工商憑證管理中心

憑證實務作業基準

（Ministry of Economic Affairs Certification Authority Certification Practice Statement）

第 2.4 版

主辦機關：經濟部

執行機構：中華電信股份有限公司

中華民國 111 年 05 月

目　　錄

摘要

依據電子簽章法授權發布訂定之「憑證實務作業基準應載明事項」規定，工商憑證管理中心憑證實務作業基準（以下簡稱本作業基準）之重要事項說明如下：

1. 主管機關核定文號：經商字第 11102413000 號

2. 簽發之憑證

(1) 種類：

A. 我國登記設立之公司、分公司、商業、有限合夥及有限合夥分支機構等事業主體（以下統稱事業主體，包括簽章用及加解密用的兩種憑證）憑證。

B. 我國登記設立之公司、商業及有限合夥等事業主體使用於「公司與商業及有限合夥一站式線上申請作業」網站之專屬授權憑證(以下簡稱一站式專屬授權憑證)。

C. 我國公司、商業或有限合夥名稱預查申請核准之有限公司及股份有限公司(以下簡稱準公司)、商業(以下簡稱準商業)與有限合夥(以下簡稱準有限合夥)等事業主體於「公司與商業及有限合夥一站式線上申請作業」網站申請設立之專屬用戶憑證(以下簡稱設立專屬用戶憑證)。

(2) 保證等級：

工商憑證管理中心（以下簡稱本管理中心）依據政府機關公開金鑰基礎建設憑證政策（以下簡稱憑證政策）保證等級第 3 級運作，簽發憑證政策所定義保證等級第 3 級的事業主體憑證及一站式專屬授權憑證。同時，亦簽發憑證政策所定義保證等級第 2 級的設立專屬用戶憑證。

(3) 適用範圍：

A. 事業主體憑證適用於電子化政府暨電子商務等符合事業主體業務活動之相關應用服務所需的身分識別、數位簽章及資料加密，所傳送的資料可以包含金錢上的交易。

B. 一站式專屬授權憑證僅可用於「公司與商業及有限合夥一站式線上申請作業」網站。

C. 設立專屬用戶憑證僅可用於「公司與商業及有限合夥一站式線上申請作業」網站之設立申請功能。

用戶及信賴憑證者，必須謹慎使用本管理中心所簽發之憑證，並依本作業基準憑證適用範圍使用。

3. 法律責任重要事項

(1) 用戶或信賴憑證者如未依照本作業基準規定之適用範圍使用憑證所引發之後果，本管理中心不負任何法律責任。

(2) 用戶或信賴憑證者因使用憑證而發生損害賠償事件時，本管

理中心之損害賠償責任以雙方契約之約定以及電子簽章法所訂之責任範圍為限。

(3) 如因不可抗力及其他非可歸責於本管理中心之事由，所導致之損害事件，本管理中心不負任何法律責任。

(4) 註冊中心因執行註冊工作所引發之法律責任依相關法令規定辦理。

(5) 如因用戶隱瞞事實，提供不正確資料，導致信賴憑證者遭受損害時，相關法律責任應由用戶自行負責。

(6) 用戶之憑證如須暫時停用、恢復使用、廢止或重發，應依照本作業基準相關規定辦理。若發生私密金鑰資料外洩或遺失等情形，必須廢止憑證時，應立即通知本管理中心，如未通知或通知後尚未異動前，用戶仍應承擔使用該憑證之法律責任。

4. 其他重要事項

(1) 本管理中心如因系統維護、轉換及擴充等需要，得暫停部分憑證服務，並儘可能事先公告於儲存庫及通知用戶，用戶或信賴憑證者不得以此作為要求本管理中心損害賠償之理由。

(2) 如因註冊中心審驗錯誤，導致用戶或信賴憑證者遭受損害時，註冊中心與管理中心之損害賠償責任以民法及電子簽章法所訂之責任範圍為限。

(3) 用戶在完成接受本管理中心所簽發之憑證作業程序後，即表示已確認憑證內容資訊之正確性，並依照本作業基準相關規定使用憑證，如憑證內容資訊有誤，用戶應主動通知本管理中心。

(4) 用戶及信賴憑證者應慎選安全的電腦環境及可信賴的應用系統，如因電腦環境或應用系統環境本身因素導致使用者權益受損時，應自行承擔責任。

(5) 本管理中心如因故無法正常運作時，用戶及信賴憑證者應儘速尋求其他途徑完成與他人應為之法律行為，不得以本管理中心無法正常運作，作為抗辯他人之事由。

(6) 信賴憑證者接受使用本管理中心簽發之憑證時，即表示已了解並同意有關本管理中心法律責任之條款，並依照本作業基準相關規定使用憑證。

(7) 本管理中心所簽發之憑證僅對憑證主體身分作確認，由憑證註冊審驗人員或審驗系統審驗用戶之身分及憑證相關資訊。

(8) 本管理中心由電子化政府主管機關依政府採購法，委外辦理政府機關公開金鑰基礎建設憑證機構之外部稽核作業，並委託公正第三方辦理外部稽核作業，就本管理中心的運作進行稽核。

1.簡介

工商憑證管理中心憑證實務作業基準（Ministry of Economic Affairs Certification Authority Certification Practice Statement，以下簡稱本作業基準）係依據政府機關公開金鑰基礎建設憑證政策（Certificate Policy for Government Public Key Infrastructure，以下簡稱憑證政策）訂定，並遵循電子簽章法及「憑證實務作業基準應載明事項」等相關規定，說明工商憑證管理中心（Ministry of Economic Affairs Certification Authority，MOEACA；以下簡稱本管理中心）如何遵照憑證政策保證等級第 3 級之規定，進行我國登記設立之公司、分公司、商業、有限合夥及有限合夥分支機構等事業主體（以下統稱事業主體）的公鑰憑證（以下簡稱憑證）及我國登記設立之公司、商業及有限合夥等事業主體使用於「公司與商業及有限合夥一站式線上申請作業」網站之專屬授權憑證(以下簡稱一站式專屬授權憑證)之簽發及管理作業。

此外，本作業基準亦說明本管理中心如何進行我國公司、商業或有限合夥名稱預查申請核准之有限公司及股份有限公司(以下簡稱準公司)、商業(以下簡稱準商業)與有限合夥(以下簡稱準有限合夥)等事業主體於「公司與商業及有限合夥一站式線上申請作業」網站申請設立之專屬用戶憑證(以下簡稱設立專屬用戶憑證)之簽發及管理作業，

惟此類憑證之組織身分鑑別程序係遵照憑證政策保證等級第 2 級之規定辦理。

本作業基準文件格式參考網際網路工程任務小組(Internet Engineering Task Force, IETF)之徵求修正意見書 RFC 3647 建議之格式。

1.1 總覽

依據憑證政策的規定，本管理中心是政府機關公開金鑰基礎建設（Government Public Key Infrastructure，GPKI，以下簡稱本基礎建設）的第 1 層下屬憑證機構（Level 1 Subordinate CA），在本基礎建設中負責簽發及管理我國登記設立之事業主體憑證（包括簽章用及加解密用的憑證）與一站式專屬授權憑證(簽章用)，同時亦負責簽發及管理我國準公司、準商業與準有限合夥之設立專屬用戶憑證(簽章用)。

本作業基準中，將說明本管理中心的憑證作業實務，以確保本管理中心的憑證簽發及管理作業符合憑證政策訂定之保證等級第 3 級之規定，惟有關設立專屬用戶憑證之組織身分鑑別程序係以符合憑證政策訂定保證等級第 2 級之規定辦理。本作業基準所載明之實務作業規範僅適用於與本管理中心相關之個體，如本管理中心、註冊中心（Registration Authority, RA）、用戶（Subscribers）、信賴憑證者（Relying Parties）及儲存庫（Repository）等。

本管理中心係由經濟部（以下簡稱本部）委外建置，由本部負責本作業基準之訂定及修訂，本作業基準經本部依電子簽章法相關規定核定公布。本作業基準並未授權本管理中心以外的憑證機構使用，其他憑證機構因引用本作業基準而引發的任何問題，概由該憑證機構自行負責。

1.2 文件名稱及識別

本作業基準之名稱為工商憑證管理中心憑證實務作業基準（Ministry of Economic Affairs Certification Authority Certification Practice Statement）。本作業基準版本為第 2.4 版，公布日期為中華民國 111 年 05 月 19 日。最新版本的本作業基準可在以下網頁取得：https://moeaca.nat.gov.tw/download/download_4.html。

本作業基準依據憑證政策訂定，本管理中心之運作遵照憑證政策保證等級第 3 級之規定，其物件識別碼名稱為 id-tw-gpki-certpolicy-class3Assurance，物件識別碼值為{id-tw-gpki-certpolicy 3}；惟有關設立專屬用戶憑證之組織身分鑑別程序係以符合憑證政策訂定保證等級第 2 級之規定辦理，其物件識別碼名稱為 id-tw-gpki-certpolicy-class2Assurance，物件識別碼值為{id-tw-gpki-certpolicy 2}。詳請參考憑證政策，憑證政策可在以下網頁取得：https://grca.nat.gov.tw/。

1.3 主要成員

本管理中心之相關成員包括：

(1) 本管理中心。

(2) 註冊中心。

(3) 用戶。

(4) 信賴憑證者。

(5) 其他相關成員，包括發卡中心及本部授權管理、建置與系統維運之委外單位。

1.3.1 本管理中心

本管理中心是本基礎建設中的第 1 層下屬憑證機構，遵循憑證政策保證等級第 3 級的規定，負責我國事業主體憑證、一站式專屬授權憑證與設立專屬用戶憑證之簽發及管理作業。惟設立專屬用戶憑證之組織身分鑑別程序則遵循憑證政策保證等級第 2 級規定辦理。

本管理中心憑證簽發可由申請者自行提出申請，亦可依政府政策之需要，由本管理中心依據事業主體於設立登記資料，遵循憑證政策保證等級第 3 級的規定，逕行簽發憑證。此兩種簽發憑證模式，在本作業基準分別簡稱為申請發證及逕行發證。

1.3.2 註冊中心

本管理中心將設立註冊中心，負責收集和驗證用戶的身分及憑證

相關資訊之註冊工作。註冊中心是由多個註冊窗口（RA Counter）組成，臨櫃註冊窗口設於負責受理事業主體登記設立之政府機關或授權單位，註冊窗口設有憑證註冊審驗人員（RA Officer, RAO），負責受理憑證之註冊申請、暫時停用申請、恢復使用申請及廢止申請等業務。另由本管理中心於網站上設置線上註冊窗口，負責受理憑證線上註冊申請作業。

註冊中心設置註冊中心伺服器（RA Server），負責驗證憑證註冊審驗人員的身分及管理註冊窗口。註冊中心伺服器由註冊中心管理員（RA Administrator）負責管理，註冊中心管理員於註冊中心伺服器上設定憑證註冊審驗人員之帳號與權限，並製發憑證註冊審驗人員 IC 卡（以下簡稱 RAO IC 卡）。註冊中心伺服器上並裝設有註冊中心之私密金鑰，註冊中心伺服器與本管理中心伺服器間的通訊，將由註冊中心之私密金鑰簽章加以保護。

1.3.3 用戶

本管理中心之用戶，係指記載於本管理中心所簽發憑證的憑證主體名稱（Certificate Subject Name）的個體，以本管理中心負責簽發公司、分公司、商業、有限合夥及有限合夥分支機構等事業主體憑證而言，用戶為公司、分公司、商業、有限合夥及有限合夥分支機構等事業主體。以一站式專屬授權憑證而言，用戶為公司、商業及有限合夥

等事業主體；以設立專屬用戶憑證而言，用戶為公司、商業或有限合夥名稱預查申請核准之準公司、準商業與準有限合夥等事業主體。

用戶使用之符記（Token）主要採 IC 卡，每個符記可同時儲存簽章用及加解密用兩種憑證，每個用戶只可申請 1 張正卡（Primary Card），但可依應用需要申請多張附卡（Secondary Card）。除了 IC 卡外，用戶申請附卡也可採用其他軟體或硬體密碼模組（以下統稱非 IC 卡類）。用戶採用非 IC 卡類密碼模組而向本管理中心申請之憑證，一律視同為附卡憑證，其憑證內容將註記為附卡憑證。不過，用戶申請非 IC 卡類憑證時，可依實際上的金鑰用途單獨申請簽章用憑證或加解密憑證之其中 1 種，而不必同時申請簽章用及加解密兩種憑證。本作業基準中有關附卡憑證的相關規定，除非特別指明針對 IC 卡附卡，否則亦將適用於非 IC 卡類憑證。

用戶必須依照 3.2 節初始註冊之識別與鑑別程序，申請或領取憑證正卡。如正卡遺失或憑證將到期時，須依照 3.2 節初始註冊之識別與鑑別程序重新辦理申請。

用戶在取得正卡後，如需申請 IC 卡附卡，可透過正卡之數位簽章線上申請，並可依應用需要申請多張 IC 卡附卡。

1.3.4 信賴憑證者

信賴憑證者係指相信憑證主體名稱與公開金鑰之連結關係的個

體。

信賴憑證者在使用本管理中心所簽發之憑證前，必須以本管理中心本身的憑證及憑證狀態資訊，檢驗所使用憑證的有效性。在確認憑證的有效性後，才可使用憑證進行以下作業：

(1) 檢驗電子文件的數位簽章之完整性。

(2) 檢驗電子文件產生者的身分。

(3) 與憑證主體間建立安全之通訊管道。

1.3.5 其他相關成員

1.3.5.1 發卡中心

本管理中心用戶使用之符記（Token）為 IC 卡時，本管理中心將委託可信賴的發卡中心進行 IC 發卡作業；IC 發卡作業包括 IC 卡內部產製金鑰對、以亂數設定 IC 卡之初始個人識別碼（以下簡稱 PIN 碼）、將申請資料及公開金鑰透過 128 位元安全套接層（Secure Socket Layer）通訊協定或其他相同或更高等級之安全管道傳送給註冊中心伺服器，再傳送給本管理中心簽發憑證、將憑證寫入 IC 卡中及印卡等工作。發卡中心並負責將 IC 卡郵寄至事業主體之登記地址給用戶或發放到經授權之單位，由事業主體負責人或其受託人領取。

1.3.5.2 委外服務單位

本部依照政府採購法委託合格廠商，負責本管理中心之建置及系

統維運作業。

1.4 憑證用途

1.4.1 憑證適用範圍

本管理中心所簽發及管理的憑證包括我國登記設立之事業主體憑證（包含簽章用及加解密用憑證）及我國登記設立之公司、商業及有限合夥等事業主體使用於「公司與商業及有限合夥一站式線上申請作業」網站之一站式專屬授權憑證。我國準公司、準商業與準有限合夥等事業主體於「公司與商業及有限合夥一站式線上申請作業」網站申請設立之設立專屬用戶憑證。

