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 2.1 版

主辦機關：內政部

執行機構：中華電信股份有限公司

中華民國 112 年 11 月 16 日

內政部憑證管理中心憑證實務作業基準

版本修訂歷程

版本	生效日期	修訂內容說明
1.0	2003-04-03	頒訂「內政部憑證管理中心憑證實務作業基準」第 1.0 版。
1.1	2003-09-18	修正通過「內政部憑證管理中心憑證實務作業基準」第 1.1 版。
1.2	2005-06-17	修正通過「內政部憑證管理中心憑證實務作業基準」第 1.2 版。
1.3	2008-02-29	修正通過「內政部憑證管理中心憑證實務作業基準」第 1.3 版。
1.4	2010-11-19	修正通過「內政部憑證管理中心憑證實務作業基準」第 1.4 版。
1.5	2011-08-19	修正通過「內政部憑證管理中心憑證實務作業基準」第 1.5 版。
1.6	2013-06-11	修正通過「內政部憑證管理中心憑證實務作業基準」第 1.6 版。
1.7	2014-08-04	修正通過「內政部憑證管理中心憑證實務作業基準」第 1.7 版。
1.8	2015-08-25	修正通過「內政部憑證管理中心憑證實務作業基準」第 1.8 版。
1.9	2016-02-01	修正通過「內政部憑證管理中心憑證實務作業基準」第 1.9 版。
1.91	2019-02-20	修正通過「內政部憑證管理中心憑證實務作業基準」第 1.91 版。
2.0	2021-11-19	修正通過「內政部憑證管理中心憑證實務作業基準」第 2.0 版。
2.1	2024-02-29	修正通過「內政部憑證管理中心憑證實務作業基準」第 2.1 版。

目　　錄

摘要

遵循數位發展部數位產業署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 OOOOOOOOOO 號

2、簽發之憑證：

(1)種類：自然人憑證

(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)適用範圍及使用限制：適用於網路中的身分識別、數位簽章與資料保護。用戶及信賴憑證者應謹慎使用憑證管理中心所簽發之憑證，並應注意本作業基準使用範圍之限制。

3、驗證服務的第三方稽核：

憑證管理中心每年接受 2 項的第三方稽核：其一為整體驗證服務通過數位發展部的 GPKI 憑證機構年度外部稽核；其二為資訊安全管理系統通過 ISO27001:2013 評鑑。最新的第三方稽核結果請見 https://moica.nat.gov.tw/bs.html 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,若可歸責於憑證管理中心或其所屬人員未依本作業基準或相關規定辦理用戶註冊、憑證簽發或停用、廢止作業，憑證管理中心依 9.9 節所訂賠償範圍內，賠償用戶或信賴憑證者因憑證作業致受有直接損害為限，但不包括間接損害。

(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、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。

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，並公告於網站；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)憑證管理中心依用戶申請簽發憑證時，當用戶臨櫃確認憑證內容並收取憑證,或當用戶完成線上確認並同意接受後,即代表用戶接受憑證中心所簽發之憑證。用戶應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用戶及信賴憑證者權益受損時，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。如因此致第三人對憑證管理中心為任何主張或請求時，由用戶及信賴憑證者負責對造成憑證管理中心的損害負賠償責任，賠償以憑證管理中心受有之直接損害為限，但不包括間接損害。

(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 簡介

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，進行自然人憑證(以下簡稱憑證)之簽發及管理作業。

1.1 總覽

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)的第一層下屬憑證機構(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

基準之制訂定及修訂，本作業基準須經電子簽章法主管機關數位發展部數位產業署核可後公告施行。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 文件名稱及識別

文件名稱：「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)

版本：第 2.1 版

公布日期：113 年 02 月 29 日

發布網址：https://moica.nat.gov.tw/law_1.html。

憑證政策物件識別碼(Certificate Policy Object Identifier, CP OID)：id-tw-gpki-certpolicy-class3Assurance、{ id-tw-gpki-certpolicy 3}

1.3 主要成員

本作業基準所參與驗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 本管理中心

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、本部移民署各縣(市)服務站，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)須符合 6.2.1 節規範，憑證管理中心將委託可信賴的卡管中心進行符記產製及管理作業。符記產製及管理作業包括符記內部產製金鑰對、以亂數設定符記之初始個人識別碼(以下簡稱 PIN 碼)及符記之配送管理。

1.3.5 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。

1.3.6 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 其他相關成員

中華電信股份有限公司接受本部委託，分別負責本管理中心之系統維運作業。

1.4 憑證用途

1.4.1 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，本憑證適用於網路中的身分識別、數位簽章及資料保護。

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驗證服務前，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。

1.4.3 憑證之禁止使用範圍

1. 犯罪。
2. 軍令戰情與核生化武器管制。
3. 核能運轉設備。

4. 航空飛行與管制系統。

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

憑證管理中心負責制訂本作業基準之各項條款。本作業基準之制訂須經電子簽章法主管機關數位發展部數位產業署核可後公告施行。

1.5.2 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方式，請參閱 https://moica.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，本作業基準必須經電子簽章法主管機關數位發展部數位產業署核定後，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

憑證實務作業基準之變更依 1.5.3「憑證實務作業基準之審定」規定辦理；憑證政策如有修訂並公告後，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 小時服務，相關資訊公告於網站：「https://moica.nat.gov.tw/」。

儲存庫之存取控制依照 2.4 節「存取控制」規定辦理。

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. 憑證廢止清冊(Certificate Revocation List, CRL)。
2. 提供線上憑證狀態協定(Online Certificate Status Protocol, OCSP)查詢服務。
3. 儲存庫之憑證查詢服務。

2.3 公告頻率或時間

1. 本作業基準審查核定後 10 個工作天內公告於儲存庫。

2. 憑證管理中心每日至少簽發並公告 1 次憑證廢止清冊，公布於儲存庫。

3. 本憑證實務作業基準所指日數，如未特別標示為"工作天"者，均以日曆天計算。

2.4 存取控制機制

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 2.2 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。

3 識別及鑑別程序

3.1 命名

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

憑證管理中心就我國籍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，就外來人口用戶的名稱是以本部移民署之入出國及移民署業務管理系統所儲存的中文或英文姓名為主。

