中華電信 HiPKI 憑證管理中心
憑證政策暨憑證實務作業基準

(Chunghwa Telecom HiPKI Certification Authority Certificate Policy/Certification Practice Statement, HiPKICA CP/CPS)

第 1.2 版

中華電信股份有限公司

中華民國 115 年 06 月 11 日

目　　錄

憑證實務作業基準修訂履歷表

版次	實施日期	修訂內容摘要
1.0	114/08/18	1. 初版發行 2. 配合 TLS 業務根憑證重新植入瀏覽器信賴清單申請之基本要求，本文件合併 HiPKI CP 及 HiPKICA CPS 之實務。 3. 配合 BR 及 Browser Root Program 規定，移除 BR 第 3.2.2.4.2, 3.2.2.4.4, 3.2.2.4.13 及 3.2.2.4.14 節之驗證方法。
1.05	114/08/25	1. 配合新 CA 金鑰產製，1.3.1 節新增 CHT TrustRoot CA 及 CHT Trust TLS CA CA 名稱 2. 附錄 4 新增 CHT TrustRoot CA - G1 及 CHT Trust TLS CA-G1 CA 憑證資訊
1.1	115/03/06	1. 配合 BR 及 Browser Root Program 規定，進行驗證方法與合規檢視，修訂範圍包含 1.1, 3.2.7, 3.2.7.1, 3.2.7.2, 3.2.7.3, 3.2.7.4, 4.2.2, 5.7.1.1, 5.7.1.2, 5.7.2 節及附錄 2。 2. 其餘修訂章節為 1.4.2, 5.2.2, 5.3.5, 6.3.2.1, 7.1.5 節, 附錄 3-1, 附錄 3-2 及附錄 4。
1.2	115/06/11	1. 配合 Root Program Policy 新增根憑證機構/下屬憑證機構簽發 CRL 之欄位及擴充欄位說明，以及進行內文文字微調。 2. 修訂範圍為 3.1.5、3.2.10、4.2.1、6.3.2.1、6.7、7.1、7.1.1、7.1.4.2、7.1.4.3、7.2、7.2.1、7.2.2、7.3.1、附錄 3、附錄 3-1、附錄 3-2 及附錄 5。

1 序論

HiPKI (簡稱本基礎建設)係配合中華電信股份有限公司(簡稱本公司)推動電子化服務及健全電子商務基礎環境之政策而設立。本憑證政策/憑證實務作業基準 (Certificate Policy/Certificate Practices Statement, CP/CPS，簡稱本文件)定義了與 HiPKI 憑證服務相關的政策、原則和實務。本基礎建設所簽發的憑證可適用於電子商務及電子化政府之各項應用，以提供更安全、可信賴及便捷的網路服務。

1.1 概要

HiPKI 下的根憑證機構(Root Certification Authority, Root CA)為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，信賴憑證者可直接信賴根憑證機構的憑證。本文件以中華電信 HiPKI 憑證管理中心(HiPKICA)之品牌名稱，稱呼本基礎建設中由本公司所擁有與營運的根憑證機構與第 1 層下屬憑證機構，HiPKICA 憑證機構清單請參閱第 1.3.1 節。

本文件係依據國際相關標準或規範如：

(1) 網際網路工程任務小組(Internet Engineering Task Force, IETF)之徵求修正意見書(Request for Comments, RFC) 3647、RFC 5280、RFC 6960、RFC 6962、RFC 5019、RFC 8659；

(2) ITU-T X.509；

及以下之最新發布版本政策文件

(1) 憑證機構與瀏覽器論壇 (CA/Browser Forum, https://www.cabforum.org) 發行的 Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server

Certificates(以下簡稱 Baseline Requirements)及 Network and Certificate System Security Requirements；

(2) Mozilla Root Store Policy；

(3) Microsoft Trusted Root Program Requirements；

(4) Apple Root Certificate Program Policy；

(5) Common CA Database (CCADB) Policy 及

(6) Google Chrome Root Program Policy

所訂定之政策文件，以做為本基礎建設各憑證機構實務上作業之依循。

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 協定運作且符合 X.509 標準之憑證，本文件以 TLS 憑證取代先前廣泛使用的 SSL 憑證稱呼。

1.1.1 本文件之適用範圍

本文件所載明之實務作業規範適用於 HiPKICA 之憑證機構、註冊中心、用戶、信賴憑證者、儲存庫及其他相關成員等。

1.1.2 憑證機構引用憑證政策物件識別碼

本基礎建設所使用的憑證政策物件識別碼(certificate policy object identifier, CP OID)，供憑證機構在簽發某一特定用途憑證時標示保證度，憑證機構可直接引用已註冊的憑證政策物件識別碼，而信賴憑證者可透過憑證政策物件識別碼檢驗憑證機構簽發憑證的適用性是否正確。

依照 ITU-T X.509 標準，本文件所定義的保證等級(Assurance Level)必須以物件識別碼(Object Identifier, OID，詳見第 1.2 節)表示，

而這些物件識別碼將會記載在憑證的憑證政策擴充欄位(certificatePolicies extension)中。

本基礎建設之憑證機構於簽發憑證時應引用適合的憑證政策物件識別碼，如此本基礎建設內的各憑證機構間便可進行互運(Interoperation)，並且可進一步與國內外公開金鑰基礎建設領域進行跨領域互運。透過成對的憑證政策物件識別碼可確認簽發憑證機構(Issuing CA)與主體憑證機構(Subject CA)之間的憑證政策對應關係。

1.2 文件名稱與識別

本文件的名稱為中華電信 HiPKI 憑證管理中心憑證政策暨憑證實務作業基準(Chunghwa Telecom HiPKI Certification Authority Certificate Policy/Certification Practice Statement)，本文件之最新版本可在以下網頁取得：

https://chtca.hinet.net/repository.html

本基礎建設之憑證機構應遵循本文件，本基礎建設依照憑證機構之鑑別方式及適用範圍的不同，將其所核發之憑證分成 4 個保證等級。保證等級越高，安全等級及可信賴度越高，且鑑別方式越嚴格。

