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 2.3 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 109 年 11 月

目　　錄

摘要 VIII

1.序論 1

1.1 概要 2

1.2 憑證實務作業基準之識別 3

1.3 主要成員及憑證適用範圍 3

1.3.1 工商憑證管理中心 4

1.3.2 註冊中心 4

1.3.3 發卡中心 5

1.3.4 儲存庫 5

1.3.5 終端個體 6

1.3.6 以委外方式提供認證服務 8

1.3.7 適用範圍 8

1.4 聯絡方式 10

1.4.1 憑證實務作業基準之制訂及管理機關 10

1.4.2 聯絡資料 10

1.4.3 憑證實務作業基準之審定 10

2.一般條款 11

2.1 職責及義務 11

2.1.1 工商憑證管理中心之職責 11

2.1.2 註冊中心之職責 11

2.1.3 發卡中心之職責 12

2.1.4 用戶之義務 12

2.1.5 信賴憑證者之義務 13

2.1.6 儲存庫服務之義務 14

2.2 法律責任 15

2.2.1 工商憑證管理中心之責任 15

2.2.2 註冊中心之責任 16

2.2.3 發卡中心之責任 17

2.3 財務責任 17

2.3.1 對用戶及信賴憑證者之賠償責任 17

2.3.2 行政程序 17
2.4 詮釋及施行 18
2.4.1 適用法律 18
2.4.2 可分割性、存續、合併、公告通知 18
2.4.3 紛爭之處理程序 18
2.5 費用 18
2.5.1 憑證簽發、展期費用 18
2.5.2 憑證廢止及線上憑證狀態協定查詢費用 18
2.5.3 其他服務之費用 19
2.5.4 請求退費之規定 19
2.6 公布及儲存庫 19
2.6.1 工商憑證管理中心之資訊公布 19
2.6.2 公布頻率 20
2.6.3 存取控制 20
2.6.4 儲存庫 21
2.7 稽核方法 21
2.7.1 稽核之頻率 21
2.7.2 稽核人員之身分及資格 21
2.7.3 稽核人員及被稽核方之關係 21
2.7.4 稽核之範圍 21
2.7.5 對於稽核結果之因應方式 22
2.7.6 稽核結果公開之範圍 22
2.8 資訊保密之範圍 22
2.8.1 機敏性之資訊種類 23
2.8.2 非機敏性之資訊種類 23
2.8.3 憑證廢止或暫時停用資訊之公開 24
2.8.4 應司法人員要求釋出資訊 24
2.8.5 應民事訴訟要求釋出資訊 24
2.8.6 應用戶要求釋出資訊 24
2.8.7 其他資訊釋出之情況 24
2.8.8 隱私權保護 25
2.9 權利歸屬 25
3.識別和鑑別程序 26

3.1 初始註冊 26
3.1.1 命名種類 26
3.1.2 命名須有意義 26
3.1.3 命名形式之解釋規則 26
3.1.4 命名之獨特性 26
3.1.5 命名爭議之解決程序 28
3.1.6 商標之辨識、鑑別及角色 28
3.1.7 證明擁有私密金鑰之方式 29
3.1.8 組織身分鑑別之程序 29
3.1.9 個人身分鑑別之程序 31
3.1.10 硬體裝置或伺服軟體鑑別之程序 31
3.1.11 寫入憑證內之電子郵件信箱驗證 31
3.2 憑證之金鑰更換及展期 32
3.2.1 憑證之金鑰更換 32
3.2.2 憑證展期 33
3.3 憑證廢止之金鑰更換 33
3.4 憑證廢止 33
3.5 憑證暫時停用與恢復使用 33
4.營運規範 34
4.1 申請憑證之程序 34
4.1.1 憑證之申請程序 34
4.1.2 申請展期憑證之程序 36
4.2 簽發憑證之程序 36
4.2.1 IC 卡正卡憑證及非 IC 卡類憑證簽發程序 37
4.2.2 IC 卡附卡及一站式專屬授權憑證簽發程序 40
4.2.3 展期憑證之簽發審核程序 40
4.2.4 設立專屬用戶憑證之申請程序 40
4.3 接受憑證之程序 40
4.3.1 申請發證 40
4.3.2 逕行發證 42
4.4 憑證暫時停用及廢止 42
4.4.1 廢止憑證之事由 42
4.4.2 憑證廢止之申請者 44

4.4.3 憑證廢止之程序 44
4.4.4 憑證廢止申請之處理期間 46
4.4.5 暫時停用憑證之事由 47
4.4.6 暫時停用憑證之申請者 47
4.4.7 暫時停用憑證之程序 48
4.4.8 暫時停用憑證之處理期間及停用期間 49
4.4.9 恢復使用憑證之程序 50
4.4.10 憑證廢止清冊之簽發頻率 51
4.4.11 憑證廢止清冊之查驗規定 51
4.4.12 線上憑證狀態協定查詢服務 52
4.4.13 線上憑證狀態協定查詢之規定 52
4.4.14 其他形式廢止公告 52
4.4.15 其他形式廢止公告之檢查規定 52
4.4.16 金鑰被破解時之其他特殊規定 52
4.5 安全稽核程序 52
4.5.1 被記錄事件種類 53
4.5.2 紀錄檔處理頻率 57
4.5.3 稽核紀錄檔保留期限 57
4.5.4 稽核紀錄檔之保護 57
4.5.5 稽核紀錄檔備份程序 58
4.5.6 安全稽核系統 58
4.5.7 對引起事件者之告知 58
4.5.8 弱點評估 59
4.6 紀錄歸檔之方法 59
4.6.1 紀錄事件之類型 59
4.6.2 歸檔之保留期限 60
4.6.3 歸檔之保護 60
4.6.4 歸檔備份程序 60
4.6.5 時戳紀錄之要求 60
4.6.6 歸檔資料彙整系統 61
4.6.7 取得及驗證歸檔資料之程序 61
4.7 金鑰更換 61
4.8 金鑰遭破解或災變時之復原程序 62
4.8.1 電腦資源、軟體或資料遭破壞之復原程序 62

