政府憑證管理中心

憑證實務作業基準

(Government Certification Authority
Certification Practice Statement)

第 1.9 版

主辦機關：國家發展委員會

執行機構：中華電信股份有限公司

中華民國 106 年 12 月 25 日

目　　錄

摘要 I

1 序論 1

1.1 概要 1

1.2 憑證實務作業基準之識別 2

1.3 主要成員及憑證適用範圍 2

1.3.1 政府憑證管理中心 3

1.3.2 註冊中心 3

1.3.3 發卡中心 4

1.3.4 儲存庫 4

1.3.5 終端個體 4

1.3.6 以委外方式提供認證服務 5

1.3.7 適用範圍 6

1.4 聯絡方式 7

1.4.1 憑證實務作業基準之制訂及管理機關 7

1.4.2 聯絡資料 7

1.4.3 憑證實務作業基準之審定 7

2 一般條款 8

2.1 職責及義務 8

2.1.1 政府憑證管理中心之職責 8

2.1.2 註冊中心之職責 8

2.1.3 發卡中心之職責 9

2.1.4 用戶之義務 9

2.1.5 信賴憑證者之義務 10

2.1.6 儲存庫服務之義務 11

2.2 法律責任 11

2.2.1 政府憑證管理中心之責任 11

2.2.2 註冊中心之責任 12

2.2.3 發卡中心之責任 13

2.3 財務責任 13

2.4 詮釋及施行 13
2.4.1 適用法律 13
2.4.2 可分割性、存續、合併、公告通知 14
2.4.3 紛爭之處理程序 14
2.5 費用 14
2.5.1 憑證簽發、展期費用 15
2.5.2 憑證查詢費用 15
2.5.3 憑證廢止、狀態查詢費用 15
2.5.4 其他服務之費用 15
2.5.5 請求退費之規定 15
2.6 公布及儲存庫 15
2.6.1 政府憑證管理中心之資訊公布 15
2.6.2 公布頻率 16
2.6.3 存取控制 16
2.6.4 儲存庫 16
2.7 稽核方法 16
2.7.1 稽核之頻率 16
2.7.2 稽核人員之身分及資格 17
2.7.3 稽核人員及被稽核方之關係 17
2.7.4 稽核之範圍 17
2.7.5 對於稽核結果之因應方式 17
2.7.6 稽核結果公開之範圍 18
2.8 資訊保密之範圍 18
2.8.1 敏感性資訊之種類 18
2.8.2 非敏感性資訊之種類 18
2.8.3 憑證廢止或暫時停用資訊之公開 19
2.8.4 應司法機關等要求釋出資訊 19
2.8.5 應用戶要求釋出資訊 19
2.8.6 其他資訊釋出之情況 19
2.8.7 隱私權保護 19
2.9 智慧財產權 20
3 識別和鑑別程序 21

3.1 初始註冊 21
3.1.1 命名種類 21
3.1.2 命名須有意義 21
3.1.3 命名形式之解釋規則 21
3.1.4 命名之獨特性 21
3.1.5 命名爭議之解決程序 23
3.1.6 商標之辨識，鑑別及角色 23
3.1.7 證明擁有私密金鑰之方式 23
3.1.8 組織身分鑑別之程序 24
3.1.9 個人身分鑑別之程序 25
3.1.10 硬體裝置或伺服軟體鑑別之程序 25
3.1.11 寫入憑證內之電子郵件驗證 25
3.1.12 網域名稱擁有者識別程序 26
3.2 憑證之金鑰更換及展期 27
3.2.1 憑證之金鑰更換 27
3.2.2 憑證展期 27
3.3 憑證廢止之金鑰更換 27
3.4 憑證廢止 28
3.5 憑證暫時停用與恢復使用 28
4.營運規範 29
4.1 申請憑證之程序 29
4.2 簽發憑證之程序 32
4.2.1 政府機關(構)、單位憑證之正卡及其他符記之憑證 32
4.2.2 政府機關(構)、單位憑證之附卡 34
4.2.3 政府機關伺服器應用軟體憑證 34
4.3 接受憑證之程序 35
4.4 憑證暫時停用及廢止 36
4.4.1 廢止憑證之事由 36
4.4.2 憑證廢止之申請者 38
4.4.3 憑證廢止之程序 38
4.4.4 憑證廢止申請之寬限期 39

4.4.5 暫時停用憑證之事由 39
4.4.6 暫時停用憑證之申請者 39
4.4.7 暫時停用憑證之程序 40
4.4.8 暫時停用憑證之處理期間及停用期間 41
4.4.9 恢復使用憑證之程序 41
4.4.10 憑證廢止清冊之簽發頻率 42
4.4.11 憑證廢止清冊之查驗規定 42
4.4.12 線上憑證狀態協定查詢服務 42
4.4.13 線上憑證狀態查詢之規定 43
4.4.14 其他形式廢止公告 43
4.4.15 其他形式廢止公告之檢查規定 43
4.4.16 金鑰被破解時之其他特殊規定 43
4.4.17 憑證問題報告機制 43
4.5 安全稽核程序 44
4.5.1 被記錄事件種類 44
4.5.2 紀錄檔處理頻率 49
4.5.3 稽核紀錄檔保留期限 49
4.5.4 稽核紀錄檔之保護 49
4.5.5 稽核紀錄檔備份程序 49
4.5.6 安全稽核系統 50
4.5.7 對引起事件者之告知 50
4.5.8 弱點評估 50
4.6 紀錄歸檔之方法 50
4.6.1 紀錄事件之類型 50
4.6.2 歸檔之保留期限 51
4.6.3 歸檔之保護 51
4.6.4 歸檔備份程序 52
4.6.5 時戳紀錄之要求 52
4.6.6 歸檔資料彙整系統 52
4.6.7 取得及驗證歸檔資料之程序 52
4.7 金鑰更換 53
4.8 金鑰遭破解或災變時之復原程序 53

4.8.1 緊急事件與系統遭破解之處理程序 53
4.8.2 電腦資源、軟體或資料遭破壞之復原程序 53
4.8.3 政府憑證管理中心之簽章金鑰憑證被廢止之復原程序 .. 53
4.8.4 政府憑證管理中心之簽章金鑰遭破解之復原程序 54
4.8.5 政府憑證管理中心安全設施之災後復原工作 54
4.9 政府憑證管理中心之終止服務 54
5.非技術性安全控管 55
5.1 實體控管 55
5.1.1 實體所在及結構 55
5.1.2 實體存取 55
5.1.3 電力及空調 56
5.1.4 水災防範及保護 56
5.1.5 火災防範及保護 56
5.1.6 媒體儲存 56
5.1.7 廢料處理 57
5.1.8 異地備援 57
5.2 程序控制 57
5.2.1 信賴角色 57
5.2.2 角色分派 59
5.2.3 每個任務所之人數 59
5.2.4 識別及鑑別每 1 個角色 60
5.3 人員控制 61
5.3.1 身家背景、資格、經驗及安全需求 61
5.3.2 身家背景之查驗程序 62
5.3.3 教育訓練需求 62
5.3.4 人員再教育訓練之需求及頻率 63
5.3.5 工作調換之頻率及順序 63
5.3.6 未授權行動之制裁 63
5.3.7 聘雇人員之規定 63
5.3.8 提供之文件資料 64
6.技術性安全控管 65

