使用使用者憑證的「CRL Distribution Point」欄位，依據記載於上的 URL，取得最新的 CRL 並存入驗章者的 CRL 資料庫中。若驗章者所保有之最新版 CRL 尚未過期，可直接使用，不須再至「CRL Distribution Point」下載。

6.2.3 UCA 憑證有效性驗證

以下原則需完全滿足：

(1) UCA 憑證的憑證效期必須涵蓋住驗章者所選定的驗章時間。
（UCA 憑證的生效日 ≦ 驗章時間 ≦ UCA 憑證到期日）

(2) UCA 憑證的「Key Usage」欄位必須包含「Key Certificate Signature」及「CRL Signature」功能。

(3) UCA 憑證中「Basic Constraints」欄位內的「CA」欄位值必須為「True」。

(4) UCA 憑證中之「Subject Key Identifier」必須與使用者憑證中的「Authority Key Identifier」相符。

(5) 使用 UCA 憑證中之「Authority Key Identifier」欄位，以取得正確 PCA 憑證，再使用 PCA Public Key 檢驗 UCA 憑證的完整性必須是正確。

(6) PCA 憑證中之「Subject」必須與 UCA 憑證中的「Issuer」相符。

(7) PCA 憑證的憑證效期必須涵蓋住 UCA 憑證的憑證效期。
（PCA 憑證的生效日 ≦ UCA 憑證的生效日，且
PCA 憑證的到期日 ≧ UCA 憑證的到期日）

(8) 使用 OCSP 或 CRL 機制檢驗時，UCA 憑證於驗章時間必須未被註銷或暫禁。

6.2.4 PCA 憑證有效性驗證

以下原則需完全滿足：

(1) PCA 憑證的憑證效期必須涵蓋住驗章者所選定的驗章時間。
（PCA 憑證的生效日 ≦ 驗章時間 ≦ PCA 憑證到期日）

(2) PCA 憑證的「Key Usage」欄位必須包含「Key Certificate Signature」及「CRL Signature」功能。

(3) PCA 憑證中「Basic Constraints」欄位內的「CA」欄位必須為「True」。

(4) PCA 憑證中之「Subject Key Identifier」必須與 UCA 憑證中的「Authority Key Identifier」相符。

(5) 使用 PCA 憑證中之「Authority Key Identifier」欄位，以取得正確 RCA 憑證，再使用 RCA Public Key 檢驗 PCA 憑證的完整性必須是正確。

(6) RCA 憑證中之「Subject」必須與 PCA 憑證中的「Issuer」相符。

(7) RCA 憑證的憑證效期必須涵蓋住 PCA 憑證的憑證效期。
（RCA 憑證的生效日 ≦ PCA 憑證的生效日，且
RCA 憑證的到期日 ≧ PCA 憑證的到期日）

(8) 使用 OCSP 或 CRL 機制檢驗時，PCA 憑證於驗章時間必須未被註銷或暫禁。

6.2.5 RCA 憑證有效性驗證

以下原則需完全滿足：

(1) RCA 憑證的憑證效期必須涵蓋住驗章者所選定的驗章時間。
（RCA 憑證的生效日 ≦ 驗章時間 ≦ RCA 憑證到期日）

(2) RCA 憑證的「Key Usage」欄位必須包含「Key Certificate Signature」及「CRL Signature」功能。

(3) RCA 憑證中「Basic Constraints」欄位內的「CA」欄位必須為「True」。

(4) RCA 憑證中之「Subject Key Identifier」必須與 RCA 憑證中的「Authority Key Identifier」相符。

(5) 使用 RCA Public Key 檢驗 RCA 憑證的完整性必須是正確。

(6) RCA 憑證中之「Subject」必須與 RCA 憑證中的「Issuer」相符。

(7) RCA 憑證之拇指紋（FingerPrint），必須與 RCA 所公告的完全相符且是使用者所信任的。

6.2.6 RCA 憑證公告

RCA 須於認證中心網站公告並維護 RCA 相關金鑰與憑證資訊，供使用者下載、安裝與驗證，內容包括：

(1)RCA 憑證名稱。

(2)RCA 所有金鑰(名稱)與憑證(序號)的使用狀態(使用中、已過期、已終止)。

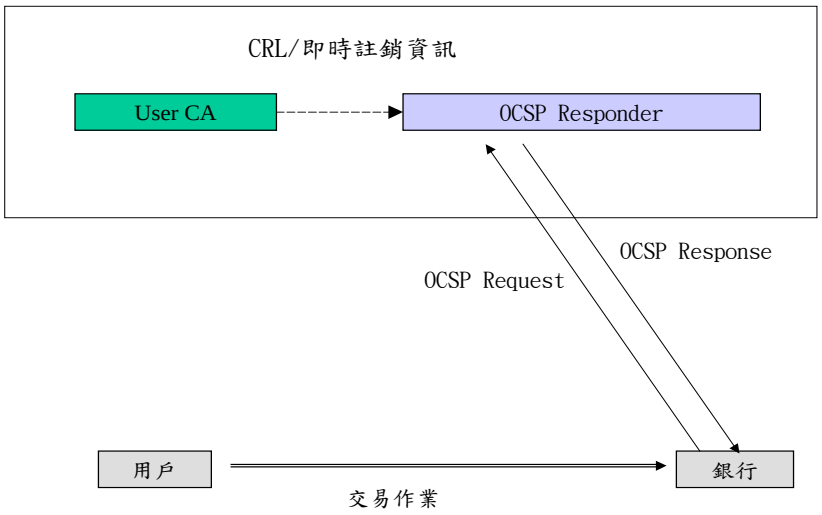
(3)RCA憑證拇指紋FingerPrint(SHA-1 或SHA256 Hashing value, 自2017/1/1 起須使用SHA256)。

6.2.7 OCSP 作業程序

為取得最新之憑證是否被註銷狀態資訊，可應用 OCSP 機制，OCSP 機制之訊息協定與格式應遵循[RFC 2560]標準規定，作業程序如下二節介紹：

6.2.7.1 跨 RA 之 OCSP 作業程序

驗章者和簽章者憑證分屬不同 RA(兩個 RA 同屬一個 UCA)的 OCSP 作業方式如下：



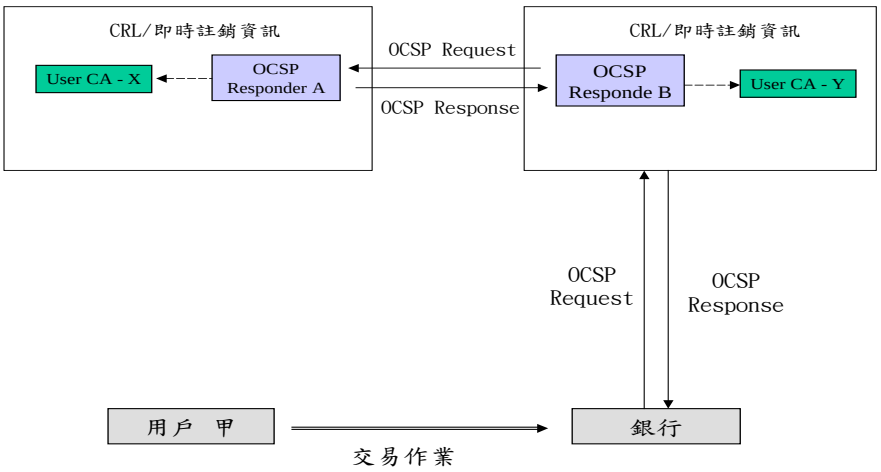
圖表 6-5 跨 RA 的 OCSP 作業圖

(1) 驗章者(金融機構)將簽章者(使用者)的憑證訊息包裝在 OCSP Request 訊息。
(2) 驗章者(金融機構)對 OCSP Request 簽章，然後遞送給驗章者(金融機構)所屬 CA 的 OCSP Responder。
(3) OCSP Responder 驗證驗章者(金融機構)的簽章。
(4) OCSP Responder 分析簽章者(使用者)的憑證是否被 UCA 註銷。
(5) OCSP Responder 將(4)的分析結果，包裝在 OCSP Response 訊息。
(6) OCSP Responder 對 OCSP Response 簽章，回覆給驗章者(金融機構)。
(7) 驗章者(金融機構)驗證 OCSP Responder 的簽章。
(8) 驗章者(金融機構)取得此張憑證最新之是否被註銷狀態資訊。

註：OCSP 伺服器回覆的憑證狀態有 Good、Revoked 和 Unknown 三種。
1. Good:憑證無被註銷或被暫禁的記錄，但不保證憑證已存在或在有效期
2. Revoked:憑證已被註銷或被暫禁
3. Unknown:憑證不在管轄範圍

6.2.7.2 跨 UCA 之 OCSP 作業程序

驗章者和簽章者憑證分屬不同 UCA(兩個 UCA 同屬一個 PCA)的 OCSP 作業方式如下：



圖表 6-6 跨 UCA 的 OCSP 作業圖

(1)驗章者(金融機構)將簽章者(使用者甲)的憑證訊息包裝在 OCSP Request 訊息。
(2)驗章者(金融機構)對 OCSP Request 簽章，然後遞送給驗章者(金融機構)所屬 CA 的 OCSP Responder B。
(3)OCSP Responder B 驗證驗章者(金融機構)的簽章。
(4)OCSP Responder B 將簽章者(使用者甲)的憑證訊息，包裝在 OCSP Request 訊息。
(5)OCSP Responder B 對 OCSP Request 簽章，使用簽章者(使用者甲)憑證「Authority Information Access Location」內容遞送給 OCSP Responder A。
(6)OCSP Responder A 驗證 OCSP Responder B 的簽章。
(7)OCSP Responder A 分析簽章者(使用者甲)的憑證是否被 UCA-X 註銷。
(8)OCSP Responder A 將(7)的分析結果，包裝在 OCSP Response 訊息。
(9)OCSP Responder A 對 OCSP Response 簽章,回覆送給 OCSP Responder B。
(10)OCSP Responder B 驗證 OCSP Responder A 的簽章。
(11)OCSP Responder B 透過 OCSP Responder A 取得簽章者(使用者甲)憑證最新之是否被註銷狀態資訊。
(12)OCSP Responder B 將(11)的分析結果，包裝在 OCSP Response 訊息。
(13)OCSP Responder B 對 OCSP Response 簽章，回覆給驗章者(金融機構)。
(14)驗章者(金融機構)驗證 OCSP Responder B 的簽章。
(15)驗章者(金融機構)取得此張憑證最新之是否被註銷狀態資訊。

6.3 跨 RA 時與跨 UCA 時憑證驗證

為達憑證共用目的，一張憑證可使用於多個註冊中心與多個認證中心系統，當驗章者與簽章者分屬不同的註冊中心(跨 RA)或不同的認證中心(跨 UCA)時，驗章者除需檢驗上面章節的驗證動作外，仍需檢驗簽章憑證資訊是否與憑證登記時所記錄的憑證資訊一致，如憑證序號等，以免客戶誤用簽章憑證。

使用本憑證的應用服務，依據其可承擔的風險大小，於驗證憑證及憑證鍊有效性時，統一選定採用本規範之 CRL 或 OCSP 作業程序。

(1) 採用 CRL 驗證時，需由驗證之註冊中心依據所驗證憑證 X.509 格式內 CRL Distribution Point 所公佈之 CRL URI 網址，各自向不同的認證中心(跨 UCA)以 Hypertext Transfer Protocol(HTTP)存取介面下載 CRL 憑證進行驗證。

