中華電信憑證管理中心

憑證實務作業基準

(ChungHwa Telecom Certification Authority Certification Practice Statement，CHTCA CPS)

版本 1.0

中華電信股份有限公司

中華民國九十四年九月二十三日

目　　錄

中華電信憑證管理中心憑證實務作業基準摘要

依據電子簽章法之子法「憑證實務作業基準應載明事項準則」規定，中華電信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：

一、主管機關核定文號：經商字第 09402419750 號

二、簽發之憑證：

1.種類：中華電信股份有限公司(以下簡稱本公司)員工、外包人員與伺服器應用軟體等三種憑證，包括簽章用及加解密用的憑證。

2.保證等級：中華電信憑證管理中心依據中華電信公開金鑰基礎建設憑證政策保證等級第三級運作，簽發憑證政策所定義保證等級第三級的憑證。

三、應用範圍：

憑證適用於本公司企業網路相關應用所需的身分認證及資料加密。

用戶及相關信賴憑證者，必須謹慎的使用中華電信憑證管理中心所簽發之憑證，不得逾越本作業基準所限制及禁止的憑證應用範圍。

四、有關法律責任重要事項

1.中華電信憑證管理中心損害賠償責任

中華電信憑證管理中心處理用戶憑證簽發作業，若故意或過失未遵照本作業基準及相關作業規定，致用戶或信賴憑證者受有損害時，依本公司人事獎懲或合約規定，對相關疏失人員進行懲處，對於相關之損害賠償，依民法相關規定辦理。

2.中華電信憑證管理中心責任之免除

用戶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損害，如該損害之造成不可歸責於中華電信憑證管理中心時，應由該用戶或信賴憑證者自負損害賠償之責。

3.註冊中心責任之免除

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，如該損害之造成不可歸責於註冊中心時，應由用戶自負損害賠償之責，又用戶或信賴憑證者未依照 1.3.5 節規定之適用範圍使用憑證所引發之損害，如該損害之造成不可歸責於註冊中心時，應由該用戶或信賴憑證者自負損害賠償之責。

4.除外條款

如因不可抗力及其他非可歸責於中華電信憑證管理中心及註冊中心之事由，所導致之損害事件，中華電信憑證管理中心及註冊中心不負任何法律責任。如因憑證系統維護、轉換及擴充等需要，得事先公告於儲存庫，暫停部分憑證服務，用戶或信賴憑證者不得以此作為要求中華電信憑證管理中心損害賠償之理由。

5.財務責任

中華電信憑證管理中心以中華電信股份有限公司為財務擔保；中華電信憑證管理中心財務依相關法律規定辦理財務稽核。

6.用戶責任

用戶應妥善保管及使用其私密金鑰，用戶之憑證如須暫停使用、恢復使用、廢止憑證，應依照 4.4 節規定辦理，如發生私密金鑰資料外洩或遺失等情形，必須廢止憑證時，應立即通知憑證中心，但用戶仍應承擔異動前所有使用該憑證之法律責任。

五、其他重要注意事項

1.用戶應遵守本作業基準申請憑證相關之規定，並確保所提供申請資料之正確性。

2.信賴憑證者在合理信賴中華電信憑證管理中心所簽發之憑證時，應確認欲信賴憑證之正確性、有效性與用途限制。

3. 本公司將委託公正之第三人，就中華電信憑證管理中心的運作進行稽核。

1.總則

中華電信公開金鑰基礎建設(eCommerce Public Key Infrastructure, ePKI，簡稱本基礎建設)是依照 ITU-T X.509 標準建置的階層式(Hierarchy) 公開金鑰基礎建設，包括公開金鑰基礎建設的信賴起源(Trust Anchor)－中華電信憑證總管理中心(ePKI Root Certification Authority, eCA，以下簡稱 eCA)及本公司所設立的下屬憑證機構(Subordinate CA)所組成，由本公司負責建置與維運。

中華電信憑證管理中心(以下簡稱憑證中心)是本基礎建設的第一層下屬憑證機構(Level 1 Subordinate CA)，在本基礎建設中負責簽發及管理中華電信股份有限公司(以下簡稱本公司)之員工、外包人員與伺服器應用軟體等三種憑證。

本文件的名稱中華電信憑證管理中心憑證實務作業基準(Chunghwa Telecom Certification Authority Certification Practice Statement; 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 Public Key Infrastructure，以下簡稱憑證政策)所訂定。

1.1 本作業基準適用範圍

本作業基準所載明之實務作業規範適用於憑證中心(Certificate Authority)、註冊中心(Registration Authority)、用戶(Subscribers)、信賴憑證者(Relying Parties)及儲存庫(Repository)等。

1.2 版本識別

本作業基準為第 1.0 版，版本發行日期為中華民國九十四年九月二十三日。本作業基準之最新版本可在以下網頁取得：

http://ca.cht.com.tw/

http://epki.com.tw

中華電信憑證管理中心之運作遵照憑證政策保證等級第三級之規定，其物件識別碼名稱為 id-tw-epki-certpolicy-class3Assurance，物件識別碼值為{id-tw-epki-certpolicy 3}。

1.3 主要成員及憑證適用範圍

中華電信憑證管理中心之相關成員包括：

(1) 憑證中心

(2) 註冊中心

(3) 儲存庫

(4) 用戶及信賴憑證者

1.3.1 憑證中心

憑證中心負責簽發憑證及憑證廢止清冊，由本公司負責建置及營運。

1.3.2 註冊中心

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，由多個註冊窗口（RA Counter）組成。註冊窗口設於本公司授權之單位，並設有憑證註冊審驗人員（RA Officer，RAO），負責受理憑證之相關申辦作業。

註冊中心設置註冊中心伺服器（RA Server），負責驗證憑證註冊審驗人員的身分及管理註冊窗口，註冊中心伺服器與註冊窗口伺服器間的通訊，使用安全插座層通訊協定（Secure Socket Layer）或其他相同或更高級之資料加密傳送方式處理。

1.3.3 儲存庫

儲存庫是負責公告及儲存由憑證中心所簽發之憑證及憑證廢止清冊，提供用戶及信賴憑證者查詢服務。儲存庫的網址為：http://ca.cht.com.tw/。

1.3.4 用戶及信賴憑證者

1.3.4.1 用戶

用戶係指記載於憑證中心所簽發憑證的憑證主體名稱(Certificate Subject Name)的個體，中華電信憑證管理中心用戶包含本公司之員工、外包人員與伺服器應用軟體。

員工及外包人員憑證可使用之符記包含 IC 卡或其他硬體密碼模

組，每個符記皆至少存有兩對金鑰對，一為簽章用金鑰對，另一為加解密用金鑰對，因此每個符記同時包含簽章用及加解密用兩種憑證。

伺服器應用軟體憑證，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，申請憑證。如符記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。

1.3.4.2 信賴憑證者

信賴憑證者係指相信用戶主體名稱與公開金鑰間連結關係之自然人或法人。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，以驗證用戶所使用的憑證的有效性。並且可以使用憑證進行以下三個工作：