3.1.3 用戶匿名或假名

本管理中心不簽發匿名憑證或假名憑證。

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 ITU-T X.520 名稱屬性定義。

3.1.5 命名獨特性

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，或移民署之入出國及移民署業務管理系統所儲存的中文或英文姓名，

serialNumber=憑證管理中心自動給定對該用戶的唯一序號。

3.1.6 商標之辨識、鑑別及角色

不適用。

3.1.7 命名爭議解決程序

憑證管理中心允許用戶的姓名相同，但會以 3.1.5 節中唯一識別名稱中的序號(serialNumber)或證件號碼加以區別，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

由憑證管理中心所信賴的卡管中心驅動符記，在符記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。

3.2.2 組織身分之鑑別程序

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。

3.2.2.1 網域名稱擁有者鑑別

憑證管理中心簽發憑證對象為自然人，無網域名稱擁有者鑑別之程序。

3.2.3 個人身分之鑑別程序

3.2.3.1 我國人士臨櫃辦理

註冊窗口的RAO在我國籍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人，以確認申請人的身分。

檢驗申請人身分資格，請參閱4.1.1節。

3.2.3.2 外來人口臨櫃辦理

註冊窗口的 RAO 在外來人口申請人本人出示居留證後，應向本部移民署之入出國及移民署業務管理系統，查詢持有該居留證者是否尚在合法居留期間內，並檢驗該居留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。

檢驗申請人身分資格，請參閱4.1.1節。

3.2.3.3 各項線上辦理的憑證管理

憑證管理中心有 8 項憑證管理以線上方式辦理，關於此 8 項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

用戶得以 4.2 節中用註冊窗口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

用戶得以傳真或線上傳輸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 4.9.15 節所述。

(3) 線上恢復使用憑證

用戶得以4.2節中用註冊窗口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

憑證用戶得以憑證管理中心依據憑證政策保證等級第 3 級之個人身分鑑別之程序，提交個人資料或其他佐證資料作為完成憑證申請人或用戶之身分識別與鑑別方式。憑證管理中心採認或信賴之組織或個人之身分識別與鑑別方式由憑證管理中心公告於網站。網站：https://moica.nat.gov.tw/。

(5) 線上申請憑證換發

憑證用戶得以憑證管理中心依據憑證政策保證等級第 3 級之個人身分鑑別之程序，提交個人資料或其他佐證資料作為完成憑證申請人或用戶之身分識別與鑑別方式。憑證管理中心採認或信賴之組織或個人之身分識別與鑑別方式由憑證管理中心公告於網站。網站：https://moica.nat.gov.tw/。

(6) 線上申請憑證

憑證用戶得以憑證管理中心依據憑證政策保證等級第 3 級之個人身分鑑別之程序，提交個人資料或其他佐證資料作為完成憑證申請人或用戶之身分識別與鑑別方式。憑證管理中心採認或信賴之組織或個人之身分識別與鑑別方式由憑證管理中心公告於網站。網站：https://moica.nat.gov.tw/。

(7) 線上申請電子郵件寫入憑證

用戶得以現行有效的憑證，並輔以其國民身分證統一編號或居留證號碼及出生年月日等資訊，經電子簽章來做為身分鑑別之依據。

(8) 線上變更用戶代碼

用戶得以現行有效的憑證，並輔以其國民身分證統一編號或居留證號碼及出生年月日等資訊，經電子簽章來做為身分鑑別之依據。

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 3.2.3 節「個人身分鑑別」規定，以身分證正本或有效居留證提出申請。

3.2.6 交互運作標準

不予規定。

3.2.7 資料正確性

本管理中心應評估資料正確性，評估過程應考慮以下事項：

1. 所提供資料的存在時間。
2. 資料來源的更新頻率。
3. 資料提供者和資料收集的目的。
4. 資料可用性。

5. 資料可公開取得之程度。

6. 偽造或變更資料的相對困難性。

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。

如用戶之私密金鑰使用期限到期必須更換金鑰時，應向憑證管理中心重新申請憑證，註冊窗口將依照 3.2 節規定，對於重新申請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 3.2.3 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

憑證展期係指簽發1張與原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)予以展延一段時間，給予1個新的憑證序號。

我國籍憑證用戶申請憑證展期如以臨櫃方式辦理或委託他人代為辦理時，用戶身分識別及鑑別程序與3.2.3節規定相同；憑證展期如以線上方式辦理時，身分識別及鑑別程序依3.2.3.3節規定進行。

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。

3.4 憑證廢止申請之識別及鑑別

用戶在以下情形時，必須向註冊窗口提出廢止憑證申請：

(1) 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、國民身分證統一編號或居留證號碼已變更。

(3) 憑證不再需要使用。

(4) 憑證毀損或遭到竊取。

憑證管理中心得就下列情形逕行廢止我國籍憑證用戶原有的憑證，毋須事先經過用戶同意，並於廢止後告知用戶廢止原因及相關事項：

(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) 用戶辦理姓名變更者。

(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)憑證管理中心系統遭破壞(如火災、地震等災害)以致無法復原時。

憑證管理中心得就下列情形逕行廢止外來人口憑證用戶原有的憑證，毋須事先經過用戶同意，並於廢止後告知用戶廢止原因及相關事項：

(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) 用戶回復或取得中華民國國籍。

(9) 用戶做姓名變更者。

(10)用戶居留證號碼變更者。

(11)用戶申請憑證內容變更者。

(12)用戶申請金鑰更換者。

(13)受監護宣告者或居留期限到期。

(14)憑證管理中心系統遭破壞(如火災、地震等災害)以致無法復原時。

(15)發生其他經本部移民署撤銷或廢止其居留許可，並註銷其居留證之事由。

3.5 憑證暫時停用與恢復使用之識別及鑑別

(1) 暫時停用憑證之我國籍憑證用戶若臨櫃辦理時，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 3.2.3 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。用戶也可填寫自然人憑證代辦事項委託書並委託他人臨櫃代辦憑證暫時停用，其身分鑑別程序與 3.2.3 節規定相同。

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 卡的卡號或身分識別資料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，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。用戶須以傳真或線上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、居留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。憑證管理中心收到申請單後會以電話聯絡申請人，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 1.5.2 節之客戶服務聯絡資料，相關細部程序與表單公布於 https://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。

(2) 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，比照本作業基準 3.2.3 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。用戶也可填寫自然人憑證代辦事項委託書並委託他人臨櫃代辦憑證恢復使用，其身分鑑別程序與 3.2.3 節規定相同。