(2) 採用 OCSP 驗證者，需符合本規範 OCSP 程序。

7. 憑證作業程序

針對各項憑證作業訂定標準的作業程序，各參加單位應遵循本規範所訂定的憑證作業程序，以達到一致程度的安全標準。

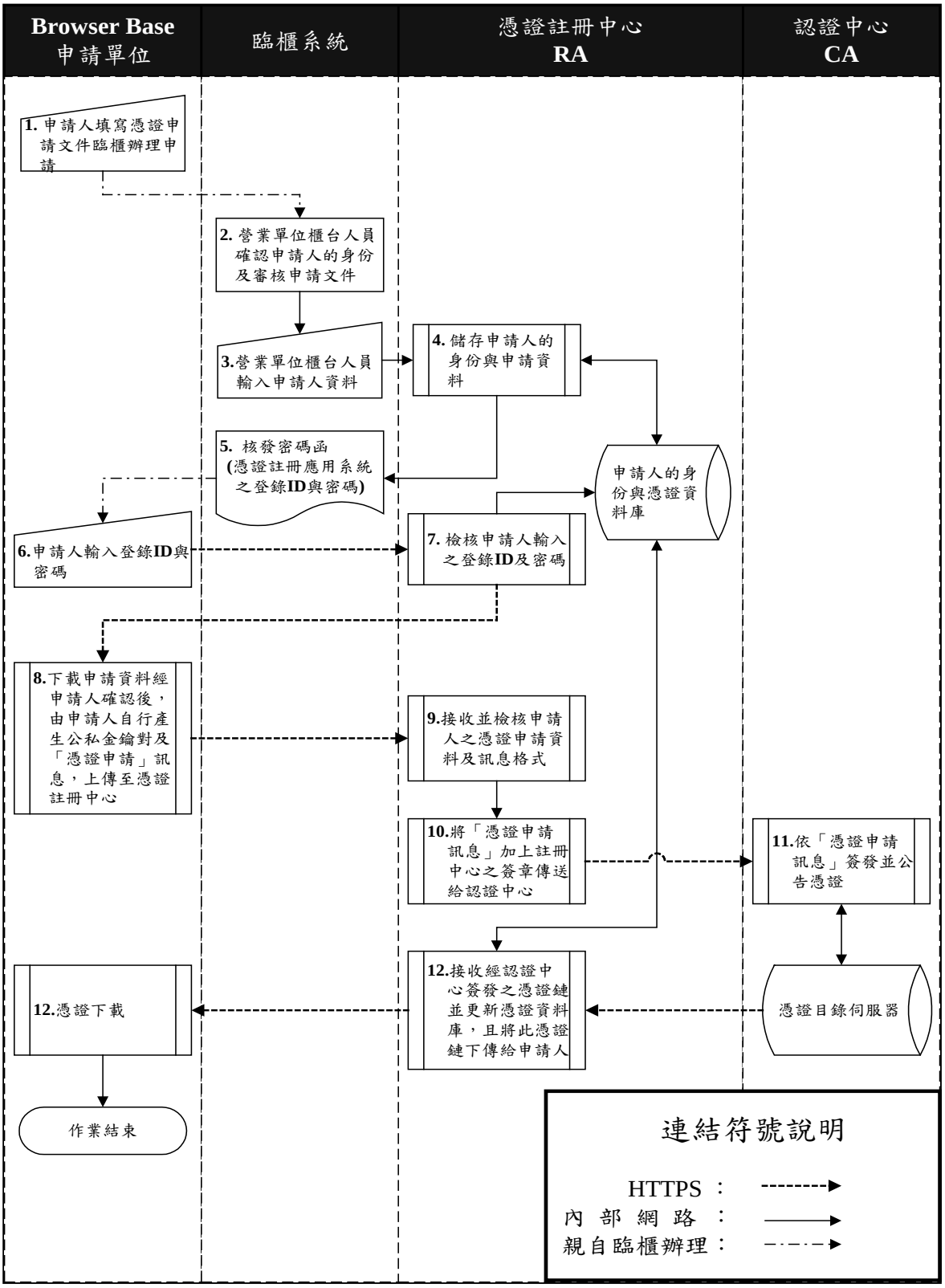
客戶依所使用的憑證管理工具可分為 Browser Base 客戶(即 Thin Client)與 Server Base 客戶；其中 Browser Base 客戶使用的憑證管理工具是由註冊中心之金融機構提供，而 Server Base 客戶使用的憑證管理工具則是由客戶自行準備。本章節之各項憑證作業將針對此兩類客戶分別訂定規範如后：

7.1 憑證註冊/申請作業

本作業可分為憑證註冊及憑證申請兩個子作業，本規範為了確實認證申請人之身份，要求各參加單位規劃憑證註冊作業一律採臨櫃申請模式；而且憑證申請作業中金鑰的產生是由申請人自行操作，其作業程序詳述如后：

7.1.1 Browser Base 客戶憑證註冊/申請作業

7.1.1.1 Browser Base 客戶憑證註冊/申請作業流程圖



圖表 7-1 Browser Base 客戶憑證註冊/申請作業流程圖

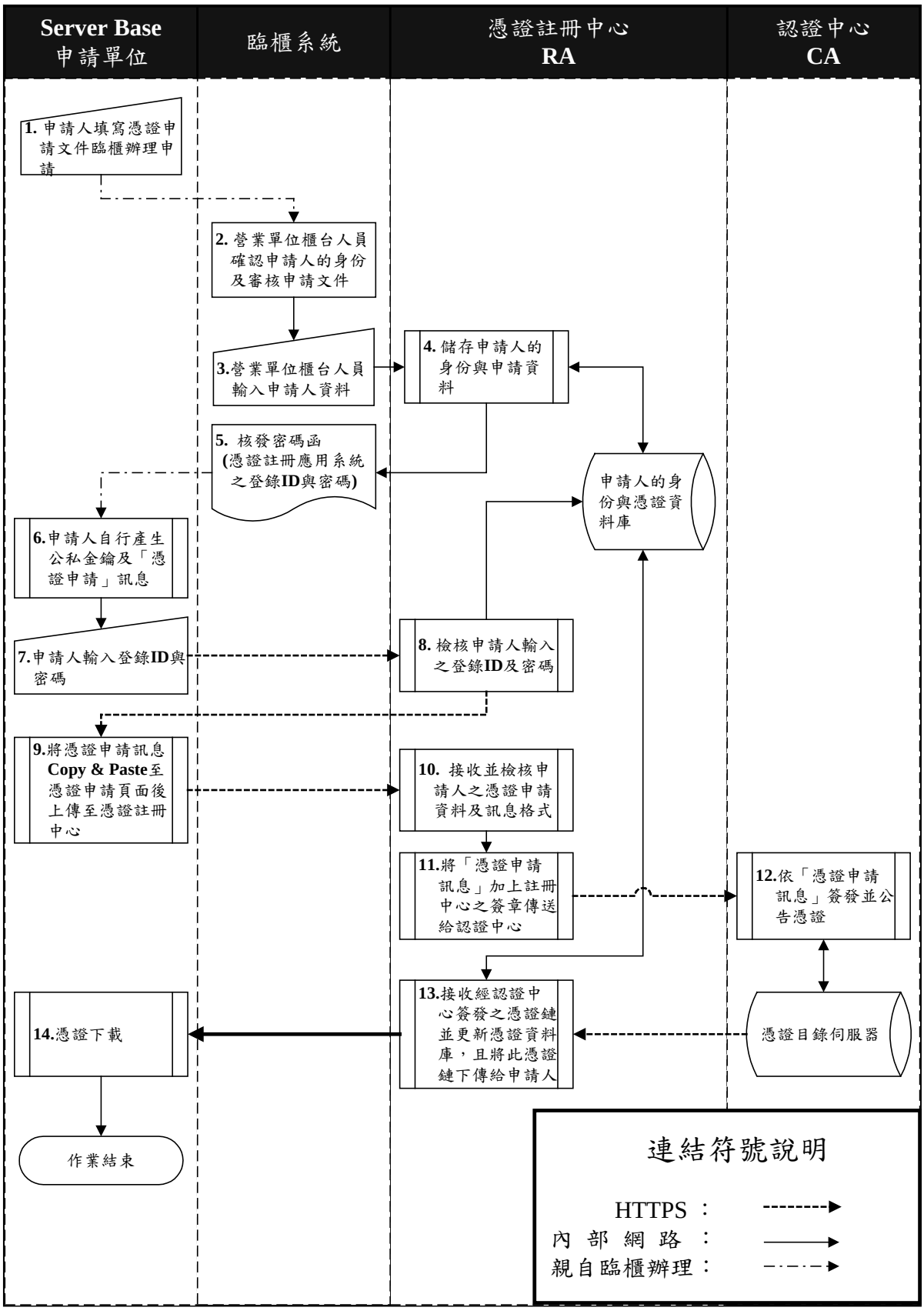
7.1.1.2 Browser Base 客戶憑證註冊/申請作業說明

表格 7-1 Browser Base 客戶憑證註冊/申請作業說明表

步驟	作業單位	作業內容
1	申請人	●填寫憑證申請文件並攜帶身份證明文件於往來之金融機構臨櫃辦理憑證申請作業。 ●申請人應準備之身份證明文件有： ■個人為身份證、護照(外國人)等 ■公司為公司執照影本、營利事業登記證影本等
2	臨櫃人員	●檢核身份證明文件確認申請人之身份 ●審核申請人填具之憑證申請文件及核對留存印鑑
3	臨櫃人員	●執行憑證註冊交易，輸入申請人相關資料
4	註冊中心	●儲存申請人身份資料與憑證註冊相關資料 ●回覆登錄 ID 及密碼
5	臨櫃人員	●核發密碼函(即憑證註冊應用系統登錄 ID 及密碼)
6	申請人	●輸入登錄 ID、密碼憑以登入憑證註冊應用系統
7	註冊中心	●檢核申請人輸入之登錄 ID、密碼 ●下傳申請人憑證申請資料 ●本項作業為申請人之憑證申請作業，故必須確認申請人之身份，除檢核登錄 ID 及密碼外，各註冊中心得自行決定採用其他輔助資料以供驗證申請人的身分，並須具備 Session Control 及加密機制，且應拒絕未經授權的存取
8	申請人	●將憑證申請資料下載至使用者端，並確認資料無誤 ●申請人自行產生金鑰對(需設定私密金鑰之密碼，以保護私密金鑰避免遭人誤用) ●產生 PKCS#10 格式[RFC 2314]之「憑證申請」訊息 ●將「憑證申請」訊息上傳至註冊中心
9	註冊中心	●接收並檢核申請人之憑證申請資料及訊息格式
10	註冊中心	●將「憑證申請」訊息加上註冊中心的簽章 ●傳送簽章後之「憑證申請」訊息至認證中心
11	認證中心	●接收「憑證申請」訊息並驗證註冊中心的簽章 ●依「憑證申請」訊息簽發憑證 ●將所簽發之憑證公告於「憑證目錄伺服器」 ●將憑證鏈(PKCS#7 格式[RFC 2315])下傳給註冊中心
12	註冊中心	●接收經認證中心簽發之憑證鏈並儲存於憑證資料庫 ●將憑證鏈下傳給申請人
13	申請人	●連接憑證註冊應用系統後，下載憑證

7.1.2 Server Base 客戶憑證註冊/申請作業

7.1.2.1 Server Base 客戶憑證註冊/申請作業流程圖



圖表 7-2 Server Base 客戶憑證註冊/申請作業流程圖

7.1.2.2 Server Base 客戶憑證註冊/申請作業說明

表格 7-2 Server Base 客戶憑證註冊/申請作業說明表

步驟	作業單位	作業內容
1	申請人	●填寫憑證申請文件並攜帶身份證明文件於往來之金融機構臨櫃辦理憑證申請作業。 ●申請人應準備之身份證明文件有： ■個人為身份證、護照(外國人)等 ■公司為公司執照影本、營利事業登記證影本等
2	臨櫃人員	●檢核身份證明文件確認申請人之身份 ●審核申請人填具之憑證申請文件及核對留存印鑑
3	臨櫃人員	●執行憑證註冊交易，輸入申請人相關資料
4	註冊中心	●儲存申請人身份資料與憑證註冊相關資料 ●回覆登錄 ID 及密碼
5	臨櫃人員	●核發密碼函(即憑證註冊應用系統登錄 ID 及密碼)
6	申請人	●申請人自行產生金鑰對(需設定私密金鑰之密碼，以保護私密金鑰避免遭人誤用) ●產生 Base64 Encode 的 PKCS#10 格式之「憑證申請」訊息
7	申請人	●輸入登錄 ID、密碼憑以登入憑證註冊應用系統
8	註冊中心	●檢核申請人輸入之登錄 ID、密碼以確認身份 ●下傳申請人憑證申請資料 ●本項作業為申請人之憑證申請作業必須確認申請人之身份，除檢核登錄 ID 及密碼外，各註冊中心得自行決定採用其他輔助資料以供驗證申請人的身分，並須具備 Session Control 及加密機制，且應拒絕未經授權的存取
9	申請人	●將憑證申請資料下載至使用者端，經確認資料無誤 ●將「憑證申請」訊息 Copy & Paste 至憑證登記頁面，上傳至註冊中心
10	註冊中心	●接收並檢核申請人之憑證申請資料及訊息格式
11	註冊中心	●將「憑證申請」訊息加上註冊中心的簽章 ●傳送簽章後之「憑證申請」訊息至認證中心
12	認證中心	●接收「憑證申請」訊息並驗證註冊中心的簽章 ●依「憑證申請」訊息簽發憑證 ●將所簽發之憑證公告於「憑證目錄伺服器」 ●將憑證鏈下傳給註冊中心

步驟	作業單位	作　　業　　內　　容
13	註冊中心	●接收經認證中心簽發之憑證鏈並儲存於憑證資料庫 ●將憑證鏈下傳給申請人
14	申 請 人	●連接憑證註冊應用系統後，下載憑證