(1)驗證具有數位簽章的電子文件之完整性。

(2)驗證文件產生者的身分。

(3)與用戶間建立安全之通訊管道。

1.3.5 適用範圍

1.3.5.1 憑證適用範圍

憑證中心係簽發憑證政策所定義保證等級第三級憑證，憑證適用於本公司企業網路相關應用所需的身分認證及資料加密。

伺服器應用軟體憑證可應用於安全插座層(Secure Socket Layer,

SSL)通訊協定及專屬開發的伺服器應用軟體。

憑證保證等級之適用範圍說明如下:

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。

使用及信賴中華電信憑證管理中心所提供的認證服務前，用戶及信賴憑證者都應詳細閱讀、遵守本作業基準，並且應注意本作業基準的更新。

1.3.5.2 憑證限制事項

用戶在使用私密金鑰時，應慎選安全的電腦環境及可信賴的應用系統，以避免私密金鑰被惡意軟硬體盜取或誤用而引發權益受損。

信賴憑證者在使用憑證中心所簽發之憑證前，應確認憑證之類別、保證等級及金鑰用途等是否符合應用需求。

信賴憑證者應依照 X.509 規範處理憑證中的關鍵性（Critical）與非關鍵性（Non-Critical）憑證擴充欄位(Extensions)。

1.3.5.3 憑證禁止事項

憑證中心所簽發的憑證禁止使用於下列的情況：

(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

對本作業基準有任何疑慮時，可直接與中華電信憑證管理中心聯絡。

聯絡電話:0800080412。

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管理中心。

電子郵件信箱：service@epki.com.tw。

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

2. 一般條款

2.1 職責與義務

本節說明憑證中心、註冊中心、用戶及信賴憑證者之權利義務及發生損害時之賠償責任歸屬。

2.1.1 憑證中心職責

(1) 依據本作業基準運作。

(2) 簽發及公布憑證服務。

(3) 廢止憑證。

(4) 簽發及公佈憑證廢止清冊。

(5) 執行憑證中心與註冊中心相關人員之識別及鑑別程序。

(6) 安全產製憑證中心及註冊中心之私密金鑰。

(7) 保護憑證中心之私密金鑰。

(8) 支援註冊中心進行憑證註冊相關作業。

2.1.2 註冊中心職責

(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給憑證中心。

(4)告知用戶及信賴憑證者有關憑證中心及註冊中心之義務與責任。

(5)告知用戶及信賴憑證者，有關接受或使用憑證中心所簽發

之憑證，必須遵守本作業基準之相關規定。

(6)執行憑證註冊審驗人員之識別與鑑別程序。

(7)保護註冊中心之私密金鑰。

(8)於 IC 卡內部安全產製用戶之金鑰對。

2.1.3 用戶義務

(1) 應遵守本作業基準之規定，並確保所提供申請資料之正確性。

(2) 如需自行產製金鑰時，應慎選安全的電腦環境安全產製私密金鑰。

(3) 在憑證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。

(4) 用戶在接受憑證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，如憑證內容資訊有誤，用戶應主動通知憑證中心。

(5) 應妥善保管及使用私密金鑰，並遵守對於金鑰及憑證之使用限制。

(6) 如須暫停使用、恢復使用、廢止憑證，應依照 4.4 節規定辦理，如發生私密金鑰資料外洩或遺失等情形，必須廢止憑證時，應立即通知中華電信憑證管理中心，但用戶仍應承擔異動前所有使用該憑證之法律責任。

(7) 應慎選安全的電腦環境及可信賴的應用系統，如因電腦環境或應用系統本身因素導致信賴憑證者權益受損時，應自行承擔責任。

2.1.4 信賴憑證者義務

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

(2) 在使用憑證中心簽發之憑證時，應先檢驗憑證之保證等級以確保權益。

(3) 在使用憑證中心簽發之憑證時，應先檢驗憑證廢止清冊，以確認該憑證是否有效。

(4) 在使用憑證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。

(5) 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。

(6) 信賴憑證者接受使用憑證中心簽發之憑證時，即視為已了解並同意有關憑證中心法律責任之條款，並依照 1.3.5 節規定範圍信賴該憑證。

2.1.5 儲存庫職責

(1) 依 2.6 節規定定期公佈簽發之憑證、憑證廢止清冊及其他憑證相關資訊。

(2) 公佈本作業基準的最新資訊。

(3) 儲存庫之存取控制依照 2.6.3 節之規定辦理。

(4) 維持儲存庫資訊之可接取狀態及可用性。

2.2 法律責任

2.2.1 憑證中心責任

2.2.1.1 責任範圍

憑證中心依照本作業基準第四章規定之程序簽發憑證、簽發並公佈憑證廢止清冊及維持儲存庫運作。

2.2.1.2 賠償責任

憑證中心處理用戶憑證簽發作業，若故意或過失未遵照本作業基準及相關作業規定，致用戶或信賴憑證者受有損害時，依本公司相關人事獎懲規定，對相關疏失人員進行懲處，對於相關之損害賠償，依民法相關規定辦理。

2.2.1.3 責任免除

用戶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損害，如該損害之造成不可歸責於憑證中心時，應由該用戶或信賴憑證者自負損害賠償之責。

2.2.1.4 除外條款

如因不可抗力及其他非可歸責於憑證中心之事由，所導致之損害事件，憑證中心不負任何法律責任。

如因憑證中心之系統維護、轉換及擴充等需要，得事先公告於儲存庫，暫停部分憑證服務，用戶或信賴憑證者不得以此作為要求憑證中心損害賠償之理由。

如因 4.4.1 節廢止憑證之事由，用戶應依照 4.4.3 節憑證廢止程序

提出廢止憑證申請，用戶提出憑證廢止申請後，憑證中心將於一個工作天內完成廢止憑證作業。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 註冊中心責任

2.2.2.1 責任範圍

註冊中心應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，註冊中心因執行註冊工作所引發之法律責任由註冊中心負責。

憑證中心所核發之憑證僅對憑證主體身分做確認，唯其確認程度係當時註冊中心審驗人員之審驗結果，不對用戶之金融信用、財務能力、技術能力、可靠性等作任何擔保。

2.2.2.2 賠償責任

註冊中心處理用戶憑證簽發作業，若故意或過失未遵照本作業基準及相關作業規定，致用戶或信賴憑證者受有損害時，依本公司相關人事獎懲規定，對相關疏失人員進行懲處，對於相關之損害賠償，依民法相關規定辦理。

2.2.2.3 責任免除

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，如該損害之造成不可歸責於註冊中心時，應由用戶自負損害賠償之責，又用戶或信賴憑證者未依照 1.3.5 節規定之適用範圍

