中華電信憑證總管理中心

憑證實務作業基準

ePKI Root Certification Authority, eCA

Certification Practice Statement

第 1.2 版(草案)

中華電信股份有限公司

中華民國一百零二年九月日

目　　錄

摘要

中華電信憑證總管理中心憑證實務作業基準之重要事項說明如下：(依據電子簽章法第十一條及經濟部頒訂之『憑證實務作業基準應載明事項準則』之規定)

1、**主管機關核定文號**：經商字第　　號（待訂）。

2、**簽發之憑證**：

(1)種類：中華電信憑證總管理中心(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：依據中華電信公開金鑰基礎建設憑證政策，簽發五種保證等級的憑證。

(3)適用範圍：

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。

自發憑證為總管理中心更換金鑰或憑證政策所簽發之憑證，用以建立新舊金鑰間或憑證政策互通信賴路徑之用。

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，包括中華電信公開金鑰基礎建設第一層之下屬憑證機構和中華電信公開金鑰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。

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本作業基準及與各該交互認證機構簽訂之契約所訂定之責任範圍為限。

(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) 本公司將委託公正之第三方,就中華電信憑證總管理中心的運作進行稽核。

1 序論

本文件的名稱為中華電信憑證總管理中心憑證實務作業基準(ePKI Root Certification Authority Certification Practice Statement of Chunghwa Telecom; 以下簡稱為本作業基準)。本作業基準係依據中華電信公開金鑰基礎建設憑證政策(Certificate Policy for the Chunghwa Telecom ecommerce Public Key Infrastructure，以下簡稱憑證政策)所訂定，並遵循電子簽章法之子法「憑證實務作業基準應載明事項準則」相關規定，主要說明中華電信憑證總管理中心(ePKI Root Certification Authority，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。

。

依據憑證政策的規定，總管理中心是中華電信公開金鑰基礎建設(Chunghwa Telecom ecommence Public Key Infrastructure, ePKI，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（Trust Anchor），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。

1.1 本作業基準之適用範圍

本作業基準所載明之實務作業規範適用於與總管理中心相關之個體，包括總管理中心、交互認證憑證機構(Subject CA)、信賴

憑證者(Relying Parties)及儲存庫(Repository)等。

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

本作業基準為 1.2 版，版本發行日期為中華民國 102 年 月 日(待定)。本作業基準之最新版本可在以下網頁取得：

http://ePKI.com.tw。

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四級之規定，所簽發之憑證保證等級共分五級，下表為在 id-cht arc 註冊的憑證政策物件識別碼：

id-cht ::= {2 16 886 1}

id-cht-ePKI ::= {2 16 886 1 100}

id-cht-ePKI-certpolicy::= {id-cht-ePKI 0}

保證等級	物件識別碼名稱	物件識別碼值
測試級	id-cht-ePKI-certpolicy-testAssurance	{id-cht-ePKI-certpolicy 0}
第一級	id-cht-ePKI-certpolicy-class1Assurance	{id-cht-ePKI-certpolicy 1}
第二級	id-cht-ePKI-certpolicy-class2Assurance	{id-cht-ePKI-certpolicy 2}
第三級	id-cht-ePKI-certpolicy-class3Assurance	{id-cht-ePKI-certpolicy 3}

保證等級	物件識別碼名稱	物件識別碼值
第四級	id-cht-ePKI-certpolicy-class4Assurance	{id-cht-ePKI-certpolicy 4}

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)中華電信憑證總管理中心。

(2)儲存庫。

(3)交互認證憑證機構。

(4)信賴憑證者。

1.3.1 中華電信憑證總管理中心

總管理中心是本基礎建設的信賴起源，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、管理本基礎建設第一層之下屬憑證機構(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://ePKI.com.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一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(Certficate Subject Name)與公開金鑰間連結關係之第三者。信賴憑證者必須依照相對的憑證機構憑證及憑證狀態資訊，以驗證所使用的憑證有效性。在確認憑證的有效性後，才可使用憑證進行以下作業：

