# HiPKI EV TLS 憑證管理中心

# 憑證實務作業基準

(HiPKI EV TLS Certification Authority Certification Practice Statement)

第 1.16 版

中華電信股份有限公司

中華民國 110 年 6 月 17 日

# 目　錄

## 文件修訂歷程

| 版次 | 發行日期 | 修訂摘要 |
|---|---|---|
| 1.0 | 2019 年 2 月 22 日 | 首次發行。 |
| 1.05 | 2020 年 3 月 2 日 | (1) 修訂第 2.2 節 CAA 名稱。<br>(2) 依據 CA/Browser Forum 投票案 SC13，新增第 3.2.5.6 與第 3.2.5.7 節。<br>(3) 依據 CA/Browser Forum 投票案 SC14 移除”和網域名稱聯絡人以電話接觸”之審驗方式。<br>(4) 依據 CA/Browser Forum 投票案 SC23，修訂第 4.9.10 節。<br>(5) 依據 RFC 3647 與營運現況，修訂第 5.3.7 節「約聘人員」用詞為「承攬商派駐人員」，並修訂安全規定。<br>(6) 依據 Baseline Requirements 第 1.6.7 版修訂第 1.5.2.1、第 3.2.5、第 4.2.1、第 4.9、第 4.10、第 7.1.2 及第 9.6 節。<br>(7) 修訂第 2.3、第 4.3.2、第 4.5.1、第 4.7.2、第 4.8.1、第 4.8.2、第 5.3.3、第 5.6 節、第 5.8、第 6.1.1、第 6.1.7、第 6.3.2、第 6.6.1、第 7.1.3、第 7.2.2、第 7.3.1、第 9.4.3、第 9.7、第 9.8 及第 9.12 節。 |
| 1.1 | 2020 年 7 月 2 日 | (1) 經濟部核定版本(涵蓋中華電信憑證政策管理委員會通過之第 1.0 與第 1.05 版)<br>(2) 修訂摘要、第 1.3.4、第 1.4.1、第 1.4.2、第 1.5.4、第 1.6.1、第 2.2、第 3.1.5、第 4.9.10 及第 9.9.1 節。 |
| 1.15 | 2021 年 4 月 13 日 | (1) 依據 BR 及 EV Guidelines 修訂第 3.1.2、第 3.2.5、第 4.2.2、第 5.5.2 及第 7.1.2 節。<br>(2) 修訂第 1.4.2 節、第 1.5.2.1、第 1.5.3、第 1.6.1、第 2.2、第 2.3、第 2.4、第 3.1.5、第 3.1.6、第 3.2.2.1、第 3.2.2.2、第 3.2.2.4、第 3.2.3.4、第 4.2.1.1、第 4.8.1、第 4.9.3、 |

| | | |
|---|---|---|
| | | 第 4.9.7、第 4.9.8、第 4.9.10、第 5.1.2、第 5.3.8、第 5.7、第 5.7.3、第 5.8、第 6.1.6、第 6.2.5、第 6.2.6、第 6.3.2、第 6.8、第 7.1.4.2、第 7.1.7、第 7.2.2、第 7.3.1、第 8.1、第 8.4、第 9.4.2、第 9.4.3、第 9.4.5、第 9.4.6、第 9.4.7、第 9.6.1、第 9.7、第 9.9.1、第 9.9.2、第 9.10、第 9.14、第 9.16.1 及第 9.16.5 節。 |
| 1.16 | 2021 年 6 月 17 日 | (1) 修訂第 1.6.1、第 3.1.2、第 3.2.4、第 3.2.5.4、第 3.5.3、第 4.3.1、第 4.9.1、第 4.9.12、第 5.4.8、第 6.7、第 7.1.4.2、第 9.5、第 9.6.1、第 9.6.3 及第 9.12.1 節。<br>(2) 2021-08-01 生效，TLS/SSL 憑證禁用組織單位名稱 (organizationalUnitName, OU)欄位。<br>(3) 依據 CA/Browser Forum 投票案 SC44 與 SC42，修訂第 3.2.5.4 與第 3.5.3 節。 |

# 摘要

HiPKI EV TLS 憑證管理中心(簡稱本管理中心)憑證實務作業基準(簡稱本作業基準)之重要事項說明如下：(依據電子簽章法第 11 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)

一、主管機關核定文號：經商字第　號

二、所簽發的憑證種類：

延伸驗證型(Extended Validation, EV) TLS/SSL 憑證。

簽發的對象為私人組織(Private Organization)、政府機關(構)、非營利國際組織與其他商業團體(Business Entity)所擁有的應用軟體(如 Web Server、e-mail Server、Application Server 或 Lync Server 等)或電腦及通訊設備(如路由器、防火牆、資料庫安全稽核硬體等)。

三、憑證等級：延伸驗證等級

HiPKI EV TLS 憑證管理中心依據 HiPKI 憑證政策及 CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates 之相關規定運作，依據申請憑證的身分鑑別程序簽發 EV TLS/SSL 憑證(參見第 1.4.1 節)。

四、應用範圍：

本管理中心所簽發的 EV TLS/SSL 憑證，適用於電子商務、電子化政府網路交易或金融交易所需的身分識別及資料保護，尤其是惡意行為(例如：網路詐騙、個資外洩、機密外洩)發生風險機率高的網路交易。

本管理中心的用戶(Subscriber)及相關信賴憑證者(Relying Party)，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、相關法律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(Registration Authority)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、相關法律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. 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。

4. 財務責任

本管理中心以本公司為財務擔保；本管理中心財務依相關法律規定辦理財務稽核。本公司已投保最高賠償金額為新台幣 120,000,000 元的一般責任險，本公司財務健全，會計師查核簽證之年度財務報告顯示流動資產符合 EV SSL Certificate Guidelines 之要求超過 5 億元美金，且流動資產與流動負債比符合不低於 1.0，具備若發生損害時足夠的賠償能力。

5. 用戶責任

用戶應妥善保管及使用其私密金鑰。用戶之憑證如須廢止或辦理重發，應遵守本作業基準第 4 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方，就 HiPKI EV TLS 憑證管理中心的運作進行稽核。稽核採用的標準為 WebTrust Principles and Criteria for Certification Authorities(簡稱 WebTrust for CA)、WebTrust Principles and Criteria for Certification Authorities－SSL Baseline with Network Security(簡稱 WebTrust for CA – SSL BR)及 WebTrust Principles and Criteria for Certification Authorities－Extended Validation SSL(簡稱 WebTrust for CA – EV SSL)。

# 1 序論

## 1.1 概要

### 1.1.1 憑證實務作業基準

HiPKI EV TLS 憑證管理中心(HiPKI EV TLS Certification Authority，簡稱本管理中心)憑證實務作業基準(Certification Practice Statement，簡稱本作業基準)係依據 HiPKI 憑證政策(HiPKI Certificate Policy)所訂定，並遵循

(1) 電子簽章法

(2) 及其子法「憑證實務作業基準應載明事項準則」

之相關規定及國際標準如：

(1) 網際網路工程任務小組(Internet Engineering Task Force, IETF)徵求修正意見書(Request for Comments, RFC) 3647 與 RFC 5280

(2) ITU-T X.509

(3) 憑證機構與瀏覽器論壇(CA/Browser Forum, http://www.cabforum.org)發行之 Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates(簡稱 Baseline Requirements)、Guidelines for the Issuance and Management of Extended Validation Certificates(簡稱 EV SSL Certificate Guidelines)及 Network and Certificate System Security Requirements

所訂定之政策文件，以做為本管理中心訂定憑證實務作業基準之依循。

依據 HiPKI 憑證政策的規定，HiPKI 憑證總管理中心(HiPKI Root Certification Authority, HiPKI RCA)為 HiPKI(簡稱本基礎建設)之最頂層憑證管理中心與信賴根源(Trust Anchor)，具備最高的公信度，信賴憑證者(Relying Party)可直接信賴 HiPKI RCA 的憑證。本管理中心是 HiPKI RCA 的第 1 層下屬憑證機構(Level 1 Subordinate CA)，由 HiPKI RCA 簽發憑證予本管理中心，在本基礎建設中負責簽發及管理延伸驗證型

(Extended Validation, EV) TLS/SSL 憑證。SSL(Secure Sockets Layer)協定已由 TLS(Transport Layer Security)協定取代，因 SSL 憑證與 TLS 憑證指的是同樣可以讓 TLS 協定運作的憑證，而且漸漸有以 TLS 憑證取代廣泛使用的 SSL 憑證稱呼，為避免混淆，本作業基準多數地方會以 TLS/SSL 憑證表示。

EV TLS/SSL 憑證其主要目的為：

(1) 確認法律實體控制某網站：提供合理的保證給網際網路瀏覽器的用戶(Subscribers)其所存取的網站是由特定的法律實體所控制並經由 EV TLS/SSL 憑證確認其名稱、營業地點(Place of Business)、管轄或註冊區域和註冊號碼與其他意義清楚的資訊。

(2) 促成和網站之加密通信：協助加密金鑰的交換以促成瀏覽器和網站間傳輸的資訊之加密。

EV TLS/SSL 憑證的次要目的是幫助組織建立其營運網站的合法性，並提供 1 種可以用來協助解決與網路釣魚以及其他形式的網路身分詐欺的問題之工具。透過提供更可靠的第三方驗證的身分和有關組織的地址資訊，EV TLS/SSL 憑證可以幫助：

(1) 難以進行網路釣魚與網路身分詐欺攻擊;

(2) 協助可能是網路釣魚攻擊或網路身分詐欺的目標的組織，為他們提供 1 個工具，以更好地讓用戶確認組織的身分;和

(3) 協助執法機構在網路釣魚和其他網路身分詐欺的調查，包括在適當情況下，接觸、調查或採取對憑證主體(Subject)的法律行動。

### 1.1.2 憑證實務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本管理中心、註冊中心(Registration Authority)、用戶及信賴憑證者等。

## 1.2 文件名稱及識別

本文件的名稱為 HiPKI EV TLS 憑證管理中心憑證實務作業基準，發行日期為中華民國 110 年 6 月 17 日。本作業基準之最新版本可在以下網頁取得：https://tls.hinet.net。

本憑證管理中心所簽發之EV TLS/SSL 憑證符合EV SSL Certificate Guidelines，並和應用軟體供應商(Application Software Suppliers，如瀏覽器或作業系統廠商)個別商議其所支援之憑證處置方式，使用憑證機構與瀏覽器論壇之 EV TLS/SSL 憑證政策物件識別碼({joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) ev-guidelines (1) }(2.23.140.1.1))。若有憑證機構與瀏覽器論壇相關文件未規範處，則依照 HiPKI 憑證政策之保證等級第 3 級運作。

若有任何本作業基準在 EV TLS/SSL 憑證簽發上與 EV SSL Certificate Guidelines 及 Baseline Requirements 之規定有任何不一致的情形,將優先遵循 EV SSL Certificate Guidelines 及 Baseline Requirements 的條款。

## 1.3 主要成員

本憑證機構之主要成員包括：

(1) HiPKI EV TLS 憑證管理中心

(2) 註冊中心

(3) 用戶

(4) 信賴憑證者

### 1.3.1 憑證機構

HiPKI EV TLS 憑證管理中心，由中華電信股份有限公司(簡稱本公司)負責建置及營運，依照 HiPKI 憑證政策之規定運作及簽發 EV TLS/SSL 憑證。

### 1.3.2 註冊中心

註冊中心負責蒐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)，負責受理本管理中心 EV TLS/SSL 憑證申請、廢止、憑證之更換金鑰、憑證變更等作業。

本管理中心不允許委派第三方(Delegated Third Parties)擔任註冊審

驗窗口審驗網域名稱或 IP 位址之擁有權或控制權，委派第三方係指非本管理中心、受委託協助憑證管理流程的自然人或法人，且不在本管理中心外稽範圍內。

### 1.3.3 用戶

向本管理中心申請憑證，而尚未完成憑證簽發作業程序的私人組織(Private Organization)、政府機關(構)、非營利國際組織或其他商業團體，稱為申請者(Applicant)，用戶係指已申請並取得本管理中心核發 EV TLS/SSL 憑證之個體，其與憑證主體之關係如下表所示：

| 憑證主體 | 用戶 |
|---|---|
| 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第 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，用戶本身不簽發憑證給其他方。

### 1.3.4 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的個體。信賴憑證者必須依照相對的憑證機構憑證(CA Certificate)及憑證狀態資訊，以驗證所收到憑證的有效性。在確認憑證的有效性後，才可使用憑證進行以下作業：

(1) 識別用戶名稱及其延伸驗證資訊。

(2) 識別用戶擁有的或控制的完全吻合網域名稱。

(3) 與憑證主體間建立安全之通訊管道。

### 1.3.5 其他相關成員

若本管理中心有選擇其他相關提供信賴服務機構做為協同運作的夥伴，會於網站揭露並於本作業基準中訂定相互運作機制及彼此的權利與義務關係，以確保本管理中心服務品質的有效及可靠。

# 1.4 憑證用途

## 1.4.1 憑證之適用範圍

本管理中心簽發 HiPKI 憑證政策所定義之 EV TLS/SSL 憑證(含簽章及加密用的憑證)，可應用於傳輸層安全(Transport Layer Security, TLS)通訊協定的伺服器應用軟體。簽發的憑證種類有單網域 EV TLS/SSL 憑證及多網域 EV TLS/SSL 憑證。

本作業基準對於 EV TLS/SSL 憑證，其適用範圍之說明如下：

| 憑證類別 | 適用範圍 |
|---|---|
| 延伸驗證型 | • 通訊管道之加密及保護<br>• 鑑別網域名稱擁有者屬於哪一個組織<br>• 瀏覽器網址列標示綠色底，並直接顯示憑證的主體之組織資訊方便訪客識別<br>• 適合下列應用範圍：<br>(1)電子商務<br>(2)電子化政府 |

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。

用戶應依據實際需求與應用環境，選擇合適的憑證類別。用戶在使用私密金鑰時，應選擇安全及可信賴的電腦環境及應用系統，以避免私密金鑰被盜取，導致權益受損。

信賴憑證者必須依照第 6.1.7 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 ITU-T X.509 標準或 RFC 5280 等)定義之憑證驗證(Certificate Validation)方法來驗證憑證的有效性。

## 1.4.2 憑證之禁用範圍

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)TLS 流量中間人攔截(man-in-the-middle TLS traffic interception)

# 1.5 政策管理

## 1.5.1 憑證實務作業基準之管理機構

中華電信股份有限公司。

## 1.5.2 聯絡資料

### 1.5.2.1 憑證實務作業基準建議

對本作業基準有疑義需要諮詢，或有修訂建議，請利用以下資訊與本管理中心聯繫：

聯絡電話：886 2-2344-4820

郵遞地址：10048 台北市信義路一段 21 號數據通信大樓 4F
HiPKI EV TLS 憑證管理中心

電子郵件信箱：caservice@cht.com.tw。

也可至 https://tls.hinet.net/查詢聯絡資料。

### 1.5.2.2 憑證問題報告

用戶、信賴憑證者、應用軟體供應商以及其他第三方組織於發現私密金鑰遺失、疑似私密金鑰遭破解、憑證遭誤用、或是憑證被偽造、破解、濫用等情況時(包含工作日以外時間)，可寄送電子郵件至 report_abuse@cht.com.tw 向本管理中心提出憑證問題報告(Certificate Problem Report)。

相關說明請參見第 4.9.3 及第 4.9.5 節，由本管理中心決定是否廢止該憑證。

## 1.5.3 憑證實務作業基準之審定

本管理中心於檢查本作業基準是否符合本基礎建設的憑證政策相關規定後，送中華電信憑證政策管理委員會(Chunghwa Telecom

Certificate Policy Management Authority，簡稱政策管理委員會)進行審查及核定。

另依據中華民國電子簽章法規定，憑證機構訂定之憑證實務作業基準，必須經主管機關經濟部核定後，始得對外提供簽發憑證服務。

本憑證管理中心定期自行稽核，以證明遵照引用於憑證政策之保證等級進行營運。為使本管理中心所發之憑證順暢運作於各作業系統、瀏覽器與軟體平台，本基礎建設已經申請參與各作業系統、瀏覽器與軟體平台之根憑證計畫(Root Certificate Program)，將 HiPKI RCA 之自簽憑證廣泛部署於各軟體平台之憑證機構信賴清單(CA Trust List)。

依據根憑證計畫之規定，採連續不中斷涵蓋整個公開金鑰基礎建設之原則，每年併同 HiPKI RCA 執行外部稽核並將最新之憑證實務作業基準與外部稽核的結果提供給各大根憑證計畫，並維護稽核標章公告於本管理中心網站。

### 1.5.4 憑證實務作業基準核准程序

本作業基準經政策管理委員會及電子簽章法主管機關經濟部核定後，由本管理中心公布。如憑證政策的修訂公告後，本作業基準將配合修訂，先送政策管理委員會審查後，再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，如修訂之版本與原本作業基準有所牴觸時，以修訂之版本為準。

## 1.6 名詞定義及縮寫

### 1.6.1 名詞定義

| 中/英文名詞 | 定義 |
|---|---|
| 存取(Access) | 運用系統資源處理資訊的能力。 |
| 存取控制<br>(Access Control) | 對於授權的使用者、程式、程序或其他系統給予資訊系統資源存取權限的處理過程。 |
| 啟動資料<br>(Activation Data) | 在存取密碼模組時(例如用來開啟私密金鑰以進行簽章或解密)，除金鑰外所需及應受保護之隱密資料。 |

| | |
|---|---|
| 申請者<br>(Applicant) | 向憑證機構申請憑證，而尚未完成憑證簽發作業程序的用戶。 |
| 應用軟體供應商<br>(Application Software Suppliers) | 顯示或使用憑證與根憑證的網際網路瀏覽器軟體或其他倚賴方的應用程式的供應商。 |
| 歸檔<br>(Archive) | 實體上(與主要資料存放處)分隔的長期資料儲存處，可用來支援稽核服務、可用性服務或完整性服務等用途。 |
| 保證<br>(Assurance) | 據以信賴該個體已符合特定安全要件之基礎。[憑證實務作業基準應載明事項準則第 2 條第 1 款] |
| 保證等級<br>(Assurance Level) | 具相對性保證層級中之某 1 級數。[憑證實務作業基準應載明事項準則第 2 條第 2 款] |
| 稽核<br>(Audit) | 評估系統控制的是否恰當、確保符合既定的政策及營運程序、並對現有的控制、政策及程序建議必要的改善而進行的獨立檢閱及調查。 |
| 鑑別(Authenticate) | 當某個體出示身分時，確認其身分之正確性。 |
| 鑑別程序<br>(Authentication) | (1)建立使用者到資訊系統身分信賴程度的程序。[NIST.SP.800-63-2 Electronic Authentication Guideline]<br>(2)用以建立資料傳送之安全措施，或是驗證個人接收特定種類資訊權限之方法。<br>(3)鑑別是身分的證明程序。[A Guide to Understanding Identification and Authentication in Trusted Systems]<br>而所謂的相互鑑別(Mutual Authentication)是指在進行通訊活動的兩方彼此進行鑑別。 |
| 憑證機構資訊存取<br>(Authority Information Access, AIA) | 記載有關存取憑證機構資訊的擴充欄位，內容可包含：線上憑證狀態協定(OCSP)回應伺服器的服務位址，以及憑證簽發機構之憑證驗證路徑的下載位址等。 |
| 經授權網域名稱<br>(Authorization Domain Name) | 用於取得對某一個特定完全吻合網域名稱(FQDN)之憑證簽發的授權之網域名稱。<br>憑證機構可使用網域名稱服務別名紀錄查詢 |

| | |
|---|---|
| | 服務(DNS CNAME lookup)所回覆之 FQDN 當作 FQDN，用來達到網域驗證的目的。如果 FQDN 包含萬用字元，則憑證機構必須從被請求之 FQDN 的最左邊移除所有萬用字元。憑證機構可從左至右刪除零個或多個標籤(label)直到遇到基礎網域名稱，也可使用任何在這個過程中的值來達到網域驗證的目的。 |
| 備份(Backup) | 將資料或程式複製，必要時可供復原之用。 |
| 基礎網域名稱<br>(Base Domain Name) | 申請的 FQDN 之一部分，是除了第一個網域名稱節點外，剩下的註冊表控制(registry-controlled)或公開字尾(public suffix)左邊第一個網域名稱節點加上註冊表控制(registry-controlled)或公開字尾(例如「example.co.uk」或「example.com」)。FQDN 最右邊之網域名稱節點(domain name node)，在其註冊協議(registry agreement)有 ICANN 規格 13(ICANN Specification 13)的通用頂級網域名稱(gTLD)，則通用頂級網域名稱本身可以當做基礎網域名稱。 |
| 連結、繫結(Binding) | 將兩個相關的資訊元素做連結(結合)的過程。 |
| 其他商業團體<br>(Business Entity) | 私人組織、政府機關或非商業性團體以外的其他商業團體。例如：包含(但不限於)合夥、非法人社團及獨資。 |
| 憑證機構憑證<br>(CA Certificate) | 簽發給憑證機構的憑證。 |
| 憑證機構金鑰對<br>(CA Key Pair) | 其公開金鑰資訊被記載於一個或多個根憑證機構憑證與/或下屬憑證機構憑證之主體公開金鑰欄位的金鑰對。 |
| 能力成熟度模型整合<br>(Capability Maturity Model Integration, CMMI) | 由美國卡內基美隆大學(Carnegie Mellon University)的軟體工程研究所(Software Engineering Institute)自 CMM 之後提出的修訂版本。CMMI 模型能為開發或改進用於達成一個組織的商業目標的過程提供指導，其目的是協助提升組織的績效。 |

| | |
|---|---|
| 憑證<br>(Certificate) | (1)指載有簽章驗證資料，用以確認簽署人身分、資格之電子形式證明。[電子簽章法第 2 條第 6 款]<br>(2)資訊之數位呈現，內容至少包括：<br>a. 簽發的憑證機構。<br>b. 用戶之名稱或身分。<br>c. 用戶的公開金鑰。<br>d. 憑證之有效期間。<br>e. 憑證機構數位簽章。<br>在本作業基準中所提及的「憑證」特別指其格式為 ITU-T X.509 v.3，且在其「憑證政策」欄位中明確地引用憑證政策之物件識別碼的憑證。 |
| 憑證遞件核准者<br>(Certificate Approver) | 憑證遞件核准者應為自然人，屬申請者、申請者所聘雇之員工，或有權代表申請者進行意思表示之授權代理人：(i)擔任憑證請求者和授權其他員工或第三方擔任憑證請求者(ii)核准其他憑證請求者所提交之 EV TLS/SSL 憑證申請。 |
| 憑證機構<br>(Certification Authority, CA) | (1)簽發憑證之機關、法人。[電子簽章法第 2 條第 5 款]<br>(2)為使用者所信任之權威機構，其業務為簽發並管理 ITU-T X.509 格式之公開金鑰憑證及憑證機構廢止清冊或憑證廢止清冊。 |
| 授權憑證機構簽發憑證(Certification Authority Authorization, CAA) | CAA 網域名稱系統資源紀錄(DNS Resource Record)允許網域名稱系統之網域名稱擁有者指定憑證機構(一個或多個)取得授權幫該網域簽發憑證。CAA 網域名稱系統資源紀錄允許公眾信賴之憑證機構實施額外之控制降低非預期之憑證誤發的風險。[RFC 8659] |
| 憑證機構廢止清冊<br>(Certification Authority Revocation List, CARL) | 可供信賴憑證者查詢用之已廢止憑證清單，該清單中記載在到期日前被廢止之憑證機構憑證(包括自發憑證、下屬憑證機構憑證或交互憑證)及廢止時間與原因等資訊，由簽發憑證之根憑證機構以數位簽章的方式確保其完整性與不可否認性。 |

| | |
|---|---|
| 憑證政策<br>(Certificate Policy, CP) | (1)某 1 憑證所適用之對象或情況所列舉之 1 套規則，該對象或情況可為特定之社群或具共同安全需求之應用。[憑證實務作業基準應載明事項準則第 2 條第 3 款]<br>(2)憑證政策係為透過憑證管理執行的電子交易所訂定之具專門格式的管理政策。憑證政策中包括與數位憑證相關之生成、產製、傳送、稽核、被破解後的復原以及其管理等各項議題。憑證政策亦可間接地控制運用憑證之安全系統，以保護通訊系統所進行的交易。藉由控制關鍵的憑證擴充欄位方式，憑證政策及其相關技術可提供特定應用所需的安全服務。 |
| 憑證實務作業基準<br>(Certification Practice Statement, CPS) | (1)由憑證機構對外公告，用以陳述憑證機構據以簽發憑證及處理其他認證業務之作業準則。[電子簽章法第 2 條第 7 款]<br>(2)宣告某憑證機構對憑證之作業程序(包括簽發、停用、廢止、展期及存取等)符合特定需求(敘明於憑證政策或其他服務契約中)之聲明。 |
| 憑證格式剖繪<br>(Certificate Profile) | 一組文件或檔案，其根據 Baseline Requirements 的第 7 章定義了對憑證內容與憑證擴充欄位的要求。例如，憑證實務作業基準中的某一章節內容或憑證機構軟體所使用的憑證模板文件。 |
| 憑證問題報告<br>(Certificate Problem Report) | 疑似金鑰遭破解、憑證遭誤用(misuse)或其他種類的詐騙、破解、濫用或與憑證相關的不當行為之投訴。 |
| 憑證金鑰更換<br>(Certificate Re-key) | 改變在密碼系統應用程式中所使用之金鑰對。通常必須藉由對新的公開金鑰簽發新的憑證來達成新的金鑰對替換的目的。 |
| 憑證展期<br>(Certificate Renewal) | 藉由簽發新的憑證，以延展原憑證內所連結資料有效性的程序。 |
| 憑證請求者<br>(Certificate Requester) | 憑證請求者應為自然人，屬申請者、申請者所聘雇之員工、有權代表申請者進行意思表示之授權代理人，或代表申請者填寫提交 EV |

| | |
|---|---|
| | TLS/SSL 憑證請求的第三方(例如：網際網路服務供應商(Internet Service Provider)或主機代管公司)。 |
| 憑證廢止<br>(Certificate Revocation) | 在憑證的有效期間內，提前終止憑證的運作。 |
| 憑證廢止清冊<br>(Certificate Revocation List, CRL) | 由憑證機構以數位方式簽署且會定期更新之已廢止憑證清冊，清冊中記載由此憑證機構所簽發且在到期日之前被廢止之憑證。 |
| 憑證透明化<br>(Certificate Transparency, CT) | 憑證透明化機制為一個公開監控與稽核網際網路上所有憑證的開放性架構(現階段以TLS/SSL 憑證為優先目標)，透過公開憑證的簽發與存在等資訊給網域所有者、憑證機構、以及網域使用者，供其判斷憑證是否被錯誤或惡意簽發；換言之，其目的係提供一個可用於監控 TLS/SSL 憑證機制與審核特定TLS/SSL 憑證的公開監控與資訊公開的環境，以遏止憑證相關威脅。憑證透明化機制，主要由憑證日誌、憑證監控者、以及憑證稽核者等三個要素所組成。 |
| 中華電信憑證政策管理委員會(Chunghwa Telecom Certificate Policy Managemet Authority，簡稱政策管理委員會) | 1 組織，其設立目的為：研議中華電信所經營之公開金鑰基礎建設其基礎建設憑證政策及電子憑證體系架構、審核下屬憑證機構與交互證認證憑證機構的互運申請及其他如審議憑證實務作業基準等電子憑證管理事項。 |
| 破解<br>(Compromise) | 資訊洩漏給未經授權的人士或違反資訊安全政策造成物件未經授權蓄意、非蓄意的洩漏、修改、毀壞或遺失。 |
| 機密性<br>(Confidentiality) | 資訊不會遭受未經授權的個體或程序獲知或取用。 |
| 確認者<br>(Confirming Person) | 在申請者的組織內負責針對有疑義的相關事實進行驗證與確認。 |
| 合約簽署者<br>(Contract Signer) | 申請者、申請者所聘雇之員工，或有權代表申請者進行意思表示之授權代理人，或有權代 |

| | |
|---|---|
| | 表申請者簽署用戶約定條款的自然人。 |
| 密碼模組 (Cryptographic Module) | 1 組硬體、軟體、韌體或前述的組合，用以執行密碼的邏輯或程序(包含密碼演算法)，並且被包含在此模組的密碼邊界之內。 |
| 活期存款帳戶 (Demand Deposit Account) | 在銀行或其他金融機構持有的存款帳戶，資金存放在此帳戶以支應付款需求。活期存款帳戶的主要目的是便於支票、銀行匯票、直接付款、電子資金轉帳等非現金付款。<br>活期存款帳戶在不同國家的使用方式各不相同，但通常被稱為一個股份帳戶(share draft account)、活期帳戶(current account)或支票帳戶(checking account)。 |
| 數位簽章 (Digital Signature) | 將電子文件以數學演算法或其他方式運算為一定長度之數位資料，以簽署人之私密金鑰對其加密，形成電子簽章，並得以公開金鑰加以驗證者。[電子簽章法第 2 條第 3 款] |
| 網域名稱聯絡人 (Domain Contact) | 於網域名稱服務 Start of Authority 紀錄(DNS SOA record)或是基礎網域名稱之 WHOIS 紀錄所列，或透過直接聯絡網域名稱受理註冊機構所得的網域名稱註冊者、技術聯絡人(Technical contact)、或管理聯絡人(Administrative contact)(或是在國碼頂級網域名稱(ccTLD)下對等的人員)。 |
| 網域名稱 (Domain Name) | 在網域名稱系統分配給 1 個節點(node)的標籤(label)。亦即轉換 IP 位址為人類容易記憶之文字名稱。 |
| 網域名稱註冊者 (Domain Name Registrant) | 有時被稱為網域名稱的擁有者(owner)，但更恰當的是表示某人或某實體被網域名稱受理註冊機構註冊為具有權利使用該網域名稱，亦即被網域名稱受理註冊機構或 WHOIS 列為「Registrant」之自然人或法人。 |
| 網域名稱受理註冊機構(Domain Name Registrar) | 接受以下三類團體贊助、支持或簽署協議：<br>(1)網際網路名稱和編號註冊中心(the Internet Corporation for Assigned Names and Numbers , ICANN), |