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 卡的卡號或身分識別資料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 憑證生命週期營運規範

4.1 申請憑證

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(https://moica.nat.gov.tw/)及憑證申請書中。

4.1.1 憑證之申請者

18 歲以上，設籍於我國之國民或持有居留證之外來人口，且未受監護宣告者。

4.1.2 註冊程序及責任

1. 憑證簽發前應確認憑證申請者之身分。
2. 憑證申請者應提供身分識別相關文件。
3. 用戶責任如下：

(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 節規定確認憑證資訊並接受憑證。

(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 1.4.1 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並申請廢止。

(4) 應妥善保管及使用憑證。

(5) 如須暫停使用、恢復使用、廢止或重新申請憑證，應依照 3.4、3.5 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，不得以憑證管理中心無法正常運作，作為抗辯他人之事由。如因此致第三人對憑證管理中心為任何主張或請求時，由用戶及信賴憑證者負責對造成憑證管理中心的損害負賠償責任，賠償以憑證管理中心受有之直接損害為限，但不包括間接損害。

4.2 申請憑證之程序

1. 臨櫃申請憑證時

初次申請時必須臨櫃申請進行身分確認，可申辦 IC 卡載具或行動裝置載具，我國籍憑證申請人應提供本人之國民身分證正本或依我國籍憑證用戶得以憑證管理中心依據憑證政策保證等級第 3 級之個人身分鑑別之程序，提交個人資料或其他佐證資料，以供 RAO 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 3.2.3 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。

外來人口申請人應提供本人之居留證正本或依我國籍憑證用戶得以憑證管理中心依據憑證政策保證等級第 3 級之個人身分鑑別之程序，提交個人資料或其他佐證資料，以供 RAO 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 3.2.3 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。

2. 集體申請憑證時

另由 RAO 視業務需要機動到各組織內臨櫃受理憑證申請時，我國籍憑證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 3.2.3 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。

3. 線上申請憑證時

持有有效期限內 IC 卡之憑證用戶，可於線上申請行動自然人憑證，並依 3.2.3.3 節「線上申請憑證」規定，進行身分鑑別程序後，再

線上申請憑證作業。

申請人應選定其個人的用戶代碼，以供 RAO 輸入到註冊窗口系統中。用戶代碼為符記遭鎖定時，用於解鎖時使用，此外符記停(復)用作業時亦會使用此用戶代碼進行憑證處理作業。

申請人得依需求申請將電子郵件信箱寫入憑證內，憑證管理中心需依照 3.2.3.節針對欲寫入憑證內之電子郵件信箱進行驗證，以確保申請單位確實擁有該電子郵件信箱之合法權利。

4.2.1 執行識別及鑑別功能

本管理中心依 3.2.3 節「個人身分之鑑別程序」規定辦理識別及鑑別程序。

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 3.2.3 節「個人身分之鑑別程序」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。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。

4.2.3 處理憑證申請之時間

申請資料符合相關規定下，憑證註冊窗口應於 3 個工作天內完成

身分鑑別及資料審核程序。

4.3 簽發憑證之程序

4.3.1 管理中心於憑證簽發時之作業

由以下的步驟完成憑證的簽發：

1. 臨櫃簽發憑證

(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。

(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，再由註冊中心將簽發的憑證寫入申請人之符記中。

2. 線上簽發憑證

(1) 依 3.2.3 節由 RAO 臨櫃或透過線上確認憑證申請人之身分後，將用戶申請資料上傳至註冊中心。

(2) 註冊中心檢驗申請人輸入之身分無誤後，就以完整的憑證申請訊息向憑證管理中心申請憑證。

(3) 憑證管理中心回傳所簽發之憑證，再由註冊中心將簽發的憑證寫入符記中。

申請人得依需求申請將電子郵件信箱寫入憑證內，憑證管理中心需依照 3.2.3 節針對欲寫入憑證內之電子郵件信箱進行驗證，以確保申請單位確實擁有該電子郵件信箱之合法權利。

4.3.2 本管理中心對憑證申請者之通知

1. 憑證簽發後優先以電子郵件方式通知憑證申請者，輔以行動電話簡訊方式另行告知，若憑證申請者上述 2 者聯絡方式皆未提供，憑證申請者則自行臨櫃查詢。

2. 憑證申請者可於憑證管理中心網站查詢憑證申請進度。

3. 如不同意簽發憑證時，應以電子郵件或電話通知憑證申請者，並明確告知不同意簽發之理由。

4.4 接受憑證之程序

1. 本管理中心預先提供憑證主體名稱與憑證主體別名供憑證申請者審視。

2. 憑證申請者確認內容正確並於審視頁面點選憑證接受後，本管理中心即進行憑證簽發並公告於儲存庫。

3. 憑證申請者如發現憑證內容不正確時，應立即通知本管理中心或註冊中心。

4. 憑證申請者如於 90 天內未完成憑證接受作業，該申請案件逕行失效，不另公布。

4.4.1 接受憑證之要件

憑證申請者確認憑證主體名稱與憑證主體別名無誤並接受後，本管理中心依此做為憑證接受之依據。

4.4.2 本管理中心之憑證發布

本管理中心將簽發之憑證公布於儲存庫，完成憑證發布作業。

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 金鑰對及憑證之用途

4.5.1 用戶私密金鑰及憑證使用

1. 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。

2. 用戶金鑰對之產製應符合 6.1.1 節「金鑰對產製」，且用戶須有私密金鑰之控制權。

3. 用戶私密金鑰不得用於簽發憑證。

4. 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。

5. 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。

2. 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)。

3. 信賴憑證者在使用憑證管理中心所提供的驗證服務前，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。

4. 信賴憑證者需驗證憑證有效性，包括憑證及其憑證串鏈中所有憑證機構之憑證。

5. 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。

6. 信賴憑證者應確認憑證用途。

4.6 憑證展期

憑證展期係指簽發1張與原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)予以展延一段時間，給予1個新的憑證序號。

我國籍憑證用戶申請憑證展期如以臨櫃方式辦理或委託他人代為辦理時，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，身分識別及鑑別程序依3.2.3.3節規定進行。

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。

4.6.1 憑證展期之事由

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，可以由我國籍憑證用戶自行決定選擇進行金鑰更換或是憑證展期。

4.6.2 憑證展期之申請者

在憑證到期前的60天開始至到期後3年內，用戶如選擇更換金鑰，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。