下表為本基礎建設對本文件提到的各類憑證、保證等級及文件所設定之物件識別碼參照表：

物件名稱	物件識別碼
HiPKI	1 3 6 1 4 1 23459 200 0
保證等級	
第 1 級	1 3 6 1 4 1 23459 200 0 1
第 2 級	1 3 6 1 4 1 23459 200 0 2
第 3 級	1 3 6 1 4 1 23459 200 0 3

物件名稱	物件識別碼
第 4 級	1 3 6 1 4 1 23459 200 0 4
Baseline Requirements	
組織驗證型 TLS 憑證	2.23.140.1.2.2

其中以{2.23.140}為開頭的物件識別碼係參照憑證機構與瀏覽器論壇依據不同文件及憑證使用範圍所定義；而 arc 值 id-pen-cht ::= {1 3 6 1 4 1 23459}是本公司在網際網路號碼分配機構(Internet Assigned Numbers Authority, IANA)註冊之私人企業號碼(Private Enterprise Number, PEN)，本基礎建設使用的物件識別碼是{1 3 6 1 4 1 23459 200}，並依照各類憑證之保證等級分配不同的物件識別碼以資區別。

根憑證機構的憑證是自簽憑證(Self-Signed Certificate)，依照國際標準及慣例，根憑證機構的憑證並無標示憑證政策物件識別碼，因應根憑證機構必須具備高公信力，以保證等級第 4 級運作。

簽發 TLS 憑證之 CA 遵循 Baseline Requirements 規範，將使用 CA/Browser Forum 之組織驗證(Organization Validation, OV)TLS 憑證政策物件識別碼({joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline- requirements(2) organization-validated(2)} (2.23.140.1.2.2))。

若本文件在 TLS 憑證簽發上與 Baseline Requirements 正式版之規定有任何不一致的情形，將優先遵循 Baseline Requirements 的條款。

簽發組織驗證型 TLS 憑證之憑證機構，若有憑證機構與瀏覽器論壇相關文件未規範處，適用本文件有關保證等級第 3 級之規範；簽發自簽、自發(Self-Issued)及交互憑證(Cross-Certificate)之根憑證機構，一律適用本文件有關保證等級第 4 級之規範。

1.3 主要成員

HiPKICA 之相關成員包括：

(1) HiPKICA 之憑證機構

(2) 註冊中心

(3) 用戶

(4) 信賴憑證者

1.3.1 憑證機構

HiPKICA 之憑證機構(列表如下)由中華電信股份有限公司(簡稱本公司)負責建置及營運，本文件中所述之相關作業準則由中華電信憑證政策管理委員會(Chunghwa Telecom Certificate Policy Management Authority，以下簡稱政策管理委員會)進行審查及核定。

根憑證機構	
	HiPKI Root CA
	CHT TrustRoot CA
下屬憑證機構	
	HiPKI OV TLS CA
	CHT Trust TLS CA

HiPKICA 的憑證機構憑證資訊與適用的本文件、外部稽核報告及管理聲明書皆公布在 CA 儲存庫中。HiPKICA 憑證機構憑證序號及憑證拇指紋等重要資訊清單請參見附錄 4。

1.3.1.1 根憑證機構

根憑證機構，也是代表本基礎建設的主要憑證機構(Principal CA)，主要工作說明如下：

(1) 負責根憑證機構之自簽憑證、自發憑證與下屬憑證機構憑證之簽發及管理。

(2) 訂定與本基礎建設外之根憑證機構間的交互認證程序，包括簽發及管理其他本基礎建設外根憑證機構的交互憑證。

(3) 將簽發的憑證廢止清冊(Certificate Revocation List，CRL)公布於儲存庫(Repository)，並且確保儲存庫之正常運作。

根憑證機構在經本公司核准後，得與本基礎建設外之根憑證機構進行交互認證。

1.3.1.2 下屬憑證機構

下屬憑證機構為本基礎建設中的另一種憑證機構，主要負責簽發及管理終端個體的憑證。但下屬憑證機構不可以直接與本基礎建設外的憑證機構進行交互認證。

1.3.1.3 交互認證憑證機構

目前 HiPKCA 之根憑證機構並無與任何本基礎建設以外之憑證機構進行交互認證。根憑證機構簽發交互憑證給本基礎建設外之根憑證機構前，應由政策管理委員會決策是否允許。

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 1 個或多個註冊窗口(RA Counter)組成，由 HiPKICA 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 HiPKICA 不同群組與類別之憑證申請、廢止、憑證之更換金鑰等作業。

根憑證機構直接受理憑證機構憑證註冊與廢止申請等工作，負責蒐集及驗證下屬憑證機構、交互認證憑證機構之身分及憑證相關資訊，不另設立註冊中心。

下屬憑證機構之註冊中心由下屬憑證機構所直接設立與維運，註冊中心也必須遵循本文件之規定運作。

HiPKICA 不允許委派第三方(Delegated Third Parties)擔任 TLS 憑證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 HiPKICA、受委託協助憑證管理流程的自然人或法人，且不在 HiPKICA 之外稽範圍內。

1.3.3 用戶

用戶係指已申請並取得 HiPKICA 簽發憑證之個體，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文件第 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。

在本基礎建設中，上層憑證機構會簽發憑證給下屬(層)憑證機構，在本文件中並不稱下屬憑證機構為用戶。

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之第三人。信賴憑證者必須依照相對的憑證機構憑證及憑證狀態資訊，以驗證所使用憑證的有效性。

1.3.5 其他相關成員

不做規定。

1.4 憑證用途

本公司將審慎評估各種風險、應用環境、可能弱點及憑證的用途，並選擇適當之保證等級進行憑證機構的運作，及簽發與管理憑證。

1.4.1 憑證適用範圍

根憑證機構簽發的憑證有 4 種，分別為自簽憑證、自發憑證、下屬憑證機構憑證與交互憑證，自簽憑證、自發憑證及交互憑證的保證等級屬於第 4 級(組織鑑別方式可參考第 3.2.2 節)，目前設立的下屬憑證機構其保證等級為第 3 級，各憑證類別與適用範圍說明如下：

