中華電信通用憑證管理中心

憑證實務作業基準

(Public Certification Authority Certification Practice Statement

of Chunghwa Telecom，PublicCA CPS)

版本 1.5(草案)

中華電信股份有限公司

中華民國 102 年 9 月

目　　錄

中華電信通用憑證管理中心憑證實務作業基準摘要

中華電信股份有限公司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，制定中華電信通用憑證管理中心（以下簡稱本管理中心）憑證實務作業基準(以下簡稱本作業基準)。本作業基準之制定及修訂應經主管機關核定後，並公布於本公司網站，始得提供簽發憑證服務。

一、主管機關核定文號：經商字第　　號（待訂）

二、所簽發的憑證種類：

自然人、組織、設備或應用軟體憑證。

三、憑證等級：

中華電信通用憑證管理中心依據中華電信公開金鑰基礎建設憑證政策(以下簡稱憑證政策)之相關規定運作，簽發憑證政策所定義的測試級、第一級、第二級與第三級憑證，依據申請憑證的身分鑑別程序，簽發不同等級的自然人、組織、設備或應用軟體憑證(參見 1.3.5.1 節)。

四、應用範圍：

本管理中心所簽發的憑證，適用於電子商務網路交易或金融交易所需的身分認證及資料加密。

本管理中心的用戶及相關信賴憑證者，必須謹慎的使用本管理中心所簽發之憑證，不得逾越本作業基準、相關法令規定及本

管理中心與用戶及相關信賴憑證者之契約約定所限制及禁止的憑證應用範圍。

五、有關法律責任重要事項

1.本管理中心及註冊中心損害賠償責任

本管理中心或註冊中心處理用戶憑證相關作業，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，分別由本管理中心或註冊中心負賠償責任。用戶得依與本管理中心或註冊中心所訂契約相關約定，請求損害賠償；信賴憑證者得依相關法律規定，請求損害賠償。

2.本管理中心責任之免除

用戶或信賴憑證者如未依照本作業基準、相關法令規定及本管理中心與用戶及相關信賴憑證者之契約約定所引發之損害，或任何損害之發生，係不可歸責於本管理中心者，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

如因可歸責於用戶之事由，導致信賴憑證者遭受損害時，或任何損害之發生，係不可歸責於註冊中心時，應由用戶或信賴憑證者自負損害賠償之責。

用戶或信賴憑證者未依照本作業基準、相關法令規定及註冊中心與用戶及相關信賴憑證者之契約約定所引發之損害，或任何損害之造成係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本管理中心及註冊中心之事由，所導致之損害，本管理中心及註冊中心不負任何法律責任。本管理中心及註冊中心就憑證之使用範圍已設有明確限制，對逾越該使用範圍所生之損害，不負任何法律責任。

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

5.財務責任

本管理中心以中華電信股份有限公司為財務擔保；本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、廢止或辦理展期或重發，應遵守本作業基準第四章規定辦理，但仍應承擔異動前所有使用該憑證之義務。

六、其他重要注意事項

1. 本管理中心所屬註冊中心之註冊工作，皆經本管理中心授權許可。

2. 用戶應遵守本作業基準相關之規定，並確保所提供申請資

料之正確性。

3. 信賴憑證者在合理信賴本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。

4. 本公司將委託公正之第三人，就中華電信通用憑證管理中心的運作進行稽核。

1. 總則

本文件的名稱為中華電信通用憑證管理中心憑證實務作業基準(Public 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。

本管理中心是中華電信公開金鑰基礎建設(Chunghwa Telecom ecommerce Public Key Infrastructure, ePKI，簡稱本基礎建設)的一層下屬憑證機構(Level 1 Subordinate CA)，在本基礎建設中負責簽發及管理自然人、組織、設備或應用軟體憑證。中華電信憑證總管理中心(ePKI Root Certification Authority, eCA)為本基礎建設之最頂層憑證管理中心，是本基礎建設的信賴根源，由中華電信股份有限公司負責營運與建置，信賴憑證者可直接信賴中華電信憑證總管理中心的憑證。

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本管理中心、註冊中心(Registration Authority)、用戶(Subscribers)、信賴憑證者(Relying Parties)及儲存庫(Repository)等。

1.2 版本識別

本作業基準為第 1.5 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://publicCA.hinet.net

本作業基準對應之憑證政策物件識別碼如下表所示：

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}

1.3 主要成員及憑證適用範圍

本管理中心之相關成員包括：

(1) 中華電信通用憑證管理中心

(2) 註冊中心(Registration Authority)

(3) 儲存庫(Repository)

(4) 用戶(Subscribers) 及信賴憑證者(Relying Parties)

1.3.1 中華電信通用憑證管理中心

中華電信通用憑證管理中心，由中華電信股份有限公司負責建置及營運，依照憑證政策之規定運作，簽發自然人、組織、設備或應用軟體憑證。

1.3.2 註冊中心(Registration Authority)

註冊中心是負責收集和驗證用戶的身分及憑證相關資訊之註冊工作。註冊中心由多個註冊窗口（RA Counter）組成，由本管理中心授權核可之組織擔任，註冊窗口設有憑證註冊審驗人員（RA Officer，RAO），負責受理憑證申請、廢止等作業。

1.3.3 儲存庫(Repository)

本管理中心儲存庫是負責公告及儲存由本管理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。儲存庫提供24 小時全天的服務，本管理中心儲存庫的網址為：http://publicCA.hinet.net。

1.3.4 用戶(Subscribers)及信賴憑證者(Relying Parties)

1.3.4.1 用戶

係指已申請並取得本管理中心核發憑證之個人，其與憑證主體之關係如下表所示：

憑證主體	用戶
自然人	本人
組織	組織授權之委任人
設備	設備之擁有者
應用軟體	應用軟體之擁有者

用戶金鑰對的產製應符合本作業基準 6.1.1 節之規定，並且用戶

必須獨自擁有控制憑證相對應私密金鑰的權力與能力。

1.3.4.2 信賴憑證者

信賴憑證者係指相信憑證主體名稱與公開金鑰間連結關係之第三人。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)驗證具有數位簽章的電子文件之完整性。