用戶如已取得展期憑證，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。

4.6.3 憑證展期之程序

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，可以由我國籍憑證用戶自行決定選擇進行金鑰更換或是憑證展期。

當我國籍憑證用戶想要申請展期憑證時，則以原憑證效期為參考，憑證展期申請方式如下：

在憑證到期前的 60 天開始至到期後 3 年內憑證且未被停用及廢止，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，用戶也可填寫自然人憑證代辦事項委託書並委託他人臨櫃代辦憑證展期，其身分鑑別程序與 3.2.3.3 節規定相同。

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

指重新產生 1 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

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 10 年到期必須更換金鑰時，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。

4.7.1.1 本管理中心憑證之金鑰更換事由

1. 私密金鑰執行簽發憑證用途之使用期限到期。

2. 本管理中心憑證被廢止。

4.7.1.2 用戶憑證之金鑰更換事由

1. 用戶私密金鑰使用期限到期。

2. 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

   政府機關(構)授權之人員。

4.7.3 憑證之金鑰更換程序

1. 本管理中心應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. 用戶應依 4.1 節「申請憑證」及 4.2 節「申請憑證之程序」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「本管理中心對憑證申請者之通知」規定辦理。

4.7.5 金鑰更換之憑證接受程序

1. 本管理中心依總管理中心之憑證實務作業基準相關規定辦理金鑰更換之憑證接受。

2. 用戶依 4.4.1 節「接受憑證之要件」規定辦理金鑰更換之憑證接受。

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

4.8.1 憑證變更之事由

本管理中心不提供用戶進行憑證變更。

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

本管理中心提供全天候(7x24)之憑證暫時停用服務，但不提供全天候(7x24)憑證廢止服務。

4.9.1 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) 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、國民身分證統一編號或居留證號碼已變更。

(3) 憑證不再需要使用。

(4) 憑證毀損或遭到竊取。

憑證管理中心得就下列情形逕行廢止我國籍憑證用戶原有的憑證，毋須事先經過用戶同意，並於廢止後告知用戶廢止原因及相關事項：

(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) 用戶辦理姓名變更者。

(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)憑證管理中心系統遭破壞(如火災、地震等災害)以致無法復原時。

憑證管理中心得就下列情形逕行廢止外來人口憑證用戶原有的憑證，毋須事先經過用戶同意，並於廢止後告知用戶廢止原因及相關事項：

(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) 用戶回復或取得中華民國國籍。

(9) 用戶辦理姓名變更者。

(10)用戶居留證號碼變更者。

(11)用戶申請憑證內容變更者。

(12)用戶申請金鑰更換者。

(13)受監護宣告者或居留期限到期。

(14)憑證管理中心系統遭破壞(如火災、地震等災害)以致無法復原時。

(15)發生其他經本部移民署撤銷或廢止其居留許可，並註銷其居留證之事由。

4.9.2 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人可為以下 5 者：

(1) 廢止憑證之用戶。

(2) 依正式公文辦理的司法機關。

(3) 本部移民署。

(4) 戶政事務所。

(5) 憑證註冊窗口。

4.9.3 憑證廢止之程序

4.9.3.1 憑證廢止方式

用戶廢止憑證 IC 卡須臨櫃辦理，廢止行動自然人憑證可採臨櫃或線上辦理。

1. 臨櫃辦理

用戶應提供本人之國民身分證或居留證正本，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。

2. 線上辦理

用戶須以自然人憑證簽章做為身分識別依據，線上廢止自然人憑證。

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確認公文後，廢止該憑證。

如本部移民署以系統通知居留證註銷資料，則憑證管理中心將於確認通知內容後，廢止該憑證。

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。

4.9.3.2 公告與通知

1. 廢止之憑證最遲於憑證廢止清冊下次更新時間(NextUpdate)前加入憑證廢止清冊中，並將憑證狀態資訊公告於儲存庫，直至該廢止憑證到期為止。

2. 本管理中心得以電子郵件、電話或公文方式通知申請者憑證廢止申請之結果。

4.9.3.3 憑證問題回應機制

1. 問題發現者可將憑證問題反應至 1.5.2 節「聯絡資料」所提供之電子郵件信箱。

2. 本管理中心提供全天候(7x24)憑證問題通報受理與憑證問題回應。

3. 本管理中心於接收到憑證問題後 24 小時內，應提供初步調查報告給用戶與問題發現者。

4. 本管理中心應與用戶及問題發現者共同討論，如須廢止該憑證，依下述準則評估與選定憑證廢止日期：

   (1) 聲稱問題的內容(範圍、內容、嚴重性、重要程度及危害風險)。

   (2) 憑證廢止的後果(對用戶與信賴憑證者的直接與間接影響)。

(3) 針對該憑證或該用戶提出之憑證問題數量。

(4) 提出憑證問題的單位或人員。

(5) 相關的法律條文。

本管理中心受理憑證問題報告或接收到憑證廢止通知之處理期限應依 4.9.5 節「本管理中心處理憑證廢止請求之處理期限」規定辦理。

4.9.4 憑證廢止申請之寬限期

不適用。

4.9.5 本管理中心處理憑證廢止請求之處理期限

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。

4.9.6 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

本管理中心將提前於憑證廢止清冊所記載之下次更新時間前發布下一次憑證廢止清冊。

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(Online Certificate Status Protocol Responder, 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. 本管理中心使用其簽章用私密金鑰簽發 RSA 2048 /SHA-256 之線上憑證狀態協定回應伺服器之憑證。

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. 用戶端至少可使用 HTTP GET 方法執行線上憑證狀態協定查詢服務。

3. 憑證狀態資訊為即時更新。

4. 尚未簽發之憑證，線上憑證狀態協定查詢服務不可回覆其狀態為「正常(Good)」。

4.9.11 其他形式廢止公告

1. 本管理中心依據 RFC 4366 規範支援線上憑證狀態協定裝訂(OCSP Stapling)。

2. 用戶如採用上述協定查詢憑證狀態，本管理中心應透過用戶約定條款或技術檢視等方式要求用戶啟用線上憑證狀態協定裝訂。

4.9.12 金鑰被破解時之其他特殊規定

不予規定。

4.9.13 暫時停用憑證之事由

用戶在以下 2 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。

4.9.14 暫時停用憑證之申請人

以下 2 者可做為暫時停用憑證之申請人：

(1) 暫時停用憑證之用戶。

(2) 依正式公文辦理的司法機關。

4.9.15 暫時停用憑證之程序

暫時停用憑證之我國籍憑證用戶若臨櫃辦理時，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 3.2.3 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。用戶也可填寫自然人憑證代辦事項委託書並委託他人臨櫃代辦憑證暫時停用，其身分鑑別程序與 3.2.3.3 節規定相同。