6.1 金鑰對之產製及安裝 65
6.1.1 金鑰對之產製 65
6.1.2 私密金鑰安全傳送給用戶 65
6.1.3 公開金鑰安全傳送給政府憑證管理中心 66
6.1.4 政府憑證管理中心公開金鑰安全傳送給信賴憑證者 66
6.1.5 金鑰長度 66
6.1.6 公鑰參數之產製 67
6.1.7 金鑰參數品質之檢驗 67
6.1.8 金鑰經軟體或硬體產製 67
6.1.9 金鑰之使用目的 67
6.2 私密金鑰保護 68
6.2.1 密碼模組標準 68
6.2.2 金鑰分持之多人控管 68
6.2.3 私密金鑰託管 68
6.2.4 私密金鑰備份 68
6.2.5 私密金鑰歸檔 69
6.2.6 私密金鑰輸入至密碼模組 69
6.2.7 私密金鑰之啟動方式 69
6.2.8 私密金鑰之停用方式 69
6.2.9 私密金鑰之銷毀方式 69
6.3 用戶金鑰對管理之其他規定 70
6.3.1 公開金鑰之歸檔 70
6.3.2 公開金鑰及私密金鑰之使用期限 70
6.4 啟動資料之保護 71
6.4.1 啟動資料之產生 71
6.4.2 啟動資料之保護 71
6.4.3 其他啟動資料之規定 71
6.5 電腦軟硬體安控措施 71
6.5.1 特定電腦安全技術需求 71
6.5.2 電腦安全評等 72
6.6 生命週期技術控管措施 72
6.6.1 系統研發控管措施 72

6.6.2 安全管理控管措施 72
6.6.3 生命週期安全評等 73
6.7 網路安全控管措施 73
6.8 密碼模組安全控管措施 73
7 格式剖繪 74
7.1 憑證之格式剖繪 74
7.1.1 版本序號 74
7.1.2 憑證擴充欄位 74
7.1.3 演算法物件識別碼 74
7.1.4 命名形式 75
7.1.5 命名限制 75
7.1.6 憑證政策物件識別碼 75
7.1.7 政策限制擴充欄位之使用 75
7.1.8 政策限定元之語法及語意 75
7.1.9 憑證政策擴充欄位之關鍵性語意註記 75
7.2 憑證廢止清冊之格式剖繪 76
7.2.1 版本序號 76
7.2.2 憑證廢止清冊擴充欄位 76
8.憑證實務作業基準之維護 77
8.1 變更程序 77
8.1.1 變更時不另作通知之變更項目 77
8.1.2 應通知之變更項目 77
8.2 公告及通知之規定 78
8.3 憑證實務作業基準之審定程序 79
附錄 1：BRS-SECTION 1.2.1 REVISIONS 80

摘要

依據電子簽章法及其子法「憑證實務作業基準應載明事項準則」規定，政府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 10600720140 號

2、簽發之憑證：

(1)種類：政府機關(構)、單位及其所屬的伺服器應用軟體等 3 種憑證(包括簽章用及加解密用的憑證)。

(2)保證等級：政府憑證管理中心(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 級的憑證。

(3)適用範圍：適用於電子化相關應用服務所需的身分認證及資料加密，並假設在網路中有惡意的使用者會去截取或篡改網路資訊，所傳送的資訊可能包含金錢上的交易。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，並排除本作業基準所限制及禁止的憑證適用範圍。

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相關法令規定所訂之責任範圍為限。

(3)如因不可抗拒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除法令另有規定外，由本管理中心負責。

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

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

4、其他重要事項：

(1) 如因本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，註冊中心之損害賠償責任以相關法令規定所訂之責任範圍為限。

(3) 用戶在接受本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，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做確認，由憑證註冊審驗人員審驗用戶之身分及憑證相關資訊，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，註冊中心相關法律責任應由用戶自行負責。

(8) 本管理中心由電子化政府主管機關依政府採購法，委託公正第三方辦理外部稽核作業，就本憑證管理中心的運作進行稽核。

1 序論

政府憑證管理中心憑證實務作業基準(Government 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，並遵循電子簽章法及其子法「憑證實務作業基準應載明事項準則」相關規定，說明政府憑證管理中心(Government Certification Authority, GCA，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，進行政府機關(構)、單位及其所屬的伺服器應用軟體等 3 種公鑰憑證(以下簡稱憑證)之簽發及管理作業。

1.1 概要

依據憑證政策的規定，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政府機關(構)、單位及其所屬的伺服器應用軟體等 3 種憑證(包括簽章用及加解密用的憑證)。

在本作業基準中，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本管理中心相關之個體，如本管理中心、註冊中心(Registration Authority)、用戶(Subscribers)、信賴憑證者(Relying Parties)及儲存庫(Repository)等。

本管理中心之 SSL 類憑證簽發管理，同意遵照憑證機構與瀏覽器論壇(CA/Browser Forum)所發行的 Baseline Requirements Certificate

Policy for the Issuance and Management of Publicly-Trusted Certificates 正式版本所揭示之原則，同時針對該正式版本所列之各項資訊的生效日期，本管理中心將配合辦理(參照附錄 1)，若本作業基準在 SSL 類憑證簽發管理上與該論壇規範有牴觸情形，將依照 CA/Browser Forum 所頒布之條款進行本作業基準之修訂，並經電子簽章法主管機關經濟部核定後實施。

國家發展委員會 (以下簡稱本會)為本管理中心的主管機關，負責本作業基準之訂定及修訂，本作業基準需經電子簽章法主管機關經濟部核可後施行。本作業基準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政府憑證管理中心憑證實務作業基準(Government Certification Authority Certification Practice Statement)，本版本為第 1.9 版，公布日期為 106 年 12 月 25 日。最新版本的本作業基準可在以下網頁取得：http://gca.nat.gov.tw/download/GCA_CPS_v1.9.pdf。

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}。(請參考憑證政策)。

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) 政府憑證管理中心。

(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 政府憑證管理中心

本管理中心是本基礎建設中的第 1 層下屬憑證機構，遵照憑證政策保證等級第 3 級的規定，負責政府機關(構)、單位及其所屬的伺服器應用軟體等 3 種憑證的簽發及管理作業。

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。註冊中心將由多個註冊窗口（RA Counter）組成，註冊窗口設於本會或本會授權的單位，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、暫停使用申請、恢復使用申請及廢止申請等業務。

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)主要採 IC 卡，本管理中心將委託可信賴的發卡中心進行 IC 卡發卡作業。IC 卡發卡作業包括 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 卡郵寄給用戶。

1.3.4 儲存庫

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：http://gca.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政府機關(構)、單位及其所屬的伺服器應用軟體等 3 種憑證而言，用戶就是政府機關(構)、單位。

政府機關(構)、單位憑證用戶使用之符記主要採 IC 卡，但也可使用其他硬體密碼模組，每個符記可同時儲存簽章用及加解密用兩種憑證。每個政府機關(構)或單位只可申請 1 張正卡，但可依應用需要申請多張附卡，每張正卡或附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正卡或附卡簽發簽章用及加解密用 2 種憑證。

伺服器應用軟體憑證没有正附卡之分別，可依應用需要申請多張憑證，憑證中的金鑰用途可為簽章用或加解密用，必要時可同時包含簽章用及加解密用兩種金鑰用途。

用戶必須依照 3.1 節初始註冊之識別與鑑別程序，申請政府機關(構)或單位憑證之正卡。如正卡遺失或憑證將到期時，必須依照 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，可再依照 3.1 節初始註冊之識別與鑑別程序申請附卡，或透過正卡之數位簽章線上申請附卡，並可依應用需要申請多張附卡。

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

中華電信股份有限公司(以下簡稱中華電信公司)接受本會委託，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政府機關(構)、單位及其所屬的伺服器應用軟體等憑證，且可包含簽章用及加解密用的憑證。

本管理中心所簽發的憑證符合憑證政策保證等級第 3 級之規定，適用於電子化政府相關應用所需的身分認證及資料加密，並假設在網路中有惡意的使用者會去截取或篡改網路資訊，所傳送的資訊可能包含金錢上的交易。

政府機關(構)、單位憑證之正卡可代表該機關進行各項應用，附卡只可使用在特定的應用。

伺服器應用軟體憑證可應用於安全插座層(Secure Socket Layer, SSL)通訊協定及開發專屬的伺服器應用軟體或是提供時戳服務之伺服器應用軟體。

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、正附卡別、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。

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。本作業基準之制訂及修訂在經電子簽章法主管機關經濟部核可後公布施行。