使用憑證所引發之損害，如該損害之造成不可歸責於註冊中心時，應由該用戶或信賴憑證者自負損害賠償之責。

2.2.2.4 除外條款

如因不可抗力事件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。

2.3 財務責任

2.3.1 財務保證

中華電信憑證管理中心由本公司營運，其財務責任由本公司負責。

2.3.2 財務保險

中華電信憑證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。

2.3.3 財務稽核

中華電信憑證管理中心之財務，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四個月內公告，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。並每半營業年度終了後二個月內，公告並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；於每營業年度第一季及第三季終了後一個月內，公告並申報經會計師核閱之財務報告。

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，悉依據我國相關法律之規定。

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八章所述。

2.4.3 爭議解決

爭議之雙方應本誠信原則協商解決之，若無法協商，需經由訴訟來解決爭議時，雙方合意以台北地方法院為第一審法院。

本公司員工用戶或本公司所屬註冊中心與憑證中心如有爭議時，依本公司組織管理體制，由共同上級主管調處解決。

本公司外包人員用戶與憑證中心如有爭議時，應依本公司與外包公司所訂之合約與本公司協商解決。

2.5 費用

2.5.1 憑證簽發或展期費用

不收費。

2.5.2 憑證查詢費用

不收費。

2.5.3 憑證廢止或狀態查詢費用

不收費。

2.5.4 退費規定

不收費，因此無請求退費之程序。

2.6 公佈及儲存庫

2.6.1 中華電信憑證管理中心資訊公佈內容

(1) 本作業基準。

(2) 憑證廢止清冊。

(3) 憑證中心本身之憑證，到該憑證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) 中華電信憑證管理中心相關最新訊息。

2.6.2 公佈方法及頻率

(1) 本作業基準於主管機關核准後公佈，本作業基準修訂依照第八章規定公佈於儲存庫。

(2) 憑證中心每天簽發一次憑證廢止清冊，公佈於儲存庫。

(3) 憑證中心本身之憑證，於簽發時公佈於儲存庫。

(4)簽發之憑證，於簽發時公佈於儲存庫。

2.6.3 存取控制

憑證中心主機建置於防火牆內部，儲存庫透過內部的防火牆連線至憑證中心憑證管理資料庫，以擷取憑證資訊或下載憑證。只允許經過授權的憑證中心相關人員管理儲存庫主機。

有關 2.6.1 節公佈的資訊，主要提供用戶與信賴憑證者使用瀏覽器查詢之用，僅可透過本公司企業內部網路進行存取，以維持其可接取狀態及可用性。

2.6.4 儲存庫

儲存庫由中華電信憑證管理中心負責管理，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://ca.cht.com.tw/

2.7 稽核方法

2.7.1 稽核頻率

中華電信憑證管理中心接受一年一次的外部稽核與不定期的內部稽核，以確認中華電信憑證管理中心的運作確實遵循本作業基準所訂的安全規定與程序。

2.7.2 稽核人員身分及資格

本公司將委外辦理中華電信憑證管理中心之外部稽核作業，由熟

悉憑證中心運作之稽核業者，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稽核或資訊安全管理稽核相關經驗，中華電信憑證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，就中華電信憑證管理中心的運作進行稽核。

2.7.4 稽核範圍

稽核範圍如下所述：

(1)憑證中心是否遵照本作業基準運作，包括實體環境、人員程序控制、金鑰控管、憑證生命週期控管、硬體密碼模組控管等管理及技術稽核。

(2)確認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

如稽核人員發現中華電信憑證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)將不符合情形通知中華電信憑證管理中心。

(3)對於不符合規定之項目，中華電信憑證管理中心將於三十

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

中華電信憑證管理中心將公佈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

以下由憑證中心產生、接收或保管之資料，均視為機密性資訊：

(1) 用於憑證中心營運的私密金鑰及通行碼。

(2) 憑證中心金鑰分持的保管資料。

(3) 用戶申請資料，未經用戶同意或符合法令規定，不得公開或提供第三人使用。

(4) 憑證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。

(6) 列為機密等級的營運相關文件。

憑證中心之人員對於保密資訊均訂有保密同意書嚴守秘密。

2.8.2 非機密之資訊種類

(1) 儲存庫公佈之簽發憑證、已廢止憑證及憑證廢止清冊不視為機密資訊。

(2) 識別資訊或記載於憑證的資訊，除特別約定外，不視為機密資訊。

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佈於儲存庫。

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；惟中華電信憑證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

用戶得查詢 2.8.1 節第(3)款之申請資料；並依照本公司相關規定提出申請。

2.8.6 其他資訊釋出之情況

中華電信憑證管理中心於操作中取得用戶之個人資料，將遵守相關法令規範，不對外揭露以確保用戶個人隱私。但法令另有規定時，不在此限。

2.8.7 隱私權保護

中華電信憑證管理中心依照電腦處理個人資料保護法處理用戶申請資料。

2.9 智慧財產權

下列項目為本公司之智慧財產:

(1)憑證中心及註冊中心的金鑰對及金鑰分持。

(2)因執行憑證管理作業而撰寫的相關文件或研發之系統。

(3)憑證中心所簽發的憑證及憑證廢止清冊。

(4)本作業基準。

本作業基準可由儲存庫自由下載，或依著作權法相關規定重製或散布，但必須保證是完整複製，並註明著作權為本公司所擁有。重製或散佈本作業基準者，不得向他人收取費用，對於不當使用或散佈本作業基準之侵害，本公司將依法予以追訴。

3.識別和鑑別

3.1 初始註冊

3.1.1 命名種類

憑證中心所簽發憑證之憑證主體名稱採用X.500唯一識別名稱(Distinguished Name, DN)。

3.1.2 命名須有意義

憑證中心所簽發的憑證，其憑證主體名稱(Subject)符合本公司對該主體命名之相關規定，以代表該主體的名稱。

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，憑證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

名稱形式的解釋規則依據 ITU-T X.520 名稱屬性定義。

3.1.4 命名獨特性

憑證中心的X.500唯一識別名稱為：

C=TW，O=中華電信股份有限公司，OU=中華電信憑證管理中心。

為使憑證中心所簽發之憑證的憑證主體名稱具備獨特性，憑證中心採用以下名稱格式：

1. 員工憑證

C=TW

O=中華電信股份有限公司

CN=員工姓名

serialNumber=識別代號

2.外包人員憑證

C=TW

O=中華電信股份有限公司

CN=外包人員姓名

serialNumber=識別代號

3.伺服器應用軟體憑證

C=TW

O=中華電信股份有限公司

OU=單位名稱(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

用戶的名稱相同，會以在唯一識別名稱中的序號(serialNumber)加以區別，以使用戶的名稱可以保持唯一性。但如發生用戶名稱所有權爭議時，由本公司資訊處協調解決。

3.1.6 商標之辨識、鑑別及角色

當憑證主體名稱可能包含商標時，則其命名必須符合我國商標相

關法規。

3.1.7 證明擁有私密金鑰之方式

(1)員工及外包人員憑證

用戶申請憑證時，由註冊窗口在 IC 卡內部自行產製金鑰對，簽發憑證時註冊窗口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。