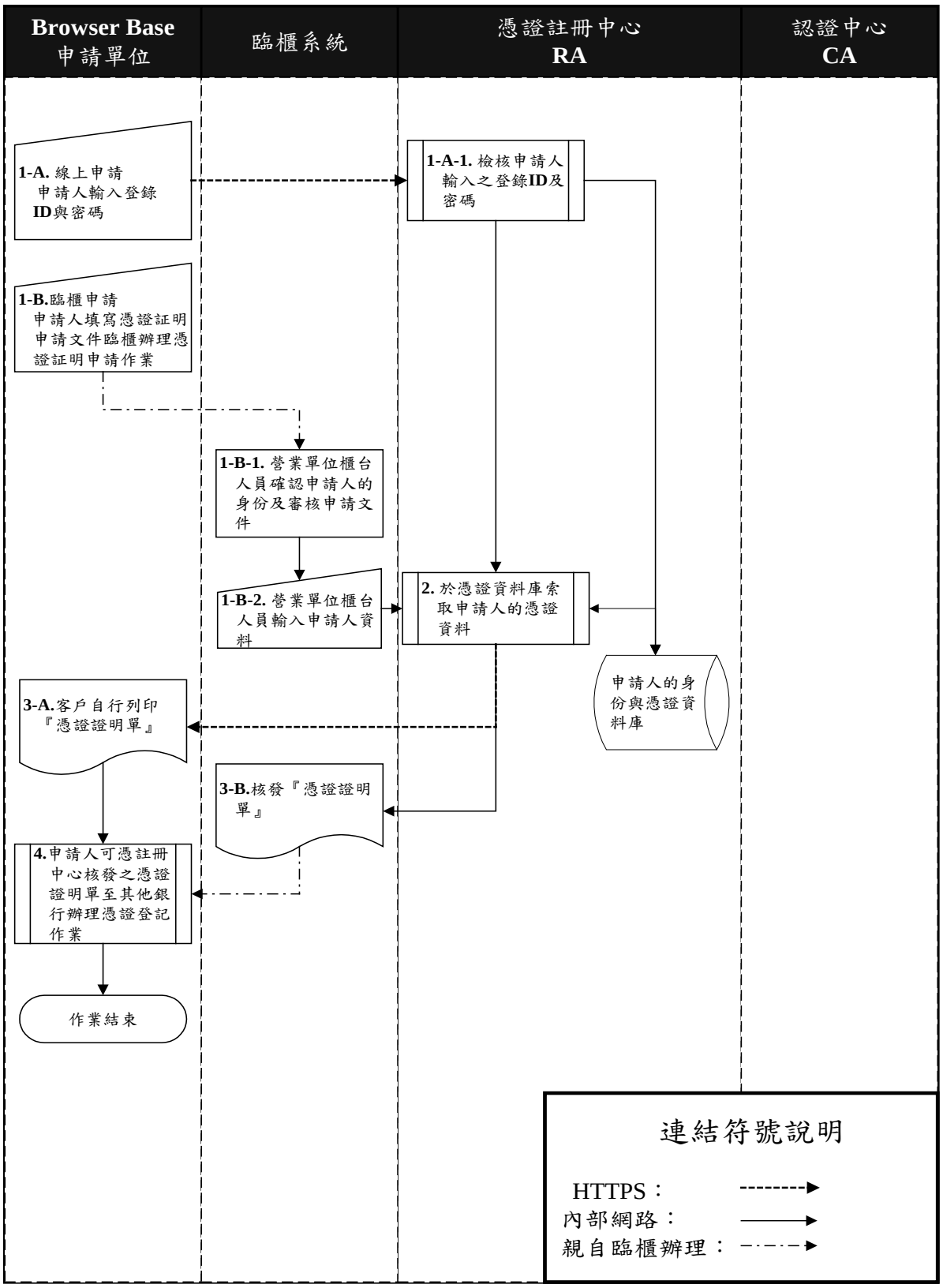
7.2 憑證登記作業

為達到憑證共用之目的，使用者可憑有效之憑證至其他參加本作業之金融機構辦理憑證登記後使用；原憑證註冊應用系統應提供列印「憑證證明單」功能以茲證明，各金融機構可由申請人提供之身份證明文件及「憑證證明單」內容來確認其與登記之憑證的關連，並於核對無誤後登記列管。

本作業可分為憑證證明單申請及憑證登記兩項子作業；其中憑證證明單申請作業，申請人可選擇至原註冊中心臨櫃申請「憑證證明單」或於線上登入憑證註冊應用系統後自行列印「憑證證明單」等兩種方式，取得註冊中心所核發之「憑證證明單」。並於取得「憑證證明單」後，方可至其他參加本作業之金融機構臨櫃辦理憑證登記作業。

7.2.1 Browser Base 客戶憑證登記作業

7.2.1.1 Browser Base 客戶憑證證明單申請作業流程圖



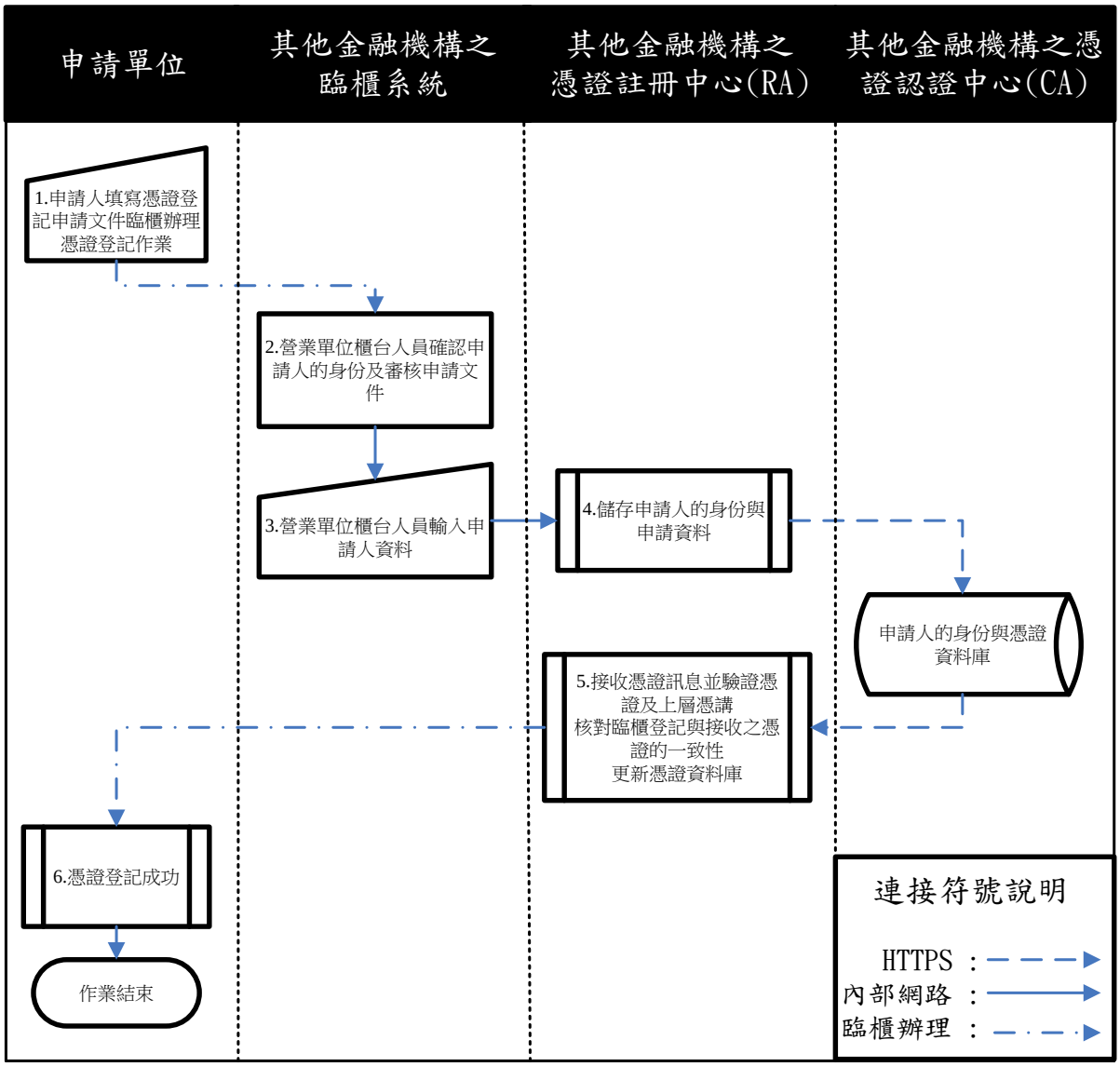
圖表 7-3 Browser Base 客戶憑證證明單申請作業流程圖

7.2.1.2 Browser Base 客戶憑證證明單申請作業說明

表格 7-3 Browser Base 客戶憑證證明單申請作業說明表

步驟	作業單位	作業內容
1-A	申請人	●線上申請 ●輸入登錄 ID、密碼憑以登入憑證註冊應用系統
1-A-1	註冊中心	●檢核申請人輸入之登錄 ID、密碼以確認身份 ●本項作業為申請人之憑證證明單申請作業，為防止申請人憑證之相關資訊外洩，應具備 Session Control 及加密機制，並應拒絕未經授權的存取
1-B	申請人	●臨櫃申請 ●填寫憑證證明申請文件並攜帶身份證明文件於原憑證註冊之金融機構臨櫃辦理憑證證明單申請作業 ●申請人應準備之身份證明文件有： ■個人為身份證、護照(外國人)等 ■公司為公司執照影本、營利事業登記證影本等
1-B-1	臨櫃人員	●檢核身份證明文件確認申請人之身份 ●審核申請人填具之憑證證明單申請文件
1-B-2	臨櫃人員	●執行憑證證明申請交易，輸入申請人相關資料
2	註冊中心	●索取憑證資料庫中申請人之憑證資料
3-A	申請人	●自行列印『憑證證明單』
3-B	臨櫃人員	●核發『憑證證明單』
4	申請人	●可憑註冊中心所核發之憑證證明單至其他參加本作業之金融機構辦理憑證登記作業

7.2.1.3 Browser Base 客戶憑證登記作業流程圖



圖表 7-4 Browser Base 客戶憑證登記作業流程圖

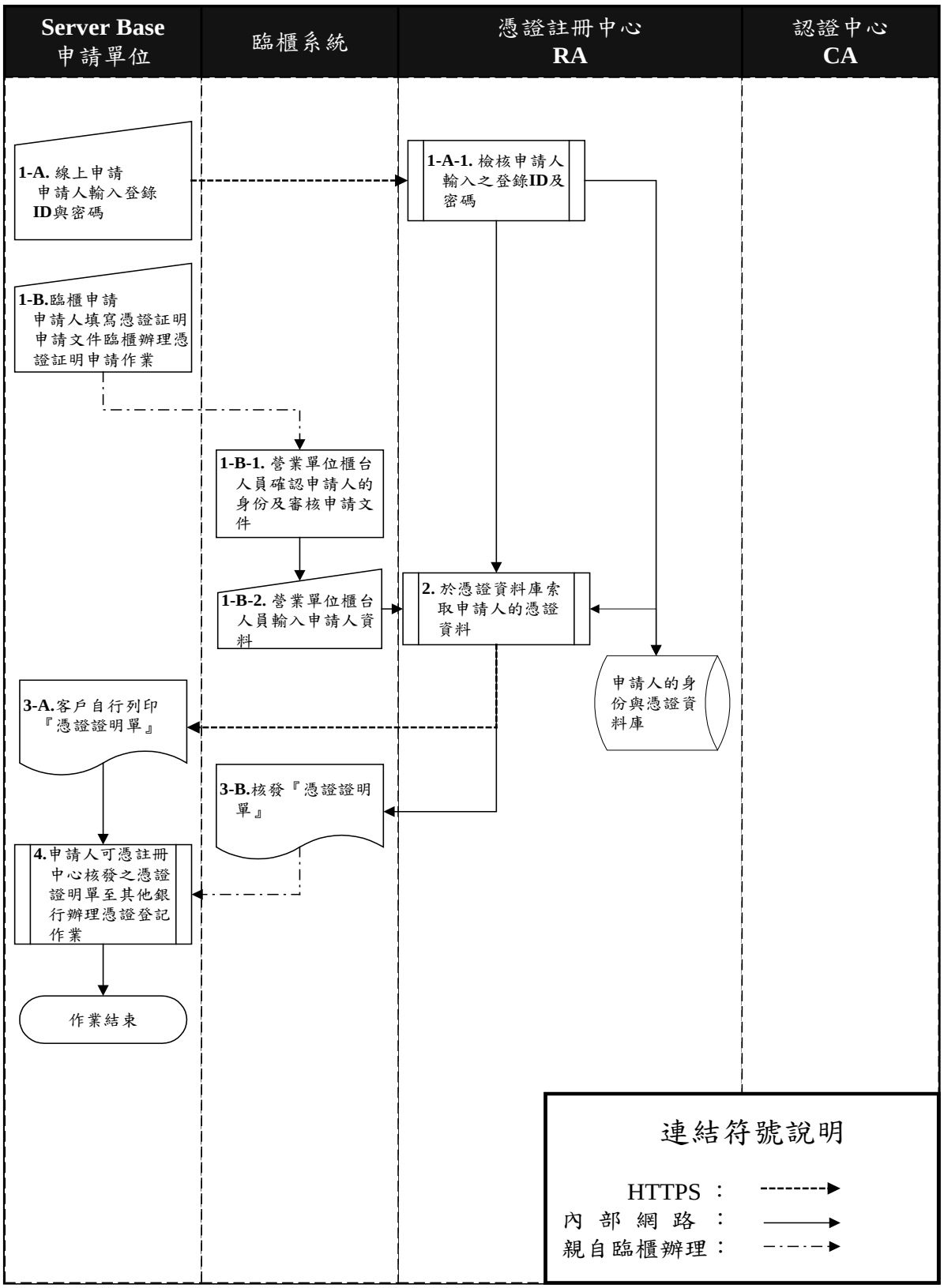
7.2.1.4 Browser Base 客戶憑證登記作業說明

表格 7-4 Browser Base 客戶憑證登記作業說明表

步驟	作業單位	作業內容
1	申請人	●填寫憑證登記申請文件並攜帶身份證明文件於其他參加本作業之金融機構(非原註冊中心所屬之金融機構)臨櫃辦理憑證登記作業 ●申請人應準備之身份證明文件有： ■「憑證證明單」 ■個人為身份證、護照(外國人)等 ■公司為公司執照影本、營利事業登記證影本等 ■無 BAN(在本國經濟部登錄之公司統一編號)之申請單位由金融機構自行維護虛擬統編者，由於憑證證明單上並無戶名，在辦理憑證登記時，為確認申請人與該憑證的關連性，應由原憑證註冊單位以發函方式出具證明，供其他金融機構執行憑證登記作業之依據；至於憑證內之使用者識別資料與 CIF 之關連，則由各金融機構自行處理。
2	臨櫃人員	●檢核身份證明文件確認申請人之身份 ●審核申請人填具之憑證登記文件及核對留存印鑑
3	臨櫃人員	●執行憑證登記交易，輸入申請人相關資料
4	註冊中心	●儲存申請人身份資料與憑證相關資料 ●亦可透過往來 CA 索取跨 RA 與跨 UCA 申請人憑證
5	註冊中心	●接收「憑證」訊息並驗證憑證及上層憑證 ●核對臨櫃登記資料與憑證的一致性及核對憑證格式的正確性。 ●更新憑證資料庫
6	申請人	●接收憑證登記作業之結果