4.8.2 工商憑證管理中心簽章金鑰憑證被廢止之復原程序 62
4.8.3 工商憑證管理中心簽章金鑰遭破解之復原程序 62
4.8.4 工商憑證管理中心安全設施之災後復原工作 63
4.9 工商憑證管理中心之終止服務 63
5.非技術性安全控管 64
5.1 實體控管 64
5.1.1 實體所在及結構 64
5.1.2 實體存取 64
5.1.3 電力及空調 65
5.1.4 水災防範及保護 65
5.1.5 火災防範及保護 65
5.1.6 媒體儲存 66
5.1.7 廢料處理 66
5.1.8 異地備援 66
5.2 程序控制 66
5.2.1 信賴角色 67
5.2.2 角色分派 68
5.2.3 每個任務所需之人數 69
5.2.4 識別及鑑別每一個角色 71
5.3 人員控制 71
5.3.1 身家背景、資格、經驗及安全需求 71
5.3.2 身家背景之查驗程序 72
5.3.3 教育訓練需求 72
5.3.4 人員再教育訓練之需求及頻率 74
5.3.5 工作調換之頻率及順序 74
5.3.6 未授權行動之制裁 74
5.3.7 聘雇人員之規定 74
5.3.8 提供之文件資料 75
6.技術性安全控管 76
6.1 金鑰對之產製及安裝 76
6.1.1 金鑰對之產製 76
6.1.2 私密金鑰安全傳送給用戶 76
6.1.3 公開金鑰安全傳送給工商憑證管理中心 77

6.1.4 工商憑證管理中心公開金鑰安全傳送給信賴憑證者 77
6.1.5 金鑰長度 78
6.1.6 公開金鑰參數之產製 78
6.1.7 金鑰參數品質之檢驗 78
6.1.8 金鑰經軟體或硬體產製 78
6.1.9 金鑰之使用目的 79
6.2 私密金鑰保護 79
6.2.1 密碼模組標準 79
6.2.2 金鑰分持之多人控管 79
6.2.3 私密金鑰託管 80
6.2.4 私密金鑰備份 80
6.2.5 私密金鑰歸檔 80
6.2.6 私密金鑰輸入至密碼模組 80
6.2.7 私密金鑰之啟動方式 81
6.2.8 私密金鑰之停用方式 81
6.2.9 私密金鑰之銷毀方式 82
6.3 用戶金鑰對管理之其他規定 82
6.3.1 公開金鑰之歸檔 83
6.3.2 公開金鑰及私密金鑰之使用期限 83
6.4 啟動資料之保護 83
6.4.1 啟動資料之產生 83
6.4.2 啟動資料之保護 84
6.4.3 其他啟動資料之規定 85
6.5 電腦軟硬體安控措施 85
6.5.1 特定電腦安全技術需求 85
6.5.2 電腦安全評等 85
6.6 生命週期技術控管措施 86
6.6.1 系統研發控管措施 86
6.6.2 安全管理控管措施 86
6.6.3 生命週期安全評等 86
6.7 網路安全控管措施 86
6.8 密碼模組安全控管措施 87
7.格式剖繪 88

7.1 憑證之格式剖繪 88
7.1.1 版本序號 88
7.1.2 憑證擴充欄位 88
7.1.3 演算法物件識別碼 88
7.1.4 命名形式 88
7.1.5 命名限制 89
7.1.6 憑證政策物件識別碼 89
7.1.7 政策限制擴充欄位之使用 89
7.1.8 政策限定元的語法及語意 89
7.1.9 憑證政策擴充欄位之關鍵性語意註記 89
7.2 憑證廢止清冊之格式剖繪 89
7.2.1 版本序號 89
7.2.2 憑證廢止清冊擴充欄位 89
8.憑證實務作業基準之維護 90
8.1 變更程序 90
8.1.1 變更時不另作通知之變更項目 90
8.1.2 應通知之變更項目 90
8.2 公告及通知之規定 91
8.3 憑證實務作業基準之審定程序 91

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 10902429290 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)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認證及資料加密，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) 用戶之憑證如需暫時停用、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.序論

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)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。

1.1 概要

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 憑證實務作業基準之識別

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 2.3 版，公布日期為中華民國 109 年 11 月 04 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 主要成員及憑證適用範圍

本管理中心之相關成員包括：

(1) 工商憑證管理中心。

(2) 註冊中心。

(3) 發卡中心。

(4)儲存庫。

(5)終端個體（End Entity，EE）。

1.3.1 工商憑證管理中心

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 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。

1.3.4 儲存庫

本管理中心自行建置及維運儲存庫，負責公告由本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。

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

1.3.5 終端個體

1.3.5.1 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，用戶為公司或有限合夥名稱預查申請核准之準公司與準有限合夥等事業主體。

用戶使用之符記主要採 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），正附 IC 卡皆存有兩對金鑰對，一為簽章用金鑰對，另一為加解密用金鑰對，因此本管理中心將對每張 IC 卡簽發簽章用及加解密用兩種憑證。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 3.1 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 3.1 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。

1.3.5.2 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。

1.3.6 以委外方式提供認證服務

本部委託中華電信股份有限公司，負責本管理中心之建置及系統維運作業。

1.3.7 適用範圍

1.3.7.1 憑證之適用範圍

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認證及資料加密，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。

1.3.7.2 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 卡需確認正附卡別。

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認證服務前，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。

1.3.7.3 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。

(5)法令公告禁止適用之範圍。

1.4 聯絡方式

1.4.1 憑證實務作業基準之制訂及管理機關

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。

1.4.2 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/。

1.4.3 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。

2.一般條款

2.1 職責及義務

2.1.1 工商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，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) 簽發及公布憑證服務。