| | |
|---|---|
| | (2)國家級網域名稱註冊中心(national Domain Name authority/registry), 或<br>(3) 網路資訊中心( Network Information Center)及其加盟人、承包商、代表、繼承人或受讓人)，受理網域名稱註冊的實體(Entity)或自然人。 |
| 網域名稱系統 (Domain Name System, DNS) | 將網域名稱轉換為 IP 位址的網路服務。 |
| 網域名稱系統授權憑證機構簽發憑證聯絡人 (DNS CAA Email Contact) | Baseline Requirements A.1.1 節所定義之郵件地址。 |
| 網域名稱系統 TXT Record 聯絡人 (DNS TXT Record Email Contact) | Baseline Requirements A.2.1 節所定義之郵件地址。 |
| 憑證效期 (Duration) | 由「有效期限起始時間」(notBefore)及「有效期限截止時間」(notAfter)兩個子欄位所組成之憑證欄位。 |
| 電子商務(E-commerce) | 使用網路科技(特別是網際網路)以提供買賣貨物及相關服務。 |
| 終端個體憑證(End-Entity Certificate) | 簽發給終端個體的憑證。 |
| 企業 EV TLS/SSL 憑證(Enterprise EV TLS/SSL Certificate) | 由企業註冊中心授權憑證機構簽發的第三及較高域名級別的 EV TLS/SSL 憑證。 |
| 企業註冊中心 (Enterprise RA) | 經由憑證機構授權核發第三及較高域名級別(third and higher domain levels)的 EV TLS/SSL 憑證的註冊中心。 |
| 延伸驗證型 TLS/SSL 憑證(EV TLS/SSL Certificate) | 依據 EV SSL Certificate Guidelines 之規定，憑證的主體欄位必須記載經過驗證的資訊。 |
| 延伸驗證(Extended | EV SSL Certificate Guidelines 所定義之驗證程 |

| | |
|---|---|
| Validation, EV) | 序。 |
| EV 授權來源<br>(EV Authority) | 為憑證遞件核准者以外的發起者，透過向 EV 授權來源查證，可確認憑證遞件核准者在 EV TLS/SSL 憑證請求提出之前，已獲得憑證申請人明確授權其依據本準則規範提出憑證請求行動。 |
| 聯邦資訊處理標準<br>(Federal Information Processing Standards, FIPS) | 為美國聯邦政府制定除軍事機構外，所有政府機構及政府承包商所引用之資訊處理標準。其中密碼模組安全需求標準為 FIPS 第 140 號標準(簡稱 FIPS 140)，到 2016 年 12 月為止此標準的最新版本為 FIPS 140-2。FIPS 140 將密碼模組區分為 11 類需求範圍，而 FIPS 140-2 則定義了 4 個安全等級。 |
| 防火牆<br>(Firewall) | 符合近端(區域)安全政策而對網路之間做接取限制的閘道器。 |
| 完全吻合網域名稱<br>(Fully Qualified Domain Name, FQDN) | 1 種用於指定電腦在網域階層中確切位置的明確網域名稱。FQDN 包含主機名稱(服務名稱)與網域名稱兩部分。以 ourserver.ourdomain.com.tw 為例，ourserver 是主機名稱，ourdomain.com.tw 是網域名稱，其中 ourdomain 是第 3 層網域名稱，com 則是次級網域名稱(Second-Level Domain)，tw 則是國碼頂級網域名稱(Country Code Top-Level Domain, ccTLD)。FQDN 的開頭一定是主機名稱。<br>另以 www.ourdomain.com 為例，www 是主機名稱，ourdomain 是次級網域名稱，com 則是通用頂級網域名稱(Generic Top-Level Domain, gTLD)。 |
| 政府主管機關<br>(Government Agency) | 針對私人組織而言，在法人設立的管轄區域內，負責核准該私人機構合法設立之政府機關(例如：核發法人登記證書的政府機關)。針對其他商業團體而言，在其他商業團體的營業管轄範圍內，負責核准該其他商業團體登記之政府機關。針對政府機關而言，即負責頒布該政府機關合法設立之相關法律、法規或 |

| | |
|---|---|
| | 法律之政府機關。 |
| 高風險憑證請求<br>(High Risk Certificate Request) | 憑證機構標示參考由憑證機構維護的內部標準和資料庫審查其憑證請求，可包括用於網路釣魚或其他不正當使用之高風險的名稱，包含在先前被拒絕的憑證請求或廢止的憑證、Miller Smiles 網路釣魚列表(Miller Smiles phishing list)或 Google 的安全瀏覽列表(Google Safe Browsing list)，或憑證機構使用其本身的風險降低標準識別的名稱。 |
| HiPKI | 中華電信股份有限公司為推動電子化服務，依照 ITU-T X.509 標準建置的階層式公開金鑰基礎建設。 |
| HiPKI 憑證總管理中心(HiPKI Root Certification Authority, HiPKI RCA) | HiPKI 的根憑證機構(Root CA)，在此階層式公開金鑰基礎建設架構中屬於最頂層的憑證機構，其公開金鑰為信賴之起源。 |
| 識別<br>(Identification) | 識別是某使用者是誰(廣為週知)的陳述方式或表達方式。[A Guide to Understanding Identification and Authentication in Trusted Systems]<br>識別是指描述或宣稱某個當事人或個體的方式，例如透過使用者帳號、姓名或電子郵件。 |
| 法人登記機關<br>(Incorporating Agency) | 針對私人組織而言，在個體註冊的管轄區域內，負責核准該個體合法設立之政府機關(例如：核發登記證書的政府機關)。<br>針對政府機關(構)而言，即負責頒布該政府機關(構)合法設立之相關法律、法規或法律之政府機關。 |
| 申請者的獨立確認<br>(Independent Confirmation From Applicant) | 憑證機構根據 EV SSL Certificate Guidelines 規定或申請人約定，對收到的特定事實進行確認。 |
| 完整性<br>(Integrity) | 對資訊的保護，使其不受未經授權的修改或破壞。資訊從來源產製後，經傳送、儲存到最終被收受方接收的期間中都維持不被篡改的 |

| | |
|---|---|
| | 一種狀態。 |
| 國際組織(International Organization) | 1 個由章程文件(例如：1 個章程、條約、公約或類似的文件，或至少有兩個國家代表簽署的文件)創立的組織。 |
| 國際化網域名稱(Internationalized Domain Name, IDN) | 1 種網際網路網域名稱，至少包含 1 個特定語言的腳本(Script)或字母字元(Ahphabetic Character)，然後以 punycode 編碼，用於只接受 ASCII 字符串的網域名稱服務。 |
| 網際網路號碼分配機構(Internet Assigned Numbers Authority, IANA) | 負責管理國際網際網路中使用的 IP 位址、網域名稱及許多其它參數之組織。 |
| 網際網路工程任務小組(Internet Engineering Task Force, IETF) | 負責網際網路標準的開發和推動之組織，包含網際網路架構及操作，使得網際網路運作更順暢，官方網站位於 https://www.ietf.org/。 |
| 簽發憑證機構(Issuing CA) | 對於 1 張憑證而言，簽發該憑證的憑證機構即稱為該憑證的簽發憑證機構。簽發憑證機構可為根憑證機構或下屬憑證機構。 |
| 管轄區域(Jurisdiction of Incorporation) | 針對私人組織而言，為國家和州或省(如適用)或地方的組織，組織合法存在是經由向適當的政府機關或實體(例如：設立地點)申請。<br>針對政府機關而言，國家和州或省(如適用)的合法實體為依法設立。 |
| 金鑰破解(Key Compromise) | 私密金鑰被他人未經授權的使用或揭露。 |
| 金鑰託管(Key Escrow) | 依據用戶必須遵守的託管協議(或類似的契約)所規定，將用戶的私密金鑰進行存放。此託管協議的條款要求 1 個或 1 個以上的代理機構基於有益於用戶、雇主或另一方的前提下，擁有用戶加密用的私密金鑰。 |
| 金鑰對(Key Pair) | 兩把數學上有相關性的金鑰，具有下列特性：<br>(1)其中 1 把金鑰用來做訊息加密，而此加密訊息只有用成對關係的另 1 把金鑰可以解 |

| | |
|---|---|
| | 密。<br>(2)從其中 1 把金鑰要推算出另 1 把金鑰(從計算的角度而言)是不可行的。 |
| 法律實體<br>(Legal entity) | 依據 EV SSL Certificate guidelines 所允許的發證對象，分為以下四大類：(1)私人組織；(2)政府機關(構)；(3)非營利國際組織及(4)其他商業團體。 |
| 合法存在<br>(Legal Existence) | 為依法設立並且非終止、解散、或拋棄的私人組織、政府機關或其他商業團體。 |
| 執業律師<br>(Legal Practitioner) | 在 EV SSL Certificate Guidelines 裡描述的律師或公證人，並且能勝任呈現申請人的實際意見。 |
| (美國)國家標準和技術研究院(National Institute of Standards and Technology, NIST) | 官方網站在 http://www.nist.gov/，類似我國的經濟部國家標準檢驗局，其使命係促進美國的創新和產業競爭力，推動度量衡學、標準、技術以提高經濟安全並改善生活品質。其所制定之硬體密碼模組標準及驗證、金鑰安全評估報告或聯邦政府的公務員和承包商身分卡標準廣泛被參考或引用。 |
| 不可否認性(Non-Repudiation) | 公開金鑰機制所提供的技術性證據以支援不可否認之安全服務。<br>對資料傳送方提供傳送證明以及對資料收受方提供傳送方的身分之保證，因而兩方在事後皆無法否認曾經處理過此項資料。技術上的不可否認性是指對信賴憑證者而言，如果某個公開金鑰可用以驗核某個數位簽章，保證此簽章必定是由相對應的私密金鑰所簽署。在法律上，不可否認性是指建立私密簽章金鑰之擁有或控管機制。 |
| 物件識別碼(Object Identifier, OID) | (1)1 種以字母或數字組成之唯一識別碼，該識別碼必須依國際標準組織(ISO)所訂定之註冊標準加以註冊，並可被用以識別唯一與之對應之憑證政策；憑證政策修訂時，其物件識別碼不必然隨之變更。[憑證實務作業基準應載明事項準則第 2 條第 4 款] |

| | |
|---|---|
| | (2)向國際標準組織註冊的特別形式的識別碼，當提及某物件或物件類別時，可以引用此唯一的識別碼做辨識。例如在公開金鑰基礎架構中，可以此識別碼來指明使用的憑證政策及使用的密碼演算法。 |
| 線上憑證狀態協定<br>(Online Certificate Status Protocol, OCSP) | 線上憑證狀態協定是一種線上憑證檢查協定，使信賴憑證者應用軟體可決定某張憑證之狀態(例如已廢止、有效等)。 |
| 線上憑證狀態協定回應伺服器<br>(OCSP Responder) | 由憑證管理中心所授權維運的線上伺服器，並連接至其儲存庫(Repository)以處理憑證狀態查詢請求。 |
| 線上憑證狀態協定裝訂(OCSP Stapling) | 一種 TLS/SSL 憑證狀態請求擴充欄位(TLS Certificate Status Request extension)，可替代線上憑證狀態協定(OCSP)成為另一種檢查 X.509 憑證狀態的方法。<br>本方法在運作上，網站會事先向 OCSP 回應伺服器取得有「時間限制(例如兩小時)」的 OCSP Response 並暫存；接下來，在每一次的 TLS Handshake 的初始過程中，網站會將此暫存的 OCSP Response 傳送給用戶(通常為瀏覽器)，用戶只需驗證該 OCSP Response 的有效性而不用再向憑證機構發送 OCSP 請求，如此可避免用戶每次連結高流量 TLS 網站都需要向憑證機構詢問其 TLS/SSL 憑證狀態，因此減輕憑證機構的負擔。<br>此種機制藉由 TLS 網站轉發 OCSP 回應伺服器定期簽發之 TLS/SSL 憑證有效性訊息，也避免 OCSP 回應伺服器可能得知有哪些用戶嘗試瀏覽該 TLS 網站的隱私疑慮。 |
| 營業地點<br>(Place of Business) | 任何申請者進行商業活動的設施位置(例如：工廠、零售店、倉庫…等)。 |
| 代表人<br>(Principal Individual) | 代表人為私人組織、政府機關(構)或其他商業團體的業主、合夥人、管理成員、董事或職員，可以經由他們的職稱、員工、承包商或由實體或組織授權進行 EV TLS/SSL 憑證的請求、簽 |

| | |
|---|---|
| | 發和使用相關業務的代理人來辨識。 |
| 私密金鑰<br>(Private Key) | (1)在簽章金鑰對中，用以產生數位簽章的金鑰。<br>(2)在加解密金鑰對中，用以對機密資訊解密的金鑰。<br>在這兩種情境中，此金鑰皆須保密。 |
| 私人組織<br>(Private Organization) | 為非政府的法律實體(不論所有權為私有或上市)，經由向註冊機關或具有等同公司註冊的管轄機關備案申請設立的實體。 |
| 公開金鑰<br>(Public Key) | (1)在簽章金鑰對中，用以驗證數位簽章有效的金鑰。<br>(2)在加解密金鑰對中，用以對機密資訊加密的金鑰。<br>在這兩種情境中，此金鑰皆須(一般以數位憑證的形式)公開可得。 |
| 公開金鑰基礎建設<br>(Public Key Infrastructure, PKI) | 由法律、政策、規範、人員、設備、設施、技術、流程、稽核和服務所組成之集合，可用於管理憑證及金鑰對。 |
| 公開金鑰密碼學標準<br>(Public-Key Cryptography Standards, PKCS) | RSA 資訊安全公司旗下的 RSA 實驗室為促進公開金鑰技術的使用，所發展一系列的公開金鑰密碼編譯標準，廣為業界採用。 |
| 合格稽核業者<br>(Qualified Auditor) | 符合 EV SSL Certificate Guidelines 第 17.6 節及 Baseline Requirements 第 8.2 節規定之稽核資格要求，且與受稽方獨立的會計師事務所、法人或個人。 |
| 合格的政府資訊來源<br>(Qualified Government Information Source, QGIS) | 定期更新且現行公眾可取得、為了準確提供可被諮詢且一般被公認為可信賴的資料庫而設計且由政府機關維護，例如經濟部全國商工登記資料庫。資料的報告是根據法律規定，且虛假或誤導性的報告將被處以刑事或民事處罰。EV SSL Certificate Guidelines 不禁止使用第三方供應商從政府機關取得的資訊，如果這些第三方供應商是從政府機關直接取得 |

| | |
|---|---|
| | 資訊。 |
| 合格的政府稅收資訊來源(Qualified Government Tax Information Source, QTIS) | 合格的政府資訊來源，須具體包含與私人組織、其他商業團體或個人相關的稅收資訊。例如我國的財稅資料中心或美國的國稅局(IRS)。 |
| 合格的獨立資訊來源(Qualified Independent Information Source, QIIS) | 為定期更新和公眾可存取的的公開資料庫，其主要用途在於準確的提供資訊，並且一般被認為這樣的資訊是可靠的來源。是經常更新並且是公眾可存取的資料庫通常被為公認為某些特定資訊可信賴之來源。若憑證機構確定某個資料庫符合合格的獨立資訊來源：<br>1、 憑證服務業以外的產業依賴此資料庫提供準確的位置、聯絡資訊和其他資訊；和<br>2、 資料庫提供者至少每年更新 1 次其資料。<br>憑證機構應使用文件化的程序檢查資料庫的準確性並確保其資料可被接受，包括審查資料庫提供者的使用條款。 |
| 隨機值(Random Value) | 由憑證機構所指定提供給申請者具備至少 112 位元之亂度(熵，Entropy)的數值。 |
| 註冊機關(Registration Agency) | 負責登記個體營業設立或核准執照之營業資訊的政府機關，可能包含(但不限於)(1)公司申登機關(2)目的事業主管機關(例如：交通部)，或(3)監管機關(例如：金融監督管理委員會、國家通訊傳播委員會)。 |
| 註冊代理人(Registered Agent) | 為個人或實體：<br>(1)被授權代理申請人辦理業務和代表申請人行意思之表示；或<br>(2)在申請人的公司註冊管轄機關的官方記錄上，被指定為上述(1)的角色。 |
| 註冊辦事處(Registered Office) | 為組織記錄在註冊機關的官方地址，作為官方文件寄送和法律文書的收件地址。 |
| 註冊中心(Registration Authority, RA) | 通常為憑證機構一部分之個體，負責對憑證的主體做身分識別及鑑別，但不做憑證簽發。 |

| | |
|---|---|
| 註冊號碼<br>(Registration Number) | (1)由法人登記機關在私人組織的管轄區域分配給私人組織的唯一註冊編號。[EV SSL Certificate Guidelines]<br>(2)對於在我國登記之公司、其他商業團體，政府也有配發稅籍統一編號；對於我國政府設立之政府機關(構)，行政院人事行政總處有編配政府機關代碼，本管理中心皆視為註冊號碼。 |
| 受監管的金融機構<br>(Regulated Financial Institution) | 由政府、國家、州或省或地方當局進行監管、監督和檢查的金融機關。 |
| 信賴憑證者<br>(Relying Party) | 指信賴所收受之憑證者。[憑證實務作業基準應載明事項準則第 2 條第 6 款] |
| 儲存庫<br>(Repository) | (1)用以儲存與檢索憑證或其他憑證相關資訊之系統。[憑證實務作業基準應載明事項準則第 2 條第 7 款]<br>(2)包含憑證政策、憑證實務作業基準及憑證相關資訊的資料庫。 |
| 請求符記<br>(Request Token) | 由憑證機構指定之方式所導出之數值，繫結(bind)對於憑證請求之控制的展現。<br>請求符記應結合用於憑證請求之公開金鑰。<br>請求符記可包含時戳以指出何時產製。<br>請求符記可包含其他資訊以確保其唯一性。<br>包含時戳的請求符記應從產製的時間開始後 30 天之內有效。<br>包含時戳的請求符記如果其時戳是在未來則應視為無效。<br>沒有包含時戳的請求符記針對單一一次使用有效，憑證機構不應該在隨後的驗證重覆使用該請求符記。<br>此繫結至少要使用與簽章憑證請求檔強度相同之數位簽章演算法或密碼學雜湊函數演算法。 |
| 徵求修正意見書 | 由 IETF 發行的一系列備忘錄，包含網際網 |

| | |
|---|---|
| (Request for Comments, RFC) | 路、UNIX 和網際網路社群之標準、協定及程序等，並以編號排定。 |
| 保留 IP 位址(Reserved IP Addresses) | IANA 設定的 IPv4 與 IPv6 為保留的位址，參見 http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml 與 http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml。 |
| 安全插座層(Secure Sockets Layer, SSL) | 由網景公司(Netscape)推出 Web 瀏覽器時所提出的協定，可於傳輸層對網路通信進行加密，並確保傳送資料之完整性以及對於伺服器端與用戶端進行身分鑑別。<br>SSL 協定的優勢在於它與應用層協定(Application Layer Protocol)獨立無關。高階的應用層協定(例如：HTTP、FTP、Telnet 等)能透通地建立於 SSL 協定之上。SSL 協定在應用層協定通信之前就已經完成加密演算法、通信密鑰的協商以及伺服器認證工作。此協定之繼任者是傳輸層安全(Transport Layer Security, TLS)協定。 |
| 簽署權力來源 (Signing Authority) | 一位或多位被指定代表申請人行意思表示的憑證遞件核准者。 |
| 下屬憑證機構 (Subordinate CA) | 在階層架構的公開金鑰基礎建設中，憑證由另 1 個憑證機構所簽發，且其活動受限於此另 1 憑證機構的憑證機構。 |
| 用戶 (Subscriber) | 具下列特性之個體，包括(但不限於)個人、機構、應用程式或網路裝置：<br>(a) 憑證中所敘明之主體名稱<br>(b) 擁有與憑證中所載公開金鑰相對應之私密金鑰<br>(c) 本身不簽發憑證給其他方 |
| 威脅 (Threat) | 對資訊系統可能造成損害(包括損毀、揭露、惡意修改資料或拒絕服務)的任何狀況或事件，可分為內部威脅(Internal Threat) 及外部威脅(External Threat)。內部威脅是指利用授與之權限，透過資料的破壞、揭露、篡改或拒 |

| | |
|---|---|
| | 絕服務等方式造成對資訊系統的損害；外部威脅是指來自外部未經授權且對資訊系統具有潛在破壞能力(包括對資料的毀壞、篡改、洩漏，或是造成阻斷服務)的個體。 |
| 時戳<br>(Time-stamp) | 由可信賴的權威機構以數位方式簽署，證明某特定數位物件在某特別時間之存在。 |
| 傳輸層安全(Transport Layer Security, TLS) | 由 IETF 將 SSL 3.0 協定制定為 RFC 2246，並將其稱為 TLS 1.0 協定，後續於 RFC 5246 及 RFC 6176 更新版本，亦即 TLS 1.2 協定。2018 年 IETF 公告最新版本 RFC 8446，即 TLS 1.3 協定。 |
| 信賴清單<br>(Trust List) | 可信賴憑證之清單，信賴憑證者用以鑑別憑證。 |
| 可信賴憑證<br>(Trusted Certificate) | 為信賴憑證者所信賴且經由安全可靠之傳送方式取得的憑證。此類憑證中所包含的公開金鑰用於信賴路徑之起始，又稱為信賴起源。 |
| 不斷電系統<br>(Uninterrupted Power System, UPS) | 在電力異常(如停電、干擾或電湧)的情況下不間斷地提供負載設備後備電源，以維持諸如伺服器或交換機等關鍵設備或精密儀器的不間斷運作，防止運算數據遺失，通信網路中斷或儀器失去控制。 |
| 驗證<br>(Validation) | 憑證申請者的識別流程。「驗證」是「識別(identification)」的子集合，是指建立憑證申請者的身分背景之識別。[RFC 3647]。 |
| 會計師驗證信<br>(Verified Accountant Letter) | 為符合 EV SSL Certificate Guidelines 第 11.11.2 節規定的文件。 |
| 法律驗證意見書<br>(Verified Legal Opinion) | 為符合 EV SSL Certificate Guidelines 第 11.11.1 節規定的文件。 |
| 通信的驗證方法<br>(Verified Method of Communication) | 為憑證機構根據 EV SSL Certificate Guidelines 第 11.5 節規定，使用電話號碼、傳真號碼、電子郵件、或郵遞地址與申請人進行通信的一個可靠的確認方式。 |

| | |
|---|---|
| WebTrust | 加拿大會計師公會(Chartered Professional Accountants Canada, CPA Canada)針對憑證機構的 WebTrust Program 項目所制定的規範。加拿大會計師公會也是 WebTrust for CA 系列標章之管理單位。 |
| WHOIS | 透過 RFC 3912 的 WHOIS、RFC 7482 的 RDAP(Registry Data Access Protocol) 或 HTTPS 網站，向網域名稱受理註冊機構或註冊管理機構(Registry)直接擷取的資訊。 |
| 零值化<br>(Zeroize) | 清除電子式儲存資料之方法，藉由改變資料儲存以防止資料被復原。[FIPS 140-2] |

### 1.6.2 縮寫

| 英文縮寫 | 全稱 | 中文名詞或定義 |
|---|---|---|
| AIA | Authority Information Access | 憑證機構資訊存取，參見第 1.6.1 節。 |
| CA | Certification Authority | 憑證機構，參見第 1.6.1 節。 |
| CAA | Certification Authority Authorization | 授權憑證機構簽發憑證，參見第 1.6.1 節。 |
| CEO | Chief Executive Officer | 執行長 |
| CFO | Chief Financial Officer | 財務長 |
| CIO | Chief Information Officer | 資訊長 |
| CISO | Chief Information Security Officer | 資安長 |
| CMMI | Capability Maturity Model Integration | 能力成熟度模型整合，參見第 1.6.1 節。 |
| COO | Chief Operating Officer | 營運長 |
| CP | Certificate Policy | 憑證政策，參見第 1.6.1 節。 |

| 英文縮寫 | 全稱 | 中文名詞或定義 |
|---|---|---|
| CPS | Certification Practice Statement | 憑證實務作業基準，參見第 1.6.1 節。 |
| CRL | Certificate Revocation List | 憑證廢止清冊，參見第 1.6.1 節。 |
| CT | Certificate Transparency | 憑證透明化，參見第 1.6.1 節。 |
| DN | Distinguished Name | 唯一識別名稱。 |
| DNS | Domain Name System | 網域名稱系統，參見第 1.6.1 節。 |
| EE | End Entities | 終端個體，參見第 1.6.1 節。 |
| EV | Extended Validation | 延伸驗證，參見第 1.6.1 節。 |
| FIPS | (U.S. Government) Federal Information Processing Standard | (美國)聯邦資訊處理標準，參見第 1.6.1 節。 |
| FQDN | Fully Qualified Domain Name | 完全吻合網域名稱，參見第 1.6.1 節。 |
| HiPKI RCA | HiPKI Root Certification Authority | HiPKI 憑證總管理中心，參見第 1.6.1 節。 |
| IANA | Internet Assigned Numbers Authority | 網際網路號碼分配機構，參見第 1.6.1 節。 |
| IDN | Internationalized Domain Name | 國際化網域名稱，參見第 1.6.1 節。 |
| IETF | Internet Engineering Task Force | 網際網路工程任務小組，參見第 1.6.1 節。 |
| NIST | (U.S. Government) National Institute of Standards and Technology | (美國)國家標準和技術研究院，參見第 1.6.1 節。 |
| OCSP | Online Certificate Status | 線上憑證狀態協定，參見 |

| 英文縮寫 | 全稱 | 中文名詞或定義 |
|---|---|---|
| | Protocol | 第 1.6.1 節。 |
| OID | Object Identifier | 物件識別碼，參見第 1.6.1 節，參見第 1.6.1 節。 |
| PIN | Personal Identification Number | 個人識別碼。 |
| PKCS | Public Key Cryptography Standards | 公開金鑰密碼學標準，參見第 1.6.1 節。 |
| PKI | Public Key Infrastructure | 公開金鑰基礎建設，參見第 1.6.1 節。 |
| QGIS | Qualified Government Information Source | 合格的政府資訊來源，參見第 1.6.1 節。 |
| QIIS | Qualified Independent Information Source | 合格的獨立資訊來源，參見第 1.6.1 節。 |
| QTIS | Qualified Government Tax Information Source | 合格的政府稅收資訊來源，參見第 1.6.1 節。 |
| RA | Registration Authority | 註冊中心，參見第 1.6.1 節。 |
| RFC | Request for Comments | 徵求修正意見書，參見第 1.6.1 節。 |
| SSL | Secure Sockets Layer | 安全插座層，參見第 1.6.1 節。 |
| TLS | Transport Layer Security | 傳輸層安全，參見第 1.6.1 節。 |
| UPS | Uninterrupted Power System | 不斷電系統，參見第 1.6.1 節。 |
| UTC | Coordinated Universal Time | 世界協調時間。 |

| 中文簡稱 | 中文(英文)全稱 |
| --- | --- |
| 本管理中心 | HiPKI EV TLS 憑證管理中心(HiPKI EV TLS Certification Authority) |
| 本公司 | 中華電信股份有限公司 |
| 本作業基準 | 憑證實務作業基準(Certification Practice Statement) |
| 本基礎建設 | HiPKI |

# 2 公布及儲存庫之責任

## 2.1 儲存庫

本管理中心儲存庫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(Certificate Revocation List, CRL)、本作業基準及 HiPKI 憑證政策，並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://tls.hinet.net。如因故無法正常運作，將於 2 個日曆天內恢復正常運作。

## 2.2 憑證機構之資訊公布

本管理中心應負責將以下之資訊公布於其儲存庫：

(1) HiPKI 憑證政策及本作業基準

(2) 憑證廢止資訊

(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

(7) 最近 1 次之外部稽核結果(如第 8.6 節所述)

(8) 提供應用軟體供應商測試安裝由本管理中心所簽發有效、過期與廢止的 EV TLS/SSL 憑證之網址

(9) 授權憑證機構簽發憑證(Certification Authority Authorization, CAA)之簽發者網域名稱(Issuer Domain Name, 如第 4.2.1 節所述)，包括 pki.hinet.net 與 tls.hinet.net。

## 2.3 公布之時間或頻率

(1) 本管理中心每年檢視與更新本作業基準，版本變更摘要將記載於版本修訂履歷，本作業基準新版或修訂後之版本於收到主管機關核准公文後儘速於儲存庫公布。

(2) 本管理中心所遵循的 HiPKI 憑證政策，於政策管理委員會核定

後儘速公布於儲存庫。

(3) 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。

(4) 本管理中心本身之憑證，於接受上層之憑證管理中心簽發後 7 個日曆天內公布於儲存庫。

## 2.4 儲存庫之存取控制

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。

有關第 2.2 節本管理中心公布的資訊為公開之資訊，主要提供用戶與信賴憑證者查詢之用，因此開放提供唯讀的閱覽存取，但為保障儲存庫之安全，實施邏輯和實體的控制防止未經授權的寫入儲存庫。

