內政部憑證管理中心

憑證實務作業基準

Ministry of the Interior

Certification Authority

Certification Practice Statement

第 1.4 版

內政部

中華民國 99 年 11 月 19 日

目　　錄

摘要

遵循經濟部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，內政部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 09900168560 號

2、簽發之憑證：

(1)種類：自然人公鑰憑證

(2)保證等級：內政部憑證管理中心(以下簡稱憑證管理中心)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，簽發依憑證政策所定義保證等級第 3 級之簽章用及加密用的憑證。

(3)適用範圍：適用於開放網路中電子化政府相關應用服務所需的身分認證及資料加密。用戶及信賴憑證者，必須謹慎使用憑證管理中心所簽發之憑證，不得違反本作業基準所限制及禁止的憑證適用範圍。

3、認證服務的第 3 人稽核：

憑證管理中心每年接受兩項的第 3 人稽核：其一為整體認證服務通過行政院研考會的 GPKI 憑證機構年度外部稽核；其二為資訊安全管理系統通過 ISO27001:2005 評鑑。最新的第 3 人稽核報告請見 http://moica.nat.gov.tw/網站。

4、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，憑證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,憑證管理中心之損害賠償責任以相關法令規定所定之責任範圍為限。

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

(4)註冊中心、註冊窗口及卡管中心因執行業務所引發之法律責任，除法令另有規定外，由憑證管理中心負責。

(5)如因用戶隱瞞事實，提供註冊窗口不正確資料，導致信賴憑證者遭受損害時，如該損害之造成不可歸責於註冊窗口時，應由用戶自負損害賠償之責。

(6)用戶之憑證如須暫停使用、恢復使用或廢止，應依照本作業基準相關規定辦理；如發生私密金鑰資料外洩或遺失等情形，必須廢止憑證時，應立即通知憑證管理中心。但用戶仍應承擔異動前所有使用該憑證之法律責任。

5、其他重要事項：

(1)如因憑證管理中心之系統維護、轉換及擴充等需要，得暫停部分憑證服務，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憑證管理中心損害賠償之理由。

(2)用戶在接受憑證管理中心所簽發之憑證後，即表示已確認憑證內容資訊之正確性，依照本作業基準相關規定使用憑證;如憑證內容資訊有誤,用戶應主動通知憑證管理中心。

(3)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本身因素導致使用者權益受損時，應自行承擔責任。

(4)憑證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，不得以憑證管理中心無法正常運作，作為抗辯他人之事由。

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

1 序論

內政部憑證管理中心憑證實務作業基準(Ministry of the Interior 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 the Government Public Key Infrastructure，以下簡稱憑證政策)訂定，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，說明內政部憑證管理中心(Ministry of the Interior Certification Authority, MOICA，以下簡稱憑證管理中心)如何遵照憑證政策保證等級第 3 級之規定，進行自然人公鑰憑證(以下簡稱憑證)之簽發及管理作業。

1.1 概要

依據憑證政策的規定，憑證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自然人憑證，包括簽章用及加密用的 2 種憑證，皆為憑證政策保證等級第 3 級之憑證。

在本作業基準中，將說明憑證管理中心的憑證作業實務，以確保憑證管理中心的憑證簽發及管理作業符合憑證政策所訂定之保證等級第 3 級之規定。本作業基準所載明之實務作業規範僅適用於與憑證管理中心相關之個體，如憑證管理中心、註冊中心(Registration Authority)、註冊窗口(Registration Authority Counter)、卡管中心(Card Management Center)、用戶(Subscribers)、信賴憑證者(Relying Parties)及儲存庫(Repository)等。

內政部(以下簡稱本部)為憑證管理中心的主管機關，負責本作業基準之訂定及修訂，本作業基準需經電子簽章法主管機關經濟部核可後施行。本作業基準未授權憑證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 憑證實務作業基準之識別

本作業基準之名稱為內政部憑證管理中心憑證實務作業基準(Ministry of the Interior Certification Authority Certification Practice Statement)，本版本為第 1.4 版，公布日期為 99 年 11 月 19 日。本作業基準的最新版本可在以下網頁取得：http://moica.nat.gov.tw/。

本作業基準依據憑證政策訂定，憑證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}。(請參考憑證政策)。

1.3 主要成員及憑證適用範圍

本作業基準所參與認證服務之相關成員包括：

(1)憑證管理中心。

(2)註冊中心。

(3)註冊窗口。

(4)卡管中心。

(5)儲存庫。

(6)終端個體。

1.3.1 內政部憑證管理中心

憑證管理中心是本基礎建設中的第 1 層下屬憑證機構，遵照憑證政策保證等級第 3 級的規定，負責自然人憑證的簽發及管理作業。

1.3.2 註冊中心

憑證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。註冊中心由多個註冊窗口（RA Counter）組成。

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（RA Officer，以下簡稱 RAO）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 RAO 之帳號與權限，製發 RAO 的 IC 卡。註冊中心伺服器上裝設註冊中心之私密金鑰，註冊中心伺服器與憑證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 註冊窗口

註冊窗口可設於各直轄市、縣（市）戶政事務所，或經由憑證管理中心授權核可的組織來擔任。其設置的地點除了在戶政事務所或是授權核可的組織內，另得視需要設立於臨時的機動地點。

註冊窗口 RAO 是負責註冊窗口的運作，以受理該註冊窗口所核可受理的憑證註冊作業，例如憑證之註冊申請、暫停使用申請、恢復使用申請及廢止申請等業務。

1.3.4 卡管中心

用戶憑證金鑰對之符記(Token)為 IC 卡，憑證管理中心將委託可信賴的卡管中心進行 IC 卡製卡及管理作業。IC 卡製卡及管理作業包括 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)及 IC 卡之配送管理。

1.3.5 儲存庫

儲存庫負責公告由憑證管理中心所簽發之憑證、憑證廢止清冊(Certificate Revocation List, CRL)及其他憑證相關資訊。

憑證管理中心除自行建置及維運儲存庫外，將憑證管理中心所簽發之憑證及憑證廢止清冊轉存至憑證管理中心目錄服務(Directory Service, DS)中。

儲存庫提供 24 小時全天的服務，網址為：http://moica.nat.gov.tw/。

1.3.6 終端個體

1.3.6.1 用戶

憑證管理中心之用戶，係指記載於憑證管理中心所簽發憑證的憑證主體名稱(Certificate Subject Name)的自然人個體。

1.3.6.2 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。

信賴憑證者在使用憑證管理中心所簽發之憑證前，必須以憑證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。

1.3.7 適用範圍

1.3.7.1 憑證之適用範圍

憑證管理中心所簽發及管理的憑證類別為自然人憑證，且包含簽章用及加密用憑證。

憑證管理中心所簽發的憑證符合憑證政策保證等級第 3 級之規定，適用於在開放網路中之電子化政府相關應用所需的身分認證及資料加密。

1.3.7.2 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。

信賴憑證者在使用憑證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。

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)。

信賴憑證者在使用憑證管理中心所提供的認證服務前，必須詳細

閱讀本作業基準，遵守本作業基準之規定，同時必須注意本作業基準之修訂。

1.3.7.3 憑證之禁止使用情形

(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。

1.3.8 以委外方式提供認證服務

本部依照政府採購法委託中華電信股份有限公司辦理憑證管理中心之建置及維運。委外對象之名單將公佈於網站。

網址:http://moica.nat.gov.tw

1.4 聯絡方式

1.4.1 憑證實務作業基準之制定及管理機關

憑證管理中心負責制定本作業基準之各項條款。本作業基準之制定及修訂在經電子簽章法主管機關經濟部核可後發布施行。

1.4.2 聯絡資料

如對本作業基準有任何建議，或是發生私密金鑰資料外洩或遺失等情形，請與憑證管理中心聯絡。憑證管理中心之聯絡電話：02-25132252，郵遞地址：104 台北市松江路 469 巷 4 號，電子郵件信