(2)伺服器應用軟體憑證

由用戶自行產製金鑰對，然後產生 PKCS#10 憑證申請檔並以私密金鑰加以簽章，並於申請憑證時將該憑證申請檔交給註冊中心，註冊中心將使用該用戶的公開金鑰驗證該憑證申請檔的簽章，以證明用戶擁有相對應的私密金鑰。

3.1.8 組織身分鑑別之程序

用戶申請憑證時，必須將憑證申請書以發函方式進行申請，註冊中心將確認該單位確實存在，並驗證函之真確性。

3.1.9 個人身分之鑑別

由用戶提供申請資料，包括姓名、身分證字號、出生日期、電話、Email等。憑證註冊審驗人員將核對用戶資料之正確性並與本公司資料庫登記資料進行比對，以確認該用戶之身分。

3.1.10 硬體裝置或伺服軟體鑑別之程序

電腦及通訊設備(如路由器、防火牆等)或伺服軟體(如Web

Server)，由硬體裝置或伺服器應用軟體之所有人或經授權之使用人提出憑證申請；對於組織或個人的身分鑑別方式依照3.1.8或3.1.9節規定辦理。

3.2 憑證之金鑰更換及展期

3.2.1 憑證更換金鑰

當用戶私密金鑰使用期限到期需要更換金鑰時，可進行憑證更換金鑰作業，註冊中心會自動為用戶產製新的金鑰，並向憑證中心重新申請憑證，依照 3.1 節規定對個人進行識別及鑑別。憑證中心不提供伺服器應用軟體憑證之金鑰更換服務，需重新申請。

3.2.2 憑證展期

用戶申請憑證展期時，使用其私密金鑰對憑證申請檔加以簽章，並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，以識別用戶之身分。

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，應向憑證中心重新申請憑證，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 3.1.8、3.1.9、3.1.10 節規定相同。

3.5 憑證暫時停用與恢復使用

憑證暫時停用或恢復使用之鑑別程序如下:

(1)申請人連線至儲存庫提出申請時,註冊中心將以用戶輸入之通行碼鑑別其身分。

(2)申請人填寫申請書,將申請書送交註冊窗口辦理,憑證註冊審驗人員將核對用戶資料之正確性。

4.營運規範

4.1 申請憑證之程序

4.1.1 員工

申請憑證時，由員工提供正確且完整之資料，註冊窗口在收到憑證申請資料後，將依本作業基準 3.1.9 節規定，進行身分鑑別程序，以作為判定是否同意簽發憑證之依據。

4.1.2 外包人員

申請憑證時，由外包人員提供正確且完整之資料，註冊窗口在收到憑證申請資料後，將依本作業基準 3.1.9 節規定，進行身分鑑別程序，以作為判定是否同意簽發憑證之依據。

4.1.3 硬體裝置或伺服器應用軟體憑證申請程序

(1)由硬體裝置或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。

(2)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。

(3)憑證申請人連線至憑證中心網站(http:// ca.cht.com.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。

(4)將憑證申請書函送註冊窗口辦理。

申請憑證所需之資料含必要資料及選擇性資料，只有憑證格式剖

繪中所列的資料才會記錄於憑證中。憑證申請者申請憑證時之申請資料，註冊中心及憑證中心依本作業基準之規定妥善保管。

4.2 簽發憑證之程序

簽發審核步驟如下：

(1) 註冊中心審驗人員確認申請人填寫資料正確。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。

(2) 憑證中心接獲註冊中心送來之憑證申請資料時，先查驗相關註冊中心之授權狀態，確認其被授權之保證等級與範圍，再依據註冊中心所送之憑證申請資料簽發憑證。

(3) 若註冊中心被授權之保證等級與範圍與憑證申請不符時，憑證中心將回傳相關錯誤信息給註冊中心，並拒絕後續相關作業；若註冊中心有任何疑問，應主動聯絡憑證中心，確實瞭解問題之所在。

(4) 為確保憑證中心及註冊中心間傳輸資料之安全、完整及不可否認性，透過網路傳輸之憑證申請資料，係經數位簽章及安全插座層通訊協定(SSL)方式加密傳送。

(5) 憑證中心保有拒絕簽發憑證給任何個體之權利，憑證中心拒絕簽發憑證對憑證申請者不負任何損害賠償責任。

4.3 接受憑證之程序

當完成憑證簽發後，申請者可使用書面或線上方式進行憑證接受。

以書面方式進行接受憑證時，申請者應檢視相關確認書所列印有關憑證的內容，如確認憑證內容無誤，就應接受所簽發的憑證，並在相關確認書簽名表示已接受所簽發的憑證。

以線上方式進行接受憑證時，憑證系統將使用網路傳遞相關憑證內容給申請者，申請者確認憑證內容無誤，依照操作說明接受憑證。

如申請者發現憑證內容不正確，則應拒絕接受憑證，並向註冊窗口重新申請憑證。

4.4 憑證暫時停用及廢止

本節主要描述在何種情形下憑證得（或必須）予以暫停使用或廢止，並說明憑證暫停使用、廢止等程序。

4.4.1 廢止憑證之事由

遇有任何下列情況時(包括但不限於)，憑證用戶應向註冊中心提出要求廢止憑證之申請：

(1) 私密金鑰遺失、遭竊、改變及未經授權之揭露或其他破壞或盜用；

(2) 憑證所載資訊發生足以影響對用戶信賴之重大改變；

(3) 憑證不再需要使用；

另外，憑證中心得就下列情形逕行廢止憑證，毋須事先通知用用戶。

(1) 確知憑證所載之部分事項不真實；

(2) 確知憑證用戶之簽章私鑰遭冒用、偽造或破解；

(3)確知憑證中心之私鑰或資訊系統遭冒用、偽造或破解，致影響憑證之可信賴性；

(4)確知該憑證未依本作業基準之規定程序簽發時；

(5)用戶已經違反或無法擔負本作業基準或任何其他合約及相關法令之規定或責任時；

(6)依司法或檢調機關之通知或依相關法律之規定；

4.4.2 憑證廢止之申請者

(1)憑證用戶單位主管。

(2)依據司法機關之通知。

(3)憑證用戶。

4.4.3 憑證廢止之程序

(1)憑證廢止申請人填寫憑證廢止申請書。

(2)將憑證廢止申請書函送註冊窗口辦理。

(3)註冊窗口在收到憑證廢止申請書後，由憑證註冊審驗人員檢查憑證廢止申請書的真偽。

(4)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。

(5)憑證中心完成憑證廢止作業。

若司法機關依正式公文通知欲廢止特定的憑證，則中華電信憑證

管理中心將於審視通知公文後，將憑證廢止。

如以上之廢止申請審核不通過時，憑證中心將拒絕廢止憑證。

4.4.4 憑證廢止申請之處理時間

註冊窗口受理憑證廢止申請後，應於一個工作天內完成憑證廢止審核。審核通過後，憑證中心將於一個工作天內完成憑證廢止作業。

4.4.5 暫時停用憑證之事由

用戶在以下兩種情形得申請憑證之暫時停用：

(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。

憑證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)依業務安全需要取消授權。

(2)依據司法機關之通知。

4.4.6 暫時停用憑證之申請者

(1)憑證用戶單位主管。

(2)依據司法機關之通知。

(3)憑證用戶。

4.4.7 暫時停用憑證之程序

分為兩種程序：

(1) 線上申請：由申請人連線至儲存庫申請暫時停用憑證，上傳至註冊中心。

(2) 填表申請：申請人填寫憑證暫時停用憑證申請書，將申請書送交註冊窗口辦理，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，憑證中心將立即停用該憑證。以上之暫時停用申請審核不通過時，憑證中心將拒絕暫時停用憑證。