# 3 識別及鑑別

## 3.1 命名

### 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)之命名應符合申請組織管轄國家之法律規定。

EV TLS/SSL 憑證之憑證主體名稱(Subject Name)與憑證主體別名(Subject Alternative Name)依照 Baseline Requirements 之規範，不得使用內部名稱(Internal Name)或保留 IP 位址(Reserved IP Addresses)。EV TLS/SSL 憑證之主體(Subject)名稱應包括第 3.2.2 節所驗證申請者之組織營業類別(OID 2.5.4.15)，若申請者之組織為私人組織時，則此營業類別須標註為「Private Organization」；若為政府機關(構)時，則須標註為「Government Entity」；若為其他商業團體(Business Entity)時，則須標註為「Business Entity」；若為非營利國際組織(Non-Commercial Entity(International))時，則須標註為「Non-Commercial Entity」)、申請者之組織機構註冊管轄區之國家代碼(OID 1.3.6.1.4.1.311.60.2.1.3)、申請者之組織機構登記營業地址之城市或鄉鎮名稱(localityName，OID 2.5.4.7)及申請者之組織身分資訊(存放於組織名稱(Organization)欄位(OID 2.5.4.11))。

根據 EV SSL Certificate Guidelines 第 9.2 節之規定，EV TLS/SSL 憑證欄位「主體」的內容又可細分為必要屬性、選擇性屬性以及不適用屬性，整理如下表：

表3-1：EV TLS/SSL憑證欄位「主體」之必要/選擇性/不適用屬性

| 憑證欄位屬性名稱 | 物件識別碼(OID) | 必要屬性 | 選擇性屬性 |
|---|---|---|---|
| 組織名稱(organizationName) | 2.5.4.10 | ● | |
| 一般名稱(commonName) | 2.5.4.3 | | ● |
| 營業類別(businessCategory) | 2.5.4.15 | ● | |
| 註冊之管轄區域的國家代碼(jurisdictionCountryName) | 1.3.6.1.4.1.311.60.2.1.3 | ● | |
| 註冊之管轄區域的州或省名(jurisdictionStateOrProvinceName) | 1.3.6.1.4.1.311.60.2.1.2 | | ● |
| 註冊之管轄區域的城市或鄉鎮名稱(jurisdictionLocalityName) | 1.3.6.1.4.1.311.60.2.1.1 | | ● |
| 識別代號(serialNumber) | 2.5.4.5 | ● | |
| 營業場所之實際地址的國家代碼(countryName) | 2.5.4.6 | ● | |
| 營業場所之實際地址的州或省名稱(stateOrProvinceName) | 2.5.4.8 | | ● |
| 營業場所之實際地址的城市或鄉鎮名稱(localityName) | 2.5.4.7 | ● | |
| 營業場所之實際地址的街道名稱(streetAddress) | 2.5.4.9 | | ● |
| 營業場所之實際地址的郵遞區號(postalCode) | 2.5.4.17 | | ● |
| 營業場所之實際組織單位名稱(organizationUnitName) | 2.5.4.11 | | ● |
| 組織識別碼 | 2.5.4.97 | | ● |

| 憑證欄位屬性名稱 | 物件識別碼(OID) | 必要屬性 | 選擇性屬性 |
|---|---|---|---|
| (organizationIdentifier) | | | |

本管理中心將於 2021 年 8 月 1 日起停用營業場所之實際組織單位名稱(organizationUnitName)。

### 3.1.2.1 主體必要屬性(Required Certificate Field)

(1) 組織名稱(organizationName)

根據EV SSL Certificate Guidelines第9.2.1節，EV TLS/SSL憑證欄位「主體」必須包含「組織名稱」屬性，其內容為憑證主體之正式組織名稱，且該名稱須為憑證主體於其所屬管轄區域登記機關或註冊機關(Registration Agency)登記的正式名稱，亦或是經本作業基準第3.2.2節驗證過之組織名稱。

本管理中心和註冊中心可縮寫組織名稱的字首或字尾，例如：將官方機構所記載的組織名稱「Company Name Incorporated」改為「Company Name, Inc.」，且該縮寫內容必須使憑證主體於其設立或註冊的管轄區域易於辨識。此外，若憑證主體使用化名時，則該化名可放在此屬性內容的開頭，並於其後以括弧註明憑證主體的正式組織名稱。

假若組織名稱長度超過64個字元(Characters)時，可縮寫組織名稱或是刪除組織名稱中不重要的文字，註冊中心須遵循EV SSL Certificate Guielines第11.12.1節有關高風險憑證請求(High Risk Certificate Request)之規範檢查此屬性的內容，且確認信賴憑證者可明確辨別憑證主體與修改後的組織名稱之間的關係，不可使其誤以為憑證主體為另外一間組織。倘若無法滿足此前提時，則本管理中心將不簽發該EV TLS/SSL憑證

(2) 營業類別(businessCategory)

根據EV SSL Certificate Guidelines第9.2.4節，EV TLS/SSL憑證欄位「主體」必須包含「營業類別」的屬性，以此區別EV TLS/SSL憑證主體之營業類別，其屬性內容可為「Private Organization」、「Government Entity」、「Business entity」、以及「Non-Commercial Entity」

等文字，分別代表私人組織、政府機關(構)、其他商業團體以及非營利國際組織，僅可擇一使用。

(3) 註冊之管轄區域的國家代碼(jurisdictionCountryName)

根據EV SSL Certificate Guidelines第9.2.5節，EV TLS/SSL憑證欄位「主體」必須記載憑證主體的登記機關或註冊機關之管轄區域的組織層級相關資訊，包括國家、州或省、或城市鄉鎮等資訊，其適用情境如下所述：

當憑證主體的登記機關或註冊機關之管轄區域的組織層級為國家時，則EV TLS/SSL憑證欄位「主體」必須包含屬性「註冊之管轄區域的國家代碼」，用於記載登記機關或註冊機關所在之國家，但不可包含屬性「註冊之管轄區域的州或省名稱」與「註冊之管轄區域的城市或鄉鎮名稱」。

當憑證主體的登記機關或註冊機關之管轄區域的組織層級為州或省時，則EV TLS/SSL憑證欄位「主體」必須同時包含屬性「註冊之管轄區域的國家代碼」與「註冊之管轄區域的州或省名稱」，用於記載登記機關或註冊機關所在之國家以及州或省名稱，但不可包含屬性「註冊之管轄區域的城市或鄉鎮名稱」。

當憑證主體的登記機關或註冊機關之管轄區域的組織層級為城市或鄉鎮時，則EV TLS/SSL憑證欄位「主體」必須同時包含屬性「註冊之管轄區域的國家代碼」、「註冊之管轄區域的州或省名稱」與「註冊之管轄區域的城市或鄉鎮名稱」，用於記載登記機關或註冊機關所在之國家、州或省名稱、以及城市或鄉鎮名稱。

因此，EV TLS/SSL憑證欄位「主體」至少必須包含屬性「註冊之管轄區域的國家代碼」，記載憑證主體的登記機關或註冊機關之管轄區域的國家，並以符合ISO國際標準所規範之國家代碼表示之。

(4) 識別代號(serialNumber)

根據EV SSL Certificate Guidelines第9.2.6節，EV TLS/SSL憑證欄位「主體」必須包含「識別代碼」的屬性，其內容可依不同營業類別而定，例如：

若憑證主體為私人組織時，則識別代號的內容須為其註冊管轄區域之註冊機關或登記機構所提供的唯一註冊登記編號(本作業基準統稱為「註冊號碼」(Registration Number))，例如：稅籍統一編號；

若未提供，則改以其設立或註冊日期表示之。

若憑證主體為政府機構，且亦無註冊號碼或是易於證實的建立日期時，則識別代號的內容須以適當語言來表示該憑證主體為政府機關(構)。

若憑證主體為其他商業團體時，則識別代號的內容須為政府註冊機關所提供之註冊號碼；若未提供，則改以其設立或註冊日期表示之。

(5) 營業場所之實際地址的國家代碼(countryName)

根據EV SSL Certificate Guidelines第9.2.7節，EV TLS/SSL憑證欄位「主體」必須包含「營業場所之實際地址的國家代碼」的屬性，用於記載憑證主體營業場所的實際地址所在之國家。

(6) 營業場所之實際地址的城市或鄉鎮名稱(localityName)

根據EV SSL Certificate Guidelines第9.2.7節之說明，EV TLS/SSL憑證欄位「主體」必須包含「營業場所之實際地址的城市或鄉鎮名稱」的屬性，用於記載憑證主體營業場所的實際地址所在之城市或鄉鎮。

#### 3.1.2.2 主體選擇性屬性(Optional Certificate Field)

(1) 註冊之管轄區域的州或省名稱(jurisdictionStateOrProvinceName)

此屬性須視情況而定，如上述必要屬性中的「註冊之管轄區域的國家代碼」之說明，當憑證主體的登記機關或註冊機關之管轄區域的組織層級為州或省或城市或鄉鎮時，則EV TLS/SSL憑證欄位「主體」除了包含屬性「註冊之管轄區域的國家代碼」以外，亦須包含屬性「註冊之管轄區域的州或省名稱」，用於記載登記機關或註冊機關之管轄區域所在之州或省名稱，且州或省名稱須為完整名稱。

若憑證主體的登記機關或註冊機關之管轄區域的組織層級為國家時，則無須包含屬性「註冊之管轄區域的州或省名稱」。

(2) 註冊之管轄區域的城市或鄉鎮名稱(jurisdictionLocalityName)

此屬性須視情況而定，如上述必要屬性中的「註冊之管轄區域的國家代碼」之說明，當憑證主體的登記機關或註冊機關之管轄區域的組織層級為城市或鄉鎮時，則EV TLS/SSL憑證欄位「主體」除了包含屬性「註冊之管轄區域的國家代碼」以及「註冊之管轄區域的州或

省名稱」外，亦須包含屬性「註冊之管轄區域的城市或鄉鎮名稱」，用於記載登記機關或註冊機關之管轄區域所在之城市或鄉鎮名稱，且城市或鄉鎮名稱須為完整名稱。

若憑證主體的登記機關或註冊機關之管轄區域的組織層級為國家或州或省時，則無須包含屬性「註冊之管轄區域的城市或鄉鎮名稱」。

(3) 營業場所之實際地址的州或省名稱(stateOrProvinceName)

根據EV SSL Certificate Guidelines第9.2.7節，EV TLS/SSL憑證欄位「主體」必須包含「營業場所之實際地址的州或省名稱」的屬性，用於記載憑證主體營業場所的實際地址所在之州或省；其中，若實際地址中有省相關資訊，亦須提供。

(4) 營業場所之實際地址的街道名稱(streetAddress)

根據EV SSL Certificate Guidelines第9.2.7節，可自行決定EV TLS/SSL憑證欄位「主體」是否包含「營業場所之實際地址的街道名稱」的屬性；若申請者有提供並經註冊中心驗證時，則可記載該憑證主體營業場所的實際地址所在之街道名稱。

(5) 營業場所之實際地址的郵遞區號(postalCode)

根據EV SSL Certificate Guidelines第9.2.7節，可自行決定EV TLS/SSL憑證欄位「主體」是否包含「營業場所之實際地址的郵遞區號」的屬性；若申請者有提供並經註冊中心驗證時，則可記載該憑證主體營業場所的實際地址所使用之郵遞區號。

#### 3.1.2.3 主體的不適用屬性(Deprecated Certificate Field)

(1) 一般名稱(commonName)

根據EV SSL Certificate Guidelines第9.2.3節，已不建議於EV TLS/SSL憑證欄位「主體」裡使用屬性「一般名稱」(commonName)，但目前亦尚未明文規定禁止使用。本管理中心所簽發EV TLS/SSL憑證欄位「主體」將提供「一般名稱」，此屬性內容記載憑證主體所擁有或控管的單一完全吻合網域名稱(Fully Qualified Domain Name, FQDN)，且該完全吻合網域名稱所對應的伺服器應為憑證主體或其承租之虛擬主機服務提供者所擁有與營運。

目前EV TLS/SSL憑證仍不支援萬用網域憑證(Wildcard certificates)，故「一般名稱」不得記載使用萬用字元之網域名稱。

根據EV SSL Certificate Guidelines第9.2.8節，除上述必要、選擇性與不適用屬性外，EV TLS/SSL憑證欄位「主體」內仍可提供其他選擇性屬性，假若有提供時，則這些屬性所記載的資訊皆須經註冊中心驗證確認無誤。

EV TLS/SSL憑證欄位「主體」裡的選擇性子欄位(Subfields)僅可記載已經註冊中心驗證確認無誤的資訊或是選擇將其內容設為空白。且不得使用「.」、「-」、「 」、以及/或是任何一種示意方來代表該欄位內容為空白、不存在、或不完整。

EV TLS/SSL憑證之憑證主體別名欄位應註記用戶擁有或能控制的一個或多個完全吻合網域名稱。且該完全吻合網域名稱所對應的伺服器應為憑證主體或其承租之虛擬主機服務提供者所擁有與營運。

多網域EV TLS/SSL憑證可記載多個用戶能控制之完全吻合網域名稱於1張憑證之憑證主體別名欄位。

### 3.1.3 用戶之匿名或假名

本管理中心沒有簽發匿名憑證(anonymous certificate)給終端用戶，原則上也不簽發假名憑證(pseudonymous Certificate)。本管理中心所發EV TLS/SSL憑證其網域名稱與組織之所有權都經憑證註冊審驗人員人工審查，屬於國際化網域名稱(Internationalized Domain Names, IDNs)之TLS/SSL憑證，其解碼的完全吻合主機名稱將如第4.2.1節視為具風險之TLS/SSL憑證請求進行額外之比對，以防止國際網域名稱同態欺騙攻擊(homographic spoofing of IDNs)。

### 3.1.4 不同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。

### 3.1.5 命名之獨特性

本管理中心的憑證機構憑證其X.500唯一識別名稱使用以下格式：

C=TW，

O=Chunghwa Telecom Co., Ltd.，

CN=HiPKI EV TLS CA - Gn，其中n=1, 2, 3…。

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標準或EV SSL Certificate Guidelines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)
- businessCategory
- jurisdictionCountryName
- jurisdictionStateOrProvinceName
- jurisdictionLocalityName
- streetAddress
- postalCode
- commonName(縮寫為 CN)
- serialNumber

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，由用戶向相關權責機關(構)或法院提出申請。

當用戶使用之識別名稱，經相關權責機關(構)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(可參考第4.9.1節)。

### 3.1.6 商標之辨識、鑑別及角色

用戶提供之憑證主體名稱包含商標或任何受法律保護之姓名、商業或公司名稱、表徵時，其命名須符合中華民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。

## 3.2 初始身分驗證

本管理中心和註冊中心採取所有合理且必要的驗證步驟，以滿足第3.2至第3.5節的驗證要求。依照HiPKI憑證政策與EV SSL Certificate Guidelines所規範之可接受的驗證方法(通常包含可選擇性的)，被視為驗證要求的最低標準。對於所有申請案件，本管理中心與註冊中心有責任採取額外的驗證步驟來滿足驗證要求。

### 3.2.1 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開金鑰成對。憑證申請者自行產製金鑰對，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，註冊中心將使用該申請者的公開金鑰驗證該憑證申請檔的簽章，以證明申請者擁有相對應的私密金鑰。

### 3.2.2 組織身分鑑別

#### 3.2.2.1 驗證要求概述

對於EV TLS/SSL憑證申請時組織(Organization)身分鑑別，其目的包含：

(1)確認申請者的存在和身分，包括：

A.驗證申請者的合法存在(Legal Existence)和身分

B.驗證申請者的實際存在(physical existence)(業務進行的實際地址)，和

C.驗證申請者的業務存在(operational existence)(商業活動)。

(2)確認註記在 EV TLS/SSL 憑證的申請者是網域名稱註冊者(Domain Name Registrant)，或擁有網域名稱控制權；

(3)確認有可靠的聯絡方式；

(4)確認申請者對 EV TLS/SSL 憑證的授權，參見第 3.2.3 與第 3.2.4 節，包括：

A.驗證合約簽署者(Contract Signer)、憑證遞件核准者(Certificate Approver)和憑證請求者(Certificate Requester)的姓名、職稱和職權。

B.確認合約簽署者已簽署用戶約定條款或經授權的申請人代表已確認和同意使用條款；和

C.確認憑證遞件核准者已簽署或以其他方式核准 EV TLS/SSL 憑證請求(EV TLS/SSL Certificate Request)。

法人登記機關及註冊機關資訊等驗證資源公布於儲存庫 https://tls.hinet.net/repository.htm。

### 3.2.2.2 驗證申請者的合法存在和身分

#### 3.2.2.2.1 驗證要求

為了驗證申請者的合法存在和身分，憑證註冊中心針對以下4種類型的組織其驗證要求為：

(1)私人組織

A.合法存在：確認申請者(例如：法人組織、公司)是在設立或註冊之管轄區域合法成立的有效個體，且在設立或註冊機關的記錄不是「歇業的」、「無效的」、「非當期的」，或同等的註記。

B.組織名稱：確認申請者在設立或註冊之管轄區域的註冊機關登記的合法名稱，與申請者在 EV TLS/SSL 憑證請求註記的名稱相符。

C.註冊號碼：取得申請者在設立或註冊之管轄區域的註冊機關的特定註冊號碼例如稅籍統一編號，如註冊機關未編配註冊號碼，憑證註冊中心將取得申請者的成立或註冊日期。

D.註冊代理人(Registered Agent)：取得申請者的註冊代理人的身分、地址或註冊辦事處(Registered Office) (適用於申請者的設立或註冊之管轄區域)。註冊辦事處為組織記錄在註冊機關的官方地址，作為官方文件寄送和法律文書的收件地址。

私人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(例如公司登記事項卡、公司變更登記事項卡、法人登記證書、扣繳單位設立(變更)登

記申請書影本(統一編號編配通知書))，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)，註冊窗口將核對申請者提供之申請資料與身分的真實性或是使用政府公開金鑰基礎建設保證等級第 3 級組織憑證所對應之私密金鑰對憑證申請資料數位簽章。

私人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本管理中心、註冊中心或本管理中心所信賴的公證人、律師、會計師或本公司人員完成符合本作業基準之識別與鑑別程序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、律師、會計師或本公司人員加蓋認證戳記)，本管理中心或註冊中心得允許該私人組織於申請憑證時出示佐證資料來取代上述識別與鑑別方式。

(2)政府機關(構)

A.合法存在：確認申請者為具法律認可的政府實體。

B.實體名稱(Entity Name)：確認申請者註記在 EV TLS/SSL 憑證請求的名稱與法定名稱相符。

C.註冊號碼：中華民國政府機關(構)將使用行政院人事行政總處之政府機關代碼。註冊中心必須嘗試取得政府機關(構)的成立或登記日期，或識別成立政府機關(構)的法令。在這些資訊不適用的情況下，必須輸入適當的語言，表明主體是政府實體。

D.政府機關(構)得以正式公文書申請憑證，註冊中心必須確認該機關(構)確實存在，並驗證公文書之真確性。政府機關(構)也可使用政府公開金鑰基礎建設保證等級第 3 級組織憑證所對應之私密金鑰對憑證申請資料數位簽章。

(3)非營利國際組織

A.合法存在：確認申請者是經法律認可的國際組織實體。

B.實體名稱：確認申請者的合法名稱，與申請者註記在 EV TLS/SSL 憑證請求的名稱相符。

C.註冊號碼：註冊中心必須試圖取得申請者的成立日期，或識別成立國際組織的法令。在這些資訊不適用的情況下，註冊中心必須輸入適當的語言，表明主體是一個國際組織。

(4)其他商業團體

A.合法存在：確認申請者提交申請的營業項目。

B.組織名稱：確認申請者在註冊機關(申請者的管轄區域) (在我國商業或有限合夥等之註冊機關也稱為申登機關)認可的合法名稱，與申請者註記在 EV TLS/SSL 憑證請求的名稱相符。

C.註冊號碼：嘗試取得申請者在註冊機關(管轄申請者的註冊)的唯一註冊號碼，若註冊機關未編配註冊號碼，註冊中心將取得申請者的登記日期。於中華民國登記的其他商業團體將使用稅籍統一編號。

D.代表人(Principal Individual)：確認代表人的身分。代表人為私人組織、政府機關(構)或其他商業團體的業主、合夥人、管理成員、董事或職員，可以經由他們的職稱、員工、承包商或由實體或組織授權進行 EV TLS/SSL 憑證的請求、簽發和使用相關業務的代理人來辨識。

其他商業團體必須提供註冊窗口正確且經主管機關核發之相關證明文件影本(例如登記機關核准商業登記之核准函、商業登記抄本、依商業登記法第 25 條規定由商業負責人或利害關係人請求商業所在地主管機關就已登記事項發給證明書、扣繳單位設立(變更)登記申請書影本(統一編號編配通知書))，證明文件影本應蓋用其他商業團體及負責人之印鑑章(與其他商業團體登記時所使用之印鑑章相符，註冊窗口將核對其他商業團體所提供之申請資料及身分的真實性。其他商業團體也可使用政府公開金鑰基礎建設保證等級第 3 級組織憑證所對應之私密金鑰對憑證申請資料數位簽章。

其他商業團體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本管理中心、註冊中心或本管理中心所信賴的公證人、律師、會計師或本公司人員完成符合本作業基準之識別與鑑別程序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、律師、會計師或本公司人員加蓋認證戳記)，本管理中心或註冊中心得允許該其他商業團體於申請憑證時出示佐證資料來取代上述識別與鑑別方式。

#### 3.2.2.2.2 可接受的驗證方法

(1) 私人組織：必須直接與申請者驗證私人組織之合法存在、私人組織正式名稱、註冊號碼及註冊代理人，或直接從申請者的設立或註冊

之管轄區域的註冊機關取得驗證。

此驗證來源可為註冊機關所管理的合格政府資訊來源(或是代表註冊機關之合格政府資訊來源)，也可親自與註冊機關聯繫，或透過從註冊機關所管理的合格的政府資訊來源(Qualified Government Information Source, QGIS)或合格的獨立資訊來源(Qualified Independent Information Source, QIIS)取得之郵件、電子信箱、網址或電話等方式來進行聯繫。

(2) 政府機關(構)：必須直接或透過以下其中一種方法來進行驗證或取得合法存在、實體名稱與註冊號碼：A.合格的政府資訊來源；B.與申請機關(構)在同一行政區的上級政府機關(構) (Superior Government Entity)，或 C.在同一個行政區之司法機關的現任法官，或 D.政府機關(構)的代表律師。

任何從法官得到的訊息應以相同的方式予以核實，如第 3.2.3.4.1 節提出的事實主張。

此驗證可親自與合適的政府機關(構)聯繫並確認，或透過從合格的獨立資訊來源取得之郵件、電子信箱、網址或電話等方式來進行聯繫。

(3) 其他商業團體：必須直接與申請者驗證其他商業團體的合法存在、組織名稱及註冊號碼，或直接從申請者的設立或註冊之管轄區域的註冊機關取得與驗證。此驗證可以從合格的政府資訊來源如經濟部工商登記資料庫及合格的政府稅收資訊來源(Qualified Government Tax Information Source, QTIS)如財政部財稅資料中心公示資料取得，或親自與註冊機關聯繫，或透過從合格的政府資訊來源及合格的政府稅收資訊來源、註冊機關或合格的獨立資訊來源取得之郵件、電子信箱、網址或電話等方式來進行聯繫。

此外，本管理中心與註冊中心必須依據以下第(4)點的說明，驗證與其他商業團體相關的代表人。

(4) 代表人：對於與其他商業團體相關的代表人，註冊中心必須以面對面的方式進行驗證。

如果本管理中心與註冊中心已經評估過註冊機關對代表人進行面對面驗證之程序，並確認其可滿足 EV SSL Certificate Guidelines 所規範之面對面驗證程序的驗證需求，則可信賴該驗證結果。

如果註冊機關沒有執行面對面驗證，或是驗證程序不符合 EV SSL Certificate Guidelines 的驗證要求，註冊中心將執行面對面驗證。

A.面對面驗證：此驗證必須在有註冊中心的員工或本公司授權之公司業務人員、公證人(或等同於申請者的管轄機構)、律師或會計師(第三方驗證人)其中之一在場時進行。

代表人(可能不只一位)必須當場提供以下文件(審核文件)給第三方驗證人：

(I) 包含以下資訊的個人聲明書(Personal Statement)：

(i) 全名，或眾所周知的名稱(包含所有慣用的名稱)；

(ii) 居住地址；

(iii) 出生日期；和

(iv) 聲明書，該聲明書須可承諾所有包含在憑證要求的資訊是真實和正確的。

(II) 現行政府機關核發的身分證明文件，包含個人照片及簽名，例如：

(i) 護照；

(ii) 駕照；

(iii) 個人身分證；

(iv) 隱藏武器許可證(槍枝持有許可證)；或

(v) 軍用 ID。

(III) 至少兩個輔助的證明文件，以確定他/她的身分(含個人的名字)，其中一個必須來自於金融機構。

(i) 可接受的金融機構文件包括：

(a) 主要使用的信用卡，包含到期日而且尚未過期。

(b) 由受監管的金融機構(Regulated Financial Institution)核發的簽帳卡或轉帳卡，包含到期日而且尚未過期。

(c) 由可辨識的貸款人提供的最近6個月的抵押聲明。

(d) 由受監管的金融機構提供的最近6個月的銀行聲明。

(ii) 可接受的非財務文件包括：

(a) 近期水電費帳單正本或在固定地址支付公用事業服務款項的收據(非行動電話帳單)。

(b) 過去6個月內支付租金的文件副本。

(c) 已核證的出生證明副本。

(d) 本年度地方當局提供的稅單。

(e) 法院命令的核證副本，例如離婚證明(協議)、廢止的文件或收養的文件。

(IV) 第三方驗證人進行面對面驗證必須：

(i) 驗證個人聲明書的簽署和簽名者的身分。

(ii) 鑑別過去用來進行驗證的原始審核文件。此外，第三方驗證人必須證明現行政府機關核發的身分證明文件是完整、真實和準確的原始文件副本。

B. 對第三方驗證人的驗證：註冊中心必須獨立驗證第三方驗證人是具有法律資格的公證人(或與管轄申請者的機構具有同等法律效力)，律師或會計師(在個人居住的管轄區，且實際提供服務並驗證個人的簽名)。

C. 資訊交叉驗證：註冊中心必須取得個人簽署的文件以及現行政府機關核發的身分證明文件副本。註冊中心必須審查文件，以確定該資訊與申請資訊是一致的，並識別代表人。本管理中心與註冊中心可以信賴文件副本的電子檔，假若：

(I) 註冊中心與第三方驗證人驗證其真偽(與正本對照無不當修改)；

(II) 經註冊中心的管轄區的法律認可此類證明文件的電子檔，是等同於原始文件的合法替本。

(5) 非營利國際組織：非營利國際組織的合法存在、合法名稱與註冊號碼須透過以下任一種方法來驗證：

A. 參考國際組織構成的文件；

B. 直接與允許本管理中心營運的簽署國政府進行驗證。這些驗證可以從適當的政府主管機關(Government Agency)或該國法律取得，或藉由確認該國政府的任務以代表申請者是國際組織；或

C. 直接對照 CA/Browser Forum 維護的網站 www.cabforum.org 所公告的最新合格非營利國際組織清單。

D. 當申請 EV TLS/SSL 憑證的國際組織為機關(organ)或機構(agency)時(包括已驗證過之國際組織的非政府組織)，註冊中心可直接與已驗證過之傘狀國際組織(umbrella International Organization，其申請者亦是機關或機構)來驗證該國際組織的申請者。(umbrella organization 通常是與特定行業合作、協調活動

或資源的機構，例如：美國勞工聯合會產業工會聯合會(AFL–CIO))

#### 3.2.2.3 申請者的合法存在和身分驗證-化名

##### 3.2.2.3.1 驗證要求

除了申請者記錄在其設立或註冊之管轄區域的法人登記機關(Incorporating Agency)或註冊機關的合法名稱外，如果申請者註記在EV TLS/SSL憑證的身分含有任何化名(例如在美國「doing business as」也被稱為「DBA」或「d/b/a」，在英國稱為「trading as」)並以此名稱辦理業務，註冊中心必須確認：

(1) 申請者已向適當的政府機關(營業場所的管轄機構)註冊營業地點。

(2) 此申請仍然有效。

##### 3.2.2.3.2 可接受的驗證方法

驗證申請者辦理業務的任何化名：

(1) 註冊中心可透過申請者營業地點所在之管轄區域內合適的政府機關所管理的合格政府資訊來源(或是代表申請者營業地點所在管轄區域內合適的政府機關的合格政府資訊來源)來驗證化名，亦可直接親自或是以郵件、電子信箱、網址、電話等方式向政府機關聯繫並驗證化名；或

(2) 若合格的獨立資訊來源已和適當的政府機關驗證化名，註冊中心可透過合格的獨立資訊來源提供的資訊進行化名驗證。

(3) 註冊中心可信賴用於表示申請者辦理業務的化名已向政府機關註冊且此申請仍然有效的法律驗證意見書(Verified Legal Opinion)或會計師驗證信(Verified Accountant Letter)。

#### 3.2.2.4 申請者實際存在的驗證

##### 3.2.2.4.1 申請者營業地點的地址

(1) 驗證要求：為了確認申請者的實際存在和商業行為，註冊中心必須驗證申請者提供的地址為申請者母/子公司的進駐地點和營業地點(舉例來說，不可為代收郵件的郵筒、郵政信箱或是轉寄地址(C/O

Address，例如組織代理人的地址))。

(2) 可接受的驗證方法

A.營業地點位於註冊或登記的國家

(I) 對於營業地點與其設立或註冊之管轄區域位於相同國家，且其營業地點與第3.2.2.2節用於驗證合法存在之相關 QGIS 是不相同的申請者：

(i) 對於與最新版本 QGIS(此 QGIS 與用來驗證合法存在的 QGIS 不相同)、QIIS 或 QTIS 等至少其中一個資訊來源列相同營業地址的申請者，註冊中心必須參考 QGIS、QIIS 或 QTIS，以確認該申請者列在 EV TLS/SSL 憑證請求裡的地址確實為對申請者或是母/子公司的有效營業地址，並可相信該申請者提出此地址為營業地點的說明；

(ii) 對於未與最新版本 QIIS 或 QTIS 等至少其中一個資訊來源列相同營業地址的申請者，註冊中心必須取得由可信賴的人(如本公司對客戶服務之專案經理/業務經理/專案工程師等相關角色)或公司至該地址實地訪查後所作的證明文件，以確認該申請者列在 EV TLS/SSL 憑證請求裡的地址確實為對申請者或是母/子公司的有效營業地址。該實地訪查證明文件必須：

(a) 確認申請者的營業地址是申請 EV TLS/SSL 憑證請求的確切地址(例如：透過常設招牌，員工確認等)，

(b) 識別建築物的類型(例如：在商業大樓的辦公室、私人住宅、店面等)，以及是否為一個永久的營業位置。

(c) 表明是否有一個固定招牌(即不能移除)，用以識別申請者。

(d) 表明是否有證據顯示，申請者在此場所進行持續的業務活動(換言之，此場所應非代收郵件的郵筒或郵政信箱等)，和

(e) 包括一張或多張該營業場所外觀的照片(須顯示包含申請者名稱的招牌，如果可能的話並顯示街道地址)，和該營業場所的內部接待區或工作區的照片。

(iii) 對於所有申請者，註冊中心可在法律驗證意見書或會計師驗證信中擇一作為依據，以表明申請者或母/子公司營業地點的地址並且在那裡進行業務營運。

(iv) 對於政府機關(構)申請，註冊中心可信賴申請者管轄區域內的 QGIS 所記錄的地址。

(v) 對於營業地點與其設立或註冊之管轄區域位於相同國家，且其 QGIS(此 QGIS 為第3.2.2.2節用於驗證合法存在)亦包含申請者營業地址的的申請者，註冊中心可信賴 QGIS 裡的地址，並以此來確認 EV TLS/SSL 憑證請求裡列出的申請者或是母/子公司的地址，且可相信該申請者提出此地址為營業地點的說明。

B. 營業地點不在註冊或登記的國家

註冊中心必須依據法律驗證意見書或會計師驗證信，以表明申請者的營業地點並且在那裡進行業務營運。

### 3.2.2.5 通信的驗證方法(Verified Method of Communication)

#### 3.2.2.5.1 驗證要求

為了協助與申請者溝通，以及確認申請者已經知道並核准簽發，註冊中心必須如通信的驗證方法與申請人確認電話號碼、傳真號碼、電子郵件或通訊地址。

#### 3.2.2.5.2 可接受的驗證方法

為了與申請者確認通信驗證方法，註冊中心必須：

(1) 透過合適的電話公司、QGIS、QTIS、QIIS、法律驗證意見書或會計師驗證信等資訊來源所提供的紀錄來比對申請者的母/子公司或關係企業的營業地點，以此驗證該通信驗證方法屬於申請者、或是屬於申請者的母/子公司或關係企業；和

(2) 透過使用此通信的驗證方法來取得足以令人確認其確實可使用該方法來與申請者或是申請者的母/子公司或關係企業進行聯繫的正面回應。

#### 3.2.2.6 憑證申請者之營運存在的驗證

##### 3.2.2.6.1 驗證要求

註冊中心必須藉由驗證憑證申請者的或其關係企業/母公司/子公司的營運存在來驗證具有從事經營業務之能力。.

