金融公開金鑰基礎建設憑證政策

(Certificate Policy for the Financial Public Key Infrastructure)

第 2.0 版

中華民國銀行商業同業公會全國聯合會

中華民國 108 年 9 月 12 日

目錄

1. 簡介

金融公開金鑰基礎建設（Financial Public Key Infrastructure，FPKI，以下簡稱本基礎建設）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。本基礎建設為階層式架構，包括金融體系單一的最高層憑證機構（Financial Root Certificate Authority，FRCA）、政策憑證機構（Financial Policy Certificate Authority，FPCA）用戶憑證機構（Financial User Certificate Authority，FUCA）（以下合稱憑證機構）及註冊中心（Registration Authority，RA）等。加入本基礎建設的憑證機構必須符合用戶憑證機構（UCA）申請辦法之資格，其簽發之憑證使得應用於各項金融業務，以提供更便捷的金融服務，提昇交易效率，促進電子商務應用發展。

為確保各憑證機構之營運及服務品質，由銀行公會（以下簡稱本會）設立憑證政策管理委員會（Policy Management Authority，PMA，以下簡稱政策管理委員會）協助進行本基礎建設之管理工作，政策管理委員會的工作任務如 1.5.1 節。

本憑證政策（Certificate Policy，CP）係依據電子簽章法規定並參酌國際相關標準及政策文件訂定之，提供本基礎建設各憑證機構訂定憑證實務作業基準（Certification Practices Statement，CPS）之遵循。

1.1 概述

X.509 標準對於憑證政策的定義為，「針對具有共同安全需求之特定社群或應用所訂定之憑證適用性規範」。規範訂定後方可確保憑證適用之對象及應用等，金融公開金鑰基礎建設之所以需要定義憑證政策，主要便是在建立一個金融領域上的憑證應用的安全標準，做為各憑證機構遵循之標的。

1.2 文件名稱與識別

文件名稱: 金融公開金鑰基礎建設憑證政策

在憑證中是以憑證政策物件識別碼（Object Identifier, OID）註明憑證政策，物件識別碼是一種以字母或數字組成之唯一識別碼，該識別碼必須依國際標準組織所訂定之註冊標準加以訂定，並可用以識別唯一與之對應之憑證政策；憑證政策修訂時，其物件識別碼不必然隨之變更。

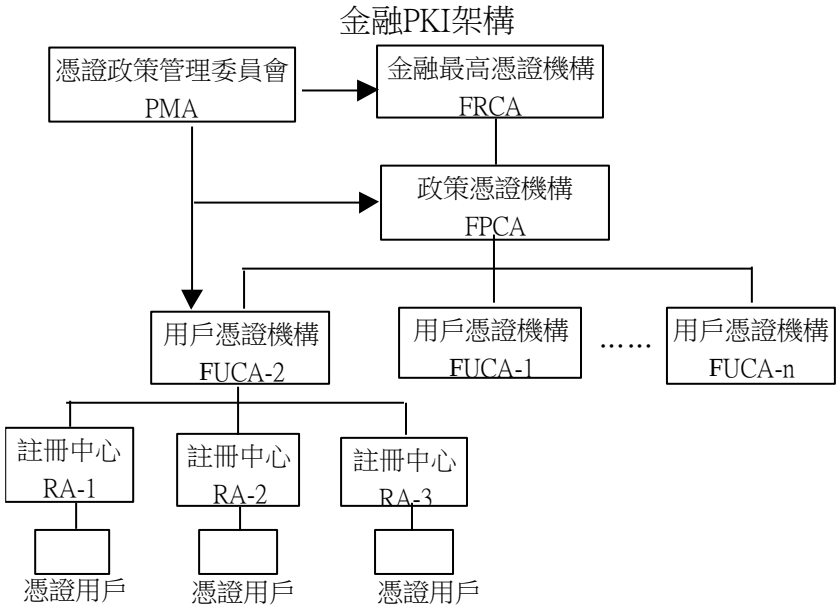
憑證機構可直接引用已註冊的憑證政策物件識別碼，信賴憑證者可透過憑證政策物件識別碼檢驗憑證機構簽發憑證的適用性是否正確。憑證機構引用本基礎建設之憑證政策物件識別碼前，必須先經政策管理委員會同意。

下列唯一之物件識別碼為本憑證政策之識別：
2.16.158.3.1.3.5

ISO 指定	**2**
組織別	**16**
國碼	**158**
中華民國銀行公會專用	**3**
營運環境	**1**
金融最高層憑證機構	**3**
憑證政策	**5**

1.3 金融公開金鑰架構之成員

本基礎建設之憑證機構架構圖示如下：



1.3.1 憑證機構 (CA)

1.3.1.1 金融最高層憑證機構（FRCA）

為本基礎建設之最高層憑證機構，其簽發之自我簽章憑證(Self-Signed Certificate)乃本基礎建設唯一之可信賴根源。透過單一最高層憑證機構將確保本基礎建設中各憑證間之互通性。

1.3.1.2 金融政策憑證機構（FPCA）

為預留日後憑證階層架構之擴充性，故建置第二階之金融政策憑證機構，未經

本會依規定程序評選前，由擔任本基礎建設最高憑證機構之單位兼任之。

1.3.1.3 用戶憑證機構（FUCA）

為本基礎建設中負責簽發用戶(個人或組織)憑證的憑證機構。

1.3.2 註冊中心（RA）

註冊中心係擔任驗證憑證申請人及憑證請求等資訊正確性之工作。

1.3.3 憑證用戶（Subscriber）

憑證用戶指憑證中所命名或識別之主體，且其持有與憑證中所載公開金鑰相對應之私密金鑰(Private Key)者。憑證用戶可以是自然人或組織。

1.3.4 信賴憑證者(Relying Party)

指相信憑證主體名稱與該主體公開金鑰及私密金鑰連結關係之個人或組織。

1.3.5 其他相關成員

憑證機構得委託其他機構協助處理憑證作業相關事宜，惟應於憑證實務作業基準說明受託之機構身分，並訂定作業程序、管理方式及責任義務。

1.4 憑證用途

1.4.1 適用範圍

本憑證適用於開放式網路環境，針對資訊的傳遞提供亂碼加密及身份認證之用，業務範圍包括線上付款、轉帳等金融相關交易，以及經由憑證政策管理委員會審核通過之項目。

1.4.2 憑證禁用範圍

本憑證禁止使用於犯罪等不法行為。

1.5 政策管理

1.5.1 憑證政策之制定及管理機關

本憑證政策之制定及管理機關為中華民國銀行公會憑證政策管理委員會(PMA)。依據中華民國銀行公會「憑證政策管理委員會設置要點」定義，憑證政策管理委員會的任務，係管理金融最高層憑證機構及其下屬各憑證機構，並定期稽核以確保各憑證機構之營運及服務品質。

憑證政策管理委員會置主任委員一人，並置委員若干人，由金融監督管理委員會、中央銀行、學者專家、業界及機關代表組成，職掌如下：

(1) 管理與監督金融最高層憑證機構及其下屬所有憑證機構的營運。
(2) 制定金融公開金鑰基礎建設憑證政策及用戶憑證機構之申請辦法，審核各憑證機構交付之憑證實務作業基準。
(3) 審核金融最高層憑證機構及金融政策憑證機構就用戶憑證機構之收費、稽核、管理及其他有關事項所訂定或修訂之相關作業規範及管理規章等。
(4) 審核金融最高層憑證機構及金融政策憑證機構與外部組織的合作與連結，以確保憑證使用之適當性。
(5) 審核金融最高層憑證機構及其下屬憑證機構之營運申請。
(6) 受理金融最高層憑證機構及其下屬憑證機構所交付備查之稽核報告，並於必要時派員查核。
(7) 評選及撤銷金融最高層憑證機構。
(8) 協調各憑證機構間共通性之法規、政策、技術及業務相關議題。
(9) 訂定「金融憑證機構管理準則」。
(10)研議其他與金融憑證相關事宜。

1.5.2 聯絡資料

如對本憑證政策有任何建議，請與政策管理委員會聯繫，聯絡資料為：

單位：中華民國銀行商業同業公會全國聯合會憑證政策管理委員會
地址：台北市德惠街九號三樓(世界之頂大樓)
電話：(02)8596-2229
傳真：(02)8596-2228
網址：https://www.ba.org.tw/
E-mail：pma@ba.org.tw

1.5.3 憑證實務作業基準與憑證政策相符之審定

憑證機構應先自行檢查憑證實務作業基準是否符合憑證政策相關規定後，再送政策管理委員會進行審查核定。

1.5.4 憑證實務作業基準之審定程序

各憑證機構之憑證實務作業基準均須遵循本憑證政策規定，檢附自行評估合乎憑證政策規定之報告，並送交憑證政策管理委員會審查以取得核准資格。

另依據電子簽章法規定，憑證機構訂定之憑證實務作業基準，必須經主管機關經濟部核定後，始得對外提供憑證簽發服務。

2. 資訊公布及儲存庫責任

2.1 儲存庫

憑證機構之憑證實務作業基準應載明儲存庫之相關資訊。

2.2 憑證資訊公佈

憑證機構應在固定的儲存庫公佈：

(1) 憑證實務作業基準。
(2) 憑證廢止清冊(或提供線上憑證狀態查詢：OCSP)，包括憑證廢止清冊之簽發時間與效期、憑證廢止時間。
(3) 憑證機構本身之憑證，至少應到該憑證相對應之私密金鑰所簽發的所有憑證效期到期為止。
(4) 簽發之所有憑證(包括簽發給其他憑證機構之憑證)。