本管理中心所簽發的事業主體憑證與一站式專屬授權憑證之適用範圍符合憑證政策保證等級第 3 級之規定，設立專屬用戶憑證則符合憑證政策保證等級第 2 級之規定。其中，事業主體憑證適用於電子化政府暨電子商務等符合事業主體業務活動之相關應用，一站式專屬授權憑證則僅可使用於「公司與商業及有限合夥一站式線上申請作業」網站，設立專屬用戶憑證僅可使用於「公司與商業及有限合夥一站式線上申請作業」網站之設立申請功能。適用之功能包含系統所需的身分識別或資料加密，所傳送的資料可以包含金錢上的交易。

事業主體憑證均可代表該事業主體進行各項應用，並由事業主體內部自行控管及限定使用範圍，但涉及事業主體存廢之事項，僅能使

用事業主體憑證之 IC 卡正卡。

1.4.2 憑證之使用限制

用戶在使用私密金鑰時，應慎選安全的電腦環境及可信賴的應用系統，以避免私密金鑰被惡意軟硬體盜取或誤用而引發權益受損。

信賴憑證者在使用本管理中心所簽發之憑證前，應確認憑證之類別、保證等級及金鑰用途等是否符合應用需求，若符記為 IC 卡須確認正附卡別。

信賴憑證者應依照 X.509 規範處理憑證中的關鍵性（Critical）與非關鍵性（Non-Critical）憑證擴充欄位（Extensions）。

信賴憑證者在使用本管理中心所提供的服務前，必須詳細閱讀本作業基準，並遵守本作業基準之規定，同時必須注意本作業基準之修訂。

1.4.3 憑證之禁止使用範圍

(1) 犯罪。

(2) 軍令戰情及核生化武器管制。

(3) 核能運轉設備。

(4) 航空飛行及管制系統。

(5) 法令公告禁止適用之範圍。

1.5 聯絡方式

1.5.1 憑證實務作業基準之制訂及管理機構

本部負責制訂本作業基準之各項條款。本作業基準之制訂及修訂在經電子簽章法主管機關核可後公布施行。

1.5.2 聯絡資料

對本作業基準有任何建議，或用戶報告遺失金鑰等事件，請與本管理中心聯絡，本管理中心之聯絡電話：(02)412-1166，郵遞地址：100 台北市信義路 1 段 21 號，電子郵件信箱：moeaca@moeaca.nat.gov.tw，請參閱 https://moeaca.nat.gov.tw/。

1.5.3 憑證實務作業基準之審定

依據電子簽章法相關規定，本作業基準經本部依電子簽章法相關規定核定公布後，始得對外提供簽發憑證服務。

1.5.4 憑證實務作業基準變更程序

本作業基準之變更依 1.5.3 節規定辦理，憑證政策或總管理中心之憑證實務作業基準如有修訂並公告後，本作業基準應配合修訂。

1.6 名詞定義及縮寫

詳參附錄 1「名詞解釋」與附錄 2「英文名詞縮寫」。

2.資訊公布及儲存庫責任

2.1 儲存庫

儲存庫應公布資訊如下：

(1) 簽發之憑證、憑證廢止清冊(Certificate Revocation List, CRL)及其他憑證相關資訊。

(2) 憑證政策及本作業基準。

(3) 最新外部稽核結果。

(4) 本管理中心本身之憑證(公布至與該憑證之公開金鑰相對應之私密金鑰所簽發之所有憑證效期到期為止)。

儲存庫提供 24 小時全天的服務，網址為：https://moeaca.nat.gov.tw/download/download_4.html，其存取控制依照 2.4 節規定辦理。如因故無法正常運作時，須於 2 個工作天內恢復正常運作。

2.2 憑證資訊公布

本管理中心採以下方式公布憑證資訊：

(1) 本作業基準。

(2) 憑證廢止清冊(Certificate Revocation List, CRL)。

(3) 提供線上憑證狀態協定(Online Certificate Status Protocol, OCSP)查詢服務。

(4)儲存庫之憑證查詢服務。

2.3 公布頻率或時間

(1)本作業基準審查核定後 10 個工作天內公告於儲存庫。

(2)本管理中心每日至少簽發並公告 1 次憑證廢止清冊(Certificate Revocation List, CRL)。

(3)本作業基準所指天數，如未特別標示為「工作天」者，均以日曆天計算。

2.4 存取控制

本管理中心主機建置於防火牆內部，外界無法直接連線。儲存庫主機透過防火牆系統控管，連線至本管理中心主機之資料庫，擷取憑證資訊或下載憑證。

有關 2.2 節憑證資訊公布，主要提供用戶或信賴憑證者查詢之用，因此開放提供閱覽存取，並將維持其可接取狀態及可用性。

同時為保障儲存庫之安全應進行存取控制，設定存取權限，有授權者方可存取。

3.識別和鑑別程序

3.1 命名

3.1.1 命名種類

本管理中心所簽發的憑證之憑證主體的名稱採用X.500唯一識別名稱(Distinguished Name，DN)。用戶憑證主體別名(Subject Alternative Name)擴充欄位須為非關鍵性擴充欄位。

3.1.2 命名須有意義

憑證主體名稱之命名方式必須符合公司法、商業登記法及有限合夥法等對事業主體命名之相關法令規定。

3.1.3 用戶匿名或假名

本管理中心不簽發匿名憑證、別名或假名憑證。

3.1.4 命名形式之解釋規則

依據本基礎建設技術規範之憑證格式剖繪，各式命名形式的解釋規則依據 ITU-T X.520 名稱屬性定義。

3.1.5 命名獨特性

本管理中心的X.500唯一識別名稱為：

C=TW，O=行政院，OU=工商憑證管理中心

為使本管理中心所簽發之憑證的憑證主體名稱具備獨特性，本管理中心採用以下名稱格式：

1. 公司憑證

   C=TW

   O=公司的正式登記名稱

   serialNumber=憑證管理中心自動給定用戶之唯一序號

2. 分公司憑證

   C=TW

   O=公司的正式登記名稱

   serialNumber=憑證管理中心自動給定用戶之唯一序號

   OU=分公司的正式登記名稱

3. 商業憑證

   C=TW

   L=縣市名稱

   O=商業的正式登記名稱

   serialNumber=憑證管理中心自動給定用戶之唯一序號

4. 有限合夥

   C=TW

   O=有限合夥的正式登記名稱

5. 有限合夥分支機構

   C=TW

   O=有限合夥的正式登記名稱

   OU=有限合夥分支機構的正式登記名稱

6. 一站式專屬授權憑證

C=TW

L=縣市名稱(選擇性欄位，只適用於商業)

O=公司、商業或有限合夥的正式登記名稱

serialNumber=憑證管理中心自動給定用戶之唯一序號(選擇性欄位，只適用於公司及商業)

7. 設立專屬用戶憑證

C=TW

L=縣市名稱(選擇性欄位，只適用於商業)

O=名稱預查核准之公司、商業或有限合夥名稱

serialNumber=憑證管理中心自動給定用戶之唯一序號

本管理中心所採用的事業主體正式登記名稱係來自於經濟部公司、商業及有限合夥登記資料。

3.1.6 商標之辨識、鑑別及角色

依 3.1.5 節規定，本管理中心所採用的事業主體正式登記名稱，係來自於經濟部公司、商業及有限合夥登記資料，商標之辨識及鑑別非本管理中心管轄範圍，如名稱有爭議，用戶應透過相關法令規定之救濟機制處理。

3.1.7 命名爭議解決程序

如發生用戶名稱所有權爭議時，將依照公司法、商業登記法及有

限合夥法等相關法令規定處理，公司、分公司及商業之命名爭議將以3.1.5 節中的唯一序號（serialNumber）加以區別，以使用戶名稱可以保持唯一性。

但是當自動給定的序號發生重複時，本管理中心得以人工給定的方式，而保持序號的唯一，以解決命名爭議的問題。

3.2 初始註冊

3.2.1 證明擁有私密金鑰之方式

用戶使用之符記為 IC 卡，由本管理中心所信賴的發卡中心代為產製金鑰對，簽發憑證時由發卡中心透過 128 位元安全套接層（Secure Socket Layer）通訊協定或其他相同或更高等級之安全管道將用戶之公開金鑰傳送至本管理中心，因此用戶在申請憑證時不必證明持有私密金鑰。

如用戶使用其他符記，自行產製金鑰對，然後產生 PKCS#10 憑證申請檔且以私密金鑰加以簽章，並於申請憑證時將該憑證申請檔交給註冊中心，註冊中心將使用該用戶的公開金鑰驗證該憑證申請檔的簽章，以證明用戶擁有相對應的私密金鑰。

3.2.2 組織身分之鑑別程序

用戶申請憑證時，必須將憑證申請書（包含事業主體正式登記名稱、統一編號及聯絡人資料等）蓋用事業主體登記及負責人之印鑑章

（與事業主體登記時所使用之印鑑章相符）送交憑證註冊窗口。註冊中心將確認該事業主體確實存在，並驗證申請書上印鑑章是否相符。

當已完成事業主體登記之用戶使用事業主體之負責人自然人憑證，以線上申辦方式申請憑證時，註冊中心須驗證事業主體負責人自然人憑證之數位簽章，並確認該負責人是否具代表該事業主體之資格，以鑑別事業主體之身分。

本管理中心逕行發證時，用戶於收受發卡中心寄發之憑證IC卡後，應依4.4節進行憑證接受作業，以鑑別事業主體之身分。如事業主體未收到寄發之憑證，事業主體必須攜帶領取通知書，於領取單上蓋用事業主體登記及負責人之印鑑章（與事業主體登記時所使用之印鑑章相符）並攜帶負責人身分證正本以及受託人身分證正本至註冊窗口（含授權單位）領取。註冊窗口將確認該事業主體確實存在，並驗證領取單上印鑑章是否相符。

用戶申請IC卡附卡或一站式專屬授權憑證時，須先取得IC卡正卡後，採線上申請方式辦理，註冊中心將驗證IC卡正卡之數位簽章來鑑別事業主體之身分。

用戶申請「設立專屬用戶憑證」時，以「公司與商業及有限合夥一站式線上申請作業」之預查資料辦理線上申請，註冊中心將直接與「公司與商業及有限合夥一站式線上申請作業」比對資料。

用戶IC卡正卡憑證使用期限屆滿應予換發時，用戶得於該憑證到期前2個月內利用線上申請方式申請換發憑證，註冊中心將驗證IC卡正卡之數位簽章來鑑別事業主體之身分。如於憑證到期後辦理換發作業，應依據本章節第一段之規定辦理。但辦理上述線上換發作業僅限1次，如再次使用期限屆滿應依據本章節第一段之規定辦理。

3.2.3 個人身分之鑑別程序

用戶於逕行發證收到憑證 IC 卡進行憑證接受作業時，註冊中心將以事業主體負責人個人身分證號碼及其民國年出生年月日作為事業申請憑證之身分鑑別依據。如逕行發證需至註冊窗口領取，將以事業主體負責人個人身分證正本以及受託人身分證正本作為事業主體領取憑證之身分鑑別依據。

當已完成事業主體登記之用戶使用事業主體之負責人自然人憑證，以線上申辦方式申請憑證時，註冊中心須驗證事業主體負責人自然人憑證之數位簽章，並確認該負責人是否具代表該事業主體之資格，以鑑別事業主體之身分。

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

用戶申請憑證時，應依 3.2.2 節與 3.2.3 節規定辦理身分鑑別。

3.2.6 交互運作標準

不適用。

3.2.7 資通訊設備或伺服器應用軟體鑑別之程序

不適用。

3.2.8 網域名稱擁有者鑑別之程序

不適用。

3.3 金鑰更換請求之識別及鑑別

3.3.1 例行性金鑰更換識別及鑑別

憑證之金鑰更換係指簽發1張與舊憑證具有相同特徵及保證等級的新憑證，而新的憑證除有新的、不同的公開金鑰（對應新的、不同的私密金鑰）及不同的序號外，亦可能被指定不同的有效期限。

當用戶之私密金鑰使用期限屆滿必須更換金鑰時，應向本管理中心辦理換發憑證作業。其中，正卡憑證得於該憑證到期前2個月內辦理申請，亦得以私密金鑰於線上辦理申請。註冊中心將依照3.2節規定，對於申請換發憑證之用戶進行識別及鑑別。