(2)驗證文件簽章產生者的身分。

(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

本管理中心簽發憑證政策所定義保證等級測試級、第一級、第二級與第三級之憑證(含簽章及加密用的憑證)。

設備或應用軟體憑證可應用於安全插座層(Secure Socket Layer, SSL)通訊協定、時戳伺服器及專屬開發的伺服器應用軟體。

各憑證保證等級之適用範圍說明如下：

保證等級	適用憑證種類	鑑別方式	適用範圍

測試級	自然人、組織、設備或應用軟體	藉由表單取得本管理中心安全主管授權給執行測試級憑證簽發程式的人員。	本管理中心系統上線與更新前回歸測試、檢查本管理中心系統狀態。
第一級	自然人、組織、設備或應用軟體	以電子郵件方式確認申請人確實可操作該郵件帳號。	適合應用於惡意篡改之威脅很低的網路環境，或無法提供較高保證等級時，可識別憑證主體名稱及保證被簽署文件的完整性；不適合應用於需要認證的線上交易。 例如電子郵件所需之資料加密與身分認證。
第二級	自然人、組織、設備或應用軟體	申請人不需臨櫃辦理，但需提供合法且正確之個人或組織身分證明文件，由憑證註冊審驗人員核對申請人提供之資料或系統自動比對可靠之資料庫後，確認申請人之資料正確性。	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)；不適合做為重要文件(與生命及高金額相關的交易之文件)的簽署。 例如小額度電子商務交易所需之資料加密與身分認證。
第三級	自然人、組織、設備或應用軟體	申請人需親臨註冊窗口申請，由憑證註冊審驗人員確認申請人資料之正確性，或使用政府公開金鑰基礎建設核發之保證等級第三級憑證簽章提出申請，由系統自動比對，確認申請人之資料正確性。	適合應用於有惡意使用者會截取或篡改資訊、較第二級危險之網路環境，傳送的資訊包括金錢上的線上交易。 適用電子商務交易或金融交易所需之資料加密與身分認證。 包含(但不限於)以下應

保證等級	適用憑證種類	鑑別方式	適用範圍
測試級	自然人、組織、設備或應用軟體	藉由表單取得本管理中心安全主管授權給執行測試級憑證簽發程式的人員。	本管理中心系統上線與更新前回歸測試、檢查本管理中心系統狀態。
			用:電子銀行之電子交易、轉帳授權、帳務通知、申請指示服務；網路下單；網路報稅

使用及信賴本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

用戶使用私密金鑰時，也應自行選擇值得信賴的電腦環境及應用系統,以避免因私密金鑰被惡意軟硬體盜取,或誤用而引起權益損害。

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

信賴憑證者應依 6.1.9 節所述記載於憑證中的金鑰用途(Key Usage)，以適當地使用個別的金鑰，並且應正確處理在憑證延伸欄位中被標示為關鍵性(critical)欄位的憑證屬性資料。

1.3.5.3 憑證禁止事項

本管理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

(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或用戶報告遺失金鑰等事件，可直接與本管理中心聯絡。

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 中華電信通用憑證管理中心。

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://publicCA.hinet.net 查詢。

2. 一般條款

2.1 職責與義務

本節說明本管理中心、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 中華電信通用憑證管理中心職責

(1) 遵循憑證政策與本作業基準運作。

(2) 對憑證申請進行識別及鑑別。

(3) 提供簽發及公布憑證服務。

(4) 廢止、停用及恢復使用憑證。

(5) 簽發及公布憑證廢止清冊。

(6) 安全產製本管理中心與註冊中心之私密金鑰。

(7) 私密金鑰安全管理。

(8) 依 6.1.9 節規定使用私密金鑰。

(9) 支援註冊中心進行憑證註冊相關作業。

(10) 對憑證機構與註冊中心人員作識別與鑑別。

2.1.2 註冊中心職責

(1) 提供憑證申請服務。

(2) 對憑證申請進行識別及鑑別。

(3) 告知用戶及信賴憑證者關於本管理中心、註冊中心的義務與責任。

(4)告知用戶及信賴憑證者，於取得或使用本管理中心所簽發之憑證，應遵守本作業基準之相關規定。

(5)執行憑證註冊審驗人員之識別與鑑別程序。

(6)管理註冊中心之私密金鑰。

2.1.3 用戶義務

(1)用戶應遵守本作業基準憑證申請之相關規定，並確認所提供申請資料之正確性。

(2)本管理中心同意憑證申請並簽發憑證後，用戶應依照 4.3 節規定接受憑證。

(3)用戶在取得本管理中心所簽發之憑證後，應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，用戶應通知註冊中心，並不得使用該憑證。

(4)用戶應妥善保管及使用其私密金鑰。

(5)用戶之憑證如須暫停使用、恢復使用、廢止或重發，應依照第 4 章規定辦理。如發生私密金鑰資料外洩或遺失等情形，必須廢止憑證時，應儘速通知註冊中心，但用戶仍應承擔異動前所有使用該憑證之法律責任。

(6)用戶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，用戶應自行承擔責任。

(7)本管理中心如因故無法正常運作時，用戶應儘速尋求其他途徑完成與他人應為之法律行為，不得以本管理中心無法正常運作，作為抗辯他人之事由。

2.1.4 信賴憑證者義務

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

(2)信賴憑證者在使用本管理中心簽發之憑證時，應先查驗憑證之保證等級以確保權益。

(3)信賴憑證者在使用本管理中心簽發之憑證時，應確認該憑證所記載之憑證及金鑰用途。

(4)信賴憑證者在使用本管理中心簽發之憑證時，應先查驗憑證廢止清冊，以確認該憑證是否有效。

(5)信賴憑證者在使用本管理中心簽發之憑證或憑證廢止清冊時，應先查驗數位簽章，以確認該憑證或憑證廢止清冊是否正確。

(6)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信賴憑證者或用戶權益受損時，信賴憑證者應自行承擔責任。

(7)本管理中心如因故無法正常運作時，信賴憑證者應儘速尋求其他途徑完成與他人應為之法律行為，不得以本管理中心無法正常運作，作為抗辯他人之事由。

(8)信賴憑證者接受使用本管理中心簽發之憑證時，即視為已了解並同意有關本管理中心法律責任之條款，並依照 1.3.5 節規定範圍使用憑證。

2.1.5 儲存庫職責

(1)依 2.6 節規定，定期公布所簽發憑證、已廢止憑證、憑證廢止清冊。

(2)公布本作業基準的最新資訊。

(3)儲存庫之存取控制依照 2.6.3 節之規定。

(4)公布外部稽核之結果。

(5)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 中華電信通用憑證管理中心之責任

2.2.1.1 責任範圍

本管理中心依照本作業基準第 4 章規定之程序執行相關之憑證管理作業。

2.2.1.2 賠償責任

本管理中心處理用戶憑證相關作業，若故意或過失未遵照本作業基準、相關法令規定及本管理中心與用戶及相關信賴憑證者之契約約定，致用戶或信賴憑證者受有損害時，由本管理中心負賠償責任。用戶得依與本管理中心或註冊中心所訂契約相關約定，請求損害賠償；信賴憑證者得依相關法律規定，請求損害賠償。本管理中心對每一用戶或信賴憑證者之賠償總金額限制如下表所示，如用戶或信賴憑證者與本公司訂有合約，另行規範憑證使用範圍與交易賠償限額者，從其約定。