1.4.2 聯絡資料

如對本作業基準有任何建議或用戶報告遺失金鑰等事件，請與本管理中心聯繫，本管理中心之聯絡電話、郵遞地址與電子郵件信箱，請參閱 http://gca.nat.gov.tw/。

1.4.3 憑證實務作業基準之審定

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

2 一般條款

2.1 職責及義務

2.1.1 政府憑證管理中心之職責

(1)依據憑證政策保證等級第 3 級規定與本作業基準運作。

(2)執行憑證申請之識別及鑑別程序。

(3)簽發及公布憑證。

(4)廢止憑證。

(5)簽發及公布憑證廢止清冊。

(6)執行本管理中心與註冊中心相關人員之識別及鑑別程序。

(7)安全產製本管理中心之私密金鑰。

(8)保護本管理中心之私密金鑰。

(9)支援註冊中心進行憑證註冊相關作業。

2.1.2 註冊中心之職責

(1)提供憑證申請服務。

(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送給本管理中心。

(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及鑑別程序。

(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) 郵寄用戶之 IC 卡。

(5) 提供 IC 卡開卡作業。

(6) 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相關規定，並確認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後，用戶應依照 4.3 節規定接受憑證。

(3) 用戶在接受本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，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) 應妥善保管及使用私密金鑰。

(5) 如須暫停使用、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，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) 本管理中心所簽發之伺服器應用軟體憑證，以標的物為憑證主體，並以該標的物之所有人或經授權之使用人為用戶。如標的物之財產所有權或使用權發生移轉時，用戶應廢止原憑證並重新申請憑證。

(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，作為抗辯他人之事由。

2.1.5 信賴憑證者之義務

(1) 在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正附卡別及金鑰用途。

(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。

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 政府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。

本管理中心另遵循憑證機構與瀏覽器論壇(CA/Browser Forum)所發行的 Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates 正式版本所揭示之原則，簽發及管理伺服器應用軟體憑證憑證。

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 其他除外條款

如因不可抗拒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。

如因本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 節憑證廢止程序向本管理中心提出廢止憑證申請，在本管理中心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，並承擔所有因使用該憑證所引發之責任。

2.2.2 註冊中心之責任

2.2.2.1 保證範圍及其限制條件

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

本管理中心所簽發之憑證僅對憑證主體身分做確認，由憑證註冊審驗人員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，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 其他除外條款

如因不可抗拒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，發卡中心因執行發卡作業所致善意第三人因信賴而受損害者本管理中心應予負責。

2.3 財務責任

本管理中心的營運由本會編列預算維持，未向保險公司投保，但本會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。

2.4 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。

本管理中心之伺服器應用軟體憑證之簽發及管理，另遵照憑證機構與瀏覽器論壇(CA/Browser Forum)所發行的 Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates 正式版本，惟 Baseline Requirements 相關規定與本管理中心所依循之我國相關法律或法規產生衝突時，本管理中心得小幅度調整相關作法以滿足法律或法規之要求，並將變更調整之部分於簽發新憑證前通知 CA/Browser Forum；若發生以下情況時，則本管理中心將刪除並修訂原先 CPS 所調整之內容，並經電子簽章法主管機關經濟部核定，上述作業須於 90 天內完成。

(1) 與 Baseline Requirements 相關規定產生衝突之我國法律或法規已修訂或刪除。
(2) Baseline Requirements 修訂相關內容，使其規定可相容於我國法律或法規。

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，並得依紛爭處理程序(請參閱 http://gca.nat.gov.tw/)，請求本管理中心就本作業基準相關條文提出解釋。

2.5 費用

本管理中心得經行政機關電子憑證推行小組同意，並依法向用

戶及信賴憑證者分攤成本費用或收取費用，相關收費方式及費用公告於本管理中心網站。

2.5.1 憑證簽發、展期費用

參照「2.5 費用」一節辦理。

2.5.2 憑證查詢費用

參照「2.5 費用」一節辦理。

2.5.3 憑證廢止、狀態查詢費用

參照「2.5 費用」一節辦理。

2.5.4 其他服務之費用

參照「2.5 費用」一節辦理。

2.5.5 請求退費之規定

參照「2.5 費用」一節辦理。

2.6 公布及儲存庫

2.6.1 政府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(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) 本管理中心之最新訊息。

2.6.2 公布頻率

本管理中心每天簽發 1 次憑證廢止清冊，並公布於儲存庫。

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，並為保障儲存庫之安全應進行存取控制，且應維持其可接取狀態及可用性。

2.6.4 儲存庫

儲存庫由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：http://gca.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不定期的內

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

本會將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

配合本會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。

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。

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等規定時，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

本管理中心將於儲存庫公布最近 1 次的憑證機構外部稽核結果，但可能導致本管理中心系統被攻擊之資訊，不在此限。

2.8 資訊保密之範圍

2.8.1 敏感性資訊之種類

以下由本管理中心產生、接收或保管之資料，均視為敏感性資訊。

(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) 未經本會同意或符合法令規定不得公開或提供第三人使用之用戶資料(用戶資料包括機關(構)或單位及其連絡人之姓名、電子郵件信箱、通訊地址及電話等)。

(4) 本管理中心產生或保管之可供稽核及追蹤之紀錄。

(5) 稽核人員於稽核過程中產生之稽核紀錄及發現，不得被完整公開者。

(6) 列為敏感性等級的營運相關文件。

現職、外部稽核及曾任職於本管理中心之人員對於敏感性資訊均負保密責任。

2.8.2 非敏感性資訊之種類

(1) 本管理中心儲存庫公布之簽發憑證、已廢止憑證及憑證廢止清冊不視為敏感性資訊。

(2) 識別資訊或記載於憑證的資訊，除特別約定外，不視為敏感性資訊。

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公布於本管理中心儲存庫。在憑證廢止清冊(CRL)或線上憑證狀態協定(OCSP)回覆封包中的憑證廢止或暫時停用資訊，必須直到該被廢止或停用憑證已過期後才能加以移除。

2.8.4 應司法機關等要求釋出資訊

司法機關、監察機關或治安機關如因調查或蒐集證據需要，必須查詢 2.8.1 節敏感性資訊之種類，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 應用戶要求釋出資訊

用戶得以申請之憑證及私密金鑰，線上查詢 2.8.1 節第(3)款本身之憑證申請資料；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。

2.8.6 其他資訊釋出之情況

不提供商業應用，至於其他資訊之釋出依相關規定法令辦理。

2.8.7 隱私權保護

本管理中心依照國內個人資料保護制度相關法令，處理用戶之申請資料。

2.9 智慧財產權

本管理中心的金鑰對及金鑰分持為本管理中心之財產。政府機關(構)、單位憑證用戶使用之符記為 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，該金鑰對之財產權屬於該政府機關(構)、單位。伺服器應用軟體憑證之金鑰對由政府機關(構)、單位自行產製，該金鑰對之財產權屬於該政府機關(構)、單位。

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，其智慧財產權為本會及中華電信公司共同擁有。

本作業基準之智慧財產權為本會及中華電信公司共同擁有。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，並註明著作權為本會及中華電信公司所擁有。另外，重製或散布本作業基準者，不得向他人收取費用，亦不得拒絕任何人請求取得。本會及中華電信公司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

政府機關(構)、單位憑證之憑證主體名稱必須符合該機關(構)或單位據以設立之組織法、組織條例、組織規程或其他相關法令規定。

伺服器應用軟體憑證之唯一識別名稱包括憑證主體名稱(伺服器應用軟體之所有人或經授權之使用人)、通用名稱(Common Name，伺服器應用軟體名稱)及序號(Serial Number，本管理中心對伺服應用軟體所編訂的識別代號)。

3.1.3 命名形式之解釋規則

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

3.1.4 命名之獨特性

本管理中心第1代與第二代的憑證機構憑證其X.500唯一識別名稱為：

C=TW，O=行政院，OU=政府憑證管理中心

為便於與國際互通，本管理中心第3代起的憑證機構憑證其X.500唯一識別名稱使用以下格式：

C=TW，O=行政院，CN=政府憑證管理中心 - Gn

其中，n=3,4…

為使本管理中心所簽發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)政府機關(構)憑證

C=TW

L=縣市名稱(選擇性欄位，只適用於地方政府)