箱：moica@moi.gov.tw，另外客戶服務中心的電話與傳真號碼，請參閱 http://moica.nat.gov.tw/。

1.4.3 憑證實務作業基準之審定

依據電子簽章法相關規定，本作業基準必須經電子簽章法主管機關經濟部核定後，始得對外提供簽發憑證服務。

2 一般條款

2.1 職責及義務

2.1.1 內政部憑證管理中心之職責

(1)依據憑證政策保證等級第 3 級規定與本作業基準運作。

(2)簽發及公布憑證。

(3)廢止、停用及恢復使用憑證。

(4)簽發及公佈憑證廢止清冊。

(5)執行憑證管理中心相關人員之識別及鑑別程序。

(6)安全產製憑證管理中心之私密金鑰。

(7)保護憑證管理中心之私密金鑰。

(8)支援註冊中心進行憑證註冊相關作業。

2.1.2 註冊中心之職責

(1)將用戶之申請資料及公開金鑰透過安全管道傳送給憑證管理中心。

(2)告知用戶及信賴憑證者有關憑證管理中心及註冊中心之義務與責任。

(3)告知用戶及信賴憑證者,有關接受或使用憑證管理中心所簽發之憑證，必須遵守本作業基準之相關規定。

(4)執行 RAO 之識別及鑑別程序。

(5)安全產製註冊中心之私密金鑰。

(6)保護註冊中心之私密金鑰。

2.1.3 註冊窗口之職責

依 1.3.3 節所述的註冊窗口類別，執行被授權的憑證註冊作業，相關的職責如下：

(1)提供憑證各項臨櫃申辦與執行憑證臨櫃申辦之身分識別及鑑別程序。

(2)負責 IC 卡之個人化製卡服務及提供憑證接受作業。

(3)依照 2.5 節所訂的各項費用標準，向申請者收取其申辦項目的費用。

2.1.4 卡管中心之職責

(1)依照 6.1.1.1 節規定，驅動 IC 卡使之在內部安全產製用戶之金鑰對。

(2)以初始碼設定 IC 卡之初始 PIN 碼。

(3)統一初始化印卡。

(4)提供 IC 卡開卡資料管理作業。

(5)提供 IC 卡鎖卡管理作業。

(6)執行 IC 卡配送管理作業。

2.1.5 用戶之義務

(1)應遵守本作業基準之相關規定，確認所提供申請資料之正確性。

(2)在憑證管理中心核定憑證申請並簽發憑證後，用戶應依照 4.3 節規定親自領取憑證 IC 卡與接受憑證。

(3)用戶在接受憑證管理中心所簽發之憑證後，即表示已確認憑證

內容資訊之正確性，依照 1.3.7 節規定使用憑證；如憑證內容資訊有誤，用戶應主動通知憑證管理中心。

(4)應妥善保管及使用憑證 IC 卡。

(5)如須暫停使用、恢復使用、廢止或重新申請憑證，應依照 4.4 節規定辦理；如發生私密金鑰資料外洩或遺失等情形，必須廢止憑證時，應立即通知憑證管理中心。但用戶仍應承擔異動前所有使用該憑證之法律責任。

(6)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本身因素導致信賴憑證者權益受損時，應自行承擔責任。

(7)在應用憑證時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，不得以無法正常運作，作為抗辯他人之事由。

2.1.6 信賴憑證者之義務

(1)在使用憑證管理中心簽發之憑證或查詢憑證管理中心儲存庫時，必須遵守本作業基準之相關規定。

(2)在使用憑證管理中心簽發之憑證時，應先檢驗憑證之保證等級以確保權益。

(3)在使用憑證管理中心簽發之憑證或憑證廢止清冊時，應先檢驗數位簽章，以確認該憑證或憑證廢止清冊是否正確。

(4)在使用憑證管理中心簽發之憑證時，應確認憑證所記載之金鑰用途。

(5)在使用憑證管理中心簽發之憑證時，應先檢驗憑證廢止清冊，以確認該憑證是否有效。

(6)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

應用系統本身因素導致信賴憑證者權益受損時,應自行承擔責任。

(7)憑證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,不得以憑證管理中心無法正常運作，作為抗辯他人之事由。

(8)接受使用憑證管理中心簽發之憑證時,即表示已了解同意有關憑證管理中心法律責任之條款，依照 1.3.7 節規定範圍使用憑證。

2.1.7 儲存庫服務之義務

(1)依照 2.6 節規定，定期公布簽發之憑證、憑證廢止清冊及其他憑證相關資訊。

(2)公布本作業基準的最新資訊。

(3)儲存庫之存取控制依照 2.6.3 節規定辦理。

(4)保障儲存庫資訊之可接取狀態及可用性。

2.2 法律責任

2.2.1 內政部憑證管理中心之責任

2.2.1.1 保證範圍及其限制條件

憑證管理中心依憑證政策保證等級第 3 級運作,遵守本作業基準規定之程序簽發及管理憑證、簽發公布憑證廢止清冊及維持儲存庫正常運作。

2.2.1.2 否認聲明及其限制條件

用戶或信賴憑證者如未依照 1.3.7 節規定之適用範圍使用憑證所

引發之後果，憑證管理中心不負任何法律責任。

2.2.1.3 其他除外條款

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

如因憑證管理中心之系統維護、轉換及擴充等需要，得暫停部分憑證服務，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憑證管理中心損害賠償之理由。

如因 4.4.1 節廢止憑證之事由，用戶應依照 4.4.3 節憑證廢止程序向憑證管理中心提出廢止憑證申請，憑證管理中心會在 1 個工作天內核定廢止憑證申請，完成憑證廢止作業、簽發憑證廢止清冊及公告於儲存庫。用戶於憑證廢止狀態未被公布之前，應採取適當的行動，以減少對信賴憑證者之影響，承擔所有因使用該憑證所引發之責任。

2.2.2 註冊中心之責任

2.2.2.1 保證範圍及其限制條件

註冊中心遵守本作業基準規定之程序，負責收集和驗證用戶的身分及憑證相關資訊之註冊工作，註冊中心將由多個註冊窗口組成，註冊中心因執行註冊工作所引發之法律責任除法令另有規定外，由憑證管理中心負責。

憑證管理中心所簽發之憑證僅對憑證主體身分做確認，由 RAO 審驗用戶之身分及憑證相關資訊；如因用戶隱瞞事實，提供註冊窗口不正確資料，導致信賴憑證者遭受損害時，如該損害之造成不可歸責於註冊窗口時，應由用戶自負損害賠償之責。

2.2.2.2 否認聲明及其限制條件

用戶或信賴憑證者應依照 1.3.7 節規定之適用範圍使用憑證。

2.2.2.3 其他除外條款

如因不可抗力及其他非可歸責於註冊中心之事由，所導致之損害事件，註冊中心不負任何法律責任。

2.2.3 卡管中心之責任

卡管中心遵守本作業基準規定之程序，負責驅動 IC 卡以產製用戶的金鑰對及相關發卡作業，卡管中心因執行卡片管理作業所引發之法律責任由憑證管理中心負責。

2.3 財務責任

憑證管理中心的營運由本部編列預算維持，未向保險公司投保。但本部由審計機關執行財會稽核，其他相關之財務責任依相關法令規定辦理。

2.4 詮釋及施行

2.4.1 適用法律

憑證管理中心因執行憑證簽發及管理作業需要，所簽署的相關協議之解釋及合法性，遵循電子簽章法等相關法令規定辦理。

2.4.2 可分割性、存續、合併及公告通知

如本作業基準的任何一章節不正確或無效時，其他章節仍然有效，本作業基準的修訂依照第 8 章規定辦理。

2.4.3 紛爭之處理程序

用戶與憑證管理中心如有爭議時，雙方應本誠信原則，先進行協商。如協商不成，需訴訟時，以臺灣臺北地方法院為第 1 審管轄法院。

2.5 費用

2.5.1 憑證簽發及展期費用

請至網站查詢相關費用：http://moica.nat.gov.tw/。

2.5.2 憑證查詢費用

請至網站查詢相關費用：http://moica.nat.gov.tw/。

2.5.3 憑證廢止及狀態查詢費用

請至網站查詢相關費用：http://moica.nat.gov.tw/。

2.5.4 其他服務之費用

請至網站查詢相關費用：http://moica.nat.gov.tw/。

2.5.5 請求退費之規定

憑證申辦人如依 4.2.2 節規定申請憑證，如因故無法辦理，所預繳之 IC 卡工本費，得於臨櫃辦理前提出退費申請，退還費用需扣除手續費(IC 卡工本費百分之 20)。相關規定請至網站查詢：http://moica.nat.gov.tw/。

2.6 公布及儲存庫

2.6.1 內政部憑證管理中心之資訊公布

(1) 憑證政策。

(2) 本作業基準。

(3) 憑證廢止清冊。

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

(5) 簽發之憑證。

(6) 憑證暫時停用資訊及其他憑證相關資訊。

(7) 隱私權保護政策。

(8) 最近 1 次之稽核結果。

(9) 憑證管理中心之最新訊息。

2.6.2 公布頻率

(1)本作業基準於主管機關核准後發布，本作業基準修訂依照第 8 章規定發布。

(2)憑證管理中心每天簽發 1 次憑證廢止清冊，公布於儲存庫。

(3)憑證管理中心本身之憑證，於簽發時公布於儲存庫。

(4)簽發之憑證，於簽發時公布於儲存庫。

(5)憑證政策於電子化政府主管機關核准後公佈，後續修訂依照憑證政策第 8 章規定發布。

2.6.3 存取控制

憑證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，連線至憑證管理中心主機之資料庫，擷

取憑證資訊或下載憑證。

有關 2.6.1 節憑證管理中心公布的資訊，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，為保障儲存庫之安全應進行存取控制，且應維持其可接取狀態及可用性。

2.6.4 儲存庫

儲存庫由憑證管理中心負責管理，如因故無法正常運作，將於 2 個工作天內恢復正常運作，儲存庫之網址為：http://moica.nat.gov.tw/。

2.7 稽核方法

2.7.1 稽核之頻率

憑證管理中心接受每年 1 次本基礎建設的外部稽核與不定期的內部稽核，以確認相關運作符合本作業基準所定的安全規定與程序。

2.7.2 稽核人員之身分及資格

由電子化政府主管機關依政府採購法委外辦理本基礎建設憑證機構之外部稽核作業，委託熟悉本基礎建設相關規定及憑證管理中心運作之稽核業者，提供公正客觀的稽核服務，憑證管理中心於稽核時應對稽核人員進行身分識別。