憑證保證等級	賠償總金額上限(新台幣:元)
第一級	3,000
第二級	100,000
第三級	3,000,000

此賠償上限為賠償金額之最高額度，實際上之賠償仍須依照用戶或憑證信賴者實際所受之損害為賠償依據。

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、或未依任何本作業基準、相關法令規定及本管理中心與用戶及相關信賴憑證者之契約約定所引發之損害，或任何損害之發生，係不可歸責於本管理中心者，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本管理中心之事由，所導致之損害事件，本管理中心不負任何法律責任。本管理中心就憑證之使用範圍已設有明確限制，對逾越該使用範圍所生之損害，不負任何法律責任。

如因本管理中心之系統維護、轉換及擴充等需要，得事先於三日前公告於儲存庫，暫停部分憑證服務，用戶或信賴憑證者不得以此作為要求本管理中心損害賠償之理由。

如因 4.4.1 節廢止憑證之事由，用戶應向註冊中心提出廢止憑證申請，在廢止憑證申請核定後，本管理中心將於 1 個工作天內完成憑證廢止作業、簽發憑證廢止清冊及公告於儲存庫。用戶於憑證廢止狀態未被公布之前，應採取適當的行動，以減少對信賴憑證者之影響，並承擔所有因使用該憑證所引發之責任。

2.2.2 註冊中心責任

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。

本管理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註冊作業，若故意或過失未遵照本作業基準、相關法令規定及註冊中心與用戶及相關信賴憑證者之契約約定，致用戶或信賴憑證者受有損害時，由註冊中心負賠償責任。用戶得依與註冊中心所訂契約之相關約定，請求損害賠償；信賴憑證者得依相關法律規定，請求損害賠償。

2.2.2.3 責任免除

如因可歸責於用戶之事由，導致信賴憑證者遭受損害時，或任何損害之發生，係不可歸責於註冊中心時，應由用戶或信賴憑證者自負損害賠償之責。

用戶或信賴憑證者未依照本作業基準、相關法令規定及註冊中心與用戶及相關信賴憑證者之契約約定所引發之損害，或任何損害之造成係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。本註冊中心就憑證之使用範圍已設有明確限制，對逾越該使用範圍所生之損害，不負任何法律責

任。

2.3 財務責任

2.3.1 財務保證

本管理中心由中華電信股份有限公司營運，其財務責任由中華電信股份有限公司負責。

2.3.2 財務保險

本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

本管理中心之財務，係屬中華電信股份有限公司整體財務之一部。中華電信股份有限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 8 章所述。

2.4.3 爭議解決

用戶或註冊中心與本管理中心如有爭議時，雙方應本誠信原則協商解決之。如有訴訟之必要時，雙方同意以臺灣臺北地方法院為第一審管轄法院。

2.5 費用

2.5.1 憑證簽發或展期費用

本管理中心與用戶之間的憑證申請、簽發、展期等計費架構，於相關業務契約條款中訂定，且相關之條款用戶可直接連結至儲存庫查詢。

2.5.2 憑證查詢費用

憑證查詢計費架構於相關業務契約條款中訂定，且相關之條款用戶可直接連結至儲存庫查詢。

2.5.3 憑證廢止或狀態查詢費用

用戶下載查詢憑證廢止清冊不收費；線上查詢憑證狀態(OCSP 功能)計費架構於相關業務契約條款中訂定，用戶可直接連結至儲存庫

查詢。

2.5.4 退費規定

本管理中心所收取之憑證簽發或展期收費，如因本管理中心之過失致用戶憑證無法使用，經本管理中心查明後得予以重新簽發憑證，若用戶不接受重新簽發憑證者，本管理中心應退還用戶本項費用。除前述情形及 4.9 節之情形外, 其他費用均不退費。

2.6 公布及儲存庫

2.6.1 中華電信通用憑證管理中心資訊公布內容

(1)本作業基準。

(2)憑證廢止清冊。

(3)本管理中心本身之憑證(至與該憑證之公開金鑰相對應之私密金鑰所簽發的所有憑證效期到期為止)。

(4)簽發之憑證。

(5)隱私權保護政策。

(6)本管理中心相關最新訊息。

2.6.2 公布方法及頻率

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

(2)本管理中心每天至少簽發兩次憑證廢止清冊，公布於儲存庫。

(3)本管理中心本身之憑證，於簽發時公布於儲存庫。

(4)簽發之憑證，於簽發時公布於儲存庫。

2.6.3 存取控制

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

有關 2.6.1 節本管理中心公布的資訊，主要提供用戶與信賴憑證者使用瀏覽器查詢之用，因此開放提供閱覽存取，並為保障儲存庫之安全應進行存取控制，且應維持其可接取狀態及可用性。

2.6.4 儲存庫

儲存庫由本管理中心負責管理，如因故無法正常運作，將於 2 個工作天內恢復正常運作，儲存庫之網址為：http://publicCA.hinet.net

2.7 稽核方法

2.7.1 稽核頻率

本管理中心接受一年一次的外部稽核與不定期的內部稽核，以確認本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

本公司將委外辦理本管理中心之外部稽核作業，委託熟悉本管理中心運作並經 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 標準之稽核業者，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，本管理中心於稽核時應對稽核人員進行身分識別。

2.7.3 稽核人員及被稽核方之關係

本公司將委託公正之第三人，就本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)本管理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程序運作。

2.7.5 對於稽核結果之因應方式

如稽核人員發現本憑證管理中心或註冊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)將不符合情形通知本管理中心。

(3)對於不符合規定之項目，本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。有關註冊中心之缺失將通知註冊中心改善。