L=鄉鎮市區名稱(選擇性欄位，只適用於區域性機關或單位)

O=機關(構)的法定名稱

OU=附屬機關(構)的法定名稱(選擇性欄位，可以有多層)

(2)政府單位憑證

C=TW

L=縣市名稱(選擇性欄位，只適用於地方政府)

L=鄉鎮市區名稱(選擇性欄位，只適用於區域性機關或單位)

O=機關(構)的法定名稱

OU=附屬機關(構)或單位的法定名稱(選擇性欄位，可以有多層)

OU=附屬單位的法定名稱

(3)伺服器應用軟體憑證

C=TW

L=縣市名稱(選擇性欄位，只適用於地方政府)

L=鄉鎮市區名稱(選擇性欄位，只適用於區域性機關或單位)

O=機關(構)的法定名稱

OU=附屬機關(構)或單位的法定名稱(選擇性欄位，可以有多層)

CN=伺服器應用軟體的名稱(可能是伺服應用軟體之網域名稱、網路位址或其他文字名稱)

serialNumber=伺服器應用軟體的識別代號

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，將依照相關之組織法、組織條例、組織規程或其他相關法令規定處理。如發生網域名稱或網路位址所有權爭議時，用戶應依法定程序處理，並將處理結果提交本管理中心。

3.1.6 商標之辨識，鑑別及角色

不適用。

3.1.7 證明擁有私密金鑰之方式

(1)政府機關(構)、單位憑證

如用戶使用之符記為 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，然後使用金鑰對產生 PKCS#10 憑證申請檔並加以簽章，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。

(2)伺服器應用軟體憑證

由用戶自行產製金鑰對，然後使用金鑰對產生 PKCS#10 憑證申請檔並加以簽章，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

(1) 一般申請

用戶須將憑證申請書(包含政府機關(構)、單位之名稱及地址等)以正式公文書方式提出申請，本管理中心將確認該機關(構)、單位確實存在，並驗證公文書之真確性。

(2) 憑證IC卡正卡申請附卡

已取得正卡之用戶，可採線上申請附卡，註冊中心將檢驗正卡之數位簽章以鑑別用戶之身分。

(3) 憑證IC卡將屆期換發

憑證IC卡將屆期換發者，可由本節之(1)一般申請外， 亦可採用線上申請方式辦理。註冊中心將檢驗將屆期憑證IC卡之數位簽章以鑑別用戶之身分，並檢驗政府目錄服務系統確認該機關(構)、單位確實存在。

(4) 配合政策換發憑證

因政策性因素(如政府組織改造、行政區域重新劃分或用戶之上級機關命名規則的變更)，而需換發憑證者，經本管理中心同意得由用戶之上級機關以公文書方式代為申請。註冊中心應

檢驗該上級機關公文書之真確性。

3.1.9 個人身分鑑別之程序

政府機關單位申請伺服器應用軟體憑證時, 必須透過正式公文書申請，此正式公文書須經由該單位主管簽核，以此證明此伺服器應用軟體憑證之申請是獲得單位授權；此外亦可使用有效之機關單位憑證採用線上申請方式辦理，註冊中心將檢驗憑證 IC 卡之數位簽章以鑑別用戶之身分，並檢驗政府目錄服務系統確認該機關(構)、單位確實存在。

3.1.10 硬體裝置或伺服軟體鑑別之程序

由用戶以設備管理者的身分提出憑證申請，鑑別程序依照3.1.8節規定辦理。

3.1.11 寫入憑證內之電子郵件驗證

(1) IC卡類憑證

用戶於取得憑證IC卡後，得提出用戶電子郵件信箱寫入憑證。

用戶以憑證IC卡線上提出申請，憑證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，以確認用戶目前確實擁有使用及管理該電子郵件信箱之權利，並確認該電子郵件信箱可代表該機關。

(2) 其他符記

用戶得依照需求於申請其他符記之憑證時，一併申請電子郵件信箱寫入憑證。

憑證管理中心除檢查憑證申請書之資料外，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，以確認用戶目前確實擁有使用及管理該電子郵件信箱之權利，並確認該電子郵件信箱可代表該機關。

3.1.12 網域名稱擁有者識別程序

用戶申請伺服器應用軟體憑證(SSL Certificate)時(包含：單網域SSL憑證、多網域SSL憑證及萬用網域SSL憑證)，憑證管理中心須依照3.1.8節之「一般申請」程序，對該組織進行身分鑑別；另應擇一使用以下方式查詢該申請之主機網域名稱確實存在且屬該申請者所註冊擁有：

- 政府 WHOIS 主機-政府中英文網域名稱註冊系統 (https://rs.gsn.gov.tw)
- TWNIC Whois Database (http://whois.twnic.net.tw)
- ICANN WHOIS（https://whois.icann.org/en）(適用通用頂級網域)
- 透過與網域名稱註冊管理單位(Domain Name Registrar)接觸，驗證申請者具備該網域之控制權

若用戶以政府網際服務網(Government Service Network, GSN)之IP Address申請伺服器應用軟體憑證時，憑證管理中心須依照3.1.8節之「一般申請」程序，對該組織進行身分鑑別，並透過與GSN IP註冊管理單位接觸，驗證該IP Address確實存在且屬該申請者所註冊擁有。

- TWNIC Whois Database (http://whois.twnic.net.tw)
- 透過與 GSN IP 註冊管理單位接觸，驗證該 IP Address 確實存在且屬該申請者所註冊擁有。

3.2 憑證之金鑰更換及展期

3.2.1 憑證之金鑰更換

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

如用戶之私密金鑰使用期限屆滿必須更換金鑰時，應向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。

3.2.2 憑證展期

本管理中心不允許所簽發的憑證進行展期。

3.3 憑證廢止之金鑰更換

如用戶之私密金鑰因憑證廢止必須更換金鑰時，應向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

(1)政府機關(構)、單位憑證之正卡申請程序如下：

A. 政府機關(構)、單位指派適當人員，代表該機關(構)、單位申請憑證。

B. 憑證申請人連線至本管理中心網站(http://gca.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。

C. 將憑證申請書以公文書方式函送註冊窗口辦理。

D. 憑證 IC 卡將屆期，另可採線上申請屆期換發正卡。註冊中心則須查驗政府目錄服務系統資料確認機關(構)存在，方可簽發憑證。

(2)政府機關(構)、單位憑證之附卡申請方式有以下三種:

A. 採用如 4.1 節第(1)項正卡的申請程序。

B. 採用線上申請方式，使用政府機關(構)、單位憑證之正卡之數位簽章，進行身分鑑別，申請程序如下：

(A) 憑證申請人連線至本管理中心網站(http://gca.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。

(B)以政府機關(構)、單位憑證之正卡對附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。

C. 憑證 IC 卡將屆期，可採線上申請屆期換發附卡。註冊中心則須查驗政府目錄服務系統資料確認機關(構)存在，方可簽發憑證。

(3)伺服器應用軟體憑證申請程序如下：

A. 由伺服器應用軟體之所有人或經授權之使用人，代表申請憑證。

B. 由憑證申請人自行產製金鑰對，然後使用金鑰對產生 PKCS#10 憑證申請檔並加以簽章。

C. 憑證申請人連線至本管理中心網站(http://gca.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及設定用戶代碼，並將 PKCS#10 憑證申請檔上傳。

D. 將憑證申請書以公文書方式函送註冊窗口辦理或線上填寫申請書並以該機關單位憑證進行數位簽章後送出辦理。

(4) 由用戶之上級機關代為申請憑證之程序如下：

依照3.1.8節第(3)項規定，欲換發憑證者之申請方式為：

A. 憑證申請人連線至本管理中心網站

(http://gca.nat.gov.tw/)閱讀用戶約定條款，填寫憑證申請書，並設定用戶代碼。

B. 經本管理中心同意得由用戶之上級機關以公文書方式代為申請。

本管理中心僅接受政府機關(構)或單位提出之憑證申請，該憑證申請如透過正式公文，需經單位主管簽核過後遞交至憑證審驗單位進行憑證申請。

RAO 審驗人員收到公文後，應依照審驗作業規範進行公文文號及發文單位進行比對，僅有符合要求的憑證申請才會予以通過；如機關單位線上申請並以有效憑證對申請資料加數位簽章，本管理中心需驗證數位簽章以完成身分鑑別。