##### 3.2.2.6.2 可接受的驗證方法

為了驗證憑證申請者具有經營業務之能力，註冊中心必須驗證申請者或其關係企業/母公司/子公司的營運存在性，驗證方法包括：

(1) 驗證申請者關係企業、母公司或子公司確實如法人登記機關或註冊機關所記載之紀錄所示已經存在至少 3 年。

(2) 驗證申請者關係企業、母公司或子公司列在現有的合格的獨立資訊來源或合格的政府稅收資訊來源。

(3) 驗證申請者關係企業、母公司或子公司具有使用中的現行符合受監管之金融機構的活期存款帳戶(Demand Deposit Account) 。

(4) 依據法律驗證意見書或會計師驗證信的內容，以此確認申請者具有活動中之現有需求符合受監管之金融機構的活期存款帳戶。

#### 3.2.2.7 申請者網域名稱之驗證

(1) 對每一個註記在 EV TLS/SSL 憑證裡面的完全吻合網域名稱，註冊中心必須以憑證簽發日為基礎，確認憑證申請者(此處申請者的母公司/子公司或關係企業統稱為「申請者」)確實為網域名稱登記者或是藉由第 3.2.5 節所述的網域名稱註冊者的授權程序驗證來確認其具備控制完全吻合網域名稱之權利。

(2) 網域名稱之混合字元組(Mixed Character Set Domain Names)：以目視的方式比對所有包含混合字元集的網域名稱以及已知的高風險網域名稱，假若發現相似處，則該 EV TLS/SSL 憑證請求必須被標示為高風險。本管理中心與註冊中心將執行合理且適當的額外之鑑別和驗證以確認關於申請者和有問題之目標是否為同一組織超過合理之懷疑。

### 3.2.3 個人身分鑑別

EV TLS/SSL憑證並不發給個人(Individual)，而是發給第3.1.2、第3.2.2.2或第4.1.1節所敘述的4種類型的組織，但組織內的憑證請求者、合約簽署者、憑證遞件核准者其個人身分必須經過驗證，說明如下。

#### 3.2.3.1 合約簽署者與憑證遞件核准者之授權、名字、職稱的驗證

##### 3.2.3.1.1 驗證要求

對於合約簽署者和憑證遞件核准者，註冊中心必須驗證以下事項：

(1)姓名、職稱和機構：如果適用的話，註冊中心必須驗證合約簽署者和憑證遞件核准者之姓名與職稱。註冊中心也必須驗證合約簽署者與憑證遞件核准者是否為代表憑證申請者之代理人。

(2)合約簽署者之簽署權力來源(Signing Authority)：註冊中心必須驗證合約簽署者得到申請者之授權代表申請者而簽訂用戶約定條款和其他任何相關合約義務)，包含指定一個或多個憑證遞件核准者代表申請者的合約。

(3)憑證遞件核准者之 EV 授權來源：註冊中心必須透過與憑證遞件核准者不同的來源來驗證憑證遞件核准者確實已取得申請者的授權，並可於 EV SSL 憑證請求提出時執行以下事項：

A.代表憑證申請者提交 EV TLS/SSL 憑證請求(亦可授權憑證請求者來進行此作業)；和

B.提供由憑證申請者所提供的由本管理中心要求之資訊，以用於 EV TLS/SSL 憑證的簽發(亦可授權憑證請求者來進行此作業)；

C.核准由憑證請求者遞交的 EV TLS/SSL 憑證請求。

##### 3.2.3.1.2 驗證姓名、職稱、機構之方式

驗證合約簽署者與憑證遞件核准者之姓名、職稱、機構狀態的方式包括：

(1)姓名和職稱：註冊中心可以藉由任何適當的方式驗證合約簽署者與憑證遞件核准者的姓名和職稱，以提供合理的保證使某人宣稱

其扮演之角色確實名符其實。

(2)機構：註冊中心可驗證合約簽署者與憑證遞件核准者的機構。

A.透過通信的驗證方法聯繫申請者，並確認合約簽署者和/或憑證遞件核准者確實為該機構之職員

B.取得憑證申請者獨立之確認(如第 3.2.3.4.4 節所述)或法律驗證意見書(如第 3.2.3.4.1 節所述)或會計師驗證信(如第 3.2.3.4.2 節所述)，以驗證合約簽署者和或憑證遞件核准者確實為該機構的員工或是已被指定為申請者的代表人；或

C.取得合格的獨立資訊來源或合格的政府資訊來源之確認合約簽署者和/或憑證遞件核准者是申請者之員工。若工作或代理狀態及合約簽署者之簽署授權已經經過核實，則註冊中心也可透過來自合約簽署者之驗證來核對憑證遞件核准者屬實(包括在本管理中心和申請者(由合約簽署者所簽名)的合約)。

### 3.2.3.1.3 驗證授權的可接受之方法

可被接受的合約簽署者之簽署權力來源以及憑證遞件核准者之EV授權來源(EV Authority)之驗證方式包括：

(1)法律意見：合約簽署者之簽署權力來源，和/或憑證遞件核准者之 EV 授權來源，可藉由法律驗證意見書來驗證(如第 3.2.3.4.1 節所述)；

(2)會計師信函：如第 3.2.3.4.2 節所述，可透過倚賴的會計師驗證信驗證憑證遞件核准者之 EV 授權來源與合約簽署者之簽署權力來源；

(3)公司決議：合約簽署者之簽署權力來源或憑證遞件核准者之 EV 授權來源，可能可透過適當的鑑別公司決議確認該名人是取得簽署權力來源，假設此決議是(i)透過適當的公司職員(例如秘書)確認，和(ii)本管理中心或註冊中心能可靠地驗證該憑據由該人有效地簽署，此人真地有必要之權限提供此驗證之資料；

(4)來自申請者之獨立確認：合約簽署者之簽署權力來源和/或憑證遞件核准者之 EV 授權來源，可透過從申請者所取得之獨立確認(如第 3.2.3.4.4 節所述)證實。

(5)本管理中心和申請者之協議(合約)：假若此合約由合約簽署者簽署且此合約簽署者的代理和簽署權力來源已經核實確認被證實，

則憑證遞件核准者的 EV 授權來源可藉由倚賴本管理中心和申請者之間的合約指派憑證遞件核准者具有此種 EV 授權來源。

(6) 先前已經建立的同等效力授權：合約簽署者的簽署授權，和/或憑證遞件核准者的 EV 授權來源可能透過倚賴先前已經建立的同等效力授權(Prior Equivalent Authority)之展現核實：

A. 當合約簽署者已經使用一個具法律效力的印章或手寫簽名來完成本管理中心或註冊中心和申請者之間的合約，且僅當此合約於 EV TLS/SSL 憑證申請的 90 天之前(甚至更久之前)開始執行時，合約簽署者在先前已經建立的同等效力授權必須依靠合約簽署者的簽署權力來源確認或核實。註冊中心必須對先前的協議進行詳細的紀錄，以正確地確認，並將其與 EV 申請連繫在一起。這些細節可包括以下任何各項：合約標題、合約簽署者之簽章日期、合約參考編號與歸檔位置。

B. 當憑證遞件核准者已經執行以下其中一個或更多的事項，則憑證遞件核准者的先前已經建立的同等效力授權，有可能倚賴確認或驗證憑證遞件核准者的 EV 授權來源：

(I) 在本管理中心之合約下，已經(或正在)擔任申請者的企業註冊中心(Enterprise RA)或

(II) 已經參與核准一個或更多憑證請求，對於本管理中心簽發的憑證為現存且可被申請者驗證在使用中。在此情形下註冊中心必須藉由先前驗證過的電話號碼以電話聯繫憑證遞件核准者，或是已經接受的經過簽署與公證的信件證明憑證請求。

(7) 合格的獨立資訊來源或合格的政府資訊來源：合約簽署者的簽署權力來源，和/或憑證授權者的 EV 授權來源，可能會透過合格的獨立資訊來源或合格的政府資訊來源而獲證實，以識別合約簽署者和/或憑證遞件核准者為公司職員、獨資經營，或是申請者的其他資深人員。

(8) 合約簽署者的陳述/擔保：假設註冊中心驗證合約簽署者是申請者的員工或代理人，註冊中心可透過取得雙重陳述或擔保(如下所述)來信賴合約簽署者的簽署權力來源：

A. 申請者授權合約簽署者代表申請者簽署用戶約定條款(購買合約條款)，

B.用戶約定條款是合法有效且可實施的合約，

C.在執行用戶約定條款後，申請者將被所有的條款和狀況限制，

D.屬於誤用 EV TLS/SSL 憑證的嚴重後果，和

E.合約簽署者有權利取得公司圖記，印章和職員的簽名的數位等效資料以建立公司網站之真確性。

**3.2.3.1.4 於授權前之憑證遞件核准者**

當本管理中心和申請者考慮遞送多個未來的EV TLS/SSL憑證請求檔時，須待本管理中心或註冊中心進行以下事項之後：

(1) 已經驗證合約簽署者之姓名和職稱，而且他/她是申請者的職員或代理人

(2) 已經根據於第 3.2.3.1.3 節當中的程序之一，驗證簽署權力來源

本管理中心或註冊中心和申請者可進入書面的合約，由代表申請者的合約簽署者簽署，因此，對於一個指定的期限，申請者明確地授權一個或多個在該協議指定的憑證遞件核准者，相對於每個未來的EV TLS/SSL憑證請求提交代表申請者行使EV授權來源，並適當地鑑定和初始簽發相同或以其它方式被憑證遞件核准者核准。

這樣的協議必須提供申請者須為在請求發出或憑證遞件核准者核准的所有的EV TLS/SSL憑證的用戶約定條款項下的義務負責，直到EV授權來源被撤銷，並且必須包括雙方同意的規定：(i)當EV TLS/SSL憑證請求被核准，鑑別憑證遞件核准者(ii)定期重新確認憑證遞件核准者的EV授權來源，(iii)申請者可以通知本管理中心或註冊中心，任何的憑證遞件核准者其EV授權被撤銷的安全程序，以及(iv)合理必要的其他適當的預防措施。

**3.2.3.2 EV TLS/SSL 憑證請求和用戶約定條款之簽章驗證**

用戶約定條款和每一個非預先授權的EV TLS/SSL憑證請求必須被簽署。用戶約定條款必須被經授權的合約簽署者簽署。除非憑證請求已經符合第3.2.3.1.4節預先授權(pre-authorized)，EV TLS/SSL憑證請求必須由憑證請求者簽署與遞交此文件。

如果憑證請求者也不是經授權的憑證遞件核准者，則經授權的憑證遞件核准者必須獨立核准EV TLS/SSL憑證請求，在所有的案例，適用的簽章必須是合法有效且包含可執行的圖記或手寫簽名(對於書面的用戶

合約和/或EV TLS/SSL憑證請求)，或合法有效和可實施的電子簽章(對於電子的用戶合約和/或EV TLS/SSL憑證請求檔，如政府機關公開金鑰基礎建設保證等級第3級憑證對應之私密金鑰的數位簽章)，繫結申請者和每個對應文件的條款。

#### 3.2.3.2.1 驗證條款

(1) 簽章：註冊中心必須鑑別合約簽署者在用戶約定條款(購買合約條款)的簽章與每個憑證請求的憑證請求者簽章的方式，使其合理地確信每個簽署者在適用的文件簽署的名字實際上確實為代表申請者於文件上簽署的人。

(2) 核准的替代方案(Approval Alternative)：假如 EV TLS/SSL 憑證請求由不是同時也擔任憑證遞件核准者的憑證請求者簽章與傳遞，第 3.2.3.3 節透過憑證遞件核准者的 EV TLS/SSL 憑證請求的核准與適用可用來取代這樣的 EV TLS/SSL 憑證請求的憑證請求者簽章之鑑別。

#### 3.2.3.2.2 簽章驗證的可接受方式

鑑別憑證請求者或合約簽署者的簽章之可接受方式包括：

(1) 使用申請者通信的驗證方法聯繫申請者，如果可以，將憑證請求者或合約簽署者列為收件者，透過某人的回應確定某人確認他們當中確實有(他/她)代表申請者簽署適用的文件；

(2) 一封信郵寄到申請者或代理人的地址，根據 EV SSL Certificate Guidelines 透過獨立之方式驗證，如適用，以憑證請求者或合約簽署者為收件者，透過通信的驗證方法從某人之回應證實某人確認他們之中，他/她代表申請者簽署適用的文件；

(3) 以安全的形式使用簽名的流程建立簽署者姓名與職稱，例如透過適當的安全登入使用或藉由恰當地驗證憑證、透過數位簽章的使用(如政府機關公開金鑰基礎建設保證等級第 3 級憑證對應之私密金鑰的數位簽章)；或

(4) 公證人的公證，前提是本管理中心或註冊中心獨立驗證這種公證人是在憑證請求者或合約簽署者的管轄區域具有法定資格的公證人。

### 3.2.3.3 對 EV TLS/SSL 憑證請求檔核准的驗證

#### 3.2.3.3.1 驗證需求

一旦EV TLS/SSL憑證請求檔藉由憑證請求者傳送，在本管理中心簽發所請求的EV TLS/SSL憑證前，註冊中心必須確認得到授權的憑證遞件核准者已審查與核准此EV TLS/SSL憑證請求檔。

#### 3.2.3.3.2 驗證的可接受方式

驗證憑證遞件核准者核准EV TLS/SSL憑證請求的可接受方式包括：

(1) 使用對於申請者的通信驗證方法聯繫憑證遞件核准者，並取得口頭或書面確認憑證遞件核准者已經檢查和核准 EV TLS/SSL 憑證請求；

(2) 通知憑證遞件核准者在特定受存取控制與安全的網站，一個或多個新的 EV TLS/SSL 憑證請求已經可以在被指定具有存取控制與安全的網站被檢查與核准，經過登入後，並且有跡象顯示憑證遞件核准者有採該網站所要求的方式核准該憑證請求；或

(3) 根據第 3.2.3.2 節驗證 EV TLS/SSL 憑證請求的憑證遞件核准者之簽章。

### 3.2.3.4 確信資料來源的驗證

#### 3.2.3.4.1 法律驗證意見書

(1) 在確信送交給註冊中心法律意見書前，註冊中心必須驗證該法律意見書符合下列需求：

A. 作者之執業資格：註冊中心必須驗證法律意見書是由申請者所聘雇並能代表申請者、獨立的執業律師(或於申請者內部工作的執業律師)(執業律師)所執筆，具備以下兩者之一：

(I) 律師(或初級律師(事務律師)、(英國有資格在任何法庭作辯護的)專門律師、出庭律師、辯護律師或同等的)，而且在申請者維持辦公室或實體設施(而且主管機關認可拉丁公證人(Latin Notary)的角色)的國家得到許可(有執照)，並在申請者的登記管轄權或註冊或任何的管轄區內執業；

(II) 公證人，為國際拉丁公證人聯盟(International Union of Latin Notaries)之會員，而且在申請者維持辦公室或實體設施(而且主管機關認可拉丁公證人的角色)的國家得到許可(有執照)，並在申請者的登記管轄權或註冊或任何的管轄區內執業；

B. 意見的基礎：註冊中心必須驗證執業律師正行使代表申請者，並且根據執業律師陳述熟悉相關事實與運用專業知識和專業判斷來檢驗法律驗證意見書的結論。

C. 真確性(Authenticity)：註冊中心必須確認法律驗證意見書之真確性。

(2) 驗證的可接受方法

建立上述要求的法律驗證意見書之可接受方式為：

A. 作者的執業資格:註冊中心必須藉由直接接觸在適用的管轄區負責執業律師註冊或執照的機構,來檢驗法律驗證意見書作者的專業地位；

B. 於中華民國執行業務之律師依現行律師法規定,會取得法務部頒發之律師證書,加入當地律師公會,並於全國任一法院登錄有案,註冊中心將透過法務部律師管理系統(http://service.moj.gov.tw/lawer/notice.htm)或中華民國律師公會全國聯合會網站(http://www.twba.org.tw/)之律師查詢功能或聯繫各地律師公會確認。

法院公證人或民間公證人將透過司法院或地方法院公證業務主管機關及各地方法院所屬民間公證人登錄名冊確認。

C. 意見的基礎:法律意見書的文字必須明確使得執業律師代表申請者,且法律意見書的結論是根據執業律師熟悉相關事實所陳述與專業知識和專業判斷的運用。法律意見書也可能包括免責聲明和其他在執業律師管轄範圍的習慣法上的限制,法律意見書如果被證明是錯誤的,前提是該免責聲明不能擴大到消除對執業律師的任何實質風險(財務、專業和/或聲譽)。

D. 真確性：為了確認法律意見書的真確性，註冊中心必須打電話或送法律意見書之副本給至表列在負責執業律師註冊(登記)或執照發放的主管機關的地址、電話、傳真或電子郵件(如果可以的話)給執業律師並取得確認，或由執業律師協助確認法律意見書

是真實可靠的。如果電話號碼無法從發執照的主管機關取得，註冊中心可使用適用的電話公司、合格的政府資訊來源或合格的獨立資訊來源紀錄中表列的執業律師之電話號碼。

在法律意見書透過數位簽章下，法律意見書與簽章者之真確性如果如第 3.2.3.4.1 節第(2).A 款經註冊中心確認，則不需要更進一步的真確性確認。

### 3.2.3.4.2 會計師驗證信

(1)驗證要求：在引用提交給註冊中心的會計師信函前，註冊中心必須確認此會計師信函符合以下需求：

A.作者之執業資格：必須驗證會計師信函是由申請者所聘雇或從事會計工作之執業會計師所執筆，而且會計師得到許可(有執照)在申請者維持辦公室或實體設施(而且主管機關認可會計師的角色)的國家且具備申請者的登記管轄權或註冊或任何管轄區執業。執照的驗證必須透過執業會計師所在國家的會員組織或監管機構，才能在該國家或司法管轄區執業的時候聯繫。這樣的國家或地區必須有一個會計標準機構與國際會計師聯合會(International Federation of Accountants)維持正式成員的地位。

B. 意見的基礎：註冊中心必須驗證執業會計師代表申請者且會計師驗證信的結論是根據執業會計師熟悉相關事實所陳述與專業知識和專業判斷的運用。

C. 真確性(Authenticity)：註冊中心必須確認會計師驗證信之真確性。

(2)可接受的驗證方法

建立上述要求的會計師驗證信之可接受方式為：

A.作者的執業資格：註冊中心必須驗證會計師驗證信作者的專業地位，藉由直接接觸在適用的管轄區負責執業會計師註冊(登記)或執照的機構；例如在中華民國執業之會計師可聯繫中華民國會計師公會聯合會，或透過其網站(http://www.roccpa.org.tw/)之會計師執業名簿查詢。

B. 意見的基礎：會計師驗證信的文字必須明確使執業會計師代表申請者，且會計師驗證信的結論是根據執業會計師熟悉相關事實所陳述與專業知識和專業判斷的運用。會計師驗證信也可能包括免責聲明和其他在執業會計師管轄範圍的習慣法上的限制。會計師

驗證信如果被證明是錯誤的，前提是該免責聲明不能擴大到消除對執業會計師的任何實質風險(財務、專業和/或聲譽)。

C. 真確性：為了確認會計師驗證信的真確性，註冊中心必須打電話或送會計師驗證信之副本給表列在負責執業會計師註冊(登記)或執照發放的主管機關的地址、電話、傳真或電子郵件(如果可以的話)給執業會計師並取得確認，或由執業會計師協助確認會計師驗證信是真實可靠的。

如果無法從發執照的主管機關取得電話號碼，註冊中心可使用適用的電信公司、合格的政府資訊來源或合格的獨立資訊來源紀錄中表列的執業會計師之電話號碼。

在會計師驗證信透過數位簽章下，會計師驗證信與簽章者之真確性如果如本節第(2).A 款經註冊中心確認，則不需要更進一步的真確性確認。

#### 3.2.3.4.3 面對面驗證

(1)驗證條款：在引用面對面審核傳遞給註冊中心的文件之前，註冊中心必須檢驗第三方驗證人滿足以下要求：

A. 第三方驗證者的合格性：註冊中心必須獨立地驗證第三方驗證者(Third-Party Validator)是有法律資格的拉丁公證人或公證人(或在申請者之被管轄區，具有同等法律效力)、在各該人員所在地之管轄區的律師或會計師；

B. 託管文件鏈：註冊中心必須驗證第三方驗證者複核檢查文件(Vetting Documents)以面對面見面之方式確認個人身分有被驗證。

C. 執業聲明書之驗證：如果第三方驗證者不是拉丁公證人，則註冊中心必須確認此執業聲明書(attestation)和檢查文件的真確性。

(2)可接受的驗證方式：建立檢查文件前述要求的可接受方式為：

A. 第三方驗證者的合格性：註冊中心必須藉由直接接觸在可適用管轄區負責第三方驗證者註冊(登記)或執照的主管機構以驗證第三方驗證者的專業地位。

B. 託管文件鏈：第三方驗證者必須向註冊中心提交一份聲明書，以聲明他們在面對面的會面期間獲得了提交給註冊中心對個人的檢查文件。

C.執業聲明書之驗證：如果第三方驗證人不是公證人，那麼註冊中心必須確認執業聲明書和第三方驗證人收到的檢查文件的可信賴性。註冊中心必須打電話給第三方驗證人並從他們得到確認或他們執行面對面驗證的協助。註冊中心可能依賴從為了執行這樣驗證流程的單一目的之第三方驗證人取得而自行登載(self-reported)的資訊。在執業聲明書透過數位簽章下，執業聲明書與簽章者之真確性如果如本節第(1)A.款之方式經註冊中心確認，則不需要更進一步的真確性確認。

#### 3.2.3.4.4 來自申請者的獨立確認

來自申請者的獨立確認(Independent Confirmation From Applicant)是針對特定的事實(例如確認合約簽署者或憑證遞件核准者的工作或代理狀態、憑證遞件核准者的EV授權來源之確認等等)，亦即：

- 由註冊中心從確認者(Confirming Person)(和負責提出請求的主體不同的某人)收到，而且有適當的授權可以確認以下之事實以及誰代表他已經確認此事實。
- 由註冊中心以鑑別和驗證此確認的來源方式收到；
- 與申請者連結(Binding)

  任何從申請者之獨立確認可能可透過以下程序取得：

  (1)確認需求：註冊中心必須透過適當的另外的安全管道之通信啟動確認需求，要求驗證或確認討論中的特定事實如下：

  A.收件人：必須定向到此確認需求者：

  (I) 在申請者的組織內的職位符合確認者(例如秘書、總裁、執行長(Chief Executive Officer, CEO)、財務長(Chief Financial Officer, CFO)、營運長(Chief Operating Officer, COO)、資訊長(Chief Information Officer, CIO)、資安長(Chief Information Security Officer, CISO)、(部門)主管等等)的資格而且可被現行的合格的政府資訊來源、合格的政府稅收資訊來源、合格的獨立資訊來源、法律驗證意見書、會計師驗證信之姓名或職稱確認，或藉由使用通信的驗證方法接觸申請者；或

  (II)在法人組織或公司的管轄範圍如同法人登記機關的正式紀錄所列之申請者的註冊代理人或登記辦公室，附

帶說明指定轉送給恰當的確認者；或

(III) 經指定的個人是透過電話或電子郵件(根據 EV SSL Certificate Guidelines 驗證其電話號碼或申請者的營業地點)接觸申請者的人力資源部門驗證在合約簽署者或憑證遞件核准者之上的直接主管。

B. 通信的方式：確認請求必須在合理可能達到此人的方式定向到確認者。下列選項是可以接受的：

(I) 通過紙本郵件郵寄給確認者於：

(i) 依照 EV SSL Certificate Guidelines 由註冊中心確認申請人的營業地點，或

(ii) 在現行合格的政府資訊來源、合格的政府稅收資訊來源、合格的獨立資訊來源、法律驗證意見書或會計師驗證信指明的確認者之營業地址，或

(iii) 於公司或法人組織管轄範圍的官方紀錄所列的申請者登記的代理人或登記辦公室之地址，或

(II) 透過電子郵件寄給確認者在現行合格的政府資訊來源、合格的政府稅收資訊來源、合格的獨立資訊來源、法律驗證意見書或會計師驗證信指明的確認者之營業地址所表列的業務電子郵件地址，或

(III) 透過打電話給確認者在申請者的營業地點之主要電話號碼(根據 EV SSL Certificate Guidelines 進行驗證)聯繫，並要求跟確認者講話且有人講電話確認他/她就是確認者；或

(IV) 藉由傳真給營業地點的確認者，傳真號碼必須列在現行合格的政府資訊來源、合格的政府稅收資訊來源、合格的獨立資訊來源、法律驗證意見書或會計師驗證信。封面頁必須清楚地給確認者。

(2) 確認回應：註冊中心必須收到從確認者對於確認請求之回應以確認討論中的特定議題。如此的回應可能藉由電話、電子郵件或紙本信件提供給註冊中心，因此註冊中心可以可倚賴地確認是由確認者提供作為確認請求之回應。

(3) 註冊中心可能倚賴經驗證的確認者以確認他們自己的聯繫資

訊：電子郵件地址、電話號碼和傳真號碼。註冊中心可能倚賴這些經驗證的聯絡資訊以作為未來和確認者聯繫，如果：

A. 電子郵件地址的網域是由申請者擁有而且是確認者自己擁有的電子郵件地址而非群組之電子郵件別名；

B. 確認者的電話/傳真號碼經由註冊中心確認為特定電話號碼是組織之電話系統的一部份，而且不是該確認者私人的電話號碼。

### 3.2.3.4.5 合格的獨立資訊來源

合格的獨立資訊來源是經常更新並且是公眾可存取的資料庫通常被為公認為某些特定資訊可信賴之來源。而且：

(1) 憑證服務業以外的產業依賴此資料庫提供準確的位置、聯絡資訊和其他資訊；和

(2) 資料庫提供者至少每年更新 1 次其資料。

本管理中心與註冊中心將使用文件化的程序檢查資料庫的準確性並確保其資料可被接受，包括審查資料庫提供者的使用條款。

本管理中心與註冊中心將不使用任何在合格的獨立資訊來源之資料屬於(i)自行登載與(ii)未經合格的獨立資訊來源確認為準確的資料。本管理中心和本公司或附屬公司若有資料庫的控股，或是任何註冊中心或本管理中心若有委外任何部分驗證程序的下包商(或其擁有者或附屬公司)維持任何資料庫的擁有權或實質利益，則不被視為合格的獨立資訊來源。