2.7.6 稽核結果公開之範圍

本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

以下由本管理中心或註冊中心產生、接收或保管之資料，均視為機密資訊。

(1)營運相關的私密金鑰及通行碼(passphrase)。

(2)金鑰分持的保管資料。

(3)用戶之申請資料。

(4)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。

(6)列為機密等級的營運相關文件。

本管理中心及註冊中心之現職及退職人員與各類稽核人員

對於機密資訊均嚴守秘密。

2.8.2 非機密之資訊種類

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

(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布於本管理中心儲存庫。

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；惟本管理中心保留向申請查詢之機關收取合理費用之權利。

2.8.5 應用戶要求釋出資訊

用戶得查詢 2.8.1 節第(3)款之申請資料；惟本管理中心保留向申請查詢之用戶收取合理費用之權利。

2.8.6 其他資訊釋出之情況

本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

本管理中心依照個人資料保護法處理用戶申請資料。

2.9 智慧財產權

下列項目為本管理中心之智慧財產:

(1)本管理中心及註冊中心的金鑰對及金鑰分持。

(2)因執行本管理中心憑證管理作業而撰寫的相關文件或研發之

系統。

(3)本管理中心所簽發的憑證及憑證廢止清冊。

(4)本作業基準。

本公司同意本作業基準可由本管理中心儲存庫自由下載，或依著作權法相關規定重製或散布，但必須保證是完整複製，並註明著作權為中華電信股份有限公司所擁有。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

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

3.1.2 命名須有意義

本管理中心所簽發的憑證，其憑證主體名稱(Subject)符合我國法律對該主體命名之相關規定，以代表該主體的名稱。

伺服軟體之憑證主體名稱與憑證主體別名不得使用內部伺服器名稱(Internal Server Name)或保留 IP 位址(Reserved IP Addresses)。

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

本管理中心的X.500唯一識別名稱為：

C=TW，

O=Chunghwa Telecom Co., Ltd.，

OU=Public Certification Authority

本管理中心將採用 X.520 標準所定義的各種命名屬性加以組合以確保用戶憑證主體名稱在本管理中心所認知的 X.500 名稱空間內具備獨特性。本管理中心之用戶憑證主體名稱允許（但不限於）使用以下 X.520 標準所定義的各種命名屬性加以組合而成：

- countryName（縮寫為 C）
- stateOrProvinceName（縮寫為 S）
- localityName（縮寫為 L）
- organizationName（縮寫為 O）
- organizationalUnitName（縮寫為 OU）
- commonName（縮寫為 CN）
- serialNumber

3.1.5 命名爭議之解決程序

當用戶之識別名稱相同時，以先申請之用戶優先使用，相關之糾紛或仲裁處理，非本管理中心之權責範圍，由用戶向相關主管機關或法院提出申請。

當用戶使用之識別名稱，經相關主管機關或有權解釋機關證實為其他申請者擁有時，由該用戶負擔相關的法律權責，本管理中心得逕行廢止該用戶之憑證。

3.1.6 商標之辨識，鑑別及角色

用戶提供之憑證主體名稱須符合我國商標法及公平交易法之相關規定，本管理中心對用戶提供之憑證主體名稱是否符合上述規定不負審查之責，相關糾紛或仲裁處理非本管理中心權責範圍，由用戶依據一般行政或司法救濟途徑處理之。

3.1.7 證明擁有私密金鑰之方式

本管理中心會驗證個體持有之私密金鑰與將記載於憑證上的公鑰成對，分為兩種方式。

(1)由註冊中心代用戶產製金鑰對，簽發憑證時由註冊中心透過安全管道將用戶之公開金鑰傳送至本管理中心，所以用戶在申請憑證時就不必證明持有私密金鑰。

(2)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 組織身分之鑑別

對於組織(Organization)身分鑑別所需之證件、鑑別確認程序及是否需臨櫃辦理等，依照不同保證等級而有不同之規定，如下表所列：

保證等級	組織身分鑑別之程序
測試級	不做鑑別。
第一級	(1)不做書面證件核對。 (2)只要申請人具有自己的電子郵件地址即可申請憑證。 (3)不需臨櫃辦理。
第二級	(1)可不做書面證件核對。 (2) 申請人提交組織資料，例如組織識別碼(如扣繳單位稅籍統一編號)、組織名稱等，本管理中心有權與政府提供之資料庫或可信賴之第三者資料庫的登記資料進行比對，以確認申請人之身分。

保證等級	組織身分鑑別之程序
	(3)不需臨櫃辦理。
第三級	組織身分鑑別分為以下三種情形： (1)民間組織之身分鑑別 民間組織必須提供註冊窗口正確且經主管機關或合法授權單位(例如法院)核發之相關證明文件影本(例如公司變更登記事項卡、法人登記證書)，證明文件影本應蓋用組織及負責人之印鑑章(與組織登記時所使用之印鑑章相符)，註冊窗口將核對組織所提供之申請資料及代表人身分的真實性，並驗證該代表人有權以該組織之名義申請憑證。申請時應由代表人親臨憑證機構或註冊中心辦理，如代表人無法親自臨櫃申請，得以書面委託書委任代理人代為臨櫃申請，並依 3.1.9 節中保證等級第三級之規定鑑別代理人之身分。 民間組織如於申請憑證前已依法完成向主管機關設立登記程序或已於憑證機構、註冊中心或憑證機構信賴之機構或個人(例如公證人、本公司對民間組織之專戶/專案經理)完成符合上述規定之臨櫃識別與鑑別程序，並留下登記或識別與鑑別之佐證資料(例如留下印鑑章圖記或由公證人或本公司對該民間組織之專戶/專案經理在申請書上加蓋認證戳記等)，則憑證機構或註冊中心得允許該組織於申請憑證時出示佐證資料來取代上述

保證等級	組織身分鑑別之程序
	識別與鑑別方式。 以上所稱民間組織係指私法人團體、非法人團體或以上兩者之附屬組織。 (2)政府機關(構)或單位之身分鑑別 政府機關(構)或單位比照前述民間組織之身分鑑別方式，或以正式公文書申請憑證，而憑證機構或註冊中心必須確認該機關(構)或單位確實存在，並驗證公文書之真確性。 (3)中華電信所屬組織之身分鑑別 中華電信所屬組織必須以正式公文書申請憑證，而註冊窗口必須確認該機構或單位確實存在，並驗證公文書之真確性。 此外，前述三類組織之憑證申請資料透過政府公開金鑰基礎建設核發之保證等級第三級憑證簽章時，代表人不需親臨辦理，註冊中心系統或註冊窗口將驗證申請資料之數位簽章是否有效。