3.3.2 憑證廢止之金鑰更換識別及鑑別

如用戶私密金鑰因憑證廢止必須更換金鑰時，應向本管理中心重新申請憑證，註冊中心將依照3.2節規定，對於重新申請憑證之用戶進行識別及鑑別。

3.3.3 憑證展期之金鑰更換

本管理中心簽發之用戶憑證不得展期。

3.4 憑證廢止申請之識別及鑑別

憑證廢止申請之鑑別程序與3.2節規定相同。

3.5 憑證暫時停用與恢復使用之識別及鑑別

申請人提出憑證暫時停用或恢復使用申請時，註冊中心系統將以用戶輸入之用戶代碼鑑別其身分。

4.憑證生命週期營運規範

4.1 申請憑證

4.1.1 憑證之申請者

憑證申請者即為1.3.3節用戶授權之人員。

4.1.2 註冊程序及責任

憑證申請者申請憑證時應提供正確資料及身分識別相關文件，註冊中心應確實進行憑證申請者身分鑑別。

用戶責任如下：

(1) 遵守本作業基準及用戶約定條款，並確保所提供申請資料之正確性。

(2) 確認憑證內容資訊之正確性，並依 4.4 節規定辦理憑證接受；若憑證內容資訊不正確，應立即通知本管理中心

(3) 依 1.4.1 節規定使用憑證。

(4) 妥善保管與使用其私密金鑰。

(5) 憑證如須暫時停用、恢復使用、廢止或重發，應依照第 4 章規定辦理，用戶仍應承擔憑證異動前所有使用該憑證之法律責任。

(6) 用戶應確保其電腦環境與應用系統之安全性。

(7) 本管理中心如因故無法正常運作時，用戶應儘速尋求其他途

徑完成與他人應為之法律行為，不得以本管理中心無法正常運作，做為抗辯他人之事由。

4.2 申請憑證之程序

用戶之憑證申請資料，本管理中心及註冊中心將依本作業基準之規定妥善保管。

(1) 申請發證

A. 用戶以紙本憑證申請書提交 IC 卡正卡或非 IC 卡類憑證申請予憑證註冊窗口，程序如下：

(A) 憑證申辦人連線至本管理中心網站，閱讀用戶約定條款（Subscriber Agreement），如同意條款內容則填寫憑證申請書，並設定用戶代碼。

(B) 完成費用繳納後列印憑證申請書，並於憑證申請書上蓋用事業主體之印鑑及代表該事業主體負責人之印鑑，印鑑必須與該事業主體登記設立所使用的印鑑章相符。

(C) 憑證申辦人將憑證申請書，送交該事業主體登記設立主管機關所設的憑證註冊窗口辦理。

B. 用戶以事業主體負責人自然人憑證申請 IC 卡正卡或非 IC 卡類憑證，程序如下：

(A) 憑證申辦人連線至本管理中心網站，閱讀用戶約定條

款（Subscriber Agreement），如同意條款內容則填寫憑證申請書，並設定用戶代碼

(B) 以事業主體負責人自然人憑證對非 IC 卡或 IC 卡正卡之憑證申請資料加簽數位簽章後，將相關資料上傳至註冊中心並完成費用繳納。

C. 用戶以 IC 卡正卡申請 IC 卡附卡、一站式專屬授權憑證或換發 IC 卡正卡，程序如下：

(A) 憑證申辦人連線至本管理中心網站，閱讀用戶約定條款（Subscriber Agreement），如同意條款內容則填寫憑證申請書，IC 卡須設定用戶代碼。

(B) 以 IC 卡正卡對 IC 卡附卡、一站式專屬授權憑證或 IC 卡正卡之憑證申請資料加簽數位簽章後，將相關資料上傳至註冊中心並完成費用繳納。

(2) 逕行發證

本管理中心為因應政策而主動簽發之憑證，於用戶完成 4.4 節更改用戶代碼及設定 PIN 碼時，視為完成申請作業。

(3) 申請設立專屬用戶憑證

A. 憑證申辦人連線至本管理中心網站，閱讀用戶約定條款（Subscriber Agreement），如同意條款內容則填寫憑證申請書。

B. 確認來自「公司與商業及有限合夥一站式線上申請作業」之預查資料無誤後，將相關資料上傳至註冊中心。

4.2.1 執行識別及鑑別功能

本管理中心或註冊中心在收到憑證申請資料後，應依本作業基準第3章規定，依申請方式進行以下審核程序，以作為判定是否同意簽發憑證之依據。

(1) 申請發證

A. 用戶以紙本憑證申請書提交 IC 卡正卡或非 IC 卡類憑證申請予憑證註冊窗口，程序如下：

(A) 憑證註冊審驗人員比對憑證申請書上的印鑑章與該事業主體辦理登記設立之印鑑章是否相符，確認憑證申請書上印鑑章的真偽。

(B) 憑證註冊審驗人員查詢該事業主體正式登記名稱及其統一編號，確定該事業主體具有申請憑證資格(解散、撤銷、廢止、破產登記或歇業之事業主體不能申請)。

(C) 憑證註冊審驗人員檢查憑證申請書之資料，如資料正確無誤，將使用該 RAO IC 卡對申請資料加簽數位簽章後，將相關資訊上傳至註冊中心。

B. 用戶以事業主體負責人自然人憑證申請IC卡正卡或非IC卡類憑證，程序如下：

註冊中心須驗證事業主體負責人自然人憑證之數位簽章，確認該負責人是否具代表該事業主體之資格，並確定該事業主體具有申請憑證資格。

C. 用戶以 IC 卡正卡申請憑證 IC 附卡、一站式專屬授權憑證或換發 IC 卡正卡，程序如下：

註冊中心以驗證正卡之數位簽章的方式進行，並確定該事業主體具有申請憑證資格。

(2) 逕行發證

本管理中心將依據事業主體設立登記資料將符合憑證發放資格（具有實際營運事實之事業主體）之資料交由發卡中心進行發卡作業。

(3) 申請設立專屬用戶憑證

註冊中心以比對「公司與商業及有限合夥一站式線上申請作業」之預查資料的方式進行。

4.2.2 憑證申請之核准或拒絕

本管理中心完成申請資料審核、身分識別及鑑別作業後，始可核准憑證申請。

本管理中心於以下狀況得拒絕簽發憑證：

(1) 未能通過第 3 章之要求。

(2) 申請者曾違反用戶約定條款。

(3) 其他經本管理中心認定得拒絕簽發之事項。

4.2.3 處理憑證申請之時間

註冊中心處理憑證申請之時間及本管理中心簽發憑證之時間，視不同憑證類別於用戶約定條款、相關文件或網站揭露。

4.3 簽發憑證程序

4.3.1 本管理中心於憑證簽發時之作業

本管理中心與註冊中心核准憑證申請後，即進行簽發程序。

4.3.1.1 申請發證

依用戶使用之符記不同分成以下簽發程序：

(1) 用戶使用符記為 IC 卡

IC 卡申請資料將交由本管理中心所信賴的發卡中心進行發卡作業，發卡作業包括：

A. IC 卡內部產製金鑰對

B. 亂數設定 IC 卡之初始 PIN 碼

C. 將申請資料及公開金鑰透過安全管道傳送給本管理中心簽發憑證並寫入 IC 卡中。

D. IC 卡印製、包裝並郵寄至該事業主體之登記地。

(2) 用戶使用符記為非 IC 卡類

憑證申請資料將由本管理中心簽發憑證。

(3)「一站式專屬授權憑證」與「設立專屬用戶憑證」

待本管理中心簽發憑證後，將私密金鑰及憑證以用戶設定之密碼

加密封裝為 PKCS#12 之個人資訊交換檔案格式供用戶使用。

4.3.1.2 逕行發證

逕行發證之發卡作業比照 4.3.1.1 節 IC 卡符記之方式辦理。惟發卡中心負責將 IC 卡以掛號以上安全等級方式郵寄予事業主體，或由註冊窗口發送予事業主體負責人或其受託人。

(1) 由註冊窗口發送 IC 卡時，應由事業主體負責人或其受託人攜帶領取通知書（包含事業主體正式登記名稱、統一編號及聯絡人資料等）於領取單上蓋用事業主體暨負責人之印鑑章（與事業主體登記時所使用之印鑑章相符）並攜帶負責人身分證正本以及受託人身分證正本向註冊窗口領取 IC 卡。

(2) 若以郵寄方式寄送 IC 卡時，應由事業主體負責人、受僱人或受託人簽收。如 IC 卡因故無法送達事業主體，將退回予發卡中心。本管理中心將由發卡中心將事業主體 IC 卡寄送至註冊窗口，並由發卡中心重新寄發領取通知書通知事業主體，事業主體負責人或其受託人必須攜帶領取通知書（包含事業主體正式登記名稱、統一編號及聯絡人資料等）於領取單上蓋用事業主體暨負責人之印鑑章（與事業主體登記時所使用之印鑑章相符）並攜帶負責人身分證正本以及受託人身分證正本至註冊窗口領取 IC 卡。

(3) 事業主體依上開方式取得 IC 卡後，應依據 4.4 節更改用戶代碼及設定 PIN 碼。

4.3.2 本管理中心對用戶之憑證簽發通知

(1) IC 卡簽發後，發卡中心以郵寄方式交予用戶。逕行發證時亦可依 4.3.1.2 節發送。

(2) 非 IC 卡類(包含一站式專屬授權憑證及設立專屬用戶憑證)簽發後，以電子郵件方式通知用戶。

(3) 用戶可於憑證管理中心網站查詢憑證申請進度。

(4) 用戶以紙本憑證申請書申請發證時，註冊窗口亦需以公文書方式通知用戶審核結果。

(5) 用戶以事業主體負責人自然人憑證或 IC 卡正卡申請發證時，如不同意簽發憑證，應以電子郵件通知用戶，並明確告知不同意簽發之理由。

4.4 接受憑證之程序

(1) 申請發證

A. 用戶使用符記為 IC 卡時，接受憑證程序如下：

(A) 申請憑證之用戶在收到 IC 卡後，應連線至本管理中心網站，進行憑證接受作業。

(B) 在進行 IC 卡憑證接受作業時，用戶應檢查憑證內容，如資料正確無誤，則輸入申請憑證時所設定之用戶代

碼，以執行接受憑證作業，並設定 IC 卡的 PIN 碼，如用戶發現憑證內容不正確，則應停止憑證接受作業。

B. 用戶申請非 IC 卡類憑證時，接受憑證程序如下：

(A) 申請憑證之用戶在收到憑證接受通知電子郵件後，應檢查電子郵件中所列憑證內容是否正確，並連線至本管理中心網站進行憑證接受作業。

(B) 用戶須於本管理中心憑證接受作業中輸入憑證序號及申請憑證時所設定之用戶代碼，以執行憑證接受作業；如用戶發現憑證內容不正確，則應停止憑證接受作業。

C. 用戶申請「一站式專屬授權憑證」或「設立專屬用戶憑證」時，於 4.2 節之申請過程中，須先行確認申請資料及接受將簽發之憑證內容後始可送出申請。

(2) 逕行發證

逕行發證之用戶完成 IC 卡重設用戶代碼作業即表示同意接受憑證，相關程序如下：

A. 用戶連線至本管理中心網站，閱讀用戶約定條款，用戶插入 IC 卡，顯示憑證內容。

B. 由用戶確認憑證內容無誤後，輸入預設之用戶代碼，即事業主體負責人身分證字號及其民國年出生年月日，同時立即變更用戶代碼，以變更後之用戶代碼設定 PIN 碼，並填寫聯絡人之電子郵件，以供本管理中心作為通知之用。如

用戶發現憑證內容不正確，則應停止憑證接受作業。

(3)用戶完成憑證接受作業後，所簽發的憑證將會公布至儲存庫中。

4.4.1 接受憑證之要件

(1)用戶申請 IC 卡或非 IC 卡類

用戶確認憑證內容無誤後，以申請憑證時所設定之用戶代碼做為憑證接受之依據。

(2)用戶申請一站式專屬授權憑證

用戶須先行確認申請資料及接受將簽發之憑證內容後始可以 IC 卡正卡之數位簽章送出申請，以此數位簽章做為憑證接受之依據。

(3)用戶申請「設立專屬用戶憑證」

用戶須先行確認申請資料及接受將簽發之憑證內容後始可送出申請，以此申請紀錄做為憑證接受之依據。

4.4.2 本管理中心之憑證發布

本管理中心將所簽發之憑證公布於儲存庫，或以郵遞方式將憑證傳遞用戶。

4.4.3 本管理中心對其他個體之憑證簽發通知

本管理中心將所簽發之憑證公布於儲存庫。

4.5 金鑰對與憑證之用途

4.5.1 用戶私密金鑰及憑證使用

(1)用戶金鑰對之產製應符合 6.1.1 節規定，且用戶須有私密金

鑰之控制權。

(2) 用戶私密金鑰不得用於簽發憑證。

(3) 用戶應保護私密金鑰不被未經授權之他人使用或揭露，且確保私密金鑰依憑證擴充欄位所註記之金鑰用途使用。

(4) 用戶須依憑證政策及本作業基準之規定使用憑證。

4.5.2 信賴憑證者公開金鑰及憑證使用

(1) 信賴憑證者使用憑證時須符合本作業基準規定。

(2) 信賴憑證者應使用符合 ITU-T X.509、IETF RFC 5280 等相關標準所規範的憑證串鏈檢驗方法驗證憑證有效性，包括憑證及其憑證串鏈中所有憑證機構之憑證。

(3) 信賴憑證者應檢驗簽發憑證機構與用戶憑證之憑證政策，以確認憑證之保證等級。

(4) 信賴憑證者應確認憑證用途。

4.6 憑證展期

本管理中心不提供憑證展期。

4.6.1 憑證展期之事由

不適用。

4.6.2 憑證展期之申請者

不適用。

4.6.3 憑證展期之程序

不適用。

4.6.4 對用戶憑證展期之簽發通知

不適用。

4.6.5 接受展期憑證之要件

不適用。

4.6.6 憑證機構之展期憑證發布

不適用。

4.6.7 本管理中心對其他個體之展期憑證簽發通知

不適用。

4.7 憑證之金鑰更換

重新產生一組公開金鑰及私密金鑰對，並以原有的註冊資訊向憑證機構申請憑證簽發。

4.7.1 憑證之金鑰更換事由

(1) 本管理中心憑證之金鑰更換

A. 私密金鑰執行簽發憑證用途之使用期限到期。

B. 本管理中心憑證被廢止。

(2) 用戶憑證之金鑰更換

A. 用戶私密金鑰使用期限到期。

B. 用戶憑證被廢止。

4.7.2 更換憑證金鑰之申請者

(1) 本管理中心憑證之金鑰更換

由本管理中心授權之人員向總管理中心提出下屬憑證機構憑證之申請。

(2) 用戶憑證之金鑰更換

憑證申請者為 1.3.3 節用戶授權之人員。

4.7.3 憑證之金鑰更換程序

(1) 本管理中心憑證之金鑰更換

依總管理中心之憑證實務作業基準相關規定重新申請憑證。

(2) 用戶憑證之金鑰更換

依 4.1 節及 4.2 節規定辦理。

4.7.4 用戶憑證金鑰更換之簽發通知

依 4.3.2 節規定辦理。

4.7.5 接受憑證金鑰更換之要件

(1) 本管理中心憑證之金鑰更換

依總管理中心之憑證實務作業基準 4.7 節相關規定接受金鑰更換之憑證。

(2) 用戶憑證之金鑰更換

依 4.4.1 節規定接受金鑰更換之憑證。

4.7.6 本管理中心之更換金鑰憑證發布

本管理中心將已完成金鑰更換之憑證公布於儲存庫，或以電子郵件、郵遞方式將憑證傳遞用戶。

4.7.7 本管理中心更換金鑰後對其他個體之通知

本管理中心將金鑰更換後之憑證公布於儲存庫。

4.8 憑證變更

本管理中心不提供憑證變更。

變更主體名稱等重要身分資料不屬憑證變更，用戶須重新申請憑證，且舊憑證須廢止。

4.8.1 憑證變更之事由

不適用。

4.8.2 憑證變更之申請者

不適用。

4.8.3 憑證變更之程序

不適用。

4.8.4 對用戶憑證變更之簽發通知

不適用。

4.8.5 接受憑證變更之要件

不適用。

4.8.6 本管理中心之憑證變更發布

不適用。

4.8.7 本管理中心對其他個體之憑證簽發通知

不適用。

4.9 憑證暫時停用及廢止

本管理中心提供憑證暫時停用及廢止服務。設立專屬用戶憑證不得暫時停止使用與恢復使用。

4.9.1 廢止憑證之事由

用戶在以下情況時(但不限)必須向註冊中心提出廢止憑證申請:

(1) 私密金鑰遭到破解。

(2) 憑證不再需要使用。

另外，本管理中心得就下列情形逕行廢止憑證，毋須事先經過用戶同意：

(1) 確認憑證記載之內容不實。

(2) 確認用戶之簽章用私密金鑰遭冒用、偽造或破解。

(3) 確認本管理中心之私密金鑰或系統遭冒用、偽造或破解，足以影響憑證之信賴度。

(4) 確認公司或有限合夥已被宣告破產、辦理解散、合併解散、撤銷或廢止登記；分公司或有限合夥分支機構撤銷或廢止；外國公司撤回、撤銷或廢止認許；商業歇業、撤銷。

(5) 確認用戶已變更名稱或統一編號。惟商業憑證用戶名稱所冠縣市名因縣市改制而改變者，不在此限。

(6) 確認用戶之憑證未依本作業基準規定之程序簽發。

(7) 確認用戶違反本作業基準或相關法令規定。

(8) 依據司法機關、監察機關或治安機關之通知。

(9) 依用戶登記設立機關或是目的事業主管機關之通知。

(10) 確認準公司與準有限合夥之預查名稱已不具備辦理設立登記申請資格。

其他因本管理中心終止服務廢止憑證，依照 5.8 節規定辦理。

4.9.2 憑證廢止之申請者

(1) 將廢止憑證之用戶。

(2) 事業主體登記設立機關或是目的事業主管機關。

4.9.3 憑證廢止之程序

(1) 用戶以紙本申請書提出憑證廢止申請時，其程序如下：

A. 憑證申辦人連線至本管理中心網站，下載並填寫憑證廢止申請書。

B. 列印憑證廢止申請書，並於憑證廢止申請書上蓋用事業主體之印鑑及代表該事業主體負責人之印鑑，印鑑必須與該事業主體登記設立所使用的印鑑章相符。

C. 憑證申辦人將憑證廢止申請書，送交該事業主體登記設立主管機關所設的憑證註冊窗口辦理。

D. 憑證註冊審驗人員比對憑證廢止申請書上的印鑑章與該事業主體辦理登記設立之印鑑章是否相符，確認憑證廢止申請書上印鑑章的真偽。

E. 憑證註冊審驗人員檢查憑證廢止申請書之資料，如資料正確無誤，將使用該 RAO IC 卡對憑證廢止申請資料加簽數位簽章後，將相關資料上傳至註冊中心，並以公文書方式通知用戶審核結果。

F. 經憑證註冊審驗人員檢查通過之憑證廢止申請資料，將由本管理中心進行廢止該憑證並以電子郵件通知用戶，不影響該用戶其他憑證的有效性。

(2) 用戶以 IC 卡正卡或負責人自然人憑證提出憑證廢止申請時，其程序如下：

A. 憑證申辦人連線至本管理中心網站，填寫憑證廢止申請書。

B. 以 IC 卡正卡或負責人自然人憑證對憑證廢止申請資料加簽數位簽章後，將資料上傳至註冊中心。

C. 註冊中心鑑別事業主體身分之方式為驗證 IC 卡正卡之數位簽章，或是驗證負責人自然人憑證之數位簽章，並確認

該負責人是否具代表該事業主體之資格。

D. 由本管理中心進行廢止該憑證並以電子郵件通知用戶，不影響該用戶其他憑證的有效性。

(3) 用戶提出「設立專屬用戶憑證」廢止時，其程序如下：

A. 憑證申辦人連線至本管理中心網站，以預查編號及用戶代碼填寫憑證廢止申請書。

B. 註冊中心與「公司與商業及有限合夥一站式線上申請作業」比對資料，鑑別事業主體身分。

C. 由本管理中心進行廢止該憑證並以電子郵件通知用戶，不影響該用戶其他憑證的有效性。

(4) 事業主體登記設立機關或是目的事業主管機關提出憑證廢止申請時，其程序如下：

A. 憑證註冊窗口之憑證註冊審驗人員查詢事業主體相關登記資料，確認事業主體已解散、歇業或其他應廢止憑證之狀況。

B. 憑證註冊審驗人員對由事業主體相關登記系統觸發之憑證廢止申請資料，如資料正確無誤，將使用該 RAO IC 卡對憑證廢止申請資料加簽數位簽章後，將相關資料上傳至註冊中心。

C. 經憑證註冊審驗人員檢查通過之憑證廢止申請資料，將由本管理中心進行憑證廢止，該用戶所有未過期憑證全部廢

止。

如以上之廢止申請審核不通過時，本管理中心將拒絕廢止該憑證。憑證廢止申請審核通過後，本管理中心將於 1 個工作天內完成憑證廢止作業。

4.9.4 憑證廢止申請之寬限期

憑證廢止事由經確認後必須提出憑證廢止申請的時間。本管理中心本身之憑證須廢止時，須於 1 小時內通報總管理中心。

4.9.5 本管理中心處理憑證廢止請求之處理期限

憑證廢止申請，註冊中心應儘速處理並最多於 3 個工作天內完成憑證廢止審核。審核通過後，本管理中心將於 1 個工作天內完成憑證廢止作業。

4.9.6 信賴憑證者檢查憑證廢止之要求

信賴憑證者使用本管理中心所簽發之憑證前，應先檢驗本管理中心公布之憑證廢止清冊或線上憑證狀態協定回應訊息，以確認該憑證之有效性及憑證串鏈之正確性。

4.9.7 憑證廢止清冊簽發頻率

(1) 憑證廢止清冊每日至少簽發 1 次，其有效期限不超過 36 小時。

(2) 本管理中心於完成憑證廢止作業後的 24 小時內須重新簽發憑證廢止清冊。

4.9.8 憑證廢止清冊發布之最大延遲時間

本管理中心最遲於憑證廢止清冊所記載之下次更新時間前發布下一次之憑證廢止清冊。

4.9.9 線上憑證廢止/狀態查驗之服務

(1) 本管理中心提供憑證查詢與下載、憑證廢止清冊及線上憑證狀態協定查詢服務。

(2) 本管理中心由線上憑證狀態協定回應伺服器(OCSP Responder)提供符合 RFC 6960 及 RFC 5019 標準規範的線上憑證狀態協定回應訊息。

(3) 本管理中心簽發線上憑證狀態協定回應伺服器之憑證其安全強度條件如下：

A. 金鑰長度至少為 RSA 2048 位元

B. 使用 SHA-256 或相同安全等級之雜湊函數演算法

(4) 線上憑證狀態協定回應伺服器之憑證須包含符合 RFC 6960 規範之擴充欄位「id-pkix-ocsp-nocheck」。

4.9.10 線上憑證廢止查驗之規定

(1) 信賴憑證者須以憑證廢止清冊或線上憑證狀態協定查詢服務驗證憑證之有效性。

(2) 本管理中心線上憑證狀態協定回應伺服器至少可支援符合 RFC 6960 及 RFC 5019 標準規範所述之 HTTP GET 方法。

(3) 線上憑證狀態協定查詢服務至少每 4 天更新 1 次憑證狀態資

訊，其線上憑證狀態協定回應訊息最大效期為 10 個工作天。

4.9.11 其他形式廢止公告

本管理中心不另提供其他形式之廢止公告。

4.9.12 金鑰被破解時之其他特殊規定

依照 4.9.1、4.9.2 及 4.9.3 節的規定辦理。

4.9.13 暫時停用憑證之事由

(1) 用戶在以下兩種情形得申請憑證暫時停用：

A. 憑證金鑰對之符記遺失或遭盜用時。

B. 自行認定必須申請憑證暫時停用。

(2) 本管理中心得就以下情形逕行暫時停用憑證，毋須事先經過用戶同意：

A. 事業主體用戶遭停業時。

B. 依用戶登記設立機關或是目的事業主管機關之通知。

C. 依據司法機關、監察機關或治安機關之通知。

D. 用戶申請發證後，未於簽發憑證之日起一年半內完成憑證接受作業。本作業基準修正前已簽發且未廢止之憑證亦適用之。

E. 逕行發證時，用戶未於該次逕行發證最後簽發憑證之日起

一年半內完成憑證接受作業。

4.9.14 暫時停用憑證之申請者

以下兩者可做為暫時停用憑證之申請者：

(1) 將暫時停用憑證之用戶。

(2) 用戶登記設立機關或是目的事業主管機關。

4.9.15 暫時停用憑證之程序

(1) 用戶提出憑證暫時停用申請，其程序如下：

A. 用戶使用符記為 IC 卡：

(A) 用戶連線至本管理中心網站，填寫 IC 卡卡號及用戶代碼線上辦理暫時停用憑證申請。

(B) 註冊中心伺服器檢驗該 IC 卡卡號及用戶代碼正確無誤後，加簽數位簽章上傳至本管理中心。

(C) 本管理中心檢驗註冊中心之數位簽章後，進行暫時停用憑證作業，此作業只將該 IC 卡之憑證暫時停用，不影響該用戶其他憑證 IC 卡的有效性。

B. 用戶使用符記為非 IC 卡類：

(A) 用戶連線至本管理中心網站，填寫憑證序號及用戶代碼線上辦理暫時停用憑證申請。

(B) 註冊中心伺服器檢驗該憑證序號及用戶代碼正確無誤後，加簽數位簽章上傳至本管理中心。

(C) 本管理中心檢驗註冊中心之數位簽章後，進行暫時停用憑證作業。

(2) 事業主體登記設立機關或是目的事業主管機關提出暫時停用憑證申請時，其程序如下：

A. 憑證註冊窗口之憑證註冊審驗人員查詢事業主體相關登記資料，確認事業主體已停業登記之狀況。

B. 憑證註冊審驗人員對由事業主體相關登記系統觸發之暫時停用憑證申請，如資料正確無誤，將使用該 RAO IC 卡對憑證暫時停用憑證申請資料加簽數位簽章後，將相關資料上傳至註冊中心。

C. 經憑證註冊審驗人員檢查通過之憑證暫時停用申請資料，將由本管理中心進行暫時停用憑證，該用戶所有未過期的憑證全部暫時停用。

如以上暫時停用申請之審核不通過時，則本管理中心將拒絕暫時停用憑證。用戶提出憑證暫時停用申請時，如忘記用戶代碼，則持卡人可以逕赴憑證註冊窗口辦理緊急掛失，經憑證註冊審驗人員確認身分後，由憑證註冊審驗人員代為向本管理中心提出憑證停用申請，並重設用戶代碼。

4.9.16 暫時停用憑證期間之限制

用戶申請暫時停用最長可停用至該憑證到期。

4.9.17 恢復使用憑證之程序

(1) 用戶申請恢復使用憑證（僅限於恢復之前用戶自行上網申請停用之憑證）之程序如下：

A. 連線至本管理中心網站，填寫 IC 卡號（使用符記為 IC 卡時）或憑證序號（使用符記為非 IC 卡類時）及用戶代碼，線上申請恢復使用憑證。

B. 註冊中心檢驗 IC 卡之卡號或憑證序號及用戶代碼正確無誤後，加簽數位簽章上傳至本管理中心。

C. 本管理中心檢驗註冊中心之數位簽章後，進行恢復使用憑證作業，將憑證狀態更改為有效 (Valid)。

(2) 事業主體登記設立機關或是目的事業主管機關提出恢復使用憑證申請時，其程序如下：

A. 憑證註冊窗口之憑證註冊審驗人員查詢事業主體相關登記資料，確認事業主體先前暫時停用之事由已消滅。

B. 憑證註冊審驗人員對由事業主體相關登記系統觸發之恢復使用憑證申請，如資料正確無誤，將使用該 RAO IC 卡對憑證恢復使用憑證申請資料加簽數位簽章後，將相關資料上傳至註冊中心。

C. 經憑證註冊審驗人員檢查通過之憑證恢復使用申請資料，將由本管理中心進行恢復使用憑證，將憑證狀態更改為有

效,但原由用戶自行線上申請暫時停用之憑證將不予恢復使用，依然維持其停用狀態。

(3)逕行發證

逕行發證之用戶未能於該次逕行發證最後完成製卡之日（目前為98 年 10 月 31 日）或申請發證之用戶未能於簽發憑證後一年半內完成接受憑證作業而停用者，用戶申請恢復之程序，應填寫申請書申請恢復使用憑證。

如以上恢復使用憑證申請審核不通過時,本管理中心或註冊中心將拒絕恢復使用憑證。

4.10 憑證狀態服務

4.10.1 服務特性

憑證廢止清冊或線上憑證狀態協定回應訊息中之憑證廢止資訊，須至該被廢止之憑證已過期後始可移除。

4.10.2 服務可用性

(1) 本管理中心提供全天候(7 x 24)不中斷之儲存庫服務，憑證狀態查詢服務之回覆時間須在 10 秒內。

(2)儲存庫服務無法正常運作時，須於 2 個工作天內恢復正常運作。

4.10.3 可選功能

不予規定。

4.11 終止服務

憑證用戶不再使用本管理中心之服務；本管理中心同意用戶終止服務之要件如下：

(1) 憑證到期。

(2) 用戶廢止憑證。

4.12 私密金鑰託管及回復

4.12.1 金鑰託管及回復政策與實務

(1) 本管理中心簽章用之私密金鑰不可被託管。

(2) 本管理中心不提供用戶私密金鑰託管與回復。

4.12.2 通訊用金鑰封裝及回復政策與實務

本管理中心不提供通訊用金鑰封裝與回復。

5.基礎設施、安全管理及作業程序控管

5.1 實體控管

5.1.1 實體位置及結構

本管理中心機房位於台北市信義路 1 段 21 號數據通信大樓內之安全機房，具備門禁、保全、入侵偵測及監視錄影等實體安全機制。

5.1.2 實體存取

(1) 本管理中心之實體控管符合保證等級第 3 級規定，包含：

A. 大門及大樓警衛。

B. 進出管制系統。

C. 指紋辨識系統。

D. 機箱監控系統。

(2) 可攜式儲存媒體須檢查並確認無電腦病毒及惡意軟體。

(3) 非授權人員進出機房時，須填寫進出紀錄，並由本管理中心人員全程陪同。

5.1.3 電力及空調

(1) 機房之電力系統包括市電、發電機(滿載油料可連續運轉 6 天)及不斷電系統，可提供至少 6 小時以上備用電力。

(2) 機房設有恆溫恆濕空調系統。

5.1.4 水災防範及保護

機房位於建築物第 3 樓層(含)以上，具備防水閘門及抽水機。

5.1.5 火災防範及保護

機房具備自動偵測火災預警功能，系統可自動啟動滅火設備，並於各機房主要出入口設置手動開關。

5.1.6 媒體儲存

稽核紀錄、歸檔及備援資料，除儲存 1 份於主機房外，另將複製 1 份送至異地備援場所儲存。

5.1.7 汰換設備處理

儲存重要資料之媒體不再使用時，須依政府機關資安規定或其他經經濟部同意之方式辦理銷毀作業。

5.1.8 異地備援

(1) 異地備援地點位於臺中，與主機房距離 30 公里以上。

(2) 備援內容包括資料及系統程式，資料備份至少 1 個月執行 1 次。

(3) 異地備援系統與主系統具相同之安全等級。

5.2 程序控制

各信賴角色依工作內容進行識別及鑑別，以確保作業程序之安全。

5.2.1 信賴角色

(1)信賴角色分為管理員、簽發員、稽核員、維運員及實體安全控管員，工作內容說明如下：

A. 管理員：

(A)安裝、設定及維護本管理中心系統。

(B)建立及維護本管理中心系統之使用者帳號。

(C)設定稽核參數。

(D)產製及備份本管理中心之金鑰。

B. 簽發員：

(A)啟動或停止憑證簽發服務。

(B)啟動或停止憑證廢止服務。

C. 稽核員：

(A)對稽核紀錄之查驗、維護及歸檔。

(B)執行或監督內部稽核，以確認本管理中心運作是否遵照本作業基準的規定。

D. 維運員：

(A)系統及設備之運作維護。

(B)系統備份作業。

(C)儲存媒體之更新。

(D)憑證管理系統外之軟硬體更新。

(E) 網路維護及系統安全與病毒防護機制及網路安全事件的偵測與通報等。

E. 實體安全控管員：系統之實體安全控管。

(2) 信賴角色依 5.3 節規定進行人員控管。

(3) 各信賴角色可由多人擔任，並設有 1 名主管。

5.2.2 工作內容所需人數

各信賴角色所需之人數如下：

(1) 管理員：至少 3 位。

(2) 簽發員：至少 3 位。

(3) 稽核員：至少 2 位。

(4) 維運員：至少 2 位。

(5) 實體安全控管員：至少 2 位。

每個任務所需之人數說明如下：

任務名稱	管理員	簽發員	稽核員	維運員	實體安全控管員
安裝、設定和維護本管理中心憑證管理系統	2				1
建立和維護本管理中心憑證管理系統之使用者帳號	2				1
設定稽核參數	2				1