4.4.8 暫時停用憑證之處理期間及停用期間

註冊窗口受理暫時停用申請後，應於一個工作天內完成憑證暫時停用審核。審核通過後，憑證中心將於一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，憑證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)填表申請：申請人填寫憑證恢復使用憑證申請書，將申請書送交註冊窗口辦理，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 憑證廢止清冊簽發頻率

憑證中心之憑證廢止清冊簽發頻率為每天一次。於更新後公佈於儲存庫，提供公眾檢核憑證狀態。

4.4.11 憑證廢止清冊查驗規定

信賴憑證者在使用憑證中心公佈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佈資訊須具備之要件，詳見於 2.6.3 節之說明。

4.4.12 線上憑證狀態查詢服務

信賴憑證者使用線上憑證狀態查詢服務時，須檢驗相關查詢結果

資料之數位簽章，確認資料來源之正確性及完整性。

4.4.13 線上憑證狀態查詢規定

如信賴憑證者無法依照 4.4.11 節之規定查詢憑證廢止清冊，則必須使用 4.4.12 節之線上憑證狀態查詢服務，檢驗所使用的憑證是否有效。

4.4.14 其他形式廢止公告

目前沒有提供其他形式的廢止公告。

4.4.15 其他形式廢止公告之檢查規定

目前沒有提供其他形式的廢止公告。

4.4.16 金鑰被破解時之其他特殊需求

沒有其他不同於 4.4.1、4.4.2 及 4.4.3 節的規定。

4.5 安全稽核程序

所有憑證中心安全相關的事件，均做安全稽核紀錄(audit log)。安全稽核紀錄包含系統自動產生、工作紀錄本、紙張等其他實體機制。所有安全稽核紀錄都被保存，且可供稽核時取得。可稽核事件之安全稽核紀錄遵循 4.6.2.所述之歸檔保留期間的維護方式進行。

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份鑑別嘗試而被鎖住的。
- 管理者改變系統的身分鑑別機制，例如從通行碼改為生物特徵值。

(3) 金鑰產製

- 憑證中心產製金鑰時(但是並不強制規定在單次或只限一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，對保存在憑證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) 憑證中心組態設定

- 憑證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。

- 安裝憑證中心系統。

- 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。
- 嘗試登入憑證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。
- 憑證中心之內部資料備份。
- 憑證中心之內部資料回復。
- 傳送任何資訊到儲存庫公佈。
- 存取憑證中心之內部資料庫。
- 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。
- 憑證中心之金鑰更換。

(15) 憑證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

- 得知或懷疑違反實體安全規定。
- 存取憑證中心之伺服器。
- 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

憑證中心每兩個月檢視稽核紀錄一次，解釋重大事件。檢視的工作包括檢視所有的紀錄項目，最後完整地檢查任何警示或異常。

4.5.3 稽核紀錄檔保留期限

稽核資料現場保留兩個月，依 4.5.4 節、4.5.5 節及 4.5.6 節所描述做為資料保留的管理機制。

當稽核資料的保留期限到期時，由稽核員移除資料，其他角色的人員不可移除。

4.5.4 稽核紀錄檔之保護

目前和已歸檔之自動事件日誌以安全之方式保存，以雜湊演算法運算每一項稽核紀錄檔並執行數位簽章，只有授權者才可調閱。

4.5.5 稽核紀錄檔備份程序

電子式稽核紀錄至少每月備份一次。

(1) 憑證中心週期性的將事件日誌歸檔。

(2) 憑證中心將事件日誌檔案存放於安全保險場所。

4.5.6 安全稽核系統

所有中華電信憑證管理中心安全相關的事件，均做安全稽核紀錄(audit log)。安全稽核紀錄包含系統自動產生、工作紀錄本、紙張等

其他實體機制。所有安全稽核紀錄都被保存，且可供稽核時取得。

4.5.7 引起事件者之公告

當事件發生而被稽核系統記錄時，稽核系統並不需要告知引起該事件的個體。

4.5.8 弱點評估

每年至少一次對憑證中心之電腦系統進行弱點掃描，並進行相關的補強措施。

4.6 紀錄歸檔

中華電信憑證管理中心採取可靠的機制，以電腦資料或書面資料精確完整地保存與憑證作業相關之紀錄，包括：

(1) 憑證中心本身金鑰對產製、儲存、存取、備援及更換等之重要追蹤紀錄。

(2) 憑證申請、簽發、廢止等之重要追蹤紀錄。

此等紀錄除提供追蹤或稽核外，必要時得作為解決爭議之佐證資料，為遵守前述規定，註冊中心必要時，得要求申請者或其代理人提出相關證明文件。

4.6.1 紀錄事件之類型

中華電信憑證管理中心記錄的歸檔資料有：

(1) 憑證中心的被稽核驗證(accreditation)資料(如適用)

(2) 本作業基準

(3) 重要的契約

(4) 系統與設備組態設定

(5) 系統或組態設定的修改與更新的內容

(6) 憑證申請的資料

(7) 廢止申請的資料

(8) 如 3.1.9 節所訂定的用戶身份識別資料

(9) 所有已簽發或公告的憑證

(10) 憑證中心金鑰更換的紀錄

(11) 所有被簽發或公告的憑證廢止清冊

(12) 所有的稽核紀錄

(13) 用來驗證及佐證歸檔內容的其它資料或應用程式

(14) 稽核者所要求的文件

(15) 憑證接受的確認紀錄。

(16) 符記啟用的紀錄。

4.6.2 歸檔之保留期限

中華電信憑證管理中心保留歸檔資料的時間為 10 年。用來處理歸檔資料的應用程式需維護管理 10 年。

4.6.3 歸檔之保護

(1) 任何使用者不被允許新增、修改或刪除歸檔的資料。

(2) 經過中華電信憑證管理中心授權程序可以將歸檔資料移到另一個儲存媒體上。

(3) 歸檔的資料存放於安全保險場所。

4.6.4 歸檔備份程序

憑證中心之電子式紀錄將依照備份程序，以複製方式定期備份至儲存媒體存放，紙本紀錄將由憑證中心所授權之人員定期整理歸檔。

4.6.5 時戳紀錄之要求

憑證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。歸檔之電子式紀錄(例如憑證、憑證廢止清冊及稽核紀錄等)每一紀錄之時戳資訊包含日期與時間資訊，並採用系統經校時後的標準時間，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。