(1)驗證具有數位簽章的電子文件之完整性。

(2)驗證電子文件簽章產生者的身分。

(3)與憑證主體間建立安全之通訊管道。

1.3.5 適用範圍

1.3.5.1 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、自發憑證與交互憑證。

自簽憑證用以建立中華電信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互通信賴路徑之用，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，包括本基礎建設第一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。

總管理中心簽發之憑證依據憑證政策之規定分為五種保證等級，各保證等級建議之適用範圍如下：

保證等級	適用範圍

測試級	僅供測試(Test)用，對於傳送的資料不負任何法律責任。
第一級	基本級(Rudimentary)的保證等級，適合應用於遭到惡意篡改威脅很低的網路環境，或無法提供較高保證等級時，可識別用戶個體名稱及保證被簽署文件的完整性；但不適合應用於需要認證的線上交易。
第二級	初級(Basic)的保證等級，適合應用於資訊可能被篡改，但不會有惡意篡改之網路環境(資訊可能被截取但機率不高)，且不適合做為重要文件的簽署。
第三級	中級(Medium)的保證等級，適合應用於有惡意使用者會截取或篡改資訊、並較第二級危險之網路環境，傳送的資訊可包括金錢上的線上交易。
第四級	高級(High)的保證等級，適合應用於潛在威脅很高之網路環境、或資訊被篡改後復原的代價很高，傳送的資訊包括高金額的線上交易或極機密的文件。

1.3.5.2 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，避免所取得儲存的總管理中心之公開金鑰或自簽憑證遭破壞或更換，俾可確保使用正確的總管理中心公開金鑰或自簽憑證來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對應(Policy Mapping)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。

信賴憑證者必須依照 6.1.9 節金鑰之使用目的之規定，適當地使用金鑰，並使用符合國際標準（例如 X.509 標準或 IETF RFC5280 等）定義之憑證驗證(certificate validation)方法來驗證憑證的有效性(validity)。

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更新。

1.3.5.3 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

對本作業基準有任何疑慮時或用戶報告遺失金鑰等事件，可直接與總管理中心聯絡。

聯絡電話:0800080365。

郵遞地址：台北市信義路一段 21 號數據通信大樓中華電信憑證總管理中心。

電子郵件信箱：caservice@cht.com.tw。

其他聯絡資料或聯絡資料有所更動，請上 http://epki.com.tw 查詢。

2 一般條款

2.1 職責及義務

2.1.1 中華電信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 1.3.5 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。

(10) 信賴憑證者應於了解並同意有關總管理中心法律責任之條款，並依照 1.3.5 節規定範圍內信賴該憑證後，始得接受使用總管理中心所簽發之憑證。

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 中華電信憑證總管理中心之責任

2.2.1.1 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。

2.2.1.2 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 1.3.5 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。

2.2.1.3 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與各該交互認證機構簽訂之契約所訂定之責任範圍為限。

2.2.1.4 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，惟應於三日前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，以減少對信賴憑證者之影響，並承擔所有因使用該憑證機構之憑證所引發之責任。

2.3 財務責任

總管理中心由本公司營運，其財務責任由本公司負責。

2.3.1 財務保險

總管理中心憑證業務目前尚未辦理保險，未來將遵守主管機關規定加入保險。

2.3.2 財務稽核

總管理中心之財務，係屬本公司整體財務之一部。本公司為股票上市公司，依證券交易法第三十六條之規定，應於每營業年度終了後三個月內公告，並向主管機關申報，經會計師查核簽證，董事會通過及監察人承認之年度財務報告。並於每會計年度第一季、第二季及第三季終了後四十五日內，公告並申報經會計師核閱及提報董事會之財務報告。於每月十日以前，公告並申報

上月份營運情形。

2.4 準據法及爭議之解決

2.4.1 準據法

依據本作業基準所簽署的任何協議之解釋，悉依據中華民國相關法律之規定。

2.4.2 可分割性及存續

本作業基準的任何一節無效時，除去無效之該部分外，本作業基準的其他章節仍繼續維持其有效性，直到本作業基準修改為止，本作業基準的修改如第 8 章所述。

2.4.3 爭議解決

本公司所屬憑證機構與總管理中心如有爭議時，依本公司組織管理體制，由共同上級主管調處解決。非本公司設立之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，依雙方契約約定之紛爭處理程序處理。如需訴訟時，以臺灣臺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 中華電信憑證總管理中心之資訊公布

