政府憑證總管理中心

憑證實務作業基準

(Government Root Certification Authority Certification Practice Statement)

第 1.5 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

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，政府憑證總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：政府憑證總管理中心(以下簡稱總管理中心)之自簽憑證、自發憑證、簽發給交互認證憑證機構之交互憑證。

(2) 保證等級：依據政府機關公開金鑰基礎建設憑證政策，簽發憑證政策所定義的 5 種保證等級的憑證。

(3) 適用範圍：

自簽憑證用以建立政府機關公開金鑰基礎建設信賴的起源；自發憑證為總管理中心更換金鑰或憑證政策需要時所簽發之憑證，用以建立新舊金鑰間或憑證政策互通憑證信賴路徑之用；交互憑證用以建立憑證機構間的互相信賴關係，以建構憑證機構互通所需的憑證信賴路徑之用。

3、法律責任重要事項：

(1) 交互認證憑證機構或信賴憑證者如未依照憑證實務作業基準規定之適用範圍使用憑證所引發之後果，總管

理中心不負任何法律責任。

(2) 與總管理中心交互認證之憑證機構，因簽發憑證或使用憑證而發生損害賠償事件時，總管理中心之損害賠償責任以憑證實務作業基準及相關契約所訂之責任範圍為限。

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

(4) 如因總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憑證機構，信賴憑證者或交互認證憑證機構不得以此作為要求總管理中心損害賠償之理由。

4、**其他重要事項**：

(1) 總管理中心直接受理憑證註冊與廢止申請等工作，因此不另設立註冊中心。

(2) 總管理中心簽發之憑證，依不同保證等級有不同之適用範圍，憑證機構於提出交互認證申請時，必須敘明所申請憑證之保證等級。

(3) 申請交互認證之憑證機構必須自行產製私密金鑰，並妥善保管及使用。

(4) 在憑證機構接受總管理中心所簽發之憑證後，即表示該憑證機構已確認憑證內容資訊之正確性。

(5) 交互認證憑證機構如有廢止憑證之必要時，應儘速通知總管理中心，並應遵守憑證實務作業基準規定程序辦理，但交互認證憑證機構於憑證廢止狀態未被公布之前，應先行採取適當的行動，以減少對交互認證憑證機構或信賴憑證者之影響，並承擔所有因使用該憑證證所引發之法律責任。

(6) 信賴憑證者在使用總管理中心簽發之憑證時，應先確認該憑證之正確性、有效性、保證等級及用途限制。

(7) 總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，就總憑證管理中心的運作進行稽核。

1 序論

政府憑證總管理中心憑證實務作業基準(Government Root 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，主要說明政府憑證總管理中心(Government Root Certification Authority, GRCA，以下簡稱總管理中心)如何遵照憑證政策保證等級第4級的規定，進行自簽憑證(Self-Signed Certificate)、自發憑證(Self-Issued Certificate)及交互憑證(Cross-Certificate)的簽發及管理作業。

1.1 概要

依據憑證政策的規定，總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)的最頂層憑證機構，也是本基礎建設的信賴起源，必須具備最高的公信度，信賴憑證者可直接信賴總管理中心本身的憑證。

本作業基準主要說明總管理中心的憑證作業實務，以確保總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 4 級之規定。本作業基準所載明之實務作業規範僅適用於與總管理中心

相關之個體，如總管理中心、交互認證憑證機構(Subject CA)、信賴憑證者(Relying Parties)及儲存庫(Repository)等。

總管理中心及有簽發伺服器應用軟體憑證之交互認證憑證機構，遵照憑證機構與瀏覽器論壇（CA/Browser Forum）所發行之 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，總管理中心將配合辦理(參照附錄 1)。

國家發展委員會(以下簡稱本會)為總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公布施行。本作業基準並未授權總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總管理中心憑證實務作業基準(Government Root Certification Authority Certification Practice Statement)，本版本為第 1.5 版，公布日期為 106 年 12 月 25 日。最新版本之本作業基準可在以下網頁取得：

http://grca.nat.gov.tw/download/GRCA_CPS_v1.5.pdf

本作業基準依據憑證政策訂定，總管理中心之運作遵照憑證政策保證等級第 4 級之規定，其物件識別碼名稱為

id-tw-gpki-certpolicy-class4Assurance ， 物 件 識 別 碼 值 為 {id-tw-gpki-certpolicy 4}。(請參考憑證政策)

1.3 主要成員及憑證適用範圍

本作業基準之主要成員包括：

(1) 政府憑證總管理中心。

(2) 儲存庫。

(3) 交互認證憑證機構。

(4) 信賴憑證者。

1.3.1 政府憑證總管理中心

總管理中心是本基礎建設的信賴起點(Trust Anchor)，將與本基礎建設領域內外憑證機構進行交互認證(Cross-Certification)，負責簽發、管理本基礎建設第 1 層之下屬憑證機構(Level 1 Subordinate CA)和本基礎建設外之憑證機構的交互憑證。

總管理中心直接受理憑證註冊與廢止申請等工作，負責蒐集及驗證交互認證憑證機構之身分及憑證相關資訊，不另設立註冊中心(Registration Authority, RA)。

1.3.2 儲存庫

儲存庫負責公告由總管理中心簽發之憑證、憑證機構廢止清冊(Certification Authority Revocation List, CARL)及其他憑證相關資訊，

並提供 24 小時全天的服務。總管理中心儲存庫之網址為：http://grca.nat.gov.tw/。

1.3.3 交互認證憑證機構

交互認證憑證機構係指與總管理中心進行交互認證之憑證機構，包括本基礎建設之第 1 層下屬憑證機構和本基礎建設外之憑證機構。欲向總管理中心申請交互認證之憑證機構，首先必須符合所引用的憑證政策保證等級之安全性規定，同時具備公開金鑰基礎建設及數位簽章及憑證簽發技術之建置及管理能力，並訂定憑證機構、註冊中心及信賴憑證者之相關責任及義務。