除上述資訊外，憑證機構應公佈可驗證數位簽章之必要資訊。憑證機構之憑證實務作業基準應載明儲存庫暫停服務時間之上限。

2.3 公佈頻率或時間

本憑證政策之公佈與後續之任何修訂將由憑證政策管理委員會核准後公告。

本憑證政策規範的更新或調整經由憑證政策管理委員會的審核通過後，至少於生效之前一個月公告於最高層憑證機構憑證管理系統的網站，並通知相關憑證機構索取。

憑證廢止清冊之公佈頻率請依照本憑證政策「4.9.7 憑證廢止清冊發布頻率 」規定辦理。

2.4 存取控制

憑證機構應保護儲存庫的資訊，以防止被惡意的公開散播或修改。公鑰憑證及憑證狀態資訊應經由網際網路公開取得。

(1) 憑證政策與憑證機構之憑證實務作業基準的取得不需存取控制。
(2) 憑證由憑證機構自行決定是否需控制存取。

3. 識別及驗證

3.1 命名

憑證機構(/註冊中心)對於憑證申請者的身分識別與驗證，必須依本憑證政策的作業管理規範，建置與訂定符合安全控管措施的作業管理程序。

對於憑證申請者的身分識別與驗證，必須選定適當的作業管理人員，以確實完成用戶的身分識別與驗證。

為了確實認證申請人之身分，憑證申請者之憑證註冊作業應採臨櫃申請模式；而且憑證申請作業中金鑰的產生是由申請人自行操作。

3.1.1 命名種類

憑證機構必須確保憑證申請者的識別名稱(Distinguished Name，DN)的明確與唯一性，並符合 X.500 識別名稱的規範(RFC 5280)，且於本憑證政策相關的憑證機構之範圍內，每一憑證申請者的識別名稱為唯一。

3.1.2 命名須有意義

憑證內容之簽發者(Issuer)與申請者(Subject)的識別名稱所存放的內容，必須為具有意義的內容，且為可以唯一識別憑證簽發者與申請者身份的資訊。

3.1.3 用戶匿名或假名

憑證內容之簽發者(Issuer)與申請者(Subject)的識別名稱所存放的內容，不可存放空白的資訊、或匿名、或不可辨識的識別名稱。

3.1.4 識別名稱之命名規則

用戶憑證識別名稱之命名規則使用X.500 之命名規範，詳細的命名規則定義於「金融XML憑證共通性技術規範」。

3.1.5 識別名稱之唯一性

憑證機構所使用於憑證內之申請者的識別名稱，於本作業規範所訂定的範圍內具有唯一性，憑證機構於編訂與使用時，必須確保每一識別名稱的辨識性與唯一性。

3.1.6 辨識，驗證與註冊商標的角色

憑證機構於憑證內使用的各種用戶識別名稱，當用戶有相同的註冊名稱或識別名稱時，以先申請註冊的用戶優先使用，後申請者於註冊名稱後加區分欄位碼或流水號以資區別與識別不同的用戶。

當識別名稱使用發生爭議時，仲裁機構為政策管理委員會。

憑證機構除與用戶另有合約等協定外，依據本憑證政策所使用的用戶識別名稱，憑證機構不保證用戶註冊商標、商號、公司名稱、或其他特殊意義之名稱的認可與驗證。

憑證機構不可於明確已知曉的情況下，接受已為相關主管機關或司法機關禁止使用之用戶識別名稱或用戶註冊名稱與註冊商標；但憑證機構無驗證用戶註冊名稱與註冊商標的權責。

3.2 初始註冊

3.2.1 私密金鑰之驗證方法

用戶於自行產生公開金鑰對後，以公開金鑰向憑證機構申請用戶憑證的簽發時，申請訊息包含用戶的註冊資訊與用戶私密金鑰的簽章，當憑證機構驗證申請訊息無誤後完成憑證簽發，即為確定用戶擁有此私密金鑰。

3.2.2 法人用戶身分之驗證

憑證機構處理組織用戶的身分驗證時，需驗證組織名稱、所在地及代表人名稱等足以識別該組織之資料。憑證機構或註冊中心除需驗證申請資料及代表人身分的真實性外，並應驗證該代表人有權以該組織之名義申請憑證。申請時應由代表人親臨憑證機構或註冊中心辦理。

若用戶無法親自臨櫃辦理，得以書面委託書委任代理人代為臨櫃申請，但憑證機構或註冊中心必須確認該委託書之真偽，並依上述規定驗證代理人身分。

3.2.3 個人用戶身分的驗證

憑證機構或註冊中心處理個人之用戶註冊的身分驗證時，需進行臨櫃身分驗證，並比對身分證明文件。若用戶無法親自臨櫃辦理，得以書面委託書委任代理人代為臨櫃申請，但憑證機構或註冊中心必須確認該委託書之真偽，並依上述規定驗證代理人身分。

3.2.4 未經驗證之用戶資訊

未經驗證之用戶資訊不得寫入憑證。

3.2.5 權責之確認

個人、法人代理人及法人之身分證明文件，應為官方核發之證明文件；註冊中心應確認文件之真偽。

3.2.6 交互運作標準

所有憑證機構除非取得憑證政策管理委員會之同意，不得對其他憑證機構洽商

交互認證等協議。

3.3 金鑰更新請求之識別及驗證

3.3.1 例行性金鑰更新之識別及驗證

於憑證有效期限屆滿前，註冊中心必須通知用戶執行憑證更新，而用戶重新產生新的公開金鑰，於舊有憑證尚未廢止或過期之前，可使用已註冊的用戶資訊向憑證機構申請簽發用戶憑證，完成例行性金鑰更新。

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例行性更新。

用戶每九年應根據 3.2 之規定重新進行註冊。

憑證機構對於用戶憑證及私密金鑰的更新，必須具有身份識別驗證與資料完整性的安全控管措施。

3.3.2 憑證廢止後金鑰更新之識別及驗證

用戶憑證已廢止後，不得執行憑證及私密金鑰的更新，新憑證的簽發應依照 3.2 規定，用戶必須重新辦理憑證申請作業。

3.4 憑證廢止請求之識別及驗證

憑證機構或註冊中心必須對於憑證廢止申請進行鑑別，憑證機構應依照「4.9 憑證暫時停用與廢止」規定，在憑證實務作業基準中載明申請者之身分鑑別方式，以確認申請者為有權提出憑證廢止之申請者。

用戶可使用私密金鑰之簽章及欲廢止之憑證來證明自己是憑證廢止申請者。

4. 憑證生命週期作業規範

4.1 憑證申請

4.1.1 憑證的申請者

憑證的申請者包含：

(1) 用戶憑證機構。

(2) 用戶憑證機構所服務的對象，包括組織或個人。

4.1.2 註冊程序與責任

用戶憑證機構申請加入時，需將相關之申請文件送至憑證政策管理委員會，憑證政策管理委員會將依公告之用戶憑證機構申請辦法核定其資格。經憑證政策管理委員會核可之用戶憑證機構，政策憑證機構方可核發其憑證。

用戶的憑證將透過註冊中心申請，註冊中心除了由憑證機構自行運作外，亦可委由其他機構擔任，惟目前為確保其安全性將只允許金融機構擔任。

憑證申請之詳細程序及規範應載明於憑證機構之憑證實務作業基準中。

不論是用戶憑證機構或其用戶，申請憑證之金鑰，都需由其自行產生，不得由所屬憑證機構代為產生。實務應用範圍內若有其他特殊狀況，須經憑證政策管理委員會同意，並應於憑證實務作業基準中載明。

4.2 憑證申請的程序

4.2.1 執行識別及驗證功能

憑證機構須依本憑證政策 3.2 節「初始註冊」之規定執行，確保系統與程序足以鑑別用戶身分。

4.2.2 憑證申請的核准或拒絕

憑證機構完成及確認身分驗證後，可核准憑證申請。

除因申請者身分識別與鑑別之原因外，憑證機構得因其他原因不同意簽發憑證。

4.2.3 處理憑證申請的時間

應於憑證實務作業基準中載明憑證機構及註冊中心完成受理憑證申請作業的時間。

4.3 簽發憑證的程序

4.3.1 憑證機構的作業

憑證機構或註冊中心在收到憑證請求時，應根據憑證實務作業基準中之相關規範執行憑證簽發。

憑證簽發時註冊中心或憑證機構必須具備相關之安全機制，以確定憑證請求來源之身分正確性、資料完整性、憑證請求內容符合本憑證政策之規定，此安全機制可以是實體管控或應用密碼學之技術性控管。

4.3.2 憑證機構對申請者的通知

憑證機構或註冊中心如不同意簽發憑證，應以適當方式通知憑證申請者，並明確告知不同意簽發的理由。

除簽發測試憑證外，憑證機構應於憑證實務作業基準中載明憑證申請結果的通知方式。

4.4 接受憑證的程序

4.4.1 接受憑證的要件

有關申請者接受與拒絕憑證之程序及條件應明訂於憑證實務作業基準中。由於本憑證政策只允許申請者自行產生金鑰，因此在申請者發出憑證請求後，將同時同意以該憑證請求之相關資訊所核發之憑證，若憑證核發時某些欄位將由憑證機構自行決定，應事先載明於憑證機構之憑證實務作業基準中，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規範核發時，申請者得以拒絕，憑證機構除應廢止該憑證外，其衍生之法律糾紛與賠償也需訂定於憑證實務作業基準中。