7.2.2 Server Base 客戶憑證登記作業

7.2.2.1 Server Base 客戶憑證證明單申請作業流程圖



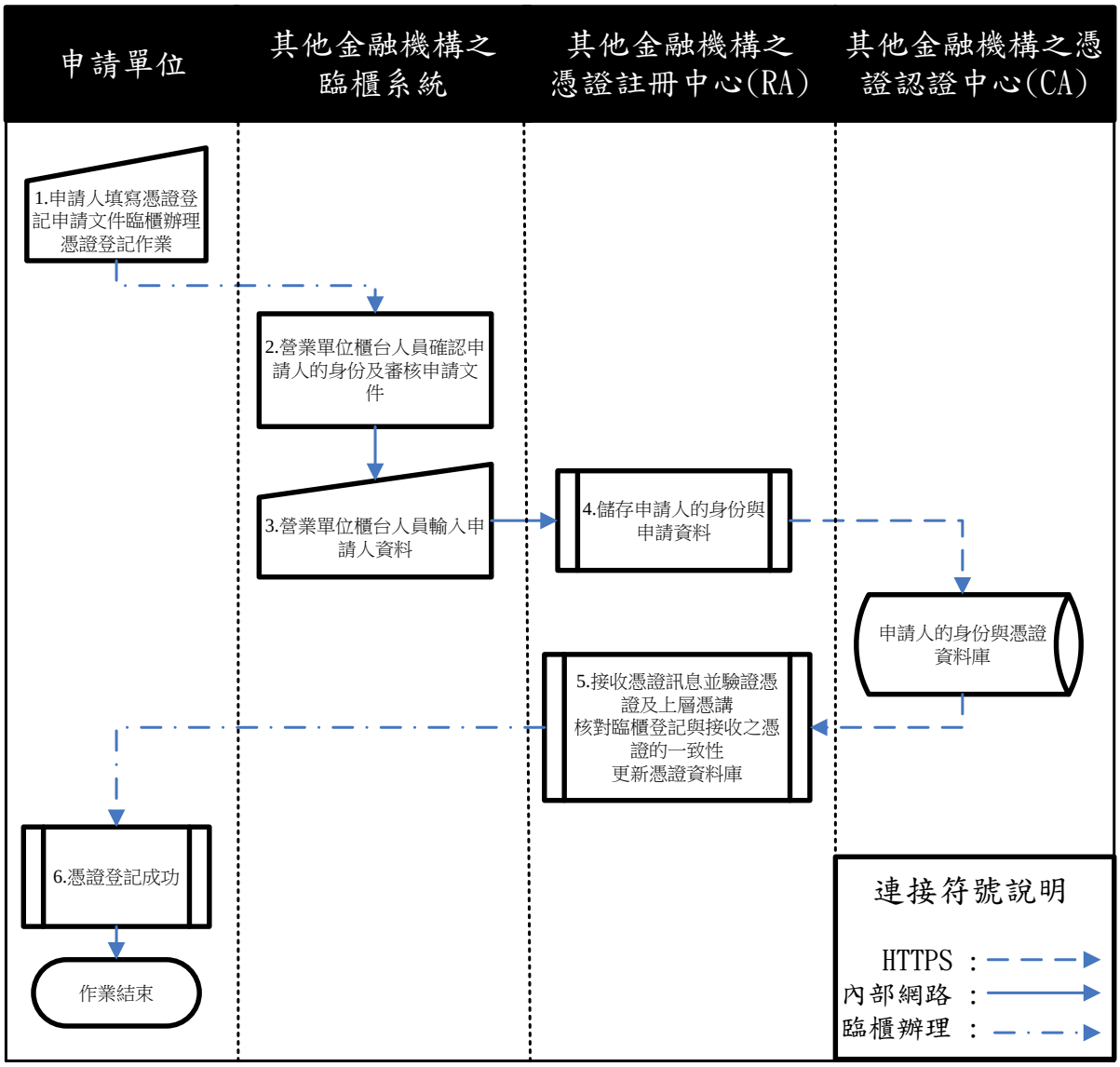
圖表 7-5 Server Base 客戶憑證證明單申請作業流程圖

7.2.2.2 Server Base 客戶憑證證明單申請作業說明

表格 7-5 Server Base 客戶憑證證明單申請作業說明表

步驟	作業單位	作業內容
1-A	申請人	●線上申請 ●輸入登錄 ID、密碼憑以登入憑證註冊應用系統
1-A-1	註冊中心	●檢核申請人輸入之登錄 ID、密碼以確認身份 ●本項作業為申請人之憑證證明單申請作業，為防止申請人憑證之相關資訊外洩，應具備 Session Control 及加密機制，並應拒絕未經授權的存取
1-B	申請人	●臨櫃申請 ●填寫憑證證明申請文件並攜帶身份證明文件於原憑證註冊之金融機構臨櫃辦理憑證證明單申請作業 ●申請人應準備之身份證明文件有： ■個人為身份證、護照(外國人)等 ■公司為公司執照影本、營利事業登記證影本等
1-B-1	臨櫃人員	●檢核身份證明文件確認申請人之身份 ●審核申請人填具之憑證證明單申請文件
1-B-2	臨櫃人員	●執行憑證證明申請交易，輸入申請人相關資料
2	註冊中心	●索取憑證資料庫中申請人之憑證資料
3-A	申請人	●自行列印『憑證證明單』
3-B	臨櫃人員	●核發『憑證證明單』
4	申請人	●可憑註冊中心所核發之憑證證明單至其他參加本作業之金融機構辦理憑證登記作業

7.2.2.3 Server Base 客戶憑證登記作業流程圖



圖表 7-6 Server Base 客戶憑證登記作業流程圖

7.2.2.4 Server Base 客戶憑證登記作業說明

表格 7-6 Server Base 客戶憑證登記作業說明表

步驟	作業單位	作業內容
1	申請人	●填寫憑證登記申請文件並攜帶身份證明文件於其他參加本作業之金融機構(非原註冊中心所屬之金融機構)臨櫃辦理憑證登記作業 ●申請人應準備之身份證明文件有： ■個人為身份證、護照等 ■公司為公司執照影本、營利事業登記證影本等 ■無BAN之申請單位由金融機構自行維護虛擬統編者，由於憑證證明單上並無戶名，在辦理憑證登記時，為確認申請人與該憑證的關連性，應由原憑證註冊單位以發函方式出具證明，供其他金融機構執行憑證登記作業之依據；至於憑證內之使用者識別資料與 CIF 之關連，則由各金融機構自行處理。
2	臨櫃人員	●檢核身份證明文件確認申請人之身份 ●審核申請人填具之憑證登記文件及核對留存印鑑
3	臨櫃人員	●執行憑證登記交易，輸入申請人相關資料
4	註冊中心	●儲存申請人身份資料與憑證相關資料 ●亦可透過往來 CA 索取跨 RA 與跨 UCA 申請人憑證
5	註冊中心	●接收「憑證」訊息並驗證憑證及上層憑證 ●核對臨櫃登記與憑證的一致性及核對憑證格式的正確性 ●更新憑證資料庫
6	申請人	●接收憑證登記作業之結果

7.2.3 憑證證明單

憑證證明單是使用者在憑證登記作業時的輔助資料，以減少登記作業錯誤的發生，上面記載使用者憑證相關資訊，序號欄以十六進位並大寫為表示方式，狀態欄為憑證的最新狀態，可能為“有效”、”|暫禁”或“註銷”三者之一。

範例如下：

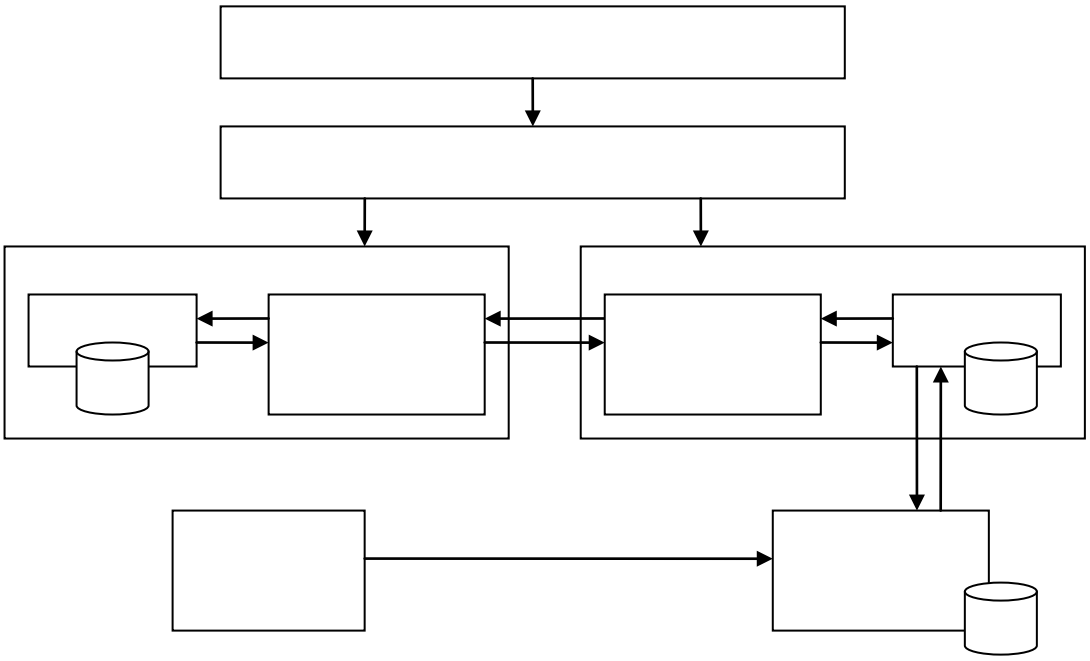
表格 7-7 憑證證明單

列印日期: 年 月 日

XX 認證中心/XX 註冊中心	
憑 證 證 明 單	
序號	3AD4 2213
發 行 者	C = TW O = CyberTrust Corporation OU = User CA CN = Banking
有效起始日	2001 年 4 月 11 日 PM 05:21:22
有效到期日	2002 年 4 月 11 日 PM 05:21:22
主 旨 (使用者識別名稱)	C = TW O = CyberTrust Finance OU = CyberTrust Banking OU = 0040000-BOT OU = FXML CN = A123456789
狀 態	有效

7.2.4 索取登記憑證

受理憑證登記金融機構與登記者持有憑證分屬不同 UCA(兩個 UCA 同屬一個 PCA)的索取登記憑證作業流程如下：



圖表 7-7 跨 CA 索取憑證系統作業流程圖

步驟	作業單位	作業內容
1	其他金融機構之註冊中心(RA)	●儲存申請人身份資料與憑證相關資料 ●亦可透過往來 UCA_A 索取跨 RA 與跨 UCA 之申請人憑證
2	其他金融機構之憑證中心(UCA_A)	●憑證機構 UCA_A 檢查若申請人為其憑證用戶，則自其憑證資料庫取出後傳送回註冊中心 ●憑證機構 UCA_A 檢查若申請人不為其憑證用戶且為同一政策憑證機構(PCA)下，則產生索取憑證 Request 訊息，遞送給另一指定憑證機構 UCA_B。
3	其他金融機構之其他憑證中心(UCA_B)	●憑證機構 UCA_B 檢查若申請人為其憑證用戶，且為 UCA_A 為同一政策憑證機構(PCA)下，則自其憑證資料庫取出後產生索取憑證 Response 訊息傳送回憑證機構 UCA_A。
4	其他金融機構之註冊中心(RA)	●接收索取憑證之結果