1.3.4 信賴憑證者

信賴憑證者係指相信憑證主體名稱(Certificate Subject Name)與公開金鑰之連結關係的個體。

信賴憑證者必須依據憑證機構的憑證及憑證狀態資訊，檢驗所使用憑證的有效性。在確認憑證的有效性後，才可使用憑證進行以下作業：

(1) 檢驗電子文件的數位簽章之完整性。

(2) 檢驗電子文件產生者的身分。

(3) 與憑證主體間建立安全之通訊管道。

1.3.5 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，負責總管理中心之建置及系統維運作業。

1.3.6 適用範圍

1.3.6.1 憑證之適用範圍

總管理中心簽發的憑證有三種，分別為自簽憑證、自發憑證以及交互憑證。

自簽憑證用以建立政府機關公開金鑰基礎建設信賴的起源；自發憑證為總管理中心更換金鑰或憑證政策需要時所簽發之憑證，用以建立新舊金鑰間或憑證政策互通憑證信賴路徑之用；交互憑證用以建立憑證機構間的互相信賴關係，以建構憑證機構互通所需的憑證信賴路徑之用。

自簽憑證之簽發對象為總管理中心本身，內含總管理中心的公開金鑰，可用來驗證總管理中心簽發之交互憑證與憑證機構廢止清冊的數位簽章。

交互憑證之簽發對象為與總管理中心進行交互認證之憑證機構，包括本基礎建設第 1 層之下屬憑證機構和本基礎建設外之憑證機構。交互憑證內含交互認證憑證機構的公開金鑰，可用來驗證該憑證機構簽發之憑證與憑證廢止清冊的數位簽章。

1.3.6.2 憑證之使用限制

信賴憑證者應依照 6.1.4 節所述之自簽憑證安全散布管道取得所信賴的總管理中心之公開金鑰或自簽憑證，始可用以驗證總管理中心簽發之自發憑證、交互憑證與憑證機構廢止清冊的數位簽章。信賴憑證者應慎選安全的電腦環境及可信賴的應用系統，以避免所使用的總管理中心之公開金鑰或自簽憑證遭到破壞或更換。信賴憑證者應確定所使用的總管理中心之公開金鑰或自簽憑證未遭到破壞或更換，始可用以驗證總管理中心簽發之自發憑證、交互憑證與憑證機構廢止清冊的數位簽章。

總管理中心簽發給憑證機構的交互憑證中，將記載該憑證機構可以簽發何種保證等級之憑證及可再與其他憑證機構進行交互認證之層數，以供信賴憑證者決定是否信賴該憑證機構及其所簽發的憑證。在簽發給本基礎建設外的憑證機構之交互憑證，會包括該憑證機構所採用的憑證政策與憑證政策間政策對應(Policy Mapping)的關係，信賴憑證者可依據該對應關係決定是否信賴該憑證機構及其所簽發的憑證。

信賴憑證者在使用總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。

1.3.6.3 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

總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，請與總管理中心聯繫，總管理中心之聯絡方式如下：

電話：(02)2192-7111

郵遞地址：台北市信義路一段 21 號

電子郵件信箱：egov@service.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 政府憑證總管理中心之職責

(1) 依據憑證政策保證等級第 4 級規定與本作業基準運作。

(2) 訂定憑證機構的交互認證申請程序。

(3) 執行憑證機構交互認證申請之識別與鑑別程序。

(4) 簽發及公布憑證。

(5) 廢止憑證。

(6) 簽發及公布憑證機構廢止清冊。

(7) 執行憑證機構人員之識別與鑑別程序。

(8) 安全產製總管理中心之私密金鑰。

(9) 保護總管理中心之私密金鑰。

(10) 執行總管理中心自簽憑證之金鑰更換及其自發憑證之簽發。

(11) 受理交互認證憑證機構之交互憑證註冊及廢止申請。

2.1.2 交互認證憑證機構之義務

(1) 遵守本作業基準及交互認證協議之規定，如未遵守導致信賴憑證者遭受損害時，應負損害賠償責任。

(2) 總管理中心簽發之憑證，依據憑證政策的規定，不同保

證等級有不同之適用範圍，憑證機構於提出交互認證申請時，必須敘明所申請憑證之保證等級。

(3) 憑證機構申請憑證應依照 4.1 節之程序進行交互認證申請，並確認申請資料之正確性。

(4) 在核可憑證機構之交互認證申請及總管理中心簽發憑證後，憑證機構應依照 4.3 節規定接受憑證。

(5) 憑證機構在接受總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 1.3.6 節規定使用憑證。

(6) 申請交互認證之憑證機構應依照第 6 章規定，自行產製私密金鑰。

(7) 交互認證憑證機構應妥善保管及使用私密金鑰。

(8) 使用與憑證之公開金鑰相對應之私密金鑰簽署之數位簽章即為憑證機構之數位簽章，憑證機構在產生數位簽章時，必須確認已接受該憑證，且該憑證仍在有效期間並未被廢止。

(9) 憑證機構如發生 4.4.1 節廢止憑證之事由(如私密金鑰資料外洩或遺失)，必須廢止憑證時，應立即通知總管理中心，並依照 4.4 節規定辦理憑證暫時停用或廢止，但憑證

機構仍應承擔憑證廢止狀態未被公布前所有使用該憑證之法律責任。

(10) 總管理中心如因故無法正常運作時，憑證機構應儘速尋求其他途徑完成與他人應為之法律行為，不得以總管理中心無法正常運作，作為抗辯他人之事由。

2.1.3 信賴憑證者之義務

(1) 信賴憑證者在使用總管理中心簽發之憑證或查詢總管理中心儲存庫時，必須遵守本作業基準之相關規定。

(2) 信賴憑證者應依照 6.1.4 節所述之自簽憑證安全散布管道取得所信賴的總管理中心之公開金鑰或自簽憑證。

(3) 信賴憑證者在使用總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。

(4) 信賴憑證者在使用總管理中心簽發之憑證時，應先檢驗憑證之用途限制，以確認該憑證之使用確實符合總管理中心設定之用途限制。

(5) 信賴憑證者在使用總管理中心簽發之憑證時，應先檢驗憑證機構廢止清冊，以確認該憑證是否有效。

(6) 信賴憑證者在總管理中心更換金鑰後使用其簽發之憑證時，應到總管理中心的儲存庫取得自發憑證，以建構總

管理中心與憑證機構間之憑證信賴路徑。

(7) 信賴憑證者在使用總管理中心簽發之憑證或憑證機構廢止清冊時，應先檢驗數位簽章，以確認該憑證或憑證機構廢止清冊是否正確。

(8) 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，信賴憑證者應自行承擔責任。

(9) 總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，不得以總管理中心無法正常運作，作為抗辯他人之事由。