當憑證申請者拒絕接受憑證，有關收費或退費之模式應載明於憑證實務作業基準中，且應依消費者保護法及公平交易原則制定之。

4.4.2 憑證機構的憑證發布

憑證機構應定期將所簽發之憑證公布於儲存庫。

4.4.3 憑證機構對其他個體的憑證簽發通知

憑證機構得自行決定其對其他個體之憑證簽發通知，本憑證政策於此不另行規定。

4.5 金鑰對及憑證之用途

4.5.1 用戶私密金鑰及憑證使用

用戶是指憑證中所命名或識別之主體，且其持有與憑證中所載公開金鑰相對應之私密金鑰(Private Key)者。用戶必須依據憑證機構規定之適用範圍使用金鑰對與憑證，憑證機構應於憑證實務作業基準中載明用戶憑證之適用範圍及私密金鑰使用之應注意事項。

4.5.2 信賴憑證者公開金鑰及憑證使用

信賴憑證者必須了解且同意憑證實務作業基準與憑證政策相關作業規範，對憑證所記載之資訊進行檢驗後，應用憑證於規範所訂定的業務範圍內，且不得違反相關法律的規定與侵害第三者的權利。

4.6 憑證展期

憑證機構未經憑證政策管理委員會之同意，不得辦理憑證展期。

4.7 憑證的金鑰更新

4.7.1 憑證金鑰更新的事由

憑證金鑰更新的事由請參見 3.3(金鑰更新請求之識別及驗證)。

4.7.2 憑證金鑰更新的申請者

憑證金鑰更新的申請者請參見 4.1.1(憑證的申請者)。

4.7.3 憑證金鑰更新的程序

憑證機構須依本憑證政策 3.3 節辦理申請者的識別與驗證，確保系統與程序足以鑑別用戶身分，並根據憑證實務作業基準中之相關規範做憑證之簽發。

4.7.4 憑證金鑰更新的簽發通知

憑證金鑰更新的簽發通知請參見 4.3.2(憑證機構對申請者的通知)。

4.7.5 接受金鑰更新後憑證的要件

接受金鑰更新後憑證的要件請參見 4.4.1(接受憑證的要件)。

4.7.6 金鑰更新後憑證的發布

金鑰更新後憑證的發布請參見 4.4.2(憑證機構的憑證發布)。

4.7.7 金鑰更新後憑證機構對其他個體的憑證簽發通知

金鑰更新後憑證機構對其他個體的憑證簽發通知請參見 4.4.3(憑證機構對其他個體的憑證簽發通知)。

4.8 憑證變更

憑證機構未經憑證政策管理委員會之同意，不得辦理憑證變更。

4.9 憑證暫時停用與廢止

4.9.1 憑證廢止的因素

憑證基於以下因素應予廢止：

(1) 憑證中的識別資訊或屬性在憑證過期前有所更動。
(2) 憑證之擁有者經證實有違反本憑證政策之相關條文或所屬憑證機構之憑證實務作業基準時。
(3) 憑證對應之金鑰懷疑或確實已遭破解、金鑰對應媒體已毀損或遺失無法再使用。
(4) 所屬憑證機構之金鑰懷疑或確實已遭破解。
(5) 憑證擁有者因其他因素要求廢止。

4.9.2 憑證廢止的申請者

基於 4.9.1 所提之相關因素，憑證可由憑證用戶申請廢止，或由憑證所屬之憑證機構或註冊中心逕行廢止。

惟憑證若由憑證機構或註冊中心逕行廢止，其相關條件及衍生之費用、權利義務等問題應載明於憑證實務作業基準中。

4.9.3 憑證廢止的程序

憑證廢止可接受讓用戶線上或臨櫃申請，但不論是採取任何方式，憑證廢止之申請，應採取適當之身份辨識機制，如臨櫃身份比對、手寫簽名或數位簽章等，如此可降低遭阻絕服務(Denial of Service)攻擊可能性。

用戶憑證之廢止必須透過註冊中心申請，註冊中心應依照憑證實務作業基準之規定在確認廢止申請之正確性後，傳送憑證廢止請求至憑證機構執行真正的憑證廢止。

憑證廢止時，請求者應儘可能載明廢止之原因，尤其是因為金鑰有安全疑慮而申請廢止憑證者，更應載明此狀態，憑證機構應將此原因反應於憑證廢止清冊或線上憑證狀態查詢資訊(OCSP)中。

憑證在廢止後必須將廢止之憑證資訊記載於最新一次公告之憑證廢止清冊中，並應於約定時間內更新線上憑證狀態查詢資訊(OCSP)的憑證狀態資料庫。憑證廢止

資訊必須於憑證過期後，才可自憑證廢止清冊或線上憑證狀態查詢資訊(OCSP)的憑證狀態資料庫中移除。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。

4.9.4 憑證廢止申請的寬限期

本政策並不規範使用者如有 4.9.1 所描述之狀況時，應於多少時間內完成憑證之廢止，用戶憑證機構對此時間若有相關之規範應載明於憑證實務作業基準中。

4.9.5 憑證機構處理憑證廢止申請的時效

不論是註冊中心或憑證機構，在確定收到的廢止請求正確無誤後，應儘可能於最短的時間內完成憑證廢止處理，相關之處理時間應載明於憑證實務作業基準中。

4.9.6 信賴憑證者檢查憑證廢止的要求

信賴憑證者除了需確保憑證簽章的正確性外，尚需驗證憑證資訊是否記載於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，信賴憑證者參考某憑證廢止清冊時一定需確認：

(1) 憑證廢止清冊來源之正確性與資料之完整性(亦即發布者名稱正確且具正確之數位簽章者)；
(2) 憑證廢止清冊尚未過期(亦即下一次更新較驗證時之日期晚)。

4.9.7 憑證廢止清冊發布頻率

用戶之憑證狀態檢核將以線上憑證狀態查詢資訊(OCSP)為主，但用戶憑證機構仍需定期發布憑證廢止清冊，發布之頻率本憑證政策將不做規範，但各用戶憑證機構應載明於憑證實務作業基準。

金融最高層憑證機構、政策憑證機構之憑證機構憑證廢止清冊則至少每一天發布一次。

4.9.8 憑證廢止清冊產生與發布間的時間差

憑證機構的憑證廢止清冊產生時間(有效日期欄位)與發布間的時間差不得超過 4 小時。

4.9.9 線上憑證狀態查詢（OCSP）服務

憑證機構除了發布憑證廢止清冊之機制外，還必須提供線上憑證狀態查詢（OCSP）之服務。

4.9.10 線上憑證狀態查詢（OCSP）的規定

信賴憑證者可透過線上憑證狀態查詢來確認憑證之有效性，採用此方式者將不需再透過最近之憑證廢止清冊驗證該憑證是否已廢止或暫時停用。

憑證機構應於憑證實務作業基準中載明信賴憑證者查驗線上憑證狀態之方式。

4.9.11 其他形式的廢止公告

憑證機構以其他形式提供之憑證狀態查詢功能，必須於憑證實務作業基準規範其作業方式，且資料保護方式至少應等同憑證廢止清冊之方式實施。

4.9.12 金鑰遭破解時的其他特殊規定

無相關規定。

4.9.13 憑證暫時停用的因素

用戶憑證機構應提供用戶憑證暫時停用之功能，憑證暫時停用之可能原因為：

(1) 暫時性懷疑憑證的安全性，如一時找不到憑證對應之金鑰，但還不完全確定其已遺失。
(2) 欲暫停使用憑證一段時間。

有關暫時停用因素的詳細規範應載明於用戶憑證機構的憑證實務作業基準中。

4.9.14 憑證暫時停用的申請者

暫時停用之請求只允許由憑證之擁有者提出，憑證機構或註冊中心不可主動對任何一使用者憑證做憑證之暫時停用。

4.9.15 憑證暫時停用的程序

憑證暫時停用可採線上暫時停用或臨櫃暫時停用，但不論是採取任何方式，憑證暫時停用之請求，都應採取適當之身分辨識機制，如臨櫃身分比對、手寫簽名或數位簽章等。

用戶憑證之暫時停用必須透過註冊中心申請，註冊中心在確認暫時停用請求之正確性後，再傳送至憑證機構端執行真正的憑證暫時停用。

憑證暫時停用後，憑證機構應將於憑證廢止清冊或線上憑證狀態查詢資訊(OCSP)中設定廢止事由(Revoke Reason)為憑證暫時停用(CertificateHold)狀態。

憑證在暫時停用後必須反應於最新一次公告之憑證廢止清冊中，並儘快更新線上憑證狀態查詢資訊(OCSP)的憑證狀態資料庫。憑證暫時停用資訊必須一直到憑證解除暫時停用或過期後，才可自憑證廢止清冊或線上憑證狀態查詢資訊(OCSP)的憑證狀態資料庫中移除。