總管理中心於儲存庫公布：

(1) 憑證政策。

(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) 相關最新消息。

(9) 最近一次之稽核結果。

2.6.2 公布頻率

總管理中心每天至少簽發兩次的憑證機構廢止清冊，並公布於儲存庫。所簽發的憑證機構廢止清冊之有效期限不超過 36 小時。在憑證機構廢止清冊尚未過期前，總管理中心即可能簽發新的憑證機構廢止清冊，因此新憑證機構廢止清冊的效期與舊的憑證機構廢止清冊的效期會可能有所重疊，在效期重疊期間，即使舊的憑證機構廢止清冊尚未過期，信賴憑證者仍可至總管理中心儲存庫取得新的憑證機構廢止清冊，以獲得更即時的憑證機構憑證廢止資訊。

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://ePKI.com.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

本公司將委外辦理總管理中心之外部稽核作業，委託熟悉總管理中心、下屬憑證機構運作並經 WebTrust for CA 標章管理單位

授權可於中華民國執行 Trust Service Principles and Criteria for Certification Authorities 之稽核業者，提供公正客觀的稽核服務，稽核人員應為合格授權之資訊系統稽核員(Certified Information System Audit，CISA)或具同等資格，且具備 2 場次 4 人天以上之憑證機構 WebTrust for CA 標章稽核或 2 場次共計 8 人天憑證機構資訊安全管理稽核相關經驗，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

本公司將委託公正之第三人，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) 將不符合情形通知總管理中心。

對於不符合規定之項目，總管理中心將於 30 日內提出改善

計畫，儘速執行，並列入後續稽核追蹤項目。

2.7.6 稽核結果公開之範圍

總管理中心將公布稽核者所提供之應公開說明資訊。

2.8 資訊保密之範圍

2.8.1 機密之資訊種類

由總管理中心產生、接收或保管之資料，均視為機密資訊，現職及曾任職於總管理中心之人員與各類稽核人員對於機密資訊均負保密責任。機密資訊包括：

(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。

(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報告，不得被完整公開。

(6) 列為機密等級的營運相關文件。

2.8.2 非機密資訊之種類

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機密資訊。

識別資訊或記載於憑證的資訊，除特別約定外，不視為機密資訊。

2.8.3 憑證廢止或暫時停用資訊之公開

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 應法定程序要求釋出資訊

司法機關、監察機關或治安機關如因調查或蒐集證據需要，必須查詢 2.8.1 節機密資訊，依法定程序辦理；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。

2.8.6 其他資訊釋出之情況

依相關規定法令辦理。

2.8.7 隱私權保護

總管理中心依照個人資料保護法處理憑證機構之交互認證申請資料。

2.9 智慧財產權

總管理中心的金鑰對及金鑰分持之所有權為總管理中心所擁

有。交互認證憑證機構的金鑰對為該憑證機構所有，但其公開金鑰經總管理中心簽發成憑證時，該憑證之所有權亦為總管理中心所擁有。

總管理中心簽發的憑證及憑證機構廢止清冊之所有權為總管理中心所擁有。

總管理中心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所有。

總管理中心將儘可能確保交互認證憑機構名稱的正確性，但不保證交互認證憑證機構名稱之商標權歸屬。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。

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

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。

為便於與國際互通，總管理中心的自簽憑證使用以下名稱格式：

C = TW，

O = Chunghwa Telecom Co., Ltd.，

OU = ePKI Root Certification Authority

此外，總管理中心之自簽憑證及自發憑證中，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公司處理。

3.1.6 商標之辨識、鑑別及角色

交互認證憑證機構提供之憑證主體名稱包含商標或任何受法律保護之姓名、商號、名稱、表徵時，總管理中心雖不負審查之責，但其命名必須符合我國商標法、公平交易法及其相關規定，總管理中心不保證憑證主體名稱商標之認可、驗證、合法及唯一性，相關之糾紛或仲裁處理，非總管理中心之權責範圍，由交互認證憑證機構向相關主管機關或法院提出申請。