(10) 信賴憑證者接受使用總管理中心簽發之憑證時，即表示已了解並同意有關總管理中心法律責任之條款，並依照 1.3.6 節規定範圍內信賴該憑證。

2.1.4 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、憑證機構廢止清冊及其他憑證相關資訊。

(2) 公布憑證政策及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 保證範圍及其限制條件

總管理中心依憑證政策保證等級第 4 級運作，並遵守本作業基準規定之程序簽發及廢止憑證、簽發並公布憑證機構廢止清冊及維持儲存庫正常運作。

總管理中心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簽發及管理憑證。

2.2.2 否認聲明及其限制條件

交互認證憑證機構或信賴憑證者如未依照 1.3.6 節規定之適用範圍使用憑證所引發之後果，總管理中心不負任何法律責任。

2.2.3 責任上限

與總管理中心交互認證之憑證機構，因簽發憑證或使用憑證而發生損害賠償事件時，總管理中心之損害賠償責任以本作業基準及相關契約所訂之責任範圍為限。

2.2.4 其他除外條款

如因不可抗拒及其他非可歸責於總管理中心之事由，所導致之損害事件，總管理中心不負任何法律責任。

如因總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交互認證憑證機構，信賴憑證者或交互認證憑證機構不得以此作為要求總管理中心損害賠償之理由。

如因 4.4.1 節廢止憑證之事由，交互認證憑證機構或其主管機關應向總管理中心提出憑證廢止申請，總管理中心在收到憑證廢止申請後，最遲於 10 個工作天內完成憑證廢止作業、簽發憑證機構廢止清冊及公告於儲存庫。交互認證憑證機構於憑證廢止狀態未被公布之前，應採取適當的行動(並於憑證實務作業基準中載明)，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。

2.3 財務責任

總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。

2.3.1 對交互認證憑證機構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

總管理中心因交互認證需要，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、合併及公告通知

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

總管理中心之憑證簽發及管理另遵照 CA/Browser Forum 所發行的 Baseline Requirements 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

交互認證憑證機構與總管理中心如有爭議時，應先進行協商以取得共識。如協商不成時，得依紛爭處理程序(請參閱 http://grca.nat.gov.tw/)，請求總管理中心就憑證政策或本作業基準相關條文提出解釋。如需訴訟時，以台灣台北地方法院為第一審管轄法院。

2.5 費用

總管理中心保留向申請交互憑證之憑證機構收取費用的權利，該項費用限應用於總管理中心的營運費用。

總管理中心如向申請交互憑證之憑證機構收取費用，將配合修正本作業基準，並訂定相關費用之查詢方法及請求退費之程序。

2.5.1 憑證簽發、展期費用

目前沒有收費。

2.5.2 憑證查詢費用

目前沒有收費。

2.5.3 憑證廢止、狀態查詢費用

目前沒有收費。

2.5.4 其他服務之費用

目前沒有收費。

2.5.5 請求退費之程序

目前沒有收費，因此無請求退費之程序。

2.6 公布及儲存庫

2.6.1 政府憑證總管理中心之資訊公布

總管理中心於儲存庫公布：

(1) 政府機關公開金鑰基礎建設憑證政策與技術規範。

(2) 本作業基準。

(3) 憑證機構廢止清冊。

(4) 總管理中心本身之自簽憑證(至與憑證之公開金鑰相對應之私密金鑰簽發的所有憑證效期到期為止)。

(5) 總管理中心新舊金鑰互簽之自發憑證(至總管理中心舊金鑰簽發之自簽憑證與其簽發之憑證之公開金鑰相對應之私密金鑰簽發的所有憑證效期到期為止)。

(6) 交互認證憑證機構之憑證。

(7) 隱私權保護政策。

(8) 工具程式下載。

(9) 最近 1 次之稽核結果。

(10) 總管理中心之最新消息。

2.6.2 公布頻率

總管理中心每天簽發 1 次憑證機構廢止清冊，並公布於儲存庫。

2.6.3 存取控制

總管理中心主機與儲存庫主機之間並無任何網路連線，因此總管理中心主機簽發的憑證及憑證機構廢止清冊無法直接透過網路傳送到儲存庫主機。在總管理中心需要公布簽發的憑證及憑證機構廢止清冊時，由總管理中心之相關人員以離線手動方式，將需公布的憑證及憑證機構廢止清冊儲存在可攜式媒體中，再將檔案複製到儲存庫主機中公布。

有關 2.6.1 節總管理中心公布的資訊，主要提供交互認證憑證機構及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

儲存庫由總管理中心負責管理，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://grca.nat.gov.tw/。

2.7 稽核方法

2.7.1 稽核之頻率

總管理中心接受每年 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(包括總管理中心及第 1 層下屬憑證機構)之外部稽核作業，委託熟悉本基礎建設相關規定及總管理中心、第 1 層下屬憑證機構運作及符合 Trust Service Principles and Criteria for Certification Authorities 標準之稽核業者，提供公正客觀的稽核服務，總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，將委託稽核業者就總管理中心的運作進行稽核。

2.7.4 稽核之範圍

(1) 總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。

2.7.5 對於稽核結果之因應方式

如稽核人員發現總管理中心之建置與維運不符合憑證政策、本

作業基準及交互認證協議的規定時，採取以下行動：

(1) 記錄不符合情形。

(2) 將不符合情形通知總管理中心。

(3) 對於不符合規定之項目，總管理中心將儘速改善，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，總管理中心將採取暫停營運、廢止簽發給交互認證憑證機構的憑證或其他配合行動。