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 卡的卡號或身分識別資料與其相對的用戶代碼，或以自然人憑證簽章做為身分鑑別依據。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，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、居留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人，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 1.5.2 節之客戶服務聯絡資料，相關細部程序與表單公布於 https://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。

4.9.16 暫時停用憑證期間之限制

憑證管理中心自註冊窗口受理憑證暫時停用申請時起，將於受理申請日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5年到期或8年到期的時間。

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)。

4.9.17 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，比照本作業基準 3.2.3 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。用戶也可填寫自然人憑證代辦事項委託書並委託他人臨櫃代辦憑證恢復使用，其身分鑑別程序與 3.2.3 節規定相同。

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 卡的卡號或身分識別資料與其相對的用戶代碼，或以自然人憑證簽章進行身分鑑別程序，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。

4.10 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。

3. 本管理中心提供全天候(7 x 24)回應窗口處理高優先權的憑證問題，聯絡方式請參閱 1.5.2 節。

4.10.3 可選功能

不予規定。

4.11 終止服務

指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

憑證管理中心機房位於本部資料中心，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 層為全年無休的安全警衛，第 2 層為樓層進出管制系統，第 3 層為機房人員對進出人員進行門禁確認管制，第 4 層為機箱門禁管制，機箱門須透過機房實體管理人員操作監控系統才能開啟。

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，須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，須填寫進出紀錄，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(含)以上，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 汰換設備處理

9.3.1 節所述之憑證管理中心重要資訊，文件資料部分在不需使

用時，應經碎紙機處理；磁帶、硬碟、磁碟、磁光碟(MO)及其他形式的記憶體，在報廢前，應經格式化程序清除儲存的資料，光碟應被實體銷毀。

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 2 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 程序控管

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，明確規定信賴角色之職務及其可執行的作業。

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。1 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

(1) 安裝、設定和維護憑證管理中心系統。

(2) 建立和維護憑證管理中心系統之使用者帳號。

(3) 設定稽核參數。

(4) 產製和備份憑證管理中心之金鑰。

2. 簽發員負責

(1) 啟動或停止憑證簽發服務。

(2) 啟動或停止憑證廢止服務。

3. 稽核員負責

(1) 對稽核紀錄的查驗、維護和歸檔。

(2) 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

(1) 系統設備的日常運作維護。

(2) 系統的備援及復原作業。

(3) 儲存媒體的更新。

(4) 除憑證管理中心憑證管理系統外之軟硬體更新。

(5) 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：

(1) 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 工作內容所需人數

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

任務名稱	管理員	簽發員	稽核員	維運員	實體安全控管員
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

5.2.3 角色識別及鑑別

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。

5.2.4 角色權責劃分

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 1 種信賴角色均不允許執行自我稽核功能。

5.3 人員控管

5.3.1 身家背景、資格、經驗及安全需求

1. 人員甄選及進用之安全評估

(1) 個人性格之評估。

(2) 申請人經歷之評估。

(3) 學術、專業能力及資格之評估。

(4) 人員身分之確認。

(5) 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，將遵守維護保密責任之約定。

4. 維護保密責任之約定

5. 憑證管理中心之相關人員均負保密之責任，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重要資訊。

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

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. 本管理中心系統安裝、設定及維護之操作程序。 3. 建立及維護系統用戶帳號之操作程序。 4. 設定稽核參數之操作程序。 5. 產製及備份本管理中心金鑰之操作程序。 6. 災難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. 憑證簽發之操作程序。 3. 憑證廢止之操作程序。 4. 災難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. 本管理中心稽核系統之使用及操作程序。 3. 稽核紀錄查驗、維護及歸檔之程序。 4. 災難復原及業務永續經營之程序。
維運員	1. 系統備份之作業程序。 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. 災難復原及業務永續經營之程序。
實體安全控管員	1. 設定實體門禁權限程序。 2. 災難復原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. 已接受相關教育訓練及通過審核，才可擔任管理員、簽發員及稽核員。

5.3.6 未授權行動之懲處

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 聘僱人員之規定

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。

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記錄方式。

5.4.1 事件記錄之類型

1. 安全稽核

   - 重要稽核參數之改變。
   - 嘗試刪除或修改稽核紀錄。

2. 識別及鑑別

   - 嘗試設定新角色。
   - 管理者調整身分鑑別嘗試之最高容忍次數。
   - 登入系統失敗。
   - 帳號解鎖。
   - 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

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

稽核紀錄保留 2 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、每星期及每月等周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

稽核系統不須告知引起事件之個體，其引發之事件已被系統記錄。

5.4.8 弱點評估

本管理中心對作業系統、實體設施、憑證管理系統、網路進行弱點評估。

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「組織身分之鑑別程序」規定所定之組織身分鑑別資料。

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 1 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

歸檔紀錄備份至異地備援中心。

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，並取得政府憑證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「公開金鑰及私密金鑰之使用期限」規定定期更換，用戶更換金鑰並申請憑證時，應依 4.2 節「申請憑證之程序」規定辦理。

5.7 金鑰遭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

本管理中心每年對安全設施之災難復原工作進行演練。

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。

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 管理中心金鑰對之產製

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,採符合 FIPS 140-2 安全等級第 3 級之亂數產生機制及 RSA 金鑰演算法,私密金鑰在硬體密碼模組內產製後,金鑰之匯出與匯入須依 6.2.2 與 6.2.6 節規定辦理。

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。

6.1.1.2 用戶金鑰對之產製

用戶使用之符記須符合 6.2.1 節規範，其金鑰對由憑證管理中心所信賴的發卡中心驅動符記，在符記內部自行產製金鑰對，且金鑰對產製完畢後，其私密金鑰無法由符記中匯出。