2.7.3 稽核人員及被稽核方之關係

配合電子化政府主管機關辦理本基礎建設憑證機構之外部稽核作業，將委託稽核業者就憑證管理中心的運作進行稽核。

2.7.4 稽核之範圍

(1)憑證管理中心是否遵照本作業基準運作。

(2)本作業基準是否符合憑證政策之規定。

(3)註冊中心、註冊窗口是否遵照本作業基準及相關規定運作。

(4)卡管中心是否遵照本作業基準及相關規定運作。

2.7.5 對於稽核結果之因應方式

如稽核人員發現憑證管理中心或註冊中心之建置與維運不符合憑證政策及本作業基準等規定時，採取以下行動：

(1)紀錄不符合情形。

(2)將不符合情形通知憑證管理中心。

(3)對於不符合規定之項目，憑證管理中心將立即改善，通知原稽核人員進行複核。

(4)依據不符合情形之種類、嚴重性及修正所需時間，憑證管理中心將採取暫停營運、廢止簽發給用戶憑證或其他配合行動。

2.7.6 稽核結果公開之範圍

憑證管理中心將公布最近 1 次的稽核結果於儲存庫，稽核結果除可能導致憑證管理中心系統被攻擊之資訊外，將公布與信賴憑證者相關之資訊。

2.8 資訊保密之範圍

2.8.1 機密之資訊種類

以下由憑證管理中心產生、接收或保管之資料，均視為機密資訊。

(1)用於憑證管理中心營運的私密金鑰及通行碼。

(2)憑證管理中心金鑰分持的保管資料。

(3)用戶憑證之申請資料，未經用戶同意或符合法令規定不得公開或提供第 3 人使用。

(4)憑證管理中心產生或保管之可供稽核及追蹤之紀錄。

(5)稽核人員於稽核過程中產生之稽核紀錄及報告，不得被完整公開。

(6)列為機密等級的營運相關文件。

憑證管理中心之現職及退職人員對於機密資訊均嚴守秘密。

2.8.2 非機密之資訊種類

(1)憑證管理中心儲存庫公布之簽發憑證、已廢止憑證及憑證廢止清冊不視為機密資訊。

(2)識別資訊或記載於憑證的資訊，除特別約定外，不視為機密資訊。

2.8.3 憑證廢止或暫時停用資訊之公開

憑證廢止或暫時停用資訊公布於憑證管理中心儲存庫。

2.8.4 應司法機關等要求釋出資訊

司法機關、監察機關或治安機關如因調查或蒐集證據需要，必須查詢 2.8.1 節機密資訊，依法定程序辦理，不對用戶另作通知；惟憑證管理中心保留向申請查詢之機關收取合理費用之權利。

2.8.5 應用戶要求釋出資訊

用戶得申請查詢 2.8.1 節第(3)款本身之憑證申請資料，憑證管理中心以郵寄信件或電子郵件通知用戶；惟憑證管理中心保留向申請查詢之用戶收取合理費用之權利。

2.8.6 其他資訊釋出之情況

不提供商業應用，至於其他資訊之釋出依相關規定法令辦理。

2.8.7 隱私權保護

憑證管理中心依照電腦處理個人資料保護法處理用戶之申請資料，憑證內容記載用戶的中文姓名，以及國民身分證統一編號的後 4 碼，所以不會因為公布憑證而洩漏個人的國民身分證統一編號，而個人電子郵件位址由用戶自行決定是否要記載於憑證，同時用戶得自行決定是否公布其憑證於憑證管理中心儲存庫，以保障申請民眾之個人資料隱私。

2.9 智慧財產權

憑證管理中心的金鑰對及金鑰分持為憑證管理中心之智慧財產。用戶使用之符記為 IC 卡，由憑證管理中心信賴的卡管中心驅動 IC 卡，而由 IC 卡自行產製金鑰對，該金鑰對之智慧財產權屬於該用

戶。

憑證管理中心所簽發的憑證及憑證廢止清冊為憑證管理中心之智慧財產。

憑證管理中心將儘可能確保用戶名稱的正確性，但不保證用戶名稱之智慧財產權歸屬。用戶名稱如發生爭議時，用戶應依法定程序處理，將處理結果提交憑證管理中心，以確保權益。

因執行憑證管理中心憑證管理作業而撰寫的相關文件，其智慧財產權為本部擁有。

本作業基準之智慧財產權為本部擁有。本作業基準可由憑證管理中心儲存庫自由下載，或依著作權法相關規定重製或散布，必須保證是完整複製，註明著作權為本部所擁有。另外，重製或散布本作業基準者，不得向他人收取費用，亦不得拒絕任何人請求取得。本部對於不當使用或散布本作業基準所引發之一切結果，不負任何法律責任。

3 識別和鑑別程序

3.1 初始註冊

3.1.1 命名種類

憑證管理中心所簽發憑證之憑證主體名稱採用X.500唯一識別名稱(Distinguished Name, DN)。

3.1.2 命名須有意義

憑證管理中心用戶的名稱是以本部戶役政系統資料庫所儲存的中文姓名為主。

3.1.3 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 ITU-T X.520 名稱屬性定義。

3.1.4 命名之獨特性

憑證管理中心的X.500唯一識別名稱為：

C=TW，O=行政院，OU=內政部憑證管理中心

為使憑證管理中心所簽發憑證的憑證主體名稱具備獨特性，憑證管理中心採用的用戶X.500唯一識別名稱格式為：

C=TW，CN=本部戶役政系統資料庫所儲存的中文姓名，serialNumber=憑證管理中心自動給定對該用戶的唯一序號

3.1.5 命名爭議之解決程序

憑證管理中心允許用戶的戶籍中文姓名相同，但會以在唯一識別名稱中的序號(serialNumber)加以區別，以使用戶的名稱可以保持唯一性。

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

3.1.6 商標之辨識、鑑別及角色

不適用。

3.1.7 證明擁有私密金鑰之方式

由憑證管理中心所信賴的卡管中心驅動IC卡，在IC卡內部自行產製金鑰對，簽發憑證時由註冊窗口透過安全管道將用戶之公開金鑰傳送至憑證管理中心，因此用戶在申請憑證時不必證明持有私密金鑰。

3.1.8 組織身分鑑別之程序

不適用。憑證管理中心簽發憑證對象為自然人，無組織身分鑑別之程序。

3.1.9 個人身分鑑別之程序

3.1.9.1 初次申請憑證

註冊窗口的RAO在憑證申請人本人出示國民身分證正本後，應向本部戶役政資料庫查驗該國民身分證是否為有效，並檢驗此國民身分證所記錄的人員是否確實為該申請者，以確認申請者的身分。

同時也應檢驗申請者的年齡是否為18歲以上，設有戶籍之國民，

且未受監護宣告者。

3.1.9.2 各項線上辦理的憑證管理

憑證管理中心有 3 項憑證管理以線上方式辦理，這些線上辦理作業的身分鑑別方式分別規範如下：

(1)線上暫時停用憑證

以 4.1.1 節中用戶所自行選定的用戶代碼來做為身分鑑別的依據。

(2)緊急暫時停用憑證

以傳真相關身分證明的文件做為身分鑑別的依據。詳細的身分證明文件如 4.4.7 節所述。

(3)線上恢復使用憑證

以 4.1.1 節中用戶所自行選定的用戶代碼來做為身分鑑別的依據。

(4)線上申請展期憑證

以現行有效的電子簽章來做為身分鑑別的依據。

3.1.10 硬體裝置或伺服軟體鑑別之程序

憑證管理中心簽發憑證對象為自然人，無硬體裝置或伺服軟體鑑別之程序。

3.2 憑證之金鑰更換及展期

3.2.1 憑證之金鑰更換

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。

如用戶之私密金鑰使用期限屆滿必須更換金鑰時，應向憑證管理中心重新申請憑證，註冊窗口將依照 3.1 節規定，對於重新申請憑證之用戶進行識別及鑑別。

3.2.2 憑證展期

憑證展期係指簽發1張與舊憑證具有相同憑證主體名稱、金鑰及相關資訊的新憑證，新憑證只對有效期限(notAfter)予以展期一段時間，給予1個新的憑證序號。

憑證展期如以臨櫃方式辦理時，用戶身分識別及鑑別程序與3.1節規定相同；憑證展期如以線上方式辦理時，用戶身分識別及鑑別程序以現行有效的私密金鑰做簽章方式進行之。

有關用戶憑證展期的允許次數、期限及其合格條件，如6.3.2.2節所述。

3.3 憑證廢止之金鑰更換

如用戶之私密金鑰因憑證廢止必須更換金鑰時，應向憑證管理中心重新申請憑證，註冊窗口將依照 3.1 節規定，對於重新申請憑證之用戶進行識別及鑑別。

3.4 憑證廢止

憑證廢止申請之鑑別程序與 3.1 節規定相同。

3.5 憑證內容變更

憑證內容變更申請之鑑別程序與 3.1 節規定相同。

3.6 憑證暫時停用與恢復使用

申請人連線至儲存庫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.營運規範

本章中有關憑證初次申請、憑證展期、憑證廢止、憑證暫停使用、憑證恢復使用及憑證內容變更等，如依 2.5 節的規定必須收取費用時,則申請者應配合作業流程的需要,先繳交相關費用後再進行辦理。

4.1 申請憑證之程序

申請人應先閱讀用戶約定條款(Subscriber Agreement)，如同意條款內容再進行憑證申請。

此用戶約定條款會記載於在憑證管理中心的網站(http://moica.nat.gov.tw/)及憑證申請書中。

4.1.1 初次申請憑證

臨櫃申請憑證時，憑證申請人應提供本人之國民身分證正本，以供 RAO 當面確認是否為本人申請。註冊窗口在收到憑證申請資料後，將依本作業基準 3.1.9 節規定，進行身分鑑別程序，以作為判定是否同意憑證申請之依據。