2.7.6 稽核結果公開之範圍

總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，但可能導致總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

由總管理中心產生、接收或保管之資料，均視為敏感性資訊，現職及曾任職於總管理中心之人員及外部稽核者對於敏感性資訊均負保密責任。敏感性資訊包括：

(1) 用於總管理中心營運的私密金鑰及通行碼。

(2) 總管理中心金鑰分持的保管資料。

(3) 交互認證憑證機構之申請資料，未經交互認證憑證機構

同意或符合法令規定不得公開者。

(4) 總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。

2.8.2 非敏感性資訊之種類

(1) 總管理中心儲存庫公布之簽發憑證、已廢止憑證及憑證機構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

總管理中心不提供暫時停用服務，憑證廢止資訊公布於總管理中心儲存庫。

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 節敏感性資訊之種類，依法定程序辦理；惟總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、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；惟總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 應交互認證憑證機構要求釋出資訊

交互認證憑證機構得查詢 2.8.1 節第(3)款之申請資料；惟總管理中心保留向申請查詢之憑證機構收取合理費用之權利。

2.8.7 其他資訊釋出之情況

依相關規定法令辦理。

2.8.8 隱私權保護

總管理中心依照國內個人資料保護制度相關法令，處理憑證機構之交互認證申請資料。

2.9 權利歸屬

總管理中心的金鑰對及金鑰分持為總管理中心之財產。交互認證憑證機構的金鑰對為該憑證機構之財產，但其公開金鑰經總管理中心簽發成憑證時，該憑證為總管理中心之財產。

總管理中心所簽發的憑證及憑證機構廢止清冊，其所有權歸屬本會。

總管理中心所簽發的自簽憑證及自發憑證所記載之憑證主體名稱為總管理中心之智慧財產。

總管理中心將儘可能確保交互認證憑證機構名稱的正確性，但

不保證交互認證憑證機構名稱之智慧財產權歸屬。交互認證憑證機構名稱如發生註冊商標爭議時，交互認證憑證機構應依法定程序處理，並將處理結果提交總管理中心，以確保權益。

本作業基準之智慧財產權為本會擁有。本作業基準可由總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

總管理中心簽發憑證之憑證主體名稱為X.500唯一識別名稱(Distinguished Name, DN)。簽發給總管理中心的自簽憑證、自發憑證及憑證機構的交互憑證使用此唯一識別名稱的格式。

3.1.2 命名須有意義

申請交互認證憑證機構之名稱應符合相關法令對於命名之規定，並足以代表及識別該憑證機構。

3.1.3 命名形式之解釋規則

依據政府機關公開金鑰基礎建設技術規範之憑證格式剖繪，各式命名形式之解釋規則依 ITU-T X.520 名稱屬性定義。

3.1.4 命名之獨特性

總管理中心將審核申請成為下屬憑證機構與交互認證憑證機構所提出的憑證機構名稱之獨特性，如名稱重複時得要求該憑證機構修改名稱。

總管理中心第1代與第2代的自簽憑證使用以下名稱格式：

C=TW，O=Government Root Certification Authority

因總管理中心第1代及第2代自簽憑證主體同名造成其相互簽發之自發憑證被誤認為自簽憑證，而導致瀏覽器驗證憑證信賴路徑時產生錯誤，故總管理中心產製第1.5代金鑰，簽發自發憑證，重新建構第1代及第2代自簽憑證之信賴路徑，並使用以下名稱格式：

C=TW，

O=行政院，

CN=Government Root Certification Authority - G1.5

為便於與國際互通，總管理中心第3代起的自簽憑證使用以下名稱格式：

C=TW，

O=行政院，

CN=Government Root Certification Authority - Gn

其中，n=3,4…

此外，總管理中心之自簽憑證中，憑證簽發者與憑證主體名稱相同。

3.1.5 命名爭議之解決程序

對於名稱所有權爭議由本會處理。

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

憑證機構申請交互認證時，總管理中心檢驗憑證機構之私密金

鑰與將記載於憑證中之公開金鑰是否成對。由該憑證機構產生 1 個 PKCS#10 憑證申請檔，總管理中心使用該憑證機構的公開金鑰檢驗簽章，以證明該憑證機構擁有相對應之私密金鑰。

3.1.8 組織身分鑑別之程序

憑證機構提交之交互認證申請書中應包含機關名稱、所在地及代表人等足以識別該機關之資料。申請資料應併同公文書，以電子公文或紙本公文送至本會。本會於確認公文書合法性與適切性後，轉交政府憑證總管理中心簽發交互憑證。

如憑證機構經營者非我國政府機關，應提交公文書及交互認證申請書，由本會確認該憑證機構存在，並驗證公文書、代表人身分及代表人是否有權代表該組織申請憑證。憑證申請時應由代表人親自辦理。

3.1.9 個人身分鑑別之程序

政府機關無須進行個人身分鑑別之程序，但非政府機關申請交互認證者必須以公文書指派代表人(被授權辦理交互認證申請的個人)申請憑證機構之憑證，鑑別程序如下：

(1)核對書面證件：

在申請憑證時，代表人應出示中華民國國民身分證正本或護照，供總管理中心鑑別代表人之身分。代表人的身分證字號、姓

名及戶籍地址等資料，需與機關提交的申請資料進行比對。

(2)提交代表人之授權證明書。

(3)代表人必須親自證明其身分。

3.1.10 硬體裝置或伺服軟體鑑別之程序

不適用。

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。

總管理中心本身的私密金鑰長度為4096位元，用來簽發憑證用途之效期至多為10年；公開金鑰憑證效期為30年。總管理中心在以下兩種情形會更換金鑰並簽發新的自簽憑證：

(1)目前使用之金鑰生命週期結束。

(2)目前使用之金鑰的安全性有問題時(例如懷疑或確定金鑰被破解)。

交互認證憑證機構更換金鑰時，應向總管理中心重新申請憑證，總管理中心依照3.1節規定，對於重新申請交互認證之憑證機構進行識別及鑑別。

3.2.2 憑證展期

總管理中心不允許本身的自簽憑證、自發憑證及下屬憑證機構的交互憑證進行展期。

3.3 憑證廢止之金鑰更換

憑證機構之憑證廢止後，新憑證申請之識別與鑑別程序依照3.1節規定，重新辦理初始註冊。

3.4 憑證廢止

交互認證憑證廢止申請之鑑別程序與3.1.8、3.1.9節規定相同。

3.5 憑證暫時停用與恢復使用

不適用。

4.營運規範

4.1 申請憑證之程序

1.起始(Initiation)