申請憑證時，憑證申請人應提供正確資料。為確保政府機關(構)及單位網站之可信賴性，申請 SSL 類伺服器應用軟體憑證之政府機關(構)及單位，必須確實擁有向政府網際服務網(Government Service Network)之政府中英文網域名稱註冊系統註冊登記之政府網域，始得向本管理中心申請 SSL 類伺服器應用軟體憑證。

此外，本管理中心僅提供政府機關(構)及單位之 SSL 類伺服器應用軟體憑證申請，其多數申請之網域均已透過 GSN 註冊，且申請之網域為政府機關(構)及單位能註冊使用之「.gov」。此外，有少數國營單位使用「.com」的網域，但此網域之申請需經嚴密的審核及管控，因此，本管理中心沒有高風險憑證申請問題。

政府機關(構)及單位如欲將電子郵件信箱寫入憑證內，應依照第 3.1.11 節要求辦理。

為確保電子化政府相關時戳服務的互通性及可信賴性，政府機關所設立的時戳服務機構（Time Stamp Authority，TSA）得向本管理中心申請時戳類伺服器應用軟體憑證。

依據 RFC 6844，本管理中心檢查網域名稱系統(Domain Name System, DNS)查閱 SSL 憑證申請案件所註記之完全吻合網域名稱(Fully Qualified Domain Names, FQDN)是否有憑證機構授權(Certificate Authority Authorization, CAA)簽發憑證之 DNS 資源紀錄(DNS Resource Record)。若憑證機構授權簽發憑證之 DNS 資源紀錄存在且將本管理中心列為授權 SSL 憑證簽發之憑證管理中心，本管理中心會視該憑證申請為同意授權本管理中心對該網域簽發 SSL 憑證。

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。

GCA 不簽發交互認證憑證(Cross Certificate)給其他 CA。

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，將依本作業基準第 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。

4.2.1 政府機關(構)、單位憑證之正卡及其他符記之憑證

政府機關(構)、單位憑證之正卡之簽發審核程序如下：

(1) 註冊窗口之憑證註冊審驗人員檢查憑證申請公文的真偽

及申請機關(構)、單位之資格(已遭裁撤或合併之機關(構)、單位不能申請)。

(2) 憑證註冊審驗人員檢查憑證申請書之資料，若用戶申請將電子郵件信箱寫入憑證內，應依照第 3.1.11 節要求辦理。如資料正確無誤，將使用憑證註冊審驗人員之 IC 卡對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) 採用線上屆期換發憑證正卡，系統須使用將屆期憑證正卡對憑證申請資料簽章，並查驗政府目錄服務資料，確認資料與該機關(構)、單位相符後，再上傳至註冊中心。

(4) 因用戶使用之符記不同分成以下兩種程序：

A.如用戶使用之符記為 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，發卡作業包括發卡中心於IC卡內部產製金鑰對、以亂數設定IC卡之初始PIN值、將申請資料及公開金鑰透過安全管道傳送給本管理中心、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 卡郵寄給用戶。

B.如用戶使用其他符記：

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給用戶。

4.2.2 政府機關(構)、單位憑證之附卡

政府機關(構)、單位憑證之附卡之簽發審核方式有以下三種：

(1) 如採用政府機關(構)、單位憑證之正卡申請程序者，則簽發審核程序比照以上程序。

(2) 如採用線上申請方式，使用政府機關(構)、單位憑證之正卡之數位簽章進行申請者，則由註冊中心以線上驗證正卡之數位簽章方式辦理。

(3) 如採線上屆期換發憑證附卡，簽發審驗程序比照 4.2.1 節之(3)辦理。

如以上之簽發審核不通過時，本管理中心將拒絕簽發憑證，憑證申請人可連線至儲存庫查詢憑證簽發情形。本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 政府機關伺服器應用軟體憑證

政府機關(構)伺服器應用軟體憑證之簽發審核程序如下：

(1) 憑證註冊審驗人員檢查憑證申請公文的真偽及申請機關(構)、單位之資格。

(2) 申請 SSL 類憑證者，憑證註冊審驗人員須依照 3.1.8 節及 3.1.12 節完成機關(構)身分鑑別及網域名稱擁有者鑑別程序。

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給用戶。

此外，本管理中心不執行預簽憑證(Precertificate)的簽發，即便未來本管理中心因應憑證透明度機制而執行預簽憑證的簽發時，該預簽憑證亦不得視為本管理中心所簽發的憑證。

4.3 接受憑證之程序

(1) 如用戶使用之符記為 IC 卡時，申請憑證之用戶完成 IC 卡開卡作業即表示接受憑證，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(http://gca.nat.gov.tw/)，進行開卡作業。

B. 在進行IC卡開卡時，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IC卡開卡，並表示已接受憑證，將獲得發卡中心以亂數設定的IC卡初始PIN碼；如用戶發現憑證內容不正確，則應停止開卡作業。

(2) 如用戶使用其他符記時，接受憑證之程序如下：

A. 申請憑證之用戶在收到憑證後，應連線至本管理中心網站(http://gca.nat.gov.tw/)。

B. 用戶應檢查憑證內容，如資料正確無誤，則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) 在用戶完成憑證接受作業後，所簽發的憑證將公布至儲存庫中。

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

4.4 憑證暫時停用及廢止

4.4.1 廢止憑證之事由

用戶在以下情形時(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) 憑證所記載之資訊重大改變，足以影響其信賴度。例如用戶之機關(構)或單位裁撤或合併，或唯一識別名稱需要做變更，這包含用戶的名稱已變更，或其上級機關已變更。

(3) 憑證不再需要使用，包括不再授權原憑證請求且不再追溯相關授權。

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) 確認用戶之機關(構)或單位裁撤或合併。

(5) 確認用戶之憑證未依本作業基準規定之程序簽發。

(6) 確認用戶違反本作業基準或相關法令規定。

(7) 依據司法機關、監察機關或治安機關之通知。

(8) 依用戶之上級機關或政府組織之主管機關之通知。

(9) 政府機關(構)、單位如因非自發性的名稱變更，而需做原先憑證的廢止時，本管理中心得視需要延後逕行廢止憑證，此憑證廢止的寬限期將公布在本管理中心儲存庫。

(10) 憑證內的完整網域名稱或者 IP 位址不再被授權給該用戶。

(11) 萬用字元憑證被用來識別一個錯誤誤導的下屬完整域名。

(12) 本憑證管理中心停止服務並且未安排另一個憑證管理中心來提供憑證廢止服務。

(13) 本憑證管理中心簽發憑證的權利已經逾期或被廢止、中止，除非本憑證管理中心有安排繼續維運 CRL/OCSP 儲存庫的服務。

(14) 依據憑證政策或憑證實務作業基準要求的廢止。

(15) 憑證的技術內容或格式對應用軟體提供者或依賴方可能

產生無法接受的風險（例如：該憑證使用已被破解或是經評估後確認為不適用之加密演算法、簽章演算法或金鑰長度)。

4.4.2 憑證廢止之申請者

(1) 欲廢止憑證之用戶。

(2) 用戶之上級機關或政府組織之主管機關。

4.4.3 憑證廢止之程序

(1) 由用戶或用戶之上級機關或政府組織之主管機關指派適當人員申請憑證廢止。

(2) 憑證廢止申請人連線至本管理中心網站(http://gca.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廢止申請書。