(3) 廢止憑證、暫時停用憑證、恢復使用憑證。

(4) 簽發及公布憑證廢止清冊。

(5) 執行本管理中心與註冊中心相關人員之識別及鑑別程序。

(6) 安全產製本管理中心之私密金鑰。

(7) 保護本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。

(9) 提供憑證接受作業。

2.1.2 註冊中心之職責

(1) 提供憑證申請、發放或線上註冊申請服務。

(2) 執行憑證申請之識別及鑑別程序。

(3) 將申請資料及公開金鑰透過安全管道傳給本管理中心。

(4) 告知用戶及信賴憑證者有關本管理中心及註冊中心之義務與

責任。

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

(6) 執行憑證註冊審驗人員之識別與鑑別程序。

(7) 安全產製註冊中心之私密金鑰。

(8) 保護註冊中心之私密金鑰。

2.1.3 發卡中心之職責

(1) 依照 6.1.1.1 節規定，於 IC 卡內部安全產製用戶之金鑰對。

(2) 以亂數設定 IC 卡之初始 PIN 碼。

(3) 將憑證寫入 IC 卡及印卡。

(4) 郵寄 IC 卡予用戶或其授權單位。

(5) 執行卡片管理作業。

2.1.4 用戶之義務

(1) 應遵守本作業基準之規定，並確保所提供申請資料之正確性。

(2) 在本管理中心核定憑證申請並簽發憑證或逕行簽發憑證後，用戶應依照 4.3 節規定接受憑證。

(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 1.3.7 節規定使用憑證，如憑證內容資訊有誤，用戶應主動通知本管理中心。

(4) 如採用其他符記自行產生金鑰，應依照 6.2.1 節規定，慎選安全的電腦環境及符記，如因電腦環境或應用符記本身因素導致信賴憑證者權益受損時，應自行承擔責任。

(5) 應依照 6.2 節及 6.4 節規定妥善保管及使用私密金鑰。

(6) 如須暫時停用、恢復使用、廢止或重發憑證，應依照第 4 章規定辦理，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。

(7) 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。

(8) 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。

2.1.5 信賴憑證者之義務

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

(2) 在使用本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) 在使用本管理中心簽發之憑證時，應確認憑證所記載之類別及金鑰用途，若符記為 IC 卡需確認正附卡別。

(4) 在使用本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。

(5) 在使用本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。

(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) 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。

(8) 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 1.3.7 節規定範圍使用憑證，並僅於憑證使用目的範圍內信賴該憑證。

2.1.6 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 工商憑證管理中心之責任

2.2.1.1 保證範圍及其限制條件

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

2.2.1.2 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，本管理中心不負任何法律責任。

2.2.1.3 責任上限

本管理中心對用戶或信賴憑證者間，因簽發憑證或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相關法令規定所訂之責任範圍為限。

2.2.1.4 其他除外條款

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。

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。

如因 4.4.1 節廢止憑證之事由，用戶應依照 4.4.3 節憑證廢止程序提出廢止憑證申請。本管理中心將在核定廢止憑證申請後 1 個工作天內完成憑證廢止作業、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，並承擔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依相關法令規定辦理。

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線上註冊窗口審驗用戶之身分及憑證相關資訊，如因用戶隱瞞事實，提供註冊中心不正確資料，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。

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 責任上限

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，註冊中心與本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。

2.2.2.4 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 發卡中心之責任

發卡中心遵守本作業基準規定之程序，負責產製用戶的金鑰對及相關發卡作業，因可歸責於發卡中心之事由所生損害，由本管理中心負責處理。

2.3 財務責任

本管理中心營運以使用者付費為原則，不足部分由本部編列預算維持。本管理中心未向保險公司投保，但每年均由審計部執行財會稽核，其他相關之財務責任依相關法令規定辦理。

2.3.1 對用戶及信賴憑證者之賠償責任

對用戶及信賴憑證者之賠償責任依相關法令規定辦理。

2.3.2 行政程序

依相關法令規定辦理。

2.4 詮釋及施行

2.4.1 適用法律

本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，遵循我國相關法令規定辦理。

2.4.2 可分割性、存續、合併、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

用戶與本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，以台灣台北地方法院為第一審管轄法院。

2.5 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。

2.5.1 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/。

2.5.2 憑證廢止及線上憑證狀態協定查詢費用

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）。

2.5.3 其他服務之費用

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

2.5.4 請求退費之規定

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/。

2.6 公布及儲存庫

2.6.1 工商憑證管理中心之資訊公布

(1) 本作業基準。

(2) 憑證廢止清冊。

(3) 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的所有憑證效期到期為止）。

(4) 簽發之憑證。

(5) 隱私權保護政策。

(6) 最近 1 次之稽核結果。

(7) 本管理中心相關最新訊息。

(8) 憑證政策。

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) 本管理中心每天簽發 1 次憑證廢止清冊，公布於儲存庫。

(3) 本管理中心本身之憑證，於簽發後 1 個工作天內公布於儲存庫。

(4) 簽發之憑證，於簽發後 1 個工作天內公布於儲存庫。

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

2.6.3 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 2.6.1 節本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，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。

2.6.4 儲存庫

儲存庫由本管理中心負責管理，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：https://moeaca.nat.gov.tw。

2.7 稽核方法

2.7.1 稽核之頻率

本管理中心接受每年 1 次本基礎建設的外部稽核與至少 1 次的內部稽核，以確認相關運作符合本作業基準所訂的安全規定與程序。

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本管理中心運作之稽核業者，提供公正客觀的稽核服務，本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，將委託稽核業者就本管理中心的運作進行稽核。在委託該稽核業者進行稽核之前，將由電子化政府主管機關評估該稽核業者對於本管理中心的中立性，以確保稽核報告的客觀性。

2.7.4 稽核之範圍

(1) 本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) 註冊中心是否遵照本作業基準及相關規定運作。

(4) 發卡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

如稽核人員發現本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規定時，採取以下行動：

(1) 記錄不符合情形。

(2) 將不符合情形通知本管理中心。

(3) 對於不符合規定之項目，本管理中心將立即改善，並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，本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