憑證類別	適用範圍
自簽憑證	自簽憑證用以建立 HiPKI 信賴的起源。 自簽憑證之簽發對象為根憑證機構本身，內含根憑證機構的公開金鑰，可用來驗證根憑證機構簽發之下屬憑證機構憑證、交互憑證、自發憑證與憑證廢止清冊(Certificate Revocation List, CRL)的數位簽章。
自發憑證	自發憑證為根憑證機構更換金鑰或憑證政策時，新舊兩代金鑰互簽或單方向舊簽發新，做為互通信賴路徑之用。
下屬憑證機構憑證	用以建構憑證機構互通所需的憑證信賴路徑之用。 下屬憑證機構憑證內含下屬憑證機構的公開金鑰，可用來驗證下屬憑證機構所簽發之憑證與憑證廢止清冊的數位簽章。
交互憑證	交互憑證用以建立不同公開金鑰基礎建設之憑證機構間的互相信賴關係，以建構憑證機構互通所需的憑證信賴路徑之用。 交互憑證之簽發對象為與根憑證機構進行交互認證之本基礎建設外之公開金鑰基礎建設的根憑證機構。

	交互憑證內含交互認證憑證機構的公開金鑰，可用來驗證該憑證機構簽發之憑證與憑證廢止清冊的數位簽章。

配合 Chrome Root Certificate 政策規範，下屬憑證機構只會簽發應用於傳輸層安全(Transport Layer Security, TLS)通訊協定之設備或應用軟體用 TLS 憑證，保證等級與組織鑑別方式可參考第 3.2.2 節。各憑證類別與適用範圍說明如下：

憑證類別	適用範圍
第 3 級 OV TLS 憑證	提供通訊管道之加密，且必須鑑別網域名稱擁有者屬於那一個組織的場合，適用於保護網路通訊。

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。使用及信賴 HiPKICA 所提供的認證服務前，用戶及信賴憑證者都應詳細閱讀、遵守本文件，並且應注意本文件的更新。

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 憑證禁止事項

HiPKICA 所簽發的憑證禁止使用於下列的情況：

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

(2) 會造成人身傷亡與精神侵害之用途，或對社會秩序與公共利益有重大危害之應用或業務

(3) 其他相關法令或各事業目的主管機關明訂禁止或排除之應用或業務

用戶應遵守所有適用瀏覽器根憑證政策(Browser root policies)的所有要求，包括本文件規定的 24 小時以及 5 天內的廢止期限。

1.5 政策管理

1.5.1 本文件之制訂與管理機構

中華電信股份有限公司。

1.5.2 聯絡資料

1.5.2.1 本文件建議

對本文件有疑義需要諮詢，或有修訂建議，請利用以下資訊與 HiPKICA 聯繫：

電子郵件信箱：caservice@cht.com.tw

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 HiPKI 憑證管理中心。

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、濫用或不當使用等情況(包含工作日以外時間)時，可寄送電子郵件至 report_abuse@cht.com.tw 向 HiPKICA 提出憑證問題報告(Certificate Problem Report)。HiPKICA 是否廢止該憑證，參見第 4.9.3 及 4.9.5 節。

1.5.3 本文件之審定

HiPKICA 自行檢查憑證實務是否符合本文件相關規定後，再送政策管理委員會進行審查及核定。在核定後 HiPKICA 正式引用本基

礎建設的憑證政策物件識別碼。

HiPKICA 定期自行稽核，以證明遵照引用於本文件的保證等級進行營運。為使 HiPKICA 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，將根憑證機構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，每年併同根憑證機構執行外部稽核並將最新之本文件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 HiPKICA 網站。

1.5.4 本文件核准程序

本文件經政策管理委員會核定後，由 HiPKICA 公布。

本文件修訂生效後，除另有規定外，如修訂之版本與原本文件有所牴觸時，以修訂之版本為準。

1.6 名詞定義及縮寫

參見附錄 1 縮寫和定義與附錄 2 名詞解釋。

2 資訊公布與儲存庫之責任

2.1 儲存庫

HiPKICA 儲存庫負責公告及儲存由 HiPKICA 所簽發之憑證及憑證廢止清冊(Certificate Revocation List, CRL)及本文件，提供用戶及信賴憑證者查詢服務，網址為 https://chtca.hinet.net/repository.html。

如因故無法正常運作，將於 2 個工作天內恢復正常運作。

2.2 憑證機構之資訊公布

HiPKICA 會將以下之資訊公布於儲存庫：

(1) 本文件。

(2) 所有憑證機構憑證、交互憑證及憑證廢止清冊。

(3) 隱私權保護政策。

(4) 最近 1 次之外部稽核結果（如第 8.6 節所述）。

簽發 TLS 憑證之 CA 會提供應用軟體供應商(Application Software Supplier)測試安裝由該 CA 所簽發有效、過期與廢止的 TLS 憑證之網址。

簽發 TLS 憑證之 CA 的 CAA(Certification Authority Authorization，授權憑證機構簽發憑證) Issuer Domain Name(如第 4.2.1 節所述)包含 "pki.hinet.net"或"tls.hinet.net"。

2.3 公布之時間或頻率

(1)HiPKICA 至少每 366 天要檢視與更新本文件，版本變更摘要將記載於版本修訂履歷。

(2) 本文件新版或修訂後之版本於政策管理委員會核定後儘速於儲存庫公布

(3) HiPKICA 每天至少簽發兩次憑證廢止清冊，公布於儲存庫。

(4) HiPKICA 本身之憑證,於簽發後 7 個工作天內公布於儲存庫。

2.4 儲存庫之存取控制

HiPKICA 提供對於儲存庫唯讀的閱覽存取，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 識別與鑑別

3.1 命名

3.1.1 命名種類

憑證之命名種類如下：

(1) 憑證主體名稱採用 ITU-T X.500 唯一識別名稱(Distinguished Name, DN)；

(2) 憑證主體別名(Subject Alternative Name)擴充欄位須為非關鍵性擴充欄位；其用於記載網域名稱時，採用 dNSName 格式。

3.1.2 命名須有意義

HiPKICA 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。

簽發憑證機構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。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。