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。由該憑證機構產生一個 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

交互認證機構之身分鑑別程序分為兩種：

由本公司自行設立之憑證機構(例如：中華電信通用憑證管理

中心)，由本公司召開政策管理委員會會議審核。

非本公司自行設立之憑證機構，由憑證機構提交交互認證申請書，申請書中包含組織名稱、所在地及代表人等足以識別該組織之資料。總管理中心將確認該組織是否存在，驗證申請書之真偽、代表人身分及代表人是否有權代表該組織，代表人應親臨本公司辦理憑證申請。

如下屬憑證機構核發之憑證用途為電子郵件之簽章及加密，下屬憑證機構應鑑別該組織身分並確認該組織確實擁有或被授權使用記載於憑證內之電子郵件信箱。

如下屬憑證機構核發之憑證用途為 SSL 伺服器加密傳輸，下屬憑證機構應鑑別該組織之身分並確認該組織確實擁有或被授權使用記載於憑證內之網域名稱(domain name)，下屬憑證機構得與可信賴之資料庫登記資料進行比對。

如下屬憑證機構核發之憑證用途為專屬類伺服器之簽章與加密，下屬憑證機構應鑑別該組織之身分並確認該組織記載於憑證內之專屬類軟體名稱是否恰當。

如下屬憑證機構核發之憑證用途為時戳類伺服器之簽章與加密，下屬憑證機構應鑑別該組織之身分並確認該組織記載於憑證內之時戳伺服器的應用軟體名稱是否恰當。

如下屬憑證機構核發之憑證用途為程式碼簽章(code signing)，下屬憑證機構應鑑別該組織之身分並確認該組織確實與記載於憑證內之組織名稱相符。

3.1.9 個人身分鑑別之程序

本公司所設立之憑證機構不適用。

非本公司所設立之憑證機構，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，需與憑證機構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。

3.2 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一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，用來簽發憑證用途的效期至多為 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 3.1.8 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 節規定相同。

3.5 憑證暫時停用與恢復使用

總管理中心不提供憑證暫時停用與恢復使用。

4.營運規範

4.1 申請憑證之程序

4.1.1 起始(Initiation)

(1)起始申請

本公司所設立之憑證機構,由本公司召開政策管理委員會會議審核，非本公司設立之憑證機構須送交互認證申請書、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中華電信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中華電信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各該機構所

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。

4.1.2 審查申請(Examination)

憑證機構提出交互認證申請時，將召開政策管理委員會會議，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。最後依該委員會之決議，決定進入下一階段，或要求補送資料，或駁回申請。

4.1.3 協議(Arrangement)

本公司設立之憑證機構，交互認證得免簽署交互認證協議書。

非本公司設立之憑證機構提出交互認證申請時，將召開會議通知申請交互認證之憑證機構參加，並進行以下步驟：

(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)。

(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。

如核可憑證申請將通知交互認證之憑證機構，由總管理中心執行憑證簽發之相關工作。憑證簽發後，如為非本公司設立之憑證機構，本公司將發函通知該憑證機構並檢附簽發的憑證。

如未核可憑證申請，將發函通知申請交互認證之憑證機構，並說明未核可的理由。

總管理中心將簽發一張自簽憑證(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通知後，必須檢查所附的憑證，確認該憑證內容之正確性，如憑證內容無誤，應通知總管理中心，非本公司設立之憑證機構必須簽署憑證接受確認文件，並函復本公司，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，包括私密金鑰資料外洩或遺失。

(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)總管理中心終止服務。

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

4.4.3.1 起始(Initiation)

(1)起始申請

發函提出申請，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，或發函通知該交互認

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。

4.4.3.2 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。憑證廢止後將發函通知交互認證憑證機構，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 憑證廢止申請之處理期間

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

不提供暫時停用憑證服務，故不適用。

4.4.7 暫時停用憑證之程序

不提供暫時停用憑證服務，故不適用。

4.4.8 暫時停用憑證之處理期間及停用期間

不提供暫時停用憑證服務，故不適用。

4.4.9 恢復使用憑證之程序

不提供恢復停用憑證服務，故不適用。

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至少一次，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