3.1.9 個人身分之鑑別

對於個人(Individual)身分鑑別之證件、確認程序及是否需臨櫃辦理等，依照不同保證等級而有不同之規定，如下表所列：

保證等級	個人身分鑑別之程序
測試級	不做規定。
第一級	(1)可不做書面證件核對。 (2)只要申請者具有自己的電子郵件地址即可申請憑證，可不進行鑑別確認程序。 (3)不需臨櫃辦理。
第二級	(1)可不做書面證件核對。 (2)申請者提交個人資料，例如個人識別碼(如身分證字號、護照號碼)、姓名等，本管理中心有權與政府提供之資料庫或可信賴之第三者資料庫的登記資料進行比對，以確認申請者之身分。 (3)不需臨櫃辦理。
第三級	(1)核對書面證件： 在申請憑證時，申請者應提供包括姓名、身分證字號、出生日期等資料，至少應出示一張被認可並附照片之證件正本(例如國民身分證或護照)，供註冊窗口鑑別申請者之身分。

保證等級	個人身分鑑別之程序
	如申請者(例如未成年人)無上述之附照片證件，可使用由政府發給之足以證明用戶身分的書面證明文件(例如戶口名薄)取代，並由一位具行為能力之成年人以書面保證申請者之身分；出具書面保證之成年人之身分必須經過上述之鑑別。 (2)申請者提交之個人資料，例如個人的識別碼(如身分證字號)、姓名及地址(如戶籍地址)等，本管理中心有權與該資料主管機關的登記資料(如戶籍資料)或其它經主管機關認可之可信賴第三者的登記資料進行比對。 (3)臨櫃辦理： 申請者必須親臨憑證機構或註冊中心證明其身分。若申請者無法親自臨櫃辦理，得以書面委託書委任代理人代為臨櫃申請，但憑證機構或註冊中心必須確認該委託書之真偽(例如比對委託書上之用戶印鑑章)，並依上述規定鑑別代理人之身分。 申請者如果事前已經受憑證機構、註冊中心或憑證機構信賴之機構或個人（例如戶政事務所、公證人）進行過符合上述規定之臨櫃識別與鑑別程序，並且留下該識別與鑑別之佐證資料（例如印鑑證明），則申請者不需親臨辦理，憑證機構或註冊中心將驗證該佐證資料。

保證等級	個人身分鑑別之程序
	(4)使用自然人憑證辦理 使用內政部憑證管理中心簽發之保證等級第三級憑證簽章辦理，則申請者不需親臨註冊窗口證明其身分，註冊中心系統或註冊窗口將驗證其數位簽章是否有效。

3.1.10 設備或應用軟體鑑別之程序

電腦及通訊設備(如路由器、防火牆等)或應用軟體(如Web Server)，因在法律上不具行為能力，必須由設備或應用軟體之擁有者提出憑證申請；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，由用戶重新申請憑證，依照 3.1 節規定進行識別及鑑別。

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數位簽章，以識別用戶之身分。過期、停用、廢

止之憑證不得展期；憑證最多展期至 6.3.2.2 節規定之用戶公開金鑰使用期限上限為止，以維護金鑰對的安全。

3.3 憑證廢止之金鑰更換

如用戶之私密金鑰因憑證廢止必須更換金鑰時，應向本管理中心重新申請憑證，註冊中心將依照3.1節規定，對於重新申請憑證之用戶進行識別及鑑別。

3.4 憑證廢止

憑證廢止申請之鑑別程序與 3.1.8、3.1.9、3.1.10 節規定相同。

3.5 憑證暫時停用與恢復使用

用戶連線至儲存庫提出申請時，註冊中心系統將以用戶輸入之通行碼鑑別其身分。

4. 營運規範

4.1 申請憑證之程序

憑證申請步驟如下：

(1) 憑證申請者填寫憑證申請資料並同意用戶約定條款。

(2) 憑證申請者將憑證申請資料及相關證明資料傳送給註冊中心。

(3) 如憑證申請者自行產製金鑰，需產生 PKCS#10 憑證申請檔並以私密金鑰加以簽章，於申請憑證時將該憑證申請檔交給註冊中心。

申請憑證時，憑證申請者應據實提供正確且完整之資料。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，註冊中心及本管理中心依本作業基準之規定妥善保管。

4.2 簽發憑證之程序

本管理中心及其註冊中心在接到憑證申請資料後，即依本作業基準第 3 章之規定，進行相關的審核程序，以作為判定是否同意簽發憑證之依據。

簽發憑證步驟如下：

(1) 註冊中心將審核通過之憑證申請資料傳送至本管理中心。

(2) 本管理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，本管理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，應主動聯絡本管理中心，確實瞭解問題之所在。

(4) 為確保本管理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) 本管理中心保有拒絕簽發憑證給任何個體之權利，本管理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

本管理中心完成憑證簽發後，將通知用戶領取憑證，用戶取得憑證後應檢查憑證內有關憑證用戶之資訊是否正確且與申請時提供之資料一致，如果發現有任何錯誤，應立即通知註冊中心處理，否則視為用戶同意遵守本作業基準或相關合約上之權利與義務。

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，本管理中心得就下列情形逕行廢止憑證，毋須事先通知用戶。

(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) 確知本管理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；

本管理中心終止服務時，若無憑證機構承接本管理中心的業務，將報請主管機關安排其他憑證機構承接；若仍無其他憑證機構承接時，本管理中心將於終止服務三十日前，於儲存庫公告廢止憑證，並通知憑證之所有人。

4.4.2 憑證廢止之申請者

用戶、註冊中心或合法授權之第三人(如司法或檢調機關、組織授權之代理人、自然人之法定繼承人)。

4.4.3 憑證廢止之程序

(1)憑證廢止申請者依據註冊中心制訂之作業規範提出憑證廢止請求，註冊中心在接到憑證廢止請求後，即進行相關的審核

程序，並保留所有憑證廢止請求紀錄，包含申請者名稱、聯絡資料、廢止原因、廢止時間與日期等，以作為後續權責歸屬之依據。

(2)註冊中心完成審核作業後,將憑証廢止申請訊息傳送至本管理中心。

(3)本管理中心接獲註冊中心送來之憑證廢止申請資料時,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廢止請求廢止該憑證。

(4)如以上之查驗不通過時,本管理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，應主動聯絡本管理中心，確實瞭解問題之所在。