另由 RAO 視業務需要機動地到各組織內臨櫃受理憑證申請時，申請人應填具憑證申請書,及提供本人之國民身分證正本,以供 RAO 當面確認是否為本人申請。RAO 再將已確認身分的憑證申請書依本作業基準 3.1.9 節規定，進行身分鑑別程序，以作為判定是否同意憑證申請之依據。

申請者應選定其個人的用戶代碼及電子郵件位址，以供 RAO 輸入到註冊窗口系統中。

4.1.2 憑證內容變更時之憑證申請

用戶如有變更個人的姓名或國民身分證統一編號等身分資料時，則原憑證由憑證管理中心逕行廢止，用戶如再取得有效的憑證，則需以變更後的姓名或國民身分證統一編號進行憑證的重新申請。申請憑證時，依 4.1.1 節規定的程序做辦理。

用戶可視應用的需要變更憑證中所記載的電子郵件位址，則原憑證由憑證管理中心逕行廢止，接著以更改的電子郵件位址進行憑證的重新申請。重新申請憑證時，依 4.1.1 與 4.2.2 節規定的程序做辦理。

上述的憑證內容變更時，憑證管理中心只對用戶最新且有效的兩張憑證做內容的變更。

4.1.3 憑證遺失時之憑證申請

若用戶曾持有憑證 IC 卡，但是因為遺失或損毀而無法使用，就必須申請新的憑證 IC 卡。在申請之前，必須依 4.4.3 節的規定先將遺失或損毀之憑證做廢止，然後再依 4.1.1 節的規定申請新的憑證。

4.1.4 憑證到期之展期憑證申請

憑證管理中心在6.3.2.2節所訂的憑證金鑰對原則使用期限到期後，可以由用戶自行決定選擇進行金鑰更換或是憑證展期。

當用戶想要申請展期憑證時，則以原憑證效期為參考，各階段憑證展期申請方式如下：

(1)在憑證到期前的 60 天開始至到期的期間內，且憑證目前仍有效下（指已完成接受憑證，未停用，且未廢止），用戶可自行使用憑證展期軟體辦理線上展期，或至各地憑證註冊窗口辦理臨櫃展期。

(2)在憑證到期後開始至到期後滿 3 年的期間內，因憑證已過期失效，無法以線上方式鑑別用戶身分，則用戶需臨櫃至各地憑證註冊窗口辦理憑證展期。

用戶如因故無法於上述憑證到期後滿 3 年內辦理憑證展期，且需繼續使用憑證者，則需依 3.2.1 節進行憑證之金鑰更換及 4.1.1 節的方式重新申請憑證。

4.2 簽發憑證之程序

4.2.1 臨櫃申請憑證時

由以下的步驟完成憑證的簽發：

(1)RAO 確認憑證申請人之身分後，便將憑證申請書的資料輸入到註冊窗口系統中。

(2)RAO 確認輸入資料正確無誤後，以其 IC 卡對憑證申請資料加簽數位簽章，進行 IC 卡的個人化的外觀印製。

(3)註冊窗口系統將相關憑證申請資料上傳至註冊中心。

(4)註冊中心檢驗 RAO 的簽章無誤後，就以完整的憑證申請

訊息向憑證管理中心申請憑證。

(5)憑證管理中心回傳所簽發之憑證，再由註冊窗口系統將簽發的憑證寫入申請人之 IC 卡中。

4.2.2 臨櫃申請憑證內容變更時

由以下的步驟完成憑證的簽發：

(1) RAO 確認憑證申請人之身分後，由註冊窗口系統呈現該申請人憑證內容變更的相關訊息。

(2) RAO 核可憑證內容變更的申請後，對憑證內容變更申請資料加簽數位簽章。

(3) 其餘的步驟如 4.2.1 節的步驟(3)，(4)，(5)。

4.2.3 臨櫃申請展期憑證時

由以下的步驟完成憑證的簽發：

(1) RAO 確認憑證申請人之身分後，由註冊窗口系統呈現是否合於申請展期憑相關的訊息。

(2) RAO 核可展期憑證的申請後，對憑證展期申請資料加簽數位簽章。

(3) 其餘的步驟如 4.2.1 節的步驟(3)，(4)，(5)。

4.2.4 線上申請展期憑證時

由以下的步驟完成憑證的簽發：

(1) 用戶於內政部憑證管理中心下載線上憑證展期軟體，由系統確認用戶之身分及使用期間。

(2) 將憑證展期申請資料進行簽章後，再透過安全加密管道上傳至註冊中心。

(3) 註冊中心檢驗用戶的簽章無誤後，待憑證管理中心完成憑證簽發後，用戶再透過安全加密管道下載憑證並寫入原用戶之 IC 卡中。

如以上之憑證簽發審核不通過時，憑證管理中心將拒絕線上簽發憑證，用戶可連線至儲存庫查詢憑證簽發情形。憑證管理中心擁有拒絕簽發憑證給任何個體之權利，同時對於被拒絕簽發憑證之憑證申請人不負任何損害賠償責任。

4.3 接受憑證之程序

4.3.1 初次申請憑證憑與憑證內容變更時

當完成憑證簽發後，申請者必須親自領取憑證 IC 卡。申請者須可視需要使用以下兩種臨櫃方式之一進行接受憑證的作業：一為臨櫃，另一種為線上方式。

臨櫃進行接受憑證時，註冊窗口系統會列印憑證 IC 卡接受確認書給申請者，申請者應檢視憑證 IC 卡接受確認書所列印有關憑證的

內容，如確認憑證內容無誤，就應接受所簽發的憑證，在憑證 IC 卡接受確認書簽名表示已接受所簽發的憑證，再由 RAO 以該申請者的憑證 IC 卡簽發憑證接受訊息，完成憑證接受的程序。

以線上方式進行接受憑證時，註冊窗口系統會呈現憑證 IC 卡接受確認訊息給申請者，申請者應檢視憑證 IC 卡接受確認訊息中有關憑證的內容，如確認憑證內容無誤，就應於註冊窗口系統上點選確認接受所簽發的憑證。

為考量憑證流通性，在簽發憑證接受訊息~~前~~時預設申請者為公布憑證且將用戶電子郵件信箱寫入其憑證中，並公布用戶憑證於儲存庫，憑證管理中心將視用戶未來的意願公布與否，讓用戶得以於憑證管理中心專屬網站內修改其憑證公布狀態。

如申請者發現憑證內容不正確，則應拒絕接受憑證，向註冊窗口重新申請憑證。如該項憑證內容的錯誤是由憑證管理中心或註冊中心或註冊窗口所引起的，則由註冊窗口主動為申請者做憑證的重新申請；如為申請者所引起的，則由申請者提出憑證的重新申請。

用戶如未能於憑證簽發後 90 個日曆天內，完成憑證接受作業，則視為拒絕接受憑證，該憑證將自動被廢止，也不公布該憑證。

4.3.2 憑證展期時

憑證展期時只展期其效期與變更其憑證序號，其餘內容與原憑證相同。

4.4 憑證暫時停用及廢止

4.4.1 廢止憑證之事由

用戶在以下情形時，必須向註冊窗口提出廢止憑證申請：

(1)懷疑或證實私密金鑰遭到破解。

(2)憑證所記載之資訊重大改變，足以影響其信賴度。例如用戶的姓名已變更。

(3)憑證不再需要使用。

憑證管理中心得就下列情形逕行廢止用戶原有的憑證，毋須事先經過用戶同意：

(1)確認憑證記載之內容不實。

(2)確認用戶之私密金鑰遭冒用、偽造或破解。

(3)確認憑證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)確認用戶之憑證未依本作業基準規定之程序簽發。

(5)確認用戶違反本作業基準或相關法令規定。

(6)依據司法機關正式公文之通知。

(7)用戶死亡或經死亡宣告者。

(8)用戶喪失中華民國國籍者。

(9)用戶做姓名變更者。

(10)用戶國民身分證統一編號變更者。

(11)用戶申請憑證內容變更者。

(12)用戶申請金鑰更換者。

(13)受監護宣告者。

(14)用戶申請憑證展期者。

4.4.2 憑證廢止之申請者

憑證管理中心所認可的憑證廢止之申請者可為以下 2 者：

(1)廢止憑證之用戶。

(2)依正式公文辦理的司法機關。

4.4.3 憑證廢止之程序

廢止憑證之用戶須臨櫃辦理，應提供本人之國民身分證正本，註冊窗口在收到憑證申請資料後，將依本作業基準第 3 章規定，進行身分鑑別程序，以作為判定是否同意廢止憑證之依據，憑證廢止申請審核通過後，用戶可連線至儲存庫查詢憑證廢止情形。

若司法機關依正式公文通知廢止特定的憑證，則憑證管理中心將於審視通知公文後，將憑證廢止。

如以上之廢止申請審核不通過時，憑證管理中心將拒絕廢止憑證。

4.4.4 憑證廢止申請之處理期間

憑證管理中心自註冊窗口受理憑證廢止申請時起，將於 1 個工作天內完成憑證廢止處理程序。

4.4.5 暫時停用憑證之事由

用戶在以下二種情形得申請憑證之暫時停用：

(1)憑證金鑰對之符記遺失或懷疑遭盜用時。

(2)自行認定必須申請憑證之暫時停用。

憑證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：

(1)依據司法機關之正式公文通知。

4.4.6 暫時停用憑證之申請者

以下二者可做為暫時停用憑證之申請者：

(1) 暫時停用憑證之用戶。

(2) 依正式公文辦理的司法機關。

4.4.7 暫時停用憑證之程序

暫時停用憑證之用戶若臨櫃辦理時，應提供本人之國民身分證正本，註冊窗口在收到憑證暫時停用申請後，將依本作業基準 3.1.9 節規定，確認用戶身分，以作為判定是否同意暫時停用憑證之依據。