4.6.6 取得及驗證歸檔資料之程序

在獲取憑證中心歸檔資訊時，相關人員必須得到正式的授權，才可以取出已歸檔的資訊。

在驗證歸檔資訊時，由稽核員進行驗證的程序，在書面文件者必須驗證文件簽署者及日期等的真偽。電子檔則驗證歸檔資料的數位簽章。

4.7 金鑰更換

憑證中心之私密金鑰依照 6.3.2 節規定定期更換，憑證中心在其金鑰生命週期有效期限結束前二個月，更換用來簽發憑證的金鑰對，

更換金鑰對後，將向中華電信憑證總管理中心申請新的憑證，以新私密金鑰簽發用戶之憑證及簽發憑證中心的憑證廢止清冊，並重簽所有已發行之用戶憑證，將其儲存在儲存庫中，供用戶下載。

憑證用戶之私密金鑰必須依照 6.3.2 有關憑證用戶私密金鑰使用期限之規定定期更換。用戶如其憑證沒有被廢止，用戶最遲必須在憑證到期前一個月內更換其金鑰對，註冊中心會自動為用戶產製新的金鑰，並向憑證中心重新申請憑證。

4.8 金鑰遭破解或災變時之復原程序

4.8.1 中華電信憑證管理中心電腦資源、軟體或資料遭破壞之復原程序

中華電信憑證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。

如憑證中心的電腦設備遭破壞或無法運作，但憑證中心的簽章金鑰並未被損毀，則優先回復憑證中心儲存庫之運作，並迅速重建憑證簽發及管理的能力。

4.8.2 中華電信憑證管理中心簽章金鑰憑證被廢止之復原程序

如憑證中心之簽章金鑰憑證被廢止，憑證中心將依照 4.7 節之程序產生新的金鑰對，新的憑證將公布於儲存庫，提供用戶及信賴憑證者下載。

4.8.3 中華電信憑證管理中心簽章金鑰遭破解之復原程序

如憑證中心簽章金鑰遭破解，採取以下復原程序：

(1) 公告於儲存庫，通知用戶及信賴憑證者

(2) 廢止憑證中心簽章金鑰憑證。

(3) 依照 4.7 節之程序產生新的金鑰對，將新的憑證公告於儲存庫，供用戶及信賴憑證者下載。

4.8.4 中華電信憑證管理中心安全設施之災後復原工作

中華電信憑證管理中心訂定災後復原之程序，同時每年進行演練，當發生災害時，將由緊急應變小組啟動災後復原程序，優先回復憑證中心儲存庫之運作，並迅速重建憑證簽發及管理的能力。

4.9 中華電信憑證管理中心之終止服務

中華電信憑證管理中心終止服務時，應依我國電子簽章法相關規定進行憑證機構終止服務的程序。為確保用戶與信賴憑證者之權益，憑證中心應遵守以下事項：

(1) 預定終止服務三十日前，通知主管機關（經濟部）與用戶；

(2) 終止服務時將採如下措施：

- 對終止當時仍具效力之憑證，安排其他憑證機構承接此業務。並將終止服務及由其他憑證機構承接其業務之事實公告於儲存庫及通知仍具效力之憑證用戶。但無法通知者，不在此限。

- 將所有營業期間之紀錄檔案，移交給承接此業務之其

他憑證機構。

■ 本公司於必要時，得公告廢止當時仍具效力之憑證。

5.實體、程序及人員安全的控管

5.1 實體控管

5.1.1 實體所在及結構

憑證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憑證中心之相關設備。

5.1.2 實體存取

憑證中心建置採適當之措施管制連接提供憑證服務的硬體、軟體和硬體密碼模組。

憑證中心機房總共有四層門禁，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器(Finger-printed)進出管制系統，指紋辨識器採用三度空間指紋取樣，可以判別被辨識物的紋深、色澤以及是否為活體，執行門禁認證。

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憑證中心系統的惡意軟體。

非憑證中心人員進出機房，需填寫進出紀錄，並由憑證中心相關人員全程陪同。

憑證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 電源和空調

憑證中心的電力系統，除了市電外，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）並及提供市電及發電機的電源自動切換。提供至少 6 小時以上備用電力供儲存庫備援資料。

憑證中心裝有恆溫恆濕的空調系統，用以控制環境的溫度及濕度，以確保機房具最佳運作環境。

5.1.4 水災防範及保護

憑證中心機房設置在基地墊高建築物的第 3 樓層以上，該建築物具備防水閘門和抽水機，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

憑證中心具備有自動偵測火災預警功能，系統自動啟動滅火設

備，並設置手動開關於各主要出入口處，以供現場人員於緊急情況時以手動方式來操作。

5.1.6 媒體儲存

記錄稽核、歸檔和備援資料的儲存媒體除了儲存一份在 5.1.1 節所述的場所，另將複製一份在安全場所。

5.1.7 廢料處理

2.8.1 節所記載的文件資料，不需要使用時，都要經過碎紙機處裡。任何磁帶、硬碟、磁碟、磁光碟（MO）和任何形式的記憶體，在報廢前，都要經過格式化程序清除所儲存的資料。光碟將被實體銷毀。

5.1.8 異地備援

異地備援的地點與憑證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。

5.2 程序控制

憑證中心經由作業程序控管(procedural controls)，以規定可以操作憑證系統的各個可信賴角色(trusted role)，每個工作的人員需求數，和每個角色的識別與鑑別(identification and authentication)，以確保系統的作業程序安全有合理的保證度。

5.2.1 信賴角色

憑證中心必須確保從事關鍵性功能的責任，能做適當的區隔分派，以防止某人惡意使用系統而不被察覺。每個使用者必須依照其被指定之任務執行該任務所需之系統存取。

憑證中心指派五個不同的 PKI 人員角色，分別為管理員、簽發員、稽核員、維運員和實體安全控管員，以抵擋可能的內部攻擊。一個角色的工作可以多個人來擔任，但是每個群組只設有一個主管(Chief Role)來領導該群組的工作，而五種角色的工作責任區分如下：

管理員主要負責：

- 安裝、設定和維護憑證系統。
- 建立和維護系統之使用者帳號。
- 產製和備份憑證中心之金鑰。

簽發員主要負責：

- 啟動/停止憑證簽發服務。
- 啟動/停止憑證廢止服務。

稽核員主要負責：

- 對稽核紀錄的查驗、維護和歸檔。
- 執行或監督內部的稽核，以確認憑證中心維運是否遵照本作業基準的規定。

維運員主要負責：

- 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。
- 除憑證管理系統以外軟硬體的更新。
- 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。

實體安全控管員主要負責：

- 系統的實體安全控管(機房的門禁管理、防火、防水、空調系統等) 。

5.2.2 角色分派

憑證中心角色分依照 5.2.1 節定義的五種信賴角色，對人員及角色分配必須符合以下規定：

- 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。
- 實體安全控管員不得兼任其他四種角色工作。
- 無論在任何條件下，任何一個角色，都不可以執行自我稽核功能，不允許自己稽核自己。