TLS 憑證之通用名稱(Common Name)與憑證主體別名欄位應註記完全吻合網域名稱(Fully Qualified Domain Name)。組織驗證型(OV)之 TLS 憑證其唯一識別名稱應包含第 3.2.2 節所驗證之組織身分資訊於組織名稱(Organization)欄位。

3.1.3 用戶之匿名或假名

HiPKICA 不簽發匿名憑證(anonymous certificate)。

如果用戶提交的申請包含國際化網域名稱(Internationalized Domain Names, IDNs)，必須轉成 Punycode 編碼才能投單申請。解碼後的國際化網域名稱將被視為高風險憑證請求，並將按照第 4.2.1 節所述進行額外檢查(例如，與之前被拒絕簽發的憑證請求或廢止的憑證進行比較)，以降低網路釣魚與其他欺詐性使用的風險。

3.1.4 不同命名形式之解釋規則

命名形式之解釋規則依 ITU-T X.520 名稱屬性定義。

3.1.5 命名之獨特性

HiPKICA 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 HiPKICA 所認知的 X.500 名稱空間內具備獨特性。HiPKICA 之用戶憑證主體名稱允許使用以下 X.520 標準所定義的各種命名屬性加以組合而成：

- countryName(縮寫為 C)
- localityName(縮寫為 L)
- organizationName(縮寫為 O)
- commonName(縮寫為 CN)

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，HiPKICA 雖不負審查之責任，但其命名須符合中華民國商標法、公平交易法及其他法律相關規定。HiPKICA 不保證用戶憑證主體名稱若含商標之認可、驗證、合法及唯一性。相關糾紛或仲裁處理非 HiPKICA 權責範圍，由用戶向相關主管機關、法院或仲裁機構提出申請。

HiPKICA 可能會拒絕任何申請或得逕行廢止(可參考第 4.9.1 節)任何屬於商標爭議的憑證。

3.2 初始身分驗證

3.2.1 證明擁有私密金鑰之方式

HiPKICA 會驗證個體(憑證機構或終端用戶)持有之私密金鑰與將記載於憑證上的公鑰成對。

金鑰對須由憑證申請者自行產製，透過以私密金鑰加以簽章產生的 PKCS#10 憑證申請檔，並於申請憑證時將該憑證申請檔交給註冊中心，註冊中心將使用該個體的公開金鑰驗證該憑證申請檔的簽章，以證明個體擁有相對應的私密金鑰。

3.2.2 組織身分之鑑別

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

保證等級	組織身分鑑別之程序
第 1 級	無須識別申請者之身分是否為真實存在，且申請者提供的識別資訊均視為自我提供的識別資訊。 (1) 不做證件核對。 (2) 確認申請者擁有完全網域名稱之控制權即可申請憑證。 (3) 不需臨櫃辦理。
第 2 級	須識別申請者是實際存在的個體，並能連結到真實世界的真實身分。 (1) 不做證件核對。 (2) 不需臨櫃辦理。 (3) 提交組織資料例如組織識別碼(如扣繳單位稅籍統一編號)、組織名稱等，HiPKICA 有權與政府提供之

保證等級	組織身分鑑別之程序
	資料庫或可信賴之第三者資料庫的登記資料進行比對，以確認申請者之身分。
第 3 級	用戶組織身分鑑別方式可分為臨櫃辦理與非臨櫃辦理： (1) 臨櫃辦理，可採用下列方式(擇一)進行申請者身分鑑別： (a) 提供所在地管轄之政府機關(構)所核發之相關證明文件或公文書 (b) 由合格的政府資訊來源(Qualified Government Information Source, QGIS)如經濟部工商登記資料庫或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取得之公示資料 (c) 中華電信所屬組織以紙本表單申請憑證 (2) 非臨櫃辦理可採用下列方式(擇一)進行申請者身分鑑別，詳細作業程序於各註冊中心內控制度中制訂之： (a) 透過政府公開金鑰基礎建設或 ePKI 公開金鑰基礎建設所簽發之保證等級第 3 級組織憑證數位簽章申請 (b) 已依法向主管機關完成設立登記程序，同(1)之(a)或(b)，並郵寄相關證明文件申請 (c) 公證人、律師或會計師的認證文書(Attestation Letter) (d) 由憑證管理中心人員或所信賴的人員到點訪視確認 (e) 中華電信所屬組織以電子表單申請憑證。 憑證機構之組織身分鑑別方式： (1) 本公司自行設立之憑證機構的身分鑑別，由本公司召開政策管理委員會會議審核。

保證等級	組織身分鑑別之程序
	(2)非本公司自行設立之憑證機構，由憑證機構提交下屬憑證機構憑證申請書，由本公司召開政策管理委員會會議審核。
第 4 級	(1)本公司自行設立之憑證機構的身分鑑別，由本公司召開政策管理委員會會議審核。 (2)非本公司自行設立之憑證機構，由憑證機構提交交互認證憑證申請書，由本公司召開政策管理委員會會議審核。
組織驗證型 TLS 憑證	適用 Baseline Requirements 及本節針對保證等級第 3 級之規定。

3.2.3 個人身分之鑑別

不做規範。

3.2.4 未經驗證之用戶資訊

所有由用戶提供將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

當某個申請代表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，HiPKICA 或註冊中心應依照 Baseline Requirements 第 3.2.5 節之規定進行授權之確認(Validation of Authority)，以確認該申請代表人所提出之憑證請求的真實性。

3.2.6 互運之準則

HiPKICA 允許其他憑證機構提出互運申請，可參考本文件之規定。

3.2.7 網域控管權驗證(Validation of Domain Control)

HiPKICA 依照 Baseline Requirements 第 3.2.2.4 節之規定，執行允許之驗證流程與程序，以驗證申請者對網域名稱之擁有權或控制權。HiPKICA 必須依照以下方式擇一鑑別申請者具備網域名稱之擁有權或控制權。

3.2.7.1 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。此方法只可以用於：簽發憑證機構也是基礎網域名稱(Base Domain Name)的網域名稱受理註冊機構或網域名稱受理註冊機構之關係企業組織。例如中華電信公司是.tw 之網域名稱受理註冊機構，並負責營運 HiPKICA。