憑證在暫時停用之原因消除後，應可透過嚴謹之恢復使用程序以繼續使用。

憑證暫時停用與恢復使用程序應載明於憑證機構之憑證實務作業基準中。

4.9.16 暫時停用時間之限制

本政策對憑證暫時停用的時間並無限制，亦即憑證暫時停用後其狀態可一直持續至憑證到期。

4.10 憑證狀態服務

4.10.1 服務特性

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

4.10.2 服務可用性

憑證機構應提供 7 x 24 小時憑證狀態查詢的服務。

4.10.3 其他服務項目

無相關規定。

4.11 終止所申請的憑證服務

用戶不再使用憑證機構的服務時，憑證機構應同意並妥善辦理終止程序。

4.12 私密金鑰託管與回復

4.12.1 金鑰託管與回復的政策與程序

不論在任何狀況下，具不可否認性之簽章金鑰絕不可接受託管。
憑證機構其他金鑰若有金鑰託管者，應載明於憑證實務作業基準中。

4.12.2 通訊用金鑰封裝與回復的政策與程序

無相關規定。

5. 設施面、管理面與作業面的安全控管

5.1實體控管

憑證機構必須建置與安裝具體實體安全管控措施的保護環境，以管理對執行憑證作業管理系統之硬體設備、密碼模組與相關設施硬軟體資源的存取使用。

存取使用該硬軟體資源必須為經過授權的「5.2.1 可信賴角色」之作業管理人員，存取的管理機制至少具有門鎖鑰匙控制、或電子式的自動門鎖控制等安全機制，以防止未經授權者的任意存取或破壞者的入侵。

5.1.1 建築物與位置

憑證機構營運與執行憑證管理系統電腦機房的建築物必須具有實體堅固的外牆，並建築於穩固的基準之上。外牆如為易碎材質必須具有實體的防破壞安控設施，且建築物四周無容易造成火災之危險產生因素。建築物實體應具備安全管控之措施，可防止與偵測任何非法的入侵破壞，及未經授權的使用及存取電腦機房內的資訊設備或系統資源的不法行為。

5.1.2 實際進出管制

憑證管理系統運作的相關實體環境中，作業管理人員進出管制必須建置與安裝適當的門禁身份識別管制機制，並留存進出紀錄；需建置與安裝防入侵警報系統，以防止與偵測任何未經授權的入侵，以保障憑證管理系統作業區域的安全。

需確保所有含敏感明文資料之可攜式儲存媒體及文件均存放於安全處所。

需兩人以上方可對電腦及密碼模組進行實體存取，並留存稽核軌跡。

憑證管理系統運作的重要設備例如密碼模組等，須安裝於有監控錄影系統保護的作業環境內，二十四小時隨時執行監控錄影與紀錄。

5.1.3 電力與空調

憑證機構必須充分提供憑證管理系統設備與相關設施運作所需的電力，於異常狀況時除提供不中斷電源系統(Uninterruptible Power Supply ,UPS)備援設備外，尚需提供備援的發電功能，以保持正常穩定之供應所需電力，使憑證管理系統的運作無斷電之虞。

憑證機構憑證管理系統運作的環境，必須具有獨立且有備援的空調系統，以保持恆溫與恆濕的作業環境。

電力與空調系統必須依據憑證機構作業管理規範，定期執行維護與測試。

5.1.4 防水處理

憑證機構憑證管理系統運作的四周環境，必須安裝適當的排水設施，以保護設備與設施免於水患的侵害。

5.1.5 防火處理

憑證機構憑證管理系統運作的相關區域，必須安裝適當的防火建材，與滅火設備或設施，且必須具備自動偵測火災預警功能，系統能自動啟動滅火設備，並設置手動開關於各主要出入口處，以供現場人員於緊急情況時以手動方式操作。

5.1.6 媒體儲存

憑證機構對於憑證管理系統所產生與使用的媒體與文件，必須儲存於具有防火、防水、防磁、防靜電干擾，且具有安全管控措施的處所。

備份及保存資訊的儲存媒體與文件，一份必須儲存於具有安全管控措施的異地備援處所。

備份及保存資訊的儲存媒體與文件，必須定期執行測試與驗證資訊的有效性與可使用性。

5.1.7 廢棄處理

憑證機構於憑證管理系統所使用的硬體設備、密碼模組、文件與媒體等，於廢棄不使用時，商業敏感性及隱密性資訊必須經過安全的清除與銷毀，且經由稽核單位的驗證，並留存查核文件。

5.1.8 異地備份

憑證機構對於因應異常事件或硬體設備毀損與系統故障，而必須執行憑證管理系統運作回復與重新開啟作業時，所需的備份資訊需求與回復程序及執行頻率，必須訂定於憑證實務作業基準，且至少一份備份必須儲存於具有安全管控措施的異地備援處所。

5.2作業程序控管

5.2.1 可信賴角色

為避免於執行憑證作業管理過程中，因過失或惡意而引發安全問題，憑證作業管理或維護人員，必須依職務功能與權責考量獨立性，選用適當人員擔任。

為保障公開金鑰基礎建設架構之安全的完整性，憑證機構應於憑證實務作業基準中訂定執行憑證管理相關作業之可信賴人員的權責。

各信賴角色作業人員分類如下：

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

2.憑證管理人員(Officer)－負責憑證及憑證廢止之請求、簽發。

3.稽核人員(Auditor)－負責進行內部稽核、檢視並維護稽核紀錄。

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

以上人員均不得互相兼任

5.2.2 作業人員需求人數

憑證機構於執行憑證管理相關作業的人員，其權責為獨立且不重疊，作業人員執行個人的職務工作，絕不影響其他作業職務的獨立性與安全性，系統資源存取使用的權限帳號，必須符合授權指派的職務工作。

為達到系統運作管理的穩定性，執行憑證管理相關作業的各個職務，應妥善規劃職務代理人，以維護憑證管理作業營運永續性。

重要系統資源的存取使用管理，例如金鑰的建置或變更管理，必須設計至少具有二位以上的作業管理人員分持控管的安全管控機制，任何一人無法單獨存取使用系統資源。

5.2.3 角色的識別與驗證

憑證機構對於執行憑證管理相關作業所需的作業人員，於存取使用系統相關的資源時，需依據其職掌設定唯一的帳號或身份識別碼與相關權限，且於使用系統資源之前，必須經由至少為密碼、或 IC 卡或指紋等生物科技的辨識驗證，才可以授權其使用系統資源。

5.2.4 角色的權責劃分

憑證機構須於實務作業基準中敘明信賴角色之權責劃分。

5.3 人員控管

5.3.1 適任條件與經歷

憑證機構對於執行憑證管理相關作業的作業人員，必須訂定任用與管理的作業管理規範，說明每一職務的電腦系統與憑證管理系統實務經驗之適任條件，並考量其對於工作盡職的熱誠度、忠實度、與可信賴度，若需要時應進行違法犯紀不良紀錄之查核。

憑證機構之執行憑證管理相關作業的作業管理人員，必須實際具有適任的職能、或經由教育訓練而達到擔任該職務之條件，才可任用並擔任相關管理作業。

5.3.2 審核

作業人員必須依據各種作業人員的職務特性，於擔任相關管理作業職務前，應先定期執行安全、實務與經歷適任職務的審查，以作為執行工作調整或調派的依據。

作業管理人員亦應接受定期審核；經審查有不適任該可信賴角色時，絕不可繼續執行該職務。

5.3.3 教育訓練

憑證機構必須給予作業人員完善的教育訓練，項目包括公開金鑰基礎建設的作

業機制、憑證管理系統、作業系統、資源管理系統、業務永續經營與災變備援作業、憑證政策與憑證實務作業基準、安全警覺與安全作業管理規範及法律權責管理規範等。

5.3.4 再教育的頻率與需求

當憑證管理系統功能更新，或加入新系統，或進用新進人員時，必須給予相關作業人員的再教育訓練。對於再教育訓練的執行，憑證機構必須依據執行管理作業的需求訂定教育訓練之時程，每年至少檢討一次。

5.3.5 職務的輪調

本憑證政策對職務的輪調無特殊規範。當憑證機構選派適任的人選輪調至適合的工作歷練時，於調派前必須施以適當且完整的知識與技能之教育訓練使能勝任職務。

5.3.6 非授權作業的懲罰

憑證機構對於憑證管理系統運作的相關作業人員，因故意或過失而執行非職務上的作業，無論造成或未造成憑證管理系統安全的問題，必須訂定相關處理作業規範。

5.3.7 委外人員需求

憑證機構有委外的作業需求時，除必須依照委外業務的工作內容簽訂相關的權責合約外，該委外人員的作業安全管理措施至少與憑證機構之內部作業管理人員相同。

5.3.8 作業文件需求

憑證機構為使憑證管理系統的運作正常及順暢，必須提供相關作業人員適當與完善的作業管理手冊與文件，包含申請作業管理手冊、憑證作業管理手冊、憑證政策、憑證實務作業基準、日常作業處理手冊、與執行憑證管理系統運作所需的其他相關系統管理手冊及設施與設備維護管理手冊等。

5.4 稽核紀錄程序

5.4.1 處理事件的紀錄種類

憑證機構對於處理註冊與憑證相關處理作業的紙本文件、與電腦媒體紀錄，無論由實體環境設施、設備至電腦系統與憑證管理系統、及人工處理的事件紀錄，必須詳實留存，包含處理事件型態、發生時間、事件發生與結束過程、訊息的發送與接收者、成功與失敗、事件處理者等。