### 3.2.3.4.6 合格的政府資訊來源

合格的政府資訊來源是定期更新且現行公眾可取得、為了準確提供可被諮詢且一般被公認為可信賴的資料庫而設計且由政府機關(構)維護，例如經濟部全國工商登記資料庫。資料的報告是根據法律規定，且虛假或誤導性的報告將被處以刑事或民事處罰。EV SSL Certificate Guidelines 不禁止使用第三方供應商從政府機關(構)取得的資訊，如果這些第三方供應商是從政府機關(構)直接取得資訊。

#### 3.2.3.4.7 合格的政府稅務資訊來源

合格的政府稅務資訊來源是特定包含與私人組織、其他商業團體或個人相關稅務資訊(例如中華民國的財稅資料中心、國稅局、美國的國稅局(IRS))的合格政府稅務資訊來源。

### 3.2.4 未經驗證之用戶資訊

所有記載於憑證裡面的資訊都必須經過驗證。

### 3.2.5 授權之確認

當某個個人與憑證主體之名稱有關連，進行憑證生命週期活動如憑證申請或廢止請求時，本管理中心或註冊中心應進行授權之驗證(Validation of Authority)，確認該個人可代表憑證主體，例如：

(1)藉由電話、郵件、電子郵件等聯絡方式(從其他非憑證申請代表人的來源取得)或其他相當之程序確認該個人確實任職於該憑證主體(某組織或公司)得到授權代表該憑證主體。

(2)藉由臨櫃面對面核對身分或其他可信賴的通信方式確認該個人代表組織。

(3)確認申請者對 EV TLS/SSL 憑證的授權，已於第 3.2.3 節詳述，包括：

A.驗證合約簽署者、憑證遞件核准者和憑證請求者的姓名、職稱和職權。

B.確認合約簽署者已簽署用戶約定條款或經授權的申請者代表已同意使用條款；和

C.確認憑證遞件核准者已簽署或以其他方式核准 EV TLS/SSL 憑證請求。

EV TLS/SSL憑證申請，必須依照EV SSL Certificate Guidelines所建議之方式擇一或多項(參酌本作業基準第3.2.5.1節至第3.2.5.7節)鑑別用戶具備網域名稱之控制權，EV TLS/SSL憑證申請，除了鑑別用戶具備網域名稱之控制權外，尚須依照第3.2.2與第3.2.3節規定進行組織或個人的身分鑑別。

#### 3.2.5.1 驗證申請者為網域名稱聯絡人

驗證申請者是網域名稱聯絡人(Domain Contact)以確認申請者具備完全吻合網域名稱之控制權。此方法只能用於本管理中心為基礎網域名稱(Base Domain Name)的網域名稱受理註冊機構 (Domain Name Registrar)或網域名稱受理註冊機構之關係企業組織。例如中華電信數據通信分公司是.tw之網域名稱受理註冊機構，並負責營運本管理中心。

一旦使用此方法驗證了某個完全吻合網域名稱，本管理中心也可以對與該經驗證的完全吻合網域名稱的所有標籤結尾相同的其他完全吻合網域名稱簽發EV TLS/SSL憑證。此方法符合Baseline Requirements第3.2.2.4.12節對網域名稱驗證之規定。

#### 3.2.5.2 寄電子郵件、傳真、寄簡訊或郵寄信件給網域名稱聯絡人

本管理中心或註冊中心透過寄電子郵件、發送傳真、簡訊或郵寄信件傳送隨機值給該網域之聯絡人，並在收到此隨機值之確認回應後，確認此申請者擁有該完全吻合網域名稱(FQDN)之控制。此隨機值必須送到確認為網域聯絡人之電子郵件地址、傳真號碼、簡訊號碼或郵寄地址。

每封電子郵件、傳真、簡訊或郵寄信件可確認多個經授權網域名稱之控制權。

本管理中心或註冊中心可發送依照本節所確認之電子郵件、傳真、簡訊或郵寄信件給一個或多個收件者，前提是每個收件者都經網域名稱受理註冊機構以電子郵件、傳真、發送簡訊或郵寄信件確認，以代表要驗證的完全吻合網域名稱(FQDN)之網域名稱註冊者。

在每封電子郵件、傳真、簡訊或郵寄信件的隨機值應為唯一的。

本管理中心或註冊中心可重新發送電子郵件、傳真、簡訊或郵寄信件的全部，包括重新使用隨機值，前提是該通信的全部內容和收件人保持不變。

隨機值從其產製後30天內得到確認回覆，應視為有效。

一旦使用此方法驗證了某個完全吻合網域名稱，本管理中心也可以對與該經驗證的完全吻合網域名稱的所有標籤結尾相同的其他完全吻合網域名稱簽發EV TLS/SSL憑證。此方法符合Baseline Requirements第3.2.2.4.2節對網域名稱驗證之規定。

#### 3.2.5.3 構建的電子郵件(Constructed Email)

確認申請者對完全吻合網域名稱之控制，藉由 (1)寄送電子郵件到經授權網域名稱前加上webmaster、hostmaster或postmaster等前置字為電子郵件帳號(例如憑證申請者其經授權網域名稱為abc.com，發電子郵件給webmaster@abc.com、hostmaster@abc.com或postmaster@abc.com)的一或多個電子郵件帳號 (2)在此電子郵件包含隨機值且 (3)收到使用隨機值的確認回應，確認申請者對完全吻合網域名稱之控制權。

每一封電子郵件可確認多個完全吻合網域名稱的控制，前提是在此封電子郵件使用的經授權網域名稱是對於每一個正被確認的完全吻合網域名稱的經授權網域名稱。

在每封電子郵件的隨機值應為唯一的。

本管理中心或註冊中心可重新發送電子郵件的全部，包括重新使用隨機值，前提是該通信的全部內容和收件人保持不變。

隨機值從其產製後30天內得到確認回覆，應視為有效。

一旦使用此方法驗證了某個完全吻合網域名稱，本管理中心也可以對與該經驗證的完全吻合網域名稱的所有標籤結尾相同的其他完全吻合網域名稱簽發EV TLS/SSL憑證。此方法符合Baseline Requirements第3.2.2.4.4節對網域名稱驗證之規定。

#### 3.2.5.4 由對特定網頁內容的約定變更

藉由確認請求符記或隨機值包含在檔案的內容，確認申請者的完全吻合網域名稱之控制：

(1) 整個請求符記或隨機值一定不能出現在用於擷取檔案的請求中；並且

(2) 管理中心必須從請求中收到成功的 HTTP 回應(意味著必須接收 2xx HTTP 狀態代碼)。

包含請求符記或隨機值的檔案：

(1) 必須位於經授權網域名稱上，並且

(2) 必須位於“ /.well-known/pki-validation”資料夾下，並且

(3) 必須透過“ http”或“ https”方式擷取，並且

(4)必須透過經授權埠擷取。

如果憑證申請者採網域名稱轉址(Redirects,也稱為URL重新導向),則適用以下條件：

(1)網域名稱轉址須在 HTTP 協定層啟動

A.對於在 110 年 7 月 1 日以後之驗證，轉導必須是如 RFC 7231 第 6.4 節定義之 301、302 或 307 狀態碼回應的結果或是 RFC 7538 定義的 308 HTTP 狀態碼回應。如 RFC 7231 第 7.1.2 節中所定義，網域名稱轉址必須是 Location HTTP response 標頭的最終值。

B.對於在 110 年 7 月 1 日以前之驗證，網域名稱轉址必須是如 RFC 7231 第 6.4 節所定義在 3xx 網域名稱轉址狀態碼分類的 HTTP 狀態碼結果。本管理中心限制可接受的狀態碼和資源 URL 在前條 A 之範圍內。

(2)必須透過“ http”或“ https”方式之網域名稱轉址到資源 URL。

(3)網域名稱轉址必須是藉由經授權埠號存取的資源 URL。

如果使用隨機值，本管理中心或註冊中心應提供針對憑證請求唯一之隨機值，而且不應使用超過30天。一旦使用此方法驗證了某個完全吻合網域名稱，管理中心也可以對該經驗證的完全吻合網域名稱的所有標籤結尾相同的其他完全吻合網域名稱簽發SSL憑證。此方法符合Baseline Requirements第3.2.2.4.18節對網域名稱驗證之規定。

### 3.2.5.5 網域名稱系統之變更(DNS Change)

對於經授權網域名稱或經授權網域名稱前置一下底線字元的標籤(label)，藉由確認隨機值、請求符記於DNS TXT、授權憑證機構簽發憑證紀錄(CAA record)之出現，以確認申請者對於完全吻合網域名稱之控制。

如果使用隨機值，本管理中心或註冊中心應提供針對憑證請求唯一之隨機值，而且不應使用超過(1)30天或(2)如果申請者遞送憑證請求，憑證相關之驗證資料允許重新使用之時間範圍(如第3.5節)。

一旦使用此方法驗證了某個完全吻合網域名稱，本管理中心也可以對與該經驗證的完全吻合網域名稱的所有標籤結尾相同的其他完全吻

合網域名稱簽發EV TLS/SSL憑證。此方法符合Baseline Requirements第3.2.2.4.7節對網域名稱驗證之規定。

#### 3.2.5.6 寄送電子郵件至網域名稱系統授權憑證機構簽發憑證聯絡人 (Email to DNS CAA Contact)

透過寄送電子郵件傳送隨機值，並在收到此隨機值之確認回應後，確認申請者對於該完全吻合網域名稱之控制。此隨機值必須寄送到網域名稱系統授權憑證機構簽發憑證聯絡人(DNS CAA Email Contact)。DNS CAA Email Contact係網域擁有者於CAA Record公布的電子郵件地址，其格式定義於Baseline Requirements Section B.1.2。相關的授權憑證機構簽發憑證資源紀錄集必須使用定義於RFC 8659第3節的搜尋演算法。

每一封電子郵件可確認多個完全吻合網域名稱的控制，前提是該電子郵件地址是正被確認的經授權網域名稱(Domain Name)之DNS CAA Email Contact。只要所有收件人都是正被確認的經授權網域名稱的DNS CAA Email Contact，就可以將同一封電子郵件發送給多個收件人。

在每封電子郵件中的隨機值應為唯一。本管理中心或註冊中心可重新發送該封電子郵件，包括重新使用隨機值，前提是該電子郵件的全部內容和收件人保持不變。隨機值從其產製後30天內得到確認回覆，則應視為有效。

一旦使用此方法驗證了某個完全吻合網域名稱，本管理中心也可以對該經驗證的完全吻合網域名稱的所有標籤結尾相同的其他完全吻合網域名稱簽發SSL憑證，此方法也適用於驗證萬用網域名稱。此方法符合Baseline Requirements第3.2.2.4.13節對網域名稱驗證之規定。

#### 3.2.5.7 寄送電子郵件至 DNS TXT Contact (Email to DNS TXT Contact)

透過寄送電子郵件傳送隨機值，並在收到此隨機值之確認回應後，即確認申請者對於該完全吻合網域名稱之控制。此隨機值必須寄送到DNS TXT Record Email Contact。DNS TXT Record Email Contact係於DNS TXT公布網域擁有者的電子郵件地址，其格式定義於Baseline Requirements Section B.1.2。

每一封電子郵件可確認多個完全吻合網域名稱的控制，前提是該電子郵件地址是正被確認的經授權網域名稱之DNS TXT Record Email Contact。只要所有收件人都是正被確認的經授權網域名稱的DNS TXT

Record Email Contact，就可以將同一封電子郵件發送給多個收件人。

在每封電子郵件中的隨機值應為唯一。本管理中心或註冊中心可重新發送該封電子郵件，包括重新使用隨機值，前提是該電子郵件的全部內容和收件人保持不變。隨機值從其產製後30天內得到確認回覆，則應視為有效。

一旦使用此方法驗證了某個完全吻合網域名稱，本管理中心也可以對該經驗證的完全吻合網域名稱的所有標籤結尾相同的其他完全吻合網域名稱簽發SSL憑證，此方法也適用於驗證萬用網域名稱。此方法符合Baseline Requirements第3.2.2.4.14節對網域名稱驗證之規定。

### 3.2.6 互運之準則

本管理中心非根憑證機構，故不適用。

### 3.2.7 資料來源正確性

在使用任何資料來源作為可靠資料來源之前，本管理中心應評估此來源的可靠性、正確性和對變更或偽造的抵抗性。本管理中心在評估過程中應考慮下列事項：

(1) 所提供資訊的存在時間。

(2) 資訊來源的更新頻率。

(3) 資料提供者和資料收集的目的。

(4) 資料可用性的公用可存取性。

(5) 偽造或變更資料的相對困難性。

由本管理中心、其擁有者或其附屬公司所維護的資料庫，如果資料庫的主要目的是為了滿足Baseline Requirements第3.2節的驗證要求而蒐集的資訊，則不符合可靠資料來源。

### 3.2.8 其他驗證條款

#### 3.2.8.1 高風險狀態

Baseline Requirement的第4.2.1節條款同樣適用於EV TLS/SSL憑證。高風險憑證請求之識別與鑑別參見本作業基準之第4.2.1節。

### 3.2.8.2 否決列表和其他合法的黑名單

(1)驗證條件:本管理中心和註冊中心必須驗證申請者、合約簽署者、憑證遞件核准者、申請者的組織註冊管轄權、註冊或營業地點是否：

A.被確認在任何政府之否決列表，禁止的人員列表或其他表列禁止和如此之組織或人員在本管理中心的營運管轄範圍之國家執行業務；或

B.於任何組織設立、登記或營業地點的國家，本管理中心的管轄範圍之法律禁止執行業務。如果申請者、合約簽署者或憑證遞件核准者或若申請者的公司或組織設立或登記或執行業務的地點之管轄範圍被列在任何的否決列表，本管理中心將不簽發 EV TLS/SSL 憑證給該申請者。

(2)可被接受的驗證方式： 採取適當合理步驟以驗證 EV SSL Certificte Guidelines 之否決列表和法規。

### 3.2.8.3 母公司/子公司/關係企業組織關係

註冊中心驗證申請者使用申請者的母公司/子公司，或當符合第3.2.2.4.1節、第3.2.2.5節、第3.2.2.6.1節或第3.2.2.7節允許情況時，必須驗證申請者和母公司、子公司或關係企業組織之關係。可接受的驗證申請者和母公司、子公司或關係企業組織關係的方法包括：

(1)合格的獨立資訊來源或合格的政府資訊來源:申請者和母公司、子公司或關係企業組織之間的關係於合格的獨立資訊來源或合格的政府資訊來源確認；

(2)從母公司、子公司或關係企業組織的獨立確認:註冊中心可藉由從適當的母公司、子公司或關係企業組織(如第 3.2.3.4.4 節所述)取得獨立的確認驗證申請者和母公司、子公司或關係企業組織關係。

(3)本管理中心或註冊中心和母公司、子公司或關係企業組織之間的合約:本管理中心或註冊中心可能驗證申請者和母公司、子公司或關係企業組織之間的關係,藉由倚賴本管理中心或註冊中心和母公司、子公司或關係企業組織之間的合約指派憑證遞件核准者具備 EV 授權來源,假設此合約是由合約簽署者簽署且假設合約

簽署者的簽署權力來源與代表性已經被驗證；

(4)法律意見:註冊中心可能藉由倚賴法律驗證意見書驗證申請者和母公司、子公司或關係企業組織之間的關係；

(5)會計師驗證信:註冊中心可能藉由倚賴會計師驗證信驗證申請者和母公司、子公司或關係企業組織之間的關係；或

(6)公司決議:註冊中心可能藉由適當鑑別核准子公司設立的公司決議驗證申請者和子公司之間的關係;或申請者倘若此決議為(I)經過適當的公司職員(例如秘書)驗證,和(II)註冊中心可以可靠地驗證此憑據是由此人有效地簽署,而且此人有此不可或缺的權力提供如此之憑據。

### 3.2.8.4 最後交互關連與基於良善管理之盡職調查

除了企業EV TLS/SSL憑證(Enterprise EV TLS/SSL Certificate)以外：

(1)驗證流程的結果和在 EV SSL Certificate Guidelines 描述的程序是為了能夠被個別與群組地雙重檢視。在所有的驗證流程和程序完成後，本管理中心必須有一名非負責蒐集資訊的人員，檢視所有的資訊和文件組合以支持 EV TLS/SSL 憑證申請，並找尋差異或其他需要更進一步解釋的資訊。

(2)本管理中心必須取得,並以文件證明從申請者、憑證遞件核准者、憑證請求者、合格獨立資訊來源，和/或其他資訊來源的更進一步解釋或澄清，以解決那些差異或需要更進一步解釋的細節。

(3)EV TLS/SSL 憑證之簽發不僅僅溝通本管理中心根據事實已經知道的資訊，而是實施基於良善管理之謹慎調查，從組合的資訊和文件發現是否有任何不正確的資訊。直到整個資訊和文件的組合得以支持 EV TLS/SSL 憑證請求，才會簽發 EV TLS/SSL 憑證。如果無法在合理的時間內收到滿意的解釋和/或額外的文件，本管理中心將拒絕 EV TLS/SSL 憑證請求而且通知申請人。

(4)如果用以支持申請的部分或所有文件不是以本管理中心正常營運所用的語言,本管理中心必須執行此最後交互關連與基於良善管理的謹慎調查，由具有適當訓練、經驗及判斷的人員，對組織之識別和授權進行確認，以符合所有在 EV SSL Certificate Guidelines 第 14.1 節符合資格的條款。當本管理中心的人員不具備此必須之語言與訓練以執行此最後交互關連與基於良善管理

的謹慎調查時，可能：

A.倚賴文件之相關部分的語言翻譯，如果此翻譯從翻譯者(Translator)而來；或

B.假設註冊中心符合本節之(1)、(2)與(3)款，本管理中心可能倚賴註冊中心之語言技能執行最後交互關連與基於良善管理之盡職調查。儘管有前述，在簽發 EV TLS/SSL 憑證之前，本管理中心必須覆核由註冊中心完成的工作並決定所有的條款都符合；或

C.當本管理中心使用註冊中心之服務，本管理中心可能倚賴該註冊中心執行最後交互關連與基於良善管理之盡職調查，假設該註冊中心符合本節與遵從 EV SSL Certificate Guidelines 第 17.5 與 17.6 節的稽核條款。

在符合 EV SSL Certificate Guidelines 第 14.2 節條款，簽發企業 EV TLS/SSL 憑證之前，企業註冊中心可執行本節所述之最後交互關連與基於良善管理之盡職調查。

## 3.3 金鑰更換請求之識別及鑑別

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，依照第3.2節規定進行識別及鑑別。

### 3.3.1 例行性金鑰更換之識別及鑑別

用戶申請EV TLS/SSL憑證即將到期前兩個月，系統將寄送電子郵件提醒用戶重新申請憑證，由申請者產製新的金鑰對並使用其新的私密金鑰對憑證申請檔加以簽章，並將該憑證申請檔及簽署之用戶約定條款交給註冊中心，註冊中心依照第3.2及第3.3節規定，對於憑證將到期重新申請憑證之用戶進行識別及鑑別。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。

本管理中心不接受用戶申請EV TLS/SSL憑證展期。

### 3.3.2 憑證廢止後金鑰更換之識別及鑑別

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，註冊中心將依照第3.2、第3.3與第3.4節規定，對於重新申請憑證之用戶進行識別及鑑別。

## 3.4 憑證廢止請求之識別及鑑別

本管理中心或註冊中心必須對於憑證廢止申請進行鑑別，以確認申請者為有權提出憑證廢止之申請者，憑證廢止申請之鑑別程序與第3.2與第3.3節規定相同。

## 3.5 現存文件之重用條款

對於每件EV TLS/SSL憑證請求，包括要求更新現存之EV TLS/SSL憑證，本管理中心或註冊中心必須執行所有EV SSL Certificate Guidelines要求的鑑別和驗證工作，以確保此請求適當地得到申請者之授權且在EV TLS/SSL憑證內之資訊仍然準確和有效。本節對於本管理中心和註冊中心蒐集之文件的使用，規定其時間限制。

### 3.5.1 現有用戶之驗證

若憑證申請者有本管理中心所簽發有效之EV TLS/SSL憑證，本管理中心和註冊中心可以倚賴先前之鑑別與驗證：

(1) 依據第 3.2.2.2.2 節第(4)款，此代表人是被本管理中心或註冊中心所驗證過的相同身分，以連結到此申請者先前被簽發與目前有效之 EV TLS/SSL 憑證；

(2) 依據第 3.2.2.4.1 節所述之申請者營業地點；

(3) 依據第 3.2.2.5 節所述之申請者通信方式的驗證，但仍必須執行由第 3.2.2.5.2 節第(2)款所要求的驗證；

(4) 依據第 3.2.2.6 節所述之申請者營運存在；

(5) 依據第 3.2.3.1 節所述之合約簽署者和憑證遞件核准者的名稱、職稱、機構與授權；與

(6) 依據第 3.2.2.7 及第 3.2.2.4 節所述之申請者使用具體說明的網域名稱的權利，前提是本管理中心或註冊中心驗證 WHOIS 紀錄仍然顯示相同的網域註冊者如同本管理中心或註冊中心驗證初始的 EV TLS/SSL 憑證之特定的網域名稱。

### 3.5.2 重新簽發請求

本管理中心可能依賴先前驗證過的憑證請求檔去簽發更新憑證，只要原憑證不是因為犯罪或其他非法行為而被廢止，如果：

(1) 更新憑證之到期日與被取代的 EV TLS/SSL 憑證之到期日相同

(2) 憑證之主體資訊和被取代的 EV TLS/SSL 憑證之主體資訊相同

### 3.5.3 驗證資料之年份

(1) 除了在第 3.5.2 節所述關於 EV TLS/SSL 憑證之重發，和除了在第 3.5.1 節所允許情形外，所有用於支援 EV TLS/SSL 憑證簽發的資料年份不應該超過以下限制：

A. 法律存在和實體：398 天

B. 化名：398 天

C. 營業地點：398 天

D. 已驗證的通信方法：398 天

E. 營運存在性：398 天

F. 網域名稱：398 天

G. 姓名、頭銜(職稱)、機構和授權：398 天，除非在本管理中心和申請者之間的合約指定其他期限，在此種情況，由該合約之期限控制。例如，合約可能包括 EV 角色的長期指派，直到由申請者或本管理中心的廢止，或直到合約期滿或終止。

(2) 上述列舉的 398 天之期限應自本管理中心蒐集上述資訊的日子起算。

(3) 本管理中心可重複使用先前提交之 EV TLS/SSL 憑證請求檔、用戶約定條款(購買合約條款)或使用者條款，包含使用單一憑證請求檔支援多張 EVSSL 憑證包含相同主體於第 3.2.3.2 節與第 3.2.3.3 節所允許的範圍。

(4) 除非是第 3.5.1 節之規定外，對於取得時間超過前述時間限制的資訊，本管理中心必須重複執行於 EV SSL Certificate Guidelines 與本作業基準所要求的確認程序。

# 4 憑證生命週期營運規定

## 4.1 憑證申請

### 4.1.1 憑證之申請者

電腦及通訊設備(如路由器、防火牆、資料庫安全稽核硬體等)或應用軟體(如 Web Server、e-mail Server、Application Server 或 Lync Server 等)等財產類別，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。EV TLS/SSL 憑證必須由組織例如政府機關(構)、私人組織、非營利國際組織或其他商業團體擔任申請者提出申請。

EV TLS/SSL 憑證之簽發必須有以下第 3 章描述由申請者授權的 3 種角色：

憑證請求者：EV 憑證請求必須由得到授權的憑證請求者簽章與傳遞。

憑證遞件核准者：EV TLS/SSL 憑證請求必須由經授權之憑證遞件核准者檢查與核准。

合約簽署者：適用於 EV TLS/SSL 憑證請求的用戶約定條款必須由經授權的合約簽署者簽署。

申請者可授權某位自然人擔任上述一個或多個角色。

### 4.1.2 註冊程序及責任

本管理中心與註冊中心負責確保憑證申請者的身分在憑證簽發前依據 HiPKI 憑證政策、本作業基準與 EV SSL Certificate Guidelines 之規定確認，憑證申請者要負責提供足夠充分與正確的資訊(如組織之法定名稱與註冊號碼、憑證申請者之姓名與網站之完全吻合網域名稱)與身分證明文件給註冊中心與本管理中心在憑證簽發前執行必要的身分識別與鑑別工作。用戶應負以下之責任：

(1) 用戶應遵守本作業基準及用戶約定條款有關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，用戶應依照第 4.4 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，並依照第 1.4.1 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。

## 4.2 憑證申請之程序

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) 憑證申請者自行產製金鑰，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透過安全管道傳遞給註冊中心。

### 4.2.1 執行識別及鑑別

本管理中心及註冊中心確保系統與程序足以鑑別用戶身分以符合 HiPKI 憑證政策與憑證實務作業基準的規定。初始註冊程序依照憑證實務作業基準第 3.2 節之規定執行，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。由憑證申請者提供之資訊及於申請過程中之聯繫紀錄由本管理中心與註冊中心依 HiPKI 憑證政策及憑證

實務作業基準之規定以安全也可被稽核之方式妥善保管。

本管理中心及註冊中心針對高風險憑證請求在憑證核准簽發前確認與執行額外之檢查，除了第 3.1.2.1 節與第 3.2.2.7 節所述程序外，於註冊中心系統維護由於先前涉嫌網路釣魚或其他詐欺使用而被拒絕的憑證請求或遭廢止憑證的內部資料庫，並據以比對而識別後續可疑或高風險的憑證請求。針對有較高的風險做為網路釣魚或其他詐騙使用的完全吻合網域名稱、本管理中心或註冊中心所蒐集一些組織如 Anti-Phishing Working Group (APWG)所公布之釣魚網站網址、先前被拒絕的憑證請求的完全吻合網域名稱或是瀏覽器廠商提供其擁有並不准發放 SSL 憑證之完全吻合網域名稱，設置有提醒憑證註冊審驗人員注意之黑名單，或由憑證註冊審驗人員輸入於憑證主體別名屬性將註記而有疑慮的完全吻合網域名稱於谷歌安全瀏覽列表 (Google Safe Browsing list)或米勒-史麥爾釣魚列表(Miller Smiles phishing list)進行檢查，以防止 EV TLS/SSL 憑證之誤發。

#### 4.2.1.1 授權憑證機構簽發憑證紀錄

核發EV TLS/SSL憑證前，對於即將簽發的EV TLS/SSL憑證註記在subjectAltName擴充欄位的每一個dNSName(亦即申請者提出憑證請求所包含的每一個完全吻合網域名稱)，憑證註冊審驗人員必須向網域名稱系統(Domain Name System, DNS)檢查依據RFC 8659所規範之授權憑證機構簽發憑證DNS資源紀錄(DNS Resource Record)，通過後始准予發放。亦即若某完全吻合網域名稱其CAA紀錄之"issue"標籤中包含"pki.hinet.net"或"tls.hinet.net"，則本管理中心將簽發其EV TLS/SSL憑證。如果"iodef"屬性標籤出現在CAA紀錄，本管理中心將和申請者溝通後決定是否簽發EV TLS/SSL憑證。

本管理中心或註冊中心檢查網域名稱系統查閱EV TLS/SSL憑證申請案件所將註記之完全吻合網域名稱是否有授權憑證機構簽發憑證DNS資源紀錄，若授權憑證機構簽發憑證DNS資源紀錄存在且未將本管理中心列為授權此EV TLS/SSL憑證簽發之憑證管理中心，本管理中心將視該憑證申請為同意授權本管理中心針對該完整網域名稱簽發EV TLS/SSL憑證，並要求用戶先行前往其網域名稱系統更新授權憑證機構簽發憑證DNS資源紀錄將本管理中心列入，完成後再簽發EV TLS/SSL憑證。

本管理中心或註冊中心在下列查詢授權憑證機構簽發憑證DNS資源紀錄失敗情況下，可簽發EV TLS/SSL憑證：(1)在非本管理中心基礎設施中查詢CAA紀錄失敗；(2)至少嘗試過一次重新找尋CAA紀錄；及(3)網域名稱所在區域不存在指向網際網路名稱和編號註冊中心(The Internet Corporation for Assigned Names and Numbers, ICANN)根之DNSSEC驗證鏈。

### 4.2.2 憑證申請之批准或拒絕

本管理中心將不會核發包含內部名稱或保留 IP 位址的 EV TLS/SSL 憑證。經授權網域名稱及基礎網域名稱之驗證須符合規範，相關驗證機制詳述於第 3.2.5 節並請參考第 1.6.1 節名詞解釋。

註冊中心會指派不同於負責搜集申請者身分識別與鑑別資訊的憑證註冊審驗人員的另一名憑證註冊審驗人員檢核所有支援 EV TLS/SSL 憑證申請的資訊和文件，並找尋是否還有和本作業基準規範之身分識別與鑑別程序不一致處或是其他需要更進一步解釋之資料。在成功完成第 3.2.8.4 節規範之最後交互關連與基於良善管理之盡職調查，確保所有驗證身分之工作在遵循相關規定與最佳實務下可以成功執行，本管理中心及註冊中心可以批准憑證之申請。註冊中心用於處理和核准 EV TLS/SSL 憑證請求的系統由至少兩名信賴角色之行動來產生 EV TLS/SSL 憑證。

若各項驗證身分的工作無法成功完成，本管理中心及註冊中心得以拒絕憑證之申請。除因申請者之身分識別與鑑別之原因外，本管理中心及註冊中心得因其他原因不同意簽發憑證。本管理中心及註冊中心可能因為申請者先前曾遭拒絕憑證申請或因曾違反用戶約定條款而遭拒絕其憑證申請。