行動自然人憑證的金鑰對是在用戶信賴之行動載具內產製,且金鑰對產製完畢後，其私密金鑰無法由行動載具內部匯出。

6.1.2 私密金鑰安全傳送予用戶

憑證管理中心簽發憑證後,由憑證管理中心提供用戶使用私密金鑰並啟用符記。

6.1.3 公開金鑰安全傳送予本管理中心

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。

6.1.4 本管理中心公開金鑰安全傳送予信賴憑證者

憑證管理中心本身之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憑證的簽章，以確保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 SHA256 雜湊函數演算法簽發憑證，用戶使用 2048 位元(含)以上的 RSA 或 521 位元(含)以上的 ECC 金鑰。

6.1.6 公開金鑰參數之產製與品質檢驗

1. RSA 演算法之公開金鑰參數為空值。

2. 憑證管理中心採用 ANSI X9.31 演算法或 FIPS 186-3 規範產生 RSA 演算法所需的質數，確保該質數為強質數(Strong Prime)。

3. 用戶金鑰於符記或用戶行動載具內部依 FIPS 186-3 規範產生 RSA 或 ECC 演算法所需之參數。

6.1.7 金鑰使用目的

憑證管理中心本身之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使用 IC 卡或用戶信賴之行動載具。

   (1) IC 卡須通過 FIPS 140-2 安全等級第 2 級或安全強度相當認證。

   (2) 行動載具須通過 FIPS 140-2 安全等級第 1 級或安全強度相當認證。

6.2.2 金鑰分持多人控管

憑證管理中心金鑰分持之多人控管是採用 Shamir 所提出之 m-out-of-n(以下簡稱 m-out-of-n)秘密分享方式，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 6.2.8

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之簽章用私密金鑰進行歸檔。

6.2.6 私密金鑰及密碼模組間傳輸

本管理中心於下列情況進行私密金鑰輸入密碼模組作業：

1. 金鑰持份備援之回復。

2. 更換密碼模組。

6.2.7 私密金鑰儲存於密碼模組

憑證管理中心只有在進行金鑰備份回復及更換密碼模組時，才可將私密金鑰輸入至密碼模組中。並應以 6.2.2 節所訂的多人控管方式進行私密金鑰輸入至密碼模組中，私密金鑰輸入方式可為加密或金鑰分持，以確保輸入過程中不得將金鑰明碼暴露於密碼模組之外。私密金鑰輸入完成後，須將輸入過程產製之相關重要參數完全銷毀。

6.2.8 私密金鑰之啟動方式

憑證管理中心之私密金鑰之啟動(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。

6.2.9 私密金鑰之停用方式

憑證管理中心之私密金鑰之停用，是以多人授權控管的手動方式進行控制。

6.2.10 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，憑證管理中心於私密金鑰生命週期到期時將完成金鑰更新及簽發新的憑證，並於舊私密金鑰不再簽發任何憑證與憑證廢止清冊後，將會把硬體密碼模組中存放舊的私密金鑰之記憶位址其內容零值化(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。

6.2.11 密碼模組評等

密碼模組評等方式依憑證政策6.2.1節「密碼模組標準及控管」規定辦理。

6.3 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可為不同形式但須符合6.2.1節規範，其中包含簽章用及加密用2種均為有效的憑證。

但憑證到期前的60天開始至到期後3年內，用戶如選擇更換金鑰，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。

用戶如已取得展期憑證，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5.5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 本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，使用期限至多為20年，以私密金鑰執行簽發憑證用途之使用期限至多為10年，簽發憑證廢止清冊與線上憑證狀態查詢(OCSP)伺服器憑證則不在此限。但若因憑證相關應用系統無法如期配合金鑰更換期程進行系統修改，導致使用者仍須持舊金鑰簽發之憑證使用應用系統，基於便民服務之立場，可將舊金鑰執行簽發憑證之年限暫時延長。

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RSA2048位元(含)以上或ECC 521位元(含)以上，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。

行動自然人憑證之公開金鑰及私密金鑰的金鑰長度為RSA 2048

位元(含)以上或ECC 521位元(含)以上，公開金鑰憑證之使用期限為1年，私密金鑰之使用期限為1年，效期到期後不得展期，需重新產製金鑰對。

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，若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

憑證管理中心系統及運作環境符合 WebTrust Principles and Criteria for Certification Authorities 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

憑證管理中心使用專用的實體或虛擬主機，以及專用的軟體，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 生命週期安全控管措施

每年至少1次評估現行金鑰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。

憑證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。

6.8 時戳

為確保下述時間之正確性，憑證管理中心定期依據受信賴之時間源每小時進行系統校時。

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「金鑰對產製及安裝」與 6.2 節「私密金鑰保護及密碼模組安全控管措施」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

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

憑證管理中心遵照 RFC 5280 與 ITU-T 規範簽發 X.509 v3 版本之憑證。

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可為其下任一種：

sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256-with-RSA-Signature(11)}

(OID：1.2.840.113549.1.1.11)

sha384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha384-with-RSA-Signature(12)}

(OID：1.2.840.113549.1.1.12)

sha512WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha512-with-RSA-Signature(13)}

(OID：1.2.840.113549.1.1.13)

憑證管理中心所簽發憑證中的主體公開金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 2 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 5280 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須依據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做關鍵性(Critical)與否的註記。

7.2 憑證廢止清冊格式剖繪

7.2.1 版本序號

憑證管理中心遵照 RFC 5280 與 ITU-T 規範簽發 X.509 v2 版本的憑證廢止清冊。

7.2.2 憑證廢止清冊與憑證廢止清冊條目擴充欄位

1. 憑證廢止清冊之憑證廢止清冊擴充欄位(crlExtensions)與憑證廢止清冊條目擴充欄位(crlEntryExtensions)遵照 ITU-T X.509、RFC 5280 及本基礎建設憑證及憑證廢止清冊格式剖繪相關規定。

2. 憑證廢止清冊所使用之必要憑證廢止清冊擴充欄位與憑證廢止清冊條目擴充欄位以及其關鍵性與內容於「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. 未來若新增其他選擇性擴充欄位時，使用方式遵照前述標準之規定。

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 及 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查詢服務之網站。

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：

   - 版本序號

- 待查詢憑證識別碼(Target Certificate Identifier)：包含雜湊函數演算法、憑證簽發者名稱之雜湊值、憑證簽發者公開金鑰之雜湊值及待查詢憑證之憑證序號。