(5)為確保本管理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。

4.4.4 憑證廢止申請之處理時間

用戶提出憑證廢止申請後,註冊中心應儘速於一個工作天內完成審核程序，審核通過後，本管理中心將於一個工作天內完成廢止憑證作業。

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)憑證金鑰對懷疑遭盜用時。

(2)自行認定必須申請憑證之暫時停用。

4.4.6 暫時停用憑證之申請者

由用戶提出申請。

4.4.7 暫時停用憑證之程序

由用戶提出申請，註冊中心檢驗申請資料正確無誤後，加簽數位簽章上傳至本管理中心，本管理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，本管理中心將拒絕暫時停用憑證。

4.4.8 暫時停用憑證之時間

用戶提出憑證暫時停用申請後，註冊中心應儘速於一個工作天內完成審核程序，審核通過後，本管理中心將於一個工作天內完成憑證暫時停用處理程序。

用戶在申請暫時停用憑證時，不必申告所需停用的期間，本管理中心所設定憑證暫時停用的最長期間為自核可申請時間到該憑證到期的時間。

如果在憑證暫時停用期間，用戶取消憑證暫時停用，即恢復使用憑證，則該憑證恢復為有效的(Valid)。

4.4.9 恢復使用憑證之程序

由用戶提出申請，註冊中心檢驗申請資料正確無誤後，加簽數位簽章上傳至本管理中心，本管理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，本管理中心將拒絕恢復使用憑證。

4.4.10 憑證廢止清冊簽發頻率

本管理中心之憑證廢止清冊簽發頻率至少每天 2 次，所簽發的憑證廢止清冊之有效期限不超過 36 小時。在憑證廢止清冊尚未過期前，本管理中心即可能簽發新的憑證廢止清冊，因此新憑證廢止清冊的效期與舊的憑證廢止清冊的效期會可能有所重疊，在效期重疊期間，即使舊的憑證廢止清冊尚未過期，信賴憑證者仍可至本管理心儲存庫取得新的憑證廢止清冊，以獲得更即時的憑證廢止資訊。

4.4.11 憑證廢止清冊查驗規定

信賴憑證者使用本管理中心所簽發之憑證前，應先檢核本管理中心公布之憑證廢止清冊或線上查詢憑證狀態，以確定該憑證是否有效。

本管理中心於儲存庫公開暫停使用及廢止之憑證資料，以供查核，對於信賴憑證者查驗憑證廢止清冊無任何限制，網址如下：

http://publicca.hinet.net

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

所有本管理中心安全相關的事件，均做安全稽核紀錄(audit log)。安全稽核紀錄採自動產生、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) 金鑰產製

- 本管理中心產製金鑰時(但是並不強制規定在單次或只限一次使用的金鑰的產製)。

(2) 私密金鑰之載入和儲存

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

(3) 憑證之註冊

- 憑證之註冊申請過程。

(4) 廢止憑證

- 憑證之廢止申請過程。

(5) 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。

(6) 憑證格式剖繪之管理

- 憑證格式剖繪之改變。

(7) 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。

(8) 實體存取及場所之安全

- 得知或懷疑違反實體安全規定。

(9) 異常

- 軟體錯誤。
- 違反本作業基準。
- 重設系統時鐘。

4.5.2 紀錄檔處理頻率

本管理中心定期檢視稽核紀錄，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。稽核檢視之結果以文件記錄。

本管理中心每 2 個月檢視稽核紀錄一次。

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，以數位簽章方式確保稽核紀錄檔之完整性，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) 本管理中心週期性的將事件日誌歸檔。

(2) 本管理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

所有本管理中心安全相關的事件，均做安全稽核紀錄(audit log)。安全稽核紀錄採自動產生、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

本管理中心每年至少一次對憑證管理系統進行弱點掃描，並進行相關的補強措施。

4.6 紀錄歸檔

本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) 本管理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、廢止及重發等之重要追蹤紀錄。

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

本管理中心記錄的歸檔資料有：

(1) 本管理中心被主管機關認證的(Accreditation)資料

(2) 憑證實務作業基準

(3) 重要的契約

(4) 系統與設備組態設定

(5) 系統或組態設定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 節所訂定的用戶身分識別資料

(9) 所有已簽發或公告的憑證

(10) 本管理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

4.6.2 歸檔之保留期限

本管理中心最少要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也被維護 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) 經過本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

本管理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，紙本紀錄將由本管理中心所授權之人員定期整理歸檔。

4.6.5 時戳紀錄之要求

本管理中心的所有電腦系統都會定期進行校時，以確保電子式紀錄中日期與時間資訊的準確性與可信度。歸檔之電子式紀錄(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 歸檔資料彙整系統

目前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

在獲取憑證機構歸檔資訊時，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。

4.7 金鑰更換

本管理中心之私密金鑰依照 6.3.2 節規定定期更換。本管理中心於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。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憑證廢止清冊，新的憑證將公布於儲存庫，提供用戶下載。舊私密金鑰也用在簽發憑證廢止清冊，所以舊私密金鑰仍須維持與保護到所簽發的所有用戶憑證到期為止。

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。

4.8 金鑰遭破解或災變時之復原程序

4.8.1 中華電信通用憑證管理中心電腦資源、軟體或資料遭破壞之復原程序

本管理中心訂定電腦資源、軟體及資料遭破壞之復原程序，同時每年進行演練。

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

4.8.2 中華電信通用憑證管理中心簽章金鑰憑證被廢止之復原程序

如本管理中心之簽章金鑰憑證被廢止，將公告於儲存庫，通知信賴憑證者，並依照 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。

本管理中心每年至少進行一次本管理中心之簽章金鑰憑證被廢止之演練。

4.8.3 中華電信通用憑證管理中心簽章金鑰遭破解之復原程序

如本管理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) 廢止本管理中心簽章金鑰憑證及所簽發之用戶憑證。

(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。

本管理中心每年至少進行一次本管理中心簽章金鑰遭破解之演練。

4.8.4 中華電信通用憑證管理中心安全設施之災後復原工作

本管理中心訂定災害復原之程序，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害復原程序，優先回復本管理中心儲存庫之運作，並迅速重建憑證簽發及管理的能力。

4.9 中華電信通用憑證管理中心之終止服務

本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，本管理中心應遵守以下事項：

(1) 本管理中心於預定終止服務三十日前，通知主管機關(經濟部)與用戶；

(2) 本管理中心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。

- 若無憑證機構願承接本管理中心之業務，將陳報主管

機關安排其他憑證機構承接。

- 若經主管機關安排其他憑證機構承接，仍無其他憑證機構承接時，本管理中心將於終止服務三十日前，於儲存庫公告廢止當時仍具效力之憑證憑證，並通知憑證之所有人。本管理中心將依憑證有效期限比例，退還憑證簽發或展期費用。