注意：一旦使用此方法驗證了某個完全吻合網域名稱，HiPKICA 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 TLS 憑證，此方法也適用於驗證萬用網域名稱(Wildcard Domain Names)。此方法符合 Baseline Requirements 第 3.2.2.4.12 節對網域名稱驗證之規定。

在簽發用戶憑證時，HiPKICA 不得依賴透過 HTTPS 網站取得之網域名稱聯絡人資訊(Domain Contact information)，無論該資訊先前取得時是否仍在允許之重複使用期限內。

HiPKICA 於取得所申請網域名稱之網域名稱聯絡人資訊時，應符合以下規定：

(1) 若使用 WHOIS 通訊協定(RFC 3912)，HiPKICA 必須查詢 IANA 之 WHOIS 伺服器，並依其回傳之轉介資訊(referrals)，連線至適當之 WHOIS 伺服器進行查詢。

(2)若使用註冊資料存取通訊協定(Registry Data Access Protocol, RDAP，RFC 7482)，HiPKICA 必須使用 IANA 所提供之 bootstrap 檔案，以識別並查詢該網域所對應之正確 RDAP 伺服器。

(3)為確保資訊為最新且正確，HiPKICA 不得依賴以下任一超過 48 小時之快取資料：

- WHOIS 伺服器資訊；
- IANA 提供之 RDAP bootstrap 資料。

3.2.7.2 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，確認申請者對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：
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。

(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，HiPKICA 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。

除 Onion 網域名稱外，HiPKICA 將依照第 3.2.10 節的規定實施多重視角簽發驗證機制(Multi-Perspective Issuance Corroboration, MPIC)。為了計算佐證數量，網路視角必須觀察與主網路視角相同的挑戰訊息(即隨機值或請求符記)。

注意：HiPKICA 不得對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憑證，除非 HiPKICA 使用授權方法對每個其他完全吻合網域名稱執行單獨的驗證。此方法不適用於驗證萬用網域名稱。此方法符合 Baseline Requirements 第 3.2.2.4.18 節對網域名稱驗證之規定。

3.2.7.3 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 CNAME、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，HiPKICA 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(參照 Baseline Requirements 第 4.2.1 節規定)。

同時，HiPKICA 將依照第 3.2.10 節的規定實施多重視角簽發驗證機制。為了計算佐證數量，網路視角必須觀察與主網路視角相同的挑戰訊息(即隨機值或請求符記)。

若 HiPKICA 或其附屬機構營運一個 DNS 區域，並允許申請者透

過 CNAME 將其以前置下底線字元為前綴之網域標籤(Domain Label)委派至該區域，則 HiPKICA 必須確保每一位申請者皆委派至該區域內唯一之完全吻合網域名稱。HiPKICA 或其附屬機構目前不營運此類服務。

注意：一旦使用此方法驗證了某個完全吻合網域名稱，HiPKICA 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 TLS 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 3.2.2.4.7 節對網域名稱驗證之規定。

3.2.7.4 由對特定網頁內容的約定變更-ACME

透過使用 RFC 8555 第 8.3 節中定義的自動憑證更新環境(Automated Certificate Management Environment, ACME) HTTP Challenge 方法，以確認申請者對該完全吻合網域名稱的控制權，此方法依照 Baseline Requirements 第 3.2.2.4.19 節及 RFC 8555 第 8.3 節的規定執行。

3.2.8 萬用網域驗證(Validation of Wildcard Domains)

如果憑證中任何萬用網域的 FQDN 部分是「註冊管理機構控制的」或「公共後綴(Public suffix)」（例如“.com”、“.co.uk”，請參閱 RFC 6454 第 8.2 節），HiPKICA 會進行額外的審查和檢查，以確保用戶對整個網域名空間擁有合法控制權。

如果使用公共後綴清單 (Public Suffix List)，HiPKICA 僅查閱「ICANN 網域(ICANN DOMAINS)」部分，而不是「私有網域(PRIVATE DOMAINS)」部分。

3.2.9 資料正確性

在使用任何資料來源作為可靠資料來源之前，HiPKICA 應評估

此來源的可靠性、正確性和對變更或偽造的抵抗性。HiPKICA 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 HiPKICA、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。

3.2.10 多重視角簽發驗證機制 (Multi-Perspective Issuance Corroboration)

自 2025 年 3 月 15 日起，HiPKICA 採用 Baseline Requirements 第 3.2.2.9 節「Multi-Perspective Issuance Corroboration」之規定實施網域授權或控管的驗證及 CAA record 檢查，多重視角簽發驗證機制可在憑證簽發之前從多個遠端網路視角輔助主網路視角做出驗證成功與否之決定(即網域驗證通過/失敗、CAA 許可/禁止)。

法定數量要求表(Quorum Requirements Table)

# of Distinct Remote Network Perspectives Used	**# of Allowed non-Corroborations**
2-5	1
6+	2

分階段實施表：

- **2025 年 3 月 15 日起**，HiPKICA 必須使用至少 2 個遠端網路視角進行多重視角簽發驗證。如果無法證實主網路視角所做決定的遠

端網路視角（「未證實」）的數量大於上述之法定數量要求表中所允許的數量，HiPKICA 可以繼續簽發憑證；

- **2025 年 9 月 15 日起**，HiPKICA 必須使用至少 2 個遠端網路視角進行多重視角簽發驗證。HiPKICA 必須確保符合上述之法定人數要求表中定義的要求，如果不符合要求，則 HiPKICA 不得繼續簽發憑證；
- **2026 年 3 月 15 日起**，HiPKICA 必須使用至少 3 個遠端網路視角進行多重視角簽發驗證。HiPKICA 必須確保符合上述之法定人數要求表中定義的要求，並且協助主網路視角進行驗證的遠端網路視角位於至少 2 個不同的區域網際網路註冊管理機構(Regional Internet Registries)的服務區域內。如果不符合要求，則 HiPKICA 不得繼續簽發憑證；
- **2026 年 6 月 15 日起**，HiPKICA 必須使用至少 4 個遠端網路視角進行多重視角簽發驗證。HiPKICA 必須確保符合上述之法定人數要求表中定義的要求，並且協助主網路視角進行驗證的遠端網路視角位於至少 2 個不同的區域網際網路註冊管理機構(Regional Internet Registries)的服務區域內。如果不符合要求，則 HiPKICA 不得繼續簽發憑證；
- **2026 年 12 月 15 日起**，HiPKICA 必須使用至少 5 個遠端網路視角進行多重視角簽發驗證。HiPKICA 必須確保符合上述之法定人數要求表中定義的要求，並且協助主網路視角進行驗證的遠端網路視角位於至少 2 個不同的區域網際網路註冊管理機構(Regional Internet Registries)的服務區域內。如果不符合要求，則 HiPKICA 不得繼續簽發憑證。