本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本管理中心系統被攻擊之資訊外，與信賴憑證者相關資訊均將公布。

2.8 資訊保密之範圍

本節說明憑證認證服務過程中，可能取得用戶個人資料之保護機敏性資訊之種類及公開資訊的範圍。

2.8.1 機敏性之資訊種類

以下由本管理中心產生、接收或保管之資料，均視為機敏性資訊：

(1) 用於本管理中心營運的私密金鑰及通行碼。

(2) 本管理中心金鑰分持的保管資料。

(3) 用戶填寫之申請資料（用戶資料包括事業主體正式登記名稱、統一編號及聯絡人之姓名、電子郵件信箱、通訊地址及電話等），未經用戶同意或符合法令規定，不得公開或提供第 3 方使用。

(4) 本管理中心因辦理逕行發證，而向其他公務機關取得之個人資料。

(5) 本管理中心產生或保管之可供稽核及追蹤之紀錄。

(6) 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。

(7) 列為機敏性資訊的營運相關文件。

現職或曾任職於本管理中心之人員，對於因營運、職務所接觸之機敏性資訊或契約規範不得外洩之內容均應負保密責任；現職或曾任職之外部稽核人員亦同。

2.8.2 非機敏性之資訊種類

(1) 本管理中心儲存庫公布之憑證、已廢止憑證及憑證廢止清冊

不視為機敏性資訊。

(2) 識別資訊或記載於憑證的資訊，除特別約定外，不視為機敏性資訊。

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將公布於本管理中心儲存庫。

2.8.4 應司法人員要求釋出資訊

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 節機敏性資訊，依法定程序辦理，不對用戶另作通知；惟本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 應民事訴訟要求釋出資訊

司法機關如因調查或蒐集證據需要，必須查詢 2.8.1 節機敏性資訊，依法定程序辦理，不對用戶另作通知；惟本管理中心保留向申請查詢之機關收取合理費用之權利。

2.8.6 應用戶要求釋出資訊

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

2.8.7 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。

2.8.8 隱私權保護

本管理中心依照個人資料保護法暨相關法規蒐集、處理及使用用戶之申請資料。

2.9 權利歸屬

本管理中心的金鑰對及金鑰分持為本管理中心之財產。用戶使用之符記為 IC 卡或其他載具，由本管理中心信賴的發卡中心代為產製金鑰對或自行產製金鑰對，該金鑰對之所有權為該用戶所有。

本管理中心所簽發的憑證及憑證廢止清冊，其著作權為本管理中心所有。

本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。用戶名稱如發生註冊商標爭議時，用戶應依法定程序處理，並將處理結果提交本管理中心，以確保權益。

因執行本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所有。

本作業基準之智慧財產權為本部所有。本作業基準可由本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，並註明著作權為本部所有。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

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）。

3.1.2 命名須有意義

事業主體憑證、一站式專屬授權及設立專屬用戶憑證之憑證主體名稱必須符合公司法、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 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。

3.1.4 命名之獨特性

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

O=名稱預查核准之公司或有限合夥名稱

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。

3.1.5 命名爭議之解決程序

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 3.1.4 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。

3.1.6 商標之辨識、鑑別及角色

依 3.1.4 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 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。

3.1.8 組織身分鑑別之程序

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，應使用線上註冊申請作業，輸入用戶代碼即事業主體負責人之身分證字號及其民國年出生年月日。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，需先取得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

一次，如再次使用期限屆滿應依據本章節第一段之規定辦理。

3.1.9 個人身分鑑別之程序

於逕行發證使用線上註冊申請作業時，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。

3.1.10 硬體裝置或伺服軟體鑑別之程序

不適用。

3.1.11 寫入憑證內之電子郵件信箱驗證

因用戶申請符記不同分成以下 2 種驗證方式：

(1) 用戶申請符記為 IC 卡

用戶於取得憑證 IC 卡後，得於本管理中心網站(https://moeaca.nat.gov.tw)提出用戶電子郵件信箱寫入憑證申請。

用戶以憑證 IC 卡線上提出申請，本管理中心將檢驗憑證之

數位簽章以鑑別用戶之身分，並寄送電子郵件驗證信至寫入憑證之電子郵件信箱。

用戶須依照驗證信之內容回覆系統，以確認用戶確實擁有該電子郵件信箱之所有權及控制權。

(2) 用戶申請符記為非 IC 卡

用戶得依照需求於本管理中心網站(https://moeaca.nat.gov.tw)申請非 IC 卡類憑證或一站式專屬授權憑證時，一併申請電子郵件信箱寫入憑證。

本管理中心除檢查憑證申請之資料外，須寄送電子郵件驗證信函至寫入憑證內之電子郵件信箱。

用戶須依照驗證信之內容回覆系統，以確認用戶確實擁有該電子郵件信箱之所有權及控制權。

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。

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3.1節規定，

對於申請換發憑證之用戶進行識別及鑑別。

3.2.2 憑證展期

本管理中心所簽發IC卡及其他符記，其憑證有效期限與6.3.2.2節規定之用戶公開金鑰最長使用期限相同且不允許展期。

3.3 憑證廢止之金鑰更換

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3.1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

4.1 申請憑證之程序

4.1.1 憑證之申請程序

4.1.1.1 申請發證程序

用戶以紙本憑證申請書提交予憑證註冊窗口之憑證IC卡正卡或非IC卡類憑證申請程序：

(1) 憑證申辦人連線至本管理中心網站（https://moeaca.nat.gov.tw），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。

(2) 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。

(3) 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。

用戶以事業主體負責人自然人憑證申請憑證IC卡正卡或非IC卡類憑證程序：

(1) 憑證申辦人連線至本管理中心網站（https://moeaca.nat.gov.tw），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。