- 主管機關於必要時，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

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

5.1.2 實體存取

本管理中心建置採適當之措施管制連接提供本管理中心服務的硬體、軟體和硬體密碼模組。

本管理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本管理中心系統的惡意軟體。

非本管理中心人員進出機房，需填寫進出紀錄，並由本管理中心相關人員全程陪同。

本管理中心相關人員離開機房時，將進行以下之查驗工作並記錄，以防止未授權人員進入機房：

(1)確認設備是否正常運作。

(2)確認機箱門是否關閉。

(3)確認門禁系統是否正常運作。

5.1.3 電源和空調

本管理中心的電力系統，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。

本管理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

本管理中心機房設置在基地墊高建築物的第 3 樓層（含）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

本管理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 節所記載本管理中心的文件資料，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

異地備援的地點與本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。

5.2 程序控制

本管理中心經由作業程序控管(procedural controls)，以規定可以操作本管理中心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

本管理中心必須確保從事關鍵性本管理中心功能的責任，能做適當的區隔分派，以防止某人惡意使用本管理中心系統而不被察覺。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。

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

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，以確認本管理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。

■ 系統軟硬體的更新。

■ 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

本管理中心角色分依照 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、設定和維護本管理中心系統	2				1
建立和維護系統之使用者帳號	2				1
產製和備份本管理中心之金鑰	2		1		1
啟動/停止憑證簽發服務		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
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
除本管理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。

本管理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

本管理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,並簽署本管理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

本管理中心對於 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、本管理中心安全原理和機制。 2、本管理中心安裝、設定和維護本管理中心系統操作程序。 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、產製和備份本管理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、本管理中心安全原理和機制。 2、本管理中心系統軟硬體的使用及操作程序。 3、憑證簽發操作程序。 4、憑證廢止操作程序。 5、災後復原以及業務永續經營之程序。
稽核員	1、本管理中心安全原理和機制。 2、本管理中心系統軟硬體的使用及操作程序。 3、產製和備份本管理中心之金鑰操作程序。 4、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

本管理中心的每一位相關工作人員，要熟悉本管理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

本管理中心之相關人員，如違反憑證政策與本作業基準或其他本管理中心公布之程序，將接受適當的管理與懲處，如情節重大而造成損害者，將採取法律行動追究其責任。

5.3.7 聘雇人員之規定

本管理中心聘僱人員安全要求遵照 5.3 節規定。

5.3.8 提供給人員之文件資料

本管理中心提供憑證政策、本作業基準、本管理中心系統操作手

冊及我國電子簽章法及其施行細則等文件給本管理中心之相關人員。

6. 技術安全控管

本章描述由本管理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

本管理中心依照 6.2.1 節規定，於硬體密碼模組內產製金鑰對，採依照 NIST FIPS 140-2 規範之演算法與流程，私密金鑰之匯出與匯入應依照 6.2.2 與 6.2.6 節規定辦理。

本管理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

由註冊中心代用戶產製金鑰對或用戶自行產製金鑰對。

6.1.2 將私密金鑰傳送給憑證用戶

如用戶金鑰由註冊中心代為產製時，註冊中心將於簽發憑證後，透過註冊窗口將含有用戶私密金鑰的符記(例如 IC 卡)交予用戶。

6.1.3 將用戶之公開金鑰傳送給憑證機構

如註冊中心代用戶產製金鑰時，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 將憑證機構之公開金鑰傳送給信賴憑證者

本管理中心本身之公鑰憑證由中華電信憑證總管理中心簽發，公布在本管理中心的儲存庫上，而讓用戶及信賴憑證者直接做下載及安裝。信賴憑證者在使用本管理中心本身之公鑰憑證前必須依照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本管理中心本身之公鑰憑證的簽章，以確保公鑰憑證中之公開金鑰是可信賴的。

6.1.5 金鑰長度

本管理中心使用金鑰長度2048位元的RSA金鑰以及SHA-1、SHA-256雜湊函數演算法簽發憑證。

到民國102年12月31日(含) 之前，用戶至少必須使用1024 位元的RSA金鑰或安全強度相當的其他種類金鑰(例如ECC 161位元)。

到民國119年12月31日(含)之前，用戶必須使用RSA 2048 位元金鑰或安全強度相當的其他種類金鑰(例如ECC 224位元）。

民國119年12月31日以後，用戶應使用RSA 3072 位元金鑰或安全強度相當的其他種類金鑰(例如ECC 256位元)。

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

本管理中心簽章用金鑰對採用NIST FIPS 140-2之規範產生RSA演算法中所需的質數，並確保該質數為強質數(Strong Prime)。

用戶金鑰可於IC卡內部或其他軟硬體密碼模組產生RSA演算法中所需的質數，但不保證該質數為強質數。

6.1.8 金鑰經軟體或硬體產製

本管理中心及其用戶使用 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。

6.1.9 金鑰之使用目的

本管理中心簽章用私密金鑰用於簽發憑證、憑證廢止清冊。

用戶金鑰對數目為一對，此金鑰對具有為簽章用及加密用的兩種用途。

6.2 私密金鑰保護

6.2.1 密碼模組標準

本管理中心使用通過FIPS 140-2 Level 3認證之硬體密碼模組。

用戶金鑰對之儲存媒體為符合ISO 7816的IC卡或其他載具。

6.2.2 金鑰分持之多人控管

對本管理中心私密金鑰備份的持份之安全控管，將以m-out-of-n金鑰分持方式來做本管理中心私密金鑰的備份及回復。

用戶私密金鑰之多人控管不另做規定。

6.2.3 私密金鑰託管

本管理中心簽章用私密金鑰不被託管，本管理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本管理中心私密金鑰，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

本管理中心簽章用私密金鑰不被歸檔，但會以憑證的資料方式依照 4.6 節執行相對公鑰的歸檔。

6.2.6 私密金鑰輸入密碼模組

本管理中心在下述情況時做私密金鑰輸入密碼模組中：

(1)金鑰產製及更換密碼模組時。

(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)的方式來做本管理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。