3.3 金鑰更換請求之識別與鑑別

3.3.1 例行性金鑰更換之識別與鑑別

當用戶或憑證機構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。用戶的身分可使用現行的簽章金鑰進行鑑別或依照第 3.2 節初始註冊之鑑別程序進行鑑別。TLS 憑證例行性金鑰更換之識別及鑑別依照 Baseline Requirements 規定辦理。

3.3.2 憑證廢止後金鑰更換之識別與鑑別

用戶或憑證機構之憑證廢止後，應辦理新憑證之申請，並依照第 3.2 節規定重新辦理初始身分驗證。

3.4 憑證廢止請求之識別與鑑別

HiPKICA 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 節規定相同。

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

申請者或被授權代表申請者申請的個人均可提出憑證之申請。

4.1.2 註冊程序與責任

憑證申請步驟如下：

- 使用合適的安全平台產製合適的金鑰對
- 使用適當的工具產製 PKCS#10 憑證請求檔(Certificate Signing Request, CSR)。
- 填寫憑證申請資料並同意用戶約定條款。
- 送交憑證申請資料(內容包含憑證請求檔、欲申請之憑證類型、組織之法定名稱或網站之完全吻合網域名稱等)並提供相關證明資料給註冊中心，憑證申請資料可為電子之形式。

註冊中心收到憑證申請後負責驗證該憑證請求之真實性與執行憑證申請者之身分識別與鑑別，確認後將該請求遞交給簽發憑證機構進行憑證簽發。

4.2 憑證申請之程序

4.2.1 執行識別與鑑別

收到憑證請求後，HiPKICA 及註冊中心應依照第 3.2 節之規定驗證申請資料。憑證請求可能包含申請者將記載於憑證中的所有真實資訊，以及必要時 HiPKICA 或註冊中心可要求申請者額外提供之其他資訊。憑證主體身份資訊(Subject Identity Information)驗證資料的重複

使用期限於 2025 年 7 月 31 日前簽發的 OV TLS 憑證允許使用 825 天內的驗證資料，2025 年 8 月 1 日(含)以後簽發的 OV TLS 憑證只允許使用 398 天內的驗證資料。由憑證申請者提供之資訊及於申請過程中之聯繫紀錄由 HiPKICA 與註冊中心依本文件之規定以安全也可被稽核之方式妥善保管。

針對 TLS 憑證，註冊中心系統設有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，且註冊中心針對高風險憑證請求在憑證核准簽發前會執行額外之檢查，以確保此類請求已依 Baseline Requirements 要求進行適當驗證。

HiPKICA 對於即將簽發的 TLS 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)會依據 RFC 8659 及 Baseline Requirements 第 3.2.2.8 節之規定檢查網域名稱系統(Domain Name System, DNS)中是否存在 CAA 紀錄。憑證若需簽發，則憑證請求所包含的每一個完全吻合網域名稱的 CAA 查詢紀錄不應超過「8 小時或 CAA 紀錄 TTL (Time to Live)值」兩者之最大值。

HiPKICA 支援“issue”CAA 標籤並記錄所有針對 CAA 紀錄採取的操作。若 CAA 紀錄存在但並沒有記載“pki.hinet.net”或“tls.hinet.net”為 CAA 之簽發者網域名稱，HiPKICA 將不會對該網域名稱簽發憑證。HiPKICA 不會寄送簽發請求的報告給 CAA 紀錄之“iodef”屬性標籤中所註記的聯絡資訊。

HiPKICA 依照 RFC 8657 規範處理 accounturi 與 validationmethods 參數，且支援 insensitive validationmethods labels。

4.2.2 憑證申請之批准或拒絕

HiPKICA 將不會簽發包含內部名稱或保留 IP 位址的 TLS 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 3.2.7 節。

自 2026 年 3 月 15 日起，HiPKICA 不得簽發包含以 IP 反向區域後綴(IP Reverse Zone Suffix)為結尾之網域名稱的憑證。

如果憑證申請之驗證在遵循本文件下可以成功完成，HiPKICA 可以批准憑證之申請並簽發憑證。若各項驗證工作無法成功完成，HiPKICA 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，HiPKICA 得因其他原因不同意簽發憑證。HiPKICA 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。

憑證機構提出下屬憑證機構或交互認證憑證申請時，將召開政策管理委員會會議審查提供之相關文件資料，以評估該憑證機構成為下屬或交互憑證機構之妥適性。再依政策管理委員會之決議，決定進入下一階段，或要求補送資料，或駁回申請。

4.2.3 處理憑證申請之時間

HiPKICA 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本文件及各項查核要求下，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群組與類別，可能於用戶約定條款、契約或註冊中心網站揭露。

憑證申請件在收件後會由憑證註冊窗口人員完成審核程序，並請申請者進行憑證接受，並由簽發憑證機構完成憑證簽發之作業，完成憑證簽發之時間依下表之憑證類別進行說明：

憑證類別	處理與簽發所需時間
OV TLS 憑證	2 個工作天

簽發時間在很大程度上取決於申請者何時提供完成驗證所需的詳細資訊和文件或完成憑證接受。處理憑證申請之時間亦可記載於用戶約定條款或與憑證申請者之契約。

4.3 憑證簽發

4.3.1 憑證簽發時憑證機構之作業

HiPKICA 在接到憑證申請資料後，即依本文件第 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簽發憑證機構。