處理事件的紀錄種類至少包含下述：實體環境門禁進出之人員授權的管理、電

腦硬體設備與設施的維護與異動管理、系統軟體與憑證管理系統的安裝建置與變更管理、註冊與憑證相關處理作業生命週期的管理、網路系統資源與稽核處理作業的管理、文件與資訊保存的管理等。

5.4.2 稽核紀錄處理頻率

憑證機構對於處理事件的紀錄，必須具有妥善安全保護的稽核紀錄，非權責管理人員無法任意存取與竄改，且至少每週由授權的稽核管理人員對稽核紀錄執行查核管理作業。

對於稽核紀錄的查核，除檢核每一處理事件的紀錄，當有任何異常或警訊的紀錄時，必須更進一步詳細追蹤查核，且留存紀錄文件與資訊。

5.4.3 稽核紀錄的保存期限

憑證機構對於稽核紀錄的保存期限，除必須符合權責主管機關與司法管轄機關的法律管理規範外，任何與憑證管理作業相關的報表與媒體稽核紀錄至少應保留十年，並於憑證機構所在處所至少保留兩個月之資料。

5.4.4 稽核紀錄的保護

憑證機構對於稽核紀錄的保護，必須具有妥善且安全的控管保護措施，非為經過授權的管理人員或處理系統無法任意存取與竄改；必須建置存取稽核紀錄之適當的資源授權控管系統，至少具備存取稽核紀錄的管理人員之身份識別驗證或者處理系統的控管措施，並且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與竄改。

稽核保存紀錄的備份，必須由權責獨立且只具有讀取功能的授權備份作業人員執行備份保存，儲存稽核保存紀錄的備份資訊媒體，至少一份必須存放於具有妥善安全保護措施的控管之異地儲存處所。

5.4.5 稽核紀錄備援程序

憑證機構對於稽核紀錄的處理作業，必須將稽核紀錄的備援程序訂定於憑證管理系統的日常作業管理程序中，且依據作業管理程序確實執行，至少每個月備份一次。

5.4.6 稽核紀錄蒐集系統

稽核紀錄的蒐集，除文件紙本的手動紀錄蒐集外，對於電腦自動稽核紀錄蒐集系統，必須於憑證作業管理系統開始執行時啟動紀錄功能，而於憑證作業管理系統關閉後才可以停止紀錄的功能。

當電腦自動稽核紀錄蒐集系統異常或故障時，則憑證作業管理系統必須停止服務，直到稽核紀錄蒐集系統回復正常運作，才可開啟憑證作業管理系統的運作；如果憑證作業管理系統必須持續運作而無法停止，則必須啟動手動紀錄蒐集或其他可

行的替代方案。

5.4.7 對引起事件者之告知

當事件發生而被稽核系統紀錄時，稽核系統並不需要告知引起該事件的個體所引發的事件已被系統所紀錄。

5.4.8 弱點的風險評估

對於異常事件的稽核紀錄處理，憑證機構必須確實對於異常事件可能造成的威脅與風險進行評估，隨時調整與修改憑證管理系統運作的安全控管措施，且每年至少應執行一次以上。

5.5 紀錄歸檔方法

5.5.1 保存紀錄的種類

憑證機構必須保存詳實完善之憑證管理系統運作的相關紀錄，以建立驗證簽章的有效性、不可否認性與公開金鑰架構運作的完整性與可信賴性；
至少必須保存下述資訊：

(1) 憑證政策、憑證實務作業基準、與用戶合約、及相關作業手冊與申請表單文件。
(2) 憑證申請、更新、暫時停用、廢止等憑證作業管理生命週期的申請、用戶身分識別資料與處理訊息。
(3) 用戶與憑證機構之憑證、憑證廢止清冊。
(4) 其他作業系統與憑證管理系統檔案資訊，與稽核紀錄等。
(5) 系統與設備組態設定。
(6) 稽核人員所要求之文件。

5.5.2 保存期限

憑證機構對於憑證管理系統運作的相關紀錄的保存期限，除必須符合權責主管機關與司法管轄機關的法律管理規範外，任何與憑證管理作業相關的報表與媒體稽核紀錄至少應保留十年。

5.5.3 保存紀錄的保護

憑證機構對於保存紀錄的保護，必須存於具安全管控措施且有防潮濕的保護環境下，非經由合法的授權人員皆無法存取。

保存紀錄必須至少有一份存放於具安全管控措施且有防潮濕保護環境的異地儲存處所。

憑證機構保存及保護的紀錄，非經主管機關或司法管轄機關經合法申請的需求，及用戶自己授權且符合作業管理規範的申請，絕不任意予第三者知悉。

5.5.4 保存紀錄的備援程序

憑證機構對於保存紀錄的備援作業，必須將保存紀錄的備援與回復程序訂定於憑證管理系統的日常作業管理程序中，且依據作業管理程序每日確實執行保存資料的備份。

5.5.5 紀錄的時序需求

憑證機構至少對於憑證作業管理之憑證申請、更新、暫時停用、與廢止等處理作業，必須具有時序的紀錄，憑證機構金鑰的更新與異動亦需具有時序的紀錄。

5.5.6 保存紀錄蒐集系統

憑證管理系統作業相關的保存紀錄文件與資訊，如無法由電腦系統處理及產出，則需由權責相關的作業人員蒐集與處理。

5.5.7 取得與驗證保存紀錄程序

憑證機構必須訂定取得保存紀錄資訊的安全控管作業程序；唯有授權的作業管理人員經過合法授權的作業管理程序才可以存取；亦需訂定驗證憑證管理系統作業相關的保存紀錄資訊完整性與可使用性之作業管理程序。

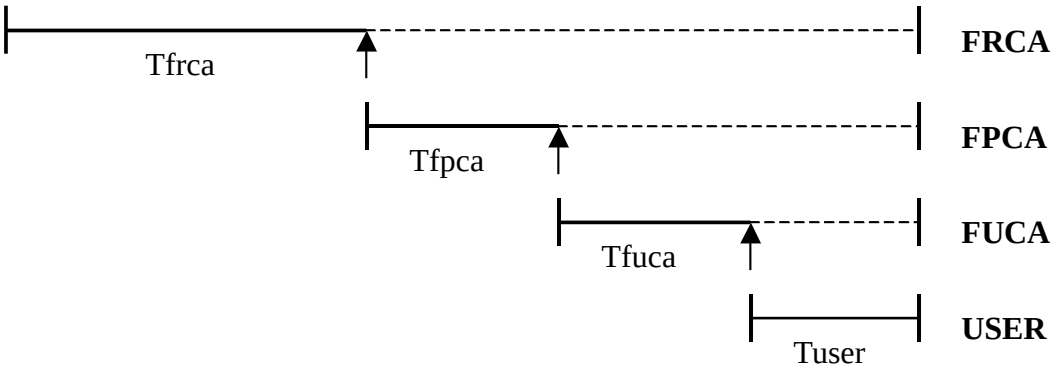
5.6 金鑰更換

憑證機構核發完憑證後，信賴憑證者將根據憑證機構的憑證來驗證其所核發出的使用者憑證之正確性，因此憑證機構在做憑證核發時一定需注意以下幾點：

(1) 不可使用已過期憑證機構憑證對應之簽章金鑰簽發使用者憑證

(2) 憑證機構憑證之效期必須涵蓋下層所有憑證之效期。

為符合以上之需求，憑證機構應於憑證到期前產生新的簽章金鑰對，並選定從適當的時間點後便開始使用新的簽章金鑰對做憑證之簽發；以下為各憑證機構簽章金鑰使用時間之關係圖，



↑ CA 金鑰更換之時間點, 此時間點後將以新金鑰簽發憑證

根據上圖本政策對各憑證機構及一般使用者憑證效期之建議為

FRCA : $T_{FRCA} + T_{FPCA} + T_{FUCA} + T_{USER}$

FPCA : $T_{FPCA} + T_{FUCA} + T_{USER}$

FUCA : $T_{FUCA} + T_{USER}$

USER : 目前建議為一年(金鑰儲存媒體使用非硬體裝置，如磁碟片)或二年(金鑰儲存媒體使用硬體裝置，如 IC 卡)

FRCA、FPCA、FUCA 分別代表最高層憑證機構、政策憑證機構及用戶憑證機構的簽章金鑰之使用時間，這些時間之長短將由最高層憑證機構決定，並於憑證實務作業基準中說明。

用戶之憑證於即將過期前將進入更新狀態，用戶可根據需要申請憑證，憑證更新之過程必須避免中斷或終止任何憑證相關的正常作業。

5.7 金鑰遭破解及災難之復原

5.7.1 緊急事件及系統遭破解之處理程序

憑證機構應於憑證實務作業基準敘明緊急事件及系統遭破解後之通報、處理及復原程序。

5.7.2 電腦資源、軟體或資料庫之復原程序

憑證機構若因設備毀損或其他因素導致無法作業，但相關之簽章金鑰仍可正常使用且無洩漏之虞時，憑證機構應具備相關之備援設備及定期之資料或系統備份復原之程序，並儘可能於最短之時間內完成復原，復原之程序及時間應載明於憑證實務作業基準中。至少每年應進行一次災難復原演練。