7.2.5 驗證登記憑證

非原註冊中心所屬之金融機構受理憑證登記作業時，需核對臨櫃登記與憑證索取所下載之憑證的一致性及核對憑證格式的正確性。

7.3 憑證更新作業

本規範規定憑證於其到期日前一至二個月開始至到期日止為更新狀態，註冊中心應於憑證到期前一至二個月通知憑證之使用者，使用者可於憑證更新狀態期間執行憑證更新作業。

為方便申請人能自動化執行憑證更新作業，本規範訂定線上憑證更新作業程序，申請人可利用憑證註冊應用系統所提供之憑證更新作業於線上完成憑證更新作業。

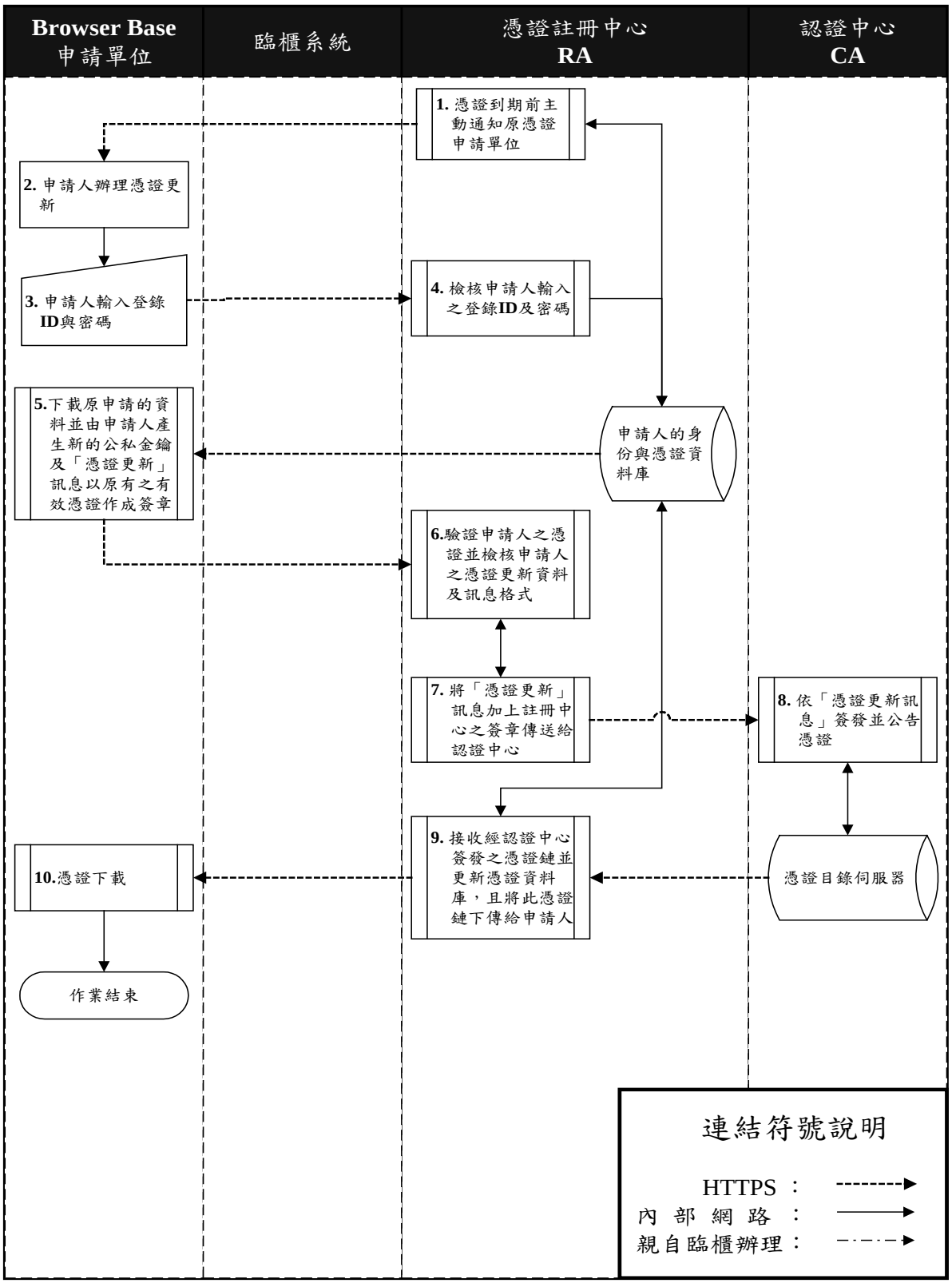
另本規範允許憑證共用，申請人可於原憑證註冊應用系統完成憑證更新作業，取得更新之憑證後，亦可於線上辦理憑證登記更新作業。

本作業僅於憑證更新狀態期間可執行，當憑證已逾該憑證之到期日期時間後，憑證將自動變更為過期狀態，申請人於憑證過期狀態擬再使用憑證則必須重新辦理憑證申請作業。

7.4 憑證更新作業

7.4.1 Browser Base 客戶憑證更新作業

7.4.1.1 Browser Base 客戶憑證更新作業流程圖



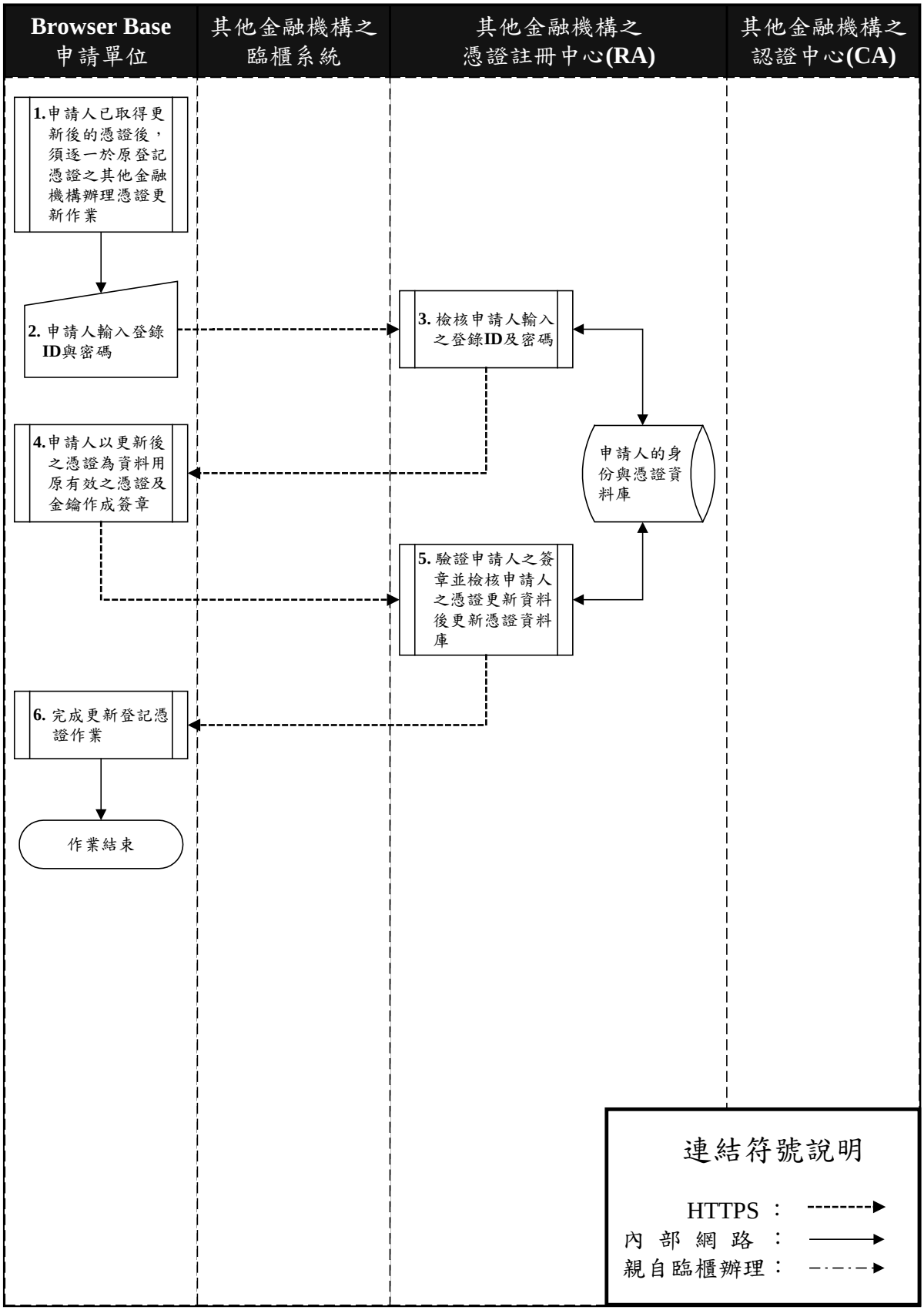
圖表 7-7 Browser Base 客戶憑證更新作業流程圖

7.4.1.2 Browser Base 客戶憑證更新作業說明

表格 7-8 Browser Base 客戶憑證更新作業說明表

步驟	作業單位	作業內容
1	註冊中心	●於憑證到期前一個月主動通知憑證之申請人，告知該憑證之狀態已在更新狀態，並請申請人於憑證到期前辦理憑證更新作業
2	申請人	●於收到註冊中心之憑證更新通知後，於憑證到期前辦理憑證更新作業
3	申請人	●輸入登錄 ID、密碼憑以登入憑證註冊應用系統
4	註冊中心	●檢核申請人輸入之登錄 ID、密碼以確認身份 ●本項作業為申請人之憑證更新作業，為防止申請人憑證之相關資訊外洩，應具備 Session Control 及加密機制，並應拒絕未經授權的存取
5	申請人	●將憑證更新資料下載至使用者端，並確認資料無誤 ●申請人自行產生金鑰對(需設定私密金鑰之密碼，以保護私密金鑰避免遭人誤用) ●產生 PKCS#10 格式之「憑證更新」訊息(格式同「憑證申請」訊息) ●以原金鑰對「憑證更新」訊息作成簽章 ●將「憑證更新」訊息傳送至註冊中心
6	註冊中心	●接收「憑證更新」訊息並驗證申請人之簽章 ●檢核申請人上傳之憑證更新資料及訊息格式
7	註冊中心	●將「憑證更新」訊息加上註冊中心之簽章 ●傳送簽章後之「憑證更新」訊息傳送至認證中心
8	認證中心	●接收「憑證更新」訊息並驗證註冊中心的簽章 ●依「憑證更新」訊息簽發憑證 ●將所簽發之憑證公告於「憑證目錄伺服器」 ●將憑證鏈傳送給註冊中心
9	註冊中心	●接收經認證中心簽發之憑證鏈並儲存於憑證資料庫 ●將憑證鏈下傳給申請人
10	申請人	●連接憑證註冊應用系統後，下載憑證