任務名稱	管理員	簽發員	稽核員	維運員	實體安全控管員
產製和備份本管理中心之金鑰	2		1		1
啟動或停止憑證簽發服務		2			1
啟動或停止憑證廢止服務		2			1
對稽核紀錄的查驗、維護和歸檔			1		1
系統設備的日常運作維護				1	1
系統的備援及復原作業				1	1
儲存媒體的更新				1	1
除本管理中心憑證管理系統外之軟硬體更新				1	1
網路和網站的維護				1	1
設定系統的實體安全控管					2

5.2.3 角色識別及鑑別

(1) 以使用者帳號、密碼及 IC 卡等，識別及鑑別管理員、簽發員、稽核員及維運員。

(2) 以中央門禁系統，識別及鑑別實體安全控管員。

5.2.4 角色權責劃分

各角色分派須符合規定如下：

(1) 管理員、簽發員及稽核員不得相互兼任。

(2) 實體安全控管員不得兼任其他信賴角色。

(3) 不允許執行自我稽核。

5.3 人員控管

5.3.1 身家背景、資格、經驗及安全需求

(1) 人員甄選及進用前須進行安全評估。

(2) 人員須定期進行考核管理。

(3) 人員須定期進行教育訓練。

(4) 人員應遵守並簽訂保密切結。

5.3.2 身家背景之查驗程序

(1) 本管理中心工作人員，須由本管理中心及人事相關部門主管依各信賴角色之資格執行實務、經歷及身分背景審查。

(2) 每年依各信賴角色之職務特性，執行實務與經歷之審查，確認是否適任。

5.3.3 教育訓練需求

各信賴角色之教育訓練需求如下：

信賴角色	教育訓練需求
管理員	1、本管理中心之安全驗證機制。 2、本管理中心安裝、設定和維護之操作程序。 3、建立和維護系統之用戶帳號操作程序。 4、設定稽核參數操作程序。 5、產製和備份本管理中心之金鑰操作程序。 6、災後復原及業務永續經營之程序。
簽發員	1、本管理中心之安全驗證機制。 2、本管理中心系統軟硬體的使用及操作程序。 3、憑證簽發操作程序。 4、憑證廢止操作程序。

信賴角色	教育訓練需求
	5、災後復原及業務永續經營之程序。
稽核員	1、本管理中心之安全驗證機制。 2、本管理中心系統軟硬體的使用及操作程序。 3、產製和備份本管理中心之金鑰操作程序。 4、稽核紀錄的查驗、維護和歸檔程序。 5、災後復原及業務永續經營之程序。
維運員	1、本管理中心之安全驗證機制。 2、系統設備的日常運作維護程序。 3、儲存媒體之更新程序。 4、災後復原及業務永續經營之程序。 5、網路和網站的維護程序。
實體安全控管員	1、設定實體門禁權限程序。 2、災後復原以及業務永續經營之程序。

5.3.4 人員再教育訓練之需求及頻率

(1) 各信賴角色每年進行 1 次教育訓練。

(2) 軟硬體升級、工作程序改變、設備更換或相關法規改變時。

5.3.5 工作調換之頻率及順序

(1) 管理員調離原職務滿 1 年後，方可轉任簽發員或稽核員。

(2) 簽發員調離原職務滿 1 年後，方可轉任管理員或稽核員。

(3) 稽核員調離原職務滿 1 年後，方可轉任管理員或簽發員。

(4) 維運員已接受相關教育訓練及通過審核並任職滿兩年方可轉任管理員、簽發員或稽核員。

5.3.6 未授權行動之懲處

人員如違反相關規定，應接受適當之管理及懲處，如情節重大致

造成損害者，本管理中心得採取法律行動追究其責任。

5.3.7 聘僱人員之規定

聘僱人員須簽訂保密協定，並依規定進行作業。

5.3.8 提供之文件資料

本管理中心提供之文件包括憑證政策、技術規範、本作業基準、系統操作手冊及電子簽章法等相關文件。

5.4 稽核記錄程序

(1) 安全相關事件均保存安全稽核紀錄(Audit Log)，且於執行稽核時可立即取得。

(2) 安全稽核紀錄可為系統自動產生或人工紙本紀錄方式。

5.4.1 事件記錄之類型

(1) 安全稽核

A. 重要稽核參數之改變。

B. 嘗試刪除或修改稽核紀錄。

(2) 識別及鑑別

A. 嘗試設定新角色。

B. 調整身分鑑別嘗試之最高容忍次數。

C. 登入系統失敗。

D. 帳號解鎖。

E. 改變系統之身分鑑別機制。

(3) 本管理中心產製金鑰時(不包括單次使用之金鑰產製)。

(4) 本管理中心私密金鑰之存取

(5) 公開金鑰之新增、刪除及儲存

(6) 除單次使用之金鑰外，其餘私密金鑰之匯出。

(7) 憑證註冊、廢止及狀態改變之申請過程。

(8) 安全相關之組態設定改變。

(9) 帳號之新增、刪除及存取權限修改

(10) 憑證格式剖繪之改變

(11) 憑證廢止清冊格式剖繪之改變

(12) 本管理中心之伺服器設定改變

(13) 實體存取及場所之安全

(14) 異常事件

(15) 其他

A. 安裝作業系統。

B. 安裝本管理中心系統。

C. 安裝硬體密碼模組。

D. 移除硬體密碼模組。

E. 銷毀硬體密碼模組。

F. 啟動系統。

G. 嘗試登入本管理中心的憑證管理作業。

H. 硬體及軟體之接收。

I.嘗試設定通行密碼。

J. 嘗試修改通行密碼。

K. 本管理中心之內部資料備份。

L. 本管理中心之內部資料回復。

M. 檔案操作（例如產生、重新命名及移動等）。

N. 傳送任何資訊到儲存庫公布。

O. 存取本管理中心之內部資料庫。

P. 任何憑證被破解之申告。

Q. 憑證載入符記。

R. 符記之傳遞。

S. 符記之零值化。

T. 本管理中心之金鑰更換。

5.4.2 紀錄處理頻率

本管理中心每月檢視 1 次稽核紀錄，並追蹤調查重大事件。

5.4.3 稽核紀錄保留期限

稽核紀錄至少保留 6 個月，保留期限屆滿時，由稽核員移除資料，不可由其他人員代理。

5.4.4 稽核紀錄之保護

(1) 使用簽章、加密技術保存之稽核紀錄，應使用無法更改或刪除紀錄之媒體儲存。

(2) 簽署事件紀錄之私密金鑰不可使用於其他用途。

(3) 稽核系統之私密金鑰應有安全保護措施。

(4) 稽核紀錄須存放於安全場所。

5.4.5 稽核紀錄備份程序

(1) 電子式稽核紀錄每月備份 1 次。

(2) 稽核系統以每日、每星期及每月等週期將稽核紀錄自動歸檔。

5.4.6 稽核紀錄彙整系統

稽核紀錄彙整系統內建於本管理中心之系統，稽核程序於管理中心系統啟動時啟用。

自動稽核系統如無法正常運作，且系統資料處於高風險狀態時，本管理中心將暫停憑證簽發服務，直至問題解決後再行提供服務。

5.4.7 對引起事件者之告知

稽核系統不需告知引起事件之個體，其引發之事件已被系統紀錄。

5.4.8 弱點評估

本管理中心每年進行 1 次風險評鑑，對作業系統、實體設施、憑證管理系統及網路進行評估。

5.5 紀錄歸檔之方法

5.5.1 歸檔紀錄之類型

(1) 本管理中心向總管理中心申請憑證之相關資料。

(2) 憑證實務作業基準。

(3) 重要契約。

(4) 系統或設備組態設定。

(5) 系統或組態設定之修改或更新之內容。

(6) 憑證申請資料。

(7) 廢止申請資料。

(8) 憑證接受之確認紀錄。

(9) 符記啟用紀錄。

(10) 已簽發或公告之憑證。

(11) 本管理中心金鑰更換之紀錄。

(12) 已簽發或公告之憑證廢止清冊。

(13) 稽核紀錄。

(14) 用以驗證及佐證歸檔內容之其他說明資料或應用程式。

(15) 稽核人員所要求之文件。

(16) 依 3.2.2 節及 3.2.3 節所定之組織及個人身分鑑別資料。

5.5.2 歸檔紀錄保留期限

(1) 歸檔紀錄及處理歸檔紀錄之應用程式，其保留期限為 10 年。

(2) 歸檔紀錄逾保留期限後，書面資料應以安全方式銷毀；電子形式之資料檔得另備份至其他儲存媒體並提供適當保護，或以安全方式銷毀。

5.5.3 歸檔紀錄之保護

(1) 不允許新增、修改或刪除歸檔紀錄。

(2) 歸檔紀錄移至另一個儲存媒體，其保護等級不得低於原保護等級。

(3) 歸檔紀錄應存放於安全場所。

5.5.4 歸檔紀錄備份程序

(1) 電子式紀錄定期備份至異地備援中心。

(2) 紙本紀錄將由本管理中心授權之人員定期整理歸檔。

5.5.5 歸檔紀錄之時戳要求

(1) 歸檔之電子式紀錄內容應包含日期及時間資訊，並經適當之數位簽章保護，用以檢測紀錄中之日期及時間資訊是否遭篡改。

(2) 電子式紀錄中之日期及時間資訊，係為電腦作業系統之日期及時間，非第三方所提供之電子式時戳資料。

(3) 本管理中心所有電腦系統均定期進行校時。

(4) 歸檔之書面紀錄亦記載日期資訊，必要時得記載時間資訊。紀錄之日期及時間紀錄如有更改時須由稽核人員簽名確認。

5.5.6 歸檔紀錄彙整系統

本管理中心無歸檔紀錄彙整系統。

5.5.7 取得及驗證歸檔紀錄之程序

(1) 歸檔紀錄須以書面申請並經同意後方可取得。

(2) 稽核員負責驗證歸檔紀錄，書面文件須驗證文件簽署者及日期等之真偽；電子檔須驗證歸檔紀錄之數位簽章。

5.6 金鑰更換

(1) 本管理中心私密金鑰於簽發憑證用途之使用期限到期前，應完成用以簽發憑證之金鑰對更換作業，並取得總管理中心核發之下屬憑證機構憑證。

(2) 用戶之私密金鑰依 6.3.2 節規定定期更換，用戶更換金鑰並申請憑證時，應依 4.2 節規定辦理。

5.7 破解或災害時之復原程序

5.7.1 緊急事件及系統遭破解之處理程序

本管理中心訂定緊急事件及系統遭破解之通報與處理程序，每年依該程序進行演練。

5.7.2 電腦資源、軟體或資料遭破壞之復原程序

本管理中心訂定電腦資源、軟體或資料遭破壞之復原程序，且每年依該程序進行演練。

電腦設備遭破壞無法運作時，須優先回復儲存庫之運作，並迅速重建憑證簽發及管理之能力。

5.7.3 本管理中心簽章金鑰遭破解之復原程序

本管理中心訂有簽章金鑰遭破解之復原程序，且每年依該程序進行演練。

5.7.4 本管理中心安全設施之災後復原工作

(1) 本管理中心每年對安全設施之災害復原工作進行演練。

(2) 當發生災害時，將啟動災害復原程序，優先回復本管理中心儲存庫之運作，並迅速重建憑證簽發及管理的能力。

5.7.5 本管理中心簽章金鑰憑證被廢止之復原程序

本管理中心訂有簽章金鑰憑證被廢止之復原程序，且每年依該程序進行演練。

5.8 本管理中心之終止服務

(1) 除無法通知者外，管理中心於預定終止服務 3 個月前，應通知所有未廢止及未過期憑證之用戶，並公告於儲存庫。

(2) 廢止全部有效憑證，並進行檔案紀錄之保管及移交工作。

(3) 針對憑證未過期而遭廢止之用戶，依比例合理退還其所繳費用，最高以其所繳費用（不含 IC 卡等其他工本費）80%為上限。

(4) 本管理中心結束業務時，對用戶或信賴憑證者，除依前項規定退費外，不負任何賠償責任。

6.技術性安全控管

6.1 金鑰對產製及安裝

6.1.1 金鑰對產製

6.1.1.1 本管理中心金鑰對之產製

(1) 本管理中心依 6.2.1 節規定，在通過 FIPS 140-2 第 3 級安全認證或同等級的硬體密碼模組內產製金鑰對，註冊中心在通過 FIPS 140-2 第 2 級安全認證或同等級的硬體密碼模組內產製金鑰對，採 RSA 金鑰演算法。

(2) 本管理中心之私密金鑰以 AES 演算法加密輸出儲存於硬碟，且此加密儲存之私密金鑰唯有在該硬體密碼模組內才可被解密及使用，金鑰之匯出與匯入須依 6.2.2 與 6.2.6 節規定辦理。

(3) 金鑰產製須準備與遵循金鑰產製腳本，於本管理中心相關人員見證下進行，且金鑰產製過程須錄影留存。

6.1.1.2 用戶金鑰對之產製

(1) 使用之符記為 IC 卡時，其金鑰對由本管理中心所信賴之發卡中心代為產製。發卡中心須採用通過 FIPS 140-2 第 2 級認證或安全強度相當之 IC 卡，並於 IC 卡內部產製金鑰對，且金鑰對產製完畢後，其私密金鑰將無法由 IC 卡中匯出。