5.7.3 憑證機構簽章金鑰遭破解之復原程序

當憑證機構簽章金鑰遭破解時，應儘快告知上層憑證機構；上層憑證機構應立即廢止該簽章金鑰對應之憑證，並公佈該憑證廢止之相關資訊。憑證機構應於其憑證實務作業基準中載明憑證機構簽章金鑰遭破解之復原程序，該程序除了重新建立一可簽發憑證之環境外，尚需包含原簽章金鑰已簽發出憑證重新簽發之相關程序。

5.7.4 憑證機構災後持續營運措施

憑證機構針對天然或其他型態災難之發生應有相關之安全措施，以確保不論是在原先的機房或者是欲成為新營運機房之備援機房，都不會有金鑰或敏感性資料曝光之風險。相關之安全措施亦應載明於憑證實務作業基準中。

5.8 憑證機構之終止服務

金融最高層憑證機構、政策憑證機構不論基於任何理由需終止服務時，應依協議無條件提供本會關於下屬憑證機構相關檔案及資訊，並配合系統移轉作業，維持營運至憑證政策管理委員會核可之下一家擔任機構接替為止。

另應依電子簽章法相關規定進行憑證機構終止服務時之相關處理作業

6. 技術性安全控管

6.1 金鑰對產生與安裝

6.1.1 金鑰對產生

不論是最高層憑證機構、政策憑證機構或用戶憑證機構，其用來核發憑證與憑證廢止清冊的金鑰對，需經兩位(含)以上之授權人員啟動經密碼模組產生。產生後的金鑰對可直接儲存於密碼模組中，供合法授權之憑證作業系統使用。另此金鑰對也可儲存於密碼模組外(如儲存於憑證作業系統的主機上)，儲存於密碼模組外的金鑰相關資訊，除了需做適當之權限控管外，亦需做亂碼加密保護(如以密碼模組的主基碼加密保護)以確保金鑰對無曝光之虞，最後還需確保如金鑰相關資訊真的遭非法使用者取得，也無法於未授權的環境下使用之。

一般使用者的金鑰對乃由使用者自行產生，產生後之金鑰對以只有使用者可使用為原則。實務應用範圍內若有其他特殊狀況，須經憑證政策管理委員會同意，並於憑證實務作業基準中載明。

不論是最高層憑證機構、政策憑證機構或用戶憑證機構，其用來核發憑證與憑證廢止清冊的金鑰對，需經由通過 FIPS 140-2 level 3(含)以上或其他相同等級認證的密碼模組所產生。

用戶的金鑰對可由硬體或軟體產生，產生後的金鑰對應做適當之隱密性保護，嚴禁將金鑰對以明碼的形式儲存於一般媒體中(如硬碟、磁片等)。

6.1.2 私有金鑰遞送

憑證機構或用戶之金鑰對皆需自行產生，因此對於私有金鑰遞送使用者並無相關規範。實務應用範圍內若有其他特殊狀況，須經憑證政策管理委員會同意，並於憑證實務作業基準中載明。

6.1.3 公開金鑰遞送

公開金鑰的遞送應確保訊息的來源辨識性及正確性，保護之機制可為:

(1) 直接於公開金鑰所屬之資料訊息做押碼(Message Authentication Code，MAC)或簽章(需為一有效憑證對應之金鑰所簽)保護以達成，採用此方式公開金鑰訊息可透過一非安全之通道做傳送(如電子郵件、磁片或檔案傳輸等)

(2) 先經適當之身份認證後傳送公開金鑰資訊，此方式需確保身份認證與資料傳送同屬一安全(如SSL伺服端認證)之Session，此方式較適合於WEB之模式。

(3) 透過另一管道確認公開金鑰資訊之正確性，如以授權之表單說明公開金鑰之檢核資訊(如公開金鑰之拇指紋)，採用此方式公開金鑰訊息同樣可透過一非安全之通道做傳送。

6.1.4 憑證機構公開金鑰遞送至信賴憑證者

憑證機構應於憑證實務作業基準中敘明憑證機構公開金鑰安全傳送予信賴憑證者之方式。

6.1.5 金鑰長度

本政策目前建議使用之簽章或加解密之演算法為 RSA，若有更有效率之演算法則其金鑰之長度乃與以下規範之金鑰長度安全強度相同者亦可，相關憑證機構及使用者之金鑰長度規範如下：

(1) 最高層憑證機構： 至少需使用RSA 4096 位元之金鑰。
(2) 政策憑證機構及用戶憑證機構：至少需使用RSA 4096 位元之金鑰。
(3) 一般用戶：至少需使用RSA 2048 位元之金鑰。

6.1.6 公開金鑰參數產製與品質的檢核

有關參數品質檢核(包含質數的測試)應遵循相關國際標準之規範，並載明於憑證實務作業基準中。

6.1.7 金鑰用途

對於憑證中所認證的公開金鑰必須在 X.509 憑證之金鑰用途(keyUsage)擴充欄位註明其金鑰用途。

用戶用來做訊息簽章(包含身分認證)的憑證，其憑證擴充欄位記載之金鑰用途應設定為簽章用(digitalSignature)及不可否認用(Repudiation)；而做為加密用之憑證，其憑證中之金鑰用途應設定為加密金鑰用(keyEncipherment)或加密資料用(dataEncipherment)。

憑證機構本身之憑證其金鑰用途需設定為簽發憑證廢止清冊用(cRLSign)及簽發憑證用(keyCertSign)。

對於用戶的憑證允許可兼具有簽章用及加密用的金鑰用途設定。

6.2 私密金鑰保護與密碼模組安全控管措施

6.2.1 密碼模組標準與控管

憑證機構用來核發憑證與憑證廢止清冊等憑證相關功能之密碼模組，需至少通過 FIPS 140-2 level 3(含)以上之認證，或相同安全級之其他認證。

用戶之密碼模組不做規範。

6.2.2 金鑰分持之多人管控

最高層憑證機構、政策憑證機構私密簽章金鑰之使用應由多位授權之管理人員所啟動，多人管控之規範之遵循本政策第五章「設施面、管理面與作業面的安全控

管」之規定。

6.2.3 私密金鑰託管

不論在任何狀況下，具不可否認性之簽章金鑰絕不可接受託管。

憑證機構其他金鑰若有金鑰託管者，應載明於憑證實務作業基準中。

6.2.4 私密金鑰備份

憑證機構為確保其憑證作業可持續進行，得備份其簽章用之私密金鑰，惟私密金鑰之備份與啟用需符合正常金鑰使用之安全控管程序，備份之作業應於多人管控下方可執行，相關程序應載明於憑證實務作業基準中。

用戶為確保交易之持續進行，可作私密簽章金鑰之備份，惟使用者端之私密金鑰備份應以不影響交易之不可否認性為原則，若相關之金鑰媒體或系統因私密金鑰之備份而無法達到簽章之唯一性與不可否認性，則禁止其做私密金鑰之備份。

6.2.5 私密金鑰歸檔

簽章用之私密金鑰不得歸檔。

加密私密金鑰得視需要歸檔保存，歸檔保存的年限以相對應之密文資料之保存年限為依據，歸檔之私密金鑰仍需符合正常金鑰使用之安全控管程序。

6.2.6 私密金鑰於密碼模組的收送傳輸

除依照「6.1.1 金鑰對產生」之規定外，私密金鑰於密碼模組的收送傳輸應有其作業之必要性，並依相關規範辦理。

6.2.7 私密金鑰儲存於密碼模組

憑證機構之私密金鑰得以密文或明文方式儲存於密碼模組，使用時需符合 6.2.2 節之多人控管原則；密碼模組如不需使用時須離線並儲存於安全場所。

6.2.8 私密金鑰之啟動方式

憑證機構啟用私密金鑰時，應至少有兩人(含)以上之合法授權人員共同啟動方可使用，授權人員啟動時應做適當之身份認證。

用戶私密金鑰之啟動，則必須由用戶出示相關的啟動資料(如密碼、通行密語等)，始得啟動使用之，本政策嚴禁未經授權之金鑰使用。

6.2.9 私密金鑰之解除使用方式

憑證機構欲解除私密金鑰的使用時，應由被授權人員執行，並須通過適當之身份認證。私密金鑰之解除使用可透過人工之方式執行或者由系統判斷在某個特定的狀況下(如一段時間未用後)自動執行。

6.2.10 私密金鑰之銷毀方式

當私密金鑰不再需要或者其對應之憑證已過期或註銷，則此金鑰應予銷毀。若為軟體之密碼模組，則原私密金鑰所儲存之檔案或記憶體應以某特定資料覆蓋之。若為硬體之密碼模組，則應執行零值化(zeroize)動作，或實體銷毀整個密碼模組。

6.2.11 密碼模組的等級

請參見 6.2.1 (密碼模組標準與控管)。

6.3 金鑰對管理的其他規範

6.3.1 公開金鑰的歸檔

公開金鑰之歸檔將視為憑證歸檔的一部份。

6.3.2 公開金鑰及私密金鑰的使用期限

依「5.6 金鑰更換」之規範辦理。

6.4 啟動資料

6.4.1 啟動資料的產生及設定

憑證機構用以啟動密碼模組及相關金鑰的啟動資料，其產生及設定應做適當之安全管控，以達到唯有授權之人員方可啟動之目的。啟動資料若為密碼，其設定時應對密碼的品質及使用期限做適當之管控，相關之控管機制亦應載明於憑證實務作業基準中。使用之密碼若是由系統產生，則產生之密碼應有妥善之保護機制，以確保在使用人員取得前無未授權人員取得該密碼。