### 4.2.3 處理憑證申請之時間

本管理中心及註冊中心將在合理時間內完成憑證申請之受理。註冊中心在申請者提交的資料齊全且符合 HiPKI 憑證政策、憑證實務作業基準及各項查核要求下，註冊審驗窗口會儘速完成憑證申請之審核。註冊中心處理憑證申請的時間及管理中心簽發憑證的時間視不同憑證類別，可能於用戶約定條款、契約或本管理中心網站揭露。

EV TLS/SSL 憑證之申請件在收件且符合相關規定下，5 個工作天

內由至少兩名憑證註冊審驗人員完成審核程序，請用戶進行憑證接受，憑證接受後，本管理中心將於 1 個工作天內或用戶指定希望取得憑證的日期完成憑證簽發之作業。

## 4.3 憑證簽發

### 4.3.1 憑證簽發時憑證機構之作業

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) 本管理中心之憑證簽發程式具有 Pre-Issuance Linting 功能，可檢查待簽發憑證其格式是否符合 EV SSL Certificate Guidelines、Baseline Requirements/RFC 5280 之規定，若不符合將予以拒絕，以防止憑證之誤發或錯發。

(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(Non-Repudiation)，透過網路傳輸之憑證申請資料，係經數位簽章及傳輸層安全協定方式加密傳送。

(6) 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。

### 4.3.2 憑證機構對用戶之憑證簽發通知

本管理中心完成憑證簽發後，將通知用戶領取憑證或是透過註冊中心通知用戶領取憑證。

本管理中心或註冊中心如不同意簽發憑證，會以電子郵件或電話通知憑證申請者，並明確告知不同意簽發的理由。

用戶接受憑證時若發現憑證內之資訊不正確或與申請時提供的資料不一致時，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 憑證接受

本管理中心所簽發 EV TLS/SSL 憑證其接受憑證之程序為：

憑證申請者預先審視將簽發之憑證內容，憑證申請者審視憑證將註記之資訊是否正確且與申請時提供之資料一致，若憑證申請者審視將簽發之憑證內容後，拒絕接受將註記於憑證之資訊，則憑證不予簽發。例如憑證申請者預先審視將簽發之多網域 EV TLS/SSL 憑證之憑證主體別名欄位，發現尚有其他需要 TLS 加密通道之完全吻合網域名稱未申請註記，可拒絕接受該張多網域 EV TLS/SSL 憑證之簽發，另依照第 4.1 與第 4.2 節重新提出憑證申請。

上述憑證申請者在決定接受憑證前應審視的憑證欄位，至少應包括憑證主體名稱及憑證主體別名欄位。

接受憑證視為憑證申請者同意遵守本作業基準、用戶約定條款或相關合約上之權利與義務。

憑證申請者拒絕接受憑證，如涉及收費或退費問題時，應依據消費者保護法及公平交易原則所訂定之契約辦理。

### 4.4.1 構成接受憑證之事由

憑證申請者預先審視將簽發之憑證內容無誤，憑證經本管理中心公布於儲存庫或傳遞給憑證申請者。

### 4.4.2 憑證機構對簽發憑證之發布

本管理中心的儲存庫服務定期公布所簽發之憑證或是藉由將憑證傳遞給憑證申請者達成憑證之發布。註冊中心得與本管理中心協議將憑證透過註冊中心傳遞給憑證申請者。

### 4.4.3 憑證機構對其他個體之憑證簽發通告

本管理中心不對申請者與其所屬註冊中心以外的其他實體進行憑證簽發之通告，信賴憑證者可逕行至本管理中心的儲存庫查詢或下載憑證。

## 4.5 金鑰對及憑證之用途

### 4.5.1 用戶私密金鑰及憑證之用途

用戶係指已申請並取得本管理中心核發 EV TLS/SSL 憑證之個體，其與憑證主體之關係如本作業基準第 1.3.3 節表格所示，EV TLS/SSL 憑證之應用範圍如本作業基準第 1.4.1 節所示，用戶金鑰對的產製應符合本作業基準第 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，用戶本身不簽發憑證給其他方。用戶應保護其私密金鑰不被他人未經授權的使用或揭露，且只使用其私密金鑰於正確的金鑰用途 (於憑證之擴充欄位有註記金鑰用途)，如 digitalSignature 或 keyEncipherment。用戶必須依據憑證所記載的憑證政策正確地應用憑證。

### 4.5.2 信賴憑證者公開金鑰及憑證之用途

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。信賴憑證者應使用符合 ITU-T X.509、IETF RFCs 或 EV SSL Certificate Guidelines 相關標準或規範的軟體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。

前述憑證狀態資訊可透過憑證廢止清冊或線上憑證狀態協定(Online Certificate Status Protocol, OCSP)查詢服務取得，憑證廢止清冊發布點(cRLDistributionPoints)的位置可在憑證的詳細資訊取得。此外，信賴憑證者也應檢驗簽發憑證機構(Issuing CA)與用戶憑證之certificatePolicies，確認憑證之保證等級。

例如信賴憑證者只有以下條件符合下才能相信數位簽章或 TLS 交

握(TLS handshake)：

(1)數位簽章或 TLS 通訊週期(TLS Session)是透過相對應有效的憑證產生，且能透過憑證串鏈驗證憑證之正確性。

(2)憑證並未被廢止且信賴憑證者在使用憑證前透過相關的憑證廢止清冊或線上憑證狀態協定回應訊息(OCSP Response)進行檢查。

(3)憑證依據其憑證實務作業基準之規定及其憑證用途使用。

## 4.6 憑證展期

憑證展期(renewal)是指在用戶識別資訊不變下重新簽發 1 張與原有憑證具有相同公開金鑰、相同憑證主體資訊、不同序號但效期展延的憑證。

基於公開金鑰隨時間延長可能導致私密金鑰安全度降低及遭破解機率增加，且 EV TLS/SSL 憑證是各類 SSL 憑證中依據 CA/Browser Forum 規範其重新驗證申請資料正確性之時間也最短(如第 3.5.1 節所述)，本管理中心不提供憑證展期之服務，請比照初始註冊另行產製金鑰對提出憑證申請。

### 4.6.1 憑證展期之情況

不適用。

### 4.6.2 憑證展期之申請者

不適用。

### 4.6.3 憑證展期之程序

不適用。

### 4.6.4 對用戶憑證展期之簽發通知

不適用。

### 4.6.5 構成接受展期之憑證的事由

不適用。

### 4.6.6 憑證機構對展期之憑證的發布

不適用。

### 4.6.7 憑證機構對其他個體之憑證簽發通知

不適用。

## 4.7 用戶憑證之金鑰更換

### 4.7.1 憑證金鑰更換之情況

用戶之私密金鑰必須依照第 6.3.2 節有關憑證用戶私密金鑰使用期限之規定定期更換。

用戶之 EV TLS/SSL 憑證沒有被廢止，本管理中心或註冊中心可於該用戶私密金鑰使用期限到期前 2 個月開始受理其更換金鑰並申請新的憑證，申請新憑證之程序依照第 4.1 與第 4.2 節規定辦理。

當用戶的 EV TLS/SSL 憑證被廢止後，其私密金鑰應停止使用，並於更換金鑰對後,依照第 4.1 與第 4.2 節規定向本管理中心申請新憑證。

### 4.7.2 更換憑證金鑰之申請者

用戶或合法授權之第三人(如組織授權之代理人)。

### 4.7.3 憑證金鑰更換之程序

用戶之憑證更換金鑰，請向本管理中心重新申請憑證，參見本作業基準第 3.1、第 3.2、第 3.3、第 4.1 及第 4.2 節之規定辦理。

### 4.7.4 對用戶憑證金鑰更換之簽發通知

依照第 4.3.2 節規定辦理。

### 4.7.5 構成接受金鑰更換之憑證的事由

依照第 4.4.1 節規定辦理。

### 4.7.6 憑證機構對金鑰更換之憑證的發布

依照第 4.4.2 節規定辦理。

### 4.7.7 憑證機構對其他個體之憑證簽發通知

註冊中心會接到金鑰更換之憑證簽發通知。

## 4.8 憑證變更

### 4.8.1 憑證變更之情況

憑證變更係指對同一憑證主體提供 1 張新的憑證，其記載資訊和舊的憑證有些許不同(例如更新主體唯一識別名稱或完全吻合網域名稱)，新的憑證有新的憑證序號，新憑證和舊憑證的公開金鑰及到期日相同。用戶如有變更組織名稱或完全吻合網域名稱時，須依第 4.1 與第 4.2 節規定的程序以變更後的組織名稱進行憑證的重新申請以取得有效的憑證。憑證變更後，舊憑證應予以廢止。

### 4.8.2 憑證變更之申請者

用戶或合法授權之第三人(如組織授權之代理人)。

### 4.8.3 憑證變更之程序

(1)憑證變更的申請者依據註冊中心制定之作業規範提出憑證變更的請求，註冊中心在接到憑證變更的請求後，即進行相關的審核程序，並保留所有變更後新憑證申請之請求以及原憑證廢止之請求紀錄，包含申請者名稱、聯絡資料、新憑證申請原因、原憑證廢止原因、原憑證廢止時間與日期等，以作為後續權責歸屬之依據。此處註冊中心制定之作業規範可參考第 4.1、第 4.2 與第 4.9 節，諸如要求變更憑證之申請者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。

(2) 註冊中心完成審核作業後，將新憑證申請與原憑證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新憑證申請與原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，之後依據註冊中心所送之新憑證申請簽發憑證，再依據註冊中心所送之原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，係經數位簽章及傳輸層安全協定加密傳送。

(6) 註冊中心應訂定憑證變更之新憑證申請與原憑證廢止之時間間隔，例如完成憑證變更簽發後，用戶使用新憑證無誤則應於新憑證簽發生效日後兩週內廢止原憑證。

### 4.8.4 對用戶憑證變更之簽發通知

依照第 4.3.2 節規定辦理。

### 4.8.5 構成接受變更之憑證的事由

依照第 4.4.1 節規定辦理。

### 4.8.6 憑證機構對變更之憑證的發布

依照第 4.4.2 節規定辦理。

### 4.8.7 憑證機構對其他個體之憑證簽發通知

本管理中心不對申請者與其所屬註冊中心以外的其他實體進行憑證變更之憑證簽發的通知，信賴憑證者可逕行至本管理中心的儲存庫查詢或下載憑證。

## 4.9 憑證廢止及停用

本節主要描述在何種情形下憑證得(或必須)予以廢止，並說明憑證廢止之程序。

### 4.9.1 憑證廢止之情況

以下幾種情況發生時，本管理中心應於 24 小時內廢止 EV TLS/SSL 憑證：

(1) 用戶以書面提交本管理中心同意廢止憑證

(2) 用戶告知本管理中心原有之憑證請求未經授權，且不追溯授予授權

(3) 本管理中心證實用戶之私密金鑰遭破解，且該私密金鑰與用戶憑證中所記載之公開金鑰成配對關係

(4) 得知一種經過驗證或證明的方法，可以根據憑證中的公鑰輕鬆計算用戶的私鑰

(5) 本管理中心證實憑證中所記載之完全吻合網域名稱或 IP 位址在網域授權或控制權之驗證上是不可信賴的

以下幾種情況發生時，本管理中心應於合理的時間範圍內(快則 24 小時內，最遲於 5 天內)廢止憑證：

(1) 用戶違反第 6.1.5 及第 6.1.6 節對於金鑰之長度及品質檢測之規定

(2) 本管理中心證實用戶之憑證遭到誤用

(3) 用戶違反用戶約定條款規定

(4) 憑證中所記載之完全吻合網域名稱或IP位址已被禁用(可能原因如網域名稱遭司法機關註銷或與網域名稱受理註冊機構之間的授權或合約到期)

(5) 憑證中所記載之資訊已變更(例如主體名稱變更、主體證號變更或主體身分因解散或死亡而消失等)

(6) 憑證未依 HiPKI 憑證政策或本作業基準之規定程序簽發時

(7) 憑證中所記載之資訊不正確(inaccurate)

(8) 本管理中心之簽發憑證的權力已逾期、被廢止或被中止，且不再

維運儲存庫、公布憑證廢止清冊或提供線上憑證狀態協定查詢服務

(9)HiPKI 憑證政策或本作業基準所規定應廢止項目

(10)獲悉已證明或經過驗證的方法會暴露用戶的私鑰，或者有明確的證據表明用於生成私鑰的特定方法存在缺陷。

本管理中心依照上述應廢止憑證之情況，得逕行廢止用戶憑證。

### 4.9.2 憑證廢止之申請者

用戶、註冊中心、本管理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)可提出憑證廢止申請。

### 4.9.3 憑證廢止之程序

(1)憑證廢止申請者依據註冊中心制定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，將憑證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。遭廢止的憑證其憑證序號及廢止理由必須包含於之後所公布的憑證廢止清冊，直到憑證到期為止。

(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，係經數位簽章及傳輸層安全協定方式加密傳送。

(6)本管理中心使用與簽發憑證時相同的管理中心私密金鑰將廢止憑證序號與憑證廢止理由等資訊經由數位簽章後記載於憑證廢止清冊。

(7)提供更即時的線上憑證狀態協定查詢服務。

(8)本管理中心提供 7 天 x 24 小時之憑證問題通報受理以及憑證問題回應機制如 4.9.3.1 節所述。

#### 4.9.3.1 憑證問題回應機制

本管理中心於網站儲存庫之「憑證實務作業基準公告事項」項目下，提供憑證問題回報之指引說明。用戶、信賴憑證者、應用軟體供應商或其他第三方可透過第 1.5.2.2 節之聯絡資訊向本管理中心提交憑證問題報告知會本管理中心合理之原因以廢止憑證。

### 4.9.4 憑證廢止請求之寬限期

憑證廢止申請的寬限期是指用戶在憑證廢止事由已經確認而必須提出憑證廢止申請的時間。註冊中心必須在 1 小時內通報本管理中心其註冊中心私密金鑰疑似遭破解的事由。用戶在其私密金鑰遺失或疑似遭破解或已被破解或是憑證所記載之資訊已經過時不正確時，應儘速向註冊中心提出憑證廢止之申請，憑證廢止申請之寬限期為 2 個工作天，本管理中心必要時得逐案延展其憑證廢止之寬限期。

### 4.9.5 憑證機構處理憑證廢止請求之處理期限

本管理中心在接收到憑證問題報告的 24 小時內，應調查有關的事實及情況，並提供 1 份初步的調查報告給用戶及報告回報者。

在審視有關的事實及情況後，本管理中心應與用戶及憑證問題報告(或其他憑證廢止通知)之回報者共同確認該憑證廢止請求是否成立。若憑證廢止請求經確認後成立，應於第 4.9.1 節規範之處理期限內完成憑證廢止作業。憑證廢止之處理期限應考量下述準則：

(1)聲稱問題的內容(包括範圍、過程、嚴重程度、重要性及危害的風險等)

(2)憑證廢止的後果(對用戶或信賴憑證者直接或間接的影響)

(3)該憑證或用戶的憑證問題報告數量

(4)提出憑證問題報告的單位

(5)相關的法律條文

### 4.9.6 信賴憑證者檢查憑證廢止之規定

信賴憑證者使用本管理中心所簽發之憑證前，應先檢驗本管理中心公布之憑證廢止清冊或線上憑證狀態協定回應訊息，以確定該憑證是否有效。信賴憑證者應檢核憑證廢止時間、憑證廢止清冊之或線上憑證狀態協定回應訊息之簽章有效性、憑證串鏈及其有效性等資訊。

本管理中心於儲存庫公開廢止之憑證資料，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://tls.hinet.net

### 4.9.7 憑證廢止清冊之簽發頻率

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中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。

### 4.9.8 憑證廢止清冊發布之最大延遲時間

本管理中心產製憑證廢止清冊後立即發佈，系統無預簽行為。

### 4.9.9 線上憑證廢止及狀態查驗之可用性

本管理中心以憑證廢止清冊、網頁式之憑證查詢與下載及線上憑證狀態協定回應訊息等方式提供憑證之廢止/狀態查詢。

本管理中心由線上憑證狀態協定回應伺服器(OCSP Responder)提供符合 RFC 6960 及 RFC 5019 標準規範的線上憑證狀態協定(OCSP)回應訊息，本管理中心簽章用私密金鑰使用 RSA-4096 或其以上 w/ SHA-256 雜湊函數演算法簽發線上憑證狀態協定回應伺服器之憑證以供信賴憑證者驗證 OCSP 回應訊息的數位簽章，確認資料來源之完整性。

### 4.9.10 線上憑證廢止查驗之規定

信賴憑證者應依照第 4.9.6 節之規定查詢憑證廢止清冊或依照第

4.9.9 節使用線上憑證狀態協定服務，檢驗所使用的憑證是否有效。

線上憑證狀態協定回應伺服器採 RSA-2048 併同 SHA-256 演算法簽發線上憑證狀態協定回應訊息。

本管理中心提供線上憑證狀態協定查詢服務，其可支援符合 RFC 6960 及 RFC 5019 標準規範所述之 HTTP-based 的 POST 與 GET 方法。

本管理中心之 OCSP 的更新頻率為每小時至少更新 1 次，OCSP 服務的回應訊息效期為 8 小時以上且 16 小時以下。

線上憑證狀態協定查詢封包內含之憑證序號可分為三種，分別為「已分配(Assigned)」、「已保留(Reserved)」及「未使用(Unused)」。「已分配」之憑證序號意即為本管理中心已簽發憑證之憑證序號，「已保留」之憑證序號為簽發 TLS/SSL 憑證所需之預簽憑證(Precertificate)的憑證序號，不符合前述條件之憑證序號皆屬於「未使用」之憑證序號。

若線上憑證狀態協定回應伺服器接收到查詢「已分配」之憑證序號的線上憑證狀態協定查詢封包時，應依該憑證序號所對應之憑證當時之狀態回覆。若線上憑證狀態協定回應伺服器接收到查詢「未使用」之憑證序號的線上憑證狀態協定查詢封包時，不可回覆其狀態為「正常(Good)」，並且本管理中心應監督線上憑證狀態協定回應伺服器對於這類請求的回覆是否符合上述安全回應程序。

### 4.9.11 廢止公告之其他發布形式

為了加速高流量網站的 EV TLS/SSL 憑證之驗證，以完成即時線上 EV TLS/SSL 憑證狀態之驗證作業，本管理中心根據 RFC 4366 支援線上憑證狀態協定裝訂(OCSP Stapling)，並透過用戶約定條款、支援憑證透明度機制及技術檢視與提供相關設定說明等方式請高流量網站之用戶落實線上憑證狀態協定裝訂之建置。

### 4.9.12 金鑰被破解時之特殊規定

如果用戶確認私密金鑰遭破解，用戶必須立即通知本管理中心依照本作業基準第 4.9.1、第 4.9.2 及第 4.9.3 節之相關規定廢止該憑證(註明該憑證廢止的原因為金鑰遭破解)，並簽發憑證廢止清冊以通知信賴憑證者該憑證不再受信任。

若本管理中心私密金鑰遭破解，將由總管理中心簽發憑證機構廢止

清冊，並通知應用軟體供應商、用戶及信賴憑證者。

第三方提交私密金鑰遭破解的證據可接受的方式為：

(1)由本管理中心提供隨機值或文件，由第三方以該私密金鑰對隨機值或文件數位簽章，經驗章而確認第三方握有遭破解之私密金鑰

(2)提交該私密金鑰

### 4.9.13 憑證停用之情況

不提供停用憑證服務。

### 4.9.14 憑證停用之申請者

不適用。

### 4.9.15 憑證停用之程序

不適用。

### 4.9.16 憑證停用期間之限制

不適用。

## 4.10 憑證狀態服務

### 4.10.1 操作特性

本管理中心提供憑證廢止清冊服務，且憑證廢止清冊服務的 HTTP URL 註記於用戶憑證的 cRLDistributionPoints 擴充欄位，本管理中心並提供線上憑證狀態協定查詢服務。

CRL 或 OCSP 所回應之某張憑證廢止紀錄的訊息，直到該被廢止憑證的效期已到，才會被移除。

### 4.10.2 服務可用性

本管理中心提供 7 天 x 24 小時不中斷之憑證狀態服務，使應用軟體隨時可針對未過期憑證進行檢查。

本管理中心提供 7 天 x 24 小時對於高優先權的憑證問題報告之內部回應機制，並適時地轉交給執法機關或進行憑證廢止。

### 4.10.3 可選功能

不做規定。

## 4.11 訂購終止

訂購終止(End of Subscription)是指憑證用戶終止使用本管理中心的服務。本管理中心允許用戶藉由廢止憑證、憑證到期而不做更新或是用戶約定條款失效而終止其對於憑證服務之訂購。

## 4.12 私密金鑰託管及回復

### 4.12.1 金鑰託管及回復之政策及實務

憑證機構及用戶的簽章用之私密金鑰不可被託管(Escrowed)。

### 4.12.2 會議金鑰封裝及回復之政策及實務

本管理中心並未支援會議金鑰(Session Key)封裝及回復。

# 5 憑證機構設施、管理及操作控管

## 5.1 實體控管

### 5.1.1 所在位置及結構

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 4 層門禁，第 1 層和第 2 層分別為全年無休的大門及大樓警衛，第 3 層為樓層讀卡機進出管制系統，第 4 層為機房人員指紋辨識器(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，須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，須填寫進出紀錄，並由本管理中心相關人員全程陪同。

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

(1) 確認設備是否正常運作。

(2) 確認機箱門是否關閉。

(3) 確認門禁系統是否正常運作。

### 5.1.3 電力及空調

本管理中心的電力系統，除了市電外，另設有發電機(滿載油料，可連續運轉 6 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

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第 5.1.1 節所述的場所，另將複製 1 份在安全場所。

### 5.1.7 廢料處理

第 9.3.1 節所述之本管理中心機密資訊，文件資料不需要使用時，都要經過碎紙機處理；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 30 公里以上，備援的內容包括資料與系統程式。

## 5.2 程序控管

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 8 個不同的 PKI 人員角色，分別為管理員、簽發員、稽核員、維運員、實體安全控管員、網路安全專員、防毒防駭專員和註冊審驗人員，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 1 個主管(Chief Role)來領導該群組的工作，而 8 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。
- 啟動/停止憑證廢止清冊簽發服務。

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。
- 網站的維護。
- 建置系統安全與病毒或惡意軟體等威脅之防護機制。

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)。

網路安全專員負責：

- 網路和網路設備的維護。
- 網路設備之弱點修補作業。
- 本管理中心之網路安全。
- 網路安全事件的偵測與通報。

防毒防駭專員負責：

- 研議、應用或提供防毒防駭、防惡意軟體等威脅之技術或措施，以確保系統和網路之安全。
- 將蒐集之電腦病毒之威脅或弱點通報管理員或網路安全專員進行修補。

註冊審驗人員負責：

- 受理憑證申請、廢止及更換金鑰之申請，包括註冊及身分識別與鑑別等作業。

如第 4.2.2 節與第 5.2.4 節所述，註冊中心之系統必須由至少兩名不同的信賴角色以雙因子鑑別登入系統處理憑證註冊審驗與憑證請求之放行。

### 5.2.2 每項任務所需之人數

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。
- 網路安全專員
  至少 1 位合格人員擔任。
- 防毒防駭專員
  至少 1 位合格人員擔任。

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 | 網路安全專員 | 防毒防駭專員 |
|---|---|---|---|---|---|---|---|
| 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 | | |
| 啟動/停止憑證廢止服務 | | 2 | | | 1 | | |
| 啟動/停止憑證廢止清冊簽發服務之操 | | 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 | 網路安全專員 | 防毒防駭專員 |
|---|---|---|---|---|---|---|---|
| 作程序。 | | | | | | | |
| 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 | | |
| 網站的維護 | | | | 1 | 1 | | |
| 網路和網路設備的日常運作維護 | | | | 1 | 1 | 1 | |
| 網路設備之弱點修補作業 | 1 | | | | 1 | 1 | |
| 電腦病毒威脅與弱點之通報事項 | | | | | | | 1 |
| 系統病毒碼與弱點之修補作業 | | | | 1 | 1 | | |

### 5.2.3 識別及鑑別每個角色

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。註冊審驗人員登入註冊中心系統及進行相關審驗動作，必須使用 IC 卡進行身分鑑別與數位簽章。

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。本管理中心利用使用者帳號、通行碼和群組之系統帳號管理功能或其他安全機制識別網路安全專員之角色。

### 5.2.4 需要職責分離之角色

本管理中心的信賴角色，其職責分離必須符合以下規定：

- 管理員、簽發員、稽核員和網路安全專員 4 種信賴角色不得相互兼任，但管理員、簽發員、稽核員可兼任維運員。
- 實體安全控管員不得兼任管理員、簽發員、稽核員和維運員。

無論在任何條件下，任何 1 個角色，都不可以執行自我稽核功能，不允許自己稽核自己。

## 5.3 人員控管

### 5.3.1 資格、經驗及清白規定

(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：

A. 個人性格之評估

B. 申請者經歷之評估。確認過往之工作經歷

C. 學術及專業能力及資格之評估。評估最高學歷或與工作職能相關之學歷、證照

D. 人員身分之確認

E. 人員操守之評估。依照 EV SSL Certificate Guidelines，檢查人員無犯罪紀錄

(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 背景調查程序

本管理中心對於第 5.2 節之各信賴角色人員及註冊中心之註冊審驗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 教育訓練規定

| 角色 | 教育訓練規定 |
|---|---|
| 管理員 | (1) 本管理中心安全原理和機制。<br>(2) 本管理中心安裝、設定和維護本管理中心系統操作程序。<br>(3) 建立和維護系統之用戶帳號操作程序。<br>(4) 設定稽核參數操作程序。<br>(5) 產製和備份本管理中心之金鑰操作程序。<br>(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。<br>(2) 本管理中心系統軟硬體的使用及操作程序。<br>(3) 啟動/停止憑證簽發之操作程序。<br>(4) 啟動/停止憑證廢止之操作程序。<br>(5) 啟動/停止憑證廢止清冊簽發服務之操作程序。 |

| 角色 | 教育訓練規定 |
|---|---|
| | (6) 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。<br>(2) 本管理中心系統軟硬體的使用及操作程序。<br>(3) 產製和備份本管理中心之金鑰操作程序。<br>(4) 對稽核紀錄的查驗、維護和歸檔程序。<br>(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。<br>(2) 系統的備援及復原作業程序。<br>(3) 儲存媒體的更新程序。<br>(4) 災後復原以及業務永續經營之程序。<br>(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。<br>(2) 災後復原以及業務永續經營之程序。 |
| 網路安全專員 | (1) 網路和網路設備的維護程序。<br>(2) 網路安全機制。 |
| 防毒防駭專員 | (1) 電腦病毒威脅與弱點及其防制。<br>(2) 作業系統與網路之安全機制。 |
| 註冊審驗人員 | (1) 公開金鑰基礎建設基本知識<br>(2) 身分鑑別和資料確認之政策與程序(包括 EV SSL Certificate Guidelines、Baseline Requirements、HiPKI 憑證政策及本作業基準)<br>(3) 憑證申請驗證過程常見之威脅，包含釣魚或其他社交工程手法<br>(4) 災後復原以及業務永續經營之程序。 |

憑證註冊審驗人員之訓練應舉行測驗並留下紀錄，以確保憑證註冊審驗人員維持足夠之知識與技能執行相關任務。

### 5.3.4 人員再教育訓練之頻率及規定

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 1 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 工作輪調之頻率及順序

(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。

(4)擔任網路安全專員滿 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)擔任防毒防駭專員滿 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 未授權行為之裁罰

本管理中心之相關人員，如違反 HiPKI 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 承攬商派駐人員之規定

承攬商派駐人員若擔任信賴角色，其職責、未授權行為之裁罰及應提供之教育訓練文件遵照第 5.3 節規定；操作行為之稽核與監控及相關紀錄保存遵照第 5.4.1 節規定。

### 5.3.8 提供之文件

本管理中心提供 HiPKI 憑證政策、本作業基準、EV SSL Cetificate Guidelines、Baseline Requirements、第 8 章所述之 3 種外稽標準、本管理中心系統操作手冊及中華民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。

## 5.4 稽核紀錄程序

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第 5.5.2 節所述之歸檔保留期間的維護方式進行。

### 5.4.1 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 1 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。

### 5.4.2 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 1 個月檢視稽核紀錄 1 次。

### 5.4.3 稽核紀錄檔保留期限

稽核資料現場保留兩個月，再移至適當場所儲存，並依照第 5.5.2 節稽核記錄保留期限之相關規定辦理。

憑證機構應確保稽核紀錄檔可於合格稽核業者執行外部稽核時取得。當稽核資料的保留期限到期時，如須移除該資料，必須由稽核員移除，不可由其他人員代理。

### 5.4.4 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。

### 5.4.5 稽核紀錄檔備份程序

電子式稽核紀錄至少每月備份 1 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。

### 5.4.6 稽核彙整系統

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。

### 5.4.7 對引起事件者之通知

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。

### 5.4.8 弱點評估

本管理中心遵照 WebTrust for CA－SSL BR 及 Network and Certificate System Security Requirements 規定之方式與頻率每季執行弱點評估至少 1 次，每年執行滲透測試至少 1 次。本管理中心於認定應用程式或基礎設施(Infrastructure)重大更新或變更後，也須執行滲透測試。本管理中心於滲透測試與弱點評估後進行補強與矯正措施。本管理中心針對足以執行可信賴的弱點掃瞄、滲透測試、資安健診或安全監控之人員或團體，記錄其技能、工具、熟練程度、遵循之道德倫理規範、競業關係以及獨立性。