(1)起始申請

以公文書函送交互認證申請書、憑證實務作業基準及 PKCS#10 憑證申請檔等資料，如憑證機構遵循的憑證政策非政府機關公開金鑰基礎建設憑證政策時，應另檢附所遵循的憑證政策。

(2)身分識別與鑑別

依照 3.1.8 節規定，執行申請交互認證之憑證機構的身分識別與鑑別程序。

(3)執行以下檢查程序

- 確認申請交互認證之憑證機構與總管理中心間沒有技術上不相容之問題。
- 如申請交互認證之憑證機構遵循的憑證政策非政府機關公開金鑰基礎建設憑證政策時，應檢查其憑證政策與總管理中心在憑證政策的對應關係。
- 檢查憑證機構之憑證實務作業基準是否遵循所引用的憑證政策。

■ 檢驗起始申請交付的 PKCS#10 憑證申請檔，以確認是否可以完成實際的交互認證作業。

2.審查申請(Examination)

政府機關之憑證機構直接由總管理中心主管機關決議是否核可申請案，如同意申請案者，由本會通知總管理中心進入簽發憑證程序。

如非政府之憑證機構申請交互認證時應召開行政機關電子憑證推行小組委員會議，審查申請之憑證機構提交之相關文件資料及總管理中心之檢查結果，以決定憑證機構與總管理中心交互認證之妥適性。最後依該小組之決議，決定進入下一階段，或要求補送資料，或駁回申請。

3.協議(Arrangement)

召開會議時，應進行以下步驟：

(1) 身分識別與鑑別

會議開始前，依照 3.1.9 節規定，執行申請交互認證之憑證機構代表人的身分識別與鑑別程序。

(2) 與申請交互認證之憑證機構協商必須遵守之條款與條件。

(3) 核定是否與申請交互認證之憑證機構進行交互認證，如

同意則與申請交互認證之憑證機構簽署交互認證協議書(Cross-Certification Agreement, CCA)，但如同為政府機關者，交互認證得免簽署交互認證協議書。

(4) 進入簽發憑證程序。

4.2 簽發憑證之程序

總管理中心依照核定結果決定是否簽發憑證。

如核可憑證申請，總管理中心將執行憑證簽發之相關工作，憑證簽發後，以公文書通知申請之憑證機構，並檢附簽發的憑證。

如未核可憑證申請，將以公文書通知申請交互認證之憑證機構，並說明未核可的理由。

總管理中心將簽發1張自簽憑證(Self-Signed Certificate)，此憑證依照6.1.4節規定傳送給信賴憑證者。

4.3 接受憑證之程序

申請交互認證之憑證機構在收到核可憑證申請公文後，必須檢查公文所附的憑證，確認該憑證內容之正確性，如憑證內容無誤，憑證機構必須簽署憑證接受確認文件，並以公文書方式函復，以完成憑證接受程序。

總管理中心在收到憑證接受確認文件後，將簽發給憑證機構之交互憑證公布於儲存庫。

如憑證機構於 30 個日曆天內未能函復憑證接受確認文件，則視為拒絕接受憑證，總管理中心將廢止該憑證，並不另行公布。

4.4 憑證暫時停用及廢止

4.4.1 廢止憑證之事由

交互認證憑證機構在以下情形時(但不限)必須提出廢止憑證申請：

(1) 懷疑或證實私密金鑰遭到破解。

(2) 憑證不再需要使用，包括憑證機構終止服務或停止與總管理中心的交互認證關係。

另外，總管理中心得就以下情形逕行廢止憑證，毋須事先經過交互認證憑證機構同意：

(1) 確認憑證記載之內容不實。

(2) 確認交互認證憑證機構之簽章用私密金鑰遭冒用、偽造或破解。

(3) 確認總管理中心之私密金鑰或系統遭冒用、偽造或破解，則廢止總管理中心簽發的所有交互認證憑證機構之憑證。

(4) 確認交互認證憑證機構的憑證未依本作業基準之程序簽發。

(5) 確認交互認證憑證機構違反其憑證實務作業基準或交互認證協議書或相關法令規定。

(6) 依據交互認證憑證機構主管機關之通知或相關法令規定。

(7) 總管理中心或交互認證憑證機構終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。

(8) 總管理中心或交互認證憑證機構簽發憑證的權利已經逾期或被廢止、中止，除非總憑證管理中心有安排繼續維運 CRL/OCSP 儲存庫的服務。

(9) 依據總管理中心憑證政策或憑證實務作業基準要求的廢止。

(10) 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）。

如憑證之憑證主體資訊必須變更時，由總管理中心審查是否同意廢止憑證申請。

4.4.2 憑證廢止之申請者

(1)欲廢止憑證的交互認證憑證機構。

(2)交互認證憑證機構的主管機關或負責單位。

4.4.3 憑證廢止之程序

1.起始(Initiation)