5.2.3 每個任務所需之人數

根據各個工作角色的作業安全需求，訂定各個工作角色所需

的人數如下：

■ 管理員(Administrator)

共需要有至少 3 位合格的人員來擔任。

■ 簽發員(Officer)

共需要有至少 2 位合格的人員來擔任。

■ 稽核員(Auditor)

共需要有 2 位合格的人員來擔任。

■ 維運員(Operator)

需要有 2 位合格的人員來擔任。

■ 實體安全控管員（Controller）

需要有 2 位合格的人員來擔任。

每個任務項目所需要的人員數在以下表格所述：

任務項目	管理員	簽發員	稽核員	維運員	實體安全控管員
安裝、設定和維護憑證中心系統	2				1
建立和維護系統之使用者帳號	2				1
產製和備份憑證中心之金鑰	2		1		1
啟動/停止憑證簽發服		2			1

任務項目	管理員	簽發員	稽核員	維運員	實體安全控管員
務					
啟動/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
除憑證中心憑證管理系統以外軟硬體的更新				1	1
網路及網站的維護				1	1

5.2.4 識別及鑑別每一個角色

使用 IC 卡識別和鑑別管理員、簽發員、稽核員和維運員角色，利用中央門禁系統設定權限識別和鑑別實體安全控管員角色。

憑證中心主機的作業系統帳號管理，使用登入者帳號、密碼和群組，提供識別和鑑別管理員、簽發員、稽核員和維運員角色。

5.3 人員控管

5.3.1 身家背景、資格、經驗及安全需求

1.人員晉用之安全評估

工作人員的甄選及晉用包含下列項目：

(1)個人性格之評估。

(2)申請者經歷之評估。

(3)學術及專業能力及資格之評估。

(4)人員身分之確認。

(5)人員操守之評估。

2.人員考核管理

憑證中心對於執行憑證業務之員工,在初任時予以資格審查,以確認其具可信度及工作能力,就任後予以適當之教育訓練,並以書面約定並註明負責的責任,並每年進行資格複查,以確認其可信度及工作能力是否維持,若無法通過資格複查則調離其職，改派其他符合資格人選擔任。

3.人員任免遷調管理

當人員任用及約聘僱條件或契約有所變更,尤其是人員離退或是約聘僱用契約終止時,必定要遵守機密維護責任約定。

4.機密維護之責任約定

工作人員,依相關規定課予機密維護責任,並簽署憑證中心所規定之維護營業秘密契約書，員工不得以口頭、影印、借閱、交付、文章發表或其他方法洩漏營業秘密。

5.3.2 身家背景查驗程序

憑證中心對於 5.2 節之各信賴角色人員在初任時予以資格審查，以確認身分資格證明相關文件是否屬實。

5.3.3 教育訓練需求

角色	教育訓練需求
管理員	1、憑證中心安全原理和機制。 2、憑證中心安裝、設定和維護憑證中心系統操作程序。 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、產製和備份憑證中心之金鑰操作程序。 6、災後復原以及業務永續經營之程序。
簽發員	1、憑證中心安全原理和機制。 2、憑證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、災後復原以及業務永續經營之程序。
稽核員	1、憑證中心安全原理和機制。 2、憑證中心系統軟硬體的使用及操作程序。 3、產製和備份憑證中心之金鑰操作程序。 4、對稽核紀錄的查驗、維護和歸檔程序。 5、災後復原以及業務永續經營之程序。
維運員	1、系統設備的日常運作維護程序。 2、系統的備援及復原作業程序。 3、儲存媒體的更新程序。 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 再教育訓練需求及頻率

憑證中心的每一位相關工作人員，要熟悉憑證中心及其相關工作程序或法規的改變。有任何重大變動時，於一個月內要安排適當的教育訓練時間實施再訓練並做記錄，以適應新的工作程序及法規的運作。

5.3.5 工作調換頻率及順序

(1)不得互兼的角色，不可工作調換。

(2)維運員經過受訓之後，且經由審核通過，2 年後可轉任管理員、簽發員、稽核員等工作。

(3)管理員、簽發員及稽核員等工作人員等如果是未兼任維運員工作的人員，可以於轉任維運員工作 1 年後，再轉任管理員、簽發員或稽核員等工作。

5.3.6 未授權行動之制裁

憑證中心之相關人員，如違反憑證政策與本作業基準或其他憑證中心公佈之程序，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

與本公司正式人員安全要求相同。

5.3.8 提供給人員之文件資料

憑證中心提供合格的工作人員，下列相關文件，包括本作業基準、憑證系統操作手冊及我國電子簽章法及其施行細則等文件。

6. 技術安全控管

本章描述由憑證中心所執行的技術安全控管。

6.1 金鑰對產製與安裝

6.1.1 金鑰對之產製

憑證中心依照 6.2.1 節規定，於密碼模組內產製金鑰對，採虛擬亂數產生器(Pseudo Random Number Generator)及 RSA 金鑰演算法，私密金鑰在密碼模組內產製後一直儲存在其中而不外洩。憑證中心之金鑰產製由相關人員見證下進行。

6.1.1.1 用戶金鑰對之產製

如用戶使用之符記為 IC 卡時，其金鑰對由註冊中心代為產製，且金鑰對產製完畢後，其私密金鑰將無法由 IC 卡中匯出。

如用戶使用其他符記時，則由用戶自行產製金鑰對。

6.1.2 將私密金鑰傳送給憑證用戶

如用戶使用之符記為 IC 卡時，註冊中心將於憑證中心簽發憑證後，透過註冊窗口將含有用戶私密金鑰的 IC 卡交予用戶。

6.1.3 將用戶之公開金鑰傳送給憑證中心

如用戶使用之符記為 IC 卡時，由註冊中心透過安全管道將用戶之公開金鑰傳送至憑證中心。

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憑證中心。

本節所指安全管道為使用安全插座層通訊協定（Secure Socket Layer）或其他相同或更高級之資料加密傳送方式。

6.1.4 將憑證中心之公開金鑰傳送給信賴憑證者

憑證中心本身之公鑰憑證由中華電信憑證總管理中心簽發，公佈在中華電信憑證總管理中心的儲存庫上，信賴憑證者可直接下載及使用。信賴憑證者在使用憑證中心本身之公鑰憑證前必須依照中華電信憑證總管理中心憑證實務作業基準規定，由安全管道取得中華電信憑證總管理中心之公開金鑰或自簽憑證，然後檢驗中華電信憑證總管理中心對憑證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