不提供線上憑證狀態查詢服務，故不適用。

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

不提供其他形式廢止公告，故不適用。

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。

4.5 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。

■ 所有為進行金鑰回復工作，對保存在憑證機構的憑證主體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一次使用之金鑰)。

(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。
- 符記之傳遞過程
- 符記之零值化
- 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一次稽核紀錄，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。憑證機構自上次稽核檢視後所發生的重大安全稽核紀錄都應加以檢視，並且對任何可能之惡意活動應進一步調查。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

稽核紀錄檔現場(on site)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

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。

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。

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一次。

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。

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

- 作業系統的弱點評估。
- 實體設施的弱點評估。
- 憑證管理系統的弱點評估。
- 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

- 總管理中心被主管機關認證(Accreditation)的資料（假設適用）。
- 憑證實務作業基準。
- 交互認證協議書（假設適用）。
- 系統與設備組態設定。
- 系統或組態設定修改與更新的內容。
- 憑證申請資料。
- 廢止申請資料。
- 憑證接受的確認文件。
- 已簽發或公告的憑證。
- 總管理中心金鑰更換的紀錄。
- 已簽發或公告的憑證機構廢止清冊。
- 稽核記錄。
- 用來驗證及佐證歸檔內容的其它說明資料或應用程式。
- 稽核人員要求的文件。
- 依照 3.1.8 及 3.1.9 所定的組織身分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二十年，用來處理歸檔資料的應用程式也將維護二十年。

歸檔資料逾保留期限後，書面資料應以安全方式銷毀；電子形式資料備份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

不允許新增、修改或刪除歸檔資料。

總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。

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。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

總管理中心最遲於其私密金鑰簽發憑證用途的使用期限到期前，更換用來簽發憑證的金鑰對，並簽發一張新的自簽憑證及兩張自發憑證。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其私密金鑰簽發憑證用途的使用期限到期前，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 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。

4.8.2 中華電信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。

4.8.3 中華電信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。

4.8.4 中華電信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 中華電信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三個月前，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四級的實體控管規定運作。機房共有四層門禁，第一層和第二層分別為全年無休的大門及大樓警衛，第三層為樓層讀卡機進出管制系統，第四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六天)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一年，一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機密資訊，文件資料部分在不需使用時，將經碎紙機處理；磁帶、硬碟、磁碟、磁光碟(MO)及其他形式的記憶體，在報廢前，將經格式化程序清除儲存的資料，光碟將被實體銷毀。

5.1.8 異地備援

異地備援的地點在臺中，與總管理中心機房距離三十公里以上。備援的內容包括資料與系統程式，全部資料備份一個星期至少執行一次，異動資料備份於異動當天執行，異地備援之非技術安全控管與總管理中心為相同的安全等級。

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。

總管理中心共有五種不同的信賴角色，分別為管理員(Administrator)、簽發員(Officer)、稽核員(Auditor)、維運員(Operator)和實體安全控管員(Controller)，每種信賴角色將依照5.3 節規定進行人員控管，以防止可能的內部攻擊。一種信賴角色可由多人擔任，每種信賴角色設有一名主管(Chief Role)，五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 節定義的五種信賴角色，總管理中心之角色分派必須符合以下規定：

(1)管理員、簽發員和稽核員三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信賴角色。

(3)任何一種信賴角色均不允許執行自我稽核功能。

5.2.3 每個任務所需之人數

依據各種信賴角色的作業安全需求，所需之人數如下：

(1)管理員：至少 3 位合格人員擔任。

(2)簽發員：至少 3 位合格人員擔任。

(3)稽核員：至少 2 位合格人員擔任。

(4)維運員：至少 2 位合格人員擔任。

(5)實體安全控管員：至少 2 位合格人員擔任。

每個任務所需之人數說明如下：

任務名稱	管理員	簽發員	稽核員	維運員	實體安全控管員
安裝、設定和維護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