(3) 將憑證廢止申請書以公文書方式函送原申請憑證之註冊窗口辦理。

(4) 註冊窗口在收到憑證廢止申請公文後，由憑證註冊審驗人員檢查憑證廢止申請公文的真偽。

(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，將使用憑證註冊審驗人員之 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。

(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

本管理中心廢止憑證。

(7) 本管理中心因組織改造或安全事由等逕行廢止憑證作業時,將由憑證註冊審驗人員填寫廢止申請書後,統一廢止。

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 憑證廢止申請之寬限期

用戶如發生 4.4.1 節第 1 項之情形，最遲應於 10 個工作天內提出憑證廢止申請。

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之暫時停用：

(1) 憑證金鑰對之符記遺失或懷疑遭盜用時。

(2) 自行認定必須申請憑證之暫時停用。

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) 依用戶之上級機關或政府組織之主管機關之通知。

(2) 依據司法機關之通知。

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)欲暫時停用憑證之用戶。

(2)用戶之上級機關或政府組織之主管機關。

4.4.7 暫時停用憑證之程序

暫時停用憑證之程序依據用戶使用之符記不同說明如下：

(1)如用戶使用之符記為 IC 卡：

A. 用戶連線至本管理中心網站(http://gca.nat.gov.tw/)，填寫 IC 之卡號及用戶代碼線上辦理暫時停用憑證申請。

B. 註冊中心檢驗 IC 卡之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 IC 卡之憑證的有效性。

(2)如用戶使用其他符記：

A. 用戶連線至本管理中心網站(http://gca.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. 註冊中心檢驗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。

如以上之暫時停用申請審核不通過時，本管理中心將拒絕暫時

停用憑證。如用戶忘記用戶代碼，則發函向原申請憑證之註冊窗口辦理暫時停用憑證申請，在憑證註冊審驗人員檢查公文的真偽後，由憑證註冊審驗人員代為向本管理中心提出暫時停用憑證申請，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。

如果在憑證暫時停用期間，用戶取消憑證暫時停用，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

分為兩種程序：

(1)線上申請：由申請人連線至儲存庫申請恢復使用憑證，上傳至註冊中心。

(2)公文書申請：申請人填寫憑證恢復使用憑證申請書，將申請書以公文書方式函送註冊窗口辦理，憑證註冊審驗人員檢查申請書資料正確無誤後，使用憑證註冊審驗人員之IC卡對申請資料加簽數位簽章後，將相關資料上傳至註冊中心。

註冊中心檢驗申請資料正確無誤後，加簽數位簽章上傳至憑證

中心，憑證中心將立即恢復該憑證之使用。以上之恢復使用申請審核不通過時，憑證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至少 1 次，有效期限不超過 36 小時；倘若因應特殊情況，須簽發有效期限較長之憑證廢止清冊時，其有效期限不得超過 CA/Browser Forum Baseline Requirements 規定之上限。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

本管理中心提供符合 RFC 6960 及 RFC 5019 標準規範之線上憑證狀態協定(OCSP)服務，其中 OCSP 回應封包須透過簽發此待廢止憑證之 CA 進行簽章。本管理中心支援使用 GET 方法的 OCSP 服務。本管理中心至少每 4 天應更新透過 OCSP 提供的資訊。OCSP 回應封包最遲 10 天逾期。如果 OCSP 提供回應者收到對於一個還未簽發的憑證之狀態請求，則不可回覆其狀態為正常；並且本管理中心應監督 OCSP 提供回應者對於這類請求的回覆是否符合上述安全回應程序。更多相關說明請參閱儲存庫。

4.4.13 線上憑證狀態查詢之規定

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

4.4.14 其他形式廢止公告

不提供。此外，為了加速高流量網站的 SSL 憑證之驗證，以完成即時線上 SSL 憑證狀態之驗證作業，本管理中心支援線上憑證狀態協定裝訂(OCSP Stapling)，並提供相關設定說明，以供高流量網站之 SSL 憑證用戶參考使用。

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。

4.4.17 憑證問題報告機制

本管理中心應提供憑證問題回報與指引說明，供用戶、應用軟體廠商、信賴憑證者以及其他第三方組織於發現疑似私密金鑰遭破解、憑證被誤用、或是憑證被偽造、破解、濫用或不當使用等情形時，可向本管理中心提出憑證問題報告。

用戶、應用軟體廠商、信賴憑證者以及其他第三方組織可至本管理中心網站，取得有關回報憑證問題的指引說明，並可依該說明向本管理中心進行憑證問題的回報。

本管理中心在接收到憑證問題報告的 24 小時內，應至少依下述

準則來調查與確認該憑證廢止請求是否成立。若憑證廢止請求經確認後成立，由本管理中心逕行廢止憑證。

(1) 聲稱問題的內容。

(2) 該憑證或用戶的憑證問題報告數量。

(3) 提出憑證問題報告的單位。

(4) 相關的法律條文。

4.5 安全稽核程序

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

4.5.1 被記錄事件種類

(1) 安全稽核

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

(2) 識別與鑑別

- 嘗試新角色的設定不論成功或失敗。
- 身分鑑別嘗試的最高容忍次數改變。

- 使用者登入系統時身分鑑別嘗試的失敗次數之最大值。
- 如管理者將已被鎖住的帳號解鎖，而且該帳號是因為多次失敗的身分鑑別嘗試而被鎖住的。
- 管理者改變系統的身分鑑別機制，例如從通行密碼改為生物特徵值。

(3) 金鑰產製

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

(4) 私密金鑰之載入和儲存

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

(5) 可信賴公開金鑰之新增、刪除及儲存

- 可信賴公開金鑰之改變，包括新增、刪除及儲存。

(6) 私密金鑰之輸出

- 私密金鑰之輸出 (不包括只用在單次或只限1次使用之金鑰)。

(7) 憑證之註冊

- 憑證之註冊申請過程。

(8) 廢止憑證

- 憑證之廢止申請過程。

(9) 憑證狀態改變之核可

- 核可或拒絕憑證狀態改變之申請。

(10) 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

- 加入或刪除角色和使用者。
- 使用者帳號或角色之存取權限修改。

(12) 憑證格式剖繪之管理

- 憑證格式剖繪之改變。

(13) 憑證廢止清冊格式剖繪之管理

- 憑證廢止清冊格式剖繪之改變。

(14) 其他

- 安裝作業系統。
- 安裝本管理中心系統。
- 安裝硬體密碼模組。
- 移除硬體密碼模組。

- 銷毀硬體密碼模組。
- 啟動系統。
- 嘗試登入本管理中心的憑證管理作業。
- 硬體及軟體之接收。
- 嘗試設定通行密碼。
- 嘗試修改通行密碼。
- 本管理中心之內部資料備份。
- 本管理中心之內部資料回復。
- 檔案操作(例如產生、重新命名及移動等) 。
- 傳送任何資訊到儲存庫公布。
- 存取本管理中心之內部資料庫。
- 任何憑證被破解之申告。
- 憑證載入符記。
- 符記之傳遞。
- 符記之零值化。
- 本管理中心之金鑰更換。

(15) 本管理中心之伺服器設定改變

- 硬體。

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

(16) 實體存取及場所之安全

- 人員進出本管理中心之機房。
- 存取本管理中心之伺服器。
- 得知或懷疑違反實體安全規定。

(17) 異常

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

- 憑證政策之違反。
- 本作業基準之違反。
- 重設系統時鐘。

4.5.2 紀錄檔處理頻率

本管理中心每兩個月檢視 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

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

如稽核紀錄檔的保留期限屆滿，由稽核員負責移除資料，不可由其他人員代理。

4.5.4 稽核紀錄檔之保護

(1) 使用簽章、加密技術保存目前和已歸檔之稽核紀錄，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) 手動的稽核紀錄存放於安全場所。

4.5.5 稽核紀錄檔備份程序

電子式稽核記錄每月備份 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，本管理中心將暫停憑證簽發服務，直到問題解決再行提供服務。

4.5.7 對引起事件者之告知

如因發生事件而被稽核系統記錄，稽核系統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審查的(Accreditation)資料。