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

(3) 若註冊中心被授權之保證等級與範圍與憑證申請不符時，簽發憑證機構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，應主動聯絡簽發憑證機構，確實瞭解問題之所在。

(4) 簽發TLS憑證之憑證機構，其憑證簽發程式具有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) 為確保簽發憑證機構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(Transport Layer Security, TLS)協定加密傳送。

HiPKICA 簽發交互憑證時，應在 basicConstraints 擴充欄位中明確標示憑證路徑長度限制(Path Length Constraint)，以確保憑證互運路徑是被允許的，憑證路徑長度限制的設定值，則視被允許的憑證互運路徑長度做設定。

4.3.2 對用戶之憑證簽發通知

HiPKICA 完成憑證簽發後，將透過電子郵件或其他等效方法通知用戶，該電子郵件可能包含憑證本身或下載連結，具體取決於所請求憑證之工作流程。

4.4 憑證接受

4.4.1 構成接受憑證之要件

如果憑證簽發後 30 天內申請者未申請廢止憑證，則該憑證被視為已被接受。接受憑證視為憑證申請者同意遵守本文件或相關合約上之權利與義務。

4.4.2 憑證機構對簽發憑證之發布

CA 憑證會公布於 HiPIKCA 之儲存庫中。用戶憑證的發布係藉由將憑證傳遞給憑證申請者來達成。

4.4.3 憑證機構對其他個體之簽發通知

HiPKICA 之根憑證機構若有新簽發的自簽憑證，將會依照各作業系統、瀏覽器與軟體平台之根憑證計畫規定提出申請植入自簽憑證於憑證機構信賴清單。

4.5 金鑰對與憑證之用途

4.5.1 用戶私密金鑰與憑證之用途

用戶金鑰對之產製應符合第 6.1.1 節之規定，且用戶須擁有私密金鑰之控制權，該私密金鑰不得用於簽發憑證。

用戶應保護私密金鑰不被未經授權之他人使用或揭露，且確保私密金鑰依憑證擴充欄位所註記之金鑰用途使用。用戶須依本文件與用戶約定條款之規定使用憑證。

4.5.2 信賴憑證者公開金鑰與憑證之用途

信賴憑證者使用憑證時，應確認憑證用途，並依本文件規定使用。信賴憑證者應使用符合其用途且滿足 ITU-T X.509、IETF RFCs 或 Baseline Requirements 等國際標準或規範之工具或方法。

信賴憑證者選用之工具或方法須於使用憑證前，驗證憑證路徑中所有憑證之欄位內容正確性、簽章完整性以及憑證狀態有效性。其中，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。待憑證驗證完成後，始可使用憑證路徑中之 TLS 憑證識別該網際網路伺服器所使用之網域名稱及其擁有者身分，並建立與該伺服器間之安全通訊管道。

信賴憑證者亦應檢驗簽發憑證機構憑證與 TLS 憑證之憑證政策擴充欄位，以確認憑證之保證等級。

4.6 憑證展期

HiPKICA 不允許憑證展期。

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要件

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

下屬/交互認證憑證機構在以下兩種情形會更換金鑰並由根憑證機構簽發新的下屬/交互認證憑證機構憑證：

(1) 目前使用之金鑰生命週期結束。

(2) 目前使用之金鑰的安全性有問題時(例如懷疑或確定金鑰被破解)。

憑證效期尚未過期之用戶可請求金鑰更換，HiPKICA 並應依照第 3.3.1 節的規定對其進行識別與鑑別。進行過金鑰更換後，HiPKICA 可能會廢止其舊憑證，且不允許舊憑證之變更或金鑰更換。

4.7.2 更換憑證金鑰之申請者

憑證用戶之主體或經授權之代表人。

4.7.3 憑證金鑰更換之程序

憑證用戶請求金鑰更換，HiPKICA 應依照本文件第 3.1、3.2、3.3、4.1 及 4.2 節之規定辦理，並且可能會根據任何先前驗證過的資料來重新驗證憑證用戶。

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 構成接受金鑰更換後之憑證的要件

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

不做規定。

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 張新的憑證其鑑別資訊和舊的憑證有些許不同(例如更新憑證中註記之完全吻合網域名稱或其他屬性資訊)，新的憑證有新的憑證序號，但新憑證和舊憑證的公開金鑰及到期日相同。憑證變更後，舊憑證應予以廢止。

4.8.2 憑證變更之申請者

憑證用戶之主體或經授權之代表人。

4.8.3 憑證變更之程序

(1) 憑證變更的申請程序如第 4.2 節之規定。

(2) 用戶如有變更組織名稱等重要的資料時,則原憑證必須廢止,用戶須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。

4.8.4 對用戶憑證變更之簽發通知

用戶憑證簽發通知依照第 4.3.2 節規定辦理。

4.8.5 構成接受變更之憑證的要件

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

不做規定。

4.9 憑證廢止與暫時停用

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

4.9.1 廢止憑證之情況

4.9.1.1 廢除用戶憑證之情況

以下幾種情況發生時，憑證機構應於 24 小時內廢止憑證：

(1)用戶以書面提交憑證機構同意廢止憑證

(2) 用戶告知憑證機構原有之憑證請求未經授權，且不追溯授予授權

(3) 憑證機構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破解用戶的私鑰

(5) 憑證機構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，憑證機構應於合理的時間範圍內(快則 24 小時內，最遲於 5 個工作天內)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) 憑證機構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註冊商之間的授權或合約到期)

(5) 萬用網域憑證被用於詐欺或釣魚網站用途

(6) 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)

(7) 憑證未依憑證機構之本文件之規定程序簽發時

(8) 憑證中所記載之資訊不正確(inaccurate)

(9) 憑證機構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

(10) 本文件所規定應廢止項目

(11) 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

4.9.1.2 廢除下屬憑證機構憑證之情況

以下幾種情況發生時，根憑證機構應於 7 個工作天內廢止下屬憑證機構之憑證：

(1) 下屬憑證機構以書面提交廢止憑證申請

(2) 下屬憑證機構告知憑證機構原有之憑證請求未經授權，且不追溯授予授權

(3) 憑證機構證實下屬憑證機構之私密金鑰遭破解或違反第 6.1.5 及第 6.1.6 節對於金鑰之長度及品質檢測之規定，且該私密金鑰與下屬憑證機構憑證中所記載之公開金鑰成配對關係