7.4.1.3 Browser Base 客戶憑證登記之更新作業流程圖



圖表 7-8 Browser Base 客戶憑證登記之更新作業流程圖

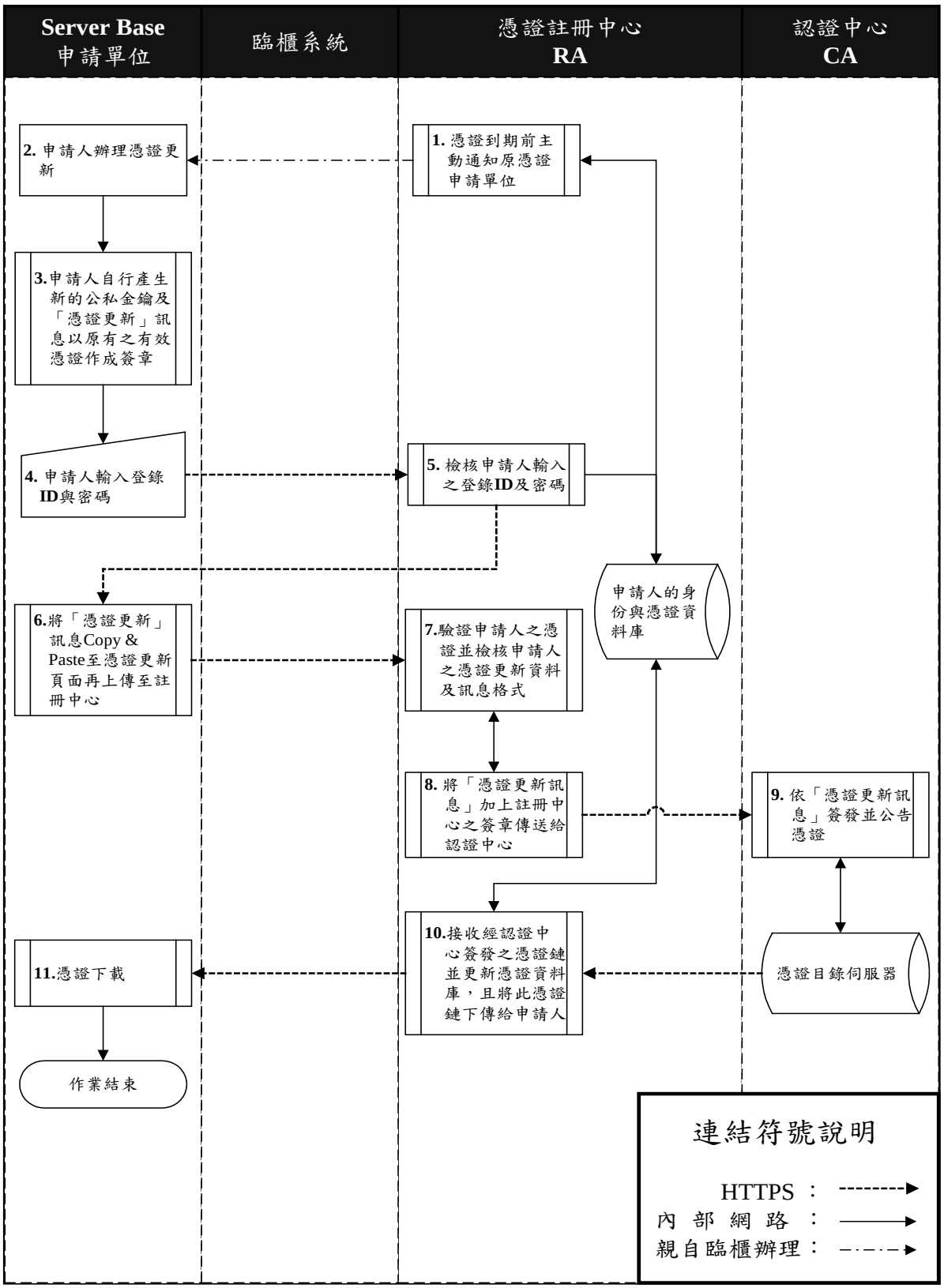
7.4.1.4 Browser Base 客戶憑證登記之更新作業說明

表格 7-9 Browser Base 客戶憑證登記之更新作業說明表

步驟	作業單位	作　　業　　內　　容
1	申 請 人	●完成憑證更新作業並取得新憑證後，須逐一至原憑證登記之憑證註冊應用系統辦理憑證登記更新作業 ✱本項作業須於原憑證到期前完成
2	申 請 人	●輸入登錄 ID、密碼憑以登入憑證註冊應用系統
3	註冊中心	●檢核申請人輸入之登錄 ID、密碼以確認身份 ●本項作業為申請人之憑證登記更新作業，為防止申請人憑證之相關資訊外洩，應具備 Session Control 及加密機制，並應拒絕未經授權的存取
4	申 請 人	●將原憑證登記資料下載至使用者端，並確認資料無誤 ●申請人將更新後之憑證為資料，以原登記之憑證及金鑰作成簽章 ●將「憑證登記更新」訊息傳送至註冊中心
5	註冊中心	●接收「憑證登記更新」訊息並驗證申請人之簽章 ●檢核更新後之憑證內容與原憑證內容的一致性 ●將更新之憑證資料儲存於憑證資料庫中
6	申 請 人	●逐一辦理憑證登記之更新作業

7.4.2 Server Base 客戶憑證更新作業

7.4.2.1 Server Base 客戶憑證更新作業流程圖



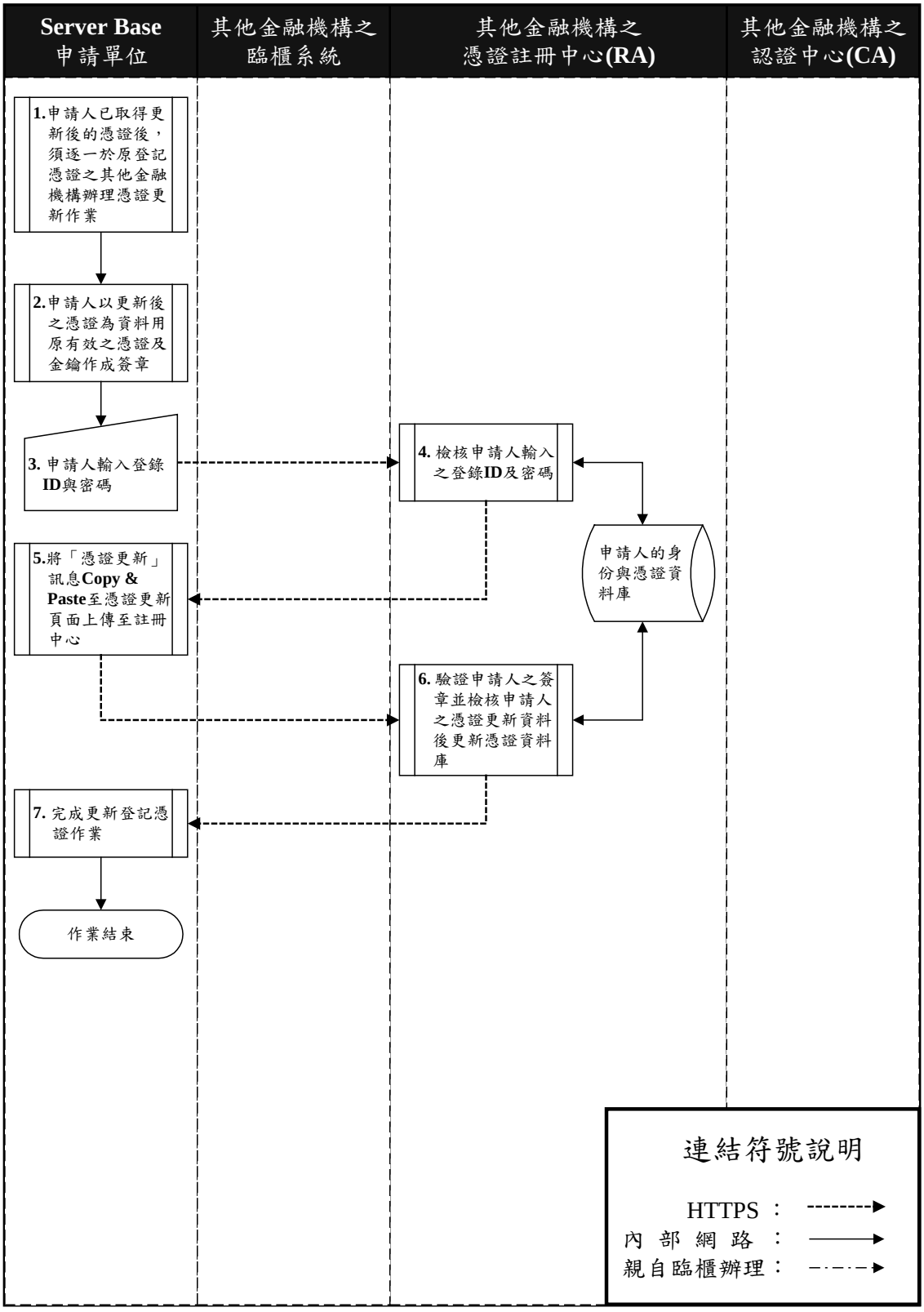
圖表 7-9 Server Base 客戶憑證更新作業流程圖

7.4.2.2 Server Base 客戶憑證更新作業說明

表格 7-10 Server Base 客戶憑證更新作業說明表

步驟	作業單位	作　　業　　內　　容
1	註冊中心	●於憑證到期前一個月主動通知憑證之申請人，告知該憑證之狀態已在更新狀態，並請申請人於憑證到期前辦理憑證更新作業
2	申 請 人	●於收到註冊中心之憑證更新通知後，於憑證到期前辦理憑證更新作業
3	申 請 人	●申請人自行產生金鑰對(需設定私密金鑰之密碼，以保護私密金鑰避免遭人誤用) ●產生 Base64 Encode 的 PKCS#10 格式之「憑證更新」訊息 ●以原金鑰對「憑證更新」訊息作成簽章
4	申 請 人	●輸入登錄 ID、密碼憑以登入憑證註冊應用系統
5	註冊中心	●檢核申請人輸入之登錄 ID、密碼以確認身份 ●本項作業為申請人之憑證登記作業，為防止申請人憑證之相關資訊外洩，應具備 Session Control 及加密機制，並應拒絕未經授權的存取
6	申 請 人	●將憑證更新資料下載至使用者端，並確認資料無誤 ●將「憑證更新」訊息傳送至註冊中心
7	註冊中心	●接收「憑證更新」訊息並驗證申請人之簽章 ●檢核申請人上傳之憑證更新資料及訊息格式
8	註冊中心	●將「憑證更新」訊息加上註冊中心之簽章 ●傳送簽章後之「憑證更新」訊息傳送至認證中心
9	認證中心	●接收「憑證更新」訊息並驗證註冊中心的簽章 ●依「憑證更新」訊息簽發憑證 ●將所簽發之憑證公告於「憑證目錄伺服器」 ●將憑證鏈傳送給註冊中心
10	註冊中心	●接收經認證中心簽發之憑證鏈並儲存於憑證資料庫 ●將憑證鏈下傳給申請人
11	申 請 人	●連接憑證註冊應用系統後，下載憑證

7.4.2.3 Server Base 客戶憑證登記之更新作業流程圖



圖表 7-10 Server Base 客戶憑證登記之更新作業流程圖

7.4.2.4 Server Base 客戶憑證登記之更新作業說明

表格 7-11 Server Base 客戶憑證登記之更新作業說明表

步驟	作業單位	作　　業　　內　　容
1	申 請 人	●完成憑證更新作業並取得新憑證後，須逐一至原憑證登記之憑證註冊應用系統辦理憑證登記更新作業 ✱本項作業須於原憑證到期前完成
2	申 請 人	●申請人以更新後之憑證為資料，以原金鑰作成簽章 ●產生 Base64 Encode 的「憑證更新」訊息
2	申 請 人	●輸入登錄 ID、密碼憑以登入憑證註冊應用系統
3	註冊中心	●檢核申請人輸入之登錄 ID、密碼以確認身份 ●本項作業為申請人之憑證登記更新作業，為防止申請人憑證之相關資訊外洩，應具備 Session Control 及加密機制，並應拒絕未經授權的存取
4	申 請 人	●將原憑證登記資料下載至使用者端，並確認資料無誤 ●將「憑證登記更新」訊息 Copy & Paste 憑證更新頁面後傳送至註冊中心
5	註冊中心	●接收「憑證登記更新」訊息並驗證申請人之簽章 ●檢核更新後之憑證內容與原憑證內容的一致性 ●將更新之憑證資料儲存於憑證資料庫中
6	申 請 人	●逐一辦理憑證登記之更新作業

7.5 憑證註銷作業

當使用者確定憑證已遺失或已遭人盜用等情況時，應立即向原核發憑證之註冊中心辦理憑證註銷作業，將憑證狀態變更為註銷狀態，而後無法再利用該憑證執行任何交易。

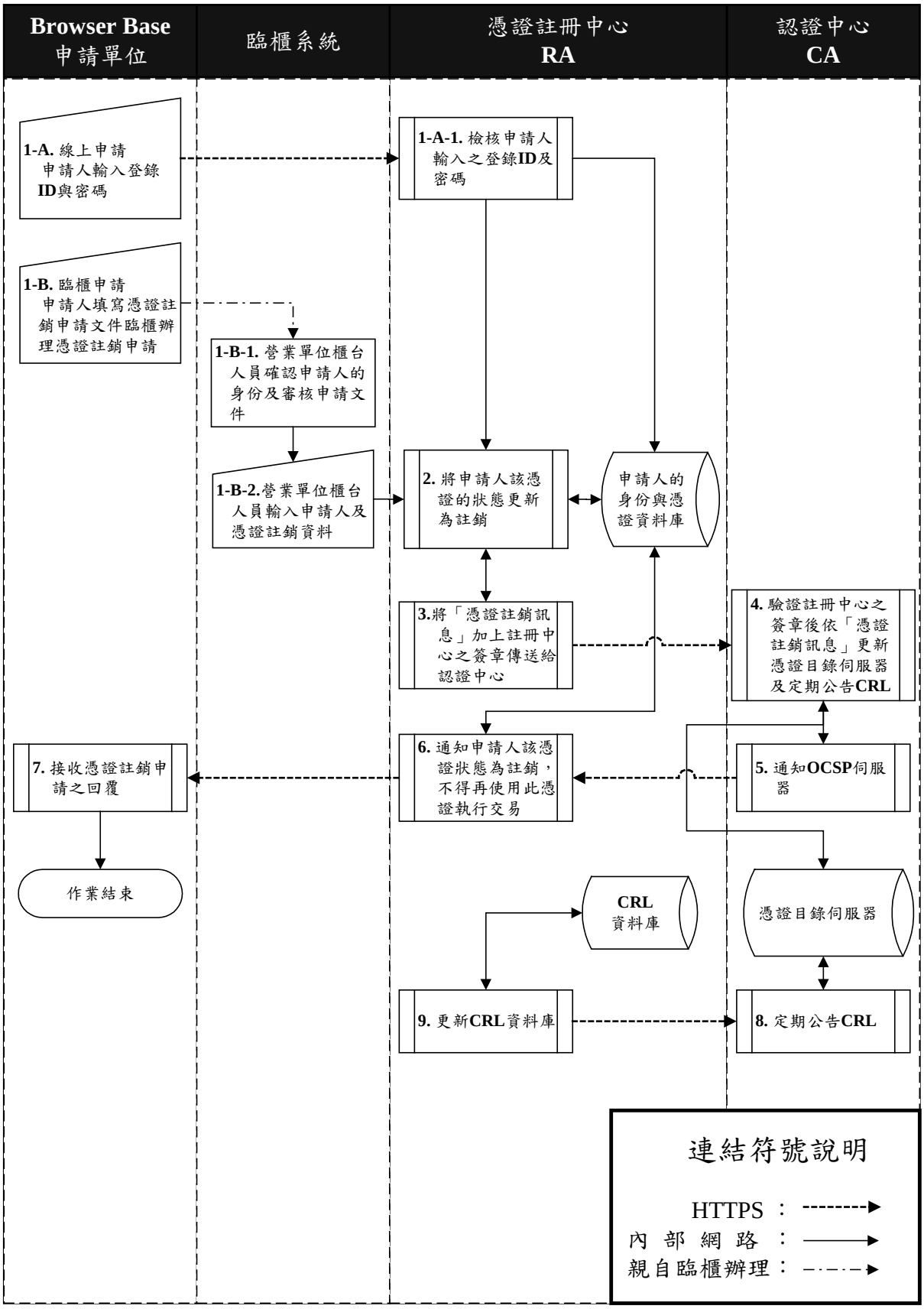
為方便申請人能立即辦理憑證註銷作業，本規範特訂定線上憑證註銷作業程序，申請人除可於臨櫃辦理憑證註銷作業外，亦可利用線上憑證註銷作業完成註銷憑證之目的。