(2) 憑證實務作業基準。

(3) 重要的契約。

(4) 系統與設備組態設定。

(5) 系統或組態設定修改與更新的內容。

(6) 憑證申請資料。

(7) 廢止申請資料。

(8) 憑證接受的確認紀錄。

(9) 符記啟用的紀錄。

(10) 已簽發或公告的憑證。

(11) 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) 稽核記錄。

(14) 用來驗證及佐證歸檔內容的其它說明資料或應用程式。

(15) 稽核人員要求的文件。

(16) 依照 3.1.8 及 3.1.9 節所定的組織及個人身分鑑別資料。

4.6.2 歸檔之保留期限

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，書面資料應以安全方式銷毀；電子形式資料檔得另備份至其他儲存媒體並提供適當保護，或逕行以安全方式銷毀。

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一個儲存媒體，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三方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

本管理中心於私密金鑰執行簽發憑證用途之使用期限到期前，完成更換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 緊急事件與系統遭破解之處理程序

本管理中心依據緊急事件與系統遭破解的種類執行相關復原程序，並依照 5.1.8「異地備援」之規定執行必要的資料備份作業。

4.8.2 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。

4.8.3 政府憑證管理中心之簽章金鑰憑證被廢止之復原程序

本管理中心訂定簽章金鑰憑證被廢止之復原程序，同時每年進行演練。

4.8.4 政府憑證管理中心之簽章金鑰遭破解之復原程序

本管理中心訂定簽章金鑰遭破解之復原程序，同時每年進行演練。

4.8.5 政府憑證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後復原工作進行演練。

4.9 政府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，以確保終止服務對於用戶與信賴憑證者造成之影響最小：

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

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，指紋辨識器採用三度空間指紋取樣，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，需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，需填寫進出紀錄，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

本管理中心機房的電力系統，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基地墊高的建築物第3樓層(含)以上，該建築物並有防水閘門和抽水機，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敏感性資訊與文件資料，或磁帶、硬碟、磁碟、磁光碟(MO)及其他形式的記憶體不再使用時，須依照政府機關頒定之標準程序辦理銷毀。

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，明確規定哪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：

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

(2)簽發員負責：

- 啟動或停止憑證簽發服務。
- 啟動或停止憑證廢止服務。

(3)稽核員負責：

- 對稽核紀錄的查驗、維護和歸檔。
- 執行或監督內部的稽核，以確認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：

- 系統設備的日常運作維護。
- 系統的備援及復原作業。
- 儲存媒體的更新。
- 除本管理中心憑證管理系統外之軟硬體更新。

- 網路及網站的維護：建置系統安全與病毒防護機制及網路安全事件的偵測與通報等。

(5)實體安全控管員負責：

- 系統的實體安全控管(如機房的門禁管理、防火、防水及空調系統等)。

5.2.2 角色分派

依照 5.2.1 節定義的 5 種信賴角色，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 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。

5.2.3 每個任務所之人數

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

5.2.4 識別及鑑別每 1 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

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

(2)人員之考核管理

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敏感性資訊。

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。
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金鑰之操作程序。 4、稽核紀錄的查驗、維護和歸檔之程序。 5、災後復原及業務永續經營之程序。
維運員	1、本管理中心之安全認證機制。 2、系統設備日常運作之維護程序。 3、儲存媒體之更新程序。

	4、災後復原以及業務永續經營之程序。 5、網路和網站的維護程序。
實體安全控管員	1、設定實體門禁權限程序。 2、災後復原以及業務永續經營之程序。

5.3.4 人員再教育訓練之需求及頻率

在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僱人員除須簽定相關保密協定外，並須具備足夠的知識技能與道德規範，並遵守本憑證實務作業基準相關規定進行作業。

5.3.8 提供之文件資料

本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

本管理中心依照 6.2.1 節規定，於硬體密碼模組內產製金鑰對，採符合 FIPS140 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 章節規定進行。

本管理中心之金鑰對產製在行政機關電子憑證推行小組委員及相關人員見證下進行。

6.1.1.1 政府機關(構)、單位憑證之金鑰對產製

如政府機關(構)、單位憑證用戶使用之符記為 IC 卡時，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 等級 2 認證或安全強度相當的 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。

如政府機關(構)、單位憑證用戶使用其他符記時，則由政府機關(構)、單位自行產製金鑰對。

6.1.1.2 伺服器應用軟體憑證之金鑰對產製

用戶申請伺服器應用軟體憑證必須自行產製金鑰對。

6.1.2 私密金鑰安全傳送給用戶

如政府機關(構)、單位憑證用戶使用之符記為 IC 卡時，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政府憑證管理中心

如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。

如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安全插座層通訊協定(Secure Socket Layer)、專屬通訊協定或資料簽章及加密傳送的方式，諸如憑證管理協定(Certificate Management Protocol)簽章封包、憑證註冊審驗人員簽章等。

6.1.4 政府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-256、SHA-384、

SHA-512雜湊函數演算法簽發憑證，用戶使用2048位元的RSA金鑰。

6.1.6 公鑰參數之產製

採用 RSA 演算法之公鑰參數為空的(Null)。

6.1.7 金鑰參數品質之檢驗

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

用戶金鑰可於IC卡內部或其他軟硬體密碼模組產生RSA演算法中所需的質數，本管理中心會檢查用戶金鑰必須符合強質數，若用戶使用RSA金鑰時，RSA演算法所使用之公鑰指數(Public Exponent)其值須為大於3的奇數，且其值介於216+1和2256− 1之間。此外，模數(Modulus)具有奇數、非質數的任意次方且沒有小於752的因數等性質。

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等級2認證或安全強度相當的IC卡，並在IC卡內部產製金鑰對或使用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。

政府機關(構)、單位憑證包含簽章用及加解密用的兩對金鑰對。

伺服器應用軟體憑證之金鑰用途可為簽章用或加解密用，必要時可同時包含簽章用及加解密用兩種金鑰用途。

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FIPS140-2安全等級第3級認證的硬體密碼模組產製亂數及金鑰對，用戶金鑰對之儲存媒體可為IC卡或其他載具。

6.2.2 金鑰分持之多人控管

本管理中心金鑰分持之多人控管，採LaGrange多項式內插法(LaGrange Polynomial Interpolation) 的 m-out-of-n(以下簡稱 m-out-of-n)，它是一種完全隱密(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。採用此方法可使本管理中心私密金鑰的多人控管具有最高的安全度，因此也用來做為私密金鑰之啟動方式(參閱6.2.7節)。

6.2.3 私密金鑰託管

本管理中心簽章用私密金鑰不可被託管，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

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

6.2.5 私密金鑰歸檔

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之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。私密金鑰輸入完成後，須將輸入過程產製之相關敏感性參數完全銷毀。

6.2.7 私密金鑰之啟動方式

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

6.2.8 私密金鑰之停用方式

本管理中心之RSA私密金鑰之停用，是以m-out-of-n控管IC卡組進行控制。

6.2.9 私密金鑰之銷毀方式

為避免本管理中心舊的私密金鑰被盜用，影響簽發憑證之正確性，本管理中心將於舊私密金鑰不再簽發任何憑證與憑證廢止清冊後，把硬體密碼模組中存放舊的私密金鑰之記憶位址填零(Zeroization)，以銷毀硬體密碼模組中舊的私密金鑰。同時，舊的私密金鑰之分持也將進行實體銷毀。

6.3 用戶金鑰對管理之其他規定

用戶必須自行管理金鑰對，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 政府憑證管理中心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；以私密金鑰執行簽發用戶憑證用途之使用期限至多為10年，但簽發憑證廢止清冊、與線上憑證狀態協定(OCSP)查詢伺服器憑證則不在此限。