用戶亦可連線至儲存庫申請暫時停用憑證，但須填寫憑證 IC 卡的卡號與其相對的用戶代碼，以做為身分鑑別依據。用戶如忘記用戶代碼，得臨櫃辦理暫時停用憑證，在 RAO 確認用戶身分後，由 RAO 代為向憑證管理中心提出暫時停用憑證申請，得併同辦理重設用戶代碼。

用戶如遺失憑證 IC 卡，也忘記用戶代碼，因時空限制，而無法利用上述程序之一辦理憑證暫時停用時，則得以緊急暫時停用憑證程序辦理。用戶須以傳真方式辦理緊急暫時停用憑證，檢附含有可鑑別身分之書面資料，例如：身分證正反面影本或警察機關報案三聯單，並署名緊急聯絡電話與本人簽名。憑證管理中心收到傳真申請單後會以電話聯絡申請者，洽詢相關問題進行身分鑑別，以作為判定是否同意緊急暫時停用憑證之依據。傳真號碼請見本作業基準 1.4.2 節之客戶服務聯絡資料，相關細部程序與表單公布於http://moica.nat.gov.tw。

如以上之暫時停用申請審核不通過時，憑證管理中心將拒絕暫時停用憑證。

4.4.8 暫時停用憑證之處理期間及停用期間

憑證管理中心自註冊窗口受理憑證暫時停用申請時起，將於 1 個工作天內完成憑證暫時停用處理程序。

用戶在申請暫時停用憑證時，不必申告所需停用的期間，憑證管理中心所設定憑證暫時停用的最長期間為自核可申請時間到該憑證到期的時間。

如果在憑證暫時停用期間，用戶如辦理完成恢復使用憑證，則該憑證恢復為有效的(Valid)。

4.4.9 恢復使用憑證之程序

用戶在暫時停用憑證後，如需要恢復憑證的使用，得以下列的臨櫃或線上程序完成。

臨櫃申請恢復使用憑證時，申請人應提供本人之國民身分證正本，註冊窗口在收到申請資料後，將依本作業基準 3.1.9 節規定，進行身分鑑別程序，以作為判定是否同意恢復使用憑證之依據。

線上申請恢復使用憑證時，用戶可連線至儲存庫申請恢復使用憑證，須填寫憑證 IC 卡的卡號與其相對的用戶代碼，進行身分鑑別程序，以作為判定是否同意恢復使用憑證之依據。

如以上之恢復使用憑證申請審核不通過時，憑證管理中心將拒絕恢復使用憑證。

4.4.10 憑證廢止清冊之簽發頻率

憑證廢止清冊之簽發頻率為每天 1 次，更新後之憑證廢止清冊公布於儲存庫。

4.4.11 憑證廢止清冊之查驗規定

信賴憑證者在使用憑證管理中心公布於儲存庫之憑證廢止清冊時，應先檢驗其數位簽章，以確認該憑證廢止清冊是否正確。有關信賴憑證者查詢儲存庫公布資訊須具備之要件，詳見於 2.6.3 節之說明。

4.4.12 線上憑證狀態查詢服務

憑證管理中心提供線上憑證狀態(OCSP)查詢服務，相關說明請參閱儲存庫。

4.4.13 線上憑證狀態查詢之規定

如信賴憑證者無法依照 4.4.10 節之規定查詢憑證廢止清冊，則必須使用 4.4.11 節之查詢服務，檢驗所使用的憑證是否有效。

4.4.14 其他形式廢止公告

目前沒有提供其他形式的廢止公告。

4.4.15 其他形式廢止公告之檢查規定

目前沒有提供其他形式的廢止公告。

4.4.16 金鑰被破解時之其他特殊規定

依照 4.4.1、4.4.2 及 4.4.3 節的規定辦理。

4.5 安全稽核程序

憑證管理中心之安全相關事件，均具有安全稽核紀錄(Audit Log)。安全稽核紀錄採系統自動產生、工作紀錄本及紙張等方式。所有安全稽核紀錄均妥善保存，且在執行稽核時可立即取得。安全稽核紀錄之維護依照 4.6.2 節歸檔之保留期限規定辦理。

4.5.1 被記錄事件種類

(1)安全稽核

- 任何重要稽核參數之改變，如稽核頻率、稽核事件型態、新舊參數的內容。
- 任何嘗試刪除或修改稽核紀錄檔。

(2)識別與鑑別

- 嘗試新角色的設定不論成功或失敗。
- 身分鑑別嘗試的最高容忍次數改變。
- 使用者登入系統時身分鑑別嘗試的失敗次數之最大值。
- 如管理者將已被鎖住的帳號解鎖，而且該帳號是因為多次失敗的身分鑑別嘗試而被鎖住的。
- 管理者改變系統的身分鑑別機制，例如從通行密碼改為生物特徵值。

(3)金鑰產製

- 憑證管理中心產製金鑰時(不包括只用在單次或只限 1 次使用的金鑰的產製)。

(4)私密金鑰之載入和儲存

- 載入私密金鑰到系統元件中。
- 所有為進行金鑰回復的工作，對保存在憑證管理中心之私密金鑰所做的存取。

(5)可信賴公開金鑰之新增、刪除及儲存

- 可信賴公開金鑰之改變，包括新增、刪除及儲存。

(6)私密金鑰之輸出

- 私密金鑰之輸出 (不包括只用在單次或只限 1 次使用之金鑰)。

(7)憑證之註冊

- 憑證之註冊申請過程。

(8)廢止憑證

- 憑證之廢止申請過程。

(9)憑證狀態改變之核可

- 核可或拒絕憑證狀態改變之申請。

(10)憑證管理中心組態設定

- 憑證管理中心安全相關之組態設定改變。

(11)帳號之管理

- 加入或刪除角色和使用者。
- 使用者帳號或角色之存取權限修改。

(12)憑證格式剖繪之管理

- 憑證格式剖繪之改變。

(13)憑證廢止清冊格式剖繪之管理

- 憑證廢止清冊格式剖繪之改變。

(14)其他

- 安裝作業系統。
- 安裝憑證管理中心系統。
- 安裝硬體密碼模組。

- 移除硬體密碼模組。
- 銷毀硬體密碼模組。
- 啟動系統。
- 嘗試登入憑證管理中心的憑證管理作業。
- 硬體及軟體之接收。
- 嘗試設定通行密碼。
- 嘗試修改通行密碼。
- 憑證管理中心之內部資料備份。
- 憑證管理中心之內部資料回復。
- 傳送任何資訊到儲存庫公布。
- 存取憑證管理中心之內部資料庫。
- 任何憑證被破解之申告。
- 憑證載入符記。
- 符記之傳遞。
- 符記之零值化。
- 憑證管理中心之金鑰更換。

(15)憑證管理中心之伺服器設定改變

- 硬體。

- 軟體。
- 作業系統。
- 修補程式 (Patches) 。
- 安全格式剖繪。

(16)實體存取及場所之安全

- 人員進出憑證管理中心之機房。
- 存取憑證管理中心之伺服器。
- 得知或懷疑違反實體安全規定。

(17)異常

- 軟體錯誤。
- 軟體檢查完整性失敗。
- 接收不合適訊息。
- 非正常路由之訊息。
- 網路攻擊(懷疑或是確定) 。
- 設備失效。
- 電力不當。
- 不斷電系統(UPS) 失敗。
- 明顯及重大的網路服務或存取失敗。

- 憑證政策之違反。
- 本作業基準之違反。
- 重設系統時鐘。

4.5.2 紀錄檔處理頻率

憑證管理中心每 2 個月檢視 1 次稽核紀錄，追蹤調查重大事件。檢視工作包括驗證稽核紀錄是否被竄改、檢視所有的紀錄項目及檢查任何警示或異常等。檢視稽核紀錄之結果以文件記錄。