本作業可於憑證之有效狀態、更新狀態或暫禁狀態下隨時執行；僅於憑證狀態為過期狀態時不得辦理憑證註銷作業。當憑證狀態為註銷狀態仍擬使用憑證時，須重新辦理憑證申請作業。

本規範採線上憑證狀態查詢(OCSP)機制，因此申請人僅須於原憑證註冊應用系統辦理憑證註銷作業；若該憑證曾於其他金融機構辦理憑證登記作業時，亦不須逐一辦理憑證註銷作業。

7.5.1 Browser Base 客戶憑證註銷作業

7.5.1.1 Browser Base 客戶憑證註銷作業流程圖



圖表 7-11 Browser Base 客戶憑證註銷作業流程圖

7.5.1.2 Browser Base 客戶憑證註銷作業說明

表格 7-12 Browser Base 客戶憑證註銷作業說明表

步驟	作業單位	作業內容
1-A	申請人	●線上辦理 ●輸入登錄 ID、密碼憑以登入憑證註冊應用系統
1-A-1	註冊中心	●檢核申請人輸入之登錄 ID、密碼以確認身份 ●本項作業為申請人之憑證註銷作業，為防止申請人憑證之相關資訊外洩，應具備 Session Control 及加密機制，並應拒絕未經授權的存取
1-B	申請人	●臨櫃辦理 ●填寫憑證註銷申請文件並攜帶身份證明文件於原憑證註冊之金融機構臨櫃辦理憑證登記作業 ●申請人應準備之身份證明文件有： ■個人為身份證、護照(外國人)等 ■公司為公司執照影本、營利事業登記證影本等
1-B-1	臨櫃人員	●檢核身份證明文件確認申請人之身份 ●審核申請人填具之憑證註銷文件及核對留存印鑑
1-B-2	臨櫃人員	●執行憑證註銷交易，輸入申請人相關資料，並於交易完成後將結果回覆申請人 ■當無法透過臨櫃系統完成註銷作業時，應立即以人工方式聯絡認證中心完成憑證註銷作業並將結果回覆申請人
2	註冊中心	●將申請人該憑證的狀態更新為註銷狀態
3	註冊中心	●將「憑證註銷」訊息加上註冊中心之簽章 ●傳送簽章後之「憑證註銷」訊息傳送至認證中心 ■當無法透過「憑證註銷」訊息完成註銷作業時，應立即改以人工方式聯絡通知認證中心完成憑證註銷作業並將結果回覆申請人
4	認證中心	●接收「憑證註銷」訊息並驗證註冊中心的簽章 ●依「憑證註銷」訊息公告於「憑證目錄伺服器」
5	認證中心	●依「憑證註銷」訊息通知 OCSP 伺服器
6	註冊中心	●接收「憑證註銷」訊息之處理結果更新憑證資料庫之狀態 ●通知申請人該憑證狀態為註銷，不得再使用此憑證執行交易
7	申請人	●接收憑證註銷申請之回覆訊息
8	認證中心	●定期公告『憑證註銷清單(CRL)』

步驟	作業單位	作　　業　　內　　容
9	註冊中心	●定期索取公告之『憑證註銷清單(CRL)』 ●更新憑證註銷清單(CRL)資料庫

7.5.2 Server Base 客戶憑證註銷作業說明

Server Base 客戶憑證註銷作業與 Browser Base 客戶憑證註銷作業相同，作業流程圖及說明請參考7.5.1.1 Browser Base 客戶憑證註銷作業流程圖及7.5.1.2 Browser Base 客戶憑證註銷作業說明。

7.6 憑證暫禁作業

當使用者懷疑憑證遺失或遭人盜用等情況時，應立即向原核發憑證之註冊中心辦理憑證暫禁作業，將憑證狀態變更為暫禁狀態，此時無法使用該憑證作為執行交易之工具。

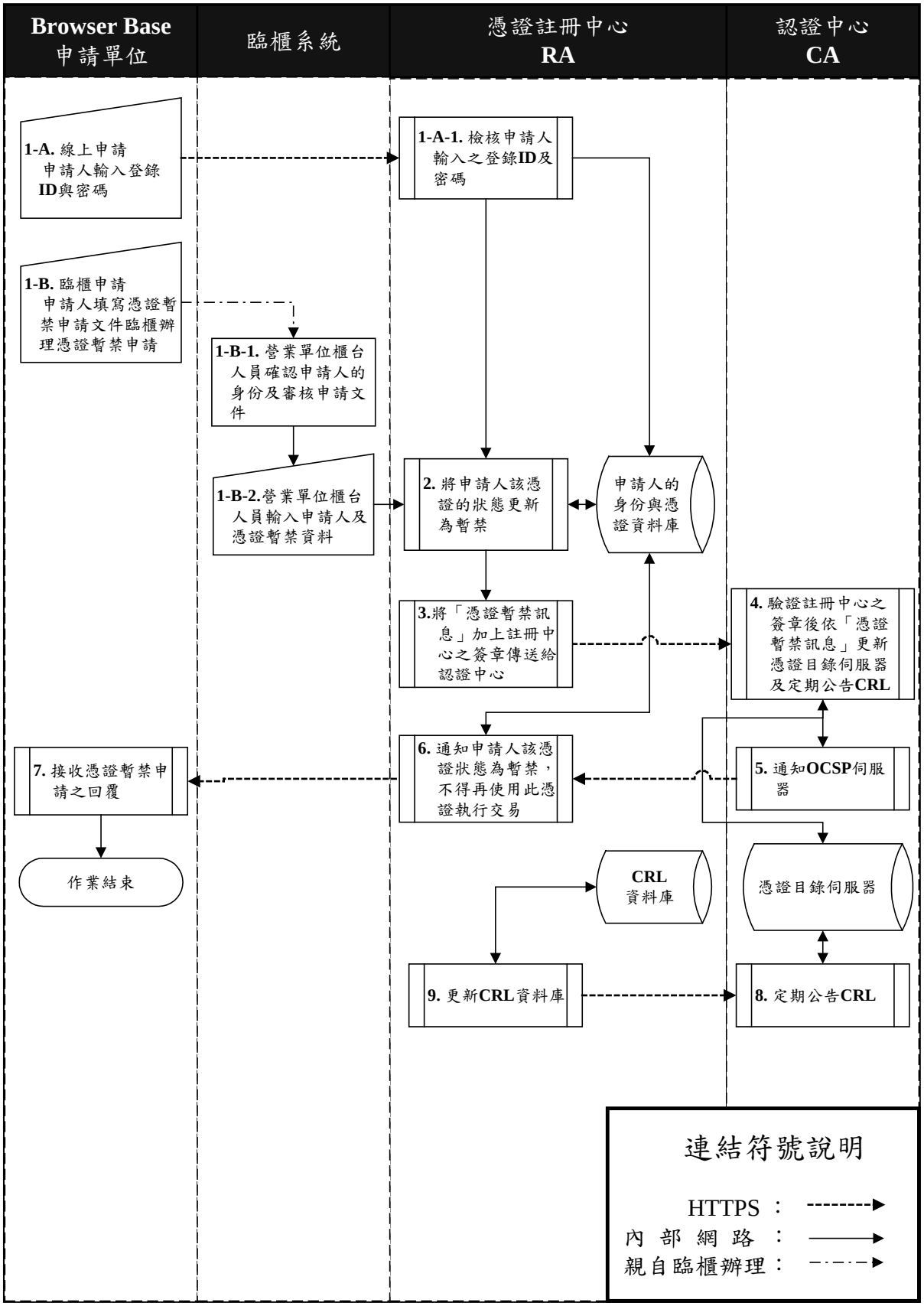
為方便申請人能立即辦理憑證暫禁作業，本規範訂定線上憑證暫禁作業程序，申請人除可於臨櫃辦理憑證暫禁作業外，亦可利用線上憑證暫禁作業完成暫禁憑證之目的。

本作業可於憑證之有效狀態、更新狀態下隨時執行。本項作業與憑證註銷作業的差異為憑證於暫禁狀態時仍可利用憑證解禁作業恢復憑證的狀態，但憑證於註銷狀態下則僅能重新辦理憑證申請作業取得新的憑證。

憑證應用服務採線上憑證狀態查詢(OCSP)機制者，因此申請人僅須於原憑證註冊應用系統辦理憑證暫禁作業；若該憑證曾於其他金融機構辦理憑證登記作業時，亦不須逐一辦理憑證暫禁作業。

7.6.1 Browser Base 客戶憑證暫禁作業

7.6.1.1 Browser Base 客戶憑證暫禁作業流程圖



圖表 7-12 Browser Base 客戶憑證暫禁作業流程圖

7.6.1.2 Browser Base 客戶憑證暫禁作業說明

表格 7-13 Browser Base 客戶憑證暫禁作業說明表

步驟	作業單位	作業內容
1-A	申請人	●線上辦理 ●輸入登錄 ID、密碼憑以登入憑證註冊應用系統
1-A-1	註冊中心	●檢核申請人輸入之登錄 ID、密碼以確認身份 ●本項作業為申請人之憑證暫禁作業，為防止申請人憑證之相關資訊外洩，應具備 Session Control 及加密機制，並應拒絕未經授權的存取
1-B	申請人	●臨櫃辦理 ●填寫憑證暫禁申請文件並攜帶身份證明文件於原憑證註冊之金融機構臨櫃辦理憑證暫禁作業 ●申請人應準備之身份證明文件有： ■個人為身份證、護照(外國人)等 ■公司為公司執照影本、營利事業登記證影本等
1-B-1	臨櫃人員	●檢核身份證明文件，確認申請人之身份 ●審核申請人填具之憑證暫禁文件及核對留存印鑑
1-B-2	臨櫃人員	●執行憑證暫禁交易，輸入申請人相關資料，並於交易完成後將結果回覆申請人 ■當無法透過臨櫃系統完成暫禁作業時，應立即以人工方式聯絡認證中心完成憑證暫禁作業並將結果回覆申請人
2	註冊中心	●將申請人該憑證的狀態更新為暫禁狀態
3	註冊中心	●組成「憑證暫禁」訊息加上註冊中心之簽章 ●傳送簽章後之「憑證暫禁」訊息傳送至認證中心 ■當無法透過「憑證暫禁」訊息完成暫禁作業時，應立即改以人工方式聯絡通知認證中心完成憑證暫禁作業並將結果回覆申請人
4	認證中心	●接收「憑證暫禁」訊息並驗證註冊中心的簽章 ●依「憑證暫禁」訊息公告於「憑證目錄伺服器」
5	認證中心	●依「憑證暫禁」訊息通知 OCSP 伺服器
6	註冊中心	●接收「憑證暫禁」訊息之處理結果更新憑證資料庫之狀態 ●通知申請人該憑證狀態為暫禁，於憑證解禁前不得再使用此憑證執行交易
7	申請人	●接收憑證暫禁申請之回覆訊息
8	認證中心	●定期公告『憑證註銷清單(CRL)』

步驟	作業單位	作　　業　　內　　容
9	註冊中心	●定期索取公告之『憑證註銷清單(CRL)』 ●更新憑證註銷清單(CRL)資料庫

7.6.2 Server Base 客戶憑證暫禁作業說明

Server Base 客戶憑證暫禁作業與 Browser Base 客戶憑證暫禁作業相同，作業流程圖及說明請參考7.6.1.1 Browser Base 客戶憑證暫禁作業流程圖及7.6.1.2 Browser Base 客戶憑證暫禁作業說明。