(2) 使用其他符記時，其金鑰對由用戶自行產製。

(3) 產製金鑰對之公開金鑰須符合 6.1.5 節與 6.1.6 節之規定，且私密金鑰不可為弱金鑰。

6.1.2 私密金鑰安全傳送予用戶

使用之符記為 IC 卡時，依 6.1.1.2 節規定，其私密金鑰由本管理中心所信賴之發卡中心代為產製，發卡中心於本管理中心簽發憑證後，將存有私密金鑰之 IC 卡掛號郵寄予用戶。

用戶於收到 IC 卡後，若確認接受，則應連線至本管理中心網站進行憑證接受作業。

6.1.3 公開金鑰安全傳送予本管理中心

(1) 本管理中心代為產製用戶金鑰

由註冊中心透過安全管道將用戶之公開金鑰傳送予本管理中心。該安全管道係指以使用安全插座層通訊協定、專屬通訊協定或資料簽章與加密等傳送方式。例如以憑證管理協定(Certificate Management Protocol)簽章封包、憑證註冊審驗人員簽章等傳送方式，將用戶之公開金鑰傳送予本管理中心。

(2) 用戶自行產製金鑰對

用戶以 PKCS#10 憑證申請檔的格式將公開金鑰送給註冊中心，註冊中心依照 3.2.1 節規定檢驗用戶確實擁有相對應的私密金鑰後，再以傳輸層安全協定或安全強度相同之資料加密傳送方式將用戶的公開金鑰傳送至本管理中心。

6.1.4 本管理中心公開金鑰安全傳送予信賴憑證者

本管理中心之公鑰憑證由總管理中心簽發，並公布於總管理中心及本管理中心之儲存庫，供用戶及信賴憑證者直接下載與使用。

6.1.5 金鑰長度

(1) 本管理中心使用金鑰長度至少為 2048 位元之 RSA 金鑰，並以 SHA-256、SHA-384 或 SHA-512 雜湊函數演算法簽發憑證。

(2) 用戶使用之金鑰可為以下 2 種：

A. 採用 RSA 密碼模組，金鑰長度至少 2048 位元。

B. 採用 ECC 密碼模組，金鑰長度至少 256 位元。

6.1.6 公鑰參數之產製與品質檢驗

(1) RSA 演算法之公鑰參數為空值。

(2) 本管理中心簽章用金鑰對採用 ANSI X9.31 演算法或 NIST FIPS 186-4 規範產生 RSA 演算法所需之質數，並確保該質數為強質數。

(3) 用戶於軟硬體密碼模組以 RSA 演算法產製金鑰程序中的質數，須確保符合密碼學計算上的安全要求。

(4) 本管理中心依據 NIST SP 800-89 第 5.3.3 節之規定，確認該金鑰之公開指數值為大於 3 的奇數，且其值介於 216+1 與 2256-1 之間。此外，模數應具有奇數、非質數的指數次方且沒有小於 752 的因數等性質。

(5) 若使用橢圓曲線密碼演算法簽發憑證，本管理中心將遵照 NIST SP 800-56A Revision 3 之規定，確認所有使用 ECC Full Public Key Validation Routine 與 ECC Partial Public Key Validation Routine 的金鑰之效期。

6.1.7 金鑰使用目的

(1) 本管理中心簽章用私密金鑰僅用於簽發憑證及憑證廢止清冊。

(2) 用戶使用之符記為 IC 卡者，其金鑰用途為簽章用與加解密用；簽章用憑證金鑰用途擴充欄位設定為 digitalSignature，加解密用憑證金鑰用途擴充欄位設定 keyEncipherment 與 dataEncipherment。

(3) 用戶使用非 IC 卡類符記(包含一站式專屬授權憑證或設立專屬用戶憑證)，其金鑰用途為簽章用。簽章用憑證金鑰用途擴充欄位設定為 digitalSignature。

6.2 私密金鑰保護及密碼模組安全控管措施

6.2.1 密碼模組標準及控管

(1) 本管理中心使用通過 FIPS 140-2 安全等級第 3 級認證之硬體密碼模組產製亂數與金鑰對。

(2) 用戶金鑰對之儲存媒體可為通過 FIPS 140-2 安全等級第 2 級認證或安全強度相當之 IC 卡或其他載具。

6.2.2 金鑰分持之多人控管

本管理中心私密金鑰以 Triple-DES 或 AES 演算法加密後由硬體密碼模組輸出儲存於硬碟，且此加密儲存之私密金鑰唯有在該硬體密碼模組內才可被解密及使用。

本管理中心之金鑰分持多人控管採 m-out-of-n 方法。m-out-of-n

方法係一種完全秘密分享的方式，其 m 與 n 皆須為大於或等於 2 的數值，且 m 必須小於或等於 n。本管理中心使用此方法做為金鑰分持備份、啟動及回復之方式。

本管理中心於金鑰產製後，採用上述之多人控管方式進行金鑰分持，分別存放於不同之安全地點。

6.2.3 私密金鑰託管

(1) 本管理中心簽章用之私密金鑰不可被託管。

(2) 本管理中心不提供用戶私密金鑰託管服務。

6.2.4 私密金鑰備份

本管理中心私密金鑰以 Triple-DES 或 AES 演算法加密後由硬體密碼模組輸出儲存於硬碟，此加密儲存之私密金鑰將會被複製 1 份至本管理中心備援主機與異地備援機房進行線上備援及離線備援，同時亦以光碟燒錄方式備份，存放至異地安全保險櫃中。

6.2.5 私密金鑰歸檔

(1) 本管理中心簽章用私密金鑰不進行歸檔。

(2) 用戶簽章用私密金鑰，本管理中心不進行歸檔。

6.2.6 私密金鑰與密碼模組間傳輸

本管理中心在硬體密碼模組內產製金鑰對，私密金鑰以 Triple-DES 或 AES 演算法加密輸出儲存於硬碟，在啟用此加密儲存之私密

金鑰時，必須匯入硬體密碼模組內，在硬體密碼模組中才能解密及使用。

6.2.7 私密金鑰儲存於密碼模組

(1) 本管理中心私密金鑰以 Triple-DES 或 AES 演算法加密輸出儲存於硬碟，而加密金鑰(Wrapper Keys)則存在硬體密碼模組中。

(2) 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

本管理中心私密金鑰之啟用是以 6.2.2 節之方式來控制，不同用途金鑰的控管 IC 卡組由管理員或簽發員所保管。

用戶之私密金鑰儲存於用戶 IC 卡中，採用 IC 卡 PIN 碼做為啟用資料，在啟用私密金鑰時，必須由用戶輸入 PIN 碼。

用戶使用其他密碼模組時，私密金鑰之啟動方式，可使用之鑑別方式包含（但不限於）通行詞組（Pass-Phrase）、個人符記、PIN 碼或生物識別。但輸入的啟動資料必須避免被洩露。

6.2.9 私密金鑰之停用方式

本管理中心私密金鑰之停用是以 6.2.2 節之方式來控制。

用戶在使用符記為 IC 卡中的私密金鑰時，若輸入 PIN 碼錯誤超過發卡中心所設定的次數上限，則該 IC 卡將會因 PIN 碼被鎖碼（Block）而遭停用。被鎖碼的 IC 卡必須經發卡中心解鎖（Unblock）並重設 PIN

碼後才能繼續使用。

用戶使用其他密碼模組時，私密金鑰之停用方式可透過手動的登出程序，或經過一段時間沒有運作後自動停止運作。如硬體密碼模組不再使用時，必須與主機分離並儲存至安全場所。

6.2.10 私密金鑰之銷毀方式

本管理中心於舊私密金鑰不再簽發任何憑證與憑證廢止清冊後，依照 FIPS 140-1 或 FIPS 140-2 第 3 級規定的程序銷毀舊私密金鑰。

用戶之私密金鑰儲存符記為 IC 卡時，當用戶更換新的 IC 卡或不再繼續使用時，且用戶確定不再需要使用該 IC 卡對檔案或訊息進行解密時，用戶可自行將該 IC 卡實體銷毀。但即使更換新的 IC 卡或不再繼續使用時，用戶仍可選擇以適當的方式安全保存該 IC 卡，以備未來仍可能需要使用該 IC 卡對舊檔案或訊息進行解密。

用戶使用其他密碼模組時，軟體密碼模組之私密金鑰銷毀必須將資料複寫至原簽章用私密金鑰佔用的記憶體或儲存媒體；硬體密碼模組之私密金鑰銷毀，必須執行零值化（Zeroize）動作，但不需做實體銷毀。

6.2.11 密碼模組評等

密碼模組評等方式依憑證政策 6.2.1 節規定辦理。

6.3 金鑰對管理之其他規定

本管理中心不負責保管用戶之私密金鑰。

6.3.1 公開金鑰之歸檔

本管理中心依 5.5 節規定進行憑證之歸檔，不另對公開金鑰進行歸檔。

6.3.2 公開金鑰及私密金鑰之使用期限

6.3.2.1 憑證機構公開金鑰及私密金鑰之使用期限

(1) 本管理中心公開金鑰與私密金鑰使用期限至多為 20 年。

(2) 以私密金鑰執行簽發用戶憑證用途之使用期限至多為 10 年。

(3) 私密金鑰執行簽發用戶憑證用途之使用期限到期後，仍須簽發憑證廢止清冊或線上憑證狀態協定回應伺服器憑證，持續至該私密金鑰簽發之所有用戶憑證到期為止。

(4) 本管理中心所簽發之線上憑證狀態協定(Online Certificate Status Protocol, OCSP)憑證，效期比照本管理中心之公開金鑰辦理。

6.3.2.2 用戶公開金鑰及私密金鑰之使用期限

用戶之公開金鑰憑證之使用期限至多為10年，私密金鑰之使用期限至多為10年。一站式專屬授權憑證之使用期限至多為1年。設立專屬用戶憑證之使用期限至多為1個月。

6.4 啟動資料之保護

6.4.1 啟動資料之產生

(1) 本管理中心之啟動資料由硬體密碼模組產生，再寫入至多人分持控管 IC 卡中。

(2) 用戶之符記使用 IC 卡，初始 PIN 碼由發卡中心以亂數產生，每張 IC 卡的 PIN 碼可能皆不相同。

(3) 用戶使用其他密碼模組時，啟動資料之產生方式由用戶決定，若以通行碼（Password）做為啟動資料時，通行碼的產生必須符合行政院及所屬各機關資訊安全管理要點及規範規定。

6.4.2 啟動資料之保護

本管理中心私密金鑰之啟動資料以 6.2.2 節之方式保護，IC 卡的 PIN 碼由保管人員自行記憶，不得紀錄於任何媒體上，如登入的失敗次數超過 3 次，則鎖住此 IC 卡。IC 卡移交時新的保管人員必須重新設定 PIN 碼。

用戶之符記使用 IC 卡，初始 PIN 碼在啟用 IC 卡時，由發卡中心透過安全的管道傳送給用戶。用戶在使用其 IC 卡中的私密金鑰時，若輸入 PIN 碼錯誤超過發卡中心所設定的次數上限，則該 IC 卡將會因 PIN 碼被鎖碼。

用戶使用其他密碼模組時，啟動資料之保護方式由用戶決定，若登入的失敗次數超過該密碼模組設定的次數上限，保護機制必須能即

時鎖住此帳號或終止應用程式。

6.4.3 啟動資料之其他規範

不予規定。

6.5 電腦軟硬體安控措施

6.5.1 特定電腦安全技術需求

本管理中心提供安全控管功能說明如下：

(1) 具備身分鑑別之登入。

(2) 提供自行定義存取控制。

(3) 提供安全稽核能力 。

(4) 對各種憑證服務與信賴角色存取控制之限制。

(5) 具備信賴角色與相關身分之識別及鑑別。

(6) 以密碼技術確保每次通訊與資料庫之安全。

(7) 具備信賴角色與相關身分識別之安全與可信賴管道。

(8) 具備程序完整性與安全控管保護。

6.5.2 電腦安全評等

本管理中心採用安全強度與 C2(TCSEC)、E2(ITSEC) 或 EAL3(CC,ISO/IEC 15408)等級相當之電腦作業系統，且系統及運作環境符合 WebTrust for CA 之安全控管原則。

6.6 生命週期技術控管措施

6.6.1 系統研發控管措施

本管理中心的系統研發遵循主管機關認可之品質管理規範進行品質控管。

本管理中心之硬體和軟體是專用的，僅能使用獲得安全授權的元件，不安裝與運作無關的硬體裝置、網路連接或元件軟體，並且每天會自動檢查是否有惡意程式碼。

6.6.2 安全管理控管措施

本管理中心的軟體在首次安裝時，將確認是由供應商提供正確的版本且未被修改。系統安裝後，本管理中心每天自動檢驗軟體的完整性。

本管理中心將記錄和控管系統的組態及任何修正與功能提升，同時偵測未經許可修改系統之軟體或組態。

6.6.3 生命週期安全控管措施

本管理中心每年至少進行 1 次現行金鑰是否有被破解之風險評估。

6.7 網路安全控管措施

本管理中心應配合資通安全管理法規定辦理相關資安防護作業。

本管理中心之主機和內部儲存庫透過雙重防火牆和外部網路連接，外部儲存庫置於外部防火牆之對外服務區（非軍事區 DMZ），連

接到網際網路（Internet）上，除必要之維護或備援外，提供不中斷之憑證與憑證廢止清冊查詢服務。

本管理中心之內部儲存庫資訊（包括憑證與憑證廢止清冊）以數位簽章保護，並自動從內部儲存庫傳送到外部儲存庫。

本管理中心之外部儲存庫透過系統修補程式的更新、系統弱點掃描、入侵偵測系統、防火牆系統及過濾路由器（filtering router）等加以保護，以防範阻絕服務和入侵等攻擊。

6.8 時戳

為確保下述時間之正確性，本管理中心定期依據受信賴之時間源進行系統校時，且系統校時作業須可被稽核。

(1) 用戶憑證簽發時間。

(2) 用戶憑證廢止時間。

(3) 憑證廢止清冊之簽發時間。

(4) 系統事件之發生時間。

6.9 密碼模組安全控管措施

密碼模組安全控管措施，依 6.1 節與 6.2 節規定辦理。

7.憑證、憑證廢止清冊及線上憑證狀態協定格式剖繪

7.1 憑證之格式剖繪

本管理中心簽發之憑證遵照 ITU-T X.509 與 IETF PKIX Working Group 的 RFC 5280 或其最新版相關之規定，其格式剖繪依本基礎建設技術規範相關規定。

本管理中心透過密碼學安全偽亂數產生器(Cryptographically Secure Pseudorandom Number Generator, CSPRNG)產生其所簽發之憑證的憑證序號，此憑證序號為長度至少 64 位元且非循序之正整數。