4.5.3 稽核紀錄檔保留期限

稽核資料現場(onsite)保留兩個月，依照 4.5.4、4.5.5、4.5.6 及 4.6 節記錄保留管理機制等相關規定辦理。

如稽核紀錄檔的保留期限屆滿，由稽核員負責移除資料，不可由其他人員代理。

4.5.4 稽核紀錄檔之保護

(1)使用簽章、加密技術保存目前和已歸檔之稽核紀錄，使用 CD-R 或其他無法更改稽核紀錄的媒體儲存。

(2)簽署事件紀錄的私密金鑰不能再使用於其他用途，嚴禁稽核系統之私密金鑰另作他用，稽核系統不可洩漏私密金鑰。

(3)手動的稽核紀錄存放於安全場所。

4.5.5 稽核紀錄檔備份程序

電子式稽核紀錄每月備份 1 次。

(1)憑證管理中心週期性地將事件紀錄備份:稽核系統將稽核軌跡資料以每日、每星期及每月等條件週期性地自動歸檔。

(2)憑證管理中心將事件紀錄檔案存放於安全場所。

4.5.6 安全稽核系統

稽核系統內建於憑證管理中心的系統。稽核程序在憑證管理中心系統啟動時啟用，唯有在憑證管理中心系統關閉時才停止。

如自動稽核系統無法正常運作，同時保護系統資料之完整性、機密性的安全機制處於高風險狀態時，憑證管理中心將暫停憑證簽發服務，直到問題解決再行提供服務。

4.5.7 對引起事件者之告知

如因發生事件而被稽核系統記錄，稽核系統不需要告知引起該事件的個體其所引發的事件已經被系統記錄。

4.5.8 弱點評估

憑證管理中心每年至少 1 次對憑證管理系統進行弱點掃描，進行相關的補強措施。

4.6 紀錄歸檔之方法

4.6.1 記錄事件之類型

(1)憑證管理中心被稽核驗證(Accreditation)資料。

(2)憑證實務作業基準。

(3)重要的契約。

(4)系統與設備組態設定。

(5)系統或組態設定修改與更新的內容。

(6)憑證申請資料。

(7)廢止申請資料。

(8)憑證接受的確認紀錄。

(9)符記啟用的紀錄。

(10)已簽發或公告的憑證。

(11)憑證管理中心金鑰更換的紀錄。

(12)已簽發或公告的憑證廢止清冊。

(13)稽核紀錄。

(14)用來驗證及佐證歸檔內容的其它說明資料或應用程式。

(15)稽核人員要求的文件。

(16)依照 3.1.8 及 3.1.9 節所定的組織及個人身分鑑別資料。

4.6.2 歸檔之保留期限

憑證管理中心歸檔資料之保留期限為 10 年；用來處理歸檔資料的應用程式也將維護 10 年。

4.6.3 歸檔之保護

(1)不允許新增、修改或刪除歸檔資料。

(2)憑證管理中心可將歸檔資料移到另一個儲存媒體，提供適當的保護，保護等級不低於原保護等級。

(3)歸檔資料存放於安全場所。

4.6.4 歸檔備份程序

歸檔資料備份至異地備援中心 (參閱 5.1.8 節)。

4.6.5 時戳紀錄之要求

歸檔之電子式紀錄(例如憑證、憑證廢止清冊及稽核紀錄等)包含日期與時間資訊，而且這些紀錄皆經過適當的數位簽章保護，可用以檢測紀錄中的日期與時間資訊是否遭到篡改。但是，這些電子式紀錄中的日期與時間資訊，非公正第 3 者所提供之電子式時戳資料，而是電腦作業系統的日期與時間。憑證管理中心的所有電腦系統都會定期進行校時，以確保電子式紀錄中日期與時間資訊的準確性與可信度。

歸檔的書面紀錄也將記載日期資訊，必要時，將記載時間資訊。書面紀錄的日期與時間紀錄不可任意更改，如需更改必須由稽核人員簽名確認。

4.6.6 歸檔資料彙整系統

憑證管理中心沒有歸檔資料彙整系統。

4.6.7 取得及驗證歸檔資料之程序

必須以書面申請獲得正式授權後，才可取得歸檔資料。

由稽核員負責驗證歸檔資料，書面文件必須驗證文件簽署者及日期等之真偽，電子檔則驗證歸檔資料的數位簽章。

4.7 金鑰更換

憑證管理中心之私密金鑰依照 6.3.2 節規定定期更換。憑證管理中心於憑證到期前 2 個月，更換用來簽發憑證的金鑰對。更換金鑰對後，將向政府憑證總管理中心申請新的憑證，信賴憑證者應使用正確的政府憑證總管理中心之憑證，以驗證憑證管理中心的新金鑰對。

用戶之私密金鑰必須依照 6.3.2 節規定定期更換。如用戶之私密金鑰使用期限屆滿必須更換金鑰時，應依照 4.1 節規定向憑證管理中心申請新的憑證。

4.8 金鑰遭破解或災變時之復原程序

4.8.1 電腦資源、軟體或資料遭破壞之復原程序

憑證管理中心訂定電腦資源、軟體及資料遭破壞之復原程序，同時每年進行演練。

如憑證管理中心的電腦設備遭破壞或無法運作，但憑證管理中心的簽章金鑰未被損毀，則優先回復憑證管理中心儲存庫之運作，迅速重建憑證簽發及管理的能力。

4.8.2 內政部憑證管理中心之簽章金鑰憑證被廢止之復原程序

憑證管理中心的簽章金鑰憑證被廢止時，憑證管理中心將重新產生金鑰對，重新簽發自簽憑證及所有用戶憑證，將所有新的憑證公布在儲存庫中(不包含用戶自行決定不公布之憑證)，公告或通知用戶更換憑證。

4.8.3 內政部憑證管理中心之簽章金鑰遭破解之復原程序

憑證管理中心的私密金鑰有危害之疑慮時，憑證管理中心將重新產生金鑰對，重新簽發自簽憑證及所有用戶憑證，將所有新的憑證公布在儲存庫中(不包含用戶自行決定不公布之憑證)，公告或通知用戶更換憑證。

4.8.4 內政部憑證管理中心安全設施之災後復原工作

憑證管理中心訂定安全設施災後之復原程序，同時每年進行演練。如災害發生時，將優先回復憑證管理中心儲存庫之運作，迅速重建憑證簽發及管理的能力。

4.9 內政部憑證管理中心之終止服務

憑證管理中心終止服務時，將依據電子簽章法相關規定辦理。

憑證管理中心遵守以下事項，以確保終止服務對於用戶與信賴憑證者造成之影響最小：

(1)憑證管理中心於預定終止服務 30 日前，應通知電子簽章法主管機關（經濟部）；將終止服務之事實公告於儲存庫。

(2)憑證管理中心終止服務時將採如下措施：

- 停止簽發新的憑證。
- 終止當時仍具效力之憑證，將於儲存庫繼續提供憑證廢止清冊之服務，直到所有用戶憑證效期到期為止。
- 由政府公開金鑰基礎建設各適當之憑證機構承接各類憑證相關業務，若該類憑證無適當之憑證機構可承接，電子簽章法主管機關得安排其他憑證機構承接。
- 將所有營業期間之紀錄檔案，移交給承接此業務之其他憑證機構。
- 電子簽章法主管機關於必要時，得公告廢止當時仍具效力之憑證。

5.非技術性安全控管

5.1 實體控管

5.1.1 實體所在及結構

憑證管理中心機房位於本部資訊中心，符合政府公信力及儲存高重要性與敏感性的機房設施水準，具備門禁、保全及監視錄影等實體安全機制，以防止未經授權存取憑證管理中心之相關設備。

5.1.2 實體存取

憑證管理中心以保證等級第 3 級的實體控管規定運作。機房共有 4 層門禁，第 1 層分別為全年無休的安全駐警，第 2 層為樓層讀卡機進出管制系統，第 3 層為機房人員指紋辨識進出管制系統，指紋辨識器採用 3 度空間指紋取樣，可以判別辨識物的紋深、色澤及是否為活體，第 4 層為機箱智慧型讀卡器，機房人員必須使用智慧卡才能開啟機箱。

除門禁系統可限制不相干人員接近機房外，機箱之監控系統可控制機箱之開啟，以防止未經授權存取硬體、軟體和硬體密碼模組等相關設備。

任何可攜式儲存媒體帶進機房，需檢查確認沒有電腦病毒及任何可能危害憑證管理中心系統的惡意軟體。

非憑證管理中心人員進出機房，需填寫進出紀錄，由憑證管理中心相關人員全程陪同。

憑證管理中心相關人員離開機房時，將進行以下之查驗工作並記錄，以防止未授權人員進入機房：

(1)確認設備是否正常運作。

(2)確認機箱門是否關閉。

(3)確認門禁系統是否正常運作。

5.1.3 電力及空調

憑證管理中心機房設有獨立之恆溫恆濕空調系統，以控制環境的溫度及濕度，使機房保持最佳運作環境。

5.1.4 水災防範及保護

憑證管理中心機房設置在基地墊高的建築物第 3 樓層，該建築物隔間有防水設施和抽水機。

5.1.5 火災防範及保護

憑證管理中心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，設置手動開關於各機房主要出入口，以供現場人員於緊急情況時以手動方式啟動。

5.1.6 媒體儲存

稽核紀錄、歸檔和備援資料的儲存媒體於憑證管理中心機房儲存 1 年，1 年後將移到異地備援場所儲存。

5.1.7 廢料處理

2.8.1 節所述之憑證管理中心機密資訊，文件資料部分在不需使用時，將經碎紙機處理；磁帶、硬碟、磁碟、磁光碟(MO)及其他形

式的記憶體，在報廢前，將經格式化程序清除儲存的資料，光碟將被實體銷毀。

5.1.8 異地備援

異地備援機房與憑證管理中心距離 30 公里以上，足以避免災害發生時二處均同時受損之情況發生。備援的內容包括資料與系統程式，全部資料備份 1 個星期至少執行 1 次，異動資料備份於異動當天執行。異地備援系統與憑證管理中心系統具有相同的安全等級。

5.2 程序控制

憑證管理中心經由作業程序控管(Procedural Controls)，以規定執行系統相關作業的各種可信賴角色(Trusted Role)、每項工作的人員需求數及每個角色的識別與鑑別，以確保系統作業程序之安全。

5.2.1 信賴角色

憑證管理中心為使執行系統相關作業的責任，能做適當的區隔，以防止某人惡意使用系統而不被察覺，對於每項系統存取作業，明確規定那些信賴角色才能執行此項作業。

憑證管理中心共有 5 種不同的信賴角色，分別為管理員(Administrator)、簽發員(Officer)、稽核員(Auditor)、維運員(Operator)和實體安全控管員(Controller)，每種信賴角色將依照 5.3 節規定進行人員控管，以防止可能的內部攻擊。一種信賴角色可由多人擔任，每種信賴角色設有 1 名主管(Chief Role)，5 種信賴角色的工作內容說明如下：