用戶金鑰的啟動資料的產生及設定，應確保唯有該用戶可使用。

6.4.2 啟動資料的保護

憑證機構用以啟動密碼模組及相關金鑰的啟動資料，在產生及設定後應對該資料做適當之保護。保護之機制可透過實體之控管或其他之存取控管，如當啟動資料需以書面方式保存時，則應透過實體之管控保護之，而當啟動資料需以數位資料的形式儲存於電腦系統或其儲存媒體中時，則除了系統之存取管控外，應輔以適當之密碼模組(不同於欲啟動之密碼模組)做適當保護。

用戶金鑰的啟動資料的保護，應確保唯有該用戶可使用。

6.4.3 其他啟動資料的規定

本政策無其他啟動資料之規定。

6.5 電腦安全控管

6.5.1 電腦安全技術需求

憑證機構對於實體安全環境的保護、作業系統的管理、與憑證管理系統的管理，及用戶憑證管理系統的管理，必須具有下述的功能：

(1)憑證管理系統的作業管理人員，於系統資源存取控管之角色與權責區分的獨立性與可稽核性，作業管理人員於系統資源存取控管時，身份識別驗證的唯一性與確實性。

(2)資料庫系統資訊存取與使用的安全控管措施，身份識別驗證的唯一性、確實性與可稽核性，資訊存取隱密性的保護管理措施，符合相關法律規範的規定。

(3)資訊傳遞訊息的安全控管措施，符合隱密性、完整性、與不可否認性等安全控管機制需求。

憑證相關交易的回復管理機制，與稽核作業的管理機制。

6.5.2 電腦系統安全等級

憑證機構執行認證作業使用的相關軟體作業系統、資料庫系統、與憑證管理系統等，其電腦軟體系統安全等級必須於憑證作業實務基準中載明。

6.6 生命週期技術控管

6.6.1 系統開發控管

憑證機構對於憑證管理系統使用的相關軟體之規劃、設計、開發作業程序控管，至少必須留存充分的文件，以為第三查核機構評估憑證機構對於系統軟體開發作業程序安全管控的依據，與使用該系統軟體對於安全控管保護之威脅與風險評估的依據。

6.6.2 安全管理控管

憑證機構對於執行認證管理系統的資訊安全管理系統環境，必須符合 *WebTrust program for CA(AICPA/CICA)及 ISO27001* 的標準規範運作。

憑證機構必須記錄和控管憑證機構相關系統的組態以及任何修正與功能升級，並具備偵測未經許可修改憑證機構之軟體或組態的機制。在首次安裝憑證機構軟體時，必須確認是由供應商提供且未被修改過，且為正確的版本。

6.6.3 生命週期的安全等級

生命週期的安全控管等級作業規範，暫無訂定。

6.7 網路安全控管

憑證機構執行憑證管理系統的網路，必須具有防火牆、防入侵偵測系統、防病毒破壞系統與網路資源安全控管系統的保護，只開放與憑證相關的作業功能，其他非憑證機構所提供的功能或通訊介面，一般使用者均無法使用，且隨時提昇更新網路防火牆、防入侵偵測、防病毒與網路資源安全控管系統的版本。

最高層憑證機構、政策憑證機構憑證管理系統為離線(Off-Line) 、獨立的作業管理系統，且需經授權後由業務相關的作業人員才可以人工方式執行作業，單獨一位作業人員絕對無法進行。

6.8 時戳

時戳之相關規範，暫無訂定。

7. 憑證及憑證廢止清冊格式

7.1 憑證格式剖繪

7.1.1 版本

憑證機構須簽發 X.509 V3 版本之憑證。

7.1.2 憑證擴充欄位

憑證機構證管理系統使用的憑證格式，必須遵循 IETF RFC 5280 或更新版之規定。

憑證機構必須於憑證實務作業基準或憑證相關作業管理規範，說明擴充欄位使用的內容。

7.1.3 演算法物件識別碼

憑證機構各憑證管理系統使用的演算法物件識別碼，必須為 ISO 物件識別碼管理單位公告的規範：

演算法安全機制	演算法(Algorithm)	物件識別代碼
金鑰產製	RSAEncryption	1.2.840.113549.1.1.1
簽章	sha256WithRSAEncryption	1.2.840.113549.1.1.11

7.1.4 識別名稱格式

憑證機構使用的識別名稱格式內容，必須符合 X.500 識別名稱的命名方式以及「金融 XML 憑證共通性技術規範」所訂定的格式內容。

7.1.5 識別名稱限制

憑證機構使用的識別名稱之限制，必須符合「金融 XML 憑證共通性技術規範」所訂定的識別名稱限制。

7.1.6 憑證政策物件識別碼

憑證機構必須於憑證內存放憑證機構憑證政策的物件識別碼。

7.1.7 憑證政策限制擴充欄位的使用

憑證機構必須於憑證實務作業基準或憑證相關作業管理規範，說明憑證政策限制擴充欄位的使用。

7.1.8 憑證政策限制語法與語意

憑證機構必須於憑證實務作業基準或憑證相關作業管理規範，說明憑證政策限制擴充欄位使用的限制語法與語意。

7.1.9 憑證政策擴充欄位必要的處理

憑證機構必須於憑證實務作業基準或憑證相關作業管理規範，說明憑證政策限制擴充欄位使用的必要處理。

7.2 憑證廢止清冊格式剖繪

7.2.1 版本

憑證機構簽發之憑證廢止清冊版本為 X.509 V2。

7.2.2 憑證廢止清冊擴充欄位

憑證機構必須於憑證實務作業基準或憑證相關作業管理規範，說明憑證廢止清冊與憑證廢止清冊擴充欄位的使用。

7.3 線上憑證狀態協定格式剖繪

7.3.1 版本

線上憑證狀態協定應符合 RFC 6960 或更新版本規定。

7.3.2 線上憑證狀態協定擴充欄位

線上憑證狀態協定之擴充欄位應符合 RFC 6960 或更新版本的規定。

8. 稽核方法

簽發憑證之憑證機構，應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機構審核後送政策管理委員會核備，以確保其運作遵照憑證實務作業基準與憑證政策之規定。

8.1 稽核之頻率

憑證機構依據本會金融憑證機構管理準則第十五條，應每年至少一次接受外部例行性稽核，憑證政策管理委員會於必要時得派員執行專案查核，憑證機構不得拒絕，並應負擔相關費用。

8.2 稽核人員之身份及資格

具備 CISA 及 CIA 資格之會計師事務所人員。

8.3 稽核人員及被稽核方之關係

稽核人員應獨立於被稽核的憑證機構外，並遵循中華民國會計師公會職業道德規範公報第十號對於「正直、公正客觀及獨立性」之相關規範。

8.4 稽核之範圍

稽核之內容至少應包括下列項目：

(1) 憑證實務作業基準是否符合憑證政策之規定。
(2) 憑證機構是否依憑證實務作業基準執行憑證管理作業。
(3) 金鑰生命週期管理是否符合憑證政策之規定。
(4) 憑證生命週期控管是否符合憑證政策之規定。
(5) 憑證機構環境控管是否符合憑證政策之規定。

8.5 稽核缺失之處理

憑證機構應依據稽核報告改善缺失，若仍未於限定時間內改善者，憑證政策管理委員會得暫停憑證機構的營運、廢止憑證機構簽發給下屬憑證機構的憑證；發現重大缺失時，憑證政策管理委員會亦得撤銷該機構擔任憑證機構之資格。

8.6 稽核結果公開之範圍

除可能危害系統安全之資訊外，與信賴憑證者信賴該憑證的相關資訊，均應公開提供。憑證機構應在其設立之公開網站公佈最近一次的稽核結果。

9. 其他業務與法律事項

9.1 費用

金融最高層憑證機構對於下屬憑證機構收取費用或收費機制之規定，應由憑證政策管理委員會同意後方得施行。

9.1.1 憑證簽發、更新費用

不做規定。

9.1.2 憑證查詢費用

不做規定。

9.1.3 憑證廢止、狀態查詢費用

不做規定。

9.1.4 其他服務費用

不做規定。

9.1.5 請求退費之程序

不做規定。

9.2 財務責任

9.2.1 保險範圍

不做規定。

9.2.2 其他資產

不做規定。

9.2.3 對用戶及信賴憑證者之賠償責任

各憑證機構應於憑證實務作業基準中載明對於下屬憑證機構、註冊中心、用戶及信賴憑證者的賠償責任。

9.3 業務資訊保密

9.3.1 機敏性資料的範圍

憑證機構對於用戶於申請憑證時所提供的相關資訊，除用戶憑證內容可公開的資訊外，其餘資訊均為機敏性資訊，應依據憑證機構的安全控管措施妥善的保護，非經用戶同意或依法令規定，不得對外公開。