（3）更換密碼模組時，私密金鑰輸入方式採加密方式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。

6.2.7 私密金鑰啟動方式

本管理中心之私密金鑰之啟動是由多人控管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。

用戶之私密金鑰啟動方式，不另做規定。

6.2.8 私密金鑰停用方式

本管理中心之私密金鑰採6.2.2節多人控管方法方式將私密金鑰停用。

本管理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

為避免舊的本管理中心私密金鑰被盜用，妨害整個憑證之真確性，本管理中心金鑰生命週期到期時其私密金鑰必須加以銷毀，因此，當本管理中心完成金鑰更新及簽發新的本管理中心憑證，且不再簽發任何憑證與憑證廢止清冊之後(參照4.7節)，將會把存在硬體密碼模組內舊的本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本管理中心私密金鑰。

而除了銷毀硬體密碼模組中舊的本管理中心私密金鑰外，該私密金鑰的金鑰備援的秘密持份IC卡也會在本管理中心金鑰更新的同時進行實體銷毀。

如果一個金鑰儲存模組已經將被永久的不再提供服務，但還是可以被取得時(accessible)，則儲存在這個安全模組中的所有私密金鑰(含已經有使用過或是可能要被使用的)，都將要被銷毀。銷毀該密碼模組中的金鑰後，必須再使用該密碼模組所提供的金鑰管理工具加以檢視，以確認是否上述所有的金鑰都已經不存在。

如果一個金鑰儲存密碼模組已經將被永久的不再提供服務，則儲存在這個安全模組中已經有使用過的所有私密金鑰，都將要被自此安全模組中刪除(erased)。

用戶之私密金鑰銷毀方式，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，本管理中心不負責保管用戶的私密金鑰。

6.3.1 公開金鑰之歸檔

本管理中心將進行用戶憑證之歸檔，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 本管理中心公開金鑰及私密金鑰之使用期限

本管理中心之公鑰及私鑰金鑰長度為RSA 2048 bits，私密金鑰與公鑰憑證使用期限至多20年，但以私密金鑰做為簽發憑證用途之使用期限至多為10年。

6.3.2.2 用戶公鑰及私鑰之使用期限

本管理中心用戶之公鑰及私鑰金鑰長度為1024位元或2048位元。當金鑰長度為1024位元時，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；當金鑰長度為2048位元時，私密金鑰之使用期限至多為10年，公鑰憑證之有效期限至多為10年。1024位元憑證原則上至多使用至民國102年12月31日止。

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

本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

本管理中心和其相關輔助系統透過作業系統，或結合作業系統、軟體和實體的保護措施提供下列電腦安全功能。

(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

本管理中心憑證伺服器採用通過 Common Criteria EAL 3 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

本管理中心的系統研發遵循 CMMI 的規範進行品質控管。

對於註冊中心之硬體和軟體，必須在初次使用時檢查是否有惡意程式碼並定期掃瞄。

系統開發環境與測試環境、上線環境應有所區隔。

系統研發單位應善盡良善管理責任，簽署安全遵循保證書確保無後門或惡意程式，並提供程式或硬體交付清單、測試報告與管理手冊、版本控管給本管理中心。

6.6.2 安全管理控管措施

本管理中心的軟體在首次安裝時，將確認是由供應商提供正確的版本且未被修改。

本管理中心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。

本管理中心將記錄和控管系統的組態及任何修正與功能提升，同時偵測未經許可修改系統之軟體或組態。

本管理中心在風險評鑑、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 CA ＆ Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates 之方法論或規定。

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

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

本管理中心主機所簽發的憑證與憑證廢止清冊以數位簽章保護，自動從本管理中心主機傳送到外部儲存庫。

本管理中心之外部儲存庫透過系統修補程式的更新、系統弱點掃描、入侵偵測系統、防火牆系統及過濾路由器（Filtering Router）等加以保護，以防範阻絕服務和入侵等攻擊。

非屬本管理中心之私密金鑰的控管活動，在緊急狀況下得允許啟用諸如SSL VPN之機制進行問題偵測及狀況排除。SSL VPN之使用將被自動記錄於稽核主機中，並遵守6.6.2節之規定，SSL VPN稽核紀錄之審查由內部稽核員負責。

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

本管理中心所簽發的憑證會遵循 ITU-T X.509、CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates 及 IETF PKIX Working Group 的 5280 或其最新版相關的規定。

7.1.1 版本序號

本管理中心簽發 X.509 V3 版本的憑證。

7.1.2 憑證擴充欄位

本管理中心簽發的憑證之憑證擴充欄位會遵循 ITU-T X.509、CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates 及 PKIX Working Group 的 5280 或其最新版相關之規定。

7.1.3 演算法物件識別碼

本管理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)：

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

(OID：1.2.840.113549.1.1.11)

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

(OID：1.2.840.113549.1.1.12)

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

(OID：1.2.840.113549.1.1.13)

本管理中心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 ITU-T X.509、CA/Browser Forum Baseline Requirementsfor the Issuance and Management of Publicly-Trusted Certificates 及 IETF PKIX Working Group 的 5280 或其最新版相關的規定。

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

本管理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

本管理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

本管理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

本管理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

本管理中心簽發 ITU-T 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

本管理中心簽發的憑證廢止清冊(CRL) 會遵照 ITU-T X.509、CA/Browser Forum Baseline Requirementsfor the Issuance and Management of Publicly-Trusted Certificates 及 IETF PKIX Working Group 的 5280 或其最新版相關之規定。

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，於本管理中心儲存庫公告 30 個日曆天，始得修訂。

(2) 影響程度小者，於本管理中心儲存庫公告 15 個日曆天，始得修訂。

8.1.2.2 通知機制

所有變更項目將公告於本管理中心儲存庫。

8.1.2.3 意見之回覆期限

對於變更項目有意見者，其回覆期限：

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

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

8.1.2.4 處理意見機制

對於變更項目有意見者，於意見回覆期限截止前，以本管理中心儲存庫公告之回覆方式傳送給本管理中心，本管理中心將考量相關意見，評估變更項目。

8.1.2.5 最後公告期限

本作業基準公告之變更項目依照 8.1.2.2 及 8.1.2.3 節規定進行修訂，公告期限依照 8.1.2.1 節規定至少公告 15 個日曆天，直到本作業基準修訂生效。

8.2 公告及通知之規定

本作業基準修訂後 7 個日曆天內公告於本管理中心儲存庫，本作業基準之修訂生效日期，除另有規定外，於公告後生效。

8.3 憑證實務作業基準之審定程序

本作業基準經電子簽章法主管機關經濟部核定後，由本管理中心

公布。

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。