## 5.5 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。

(3) 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。

### 5.5.1 歸檔紀錄之種類

本管理中心歸檔的紀錄有：

(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) 憑證廢止的資料

(8) 用戶身分識別資料

(9) 已簽發或公告的憑證

(10)本管理中心金鑰更換的紀錄

(11)已簽發或公告的憑證廢止清冊

(12)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

### 5.5.2 歸檔資料保留期限

本管理中心最少要保留歸檔資料的時間為 2 年。用來處理歸檔資料的應用程式也被維護 10 年。

### 5.5.3 歸檔資料之保護

(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。

### 5.5.4 歸檔資料備份程序

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。

### 5.5.5 記錄之時戳規定

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。

### 5.5.6 歸檔資料彙整系統

目前沒有歸檔資料彙整系統。

### 5.5.7 取得及驗證歸檔資料之程序

在取得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，書面文件必須驗證文件簽署者及日期等的真偽。

## 5.6 憑證機構之金鑰更換

本管理中心之私密金鑰依照第 6.3.2.1 節規定定期更換，最遲應於其私密金鑰簽發用戶憑證的使用期限到期前更換金鑰對。更換金鑰對後，以新金鑰對向 HiPKI RCA 申請新的憑證機構憑證，並公布於儲存庫，提供用戶或信賴憑證者下載。

本管理中心以新私密金鑰簽發用戶之憑證及憑證廢止清冊時，舊私密金鑰仍須簽發憑證廢止清冊或線上憑證狀態協定回應訊息，維持與保護至以舊私密金鑰簽發的所有用戶憑證到期為止。

如本管理中心本身的憑證被廢止後，其私密金鑰應停止使用，並需更換金鑰對。

## 5.7 遭破解及災變之復原

### 5.7.1 緊急事件及系統遭破解之處理程序

本管理中心訂定緊急事件與系統遭破解之通報與處理程序，同時每年進行演練、審視及更新。

### 5.7.2 電腦資源、軟體或資料遭破壞

本管理中心訂定電腦資源、軟體或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，使憑證狀態資訊能正常提供。

### 5.7.3 憑證機構私密金鑰遭破解之處理程序

如本管理中心簽章金鑰疑似遭破解，將依照事件記錄及通報程序，成立緊急應變小組搜集與事件有關的資訊；調查事件並確認金鑰遭破解的影響和範圍。若經緊急應變小組確認本管理中心簽章私密金鑰遭破解，則採取以下復原程序以迅速恢復憑證之簽發及管理作業能力：

(1) 召開「中華電信憑證政策管理委員會」請委員會同意更換金鑰，矯正問題並提出防止再次發生所應採取的行動。

(2) 聯繫政府主管機關與執法部門，並啟動其他適當的安全措施。

(3) 立即通知應用軟體供應商。

(4) 公告於儲存庫並通知用戶及信賴憑證者。

(5) 廢止本管理中心簽章金鑰憑證及所簽發之用戶憑證。

(6) 依照第 5.6 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，並將本管理中心新的憑證機構憑證登錄於 Mozilla 所管理的 Common CA Data Base (CCADB)。

本管理中心每年至少進行 1 次本管理中心簽章金鑰遭破解之演練。

### 5.7.4 災變後業務持續營運能力

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。

## 5.8 憑證機構或註冊中心之終止

本管理中心終止服務時，應依中華民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 30 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 30 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，退還憑證簽發費用。
- 主管機關於必要時，得公告廢止當時仍具效力之憑證。

註冊中心終止服務時，由本管理中心停止註冊中心審驗憑證之權利。

# 6 技術性安全控管

## 6.1 金鑰對之產製及安裝

### 6.1.1 金鑰對之產製

本管理中心使用第 6.2.1 節規定之安全密碼模組產製虛擬隨機亂數和公開金鑰對。

本管理中心依照第 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第 6.2.2 與第 6.2.6 節規定辦理。

本管理中心之金鑰產製由政策管理委員會之委員及合格稽核業者(Qualified Auditor)見證及錄影留存。

#### 6.1.1.1 用戶金鑰對之產製

由用戶自行安全地產製金鑰對並妥善保管其私密金鑰。

### 6.1.2 私密金鑰傳送給用戶

本管理中心不應代用戶產製金鑰對。私密金鑰應由用戶於其密碼模組內產製及儲存。

### 6.1.3 公開金鑰傳送給簽發憑證機構

用戶自行產製金鑰對，並以 PKCS# 10 憑證申請檔的格式將公開金鑰傳送給註冊中心，註冊中心依照第 3.2.1 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傳輸層安全協定或其他相同或更高級之資料加密傳送方式。

### 6.1.4 憑證機構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 HiPKI RCA 簽發，公布在 HiPKI RCA 與本管理中心的儲存庫上，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公鑰憑證前必須依照 HiPKI RCA 憑證實務作業基準規定，由安全管道取得 HiPKI RCA 之公開金鑰或自簽憑證，然後檢驗本管理中心公鑰憑證的簽章，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 4096 位元或其以上的 RSA 金鑰及 SHA-256 雜湊函數演算法簽發憑證。

到民國 119 年 12 月 31 日以前，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。

民國 120 年 1 月 1 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。

若本管理中心使用橢圓曲線密碼演算法(Elliptic Curve Cryptography, ECC)簽發憑證將使用符合 NIST P-256 或 P-384 的金鑰長度。

對於 ECDSA 金鑰，本管理中心應使用以下曲線-雜湊對其中之一：P-256 with SHA-256，P-384 with SHA-384。

### 6.1.6 公開金鑰參數之產製及品質檢驗

RSA 演算法公鑰參數為空的(Null)。

本管理中心簽章用金鑰對採用 NIST FIPS 186-4 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。

根據 NIST SP 800-89 第 5.3.3 節，本管理中心確認公開指數(public exponent)的值為大於 3 的奇數，且其值介於 $2^{16}+1$ 和 $2^{256}-1$ 之間。此外，模數應具有奇數、非質數的指數次方且沒有小於 752 的因數的性質。

若使用橢圓曲線密碼演算法簽發之憑證，本管理中心將遵循 NIST SP 800-56A Revision 2 第 5.6.2.3.2 節與第 5.6.2.3.3 節，確認所有使用 ECC Full Public Key Validation Routine 與 ECC Partial Public Key Validation Routine 的金鑰之效期。

### 6.1.7 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及憑證廢止清冊。本管理中心本身之公鑰憑證由 HiPKI RCA 簽發；其中金鑰用途(keyUsage)擴充欄位設定使用的 keyUsage 位元為 keyCertSign 及 cRLSign。若本管理中心欲使用其簽章用私密金鑰簽發線上憑證狀態協定回應訊息時，則金鑰用途位元尚須包含 digitalSignature。

EV TLS/SSL 憑證之 keyUsage 擴充欄位包含 digitalSignature，且可視需求包含 keyEncipherment。擴充金鑰用途(extKeyUsage)擴充欄位包含 serverAuth 與 clientAuth。

## 6.2 私密金鑰保護及密碼模組工程控管

### 6.2.1 密碼模組標準及控管

本管理中心使用通過 FIPS 140-2 Level 3 認證之硬體密碼模組。

### 6.2.2 私密金鑰分持之多人控管

本管理中心金鑰分持之多人控管，採 LaGrange 多項式內插法(LaGrange Polynomial Interpolation)的 n-out-of-m(簡稱 n-out-of-m)，他是一種完全秘密分享(Perfect Secret Sharing)的方式，可做為私密金鑰分持備份及回復方法；其中，n 與 m 皆須為大於或等於 2 的數值，且 n 必須小於或等於 m。採用此方法可使本管理中心私密金鑰的多人控管具有最高的安全度，因此也用來做為私密金鑰之啟動方式(參閱第 6.2.8 節)。

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 私密金鑰備份

依照第 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 私密金鑰歸檔

本管理中心簽章用私密金鑰不被歸檔，但會以憑證資料的方式依照第 5.5 節執行相對公開金鑰的歸檔。

### 6.2.6 私密金鑰匯入、匯出密碼模組

本管理中心在下述情況時會將私密金鑰匯入至密碼模組中：

(1) 金鑰產製。

(2) 金鑰持份備援的回復時。在此情況是以秘密持份(n-out-of-m 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，私密金鑰匯入方式採加密方式以確保匯入過程中不得將金鑰明碼暴露於密碼模組之外，私密金鑰匯入完成後，須將匯入過程產製之相關機密參數完全銷毀。

### 6.2.7 私密金鑰儲存於密碼模組

依照第 6.1.1 節及第 6.2.1 節規定。

### 6.2.8 啟動私密金鑰之方式

本管理中心之私密金鑰之啟動是由多人控管 IC 卡來控制，不同用途的控管 IC 卡由管理員、簽發員所保管。

用戶應慎選安全的電腦環境及可信賴的應用系統，妥善保管及使用其私密金鑰。用戶之私密金鑰啟動方式依照私密金鑰儲存媒體分類如下：

(1) 若為硬體密碼模組，則私密金鑰之啟動方式，是由多人控管 IC 卡來控制，不同用途的控管 IC 卡由不同的人員所保管。

(2) 其他私密金鑰載具，用戶應使用強效通行碼或相同等級的鑑別方式啟動私密金鑰以防止未經授權的存取或使用私密金鑰。

### 6.2.9 停用私密金鑰之方式

本管理中心之私密金鑰採第 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。

### 6.2.10 銷毀私密金鑰之方式

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 HiPKI RCA 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(參照第 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 1 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)，則儲存在這個密碼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 1 個金鑰儲存密碼模組已經將被永久的不再提供服務，則儲存在這個密碼模組中已經有使用過的所有私密金鑰，都將要被自此密碼模組中刪除(erased)。

用戶之私密金鑰銷毀方式，不另做規定。

### 6.2.11 密碼模組評等

參見第 6.2.1 節。

## 6.3 金鑰對管理之其他規範

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 公開金鑰歸檔

本管理中心將進行用戶憑證之歸檔，且依照第 5.5 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 憑證操作及金鑰對之效期

#### 6.3.2.1 本管理中心憑證操作及金鑰對之效期

本管理中心憑證操作及金鑰對之效期為：

| 憑證類別 | 私密金鑰效期 | 憑證效期 |
|---|---|---|
| 本管理中心之憑證機構憑證 | ■ 簽發用戶憑證：10年<br>■ 簽發憑證廢止清冊或線上憑證狀態協定回應伺服器憑證：20年 | 20年 |
| 線上憑證狀態協定回應伺服器憑證 | ■ 簽發線上憑證狀態協定回應訊息：36小時 | 36小時 |

本管理中心每天會公布新的線上憑證狀態協定回應伺服器憑證(透過新的私密金鑰簽署過的線上憑證狀態協定回應訊息包含該憑證給信賴憑證者)。

#### 6.3.2.2 用戶憑證操作及金鑰對之效期

本管理中心用戶之公開金鑰及私密金鑰之金鑰長度為 RSA-2048 位元或其以上，或為 ECC-256 位元或其以上。用戶憑證操作及金鑰對之效期為：

| 憑證類別 | 金鑰效期 | 憑證效期 |
|---|---|---|
| EV TLS/SSL憑證 | ■ 參照第6.1.7節：不做規定 | 398天 |

## 6.4 啟動資料

### 6.4.1 啟動資料之產生及安裝

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

### 6.4.2 啟動資料之保護

啟動資料由 n-out-of-m 控管 IC 卡保護，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 啟動資料之其他規範

本管理中心的私密金鑰的啟動資料不做歸檔。

## 6.5 電腦安全控管

### 6.5.1 特定電腦安全技術規定

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) 具備身分鑑別之登入

(2) 依所擔任之角色定義存取權限

(3) 提供安全稽核能力

(4) 具備程序完整性及安全控管保護

本管理中心設備建構在經過安全評估的作業平臺上，且硬體、軟體、作業系統在經過安全評估的組態下運作，對能夠導致簽發憑證之帳號實施多因子認證。

### 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

本管理中心的系統研發遵循能力成熟度模型整合(Capability Maturity Model Integration, 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。並定期使用工具包括防毒軟體、惡意軟體移除工具掃瞄。

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、管理手冊、與原始程式碼掃瞄報告給本管理中心，並進行程式版本控管。

### 6.6.2 安全管理控管

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、Baseline Requirements、EV SSL Certificate Guidelines、Network and Certificate System Security Requirements、WebTrust for CA、WebTrust for CA－EV SSL 及 WebTrust for CA－SSL BR 之方法論或規定。

### 6.6.3 生命週期安全控管

每年至少 1 次評估現行金鑰是否有被破解之風險。

## 6.7 網路安全控管

本管理中心遵循 CA/Browser Forum 的 Network and Certificate System Security Requirements 實施網路安全控管措施。

本管理中心之主機和儲存庫透過防火牆和外部網路連接，儲存庫置於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儲存庫。

本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、入侵防禦系統/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。

本管理中心監督存取控制權限，持續監督系統健康與安全事件並安排滲透測試。

## 6.8 時戳

本管理中心定期根據受信賴的時間源進行系統校時，以維持系統時間的正確性，並確保以下時間之正確性：

(1) 用戶憑證簽發時間。

(2) 用戶憑證廢止時間。

(3) 憑證廢止清冊之簽發時間。

(4) 系統事件之發生時間。

可能會使用自動與手動程序來進行系統時間調整，系統校時動作須可被稽核。

# 7 憑證、憑證廢止清冊及線上憑證狀態協定之格式剖繪

## 7.1 憑證之格式剖繪

本管理中心所簽發的憑證遵循 ITU-T X.509、EV SSL Certificate Guidelines 及 RFC 5280 正式版之規定。

本管理中心透過密碼學安全偽亂數生成器(Cryptographically secure pseudorandom number generator, CSPRNG)，產生大於零、非循序、且至少包含 64 位元的亂度之憑證序號。

### 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遵循 ITU-T X.509、EV SSL Certificate Guidelines 及 RFC 5280 正式版之規定。

#### 7.1.2.1 本管理中心之憑證機構憑證

HiPKI RCA 簽發給本管理中心之下屬憑證機構憑證(Subordinate CA Certificate)的擴充欄位說明如下：

a.憑證政策(certificatePolicies)

此擴充欄位為必要欄位，其標示為非關鍵性(non-critical)欄位，其內容用於註記憑證政策識別碼(policyIdentifier)。可視憑證需求使用憑證政策限定元(policyQualifier)，用於標示 HiPKI RCA 憑證實務作業基準公告之網址。

b.憑證廢止清冊發布點(cRLDistributionPoints)

此擴充欄位為必要欄位，其標示為非關鍵性(non-critical)欄位，其內容用於註記 HiPKI RCA 之憑證廢止清冊服務的 HTTP URL。

c.憑證機構資訊存取(authorityInfoAccess)

此擴充欄位為必要欄位，其標示為非關鍵性(non-critical)欄位。其內容用於註記 HiPKI RCA OCSP 回應伺服器的 HTTP URL，其內容也用於註記 HiPKI RCA 之自簽憑證的 HTTP URL。

d.基本限制(basicConstraints)

此擴充欄位為必要欄位，其標示為關鍵性(critical)欄位。其內容用於註記 cA 欄位值為 true。因本管理中心不再往下簽署下層憑證機構憑證，故 pathLenConstraint 欄位設定為 0。

e.金鑰用途(keyUsage)

此擴充欄位為必要欄位，其標示為關鍵性(critical)欄位，其內容用於註記 keyUsage 位元為 keyCertSign 和 cRLSign。因並非由本管理中心簽章用私密金鑰簽 OCSP 回應訊息，而是經由本管理中心簽發 OCSP 回應伺服器憑證後，由 OCSP 回應伺服器簽發 OCSP 回應訊息，所以設定未使用 digitalSignature。

f.命名限制(nameConstraints)

HiPKI RCA 簽發給本管理中心之下屬憑證機構憑證無此選擇性欄位。

g.擴充金鑰用途(extKeyUsage)

對於 HiPKI RCA 簽發給本管理中心之下屬憑證機構憑證，此擴充欄位為必要欄位，其標示為非關鍵性(non-critical)欄位，包含 serverAuth 及 clientAuth；此外，不得設定 emailProtection、codeSigning、timeStamping、與 anyExtendedKeyUsage。

h.憑證機構金鑰識別碼(authorityKeyIdentifier)

此擴充欄位為必要欄位，其標示為非關鍵性(non-critical)欄位。其必須包含一個金鑰識別碼欄位，且其不得包含一個 authorityCertIssuer 或 authorityCertSerialNumber 欄位。

#### 7.1.2.2 用戶憑證

a.憑證政策(certificatePolicies)

此擴充欄位為必要欄位，其標示為非關鍵性(non-critical)欄位，其內容用於註記憑證政策識別碼(policyIdentifier)。可視憑證需求使用憑證政策限定元(policyQualifier)，用於標示本作業基準公告之網址。

b.憑證廢止清冊發布點(cRLDistributionPoints)

此擴充欄位為必要欄位，其標示為非關鍵性(non-critical)欄位，其內容用於註記本管理中心之憑證廢止清冊服務的 HTTP URL。

c.憑證機構資訊存取(authorityInfoAccess)

此擴充欄位為必要欄位，其標示為非關鍵性(non-critical)欄位。其內容用於註記本管理中心 OCSP 回應伺服器的 HTTP URL，其內容也用於註記本管理中心之憑證的 HTTP URL。

d.基本限制(basicConstraints)

此擴充欄位為選擇性欄位，若有的話，其標示為非關鍵性(non-critical)欄位。其內容用於註記 cA 欄位值為 false。因用戶憑證不會往下簽署下層憑證機構憑證，故 pathLenConstraint 欄位設定為 0。

e.金鑰用途(keyUsage)

此擴充欄位為選擇性欄位，若有的話，其標示為關鍵性(critical)欄位，其內容不能註記使用的 keyUsage 位元為 keyCertSign 和 cRLSign。EV TLS/SSL 憑證之 keyUsage 參見第 6.1.7 節。

f.擴充金鑰用途(extKeyUsage)

本管理中心核發之 EV TLS/SSL 憑證，此擴充欄位為必要欄位，其標示為非關鍵性(non-critical)欄位，其內容用於註記 serverAuth 與 clientAuth。此外，不得設定 anyExtendedKeyUsage。

g.憑證機構金鑰識別碼(authorityKeyIdentifier)

此擴充欄位為必要欄位，其標示為非關鍵性(non-critical)欄位。其必須包含一個金鑰識別碼欄位，且其不得包含一個 authorityCertIssuer 或 authorityCertSerialNumber 欄位。

除非知道包含某些資料於憑證的理由，本管理中心不允許簽發下述兩種情境之憑證：

(1)憑證的擴充欄位內含無法應用於公眾網路(Public Internet)的設定，例如：extKeyUsage 擴充欄位包含僅適用於私有網路服務的設定值。

(2)憑證內容包含可能誤導信賴憑證者相信該憑證資訊已經由本管理中心驗證。

針對 EV TLS/SSL 憑證，關於憑證透明度(Certificate Transparency,

CT)之支援，本管理中心採用當前最為普遍使用的 X.509 v3 Extension 機制進行 SCTs 傳輸。因此會先透過提交預簽 precertificate 之憑證串列向複數個憑證透明度日誌分別取得 SCT 後，再將 SCT 串列嵌入目標憑證後才簽發給與用戶。根據目前最新版 Google 與 Apple 之 CT 政策，採用 X.509v3 Extension 機制可以達到以下好處：SSL 憑證客戶可以用過去申請憑證方式取得符合 CT 規範的 SSL 憑證；無存在額外限制如 RFC 6962 所列的 OCSP 裝訂(OCSP Stapling)SCT 傳輸機制(須啟用客戶端網頁伺服器 OCSP Stapling 組態設定，且至今仍有少數網頁伺服器不支援 OCSP Stapling)；本管理中心僅須確保目標憑證簽發當下所介接的憑證透明度日誌狀態正常，因此可不受日後憑證透明度日誌狀態變更所影響。

### 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：

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

(OID：1.2.840.113549.1.1.11)

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

(OID：1.2.840.113549.1.1.12)

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

(OID：1.2.840.113549.1.1.13)

| | |
|---|---|
| ecdsaWithSHA256 | {iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA256(2)} |

(OID：1.2.840.10045.4.3.2)

| | |
|---|---|
| ecdsaWithSHA384 | {iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA384(3)} |

(OID：1.2.840.10045.4.3.3)

| | |
|---|---|
| ecdsaWithSHA512 | {iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA512(4)} |

(OID：1.2.840.10045.4.3.4)

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) rsaEncryption(1)} |

(OID: 1.2.840.113549.1.1.1)

| | |
|---|---|
| ecPublicKey | {iso(1) member-body(2) us(840) ansi-x962(10045) keyType(2) ecPublicKey(1)} |

(OID: 1.2.840.10045.2.1)

對於 ECC 演算法，須同時註記下述橢圓曲線參數之物件識別碼：

| | |
|---|---|
| secp256r1 | {iso(1) member-body(2) us(840) ansi-x962(10045) curves(3) prime(1) prime256v1(7)} |

(OID: 1.2.840.10045.3.1.7)

| | |
|---|---|
| secp384r1 | {iso(1) identified-organization(3) certicom(132) curve(0) ansip384r1(34)} |

(OID: 1.3.132.0.34)

### 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、EV SSL Certificate Guidelines 及 RFC 5280 正式版之規定。

本管理中心的憑證機構憑證之主體資訊必須包含 countryName (OID 2.5.4.6)欄位，其值為本管理中心所在地之雙字母 ISO 3166-1 國家代碼。除此之外，必須包含 organizationName (OID 2.5.4.10)欄位，其值必須包含可識別本管理中心之名稱、商標或其他有意義的識別名稱，以供能更準確地識別本管理中心，而不能僅包含通用名稱，例如：CA 1。本管理中心的憑證機構憑證其 X.500 唯一識別名稱參見第 3.1.5 節。

#### 7.1.4.1 簽發者資訊

依據 RFC 5280 名稱串鍊(Name chaining)的規定，憑證簽發者之唯一識別名稱欄位(Issuer DN)的內容，必須與簽發該憑證之憑證管理中心的主體唯一識別名稱(Subject DN)相同。故本管理中心簽發的用戶憑證，其簽發者唯一識別名稱欄位內容必須與本管理中心主體的唯一識別名稱欄位內容相同。

#### 7.1.4.2 用戶憑證之主體資訊

藉由簽發用戶憑證，表示本管理中心與註冊中心在憑證的簽發日期前已遵循憑證政策和/或憑證實務作業基準所闡述的程序來作驗證，確保所有記載於 EV TLS/SSL 憑證之主體資訊的值是準確的。憑證主體的 commonName 欄位若出現，其值必須為 subjectAltNames(即依照第 3.2.5 節其中一個方法所驗證過的完全吻合網域名稱)的其中之一。此外，憑證主體屬性不得僅包含如「.」、「-」、及「 」(即空格)等詮釋字元，及/或任何其他標示來代表該值不存在、不完整、或不適用。

##### 7.1.4.2.1 主體別名擴充欄位

EV TLS/SSL 憑證之主體別名擴充欄位如下：

| 憑證欄位 | 必要/選擇性擴充欄位 |
|---|---|
| extension:subjectAltName | 必要 |

下底線字符(“_”)不得出現於 dNSName。

此擴充欄位應由註冊審驗人員依照第 3.2.5 節進行網域名稱擁有權或控制權之驗證。

##### 7.1.4.2.2 主體唯一識別名稱欄位

請參考本作業基準表 3-1。

##### 7.1.4.2.3 cabfOrganizationIdentifier 擴充欄位

EV TLS/SSL 憑證之 cabfOrganizationIdentifier 擴充欄位如下：

| 憑證欄位 | 必要/選擇性擴充欄位 |
|---|---|
| extension:<br>cabfOrganizationIdentifier | 選擇性 |

若 subject:organizationIdentifier 存在，此擴充欄位必須存在。

#### 7.1.4.3 憑證機構憑證之主體資訊

本管理中心之憑證機構憑證是由上層的 HiPKI RCA 依循憑證政策和/或其憑證實務作業基準所闡述的程序來作驗證後簽發。其主體唯一識別名稱欄位(Subject Distinguished Name Field)如下表：

| 憑證欄位 | 必要/選擇性擴充欄位 |
|---|---|
| subject:commonName (OID 2.5.4.3) | 必要 |
| subject:organizationName (OID 2.5.4.10) | 必要 |
| subject:countryName(OID 2.5.4.6) | 必要 |

### 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使用 CA/Browser Forum 之 EV SSL 憑證政策物件識別碼({joint-iso-itu-t(2) international-organizations(23) ca - browser - forum(140) certificate - policies(1) ev-guidelines (1) }(2.23.140.1.1))。

### 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限制擴充欄位。

### 7.1.8 政策限定元之語法及語意

本管理中心簽發的憑證其政策限定元識別代碼(policyQualifierId)須為國際標準 RFC 5280 所規範之「id-qt 1」，亦即為標示憑證實務作業基準之用的政策限定元識別代碼，物件識別碼為 1.3.6.1.5.5.7.2.1。

### 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 版本 2 的憑證廢止清冊。

### 7.2.2 憑證廢止清冊及憑證廢止清冊條目之擴充欄位

本管理中心簽發的憑證廢止清冊，其憑證廢止清冊擴充欄位(crlExtensions)及憑證廢止清冊條目擴充欄位(crlEntryExtensions)會遵照 ITU-T X.509、EV SSL Certificate Guidelines 及 RFC 5280 正式版之規定。憑證廢止清冊欄位如下表：

| 欄位 | 內容 | 說明 |
|---|---|---|
| version | V2(1) | CRL 的版本為 V2(注意 V2 的值是1 而不是2) |
| signature | | 簽 CRL 之簽章演算法之 AlgorithmIdentifier，此欄的值必須與外層 SIGNED憑證之algorithmIdentifier欄的值相同 |
| .algorithm | sha256WithRSAEncryption(1 2 840 113549 1 1 11) 或 ecdsaWithsha384(1 2 840 10045 4 3 3) | 簽章演算法之OID |
| .parameter | NULL | 簽章演算法雖然不需要 parameters，但其parameters必須填上NULL，不可省略，NULL 之 DER 編碼為 |

| 欄位 | 內容 | 說明 |
|---|---|---|
| | | 0x0500 |
| issuer | CA的DN | 此DN必須要與簽發該CRL之憑證管理中心的主體唯一識別名稱(Subject DN)相同(註：在本管理中心中keyCertSign Certificate與cRLSign Certificate是同1張) |
| thisUpdate | 本次CRL更新的格林威治<br>時間(GMT) | 依PKIX規定在2049/12/31 23:59:59之前使用UTCTime資料型態，格式為YYMMDDHHMMSSZ，其中即使秒數SS為00也不可省略，而最後的Z表示GMT時間也不可省略。 |
| nextUpdate | 預計下次CRL更新的格林威治時間(GMT) | 依PKIX規定在2049/12/31 23:59:59之前使用UTCTime資料型態，格式為YYMMDDHHMMSSZ，其中即使秒數SS為00也不可省略，而最後的Z表示GMT時間也不可省略。 |
| revokedCertificates | RevokedCertificates ::= SEQUENCE OF RevokedCertificate<br><br>填入一連串的RevokedCertificate紀錄 | 在thisUpdate之前的發生的所有有效(Effective)的憑證廢止(Revocation)事件都會記錄在revokedCertificates中(註:所謂有效是指該憑證尚未過期) |
| *.RevokedCertificate | 每1個RevokedCertificate紀錄的內容如下： | *代表多個RevokedCertificate紀錄 |
| .userCertificate | 填入被廢止憑證之憑 | 本管理中心中所使用之憑 |

| 欄位 | 內容 | 說明 |
|---|---|---|
| | 證序號(Certificate Serial Number) | 證序號是1個長度為16位元組的正整數，根據DER編碼對正數所使用的2's Complement規則，可能會在前面補上0x00，而使得16位元組的正整數實際上佔用17位元組的空間 |
| .revocationDate | 憑證被廢止的格林威治時間(GMT) | 依PKIX規定在2049/12/31 23:59:59之前使用UTCTime資料型態，格式為YYMMDDHHMMSSZ，其中即使秒數SS為00也不可省略，而最後的Z表示GMT時間也不可省略。 |
| Issuer's Signature | CA對CRL的簽章值 | |