6.3.2.2 用戶公開金鑰及私密金鑰之使用期限

用戶之公開金鑰及私密金鑰之金鑰長度為RSA 2048位元，公開金鑰憑證之使用期限至多為9年，私密金鑰之使用期限至多為9年。

用戶申請之伺服器應用軟體憑證(SSL Certificate)之金鑰長度為RSA 2048位元，其公開金鑰憑證之使用期限遵循憑證機構與瀏覽器論壇(CA/Browser Forum)所發行的Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates正式版本之規定，107年3月1日後之伺服器應用軟體憑證效期不得超過825天，105年7月1日至107年2月28日間簽發之伺服器應用軟體憑證效期不得超過39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。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

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

6.4.3 其他啟動資料之規定

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

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，並公布於 GCA 網站之儲存庫。

系統開發環境、測試環境與上線運作環境必須有所區隔防止未經授權存取或變更的風險。

各項交付本管理中心之產品或程式應簽署安全遵循保證書確保無後門或惡意程式，並提供程式硬體交付清單、測試報告和系統管理手冊等、並進行程式版本控管。

6.6.2 安全管理控管措施

本管理中心不安裝與運作無關的硬體裝置、網路連接或元件軟體。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，並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。

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)，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

參照 6.1及6.2 節規定辦理。

7 格式剖繪

7.1 憑證之格式剖繪

本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

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：

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

(OID：1.2.840.113549.1.1.11)

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

(OID：1.2.840.113549.1.1.12)

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

(OID：1.2.840.113549.1.1.13)

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 相關規定。

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

本管理中心所簽發憑證之憑證政策擴充欄位使用本基礎建設之憑證政策物件識別碼。

本管理中心所簽發伺服器應用軟體憑證在憑證管理及憑證信賴保證上，除符合本基礎建設保證等級要求外，還符合 CA/Browser Forum Baseline Requirements 的規範。因此，本管理中心所簽發伺服器應用軟體憑證之憑證政策擴充欄位中除前述本基礎建設之憑證政策物件識別碼外，還必須包括 CA/Browser Forum Baseline Requirements 指定之憑證政策物件識別碼「 2.23.140.1.2.2」。

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 政策限定元之語法及語意

本管理中心簽發之憑證不含政策限定元(policyQualifiers)。

7.1.9 憑證政策擴充欄位之關鍵性語意註記

本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)的註記。

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。

此外，本憑證管理中心每年定期檢視憑證機構與瀏覽器論壇(CA/Browser Forum)所發行的 Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates 正式版本所頒布之條款，評估本作業基準是否需要修訂。倘若本作業基準與該論壇規範有牴觸情形，將依照 CA/Browser Forum 所頒布之條款進行本作業基準之修訂，並經電子簽章法主管機關經濟部核定後實施。

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 意見之回覆期限

對於變更項目有意見者，其回覆期限：

(1) 8.1.2.1 節之(1)影響程度大者，回覆期限為自公告日起 15 個日曆天內。

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

8.1.2.4 處理意見機制

對於變更項目有意見者，於意見回覆期限截止前，以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經濟部核定後，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經濟部核定。

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

附錄 1：BRs-Section 1.2.1 Revisions

Ver.	Ballot	Description	Adopted	Effective*	Implementation
1.0.0	62	Version 1.0 of the Baseline Requirements Adopted	22-Nov-11	01-Jul-12	—
1.0.1	71	Revised Auditor Qualifications	08-May-12	01-Jan-13	Compliant
1.0.2	75	Non-critical Name Constraints allowed as exception to RFC 5280	08-Jun-12	08-Jun-12	Compliant
1.0.3	78	Revised Domain/IP Address Validation, High Risk Requests, and Data Sources	22-Jun-12	22-Jun-12	Compliant
1.0.4	80	OCSP responses for non-issued certificates	02-Aug-12	01-Feb-13 01-Aug-13	Completed
--	83	Network and Certificate System Security Requirements adopted	03-Aug-13	01-Jan-13	Compliant
1.0.5	88	User-assigned country code of XX allowed	12-Sep-12	12-Sep-12	Compliant
1.1.0	--	Published as Version 1.1 with no changes from 1.0.5	14-Sep-12	14-Sep-12	—
1.1.1	93	Reasons for Revocation and Public Key Parameter checking	07-Nov-12	07-Nov-12	Compliant
1.1.2	96	Wildcard certificates and new gTLDs	20-Feb-13	20-Feb-13 01-Sep-13	Compliant
1.1.3	97	Prevention of Unknown Certificate Contents	21-Feb-13	21-Feb-13	Compliant
1.1.4	99	Add DSA Keys (BR v.1.1.4)	3-May-2013	3-May-2013	Compliant
1.1.5	102	Revision to subject domainComponent language in section 9.2.3	31-May-2013	31-May-2013	Compliant
1.1.6	105	Technical Constraints for Subordinate Certificate Authorities	29-July-2013	29-July-2013	Compliant
1.1.7	112	Replace Definition of “Internal Server Name” with “Internal Name”	3-April-2014	3-April-2014	Compliant
1.1.8	120	Affiliate Authority to Verify Domain	5-June-2014	5-June-2014	Compliant
1.1.9	129	Clarification of PSL mentioned in Section 11.1.3	4-Aug-2014	4-Aug-2014	Compliant
1.2.0	125	CAA Records	14-Oct-2014	15-Apr-2015	Compliant
1.2.1	118	SHA-1 Sunset	16-Oct-2014	16-Jan-2015 1-Jan-2016 1-Jan-2017	Compliant

1.2.2	134	Application of RFC 5280 to Pre-certificates	16-Oct-2014	16-Oct-2014	Compliant
1.2.3	135	ETSI Auditor Qualifications	16-Oct-2014	16-Oct-2014	—
1.2.4	144	Validation Rules for .onion Names	18-Feb-2015	18-Feb-2015	Compliant
1.2.5	148	Issuer Field Correction	2-April-2015	2-April-2015	Compliant
1.3.0	146	Convert Baseline Requirements to RFC 3647 Framework	16-Apr-2015	16-Apr-2015	—
1.3.1	151	Addition of Optional OIDs for Indicating Level of Validation	28-Sep-2015	28-Sep-2015	Compliant
1.3.2	156	Amend Sections 1 and 2 of Baseline Requirements	3-Dec-2015	3-Dec-2016	Compliant
1.3.3	160	Amend Section 4 of Baseline Requirements	4-Feb-2016	4-Feb-2016	Compliant
1.3.4	162	Sunset of Exceptions	15-Mar-2016	15-Mar-2016	Compliant
1.3.5	168	Baseline Requirements Corrections (Revised)	10-May-2016	10-May-2016	Compliant
1.3.6	171	Updating ETSI Standards in CABF documents	1-July-2016	1-July-2016	—
1.3.7	164	Certificate Serial Number Entropy	8-July-2016	30-Sep-2016	Compliant
1.3.8	169	Revised Validation Requirements	5-Aug-2016	1-Mar-2017	Compliant
1.3.9	174	Reform of Requirements Relating to Conflicts with Local Law	29-Aug-2016	27-Nov-2016	Compliant
1.4.0	173	Removal of requirement to cease use of public key due to incorrect info	28-July-2016	11-Sep-2016	Compliant
1.4.1	175	Addition of givenName and surname	7-Sept-2016	7-Sept-2016	Compliant
1.4.2	181	Removal of some validation methods listed in section 3.2.2.4	7-Jan-2017	7-Jan-2017	Compliant
1.4.3	187	Make CAA Checking Mandatory	8-Mar-2017	8-Sep-2017	Compliant
1.4.4	193	825-day Certificate Lifetimes	17-Mar-2017	1-Mar-2018	Compliant
1.4.5	189	Amend Section 6.1.7 of Baseline Requirements	14-Apr-2017	14-May-2017	Compliant
1.4.6	195	CAA Fixup	17-Apr-2017	18-May-2017	Compliant
1.4.7	196	Define “Audit Period”	17-Apr-2017	18-May-2017	—
1.4.8	199	Require commonName in Root and Intermediate Certificates 9	9-May-2017	8-June-2017	Compliant

* Effective Date and Additionally Relevant Compliance Date(s)