(2) 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。

4.1.1.2 逕行發證程序

本管理中心為因應政策而主動簽發之憑證，於用戶完成4.3.2節更改用戶代碼及設定PIN碼時，視為完成申請作業。

4.1.1.3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

用戶申請憑證IC卡附卡、一站式專屬授權憑證或依3.2.1節規定線上辦理之IC卡正卡申請換發程序如下：

(1) 憑證申辦人連線至本管理中心網站（https://moeaca.nat.gov.tw），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 卡需設定用戶代碼。

(2) 以事業主體憑證 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。

4.1.1.4設立專屬用戶憑證之申請程序

(1) 憑證申辦人連線至本管理中心網站（https://moeaca.nat.gov.tw），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。

(2) 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。

申請憑證時，憑證申辦人應提供正確資料。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。

用戶得依照第3.1.11節針對欲寫入憑證內之電子郵件信箱配合本管理中心進行驗證。

4.1.2 申請展期憑證之程序

本管理中心所簽發 IC 卡及其他符記，其憑證有效期限與 6.3.2.2 節規定之用戶公開金鑰最長使用期限相同並不允許展期。

4.2 簽發憑證之程序

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，進行以下審核程序，以作為判定是否同意簽發憑證之依據。憑證申請人可逕至本管理中心查詢憑證申請結果與簽發情形，而註冊窗口亦需以公文書方式通知用戶審核結果。

若用戶申請電子郵件信箱寫入憑證，則須依照第 3.1.11 節方式進行電子郵件信箱驗證。

4.2.1 IC 卡正卡憑證及非 IC 卡類憑證簽發程序

依 3.2.1 節規定線上辦理申請之 IC 卡正卡憑證簽發程序將依照 4.2.2 節規定辦理。

4.2.1.1申請發證審核程序

(1) 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。

(2) 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）。

(3) 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。

(4) 因用戶使用之符記不同分成以下兩種簽發程序：

A. 如用戶使用符記為 IC 卡：

經憑證註冊審驗人員檢查通過之憑證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 IC 卡內部產製金鑰對、以亂數設定 IC 卡之初始 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 卡郵寄至該事業主體之登記地給用戶。

B. 如用戶使用符記為非 IC 卡類：

經憑證註冊審驗人員檢查通過之憑證申請資料將由本管理中心簽發憑證，並將憑證以電子郵件方式傳送用戶。

若上述 IC 卡正卡依 3.2.1 節規定辦理重新申請，採用線上申請方式，使用正卡之數位簽章進行憑證申請，由註冊中心驗證正卡之數位簽章的方式進行，後續發卡作業比照上述符記為 IC 卡之簽發程序。

當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，後續則比照上述之簽發程序辦理。

4.2.1.2 逕行發證審核程序

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，發卡作業包括將由 IC 卡內部產製金鑰對、憑證寫入 IC 卡中、以亂數預設憑證 IC 卡 PIN 碼及印卡等工作。發卡中心並負責

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。如憑證 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 4.3.2 節更改用戶代碼及設定 PIN 碼。

4.2.2 IC 卡附卡及一站式專屬授權憑證簽發程序

採用線上申請方式，使用正卡裡的私密金鑰來做數位簽章進行憑證申請，由註冊中心驗證正卡之數位簽章的方式進行。IC 卡附卡後續簽發程序比照 4.2.1.1 節符記為 IC 卡之簽發步驟；一站式專屬授權憑證後續簽發程序則為由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。

4.2.3 展期憑證之簽發審核程序

本管理中心所簽發 IC 卡及其他符記，其憑證有效期限與 6.3.2.2 節規定之用戶公開金鑰最長使用期限相同並不允許展期。

4.2.4 設立專屬用戶憑證之申請程序

採用線上申請方式，使用「公司與商業及有限合夥一站式線上申請作業」之預查資料進行憑證申請，由註冊中心比對「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。簽發程序為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 接受憑證之程序

4.3.1 申請發證

(1) 用戶使用符記為 IC 卡時，申請發證之用戶完成 IC 卡接受作業，相關程序如下：

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（https://moeaca.nat.gov.tw），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。

(2) 用戶申請非 IC 卡類憑證時，接受憑證之程序如下：

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（https://moeaca.nat.gov.tw）進行憑證接受作業。

B. 用戶需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。

(3) 用戶申請一站式專屬授權憑證時，於 4.1.1.3 節之申請過程中，需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。

(4) 用戶申請「設立專屬用戶憑證」時，於 4.1.1.4 節申請過程中，需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。

(5)在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。

4.3.2 逕行發證

用戶使用 IC 卡時，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：

(1)用戶連線至本管理中心網站（https://moeaca.nat.gov.tw），閱讀用戶約定條款（Subscriber Agreement），用戶插入憑證 IC 卡，顯示憑證內容，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後，用戶應立即變更用戶代碼後，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。