(1)管理員負責

- 安裝、設定和維護憑證管理中心系統。
- 建立和維護憑證管理中心系統之使用者帳號。
- 設定稽核參數。
- 產製和備份憑證管理中心之金鑰。

(2)簽發員負責

- 啟動或停止憑證簽發服務。
- 啟動或停止憑證廢止服務。

(3)稽核員負責

- 對稽核紀錄的查驗、維護和歸檔。
- 執行或監督內部的稽核，以確認憑證管理中心運作是否遵照本作業基準的規定。

(4)維運員負責

- 系統設備的日常運作維護。
- 系統的備援及復原作業。
- 儲存媒體的更新。
- 除憑證管理中心憑證管理系統外之軟硬體更新。
- 網路及網站的維護：建置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。

(5)實體安全控管員負責：

- 系統的實體安全控管(如機房的門禁管理、防火、防水及空調系統等)。

5.2.2 角色分派

依照 5.2.1 節定義的 5 種信賴角色，憑證管理中心之角色分派必須符合以下規定：

(1) 管理員、簽發員和稽核員 3 種信賴角色不得相互兼任。但可兼任維運員。

(2) 實體安全控管員不得兼任其他 4 種角色工作。

(3) 任何一種信賴角色均不允許執行自我稽核功能。

5.2.3 每個任務所需之人數

依據各種信賴角色的作業安全需求，所需之人數如下：

(1)管理員：至少 3 位合格人員擔任。

(2)簽發員：至少 3 位合格人員擔任。

(3)稽核員：至少 2 位合格人員擔任。

(4)維運員：至少 2 位合格人員擔任。

(5)實體安全控管員：至少 2 位合格人員擔任。

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、設定和維護憑證管理中心憑證管理系統	2				1
建立和維護憑證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
產製和備份憑證管理中心之金鑰	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
除憑證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

5.2.4 識別及鑑別每一個角色

憑證管理中心利用使用者帳號、密碼和群組之系統帳號管理功能及 IC 卡，識別及鑑別管理員、簽發員、稽核員及維運員等不同角色，利用中央門禁系統之權限設定功能，識別及鑑別實體安全控管員。

5.3 人員控制

5.3.1 身家背景、資格、經驗及安全需求

(1)人員甄選及進用之安全評估

- 個人性格之評估。
- 申請者經歷之評估。
- 學術、專業能力及資格之評估。
- 人員身分之確認。
- 人員操守之評估。

(2)人員之考核管理

憑證管理中心之相關人員在進用前先進行資格審查，以確認其資格及工作能力。正式進用後，必須接受適當之教育訓練，以書面方式簽定應負之責任，同時每年進行資格複查，如無法通過資格複查將調離現職，改派其他符合資格人員擔任。

(3)人員之任免及遷調管理

如人員之進用、約聘僱條件或契約有所變更，特別是人員離職或聘僱契約終止時，將遵守維護機密責任之約定。

(4)維護機密責任之約定

憑證管理中心之相關人員均負維護機密之責任，簽署保密切結書，不得以口頭、影印、借閱、交付、文章發表或其他方法洩漏機密。

5.3.2 身家背景之查驗程序

憑證管理中心對於 5.2.1 節所述之各種信賴角色人員，在進用前予以資格審查，以確認其身分資格相關證明文件是否屬實。

5.3.3 教育訓練需求

信賴角色	教育訓練需求
管理員	1、憑證管理中心之安全認證機制。 2、憑證管理中心安裝、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、產製和備份憑證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、憑證管理中心之安全認證機制。 2、憑證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。 5、災後復原及業務永續經營之程序。
稽核員	1、憑證管理中心之安全認證機制。 2、憑證管理中心系統軟硬體的使用及操作程序。 3、產製和備份憑證管理中心金鑰之操作程序。 4、稽核紀錄的查驗、維護和歸檔之程序。 5、災後復原及業務永續經營之程序。
維運員	1、憑證管理中心之安全認證機制。 2、系統設備日常運作之維護程序。 3、儲存媒體之更新程序。 4、災後復原以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

在憑證管理中心之軟硬體升級、工作程序改變、設備更換或相關

法規改變時，將安排相關人員再教育訓練並記錄受訓情形，以確實瞭解相關作業程序及法規之改變。

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，才可轉任簽發員或稽核員。

(2)簽發員調離原職務滿 1 年後，才可轉任管理員或稽核員。

(3)稽核員調離原職務滿 1 年後，才可轉任管理員或簽發員。

(4)擔任維運員滿 2 年，且已接受相關教育訓練及通過審核，才可轉任管理員、簽發員及稽核員。

5.3.6 未授權行動之制裁

憑證管理中心之相關人員，如違反憑證政策與本作業基準或其他憑證管理中心公布之程序，將接受適當的管理與懲處，如情節重大而造成損害者，將採取法律行動追究其責任。

5.3.7 聘雇人員之規定

憑證管理中心聘僱人員安全要求遵照 5.3 節規定。

5.3.8 提供之文件資料

憑證管理中心提供本基礎建設憑證政策、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給憑證管理中心之相關人員。

6.技術性安全控管

6.1 金鑰對之產製及安裝

6.1.1 金鑰對之產製

憑證管理中心依照 6.2.1 節規定，於硬體密碼模組內產製金鑰對，採真實亂數產生器(True Random Number Generator)及 RSA 金鑰演算法，私密金鑰在硬體密碼模組內產製後一直儲存在其中而不外洩。

憑證管理中心之金鑰對產製在本部電子憑證推動小組委員及相關人員見證下，以多人的安全控管機制進行。

用戶使用之符記為 IC 卡，其金鑰對是在卡管中心以安全控管機制驅動 IC 後，在 IC 卡內部自行產製，且金鑰對產製完畢後，其私密金鑰將無法由 IC 卡中匯出。

6.1.2 私密金鑰安全傳送給用戶

憑證管理中心簽發憑證後，由 RAO 將存有私密金鑰的 IC 卡交給用戶。

6.1.3 公開金鑰安全傳送給內政部憑證管理中心

由註冊窗口透過安全管道將用戶之公開金鑰傳送至憑證管理中心。

本節所指的安全管道為使用安全插座層通訊協定（Secure Socket Layer）128bits 或其他相同或更高等級之資料加密傳送方式。

6.1.4 內政部憑證管理中心公開金鑰安全傳送給信賴憑證者

憑證管理中心本身之公鑰憑證由政府憑證總管理中心簽發，公布在政府憑證總管理中心的儲存庫上，信賴憑證者可直接下載及使用。信賴憑證者在使用憑證管理中心本身之公鑰憑證前必須依照政府憑證總管理中心憑證實務作業基準規定，由安全管道取得政府憑證總管理中心之公開金鑰或自簽憑證，然後檢驗政府憑證總管理中心對憑證管理中心本身之公鑰憑證的簽章，以確保公鑰憑證中之公開金鑰是可信賴的。

6.1.5 金鑰長度

憑證管理中心使用2048位元的RSA金鑰以及SHA-1雜湊函數演算法簽發憑證，用戶使用1024或2048位元的RSA金鑰。

6.1.6 公鑰參數之產製

採用 RSA 演算法之公鑰參數為空的(Null)。

6.1.7 金鑰參數品質之檢驗

憑證管理中心採用ANSI X9.31演算法產生RSA演算法所需的質數，該法可保證該質數為強質數(Strong Prime)。

用戶金鑰可於IC卡內部或其他軟硬體密碼模組產生RSA演算法中所需的質數。但不保證該質數為強質數。

6.1.8 金鑰經軟體或硬體產製

憑證管理中心依照6.2.1節規定，使用硬體密碼模組產製亂數、公開金鑰對和對稱金鑰。

卡管中心依照6.2.1節規定，使用IC卡硬體密碼模組產製用戶之金

鑰對。

6.1.9 金鑰之使用目的

憑證管理中心本身之公鑰憑證由政府憑證總管理中心簽發；其中憑證金鑰用途擴充欄位設定使用的金鑰用途位元為 keyCertSign 及 cRLSign。憑證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。

用戶憑證包含簽章用及加密用的 2 對金鑰對。

6.2 私密金鑰保護

6.2.1 密碼模組標準

為符合憑證政策6.2.1節保證等級第3級的規定，憑證管理中心使用安全等級3的獨立(Standalone)硬體密碼模組，用戶是使用安全等級2的IC卡硬體密碼模組。

憑證管理中心所使用的獨立硬體密碼模組是有安全性佐證資料，用戶所使用的IC卡是有可資公信佐證資料。

6.2.2 金鑰分持之多人控管

憑證管理中心金鑰分持之多人控管是採用Shamir’s Secret Sharing的m-out-of-n(以下簡稱m-out-of-n)，這是一種完全隱密(Perfect Secret)的秘密分享(Secret Sharing)方式，可做為私密金鑰分持備份及回復方法。採用此方法可使憑證管理中心私密金鑰的多人控管具有最高的安全度，因此也用來做為私密金鑰之啟動方式(參閱6.2.7節)。