7.1.1 版本序號

本管理中心簽發遵照 RFC5280 與 ITU-T 規範之 X.509 v3 版本之憑證。

7.1.2 憑證擴充欄位

(1) 憑證擴充欄位遵照 ITU-T X.509、IETF PKIX Working Group RFC 5280 及本基礎建設技術規範相關規定。

(2) 憑證所使用之必要擴充欄位與該擴充欄位的關鍵性與內容於「政府機關公開金鑰基礎建設憑證及憑證廢止清冊格式剖繪」中敘明。

(3) 其他選擇性擴充欄位依情況不同使用時，其使用方式遵照前述標準之規定。

(4) 本管理中心不允許簽發下述情境之憑證：

A. 憑證的內容包含可能誤導信賴憑證者相信該憑證資訊已經由本管理中心驗證之語意。

7.1.3 演算法物件識別碼

(1) 本管理中心使用之演算法之物件識別碼(Object Identifier)如下：

sha1WithRSAEncryption	{iso（1） member-body（2） us（840） rsadsi（113549） pkcs（1） pkcs-1（1） 5}

（OID：1.2.840.113549.1.1.5）

sha256WithRSAEncryption	{iso（1） member-body（2） us（840） rsadsi（113549） pkcs（1） pkcs-1（1） 11}

（OID：1.2.840.113549.1.1.11）

(2) 本管理中心所簽發憑證之主體公鑰，其演算法之物件識別碼如下：

rsaEncryption	{iso（1） member-body（2） us（840） rsadsi（113549） pkcs（1） pkcs-1（1） 1}

（OID:1.2.840.113549.1.1.1）

7.1.4 命名形式

憑證之主體與簽發者兩個欄位使用 X.500 之唯一識別名稱，其欄位屬性型態係遵照 ITU-T X.509、IETF PKIX Working Group RFC5280 等相關規定。

7.1.4.1 簽發者資訊

依據RFC 5280名稱串鏈之規定，本管理中心所簽發之用戶憑證，其簽發者唯一識別名稱欄位(Issuer Distinguished Name)內容須與本管理中心本身憑證之主體唯一識別名稱欄位(Subject Distinguished Name)

內容相同。

7.1.4.2 用戶憑證之主體資訊

本管理中心所簽發用戶憑證主體唯一識別名稱欄位、主體別名擴充欄位與其他必要擴充欄位的關鍵性與格式，於「政府機關公開金鑰基礎建設憑證及憑證廢止清冊格式剖繪」中敘明。

7.1.4.3 本管理中心之主體資訊

本管理中心之憑證機構憑證主體唯一識別名稱欄位中各屬性的格式與必要性，於「政府機關公開金鑰基礎建設憑證及憑證廢止清冊格式剖繪」中敘明，憑證主體名稱欄位說明參考3.1.5節。

7.1.5 命名限制

本管理中心簽發之憑證不採用命名限制(nameConstraints)。

7.1.6 憑證政策物件識別碼

本管理中心所簽發憑證之憑證政策擴充欄位使用本基礎建設之憑證政策物件識別碼。

7.1.7 政策限制擴充欄位之使用

本管理中心簽發之憑證不含政策限制擴充欄位(policyConstraints)。

7.1.8 政策限定元之語法及語意

本管理中心簽發之憑證不含政策限定元(policyQualifiers)。

7.1.9 關鍵憑證政策擴充欄位之語意處理

本管理中心簽發之憑證，其所含之憑證政策擴充欄位，須依「政府機關公開金鑰基礎建設憑證及憑證廢止清冊格式剖繪」之規定，進行關鍵性之註記。

7.2 憑證廢止清冊格式剖繪

7.2.1 版本序號

本管理中心簽發 ITU-T X.509 v2 版本之憑證廢止清冊。

7.2.2 憑證廢止清冊與憑證廢止清冊條目擴充欄位

本管理中心簽發的憑證廢止清冊、憑證廢止清冊擴充欄位(crlExtensions)及憑證廢止清冊條目擴充欄位(crlEntryExtensions)會遵照 ITU-T X.509 與 IETF PKIX Working Group 的 RFC 5280 或其最新版相關之規定。

憑證廢止清冊之擴充欄位內容均詳述於「政府機關公開金鑰基礎建設憑證及憑證廢止清冊格式剖繪」。

7.3 線上憑證狀態協定格式剖繪

(1) 本管理中心提供符合 RFC 6960 與 RFC 5019 標準規範之線上憑證狀態協定查詢服務，並於憑證之憑證機構存取資訊擴充欄位中註明本管理中心線上憑證狀態協定之服務網址。

(2) 本管理中心線上憑證狀態協定查詢服務之線上憑證狀態協定查詢封包，應包括資訊如下：

A. 版本序號

B. 待查詢憑證識別碼，包括：雜湊演算法、憑證簽發者名稱、憑證簽發者公開金鑰及待查詢憑證之憑證序號等。

(3) 本管理中心線上憑證狀態協定回應訊息基本欄位說明如下：

欄位	說明
版本序號(Version)	v.1 (0x0)
線上憑證狀態協定回應伺服器 ID(Responder ID)	線上憑證狀態協定回應伺服器之主體名稱
產製時間(Produced Time)	回應訊息簽署時間
待查詢憑證識別元(Identifier)	包括雜湊演算法、憑證簽發者名稱、憑證簽發者公開金鑰及待查詢憑證之憑證序號等
憑證狀態碼(Certificate Status)	憑證狀態對應碼(0:有效/1:廢止/2:未知)
效期(ThisUpdate/NextUpdate)	此回應訊息建議之效期區間，包括生效時間(ThisUpdate) 與下次更新時間
簽章演算法(Signature Algorithm)	回應訊息之簽章演算法，可為 sha256WithRSAEncryption
簽章(Signature)	線上憑證狀態協定回應伺服器之簽章
憑證(Certificates)	線上憑證狀態協定回應伺服器之憑證

7.3.1 版本序號

版本序號以 RFC 5019 及 RFC 6960 規定為依據。

7.3.2 線上憑證狀態協定服務擴充欄位

(1) 線上憑證狀態協定擴充欄位會依照 ITU-T X.509、RFC 5019 及 RFC 6960 之規定。

(2) 線上憑證狀態協定回應訊息應包括線上憑證狀態協定伺服器之憑證機構金鑰識別碼(Authority Key Identifier)。

(3) 憑證狀態協定查詢封包有隨機數欄位時，線上憑證狀態協定回應訊息亦須包括相同之隨機數欄位。

7.3.3 線上憑證狀態協定服務運轉規範

本管理中心線上憑證狀態協定服務運轉作業說明如下：

(1) 可以處理與接受 HTTP GET/POST 方法所傳送線上憑證狀態協定用戶端之線上憑證狀態協定查詢封包。

(2) 線上憑證狀態協定回應伺服器使用短效期憑證，由本管理中心定期簽發與更新。

8. 稽核方法

8.1 稽核頻率或評估事項

(1) 本管理中心每年至少 1 次內部稽核。

(2) 本管理中心每年接受 1 次外部稽核，且查核區間不可超過 12 個月。

(3) 稽核採用之標準為 WebTrust Principles and Criteria for Certification Authorities。

8.2 稽核人員之身分及資格

(1) 稽核方須經 WebTrust 認證標章管理單位授權可於我國執行 WebTrust Principles and Criteria for Certification Authorities 稽核標準之合格稽核業者。

(2) 稽核人員應通過國際電腦稽核師(Certified Information Systems Auditor, CISA)認證或具同等資格。

(3) 本管理中心於稽核時應對稽核人員進行身分識別。

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之憑證管理中心，為獨立且公正之第三方人員。

8.4 稽核之範圍

(1) 本作業基準是否符合憑證政策及總管理中心憑證實務作業基準之規定。

(2) 本管理中心及註冊中心是否遵照本作業基準運作。

8.5 對於稽核結果之因應方式

(1) 本管理中心對不符合規定之項目進行改善，並於完成後通知原稽核人員進行複核。

(2) 依不符合情形之種類、嚴重性及修正所需時間，本管理中心得採取必要措施。

8.6 稽核結果公開之範圍

除可能導致系統安全風險及依 9.3 節規定外，本管理中心應於儲存庫公布最近 1 次外部稽核結果。

9.其他業務和法律事項

9.1 費用

本管理中心得在本部核可後向用戶及信賴憑證者收取費用，該項費用限應用於本管理中心營運及管理維護。

9.1.1 憑證簽發、展期費用

請至以下網站查詢相關費用：https://moeaca.nat.gov.tw/。

9.1.2 憑證查詢費用

本管理中心提供信賴憑證者，使用憑證廢止清冊查詢憑證狀態，免收查詢費用。

提供線上憑證狀態協定（Online Certificate Status Protocol, OCSP）查詢服務，收費標準公告於本管理中心網站（https://moeaca.nat.gov.tw）。

9.1.3 憑證廢止、狀態查詢費用

請至以下網站查詢相關費用：https://moeaca.nat.gov.tw/。

9.1.4 其他服務費用

請至以下網站查詢相關費用：https://moeaca.nat.gov.tw/。

9.1.5 請求退費程序

憑證申辦人如依 4.1 節規定申請憑證，如因故無法辦理，所預繳交予本管理中心之費用，得於送交憑證申請書至憑證註冊窗口辦理前

提出退費申請。相關規定請至網站查詢：https://moeaca.nat.gov.tw/。

9.2 財務責任

本管理中心之營運以使用者付費為原則，不足部分由本部編列預算維持，未向保險公司投保，財務責任依政府法令規定辦理。

9.2.1 保險範圍

不適用。

9.2.2 其他資產

不予規定。

9.2.3 對終端個體之保險或保固責任

不適用。

9.3 業務資訊之保密

9.3.1 重要資訊之範圍

(1) 本管理中心營運之私密金鑰與通行碼。

(2) 本管理中心金鑰分持之相關資料。

(3) 未經同意公開之用戶資料。

(4) 本管理中心產生或保管之可供稽核與追蹤之紀錄。

(5) 稽核人員於稽核過程中產生之稽核紀錄與發現，不得被完整公開者。

(6) 本管理中心列為不得公開之營運相關文件。

(7) 其他經法令規定不得公開之資料。

9.3.2 一般資訊之範圍

非 9.3.1 節規定之資訊，原則皆屬一般資訊。

9.3.3 保護重要資訊之責任

本管理中心依電子簽章法、Trust Service Principles and Criteria for Certification Authorities 標準及個人資料保護法等規定，處理本管理中心之重要資料。

9.4 個人資訊之隱私性

9.4.1 隱私保護計畫

(1) 本管理中心於網站公告隱私權保護政策。

(2) 本管理中心實施隱私衝擊分析與個資風險評鑑等措施。

9.4.2 隱私資料之種類

(1) 憑證申請時記載之個人資訊。

(2) 本管理中心運作所取得之個人資訊。

9.4.3 非隱私資料之種類

非 9.4.2 節規定之資訊，原則皆屬非隱私資料。

9.4.4 保護隱私資料之責任

依網站公告之隱私權保護政策、WebTrust Principles and Criteria for Certification Authorities 標準及個人資料保護法等相關規定進行隱

私資料保護。

9.4.5 利用隱私資訊之公告與同意

(1) 隱私權保護政策公告於網站。

(2) 利用個人隱私資訊須經用戶同意。

9.4.6 應司法或行政程序提供資訊

司法機關或檢調單位如應依法調查或蒐集證據需要，須查詢重要資訊時，本管理中心依法辦理，不另通知用戶。

9.4.7 其他資訊釋出之情形

依相關規定法令辦理。

9.5 智慧財產權

除個人資料外，本管理中心產製之文件(含電子檔案)，其智慧財產權皆屬本管理中心所有，重製、散布或公開傳輸須依網站公布之著作權聲明規定辦理。

9.6 職責與義務

9.6.1 本管理中心職責與義務

(1) 依據憑證政策保證等級第 3 級規定與本作業基準運作，惟有關設立專屬用戶憑證之組織身分鑑別程序係以符合憑證政策訂定保證等級第 2 級之規定辦理。

(2) 執行憑證申請之識別及鑑別程序。

(3) 簽發、公布、廢止憑證。

(4) 簽發與公布憑證廢止清冊。

(5) 提供線上憑證狀態協定查詢服務。

(6) 產製及管理本管理中心之私密金鑰。

(7) 公布憑證實務作業基準。

(8) 執行本管理中心與註冊中心相關人員之識別及鑑別程序。

(9) 提供憑證接受作業。

9.6.2 註冊中心職責與義務

(1) 提供憑證申請服務。

(2) 執行憑證申請之識別及鑑別程序。

(3) 管理註冊中心之私密金鑰，且不得用於憑證註冊以外作業。

9.6.3 用戶之義務

(1) 提供正確完整之資訊。

(2) 遵守本作業基準相關規定。

(3) 妥善管理與使用私密金鑰。

(4) 私密金鑰遭冒用、破解或遺失時，應立即通知本管理中心廢止憑證，惟用戶仍應承擔異動前所有使用該憑證之法律責任。

(5) 安全產製其私密金鑰並避免遭受破解。

(6) 用戶應慎選安全之電腦環境與可信賴之應用系統，如因電腦

環境或應用系統本身因素，導致信賴憑證者權益受損時，用戶應自行承擔責任。

(7) 本管理中心如因故無法正常運作時，用戶應儘速尋求其他途徑完成與他人應為之法律行為，不得以本管理中心無法正常運作，作為抗辯他人之事由。

9.6.4 信賴憑證者之義務

(1) 遵守本作業基準相關規定。

(2) 正確檢驗憑證保證等級、數位簽章、有效性、正附卡別及金鑰用途。

(3) 信賴憑證者應確保憑證使用環境之安全，如非可歸責於本管理中心之事由導致權益受損時，應自行承擔責任。

(4) 本管理中心如因故無法正常運作時，信賴憑證者應儘速尋求其他途徑完成與他人應為之法律行為，不得以本管理中心無法正常運作，作為抗辯他人之事由。

9.6.5 其他參與者之義務

9.6.5.1 發卡中心之義務

(1) 依本作業基準 6.1.1.1 節規定產製用戶之金鑰對。

(2) 執行憑證寫入及製卡作業，並以亂數設定 IC 卡之初始 PIN 碼。

(3) 寄送用戶之 IC 卡。

9.6.5.2 委外方式提供認證服務機構之義務

本管理中心由經濟部依政府採購法規定辦理委外服務，承商依契約規定辦理。

9.7 免責聲明

用戶或信賴憑證者如未依本作業基準相關規定申請、管理及使用憑證，或其他非可歸責於本管理中心之事由，而造成之損害，由用戶或信賴憑證者自行負責，本管理中心不負任何法律責任。