任務名稱	管理員	簽發員	稽核員	維運員	實體安全控管員
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
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 識別及鑑別每一個角色

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，將遵守維護機密責任之約

定。

(4)維護機密責任之約定

總管理中心之相關人員均負維護機密之責任，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密。

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

管理員調離原職務滿 1 年後，才可轉任簽發員或稽核員。

簽發員調離原職務滿 1 年後，才可轉任管理員或稽核員。

稽核員調離原職務滿 1 年後，才可轉任管理員或簽發員。

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

總管理中心聘僱人員安全要求遵照 5.3 節規定。

5.3.8 提供之文件資料

總管理中心提供中華電信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，依照 NIST FIPS 140-2 規範之演算法，私密金鑰之匯出與匯入依照 6.2.2 與 6.2.6 節規定辦理。

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中華電信憑證總管理中心

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 中華電信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)可信賴之第三者所發行的軟體中，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-1 或 SHA-2 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 NIST FIPS 186-3 規範產生 RSA 演算法所需的質數，並保證該質數為強質數(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，但總管理中心之自簽憑證並不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，使用安全等級 3 的硬體密碼模組。

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，採採用通過 NIST FIPS

140-2 規範的秘密分享(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。

如欲簽發保證等級第三及第四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 6.2.2 節之規定採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機密參數完全銷毀。

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)，是以多人控管 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，將採多人控管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

為避免總管理中心舊的私密金鑰被盜用，影響簽發憑證之正確性，總管理中心之私密金鑰生命週期屆滿時將加以銷毀。因此，在總管理中心完成金鑰更新及簽發新的總管理中心自簽憑證，且不再簽發任何憑證與憑證機構廢止清冊之後，將會把硬體密碼模組中存放舊的總管理中心私密金鑰之記憶位置填零(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。

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 中華電信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

(1)RSA 2048 位元：公開金鑰憑證及私密金鑰之之使用期限至多為 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

總管理中心的私密金鑰的啟動資料不做歸檔。

6.5 電腦軟硬體安控措施

6.5.1 特定電腦安全技術需求

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：

- 具備身分鑑別的登入。
- 提供自行定義(Discretionary)存取控制。
- 提供安全稽核能力。
- 對於各種憑證服務和信賴角色存取控制的限制。
- 具備信賴角色及身分的識別和鑑別。
- 以密碼技術確保每次通訊和資料庫之安全。
- 具備信賴角色和相關身分識別的安全及可信賴的管道。
- 具備程序完整性及安全控管保護。

6.5.2 電腦安全評等

憑證中心憑證伺服器採用通過 Common Criteria EAL 4 認證的電腦作業系統。

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 CMMI 的規範進行品質控管。

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。

各項交付總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，並提供產品或程式交付清單、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

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。

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。

總管理中心在風險評鑑、風險處理與安全管理控管措施參考 ISO/IEC 27001、ISO/IEC 27002、ISO/IEC 27005、ISO/IEC 31000 及 AICPA/CICA Trust Service Principles and Criteria for Certification

Authorities 及 Browser Forum Baseline Requirements 之方法論或控制項。

6.6.3 生命週期安全評等

每年至少一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

總管理中心之主機不與外部網路連接，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)。

總管理中心主機所簽發之憑證及憑證機構廢止清冊以數位簽章保護，使用手動方式，從總管理中心主機傳送到儲存庫。

總管理中心之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 ITU-T X.509、CA/Browser Forum 及 IETF PKIX Working Group 的相關規定。

7.1.1 版本序號

總管理中心簽發 ITU-T 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遵循 IETF PKIX Working Group RFC 5280 之規定。

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：

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

(OID：1.2.840.113549.1.1.5)

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 IETF PKIX Working Group RFC5280 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

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

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 關鍵憑證政策擴充欄位之語意處理

總管理中心簽發之憑證所含之憑證政策擴充欄位不註記為關鍵擴充欄位。

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 ITU-T 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 ITU-T X.509、CA/Browser Forum 及 IETF PKIX Working Group 的相關規定。

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

評估變更項目對交互認證憑證機構或信賴憑證者之影響程度：

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。

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，將發函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：

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。

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。