9.3.2 非機敏性資料的範圍

憑證機構管理的憑證政策、憑證實務作業基準，用戶與憑證機構的憑證資訊、憑證廢止清冊資訊，及憑證內的用戶資訊為可公開的非隱密性資訊。

9.3.3 保護機敏性資料的責任

憑證機構應於憑證實務作業基準中敘明保護機敏性資訊的責任。

9.4 個人資料的隱密性

對於用戶隱密性資訊的保護，除符合本憑證政策之規範外，亦須符合相關法令規定。

憑證機構對於用戶隱密性資訊的保護，非經用戶同意或依法令規定，絕不以任意方式對外公開、銷售、租借。

憑證機構為憑證管理作業的需求而使用與存取用戶資訊時，必須合於業務的需求與具體嚴謹的安全管控措施，由業務有權存取的作業人員執行。相關作業應留存稽核軌跡，以供查核之用。

9.4.1 保護計畫

憑證機構應於憑證實務作業基準中敘明。

9.4.2 隱密資料

憑證機構應於憑證實務作業基準中敘明。

9.4.3 非隱密資料

憑證機構應於憑證實務作業基準中敘明。

9.4.4 保護隱密資料的責任

憑證機構應於憑證實務作業基準中敘明。

9.4.5 使用隱密資料的告知與同意

憑證機構應於憑證實務作業基準中敘明。

9.4.6 因應法規與管理程序的應揭露事項

憑證機構應於憑證實務作業基準中敘明，並依相關法令規定辦理。

9.4.7 其他應揭露事項

憑證機構應於憑證實務作業基準中敘明。

9.5 智慧財產權

本憑證政策之智慧財產權屬於銀行公會擁有，本會保有本憑證政策的所有權利。

9.6 職責與義務

9.6.1 憑證機構職責與義務

(1) 未依憑證實務作業基準及相關之規範，處理相關作業，致下屬憑證機構、用戶或信賴憑證者遭受之損害，該憑證機構應負賠償責任。
(2) 未依憑證實務作業基準履行相關之責任及擔保，致下屬憑證機構、用戶或信賴憑證者所受之損害，該憑證機構應負賠償責任。
(3) 因網際網路傳輸的中斷或設備的故障或其他不可抗拒的天災事故(例如戰爭或地震等)，而非可歸責之事由，所致下屬(用戶或信賴憑證者)機構的損失，該憑證機構不負賠償責任。
(4) 憑證機構對因其經營或提供認證服務之相關作業程序，致當事人受有損害，或致善意第三人因信賴該憑證而受有損害者，應負賠償責任。但能證明其行為無過失者，不在此限。憑證機構就憑證之使用範圍設有明確限制時，對逾越該使用範圍所生之損害，不負賠償責任。(電子簽章法第 14 條)
(5) 其他依電子簽章法規定應負之賠償責任。
(6) 對憑證內容與核發之正確性負擔保責任。
(7) 用戶憑證機構應於憑證實務作業基準或與註冊中心之契約或協議中載明註冊中心之責任。
(8) 訂定並公告憑證實務作業基準。
(9) 公告憑證廢止清冊（CRL）的內容。
(10) 簽發、管理、遞送與廢止下屬憑證機構/用戶之憑證。
(11) 公告、管理憑證作業程序與驗證的作業規範。
(12) 依據憑證實務作業基準之規範，執行相關之作業程序。
(13) 用戶憑證機構並應管理與公告憑證廢止清冊與憑證狀態線上查詢（Online Certificate Status Protocol，以下簡稱OCSP）資訊時的作業程序與身份驗證及訊息安控措施的作業規範。

(14)依據本憑證政策各項規定提供相關控制。

9.6.2 註冊中心職責與義務

由於註冊中心係代理憑證機構執行身分識別工作所引發的所有責任，註冊中心之責任應依其與憑證機構間約定之權利義務而定。考量整體作業安全，本基礎建設目前僅允許金融機構擔任註冊中心。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之責任。

(1) 負責確認憑證申請人之身分，但不負責簽發及管理憑證。
(2) 管理與公告用戶註冊申請的作業程序與身分驗證的作業規範。
(3) 驗證用戶憑證之簽發與廢止及查詢等申請訊息、身分合法性與訊息正確性。
(4) 遞送用戶的申請憑證、廢止憑證、查詢申請等訊息至憑證機構，並驗證回覆訊息的正確性後傳回用戶。
(5) 管理、公告並提供用戶憑證查詢、廢止及憑證機構的憑證鏈。
(6) 用戶申請或廢止、暫時停用等憑證作業時必須驗證用戶身分，用戶憑證相關申請訊息轉送至憑證機構時，必須驗證訊息的安全性與正確性。
(7) 註冊中心與其作業人員必須善盡保管用戶資料及相關訊息之責任、避免相關資訊洩漏、被冒用、篡改及任意使用。
(8) 註冊中心與憑證相對應的私密金鑰有被冒用、曝露及遺失等不安全的顧慮時，或憑證內註冊中心相關的資訊有異動時，必須依相關作業的規定，即刻向憑證機構辦理申告與處理。
(9) 憑證機構遞送的用戶憑證，必須提供用戶憑證適時更新的機制。
(10) 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註冊中心並留存相關資料於註冊中心。
(11) 註冊中心應通知憑證即將到期的用戶辦理更新憑證作業。

9.6.3 用戶的義務

接受憑證機構簽發憑證的用戶應負以下義務：

(1) 向註冊中心申請憑證時，必須提供詳細且正確的身分證明文件與資料供註冊中心審核。
(2) 其憑證與憑證對應的私密金鑰使用的業務範圍，皆依憑證機構「憑證實務作業基準」與「憑證政策」之規範，運用於相關業務上。
(3) 合法且正確的使用私密金鑰與憑證，無任何違反相關法律的規定與侵害第三者的權利。
(4) 用戶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。
(5) 憑證內用戶相關的資訊有異動時，用戶必須依相關作業的規定，即刻向註冊中心辦理申告與處理。

9.6.4 信賴憑證者的義務

使用憑證機構簽發憑證的信賴憑證者應負以下義務：

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

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

9.6.5 其他參與者的義務

不做規定。

9.7 免責聲明

憑證機構應於憑證實務作業基準中敘明免責聲明及其限制條件，惟不得將因自行疏忽所引起之後果列入免責聲明中。

9.8 責任限制

憑證機構應於憑證實務作業基準中敘明責任限制。

9.9 賠償

憑證機構應於憑證實務作業基準中敘明對用戶及信賴憑證者的賠償責任。

9.10 有效期限與終止

憑證機構應於憑證實務作業基準中敘明有效期限與終止。

9.10.1 有效期限

本憑證政策於公告後即生效，嗣後修正時亦同。

9.10.2 終止

本憑證政策之終止須經由銀行公會憑證政策管理委員會決議。

9.10.3 終止與存續之效力

本憑證政策終止後，其效力須維持至所簽發之最後一張憑證失效為止。

9.11 對參與者的個別通知與溝通

應以適當方式對參與者進行個別通知及溝通。

9.12 修訂

9.12.1 修訂程序

本憑證政策規範的權責管理單位為銀行公會憑證政策管理委員會，任何憑證政策內容的更新或調整，必須經由憑證政策管理委員會的審核與公告。

本憑證政策有更新建議時，必須將詳細的相關文件郵寄或 E-mail 至「1.5.2 聯絡資料」，經憑證政策管理委員會的審查與覆核。

9.12.2 通知機制與期限

對用戶可能產生重大影響之變更項目，憑證機構應公告於儲存庫，並於憑證實務作業基準敘明變更項目通知機制及公告期限。

9.12.3 修改憑證政策物件識別碼的事由

憑證政策的修改不影響憑證政策所聲明的憑證使用目的與保證程度時，憑證政策之物件識別碼不需修改，憑證政策之物件識別碼變更，憑證實務作業基準應作相對應之變更。

當憑證政策內容有更新版本時，相對應的物件識別碼不隨之異動，只變更憑證政策物件識別碼的版本序號。

9.13 紛爭之處理程序

加入本基礎建設之憑證機構、註冊中心、所有用戶因憑證服務發生爭議時，應秉持誠信原則協商解決之。若無法於爭議發生後十四天內解決爭議，得經雙方同意由憑證政策管理委員會協助解決雙方之爭議；若爭議發生後一個月內爭議仍未解決者，則除雙方另合意提交仲裁外，雙方合意以台灣台北地方法院為第一審管轄法院。

9.14 管轄法律

憑證機構應於憑證實務作業基準中明訂以中華民國法律為準據法，並明訂在中華民國地區的法院為管轄法院。

9.15 適用法律

憑證機構應於憑證實務作業基準中述明適用的法律。

9.16 雜項條款

9.16.1 完整協議

不另行規定。

9.16.2 轉讓

憑證機構應於憑證實務作業基準中敘明主要成員之權利或責任之轉讓規定。

9.16.3 可分割性

如本憑證政策的任一章節不正確或無效時，其他章節仍然有效。

9.16.4 契約履行

用戶或信賴憑證者違反本憑證政策相關規定，致憑證機構受有損害，如可歸責於用戶或信賴憑證者之故意或過失時，憑證機構除得請求損害賠償外，亦得向可歸責之一方請求支付處理該爭議或訴訟之律師費用。

憑證機構未向違反本憑證政策相關規定者主張權利，不代表憑證機構對其繼續或未來違反本憑證政策情事有拋棄權利主張之意思。

9.16.5 不可抗力

憑證機構得於憑證實務作業基準中敘明排除條款。

9.17 其他條款

不另規定。

附錄

參考文件

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