(2)在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 憑證暫時停用及廢止

4.4.1 廢止憑證之事由

用戶在以下情況時(但不限)必須向註冊中心提出廢止憑證申請：

(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 4.9 節規定辦理。

4.4.2 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。

4.4.3 憑證廢止之程序

用戶以紙本申請書提出憑證廢止申請時，其程序如下：

(1) 憑證申辦人連線至本管理中心網站（https://moeaca.nat.gov.tw），下載並填寫憑證廢止申請書。

(2) 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。

(3) 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。

(4) 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。

(5) 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。

(6) 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。

用戶以憑證 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：

(1) 憑證申辦人連線至本管理中心網站（https://moeaca.nat.gov.tw），填寫憑證廢止申請書。

(2) 以憑證 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。

(3) 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。

(4) 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。

用戶提出「設立專屬用戶憑證」廢止時，其程序如下：

(1) 憑證申辦人連線至本管理中心網站（https://moeaca.nat.gov.tw），以預查編號及用戶代碼填寫憑證廢止申請書。

(2) 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。

(3) 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。

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：

(1) 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。

(2) 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。

(3) 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。

4.4.4 憑證廢止申請之處理期間

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。

4.4.5 暫時停用憑證之事由

用戶在以下兩種情形得申請憑證暫時停用：

(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暫時停用。

另外，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：

(1) 事業主體用戶遭停業時。

(2) 依用戶登記設立機關或是目的事業主管機關之通知。

(3) 依據司法機關、監察機關或治安機關之通知。

(4) 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。

(5) 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。

4.4.6 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。

4.4.7 暫時停用憑證之程序

用戶提出憑證暫時停用申請，其程序如下：

(1) 用戶使用符記為 IC 卡：

A. 用戶連線至本管理中心網站（https://moeaca.nat.gov.tw），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。

(2) 用戶使用符記為非 IC 卡類：

A. 用戶連線至本管理中心網站（https://moeaca.nat.gov.tw），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。

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：

(1) 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。

(2) 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。

(3) 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。

4.4.8 暫時停用憑證之處理期間及停用期間

憑證暫時停用申請，註冊中心應儘速處理並最多於 3 個工作天內完成憑證暫時停用審核。審核通過後，本管理中心將於 1 個工作天內完成憑證暫時停用作業。

用戶在申請暫時停用憑證時，不必申告所需停用的期間，本管

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。

若在憑證暫時停用期間，用戶取消憑證暫時停用，意即恢復使用憑證，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：

(1) 連線至本管理中心網站（https://moeaca.nat.gov.tw/），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。

(2) 註冊中心在檢驗 IC 卡之卡號（使用符記為 IC 卡時）或憑證序號（使用符記為非 IC 卡類時）及用戶代碼正確無誤後，加簽數位簽章上傳至本管理中心。

(3) 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。

逕行發證之用戶未能於該次逕行發證最後完成製卡之日（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。

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：

(1) 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。

(2) 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。

(3) 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，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。

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。

4.4.10 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

信賴憑證者在使用本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 線上憑證狀態協定查詢服務

本管理中心提供付費線上憑證狀態協定（OCSP）查詢服務，相關說明請參閱儲存庫。

4.4.13 線上憑證狀態協定查詢之規定

如信賴憑證者無法依照 4.4.11 節之規定查詢憑證廢止清冊，則必須依 4.4.12 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

不提供。

4.4.15 其他形式廢止公告之檢查規定

不適用。

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

本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

A. 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。

B. 任何嘗試刪除或修改稽核紀錄檔。

(2) 識別與鑑別

A. 嘗試新角色的設定不論成功或失敗。

B. 身分鑑別嘗試的最高容忍次數改變。

C. 使用者登入系統時身分鑑別嘗試的失敗次數之最大值。

D. 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。

E. 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

本管理中心產製金鑰時（不包括只用在單次或只限 1 次使用的金鑰產製）。

(4) 私密金鑰之載入和儲存

A. 載入私密金鑰到系統元件中。

B. 所有為進行金鑰回復的工作，對保存在本管理中心之私密

金鑰所做的存取。

(5) 可信賴公開金鑰的新增、刪除及儲存。

可信賴公開金鑰之改變，包括新增、刪除與儲存。

(6) 私密金鑰之輸出

私密金鑰之輸出 （不包括只使用在單次或只限 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) 本管理中心組態設定

本管理中心安全相關之組態設定改變。

(11) 帳號之管理

A. 加入或刪除角色和使用者。

B. 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

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。

(15) 本管理中心之伺服器設定改變

A. 硬體。

B. 軟體。

C. 作業系統。

D. 修補程式（Patches）。

E. 安全格式剖繪。

(16) 實體存取及場所之安全

A. 人員進入本管理中心之機房。

B. 存取本管理中心之伺服器。

C. 得知或懷疑違反實體安全規定。

(17) 異常

A. 軟體錯誤。

B. 軟體檢查完整性失敗。

C. 接收不合適訊息。

D. 非正常路由之訊息。

E. 網路攻擊（懷疑或是確定）。

F. 設備失效。

G. 電力不當。

H. 不斷電系統（UPS）失敗。

I. 明顯及重大網路服務或存取失敗。

J. 憑證政策之違反。

K. 本作業基準之違反。

L. 重設系統時鐘。

4.5.2 紀錄檔處理頻率

本管理中心每 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（on site）保留 2 個月，並依照 4.5.4 節、4.5.5 節、4.5.6 節及 4.6 節紀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) 使用簽章技術保存目前和已歸檔之稽核紀錄，並使用 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) 所有稽核紀錄均須存放於安全場所。

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) 本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) 本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

稽核系統內建於本管理中心的系統。稽核程序在本管理中心系統啟動時啟用，唯有在本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，本管理中心會暫停憑證簽發的服務，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，稽核系統並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

(1) 作業系統的弱點評估。

(2) 實體設施的弱點評估。

(3) 憑證管理系統的弱點評估。

(4) 網路的弱點評估。

4.6 紀錄歸檔之方法

4.6.1 紀錄事件之類型

(1) 本管理中心被主管機關認證（Accreditation）過程及結果的資料。

(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) 本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

本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。

歸檔資料逾保留期限後，得以安全方式銷毀，但電子型式資料檔如涉及未來法律舉證需求者得備份至其他媒體並提供適當保護。

4.6.3 歸檔之保護

(1) 不允許新增、修改或刪除歸檔資料。

(2) 本管理中心可將歸檔資料移到另 1 個儲存媒體，並提供適當的保護，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並非公正第 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。本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，必要時並將記載時間資訊。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

本管理中心沒有歸檔資料之彙整系統。

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

本管理中心之私密金鑰依照 6.3.2 節規定定期更換。本管理中心於私密金鑰執行簽發憑證用途之使用期限到期前 2 個月內，更換其用來簽發憑證的金鑰對，並取得政府憑證總管理中心核發之交互憑證。

用戶之私密金鑰必須依照 6.3.2 節規定定期更換。如用戶之憑證

未被廢止，最遲必須在憑證到期前 1 個月內更換其金鑰對，並依照 4.1 節的規定向本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