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
待查詢憑證識別碼	包含雜湊函數演算法、憑證簽發者名稱之雜湊值、憑證簽發者公開金鑰之雜湊值及待查詢憑證之憑證序號
憑證狀態碼(Certificate Status)	憑證狀態碼說明如下： 0：表示憑證狀態有效。 1：表示憑證已被廢止。當此欄位註記憑證已被廢止時，尚需註記此憑證廢止之時間與廢止原因，廢止原因應與憑證機構廢止清冊所註記之原因代碼相符。 2：表示憑證狀態未知。
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 線上憑證狀態協定擴充欄位

1. 線上憑證狀態協定擴充欄位欄位依照 RFC 5019 與 RFC 6960 之規定。

2. 線上憑證狀態協定回應訊息擴充欄位應包括線上憑證狀態協定伺服器之憑證機構金鑰識別元(Authority Key Identifier)。

3. 線上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查詢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. 本管理中心每年執行 1 次內部稽核。
2. 本管理中心每年接受 1 次外部稽核，且查核期間不可超過 12 個月。
3. 稽核採用之標準為 WebTrust for CA。

8.2 稽核人員之身分及資格

1. 稽核方須經 WebTrust for CA 標章管理單位授權可於我國執行 WebTrust for CA 及 WebTrust for CA – SSL BR 稽核標準之合格稽核業者。
2. 稽核人員應為合格授權之資訊系統稽核員或具同等資格。
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。

3. 本管理中心每季隨機抽樣至少 3%(不足 1 張則隨機抽樣 1 張)憑證進行審驗。

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

1. 除可能導致系統安全風險及依 9.3 節「業務資訊保密」規定外，本管理中心應於查核區間結束後 3 個月內將最近 1 次外部稽核報告與管理聲明書公布於儲存庫，若延遲公布，應提供合格稽核業者簽署之解釋函。

2. 稽核結果以 WebTrust Principles and Criteria for Certification Authorities 標章之方式呈現於本管理中心網站首頁，點選標章後可閱覽外稽報告與管理聲明書。

3. 公開之稽核文件內容須符合各瀏覽器信賴根憑證計畫相關規定。

9 其他業務與法律事項

9.1 費用

暫不收費。

9.1.1 憑證簽發、展期費用

暫不收費。

9.1.2 憑證查詢費用

暫不收費。

9.1.3 憑證廢止、狀態查詢費用

暫不收費。

9.1.4 其他服務費用

暫不收費。

9.1.5 請求退費程序

不適用。

9.2 財務責任

本管理中心之營運由政府編列預算維持，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「重要資訊之範圍」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、證書頒發機構之 WebTrust 原則和標準 WebTrust Principles and Criteria for Certification Authorities 及個人

資料保護法等規定，處理本管理中心之重要資訊。

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「隱私資料之種類」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、證書頒發機構之 WebTrust 原則和標準 WebTrust Principles and Criteria for Certification Authorities 及個人資料保護法等相關規定進行隱私資料保護。

9.4.5 使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. 使用個人隱私資訊須經用戶同意。

9.4.6 應司法或管理程序釋出資訊

司法機關或檢調單位如因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，重製或散布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 本管理中心之職責與義務

1. 依憑證政策保證等級第 3 級規定與本作業基準運作。
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。

9.6.2 註冊中心之職責與義務

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. 正確檢驗憑證數位簽章、有效性及金鑰用途。

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

本管理中心由本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，產生因不可抗拒與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 日前公告於網站。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「憑證暫時停用及廢止」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

本作業基準由電子簽章法主管機關核定並公告後生效，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數位發展部決議，並經電子簽章法主管機關核定。

9.10.3 終止與存續之效力

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 對參與者之個別通知及溝通

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評估本作業基準是否需要修訂，並經總電子簽章法主管機關核定後實施。

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數位發展部審查，並經電子簽章法主管機關核定後公告。

9.12.2 通知機制與期限

9.12.2.1 通知機制

所有變更項目將公告於儲存庫。

9.12.2.2 變更項目

依變更項目對用戶或信賴憑證者影響程度之不同，經數位發展部審查後公告草案於儲存庫，其通知期限如下：

1. 影響程度大者，於儲存庫公告 15 天，始得提交電子簽章法主管機關進行審查。

2. 影響程度小者，於儲存庫公告 7 天，始得提交電子簽章法主管機關進行審查。

本作業基準如重新排版、辭彙變更或錯別字修訂時，則不另行公告。

9.12.2.3 意見反應期限

用戶或信賴憑證者對變更項目有意見時，其反應期限如下：

1. 影響程度大者，反應期限為自公告日起 15 天內。

2. 影響程度小者，反應期限為自公告日起 7 天內。

9.12.2.4 處理意見機制

1. 對變更項目有意見者於回覆期限截止前，將意見以電子郵件方式提供給本管理中心。

2. 本管理中心進行評估後回覆反應者。

9.12.2.5 最後公告期限

本作業基準之修訂，於電子簽章法主管機關核定後 10 天內公告。

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

用戶與本管理中心發生爭議時，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

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。

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。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，不得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

因不可抗拒與其他非可歸責於本管理中心所導致之損害事件，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。

- **憑證問題報告(Certificate Problem Report)**：金鑰遭破解、憑證被誤用、或憑證遭偽造、破解、濫用或不當使用之投訴。

- **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。

- **授權憑證機構簽發憑證(Certification Authority**

Authorization，CAA)：根據 RFC 6844 規定，授權憑證機構簽發憑證網域名稱系統資源紀錄(The Certification Authority Authorization DNS Resource Record)允許網域名稱系統之網域名擁有者指定憑證機構(一個或多個)取得授權幫該網域簽發憑證。發布授權憑證機構簽發憑證網域名稱系統資源紀錄允許公眾信賴之憑證機構實施額外之控制降低非預期之憑證誤發風險。

- **憑證變更(Certificate Modification)**：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驗證業務之作業準則。

  - 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)。

- **憑證透明度(Certificate Transparency, CT)**：為一個公開監控與稽核網際網路上所有憑證之開放性架構(現以 TLS/SSL 憑

證為優先目標)，透過公開憑證的簽發與存在等資訊給網域所有者、憑證機構、以及網域使用者，供其判斷憑證是否被錯誤或惡意簽發；換言之，其目的係提供一個可用於監控 TLS/SSL 憑證機制與審核特定 TLS/SSL 憑證的公開監控與資訊公開的環境，以遏止憑證相關威脅。憑證透明化機制，主要由憑證透明度日誌、憑證監控者、以及憑證稽核者等三個要素所組成。