6.2.3 私密金鑰託管

憑證管理中心簽章用私密金鑰不可被託管，憑證管理中心也不負責保管用戶的簽章用私密金鑰。

6.2.4 私密金鑰備份

依照6.2.2節的金鑰分持之多人控管方法備份私密金鑰，使用高安全性的IC卡做為秘密分持的儲存媒體。

6.2.5 私密金鑰歸檔

憑證管理中心簽章用私密金鑰不可被歸檔。憑證管理中心亦不對用戶簽章用私密金鑰進行歸檔。

6.2.6 私密金鑰輸入至密碼模組

憑證管理中心只有在進行金鑰備份回復時，才可將私密金鑰輸入至密碼模組中。

6.2.7 私密金鑰之啟動方式

憑證管理中心之RSA私密金鑰之啟動(Activation)，是以m-out-of-n控管IC卡組進行控制，不同用途的控管IC卡組分別由管理員及簽發員保管。

6.2.8 私密金鑰之停用方式

憑證管理中心之RSA私密金鑰之停用，是以多人授權控管的手動方式進行控制。

6.2.9 私密金鑰之銷毀方式

為避免憑證管理中心舊的私密金鑰被盜用，影響簽發憑證之正確

性，憑證管理中心之私密金鑰生命金鑰屆滿時將加以銷毀，因此，在憑證管理中心完成金鑰更新及簽發新的憑證後，將會把硬體密碼模組中存放舊的私密金鑰之記憶位址填零(Zeroization)，以銷毀硬體密碼模組中舊的私密金鑰。同時，舊的私密金鑰之分持也將進行實體銷毀。

6.3 用戶金鑰對管理之其他規定

用戶必須自行管理金鑰對，憑證管理中心不負責保管用戶的私密金鑰。

用戶憑證金鑰對之符記為IC卡，且1位用戶原則上只能擁有1張憑證IC卡，其中包含兩張均為有效的憑證。

但憑證到期前的60天開始至到期的期間內，用戶如選擇更換金鑰(更換IC卡)，就不能做原有憑證的展期；反之，用戶如選擇將原有的憑證展期，就不能做更換金鑰(更換IC卡)。

用戶如在原憑證到期前，已取得展期憑證時，而申請憑證廢止，則依金鑰對共存共廢的原則，憑證管理中心將會廢止該用戶的所有憑證。

6.3.1 公開金鑰之歸檔

憑證管理中心將進行憑證之歸檔，且依照4.6節規定執行歸檔系統之安全控管，不再另外進行公開金鑰之歸檔。

6.3.2 公開金鑰及私密金鑰之使用期限

6.3.2.1 內政部憑證管理中心公開金鑰及私密金鑰之使用期限

憑證管理中心公開金鑰及私密金鑰之金鑰長度為RSA 2048位元，公開金鑰憑證之使用期限至多為20年，私密金鑰之使用期限至多

為10年。

6.3.2.2 用戶公開金鑰及私密金鑰之使用期限

用戶之公開金鑰及私密金鑰之金鑰長度為RSA 1024位元，公開金鑰憑證之使用期限為5年，私密金鑰之使用期限為5年，於效期到期時得展期1次，且為期3年，而使公開金鑰及私密金鑰的使用期限最長為8年。

憑證管理中心考量RSA 1024位元金鑰被破解之虞，與核發更新使用RSA 2048位元安全強度相當的金鑰所需的時程，因此只對於99年12月31日(含)以前簽發的RSA 1024位元憑證提供憑證展期服務。

用戶之公開金鑰及私密金鑰之金鑰長度為RSA 2048位元，公開金鑰憑證之使用期限為5年，私密金鑰之使用期限為5年，私密金鑰之使用期限為5年，屆時再依金鑰之安全性評估是否可辦理展期。

6.4 啟動資料之保護

6.4.1 啟動資料之產生

憑證管理中心之啟動資料由硬體密碼模組產生，再寫入至m-out-of-n控管IC卡組中。IC卡中的啟動資料將由硬體密碼模組內建的讀卡機直接存取。IC卡的PIN碼直接在硬體密碼模組內建的鍵盤上輸入。

6.4.2 啟動資料之保護

憑證管理中心之啟動資料由m-out-of-n控管IC卡組保護，IC卡的PIN碼由保管人員負責保存，不得記錄於任何媒體上，如登入的失敗次數超過3次，則鎖住此IC卡；IC卡移交時，新的保管人員必須重新

設定新的PIN碼。

6.4.3 其他啟動資料之規定

憑證管理中心的私密金鑰的啟動資料不做歸檔。

6.5 電腦軟硬體安控措施

6.5.1 特定電腦安全技術需求

憑證管理中心和其相關輔助系統透過作業系統，或結合作業系統、軟體和實體的保護措施提供以下安全控管功能：

(1) 具備身分鑑別的登入。

(2) 提供自行定義(Discretionary)存取控制。

(3) 提供安全稽核能力 。

(4) 對於各種憑證服務和信賴角色存取控制的限制。

(5) 具備信賴角色及身分的識別和鑑別。

(6) 以密碼技術確保每次通訊和資料庫之安全。

(7) 具備信賴角色和相關身分識別的安全及可信賴的管道。

(8) 具備程序完整性及安全控管保護。

6.5.2 電腦安全評等

憑證管理中心採用安全強度與TCSEC (Trusted Computer System Evaluation Criteria) C2相當的電腦作業系統。

6.6生命週期技術控管措施

6.6.1系統研發控管措施

憑證管理中心的系統研發遵循 ISO 9001 的規範進行品質控管。

憑證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，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

憑證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，憑證管理中心每天自動檢驗軟體的完整性。

憑證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 生命週期安全評等

每年至少1次評估現行金鑰長度是否有被破解之風險。

6.7 網路安全控管措施

憑證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)，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。

憑證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，自動從內部儲存庫傳送到外部儲存庫。

憑證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 密碼模組安全控管措施

參照 6.1 及 6.2 節規定辦理。

7 格式剖繪

7.1 憑證之格式剖繪

憑證管理中心簽發的憑證之格式剖繪依照本基礎建設技術規範相關規定。

7.1.1 版本序號

憑證管理中心簽發 X.509 v3 版本的憑證。

7.1.2 憑證擴充欄位

憑證管理中心簽發的憑證之憑證擴充欄位依照本基礎建設技術規範相關規定。

7.1.3 演算法物件識別碼

憑證管理中心所簽發憑證中的簽章之演算法的物件識別碼：

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

(OID：1.2.840.113549.1.1.5)

憑證管理中心所簽發憑證中的主體公鑰之演算法的物件識別碼：

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

憑證之主體及簽發者兩個欄位值，使用 X.500 的唯一識別名稱，此名稱的屬性型態遵循 RFC 3280 相關規定。

7.1.5 命名限制

憑證管理中心簽發之憑證，不使用命名限制(nameConstraints)。

7.1.6 憑證政策物件識別碼

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

憑證管理中心簽發之憑證，不使用政策限制擴充欄位(policyConstraints)。

7.1.8 政策限定元之語法及語意

憑證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

憑證管理中心簽發之憑證所含之憑證政策擴充欄位不註記為關鍵擴充欄位。

7.2 憑證廢止清冊之格式剖繪

7.2.1 版本序號

憑證管理中心簽發 X.509 v2 版本的憑證廢止清冊。

7.2.2 憑證廢止清冊擴充欄位

憑證管理中心簽發的憑證廢止清冊依照本基礎建設技術規範相關規定。

8.憑證實務作業基準之維護

8.1 變更程序

本作業基準每年定期評估是否需要修訂，以維持其保證度。修訂方式包括以附加文件方式修訂及直接修訂本作業基準的內容。如憑證政策修訂或物件識別碼變更時，本作業基準將配合修訂。

8.1.1 變更時不另作通知之變更項目

本作業基準重新排版時，不另作通知。

8.1.2 應通知之變更項目

8.1.2.1 變更項目

評估變更項目對用戶或信賴憑證者之影響程度：

(1) 影響程度大者，於憑證管理中心儲存庫公告 30 個日曆天，始得修訂。

(2) 影響程度小者，於憑證管理中心儲存庫公告 15 個日曆天，始得修訂。

8.1.2.2 通知機制

所有變更項目將公告於憑證管理中心儲存庫。

8.1.2.3 意見之回覆期限

對於變更項目有意見者，其回覆期限：

(1) 8.1.2.1 節之(1)影響程度大者，回覆期限為自公告日起 15

個日曆天內。

(2)8.1.2.1 節之(2)影響程度小者，回覆期限為自公告日起 7 個日曆天內。

8.1.2.4 處理意見機制

對於變更項目有意見者，於意見回覆期限截止前，以憑證管理中心儲存庫公告之回覆方式傳送給憑證管理中心，憑證管理中心將考量相關意見，評估變更項目。

8.1.2.5 最後公告期限

本作業基準公告之變更項目依照 8.1.2.2 及 8.1.2.3 節規定進行修訂，公告期限依照 8.1.2.1 節規定至少公告 15 個日曆天，直到本作業基準修訂生效。

8.2 公告及通知之規定

本作業基準修訂後 7 個日曆天內公告於憑證管理中心儲存庫，本作業基準之修訂生效日期，除另有規定外，於公告時生效。

8.3 憑證實務作業基準之審定程序

本作業基準經電子簽章法主管機關經濟部核定後，由憑證管理中心公布。如憑證政策的修訂公告後，本作業基準將配合修訂，送交電子簽章法主管機關經濟部核定。

本作業基準修訂生效後，除另有規定外，如修訂之本作業基準之內容與原本作業基準有所牴觸時，以修訂之本作業基準之內容為準；如以附加文件方式修訂，而該附加文件之內容與原本作業基準有所牴

觸時，以該附加文件之內容為準。