9.8 責任限制

(1) 本管理中心如因系統維護、轉換及擴充等事由，須暫停部分憑證服務時，得於 3 天前公告於儲存庫。用戶或信賴憑證者不得以此作為要求本管理中心損害賠償之理由。

(2) 用戶如有廢止憑證事由時，應依 4.9 節規定提出憑證廢止申請。廢止憑證申請核定後，本管理中心將於 1 個工作天內完成憑證廢止作業、簽發憑證廢止清冊與公告於儲存庫。

(3) 用戶於憑證廢止狀態未被公布前，應採取適當之行動，以減少對信賴憑證者之影響，並承擔所有因使用該憑證所引發之責任。

9.9 賠償

9.9.1 本管理中心之賠償責任

本管理中心如未依本作業基準及相關法令規定導致利害關係人

權益損害時，由本管理中心負賠償責任；用戶及信賴憑證者得依相關法律規定請求損害賠償。

9.9.2 註冊中心之賠償責任

註冊中心如未依本作業基準及相關法令規定導致利害關係人權益損害時，由註冊中心負賠償責任；用戶及信賴憑證者得依相關法律規定請求損害賠償。

9.10 有效期限與終止

9.10.1 有效期限

本作業基準由總管理中心核定並公告後生效，直至被新版本取代前仍然有效。

9.10.2 終止

本作業基準之終止須由行政機關電子憑證推行小組委員決議，並經電子簽章法主管機關核定。

9.10.3 終止及存續之效力

(1) 本作業基準效力終止之說明，應公告於本管理中心儲存庫。

(2) 本作業基準終止後，其效力須維持至所簽發之最後一張憑證失效為止。

9.11 對參與者之個別通告及溝通

本管理中心、註冊中心、用戶及信賴憑證者間得採網站公告、儲

存庫、公文、書信、電話、傳真、電子郵件等方式建立通知與聯絡管道。

9.12 修訂

本管理中心每年定期檢視及評估本作業基準，本作業準修訂方式如下：

(1) 直接修訂本作業基準之內容。

(2) 以附加文件方式增修。

9.12.1 修訂程序

本作業基準之修訂經行政機關電子憑證推行小組委員審查，並經電子簽章法主管機關經濟部核定後頒布。

9.12.2 通知機制與期限

本作業基準之修訂，經電子簽章法主管機關核定後須於 10 個工作天內公告，所有變更項目將公告於儲存庫。

9.12.3 須修改憑證政策物件識別碼之事由

憑證政策修訂或其物件識別碼如有變更時，本作業基準須配合修訂。

9.13 紛爭之處理程序

用戶與本管理中心如有爭議時，雙方應本誠信原則先進行協商，由本管理中心就本作業基準相關條文提出解釋。

9.14 管轄法律

依我國相關法令規定辦理。

9.15 適用法律

依我國相關法令規定辦理。

9.16 雜項條款

9.16.1 完整協議

本作業基準所約定者，構成主要成員間最終且完整之約定，主要成員包括本管理中心、註冊中心、用戶及信賴憑證者等。主要成員間就同一事項縱使以口頭或書面進行其他表示，最終仍應以本作業基準之約定為準。

9.16.2 轉讓

本作業基準所敘述之主要成員間權利或責任，不可於未通知本管理中心下以任何形式轉讓予其他方。

9.16.3 可分割性

本作業基準之任一章節不適用而須修正時，其他章節仍屬有效。

9.16.4 契約履行

用戶或憑證信賴者違反本作業基準相關規定，致本管理中心遭受損害，如可歸責於用戶或憑證信賴者之故意或過失時，本管理中心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。

9.16.5 不可抗力

因不可抗力所導致之損害事件，本管理中心不負任何法律責任。

9.17 其他條款

不予規定。

附錄 1：名詞解釋

◆ A

- 啟動資料(Activation Data)：存取密碼模組時(例如用以開啟私密金鑰以進行簽章或解密)，除金鑰外所需之隱密資料。
- 申請者(Applicant)：向憑證機構申請憑證，而尚未完成憑證作業程序之用戶。
- 歸檔(Archive)：實體上(與主要資料存放處)分隔之長期資料儲存處，可用以支援稽核服務、可用性服務或完整性服務等用途。
- 保證(Assurance)：據以信賴該個體已符合特定安全要件之基礎。
- 保證等級(Assurance Level)：具相對性保證層級中之某一級數。
- 稽核(Audit)：評估系統控制是否恰當，以確保符合既定之政策與營運程序，並對現有之控制、政策與程序等，建議必要之改善所進行之獨立檢閱與調查。
- 稽核紀錄(Audit Log)：依發生時間順序之系統活動紀錄，可用以重建或調查事件發生之順序與某個事件中之變化。
- 鑑別(Authenticate)：驗證某個聲稱的身分是合法且屬於提出此聲稱者的程序。
- 鑑別程序(Authentication)

- 建立使用者或資訊系統身分信賴程度的程序。
- 用以建立資料傳送、訊息、來源者之安全措施，或是驗證個人接收特定種類資訊權限之方法。

◆ C

- 憑證(Certificate)
  - 指載有簽章驗證資料，用以確認簽署人身分、資格之電子形式證明。
  - 資訊之數位呈現內容包括：
    - ✓ 簽發之憑證機構。
    - ✓ 用戶之名稱或身分。
    - ✓ 用戶之公開金鑰。
    - ✓ 憑證之有效期間。
    - ✓ 憑證機構數位簽章。
- 憑證政策(Certificate Policy, CP)：係為透過憑證管理執行之電子交易所訂定具專門格式之管理政策。憑證政策中包括與數位憑證相關之生成、產製、傳送、稽核、被破解後復原及其管理等各項議題。憑證政策與其相關技術可提供特定應用所需之安全服務。
- 憑證廢止清冊(Certificate Revocation List, CRL)
  - 憑證機構以數位方式簽章，並可供信賴憑證者使用之

已廢止憑證表列。

- 由憑證機構維護之清單，清單中記載由此憑證機構所簽發且於到期日前被廢止之憑證。

- 憑證機構(Certification Authority, CA)
  - 簽發憑證之機關。
  - 為使用者所信任之權威機構，其業務為簽發並管理 X.509 格式之公開金鑰憑證、憑證機構廢止清冊及憑證廢止清冊。

- 憑證變更(Certificate Modification)：係指對同一憑證主體提供一張新憑證取代原憑證，惟新憑證有效截止日須與舊憑證到期日相同，憑證變更後，舊憑證應予以廢止。

- 憑證實務作業基準(Certification Practice Statement, CPS)
  - 由憑證機構對外公告，用以陳述憑證機構據以簽發憑證與處理其他身分識別業務之作業準則。
  - 宣告某憑證機構對憑證之作業程序(包括簽發、停用、廢止、展期及存取等)符合特定需求之聲明(需求敘明於憑證政策或其他服務契約中)。

- 破解(Compromise)：資訊洩漏予未經授權人士或違反資訊安全政策，造成物件未經授權蓄意、非蓄意洩漏、修改、毀壞或遺失。

- 交互憑證(Cross-Certificate)：在兩個根憑證機構之間建立

信賴關係的一種憑證，屬於一種憑證機構憑證，而非用戶憑證。

- 密碼模組(Cryptographic Module)：一組硬體、軟體、韌體或前述之組合，用以執行密碼之邏輯或程序(包含密碼演算法)，且被包含於此模組之密碼邊界內。

◆ D

- 數位簽章(Digital Signature)：將電子文件以數學演算法或其他方式運算為一定長度之數位資料，以簽署人之私密金鑰對其加密，形成電子簽章，並得以公開金鑰加以驗證者。

- 憑證效期(Duration)：憑證欄位，由有效期限起始時間與有效期限截止時間二個子欄位所組成。

◆ E

- 終端個體(End Entity, EE)：在 GPKI 中包括以下兩類個體：
  - 負責保管與應用憑證的私密金鑰擁有者。
  - 信賴 GPKI 憑證機構所簽發憑證的第三者(不是私密金鑰擁有者，也不是憑證機構)，亦即終端個體為用戶與信賴憑證者，包括人員、組織、客戶、裝置或站台。

◆ F

- 聯邦資訊處理標準(Federal Information Processing

Standard, FIPS)：為美國聯邦政府制定除軍事機構外，所有政府機構與政府承包商所引用之資訊處理標準。其中密碼模組安全需求標準為 FIPS 第 140 號標準(簡稱 FIPS 140)，FIPS 140-2 將密碼模組區分為 11 類安全需求，每一個安全需求類別再分成 4 個安全等級。

◆ G

- 政府憑證總管理中心(Government Root Certification Authority)：GPKI 根憑證機構，在此階層式公開架構中最頂層之憑證機構，其公開金鑰為信賴之起源。

◆ I

- 網際網路工程任務小組(Internet Engineering Task Force, IETF)：負責網際網路標準之開發與推動，其願景係藉由產製高品質之技術文件影響人類設計、使用與管理網際網路，使得網際網路運作更順暢。(官方網站：https://www.ietf.org)

- 簽發憑證機構(Issuing CA)：對一張憑證而言，簽發該憑證之憑證機構即稱為該憑證之簽發憑證機構。

◆ K

- 金鑰託管(Key Escrow)：依用戶須遵守之託管協議(或類似契約)所規定相關資訊，將用戶之私密金鑰進行存放，此託管協議條款要求一個或以上之代理機構，基於有益於用戶、雇主或另一方之前提下，依協議規定擁有用戶之金鑰。

- 金鑰對(Key Pair)：兩把數學上有相關性之金鑰，其特性如下：
  - 其中一把金鑰用以進行訊息加密，而此加密訊息僅有另一把可解密。
  - 從其中一把金鑰要推出另一把金鑰(從計算之角度而言)是不可行。

◆ O

- 物件識別碼(Object Identifier, OID)
  - 一種以字母或數字組成之唯一識別碼，該識別碼須依國際標準組織所訂定之註冊標準加以註冊，並可被用以識別唯一與之對應之憑證政策。
  - 向國際標準機構(International Organization for Standardization)註冊之特別形式數碼，當提及某物件或物件類別時，可以引用此唯一之數碼進行辨識。例如於公開金鑰基礎架構中以此數碼指明使用之憑證政策與使用之密碼演算法。
- 線上憑證狀態協定(Online Certificate Status Protocol, OCSP)：一種線上憑證檢查協定，使信賴憑證者應用軟體可決定某張憑證之狀態(例如已廢止、有效等)。

◆ P

- 私密金鑰(Private Key)：下述二情況下此金鑰均須保密。
  - 簽章金鑰對中用以產生數位簽章之金鑰。

- 加解密金鑰對中用以對加密資訊解密之金鑰。

- 公開金鑰(Public Key)：下述二情況下此金鑰均須公開可得(一般以數位憑證形式)。
  - 簽章金鑰對中用以驗證數位簽章有效之金鑰。
  - 加解密金鑰對中用以對資訊加密之金鑰。

- 公開金鑰基礎建設(Public Key Infrastructure, PKI)：由法律、政策、規範、人員、設備、設施、技術、流程、稽核及服務之集合，在廣泛尺度上發展與管理非對稱式密碼學及公鑰憑證。

◆ R

- 註冊中心(Registration Authority, RA)
  - 負責確認憑證申請人之身分或其他屬性，惟不簽發憑證亦不管理憑證。註冊中心是否需為其行為負責及其應負責任之範圍，依所適用之憑證政策或協議訂之。
  - 負責對憑證主體做身分識別及鑑別，惟不做憑證簽發。

- 金鑰更換(Re-key a Certificate)：憑證金鑰更換係指簽發一張與舊憑證具有相同特徵與保證等級之新憑證，新憑證除具有全新、不同之公開金鑰(對應新且不同之私密金鑰)及不同序號外，亦可被指定不同之有效期限。

- 信賴憑證者(Relying Party)
  - 信賴所收受之憑證與可用憑證中所載之公開金鑰加

以驗證之數位簽章者，或信賴憑證中所命名主體之身份(或其他屬性) 與憑證所載公開金鑰之對應關係者。

- 個人或機構收到包含憑證與數位簽章之資訊，且可能信賴這些資訊(此數位簽章可藉由憑證上所列之公開金鑰做驗證)。

- 憑證展期(Renew a Certificate)：係指簽發一張與舊憑證具有相同憑證主體名稱、金鑰及相關資訊之新憑證，使憑證之有效期限予以展延，並付予一個新序號。

- 儲存庫(Repository)
  - 用以儲存與檢索憑證或其他憑證相關資訊之可信賴系統(Trustworthy System)。
  - 包含憑證政策、憑證實務作業基準及憑證相關資訊之資料庫。

- 憑證廢止(Revoke a Certificate)：在憑證之有效期間內，提前終止憑證之運作。

- 根憑證機構(Root Certification Authority, Root CA)：公開金鑰基礎建設中最頂層的憑證機構，除了簽發下屬 CA 憑證與自簽憑證外，其自簽憑證由應用軟體供應商負責散布。亦可稱為憑證總管理中心或最頂層憑證機構。

◆ S

- 自簽憑證(Self-Signed Certificate)：自簽憑證係指憑證的簽發者名稱與憑證主體的名稱相同的一種憑證。亦即使

用同一對金鑰對的私密金鑰針對其成配對關係的公開金鑰與其他資訊所簽發的憑證。一個公開金鑰基礎建設內的自簽憑證，可做為憑證路徑信賴的起源，其簽發對象為總管理中心本身，內含總管理中心的公開金鑰，且憑證簽發者名稱與憑證主體名稱相同，可供信賴憑證者用於驗證總管理中心簽發之自發憑證、下屬憑證機構憑證、交互憑證以及憑證機構廢止清冊的數位簽章。

- 下屬憑證機構(Subordinate Certification Authority)：階層架構之公開金鑰基礎建設中，憑證由另一個憑證機構所簽發，且其活動受限於此另一憑證機構之憑證機構。

- 用戶(Subscriber)

  - 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者。

  - 具下列特性之個體，包括(但不限於)個人、機構或網路裝置：

    - ✓ 簽發憑證上所敘明之主體。

    - ✓ 擁有與憑證上所列公開金鑰對應之私密金鑰。

    - ✓ 本身不簽發憑證予其他方。

◆ T

- 可信賴系統(Trustworthy System)：具有下列性質之電腦硬體、軟體與程序：

  - 對於入侵與誤用有相當之保護功能。

- 提供合理之可用性、可靠度及正確操作。
- 適當地執行預定功能。
- 與一般為人所接受之安全程序一致。

◆ Z

- 零值化(Zeroize)：清除電子式儲存資料之方法，藉由改變資料儲存，以防止資料被復原。

附錄 2：英文名詞縮寫

縮寫	全稱
AIA	Authority Info Access
CA	Certification Authority
CAA	Certification Authority Authorization
CP	Certificate Policy
CP OID	Certificate Policy Object Identifier
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
FIPS	(US Government) Federal Information Processing Standard
IETF	Internet Engineering Task Force
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standard
PKI	Public Key Infrastructure
RA	Registration Authority
RFC	Request for Comments