本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。

如本管理中心的電腦設備遭破壞或無法運作，但本管理中心的簽章金鑰並未被損毀，則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。

4.8.2 工商憑證管理中心簽章金鑰憑證被廢止之復原程序

本管理中心的簽章金鑰憑證被廢止時，本管理中心將重新產生金鑰對，重新向政府憑證總管理中心申請本管理中心本身之憑證，並重新簽發所有用戶憑證，並將所有新的憑證公布在儲存庫中，公告或通知用戶更換憑證。

4.8.3 工商憑證管理中心簽章金鑰遭破解之復原程序

本管理中心的私密金鑰有危害之疑慮時，本管理中心將重新產生金鑰對，重新向政府憑證總管理中心申請本管理中心本身之憑證，並重新簽發所有用戶憑證，並將所有新的憑證公布在儲存庫中，公告或通知用戶更換憑證。

4.8.4 工商憑證管理中心安全設施之災後復原工作

本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。

4.9 工商憑證管理中心之終止服務

本管理中心終止服務時，將依據電子簽章法相關規定辦理。

本管理中心遵守以下事項，以為確保終止服務對用戶與信賴憑證者所造成之影響最小：

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

(2) 本管理中心終止服務時必須：

A. 廢止所有未廢止或未過期之憑證，並依電子簽章法相關規定進行檔案紀錄之保管及移交。

B. 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。

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。

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

本管理中心機房位於中華電信股份有限公司數據通信分公司，符合儲存高重要性及敏感性資訊的機房設施水準，並具備門禁、保全、入侵偵測及監視錄影等實體安全機制，以防止未經授權存取本管理中心之相關設備。

5.1.2 實體存取

本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 層和第 2 層分別為全年無休的大門及大樓警衛，第 3 層為樓層讀卡機進出管制系統，第 4 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。

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，須檢查並確認沒有電腦病毒及任何可能危害本管理中心系統的惡意軟體。

非本管理中心人員進出機房，須填寫進出紀錄，並由本管理中心

相關人員全程陪同。

本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

本管理中心的電力系統，除市電外，另設有發電機（滿載油料可連續運轉 6 天）及不中斷電源系統（UPS），並具有市電及發電機的電源自動切換功能，可提供至少 6 小時以上備用電力，供儲存庫備援資料。

本管理中心機房設有恆溫恆濕空調系統，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

本管理中心機房設置在安全樓層，安全樓層須具備水災安全防護措施，且沒有因為水災造成重大損害紀錄。

5.1.5 火災防範及保護

本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，並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本管理中心機房儲存 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 節所述之本管理中心機敏性資訊，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

異地備援的地點在臺中，與本管理中心機房距離 30 公里以上。備援的內容包括資料與系統程式，全部資料(稽核紀錄檔之備份週期請參照 4.5.5 節)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。異地備援系統與本管理中心系統具有相同的安全等級。

5.2 程序控制

本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

本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。

本管理中心共有 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：

A. 安裝、設定和維護本管理中心系統。

B. 建立和維護本管理中心系統之使用者帳號。

C. 設定稽核參數。

D. 產製和備份本管理中心之金鑰。

(2) 簽發員負責：

A. 啟動/停止憑證簽發服務。

B. 啟動/停止憑證廢止服務。

(3) 稽核員負責：

A. 對稽核紀錄的查驗、維護和歸檔。

B. 執行或監督內部的稽核，以確認本管理中心運作是否遵照本作業基準的規定。

(4) 維運員負責：

A. 系統設備的日常運作維護。

B. 系統的備援及復原作業。

C. 儲存媒體的更新。

D. 除本管理中心憑證管理系統外之軟硬體更新。

E. 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，本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四種角色工作。

(3)任何 1 種信賴角色均不允許執行自我稽核功能。

5.2.3 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
產製和備份本管理	2		1		1

任務名稱	管理員	簽發員	稽核員	維運員	實體安全控管員
中心之金鑰					
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					2

任務名稱	管理員	簽發員	稽核員	維運員	實體安全控管員
全控管					

5.2.4 識別及鑑別每一個角色

本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，並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

A. 個人性格之評估。

B. 申請者經歷之評估。

C. 學術、專業能力及資格之評估。

D. 人員身分之確認。

E. 人員操守之評估。

(2) 人員之考核管理

本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，並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，特別是人員離職或約聘僱契約終止時，將遵守維護保密責任之約定。

(4) 維護保密責任之約定

本管理中心之相關人員均負維護保密之責任，並簽署保密切結書，不得以口頭、影印、借閱、交付、文章發表或其他方法洩漏機敏性資訊。

5.3.2 身家背景之查驗程序

本管理中心對於 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、本管理中心之安全認證機制。 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。

信賴角色	教育訓練需求
簽發員	1、本管理中心之安全認證機制。 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。 5、災後復原及業務永續經營之程序。
稽核員	1、本管理中心之安全認證機制。 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、本管理中心之安全認證機制。 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

在本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

本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本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

本管理中心任職之聘雇人員須具備足夠的知識技能與道德規範，遵守本作業基準相關規定，並依循本作業基準相關規定及簽定之相關保密協定進行作業。

5.3.8 提供之文件資料

本管理中心提供憑證政策、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本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

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。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。

本管理中心金鑰產製在公正第三方代表及本部工商憑證工作小組相關人員見證下進行。

6.1.1.1 用戶金鑰對之產製

用戶所使用之符記為 IC 卡，其金鑰對由本管理中心所信賴的發卡中心代為產製。發卡中心必須採用通過 FIPS 140-2 第 2 級安全認證或相當安全強度的 IC 卡，並在 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。