(1)起始申請

以公文書提出申請，並檢具憑證廢止申請書。

(2)身分識別與鑑別

依照 3.1.8 節規定，執行交互認證憑證機構的身分識別與鑑別程序。

(3)審查申請

審查提交之相關文件資料，以決定憑證廢止申請之妥適性。

(4)決定點

決定進入下一階段，或要求補送資料，或以公文書通知該交互認證憑證機構未核可憑證廢止申請，並明確說明未核可之理由。

2.廢止憑證

總管理中心最遲於下次公布憑證機構廢止清冊前，將廢止憑證加入憑證機構廢止清冊中，並公告於儲存庫。憑證廢止後將以公文書通知交互認證憑證機構及其主管機關或負責單

位，儲存庫公告的憑證狀態資訊將包括廢止的憑證，直到憑證到期為止。

4.4.4 憑證廢止申請之寬限期

交互認證憑證機構如發生 4.4.1 節之情形，最遲應於 10 個工作天內提出憑證廢止申請，並且儘可能於總管理中心下一次簽發憑證機構廢止清冊前提出。

總管理中心在收到憑證廢止申請後，最遲於 10 個工作天內完成憑證廢止相關作業。

4.4.5 暫時停用憑證之事由

不提供暫時停用憑證服務。

4.4.6 暫時停用憑證之申請者

不適用。

4.4.7 暫時停用憑證之程序

不適用。

4.4.8 暫時停用憑證之寬限期

不適用。

4.4.9 恢復使用憑證之程序

不適用。

4.4.10 憑證機構廢止清冊之簽發頻率

憑證機構廢止清冊之簽發頻率為每天 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。更新後之憑證機構廢止清冊公布於儲存庫。

4.4.11 憑證機構廢止清冊之查驗規定

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

4.4.12 線上憑證狀態查詢服務

不提供線上憑證狀態查詢服務。

4.4.13 線上憑證狀態查詢之規定

不適用。

4.4.14 其他形式廢止公告

不提供其他形式廢止公告。

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需求

如交互認證憑證機構之私密金鑰被破解時，總管理中心將於公布之憑證機構廢止清冊中註明該憑證廢止的原因為金鑰被破解。

4.4.17 憑證問題回報機制

總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，可向總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總管理中心網站，取得有關回報憑證問題的指引說明，並可依該說明向總管理中心進行憑證問題的回報。

總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，由總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

總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、新舊參數的內容等。
- 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

■ 總管理中心產製金鑰時。

(4) 私密金鑰之載入和儲存

■ 載入私密金鑰到系統元件中。

(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) 總管理中心組態設定

■ 總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) 憑證機構廢止清冊格式剖繪之管理

■ 憑證機構廢止清冊格式剖繪之改變。

(14) 其他

■ 安裝作業系統。

■ 安裝總管理中心系統。

■ 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。

■ 嘗試登入總管理中心的憑證管理作業。

■ 硬體及軟體之接收。

■ 嘗試設定通行碼。

■ 嘗試修改通行碼。

■ 總管理中心之內部資料備份。

■ 總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。
- 存取總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。
- 總管理中心或交互認證憑證機構之金鑰更換。

(15) 總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

- 人員進出總管理中心之機房。
- 存取總管理中心之伺服器。
- 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

總管理中心每月檢視 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

稽核紀錄檔保留兩個月，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

電子式稽核紀錄每月備份 1 次。

(1) 總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) 總管理中心將事件紀錄檔存放於安全場所。

4.5.6 安全稽核系統

稽核系統內建於總管理中心的系統。稽核程序在總管理中心系統啟動時啟用，唯有在總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，總管理中心將暫停憑證簽發服務，直到問題解決後再行提供服務。

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) 憑證機構被主管機關認證過程及結果的(Accreditation)資料(假設適用)。

(2) 憑證實務作業基準。

(3) 交互認證協議書。

(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) 憑證接受的確認文件。

(9) 已簽發或公告的憑證。

(10) 總管理中心金鑰更換的紀錄。

(11) 已簽發或公告的憑證機構廢止清冊。

(12) 稽核記錄。

(13) 用來驗證及佐證歸檔內容的其它說明資料或應用程式。

(14) 稽核人員要求的文件。

(15) 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

總管理中心歸檔資料之保留期限為 20 年，用來處理歸檔資料的應用程式也將維護 20 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) 總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，異地備援的地點，目前設在臺中(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、憑證機構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。總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

總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

總管理中心最遲於私密金鑰使用期限到期前 3 個月，更換用來簽發憑證的金鑰對，並簽發1張新的自簽憑證及2張自發憑證。新簽發的自簽憑證依照 6.1.4 節規定傳送給信賴憑證者，自發憑證公布在儲存庫供信賴憑證者下載。

交互認證憑證機構最遲於憑證機構本身之憑證到期前 2 個月，更換用來簽發憑證的金鑰對。交互認證憑證機構更換金鑰對後，依照 4.1 節規定向總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

總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

總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。

如總管理中心的電腦設備遭破壞或無法運作，但總管理中心的簽章金鑰並未被損毀，則優先回復總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 政府憑證總管理中心之簽章金鑰憑證被廢止之復原程序

總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 政府憑證總管理中心之簽章金鑰遭破解之復原程序

總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 政府憑證總管理中心安全設施之災後復原工作

總管理中心每年對安全設施之災後復原工作進行演練。

4.9 政府憑證總管理中心之終止服務

總管理中心終止服務時，將依據電子簽章法相關規定辦理。

總管理中心遵守以下事項，以確保終止服務對於交互認證憑證機構與信賴憑證者造成之影響最小：

(1) 總管理中心於預定終止服務 3 個月前，將通知交互認證憑證機構(無法通知者，不在此限)，並公告於儲存庫。

(2) 總管理中心終止服務時，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

總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總管理中心之相關設備。

5.1.2 實體存取

總管理中心以保證等級第 4 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總管理中心系統的惡意軟體。

非總管理中心人員進出機房，需填寫進出紀錄，並由總管理中心

相關人員全程陪同。

總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

總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。

總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

總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

總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總管理中心機房儲存 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 節所述之總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，與總管理中心機房距離 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。異地備援系統與總管理中心系統具有相同的安全等級。

5.2 程序控制

總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

總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。

總管理中心共有 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、設定和維護總管理中心系統。
- 建立和維護總管理中心系統之使用者帳號。
- 設定稽核參數。
- 產製和備份總管理中心之金鑰。
- 公布憑證機構廢止清冊於儲存庫。

(2) 簽發員負責：

- 執行憑證簽發。
- 執行憑證廢止。

(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，以確認總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。
- 除總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，總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 種信賴角色。

(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、設定和維護總管理中心憑證管理系統	2				1
建立和維護總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
產製和備份總管理中心之金鑰	2		1		1
執行憑證簽發		2			1
執行憑證廢止		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
公布憑證機構廢止清冊在儲存庫	1				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
除總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