7.7 憑證解禁作業

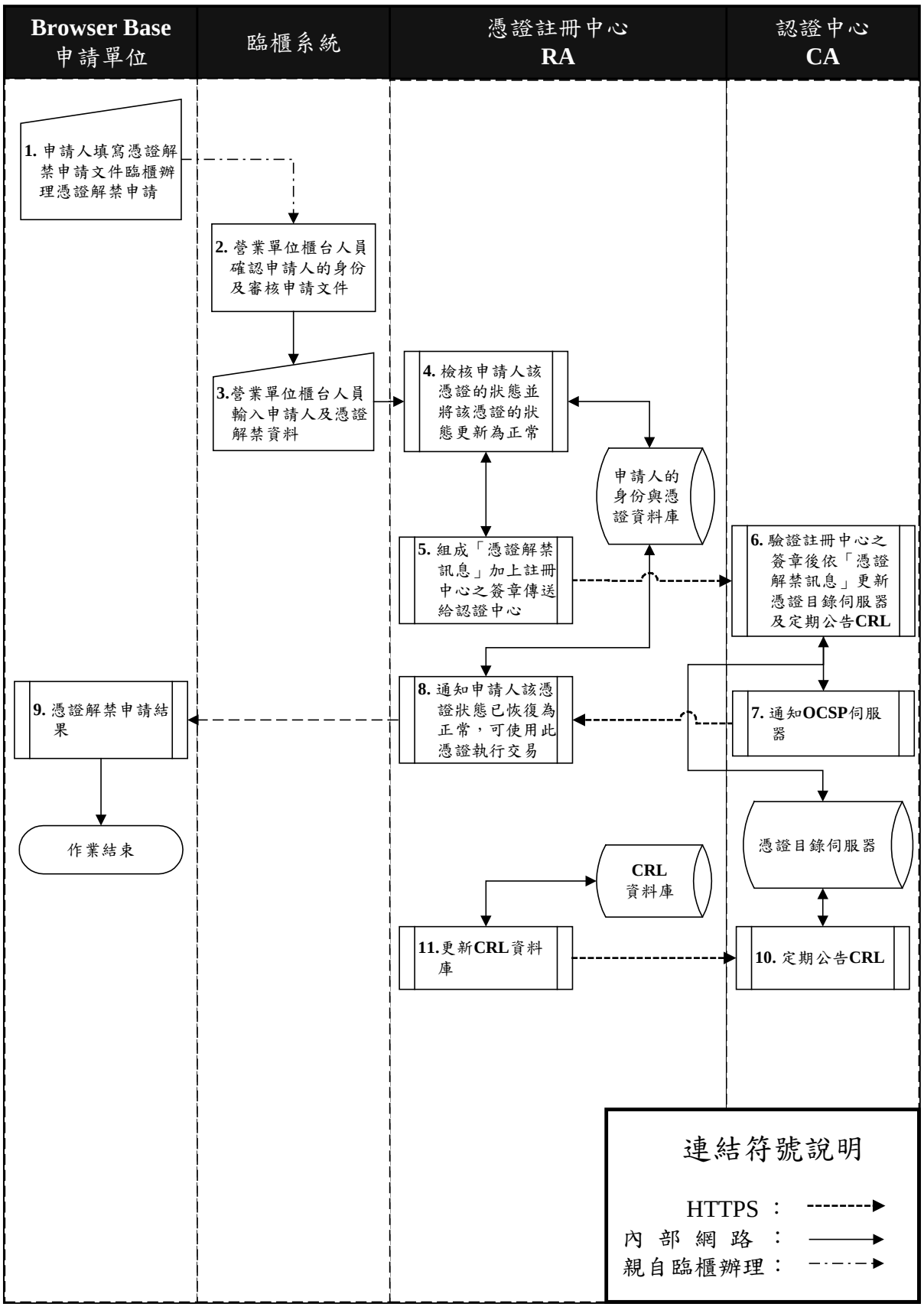
使用者懷疑憑證遺失或遭人盜用等情況時，使用者應立即向原核發憑證之註冊中心辦理憑證暫禁作業，將憑證狀態變更為暫禁狀態。

當上述不利憑證之因素消失且使用者仍希望使用該憑證執行交易時，使用者可填具憑證解禁申請文件及攜帶身份證明文件向原核發憑證之註冊中心申請憑證解禁。

為確認申請人之身份，憑證解禁作業一律必須臨櫃申請。當憑證解禁作業完成後，依憑證到期日期時間的不同，憑證狀態將由暫禁狀態變更為有效狀態或更新狀態。

7.7.1 Browser Base 客戶憑證解禁作業

7.7.1.1 Browser Base 客戶憑證解禁作業流程圖



圖表 7-13 Browser Base 客戶憑證解禁作業流程圖

7.7.1.2 Browser Base 客戶憑證解禁作業說明

表格 7-14 Browser Base 客戶憑證解禁作業說明表

步驟	作業單位	作業內容
1	申請人	●填寫憑證解禁申請文件並攜帶身份證明文件於原憑證註冊之金融機構臨櫃辦理憑證解禁作業 ●申請人應準備之身份證明文件有： ■個人為身份證、護照(外國人)等 ■公司為公司執照影本、營利事業登記證影本等
2	臨櫃人員	●檢核身份證明文件確認申請人之身份 ●審核申請人填具之憑證解禁申請文件及核對留存印鑑
3	臨櫃人員	●執行憑證解禁交易，輸入申請人及憑證解禁相關資料，並於交易完成後將結果回覆申請人
4	註冊中心	●檢核該憑證的狀態及憑證解禁相關資料
5	註冊中心	●組成「憑證解禁」訊息加上註冊中心之簽章 ●傳送簽章後之「憑證解禁」訊息至認證中心
6	認證中心	●接收「憑證解禁」訊息並驗證註冊中心的簽章 ●依「憑證解禁」訊息公告於「憑證目錄伺服器」
7	認證中心	●依「憑證解禁」訊息通知「OCSP 伺服器」 ●傳送「憑證解禁」訊息處理結果給註冊中心
8	註冊中心	●接收「憑證解禁」訊息之處理結果更新憑證資料庫之狀態 ●通知申請人該憑證狀態已由暫禁狀態變更為有效狀態，可使用此憑證執行交易
9	申請人	●接收憑證解禁申請之回覆訊息
10	認證中心	●定期公告『憑證註銷清單(CRL)』
11	註冊中心	●定期索取公告之『憑證註銷清單(CRL)』 ●更新憑證註銷清單(CRL)資料庫

7.7.2 Server Base 客戶憑證解禁作業

Server Base 客戶憑證解禁作業與 Browser Base 客戶憑證解禁作業相同，作業流程圖及說明請參考7.7.1.1 Browser Base 客戶憑證解禁作業流程圖及7.7.1.2 Browser Base 客戶憑證解禁作業說明。

7.8 存證管理作業程序

存證管理作業主要是防止網際網路交易的任一方否認其所做過的事，包括送出文件、接收文件、存取資料等，此特性又可稱為「不可否認性」。

7.8.1 存證

任何交易皆涉及兩方，不論是使用者端和伺服器，還是使用者和金融機構端。為達到雙方不可否認之目的，伺服器和金融機構端必須要有存證功能，且需提供使用者端存證功能供使用者選擇。

7.8.2 交易存證資料產生

在網際網路交易過程中，交易雙方之應用程式，為達到雙方不可否認之目的，均應各自產生交易存證資料。

7.8.3 交易存證資料之驗證

為確認交易存證資料之正確性，接受方必須加以驗證，此步驟可與受信賴之公正第三者合作進行。

7.8.4 糾紛之處理

當交易糾紛發生時，不論由交易雙方儲存的交易存證資料，均應重新被檢視並由交易雙方事前約定之公證者處理。

8. 其他相關作業說明

8.1 憑證各狀態查詢作業

認證中心保留與所有註冊中心之間的憑證作業記錄，以供註冊中心查詢使用，此憑證作業記錄稱為憑證區。

憑證區只提供各 UCA 之註冊中心 Lightweight Directory Access Protocol (LDAP) [RFC 2251]存取介面和 Hypertext Transfer Protocol(HTTP)存取介面以下載或查詢此註冊中心所經手憑證之完整資料。

憑證區亦只提供註冊中心 Hypertext Transfer Protocol(HTTP)存取介面以下載或查詢其他註冊中心所經手憑證之基本資料。

憑證存放於目錄伺服器位置與 CA 憑證的識別名稱(Subject)或是使用者憑證的識別名稱(Subject)相同，以 LDAP 存取 CA 的 CRL 時即可以至 CA 憑證識別名稱處下載 CRL，以 LDAP 存取使用者憑證時則可依使用者憑證識別名稱至目錄伺服器下載憑證。

憑證相關資訊於目錄伺服器內置放的屬性名稱對照表依[RFC 2256]規範如下：

憑證資訊	屬性名稱
CA 憑證	cACertificate;binary
憑證註銷清單	certificateRevocationList;binary
CA 註銷清單	authorityRevocationList;binary
使用者憑證	userCertificate;binary

8.2 金融機構所使用之憑證申請事項

金融機構在擔任註冊中心所需要的RA憑證，以及本身在處理客戶交易時所需使用之使用者憑證，應直接透過認證中心所提供之註冊中心機制向認證中心申請。受理客戶憑證註冊或資料異動時，其臨櫃作業應增加額外具「兩項(含)以上技術」之安全設計或經由另一位人員審核。

金融機構向認證中心申請憑證的作業與 Server Base 使用者申請憑證的作業相同，請參考7.1章節，其餘作業如憑證更新、註銷等亦相同。

上述「兩項(含)以上技術」之安全設計，係指應具有下列兩項(含)以上技術：

- 所知悉的資訊(如設備密碼、登入密碼等)。
- 所持有的設備(如密碼產生器、密碼卡、晶片卡、電腦、手機、憑證載具等)。
- 所擁有的生物特徵(如指紋、臉部、虹膜、聲音、掌紋、靜脈等)。

8.3 憑證（金鑰）儲存媒體保護機制

應用於高風險交易時，憑證金鑰應儲存於符合 Common Criteria EAL 4+(至少包含增項 AVA_VLA.4 或 AVA_VAN.5)或 ITSEC level E4 或 FIPS 140-1 Level 2 或其他相同安全強度之認證等晶片硬體內，以防止該私鑰被匯出或複製，且該晶片硬體不得常駐於產生交易指示之設備，確保交易安全。

為確保整體作業安全等級之一致性，設備代理行存取登記憑證時，需核對該憑證(金鑰)儲存媒體須使用經本會審核通過之中介軟體所支援的憑證載具。

9. 安控系統軟體

9.1 使用者端安控系統

使用者端軟體以 Thin Client 理念設計，以瀏覽器為使用者界面，而安控系統使用到的硬體裝置相關軟體需事先安裝外，金鑰產生模組與交易簽章模組可於使用時再由網路下載自動安裝，Thin Client 設計主要在降低使用者自己動手安裝的機會和減少安裝上碰到的困擾，進而增加客戶的使用意願，而在使用者端軟體需要改版更新時，將可由網路下載自動安裝改版，以持續維繫客戶之使用信心。接受他行憑證並應用於跨網使用時必須使用經本會審核通過之中介軟體所支援的憑證載具。

以下為一 Thin Client 的範例說明，僅供參考。

如使用者使用的是以硬碟為金鑰儲存媒體的話，則使用者端不必先行安裝軟體，如使用者使用的是以 Smart Card 為金鑰儲存媒體的話，使用者端需事先安裝硬體裝置相關軟體，而所需之安控軟體(含憑證申請、下載及交易之安控功能)是利用 PKCS#11 或 Microsoft Cryptographic API(CAPI)開發 Active X 元件並置放於金融機構端 Web Server，客戶於第一次與交易系統連線時，Active X 元件將自動下載並安裝於使用者的電腦系統，之後，使用者與金融機構連線時，電腦系統則會自動檢查 Active X 元件版本，如版本有所異動時，才會再重新下載 Active X 元件並安裝。

9.2 金融機構端安控系統

金融機構 Server 端可依金融機構環境提供不同安控元件，供金融機構與應用系統整合，如金融機構使用 NT 環境，則可提供 CAPI 版安控軟體，如金融機構使用 UNIX 平台，則需搭配該平台安控軟體。

為考量金融機構高安全度之需求，金融機構應使用 Hardware Secure Module(HSM)為金鑰儲存媒體，該設備應符合 Common Criteria EAL 4+(至少包含增項 AVA_VLA.4 或 AVA_VAN.5)或 ITSEC level E4 或 FIPS 140-1 Level 2 或其他相同安全強度之認證。

●

10.附錄

個別金融機構視其內部考量斟酌支援載具共通。為達載具共通，金融機構交易系統與其載具標準須符合本附錄各項規格以確保介面標準及載具一致性，並採用經銀行公會審核通過之載具，以確保安全等級一致性，使該金融機構用戶持有之憑證載具可至支援載具共通之其他金融機構交易系統使用。

10.1 附件一 金融 XML 憑證載具 API 介面應用規範

10.2 附件二 金融 XML 憑證載具規格書

10.3 附件三 金融 XML 憑證載具安全規範

10.4 參考文獻

1. [FIPS 140-1] Federal Information Processing Standards Publication (FIPS PUB) 140-1, Security Requirements Requirements For Cryptographic Modules, 11 January 1994.

2. [IETF PKIX roadmap] Internet X.509 Public Key Infrastruecture, internet draft, Nov. 2000 by IETF PKIX working group

3. [X.509] ITU-T Recommendation X.509 (1997 E): Information Technology - Open Systems Interconnection – The Directory: Authentication Framework, June 1997.

4. [RFC 2251] M. Wahl, T. Howes, S. Kille,” Lightweight Directory Access Protocol (v3)”, RFC 2251, December 1997.

5. [RFC 2256] M. Wahl,” A Summary of the X.500(96) User Schema for use with LDAPv3”, RFC 2256, December 1997.

6. [RFC 2314] B. Kaliski,” PKCS #10: Certification Request Syntax version 5”, RFC 2314, March 1998.

7. [RFC 2315] B. Kaliski,” PKCS #7: Cryptographic Message Syntax”, RFC 2315, March 1998.

8. [RFC 2459] R. HOUSLEY, W. FORD, W. POLK, D. SOLO., "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", RFC 2459, January 1999.

9. [RFC 2560] M. Myers, R. Ankney, A. Malpani, A. Malpani, C. Adams,” X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP”, RFC 2560, June 1999.

10. 「財稅中心-所得人基本資料維護」http://www.itax.com.tw/imx/imxhelp/PERSON.htm

11. 銀行公會，金融機構辦理電子銀行業務安全控管作業基準，2000 年八月

12. 銀行公會，金融 XML 系統建置指引，2001 年六月。