- **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。

- **密碼學安全偽亂數生成器(Cryptographically Secure Pseudorandom Number Generator, CSPRNG)**：用於加密系統之亂數生成器。

◆ **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)**：在本基礎建設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。

- **完全吻合網域名稱(Fully Qualified Domain Name, FQDN)**：一種用於指定電腦在網域階層中確切位置的明確網域名稱，由主機名稱(服務名稱)與網域名稱組成，且主機名稱須放置於該名稱之起始位置。其參考範例如下：
  - 「ourserver.ourdomain.com.tw」：ourserver 是主機名稱，ourdomain.com.tw 是網域名稱，其中 ourdomain 是第 3 層網域名稱，com 則是次級網域名稱，tw 則是國碼頂級網域名稱。
  - 「www.ourdomain.com」：www 是主機名稱，ourdomain 是次級網域名稱，com 則是通用頂級網域名稱。

◆ **G**

- **政府憑證總管理中心(Government Root Certification Authority)**：本基礎建設之根憑證機構，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**

- **資訊技術安全評估準則(Information Technology Security Evaluation Criteria, ITSEC)**：於 1991 年由英、法、德、荷等

歐洲國家提出，為歐洲安全評估準則，其定義了 7 種安全評估等級，分別為 E0 至 E6。與可信賴電腦系統安全評估準則不同，其僅說明技術安全之要求，將機密性作為安全增強功能，同時，強調對資訊安全之機密性、完整性及可用性的重要性。

- **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。

◆ **M**

- **行動載具(Mobile Device)**
  - 行動載具係指具基本電腦功能且可運用無線通訊介面存取網路資源的可攜式裝置，亦稱行動裝置。
- **行動自然人憑證(Mobile MOICA Certificate)**
  - 行動自然人憑證係指安裝儲存於內政部行動身分識別應用程式(Application)中的自然人憑證。內政部行動身分識別應用程式安裝於用戶信賴之行動載具。
- **自然人憑證(MOICA Certificate)**
  - 自然人憑證係指由內政部憑證管理中心依本憑證實務作業基準所簽發之憑證。

◆ **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)。

- **線上憑證狀態協定回應伺服器(Online Certificate Status Protocol Responder, OCSP Responder)**：由憑證管理中心授權維運之線上伺服器，其連接至儲存庫，以處理憑證狀態查詢請求。

- **線上憑證狀態協定裝訂(OCSP Stapling)**
  - 一種 TLS/SSL 憑證狀態請求擴充欄位，可替代線上憑證狀態協定成為另一種檢查 X.509 憑證狀態的方法。其運作機

制如下：

✓ 網站向線上憑證狀態協定回應伺服器取得具有「時間限制」之線上憑證狀態協定回應訊息，並暫存之。

✓ 於每次 TLS 連線初始過程中，網站將此暫存之線上憑證狀態協定回應訊息傳送給用戶(通常為瀏覽器)，用戶僅需驗證該回應訊息之有效性，無需向憑證機構發送線上憑證狀態協定查詢封包。

- 此機制可透過網站轉發線上憑證狀態協定回應伺服器定期簽發之 TLS/SSL 憑證有效性訊息，減少用戶向憑證機構查詢 TLS/SSL 憑證狀態之頻率，減輕憑證機構之負擔。

- **組織驗證(Organization Validation, OV)**：SSL/TLS 憑證核發過程中，除了識別及鑑別用戶之網域名稱控制權外，並且依照憑證的保證等級識別及鑑別用戶之組織或個人身分。故連結安裝組織驗證型 SSL/TLS 憑證之網站，可提供 TLS 加密通道，知道該網站之擁有者是誰，並確保傳遞資料之完整性。

◆ **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憑證。

◆ **Q**

- **合格稽核業者(Qualified Auditor)**：符合憑證機構與瀏覽器論壇所發行之 Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates 第 8.2 節規定之稽核資格要求，且與受稽方獨立之的會計師事務所、法人或個人。

◆ **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分(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)**：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)**：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。

- **安全插座層(Secure Socket Layer, SSL)**：由網景公司(Netscape)所設計，主要用於全球資訊網(Web)之安全通訊協定，其可於傳輸層進行網路通信之加密，確保傳送之資料完整性，並可

對伺服器端與用戶端進行身分驗證。其應用獨立於應用層協定，故應用層通訊前，即可透過此安全通訊協定完成加密演算、通信密鑰之協商及伺服器驗證作業。現今最新版本為 SSL 3.0，其於 2014 年 10 月經 Google 發現設計缺陷並建議禁用，現多改採用 TLS 1.3 版安全通訊協定。

◆ **T**

- **傳輸層安全(Transport Layer Security, TLS)**：為一種安全通訊協定，1999 年網際網路工程任務小組將 SSL 進行標準化，公告第一版 TLS 標準(即為 RFC 2246)，隨後陸續公布 RFC 4346、RFC 5246 與 RFC 6176 等更新版本，分別說明 TLS 1.1 與 TLS 1.2 版，現今最新版本為 2018 年網際網路工程任務小組公告之 RFC 8446，即為 TLS 1.3，其移除許多過時或不安全的功能(包括 MD5 與 SHA-224 加密功能)，新增對 ChaCha20、Poly1305、Ed25519、Ed448 、x25519 及 x448 之支援，同時，支援 1-RTT、0-RTT，以減少伺服器端與用戶端連結之延遲時間。

- **可信賴電腦系統安全評估準則(Trusted Computer System Evaluation Criteria,TCSEC)**：為電腦系統安全評估的第一個正式標準，於 1970 年由美國國防科學委員會提出，1985 年由

美國國防部公布，其將電腦系統之安全劃分為四個等級與七種安全等級，主要著重於作業系統的安全性，非強調系統之整體性。

- **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(Zeroization)**：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
CSPRNG	Cryptographically Secure Pseudorandom Number Generator
DN	Distinguished Name
DNS	Domain Name System
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
IETF	Internet Engineering Task Force
ITSEC	Information Technology Security Evaluation Criteria
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OV	Organization Validation
PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standard
PKI	Public Key Infrastructure
RA	Registration Authority

縮寫	全稱
RFC	Request for Comments
SSL	Security Socket Layer
TCSEC	Trusted Computer System Evaluation Criteria
TLS	Transport Layer Security