總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

- 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

總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

總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。

5.3.2 身家背景之查驗程序

總管理中心對於 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、總管理中心之安全認證機制。 2、總管理中心系統安裝、設定和維護之操作程序。 3、建立和維護系統交互認證憑證機構帳號之操作程序。 4、設定稽核參數之操作程序。 5、產製和備份總管理中心金鑰之操作程序。 6、災後復原及業務永續經營之程序。
簽發員	1、總管理中心之安全認證機制。 2、總管理中心系統軟硬體的使用及操作程序。 3、憑證簽發之操作程序。 4、憑證廢止之操作程序。 5、災後復原及業務永續經營之程序。
稽核員	1、總管理中心之安全認證機制。 2、總管理中心系統軟硬體的使用及操作程序。 3、產製和備份總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、總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

在總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

總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總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

總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

總管理中心提供政府機關公開金鑰基礎建設憑證政策、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總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

總管理中心依照 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，除金鑰備份回復及更換密碼模組情形外，皆應儲存於硬體密碼組內不得匯出。

總管理中心之金鑰產製由相關人員見證並簽署金鑰啟用見證書(其中記載產製的金鑰對之公開金鑰)，並透過公信管道公布，以昭公信。

交互認證之憑證機構必須依照憑證政策之規定進行金鑰對之產製。

總管理中心在簽發交互認證憑證機構之憑證時，將檢查憑證申請檔中之公開金鑰，確定該憑證機構的公開金鑰在總管理中心所簽發過的憑證中是唯一的。

6.1.2 私密金鑰安全傳送給交互認證憑證機構

與總管理中心交互認證憑證機構必須自行產製私密金鑰，因此總管理中心不需將私密金鑰傳送給交互認證憑證機構。

6.1.3 公開金鑰安全傳送給政府憑證總管理中心

由提出交互認證憑證機構於申請時提交 PKCS#10 的憑證申請檔。

6.1.4 政府憑證總管理中心公開金鑰安全傳送給信賴憑證者

總管理中心本身之自簽憑證內含總管理中心之公開金鑰，安全散布管道包括以下幾種：

(1) 總管理中心在簽發交互憑證給憑證機構後，於遞交交互憑證時，一併將總管理中心之自簽憑證或公開金鑰遞交給該憑證機構，該憑證機構以符記(例如 IC 卡)儲存總管理中心之自簽憑證或公開金鑰，並以安全方式傳送給該憑證機構的用戶或信賴憑證者。

(2) 將總管理中心本身之自簽憑證存至(Build-in)可信賴之第三方所發行的軟體中，使用者透過安全管道取得軟體(例如向可信賴的經銷商購買軟體的安裝光碟)並安裝後，便可得到總管理中心本身之自簽憑證。

(3) 在大量發行的光碟中放置總管理中心之自簽公開金鑰憑證，使用者透過安全管道取得這些光碟，便可得到總管理中心本身之自簽憑證。

(4) 總管理中心啟用時，當場公布總管理中心之公開金鑰，

並由相關人員簽署總管理中心公開金鑰見證書，同時交由媒體公布。信賴憑證者可利用媒體公布之總管理中心公開金鑰，比對從網路下載之總管理中心自簽公開金鑰憑證中所記載之公開金鑰。

6.1.5 金鑰長度

總管理中心使用 4096 位元的 RSA 金鑰及SHA-256、SHA-384、SHA-512雜湊函數演算法簽發憑證。

交互認證之憑證機構必須依照憑證政策之規定選擇適當的金鑰長度；總管理中心於簽發交互憑證前將審查該憑證機構所選擇的金鑰長度是否恰當。

6.1.6 公鑰參數之產製

採用 RSA 演算法之公開金鑰參數為空的(Null)。

6.1.7 金鑰參數品質之檢驗

總管理中心採用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)。

交互認證之憑證機構必須依據所選用的演算法，進行適當的金鑰參數品質檢驗。

6.1.8 金鑰經軟體或硬體產製

總管理中心使用硬體密碼模組產製亂數、公開金鑰對和對稱金鑰。

交互認證之憑證機構必須依照憑證政策之規定，選擇適當的軟體或硬體進行金鑰產製；總管理中心於簽發交互憑證前將審查該憑證機構所選擇的軟體或硬體是否恰當。

6.1.9 金鑰之使用目的

總管理中心之自簽憑證相對應的私密金鑰僅限用於簽發憑證及憑證機構廢止清冊。本版本起新簽發之自簽憑證須含金鑰用途擴充欄位。

總管理中心簽發給交互認證憑證機構的憑證，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。

6.2 私密金鑰保護

6.2.1 密碼模組標準

總管理中心依據憑證政策的規定，使用通過FIPS140-2 Level 3認證安全等級的硬體密碼模組產製亂數及金鑰對。

交互認證之憑證機構必須依照憑證政策之規定，選擇適當的密碼模組；總管理中心於簽發交互憑證前將審查該憑證機構所選擇的密碼模組之安全等級是否恰當。

6.2.2 金鑰分持之多人控管

總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。採用此方法可使總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)。

如欲簽發保證等級第 3 及第 4 級憑證的憑證機構之簽章用私密金鑰，必須依據憑證政策規定採用多人控管程序。總管理中心於簽發交互憑證前將審查該憑證機構所採用的多人控管程序是否恰當。

6.2.3 私密金鑰託管

總管理中心簽章用私密金鑰不可被託管，總管理中心也不負責保管交互認證憑證機構的簽章用私密金鑰。

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。

交互認證之憑證機構必須依照憑證政策之規定，選擇適當的私密金鑰備份方法；總管理中心於簽發交互憑證前將審查該憑證機構所選擇的私密金鑰備份方法是否恰當。

總管理中心不負責保管交互認證憑證機構的私密金鑰備份。

6.2.5 私密金鑰歸檔

總管理中心簽章用私密金鑰不可被歸檔。總管理中心亦不對交互認證憑證機構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

總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「產製和備份總管理中心之金鑰」任務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敏感性參數完全銷毀。