用戶使用其他符記時，則由用戶自行產製金鑰對。

6.1.2 私密金鑰安全傳送給用戶

用戶所使用之符記為 IC 卡，其私密金鑰依照 6.1.1.1 節規定由本

管理中心所信賴的發卡中心代為產製，發卡中心將於本管理中心簽發憑證後，將存有私密金鑰的 IC 卡郵寄給用戶。

6.1.3 公開金鑰安全傳送給工商憑證管理中心

用戶之金鑰對由本管理中心所信賴的發卡中心代為產製時，則由註冊中心透過安全管道將用戶之公開金鑰傳送至本管理中心。

用戶自行產製金鑰對時，則用戶必須以 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 3.1.7 節規定檢驗用戶確實擁有相對應的私密金鑰後，以安全的管道將用戶的公開金鑰傳送至本管理中心。

本節所指的安全管道為使用專屬通訊協定、資料簽章及加密傳送方式，諸如安全套接層通訊協定、憑證管理協定（Certificate Management Protocol, CMP）簽章封包、憑證註冊審驗人員簽章等。

6.1.4 工商憑證管理中心公開金鑰安全傳送給信賴憑證者

本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。信賴憑證者在使用本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本管理中心本身之公鑰憑證的簽章，以確保由公鑰憑證中之公開金鑰是可信賴

的。

6.1.5 金鑰長度

本管理中心使用2048位元的RSA金鑰，以及SHA-1、SHA256雜湊函數演算法簽發憑證及憑證廢止清冊。

用戶使用1024位元或2048位元的RSA金鑰。

6.1.6 公開金鑰參數之產製

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

本管理中心採用ANSI X9.31演算法產生RSA 演算法中所需的質數，該法可保證該質數為強質數（Strong Prime）。強質數為密碼學上具有某種數學特性之質數，利用強質數所組成之金鑰，其安全性高於一般質數。

用戶之金鑰則於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

本管理中心依照6.2.1節規定，使用通過FIPS 140-2第3級安全認證的硬體密碼模組產製亂數、公開金鑰對和對稱金鑰。

用戶使用通過FIPS 140-2第2級安全認證或相當安全強度的IC卡，並由IC卡內部產製金鑰對或其他軟硬體密碼模組產製金鑰對。

6.1.9 金鑰之使用目的

本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與cRLSign。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。

用戶之金鑰對分為簽章用及加解密用的兩對金鑰對，其中簽章用私密金鑰憑證，其憑證金鑰用途擴充欄位設定使用的金鑰用途位元為digitalSignature；加解密用私密金鑰憑證，其憑證金鑰用途擴充欄位設定使用的金鑰用途位元為keyEncipherment及dataEncipherment。

6.2 私密金鑰保護

6.2.1 密碼模組標準

依據憑證政策6.2.1節規定，本管理中心使用通過FIPS 140-2第3級安全認證的硬體密碼模組。

用戶使用通過FIPS 140-1或FIPS 140-2第2級安全認證或相當安全強度的IC卡或其他密碼模組。

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。此加密儲存之私密金鑰的啟用資料是採

LaGrange多項式內插法(LaGrange Polynomial Interpolation)的m-out-of-n(以下簡稱m-out-of-n)控管之IC卡組來控制及保護。m-out-of-n是一種完全秘密分享(Perfect Secret Sharing)的方式，可做為私密金鑰分持備份及回復方法。採用此方法可使本管理中心私密金鑰的啟用資料之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

本管理中心簽章用私密金鑰不可被託管（Escrow），本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

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

本管理中心簽章用私密金鑰不可被歸檔，本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

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。此加密儲存之私密金鑰的啟用資料是以6.2.2節之方式來控制及保護。本管理中心之私密金鑰出現在硬體密碼模組外時，必定是以加密型態存在。

6.2.7 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，可使用之認證鑑別方式包含（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。

6.2.8 私密金鑰之停用方式

本管理中心私密金鑰之停用是由 m-out-of-n 控管IC卡組來控制。

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。

6.2.9 私密金鑰之銷毀方式

為避免本管理中心過期的舊私密金鑰被盜用，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。

6.3 用戶金鑰對管理之其他規定

用戶必須自行管理金鑰對，本管理中心不負責保管用戶的私密金鑰。

6.3.1 公開金鑰之歸檔

本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 憑證機構公開金鑰及私密金鑰之使用期限

本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，但以私密金鑰執行簽發憑證用途之使用期限至多為10年。本管理中心所簽發之OCSP憑證，其金鑰長度亦為RSA 2048位元，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

當用戶之公開金鑰及私密金鑰之金鑰長度為1024位元時，公開金鑰憑證之使用期限至多為5年，私密金鑰之使用期限至多為5年。當金鑰長度為2048位元時，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

本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。

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。用戶啟用後可自行設定的PIN碼；在設定PIN碼時，需要輸入舊的PIN碼。

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。如啟動資料必須傳送，應透過適當的安全管道。

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 其他啟動資料之規定

沒有規定。

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安全。

(7) 具備信賴角色和相關身分識別之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

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

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 生命週期安全評等

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

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 密碼模組安全控管措施

依照 6.1 及 6.2 節規定辦理。

7.格式剖繪

7.1 憑證之格式剖繪

7.1.1 版本序號

本管理中心簽發 X.509 v3 版本的憑證。

7.1.2 憑證擴充欄位

本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

本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：

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）

本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

憑證中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 5280 的規定。

7.1.5 命名限制

本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

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

7.1.8 政策限定元的語法及語意

本管理中心簽發的憑證不含政策限定元（policyQualifiers）。

7.1.9 憑證政策擴充欄位之關鍵性語意註記

本管理中心簽發的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」之規定註記關鍵性（Critical）。

7.2 憑證廢止清冊之格式剖繪

7.2.1 版本序號

本管理中心簽發 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

本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，於本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，於本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本管理中心儲存庫。

8.1.2.3 意見回覆期限

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，以本管理中心儲存庫公告之回覆方式傳送給本管理中心，本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 個日曆天內公告於本管理中心儲存庫，本作業基準之修訂生效日期，除另有規定外，於公告後生效。

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核定後，由本管理中心公布。如憑證政策的修訂公告後，本作業基準將配合修訂，並送交電子簽章法主管機關核定。

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。