憑證中心的金鑰長度為 2048 位元的RSA金鑰。

用戶的金鑰長度為 1024 位元的RSA金鑰。

6.1.6 公鑰參數產製

RSA 演算法公鑰參數為空的(Null)。

6.1.7 金鑰參數品質查驗

憑證中心簽章用金鑰對採ANSI X9.31演算法產生RSA演算法中所需的質數，該法可保證該質數為強質數(Strong Prime)。

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，但不保證該質數為強質數。

6.1.8 金鑰經軟體或硬體產製

憑證中心使用 6.2.1 節規定之安全密碼模組產製虛擬隨機亂數、公開金鑰對和對稱金鑰。用戶使用符合ISO 7816 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

憑證中心簽章用私密金鑰用於簽發憑證、憑證廢止清冊。

用戶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

憑證中心簽發憑證使用通過FIPS 140-2 Level 3認證的硬體密碼模組。

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

憑證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。採用此方法可使憑證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

憑證中心簽章用私密金鑰不被託管，憑證中心也不負責保管用戶的私密金鑰。

6.2.4 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，並使用通過FIPS 140-2 Level 2以上之驗證的IC卡做為秘密分持的儲存媒體。

6.2.5 金鑰歸檔

憑證中心簽章用私密金鑰不可被歸檔。憑證中心亦不對用戶簽章用私密金鑰進行歸檔。

6.2.6 私密金鑰輸入密碼模組

憑證中心在兩種情況時做私密金鑰輸入密碼模組中：

(1)金鑰產製時。

(2)金鑰持份備援的回復時。在此情況是以秘密持份(*m*-out-of-*n* control)的方式來做憑證中心私密金鑰的回復，經由私密金鑰秘密持份IC卡的回復後，便即時將完整的私密金鑰寫入到硬體密碼模組中。

6.2.7 私密金鑰啟動方式

憑證中心之私密金鑰之啟動是由m-out-of-n控管IC卡組來控制，不同用途的控管IC卡組由管理員、簽發員所保管。

用戶之私密金鑰儲放於IC卡中，需由一組用戶所屬之PIN碼來啟動。

用戶之私密金鑰儲放於其他儲存載具中，其啟用方式不另做規定。

6.2.8 私密金鑰停用方式

憑證中心私密金鑰之停用是採用m-out-of-n方式將私密金鑰停用。

本憑證中心不提供用戶之私密金鑰停用。

6.2.9 私密金鑰銷毀方式

為避免憑證中心舊的私密金鑰被盜用，影響簽發憑證之正確性，憑證中心之私密金鑰生命金鑰屆滿時將加以銷毀，因此，在憑證中心完成金鑰更新及簽發新的憑證後，將會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。

用戶私密金鑰之銷毀方式不另做規定。

6.3 金鑰對管理之其他要點

用戶必須自行管理金鑰對，憑證中心不負責保管用戶的私密金鑰。

6.3.1 公開金鑰之歸檔

憑證中心將進行用戶憑證之歸檔，且依照4.6節規定執行歸檔系統之安全控管，不再另外進行用戶公開金鑰的歸檔。

6.3.2 公開金鑰及私密金鑰之使用期限

6.3.2.1 憑證中心公開金鑰及私密金鑰之使用期限

憑證中心之公鑰及私鑰金鑰長度為RSA 2048 bits，私密金鑰使用期限為10年；公鑰憑證有效期限20年。

6.3.2.2 用戶公鑰及私鑰之使用期限

用戶之公鑰及私鑰金鑰長度為RSA 1024 bits：私密金鑰使用期限至多為5年；公鑰憑證有效期限至多為5年。

6.4 啟動資料之保護

6.4.1 啟動資料的產生及安裝

啟動資料以亂數產生後寫入密碼模組內，並分持至m-out-of-n控管IC 卡組中，存取IC卡中的啟動資料時必須輸入IC卡的個人識別碼(以下簡稱為PIN碼)。

6.4.2 啟動資料之保護

啟動資料由m-out-of-n控管IC卡組保護，IC卡的PIN碼由保管人員自行記憶，不得記錄於任何媒體上，IC卡移交時由新的保管人員重新設定新的PIN碼。

若登入的失敗次數超過3次，即鎖住此控管IC卡。

6.4.3 其他啟動資料之要點

憑證中心的私密金鑰的啟動資料不做歸檔。

6.5 電腦軟硬體安控措施

6.5.1 特定電腦安全技術需求

憑證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下列電腦安全功能。

(1) 具備角色或身分鑑別的登入。

(2) 提供自行定義(discretionary)存取控制。

(3) 提供安全稽核能力。

(4) 對各種憑證服務和PKI信賴角色存取控制的限制。

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

6.6.1 系統研發控管措施

憑證中心的系統研發遵循 ISO 9001 的規範進行品質控管。

憑證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。

6.6.2 安全管理控管措施

憑證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。

憑證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

每年至少一次評估現行金鑰長度是否有被破解之風險。

6.7 網路安全控管措施

憑證中心之主機和內部儲存庫透過雙重防火牆和外部網路連接，外部儲存庫置於外部防火牆之對外服務區(非軍事區DMZ)，連接到網際網路(Internet)，除必要之維護或備援外，提供不中斷之憑證與憑證廢止清冊查詢服務。

憑證中心之內部儲存庫資訊(包括憑證與憑證廢止清冊)以數位簽

章保護，自動從內部儲存庫傳送到外部儲存庫。

憑證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、6.2 節

7. 憑證及憑證廢止清冊之格式剖繪

7.1 憑證格式剖繪

憑證中心所簽發的憑證會遵循本作業基準的規定。

7.1.1 版本序號

憑證中心簽發 X.509 V3 版本的憑證。

7.1.2 憑證擴充欄位

憑證中心簽發的憑證之憑證擴充欄位會遵循 RFC2459 之規定。

7.1.3 演算法物件識別碼

憑證中心 簽發的憑證於簽章時,所使用的演算法物件識別碼為:

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):

憑證中心簽發的憑證於識別產製主體金鑰時,所使用的演算法物件識別碼為:

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

(OID:1.2.840.113549.1.1.1)

7.1.4 命名形式

憑證中的主體及簽發者兩個欄位值,必須使用 X.500 的唯一識

別名稱，且此名稱的屬性型態必須遵循 RFC 3280 的規定。

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

憑證中心簽發憑證的憑證政策物件識別碼為 2.16.886.1.100.1.1.2。

7.1.7 政策限制擴充欄位之使用

憑證中心簽發憑證不含政策政策限制擴充欄位。

7.1.8 政策限定元的語法及語意

憑證中心簽發的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

憑證中心簽發的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 憑證廢止清冊之格式剖繪

7.2.1 版本序號

憑證中心簽發 X.509 v2 版本的憑證廢止清冊(CRL)。

7.2.2 憑證廢止清冊擴充欄位

憑證中心簽發的憑證廢止清冊(CRL) 遵照 RFC3280 之規定。

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，本作業基準之修訂不會變更物件識別碼。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。

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，於儲存庫公告 15 個日曆天，始得修訂。

(2) 影響程度小者，於儲存庫公告 7 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 7 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 3 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，以儲存庫公告之回覆方式傳送給中華電信憑證管理中心，中華電信憑證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 7 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，由中華電信憑證管理中心公佈。

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。