憑證廢止清冊條目擴充欄位與憑證廢止清冊擴充欄位如下表：

| 欄位 | 內容 | 說明 |
|---|---|---|
| .crlEntryExtensions | SEQUENCE OF CRLEntryExtension (註：CRLEntryExtension資料型態的格式與Public-Key Certificate的Extension 資料型態的格式完全相同) | 可填入一連串CRLEntryExtension，但本管理中心只使用reasonCode這個CRLEntryExtension |
| .reasonCode | HiPKI只使用reasonCode這個CRLEntryExtension，其內容如下： | |
| .extnId | 填入代表此擴充欄位的OID id-ce- | |

| 欄位 | 內容 | 說明 |
|---|---|---|
| | cRLReasons (2.5.29.21) | |
| .critical | reasonCode必定是non-critical extension，所以critical 的值必定是FALSE | 注意由於FALSE是DEFAULT VALUE，所以DER編碼中，此欄位會被省略掉 |
| .extnValue | extnValue的資料型態是OCTET STRING，對於reasonCode這種Extension而言，必須使用以下CRLReason的DER編碼之一做為此OCTET STRING的值，CRLReason 本身為1個ENUMERATED | 在本管理中心中規定有些CRLReason不得使用於Complete CRL中。 |
| | Unused(0) | 遵照PKIX的規定，在本管理中心中不得使用此CRLReason |
| | keyCompromise(1) | 當終端個體(End Entities, EE)的私密金鑰遺失或懷疑被竊取或破解，而欲廢止憑證，則使用此CRLReason |
| | caCompromise(2) | 當懷疑或確定CA keyCertSign或cRLSign私密金鑰遭竊或被破解時使用此CRLReason，但此CRLReason不得使用於廢止EE Certificate，只能用於廢止CA Certificate(註：當懷疑或確定CA keyCertSign 私密金鑰遭竊或被破解而必須廢止已經 |

| 欄位 | 內容 | 說明 |
| --- | --- | --- |
| | | 簽發的所有EE憑證，重新產製CA金鑰對，並重新簽發所有EE憑證時，則EE憑證廢止的 CRLReason 應該使用 superseded) |
| | affiliationChanged(3) | 當EE與憑證內容相關之身分資料改變(例如更改公司名稱、地址)時必須廢止憑證，則使用此CRLReason |
| | superseded(4) | 當EE因某種需要(例如更換新憑證、CA Hand-Over而重發所有憑證、CA為了更新憑證格式而重發所有憑證、或因密碼破解方法的突破而必須改用更安全的金鑰種類或長度)而更新憑證，必須廢止原來之憑證時，使用此CRLReason |
| | cessationOfOperation(5) | 當EE憑證並沒有任何特殊理由，而純粹不想再繼續使用或不得不作廢時，使用此CRLReason |
| | certificateHold(6) | SSL 憑證不得使用此CRLReason |
| | removeFromCRL(8) | SSL 憑證不得使用此CRLReason |
| | privilegeWithdrawn(9) (註：X.509 4th Edition) | 1. EE的privilege被取消(例如遭撤銷登記或褫奪公權)時，使用此CRLReason<br>2. 此CRLReason通常不是由EE主動發起，而通常是在CA/RA 或屬性憑證機構 |

| 欄位 | 內容 | 說明 |
| --- | --- | --- |
| | | (Attribute Authority, AA)「逕行廢止」EE憑證時才會使用<br>3.此CRLReason 通常用於廢止屬性憑證(Attribute ertificate)，但也可能用於廢止公開金鑰憑證(Public-Key certificate) |
| | aACompromise(10)<br>(註：X.509 4th Edition) | 當懷疑AA簽發屬性憑證(Attribute Certificate)用之私密金鑰遭竊或被破解時使用此CRLReason，但此CRLReason不得使用於廢止公鑰憑證，只能用於廢止AA本身之公鑰憑證與EE之屬性憑證 |
| crlExtensions | SEQUENCE OF CRLExtension (註：CRLExtension 資料型態的格式與公開金鑰憑證的Extension資料型態的格式完全相同) | 內容為一串擴充欄位，包含以下的擴充欄位種類(實際在憑證中的順序可能不是照以下的順序)： |
| .authorityKeyIdentifier | Authority Key Identifier 擴充欄位，Key Identifier的產生方式依照PKIX標準，取簽發憑證機構的公開金鑰的SHA-1雜湊函數值做為Key Identifier | 此擴充欄位的目的是標示CA用來簽發本CRL所使用的金鑰是哪一把，以便在CA更換金鑰及其本身憑證時判斷應該使用CA的哪一張CA憑證來檢驗此憑證 |
| .extnId | 填入代表此擴充欄位的OID | |

| 欄位 | 內容 | 說明 |
|---|---|---|
| | id-ce-authorityKeyIdentifier (2.5.29.35) | |
| .critical | 在HiPKI中，authorityKeyIdentifier必定是non-critical extension，所以critical 的值必定是FALSE | 注意由於FALSE是DEFAULTVALUE，所以DER編碼中，此欄位會被省略掉 |
| .extnValue | extnValue的資料型態是OCTET STRING | 對於authorityKeyIdentifier這種Extension而言，必須使用AuthorityKeyIdentifier的DER編碼做為此OCTET STRING的值 |
| .authorityKeyIdentifier | authorityKeyIdentifier的資料結構含有3個Optional的欄位，分別是keyIdentifier、authorityCertIssuer與authorityCertSerialNumber欄位 | 在本管理中心中，CRL依據PKIX，只採用keyIdentifier欄位，而不使用authorityCertIssuer與authorityCertSerialNumber欄位 |
| .keyIdentifier | keyIdentifier欄為的資料型態是KeyIdentifier，而KeyIDentifier本身為1個OCTET STRING資料型態 | KeyIdentifier的產生方式依照PKIX標準，取Subject的公開金鑰的SHA-1雜湊函數值做為KeyIdentifier的OCTET STRING值 |
| .cRLNumber | cRLNumber CRLExtension的內容如下： | cRLNumber擴充欄位的內容是用來記錄此CRL的序號 |
| .extnId | 填入代表此擴充欄位的OID id-ce- | |

| 欄位 | 內容 | 說明 |
|---|---|---|
| | cRLNumber (2.5.29.20) | |
| .critical | cRLNumber必定是non-critical extension，所以critical 的值必定是FALSE | 注意由於FALSE是DEFAULT VALUE，所以DER編碼中，此欄位會被省略掉 |
| .extnValue | extnValue的資料型態是OCTET STRING，對於cRLNumber這種Extension而言，必須使用CRLNumber的DER 編碼做為此OCTET STRING的值，而CRLNumber本身為1個INEGER (0..MAX)正整數資料型態 | 根據X.509標準，CRL Number必須是1個單調遞增序號(monotonically increasing sequence number)。在HiPKI中，憑證廢止清冊的CRLNumber值應為1個長度小於或等於7個位元組的正整數。 |
| .issuingDistributionPoint | issuingDistributionPoint CRLExtension，其內容如下： | issuingDistributionPoint擴充欄位是用來提供憑證應用軟體比對此CRL是否與要驗證的憑證的CRL位址相符合，目前Partitioned CRL所使用之Issuing Distribution Point為1個URL網址，即是此CRL的發布點位址 |
| .extnId | 填入代表此擴充欄位的OID id-ce-issuingDistributionPoint (2.5.29.28) | |
| .critical | 在Partitioned CRL中，issuingDistributionPoi | 注意由於TRUE不是DEFAULT VALUE，所以DER編碼中，此欄位不可被 |

| 欄位 | 內容 | 說明 |
|---|---|---|
| | nt必定是critical extension，所以 critical 的值必定是 TRUE | 省略掉 |
| .extnValue | extnValue的資料型態是OCTET STRING | 對於 issuingDistributionPoint 這種Extension而言，必須使用 IssuingDistributionPoint 資料型態的DER編碼做為此OCTET STRING的值。 |
| .IssuingDistributionPoint | IssuingDistributionPoint 為一 SEQUENCE，內含 distributionPoint、 onlyContainsUserCerts、 onlyContainsCACerts、onlySomeReasons與indirectCRL 5 欄 | 在 Partitioned CRL 中，issuingDistributionPoint 擴充欄位只使用 distributionPoint 欄位，而不使用其他4種欄位。 |
| .distributionPoint | distributionPoint 欄位的資料型態是 DistributionPointName，而 DistributionPointName本身為1個CHOICE資料型態，可選用 fullName或 nameRelativeToCRLIssuer | 在本管理中心中，Partitioned CRL 的 distributionPoint 是採用fullName。 |
| .fullName | fullName的資料型態是GeneralNames 而 GeneralNames 的資料型態是 SEQUENCE SIZE | 在本管理中心中，Partitioned CRL的distributionPoint 欄位之 fullName 只會包含 1 個 GeneralName。 |

| 欄位 | 內容 | 說明 |
|---|---|---|
| | (1..MAX) OF GeneralName | |
| .GeneralName | GeneralName是1個CHOICE資料型態 | 本管理中心選用CHOICE中的uniformResourceIdentifier，並在此欄中記載本CRL的發布點URL。若使用此Partitioned CRL驗證憑證有效性時，則被驗憑證cRLDistributionPoints欄位所記載的各個URL必須至少有1個與此欄所記載的URL完全相同。 |

## 7.3 線上憑證狀態協定之格式剖繪

本管理中心提供符合 RFC 6960 及 RFC 5019 標準規範之線上憑證狀態協定(OCSP)查詢服務，並在憑證的憑證機構資訊存取(authorityInfoAccess)擴充欄位中包含本管理中心 OCSP 的服務網址。

### 7.3.1 版本序號

本管理中心接受的線上憑證狀態協定查詢封包包含以下資訊：

- 版本序號
- 待查詢憑證識別碼(Target certificate identifier)

待查詢憑證識別碼包含：雜湊演算法、憑證簽發者名稱之雜湊值、憑證簽發者公開金鑰之雜湊值及待查詢憑證之憑證序號。

OCSP 回應伺服器簽發的線上憑證狀態協定回應封包含有以下基本欄位：

| **欄位** | **說明** |
|---|---|
| 狀態 | 回應狀態，包括成功、請求格式錯誤、內部錯誤、稍候重試、請求沒有簽章或請求憑證無授 |

| 欄位 | 說明 |
|---|---|
| | 權，當狀態為成功時必須包括以下各項。 |
| 版本序號(Version) | v.1(0x0) |
| OCSP 回應伺服器 ID (Responder ID) | OCSP 回應伺服器的主體名稱(Subject DN) |
| 產製時間(Produced Time) | 回應封包簽署時間 |
| 待查詢憑證識別碼 (Target certificate identifier) | 包含：雜湊演算法、憑證簽發者(CA)名稱(Issuer Name) 之雜湊值、憑證簽發者公開金鑰(Issuer Key) 之雜湊值及待查詢憑證之憑證序號 |
| 憑證狀態碼(Certificate Status) | 憑證狀態對應碼(0：有效/1：廢止/2：未知) |
| 效期 (ThisUpdate/NextUpdate) | 此回應封包建議的效期區間，包含：生效時間(ThisUpdate)及下次更新時間(NextUpdate) |
| 簽章演算法(Signature Algorithm) | 回應封包的簽章演算法，可為 sha256WithRSAEncryption 或 ecdsaWithsha384 |
| 簽章(Signature) | OCSP 回應伺服器的簽章 |
| 憑證(Certificates) | OCSP 回應伺服器的憑證 |

### 7.3.2 線上憑證狀態協定擴充欄位

OCSP 回應伺服器簽發的線上憑證狀態協定回應封包包含有以下擴充欄位：

- OCSP 回應伺服器的憑證機構金鑰識別碼(Authority Key Identifier)
- 此外當 OCSP 請求封包含有隨機數(nonce)欄位時，OCSP 回應封包也必須包含相同的隨機數欄位。
- 簽章憑證時戳(Signed Certificate Timestamp)
- OID 為 1.3.6.1.4.1.11129.2.4.5，為配合憑證透明度(Certificate Transparency) 使用。

### 7.3.3 線上憑證狀態協定服務運轉規範

本管理中心線上憑證狀態協定服務運轉作業包含有以下：

- 可以處理與接受 HTTP Get/Post 管道或方法所傳送 OCSP 用戶端之查詢請求封包(OCSP Request)。

線上憑證狀態協定服務伺服端所使用的 OCSP 回應伺服器憑證為本管理中心所簽發，且必須為短效期之有效憑證，由本管理中心定期簽發與更新。

# 8 稽核及其他評核

## 8.1 稽核頻率或評核事項

本管理中心接受每年1次的外部稽核(且查核期間不可超過12個月)與不定期的內部稽核，以確認本管理中心的運作確實遵循 HiPKI 憑證政策及本作業基準所訂的安全規定與程序。

## 8.2 稽核人員之身分及資格

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 WebTrust for CA、 WebTrust for CA – EV SSL 及 WebTrust for CA – SSL BR 稽核標準之合格稽核業者，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 Auditor)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。執行 WebTrust for CA – EV SSL 外部稽核之業者應投保專業責任/錯誤和疏漏險(Professional Liability/Errors and Omissions Insurance)，保險理賠金額至少為 100 萬美元。本管理中心於稽核時應對稽核人員進行身分識別。

## 8.3 稽核人員及被稽核方之關係

本公司將委託公正之第三方，就本管理中心的運作進行稽核。

## 8.4 稽核項目

稽核採用的標準為 WebTrust for CA、WebTrust for CA – EV SSL 及 WebTrust for CA – SSL BR。

稽核項目如下所述：

(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) 註冊中心是否遵照本作業基準及相關程序運作

(3) 本作業基準是否符合憑證政策之規定，且對本管理中心之實務作業而言是否允當

負責審驗 EV TLS/SSL 憑證的申請或廢止審核的註冊中心應接受每 1 年 1 次之外部稽核，記錄任何和 HiPKI 憑證政策或憑證實務作業基準不符合或例外之事項，並採取行動矯正缺失。

本公司保留對於註冊中心是否遵循 HiPKI 憑證政策及本作業基準的符合性查核(compliance audit)權力，以降低任何有不符合 HiPKI 憑證政策或憑證實務作業基準衍生的風險。本公司有權執行其他包含但不限於以下項目的查核或調查，以確保本管理中心之公信力：

(1) 若有事件造成本公司合理懷疑註冊中心由於電腦緊急事件或金鑰遭破解而無法符合 HiPKI 憑證政策與本作業基準。

(2) 在符合性查核有不完整或特殊發現下，本公司有權執行風險管理之查核。

(3) 由於註冊中心的行動或不採取行動造成實際或潛在對於本基礎建設之安全性與完整性之威脅，本公司有權執行相關之查核或調查。

本公司有權將稽核調查的功能委託第三方稽核業者執行，受稽之註冊中心應提供本公司和執行稽核或調查的人員充分而合理之合作。

本管理中心由稽核員依據 EV SSL Certificate Guidelines，至少每季針對簽發 EV TLS/SSL 憑證的註冊中心，自前 1 次抽樣後執行持續性之內部稽核，隨機選擇 EV TLS/SSL 憑證簽發數量的至少 3%(若不足 1 張視為 1 張)進行內部稽核。對於若由註冊中心執行第 3.2.8.4 節最後交互關連與基於良善管理之盡職調查所簽發的 EV TLS/SSL 憑證，為了控制服務品質，必須由前次抽樣後的期間執行持續性隨機抽樣 EV TLS/SSL 憑證簽發數量的至少 6%(若不足 1 張視為 1 張)進行自我檢查。

## 8.5 對於稽核結果之因應方式

如稽核人員發現本管理中心或註冊中心之建置與維運不符合本作業基準規定時，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，如不符合情形為嚴重缺失，稽核

人員應通知政策管理委員會

(3) 對於不符合規定之項目，本管理中心將於 30 日內提出改善計畫，儘速執行，並列入後續稽核追蹤項目。有關註冊中心之缺失將通知註冊中心改善。

## 8.6 稽核結果之公開

除可能導致系統被攻擊以及第 9.3 節規定之範圍外，本管理中心將公布合格稽核業者所提供之應公開說明資訊。稽核結果以 WebTrust for CA、WebTrust for CA – EV SSL 或 WebTrust for CA – SSL BR 標章之方式呈現於本管理中心網站首頁，點選標章後可閱覽外稽報告與管理聲明書。最近 1 次的外稽報告與管理聲明書亦於查核區間結束後 3 個月內公布於儲存庫。若因故延遲公布最近 1 次稽核結果，本管理中心將提供合格稽核業者簽署之解釋函。

# 9 其他業務及法律事項

## 9.1 費用

### 9.1.1 憑證簽發、展期費用

本管理中心與用戶之間的憑證申請及簽發等計費架構，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。

### 9.1.2 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。

### 9.1.3 憑證廢止、狀態查詢費用

用戶下載查詢憑證廢止清冊不收費；線上憑證狀態協定查詢服務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。

### 9.1.4 其他服務費用

不做規定。

### 9.1.5 退費

本管理中心所收取之憑證簽發收費，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。除前述情形及第 4.9 節之情形外，其他費用均不退費。

## 9.2 財務責任

發生損害而非屬於第 9.2.1 節所揭露之一般商業責任險的理賠涵蓋範圍時，將以第 9.2.2 節所揭露符合 EV SSL Certificate Guidelines 規範之其他資產負責損害賠償。

### 9.2.1 保險涵蓋範圍

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。本公司已投保最高賠償金額為新台幣 120,000,000 元的一般商業責任險，未來若主管機關有規範憑證業務之財務保險將配合辦理。

### 9.2.2 其他資產

本管理中心之財務，係屬本公司整體財務之一部分。本公司為股票上市公司，也是於美國紐約證券交易所上市的中華民國公司，依證券交易法第 36 條之規定，應於每營業年度終了後 3 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 1 季、第 2 季及第 3 季終了後 45 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 10 日以前，公告並申報上月份營運情形。本管理中心可提供自我擔保之資產價值依本公司年度財務報告為準。本公司財務健全，會計師查核簽證之年度財務報告顯示流動資產符合 EV SSL Certificate Guidelines 之要求超過 5 億元美金，且流動資產與流動負債比符合不低於 1.0，具備若發生損害時足夠的賠償能力。

### 9.2.3 對終端個體之保險或保固

對終端個體(用戶及信賴憑證者)之保險或保固責任不做規定。

## 9.3 業務資訊之保密

### 9.3.1 機密資訊之範圍

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，不得被完整公開。

(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。

### 9.3.2 非機密之資訊

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

### 9.3.3 保護機密資訊之責任

本管理中心依照電子簽章法、Baseline Requirements、EV SSL Certificate Guidelines、WebTrust for CA 稽核標準、WebTrust for CA－EV SSL 稽核標準、WebTrust for CA－SSL BR 稽核標準及個人資料保護法處理本管理中心之用戶申請資料。

## 9.4 個人資訊之隱私

### 9.4.1 隱私保護計畫

本管理中心於網站公告個人資料保護與隱私權聲明。本管理中心實施隱私衝擊分析、個資風險評鑑等措施並訂定隱私保護計畫。

### 9.4.2 隱私之資訊

(1)任何在憑證申請時記載之個人資訊，未經用戶同意或依法律規定不得公開。

(2)無法透過憑證、憑證廢止清冊所記載之資訊或憑證目錄服務所取得的用戶資訊。

(3)憑證機構信賴角色維運之可識別的個人資料如姓名搭配掌紋特徵與指紋特徵。

(4)保密協定或契約之個人資訊。

本管理中心及註冊中心實施安控措施防止隱私資料遭未經授權的揭露、洩漏或破壞。

### 9.4.3 非隱私之資訊

識別資訊或記載於憑證的資訊與憑證，除特別約定外，不視為隱私資訊。

儲存庫公布之簽發憑證、已廢止憑證或暫時停用資訊及憑證廢止清冊非隱私資訊。

### 9.4.4 保護隱私資訊之責任

配合本管理中心運作所需之個人資料，無論紙本或是電子之形式，必須依照於網站公告的個人資料保護暨隱私權聲明，安全存放與受到保護，符合電子簽章法、Baseline Requirements、EV SSL Certificate Guidelines、WebTrust for CA 稽核標準、WebTrust for CA－EV SSL 稽核標準、WebTrust for CA－SSL BR 稽核標準及個人資料保護法相關規定。本管理中心並與註冊中心協議保護隱私資訊的責任。

### 9.4.5 使用隱私資訊之告知與同意

遵循個人資料保護法，非經用戶同意或本管理中心網站公告之個人資料保護與隱私權聲明與本作業基準另有規範，不會將個人資料用於其他地方。用戶得查詢第 9.3.1 節第(3)款用戶本身之申請資料；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。

### 9.4.6 應司法或管理程序釋出資訊

司法機關、監察機關或治安機關如因調查或蒐集證據需要，必須查詢第 9.4.2 節隱私之資料，依法律規定辦理；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。

### 9.4.7 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，將遵守相關法律規範，不對外揭露以確保用戶個人隱私。但法律另有規定時，不在此限。

## 9.5 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。

本作業基準可由儲存庫自由下載，或依著作權法相關規定合理使用。散布本作業基準者，不得向他人收取費用，對於不當使用或散布本作業基準之侵害，本公司將依法予以追訴。

## 9.6 聲明及擔保

### 9.6.1 憑證機構之聲明及擔保

本管理中心向憑證之受益人(包括用戶、信賴憑證者及應用軟體供應商)聲明及擔保在憑證效期內，係遵照憑證政策及本作業基準之規定進行憑證之簽發及管理。

具體地憑證擔保包含(但不限於)以下事項：

(1) 有權使用網域名稱

於憑證核發時，本管理中心會(i)驗證申請者確實擁有記載於憑證主體欄位或主體別名延伸欄位之網域的授權或控制權；(ii)依照此程序進行憑證之簽發；及(iii)正確地將此程序描述於本作業基準(參見第 3.2 節)。

(2) 憑證授權

於憑證核發時，本管理中心會(i)驗證憑證之主體已授權憑證之簽發且申請代表人為憑證之主體所授權進行憑證請求；(ii)依照此程序進行憑證之簽發；及(iii)正確地將此程序描述於本作業基準(參見第 3.2.5 節)。

(3) 資訊正確性

於憑證核發時，本管理中心會(i)驗證記載於憑證內之所有資訊的正確性；(ii)依照此程序進行憑證之簽發；及(iii)正確地將此程序描述於本作業基準(參見第 3.2.2、第 3.2.3 及第 3.2.7 節)。

(4) 無誤導資訊

於憑證核發時，本管理中心會(i)降低記載於憑證主體附屬單位的資訊可能會造成誤導之可能性；(ii)依照此程序進行憑證之簽發；及(iii)正確地將此程序描述於本作業基準(參見第 3.2.2、第 3.2.3 及第 3.2.7 節)。

(5) 申請者的身分

若憑證中包含主體身分資訊，本管理中心會(i)依照第 3.2.2 及第 3.2.3 節的規定驗證申請者之身分；(ii)依照此程序進行憑證之簽發；及(iii)正確地將此程序描述於本作業基準。

(6) 用戶協議

若本管理中心與用戶非隸屬同一組織，則用戶與本管理中心是符合 Baseline Requirements 要求之合法有效且可執行用戶協議的當事方；若本管理中心與用戶隸屬同一組織，則由申請代表人轉知使用條款。

(7) 狀態

本管理中心維護一個 7 天 x 24 小時可公開存取的儲存庫，其中包含所有未到期憑證狀態(有效或已廢止)的最新資訊(參見第 4.10.2 節)。

(8) 廢止

本管理中心將根據 Baseline Requirements 及/或 EV SSL Certificate Guidelines 中所規定的任何理由廢止憑證(參見第 4.9.1 節)。

對於延伸驗證型 TLS/SSL 憑證，本管理中心向用戶、信賴憑證者及應用軟體供應商聲明，本管理中心係遵照 EV SSL Certificate Guidelines 之規定進行資訊驗證及延伸驗證型 TLS/SSL 憑證之簽發。

### 9.6.2 註冊中心之聲明及擔保

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。

註冊中心應聲明及擔保：

(1)對於憑證註冊審驗，係遵照憑證政策及本作業基準之規定

(2)提供給簽發憑證機構之資訊皆為正確且無誤之資訊

(3)若需提供服務內容之翻譯皆為精確翻譯之資訊

(4)提出之憑證請求符合本作業基準之規定

(5)實施憑證註冊審驗人員之識別與鑑別程序

(6)安全地管理註冊中心之私密金鑰

### 9.6.3 用戶之聲明及擔保

為了本管理中心及憑證受益人之明確利益，申請人應擔保憑證核發前，本管理中心會收到：

(1)申請人同意的用戶協議；或

(2)申請人對用戶條款的確認。

申請人(或設備憑證之保管人、存在分包商或託管服務關係之代理商)應向本管理中心聲明及擔保下列事項：

(1)安全地產製其私密金鑰並避免遭受破解

(2)提供本管理中心及註冊中心正確及完整之資訊

(3)遵守第 3 及第 4 章之規定及程序

(4)於使用憑證前確認憑證中資料之正確性

(5)立即通知本管理中心、停止使用憑證並要求廢止憑證，包括：

(i) 記載於憑證中的資訊已經變更或可能誤導；

(ii) 有任何實際或懷疑憑證所記載之公開金鑰其相對應的用戶私密金鑰遭誤用或破解 (並停用私密金鑰)

(6)憑證只用於符合憑證政策、本作業基準及用戶協議之合法及經授

權的使用目的，包含只安裝 TLS/SSL 憑證於憑證中所註記之完全吻合網域名稱的伺服器

(7)於憑證到期後，立即停止使用憑證及其對應之私密金鑰

### 9.6.4 信賴憑證者之聲明及擔保

信賴憑證者應聲明與擔保以下之責任：

(1)使用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)使用憑證前，應先查驗該憑證之保證等級

(3)使用憑證前，應確認該憑證所記載之金鑰用途

(4)使用本管理中心簽發之憑證廢止清冊或線上憑證狀態協定查驗本管理中心簽發之憑證，以確認該憑證之有效性

(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或用戶權益受損時,信賴憑證者應自行承擔責任

(6)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

(7)接受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，並依照第 1.4.1 節規定範圍使用憑證

如有違反，應依照民法及相關法規之規定負擔對他人的損害賠償責任。

### 9.6.5 其他參與者之聲明及擔保

不做規定。

## 9.7 免責聲明

除法律或本作業基準另有規範禁止之範圍外，HiPKI 在此特別對商品使用及特定目的合用性之明示及默示的保證作免責聲明。

## 9.8 責任限制

用戶或信賴憑證者如未依照 Baseline Requirements 及本作業基準之適用範圍使用憑證所引發之損失，HiPKI 不負任何賠償責任。若屬可歸咎於 HiPKI 之責任，其賠償金額上限依照本作業基準第 9.9 節規範。

## 9.9 賠償

### 9.9.1 本管理中心之賠償責任

本管理中心處理用戶憑證相關作業，若故意或過失未遵照 HiPKI 憑證政策、本作業基準、EV SSL Certificate Guidelines、相關法律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，由本公司負賠償責任。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。本公司之財務責任如第 9.2.1 與第 9.2.2 節所述，若發生誤發憑證或憑證機構私密金鑰遭破解之損害時的賠償能力符合 EV SSL Certificate Guidelines 之規範。

### 9.9.2 註冊中心之賠償責任

註冊中心由本公司建置，處理用戶憑證註冊作業，若故意或過失未遵照本作業基準、相關法律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，由本公司負賠償責任，賠償上限遵循第 9.9.1 節規定。用戶或信賴憑證者與註冊中心若訂有合約，另行規範憑證使用範圍與交易賠償限額者，從其約定。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。

## 9.10 本文件之生效與終止

### 9.10.1 生效

本作業基準於主管機關依電子簽章法核定通過後，於本管理中心儲存庫公布後即生效。

### 9.10.2 終止

本作業基準新版本經主管機關核定後公布，現有版本即告終止。

### 9.10.3 終止與保留之效力

本作業基準之效力，維持至遵循本作業基準所簽發之最後一張憑證到期或廢止為止。

## 9.11 主要成員之個別告知及溝通

本管理中心、註冊中心、用戶、信賴憑證者彼此間得採適當的方式，建立通告與聯絡管道，包括但不限於：公文、書信、電話、傳真、電子郵件或安全電子郵件。

## 9.12 修訂

### 9.12.1 修訂程序

如 HiPKI 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，且以適當之版本編號代表本作業基準有進行修訂，並依據第 2.3 節規定進行公告。

### 9.12.2 通知之機制及期限

重大變更項目及修訂之憑證實務作業基準生效日期將公告於本管理中心網站。用戶或信賴憑證者對於變更項目有意見者，可於公告之意見回覆期限截止前提出，由本管理中心考量相關意見，評估變更項目與回覆。

本作業基準重新排版時，不另作通知。

### 9.12.3 物件識別碼必須更改之情況

憑證政策的修改不影響憑證政策所聲明的憑證使用目的與保證度時，憑證政策之物件識別碼不需修改，憑證政策之物件識別碼變更，憑證實務作業基準應作相對應之變更。

## 9.13 爭議解決條款

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。

## 9.14 管轄法律

牽涉本管理中心所簽發之憑證的任何爭議由中華民國相關法律規定管轄。

## 9.15 適用法律

依據本作業基準所簽署的任何協議之解釋及合法性，必須遵循中華民國相關法律之規定。

## 9.16 雜項條款

### 9.16.1 完整協議

本作業基準所約定者，係主要成員(本管理中心、註冊中心、用戶、信賴憑證者)間最終且完整的約定。

### 9.16.2 轉讓

本作業基準所敘述的主要成員之間的權利或責任，不能在未通知本管理中心下以任何形式轉讓給其他方。

### 9.16.3 可分割性

本作業基準的任一條款不正確或無效時，其他條款仍然有效，直到本作業基準修改為止。

本作業基準遵循 Baseline Requirements 及 EV SSL Certificate Guidelines 對憑證機構之要求，惟 Baseline Requirements 及 EV SSL Certificate Guidelines 相關規定若與本作業基準所依循之本國相關法律或法規產生衝突時，本作業基準得調整相關作法以滿足法律或法規之要求，並將變更調整之部分通知憑證機構與瀏覽器論壇；若本國法律或法

規已不再適用時，或憑證機構與瀏覽器論壇修訂 Baseline Requirements 及 EV SSL Certificate Guidelines 之相關內容使其規定可相容於本國法律時，則本作業基準將刪除並修訂原先所調整之內容，上述作業須於 90 個工作天內完成。

### 9.16.4 契約履行

因可歸責於用戶或信賴憑證者之故意或過失違反本憑證作業基準相關規定，致本管理中心受有損害時，本管理中心除得請求損害賠償以外，並得向可歸責之一方請求支付為處理該爭議或訴訟之律師費用。

本管理中心未向違反本憑證作業基準相關規定者主張權利，不代表本管理中心對於其繼續或未來違反本憑證作業基準情事，有拋棄權利主張之意思。

### 9.16.5 不可抗力

因不可抗力或其他非可歸責於本管理中心之事由致用戶或信賴憑證者受有損害，包含因天然災害、戰爭、恐怖攻擊等致電信網路中斷之事件，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。

## 9.17 其他條款

不做規定。