交互認證之憑證機構如需將私密金鑰輸入密碼模組，必須依照憑證政策之規定，選擇適當的私密金鑰輸入方法；總管理中心於簽發交互憑證前將審查該憑證機構所選擇的私密金鑰輸入方法是否恰當。

6.2.7 私密金鑰之啟動方式

總管理中心之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。

交互認證之憑證機構必須依照憑證政策之規定，選擇適當的私密

金鑰啟動方式；總管理中心於簽發交互憑證前將審查該憑證機構所選擇的私密金鑰啟動方式是否恰當。

6.2.8 私密金鑰之停用方式

由於總管理中心採離線作業方式，因此平常總管理中心之金鑰對保持在停用(Deactivation)狀態，以避免私密金鑰遭非法使用。

每次完成簽發憑證及相關管理作業後，將採m-out-of-n方式將私密金鑰停用。

交互認證之憑證機構必須依照憑證政策之規定，選擇適當的私密金鑰停用方式；總管理中心於簽發交互憑證前將審查該憑證機構所選擇的私密金鑰停用方式是否恰當。

6.2.9 私密金鑰之銷毀方式

為避免舊的總管理中心私密金鑰被盜用，妨害憑證之真確性，本管理中心CA金鑰到期時其私密金鑰必須加以銷毀。當總管理中心完成金鑰更換及取得新的總管理中心憑證，且不再簽發任何憑證與憑證廢止清冊之後，將會把存在硬體密碼模組內舊的總管理中心私密金鑰做零值化處理(Zeroization)，以便確保銷毀硬體密碼模組中舊的總管理中心私密金鑰。

交互認證之憑證機構必須依照憑證政策之規定，選擇適當的私密金鑰銷毀方式；總管理中心於簽發交互憑證前將審查該憑證機構所選

擇的私密金鑰銷毀方式是否恰當。

6.3 交互認證憑證機構金鑰對管理之其他規定

交互認證憑證機構必須自行管理金鑰對，總管理中心不負責保管交互認證憑證機構的私密金鑰。

6.3.1 公開金鑰之歸檔

總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，因憑證之歸檔可代替公開金鑰之歸檔。

6.3.2 公開金鑰及私密金鑰之使用期限

6.3.2.1 政府憑證總管理中心公開金鑰及私密金鑰之使用期限

總管理中心公開金鑰及私密金鑰之金鑰長度為RSA 4096位元，使用期限至多為30年；但以其執行簽發憑證用途之使用期限至多為10年。

6.3.2.2 交互認證憑證機構公開金鑰及私密金鑰之使用期限

RSA 2048 位元：公開金鑰憑證及私密金鑰之使用期限至多為 20 年，但以私密金鑰執行簽發憑證之用途，其使用期限至多為 10 年。

總管理中心簽發給交互認證憑證機構的憑證，其憑證生命週期，加上總管理中心用來簽署憑證之簽章用私密金鑰生命週期，合計不得超過總管理中心自簽憑證生命週期。

6.4 啟動資料之保護

6.4.1 啟動資料之產生

總管理中心之啟動資料由硬體密碼模組產生，再寫入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卡的個人識別碼(以下簡稱PIN碼)直接在硬體密碼模組內建的鍵盤上輸入。

交互認證之憑證機構必須依照憑證政策之規定，選擇適當的啟動資料產生方式；總管理中心於簽發交互憑證前將審查該憑證機構所選擇的啟動資料產生方式是否恰當。

6.4.2 啟動資料之保護

總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。

交互認證之憑證機構必須依照憑證政策之規定，選擇適當的啟動資料保護方式；總管理中心於簽發交互憑證前將審查該憑證機構所選擇的啟動資料保護方式是否恰當。

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

總管理中心和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

總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

總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，該規範並公布於 GRCA 網站之儲存庫。

總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，並且在每次使用時會檢查是否有惡意程式碼。

6.6.2 安全管理控管措施

總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，總管理中心於每次使用時檢驗軟體的完整性，同時每月將例行檢驗證軟體的完整性。

總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

總管理中心之主機和內部儲存庫不與外部網路連接，外部儲存庫連接到網際網路(Internet)上，提供不中斷之憑證及憑證機構廢止清冊查詢服務(除必要之維護或備援外)。

總管理中心之內部儲存庫資訊(包括憑證及憑證機構廢止清冊)以數位簽章保護，使用手動方式，從內部儲存庫傳送到外部儲存庫。

總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，以防範阻絕服務及入侵等攻擊。

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

總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

總管理中心簽發 X.509 v3 版本的憑證。

7.1.2 憑證擴充欄位

總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

總管理中心簽署在憑證中的簽章其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)

總管理中心所簽發憑證中的主體公鑰之演算法，必須使用下述之物件識別碼：

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

不採用命名限制。

7.1.6 憑證政策物件識別碼

總管理中心的自簽憑證不含憑證政策(certificatePolicies)擴充欄位。總管理中心簽發的自發憑證或給下層憑證管理中心的交互憑證，其憑證政策(Certificate Policy)欄位必須使用本基礎建設之憑證政策物件識別碼。此外亦可包含 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

總管理中心簽發之交互憑證，必要時將使用政策限制擴充欄位。

7.1.8 政策限定元之語法及語意

總管理中心簽發之憑證不含政策限定元(Policy Qualifiers)。

7.1.9 憑證政策擴充欄位之關鍵性語意處理

總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 憑證機構廢止清冊之格式剖繪

7.2.1 版本序號

總管理中心簽發 X.509 v2 版本的憑證機構廢止清冊。

7.2.2 憑證機構廢止清冊擴充欄位

總管理中心簽發的憑證機構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，總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

評估變更項目對交互認證憑證機構或信賴憑證者之影響程度：

(1) 影響程度大者，於總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，於總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總管理中心儲存庫，8.1.2.1 節之(1)影響程度大者，將以公文書通知交互認證憑證機構。

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，以總管理中心儲存庫公告之回覆方式傳送給總管理中心，總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 個日曆天內公告於總管理中心儲存庫，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，由總管理中心公布。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)