(4) 憑證機構證實下屬憑證機構憑證遭到誤用

(5) 憑證未依本文件之規定程序簽發時

(6) 憑證中所記載之資訊不正確(inaccurate)或已變更

(7) 憑證機構終止營運，且未安排其他憑證機構承接以提供憑證廢止服務

(8) 憑證機構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) 本文件所規定應廢止項目

憑證機構依照上述應廢止憑證之情況，得逕行廢止用戶、下屬憑證機構或交互認證憑證機構之憑證。

4.9.2 憑證廢止之申請者

用戶或合法授權之第三人，如司法或檢調機關、用戶或下屬憑證機構授權之代表人、自然人之法定繼承人等。

此外，用戶、信賴憑證者、應用軟體廠商或其他第三方可提交憑證問題報告(Certificate Problem Reports)知會 HiPKICA 合理之原因以廢止憑證。HiPKICA 接收到憑證問題報告後，將依第 4.9.5 節之規定，確認憑證廢止請求是否成立。

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訂之作業規範提出憑證廢止請求，註冊中心在接到憑證廢止請求後，即進行相關的審核程序，並保留所有憑證廢止請求紀錄，包含申請者名稱、聯絡資料、廢止原因、廢止時間與日期等，以作為後續權責歸屬之依據。

(2) 註冊中心完成審核作業後，將憑證廢止申請傳送至簽發憑證機構。

(3) 簽發憑證機構接獲註冊中心送來之憑證廢止申請資料時，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廢止請求廢止該憑證。

(4) 如以上之查驗不通過時，簽發憑證機構將回傳相關錯誤信息給註冊中心；若註冊中心有任何疑問，應主動聯絡簽發憑證機構，確實瞭解問題之所在。

(5) 為確保簽發憑證機構與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廢止申請資料，係經數位簽章及傳輸層安全(Transport Layer Security, TLS)協定加密傳送。

(6) 簽發憑證機構使用與簽發憑證時相同的憑證機構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) HiPKICA 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第 4.9.3.1 節所述。

4.9.3.1 憑證問題回應機制

HiPKICA 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，供用戶、應用軟體廠商、信賴憑證者以及其他第三方組織於發現疑似私密金鑰遭破解、憑證被誤用、或是憑證被偽造、破解、濫用或不當使用等情形時，可透過第 1.5.2.2 節之聯絡資訊向 HiPKICA 提出憑證問題報告。

4.9.4 憑證廢止請求之寬限期

憑證廢止請求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。用戶在其私密金鑰遺失或疑似遭破解時，應儘速向註冊中心提出憑證廢止之申請，憑證廢止請求之寬限期為 2 個工作天，HiPKICA 必要時得逐案延展其憑證廢止之寬限期。

HiPKICA 之憑證機構或註冊中心如發生第 4.9.1 節之情形，最遲應於 10 個工作天內提出憑證廢止申請。

4.9.5 憑證機構處理憑證廢止請求之處理期限

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，並提供一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，HiPKICA 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

使用憑證前，信賴憑證者須透過 HiPKICA 提供之憑證廢止清冊或選擇性提供之線上憑證狀態協定查詢服務確認憑證路徑中所有憑證之狀態。信賴憑證者須考量風險、責任及影響，自行決定擷取憑證廢止資訊之時間或頻率。

4.9.7 憑證廢止清冊之簽發頻率

HiPKICA 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，HiPKICA 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 HiPKICA 之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

除根憑證機構有預簽行為外，其餘憑證機構產製憑證廢止清冊後立即發布。

4.9.9 線上憑證廢止與狀態查驗之可用性

HiPKICA 透過憑證廢止清冊與網頁式之憑證查詢/下載等方式，提供憑證廢止與狀態查詢服務，並依簽發憑證機構所提供之服務項目，

選擇性提供線上憑證狀態協定查詢服務。

若簽發憑證機構提供線上憑證狀態查詢服務，其線上憑證狀態協定回應伺服器(Online Certificate Status Protocol Responder, OCSP Responder)應負責提供符合 RFC 6960 與/或 RFC 5019 標準規範之線上憑證狀態協定回應訊息，並使用金鑰長度至少為 2048 位元且可被 8 整除之 RSA 金鑰以及安全強度相當或優於 SHA-256 之雜湊函數演算法簽發前述回應訊息，同時提供簽發憑證機構所簽發之線上憑證狀態協定回應伺服器憑證，該回應伺服器憑證包含符合 RFC 6960 規範之擴充欄位「id-pkix-ocsp-nocheck」。

4.9.10 線上憑證廢止查驗之規定

信賴憑證者於使用憑證前須依第 4.9.6 節之規定確認憑證有效性。

若 HiPKICA 提供線上憑證狀態協定查詢服務，則其應支援符合 RFC 6960 與/或 RFC 5019 標準規範所述之 HTTP-based 的 POST 與 GET 方法，且其所回應之憑證狀態資訊應符合下述規定：

(1) TLS 憑證或其對應之預簽憑證(Precertificate)：最遲於該憑證發布後的 15 分鐘內提供對應的線上憑證狀態協定回應訊息，其應於每次「下次更新時間(nextUpdate)」之前的效期一半時間內進行更新；每次簽發之線上憑證狀態協定回應訊息效期至少 8 小時，最長不超過 16 小時；

(2) 自發憑證、下屬憑證機構憑證及交互憑證：至少每 12 個月更新 1 次憑證狀態資訊；若憑證被廢止，則於該憑證廢止後 24 小時內更新憑證狀態資訊。

線上憑證狀態協定查詢封包內含之憑證序號可分為兩種，分別為：

(1) 已分配：簽發憑證機構已簽發憑證之憑證序號，或簽發憑證機構簽發 TLS 憑證所需之預簽憑證的憑證序號；

(2) 未分配：不符合前述條件之憑證序號。

若線上憑證狀態協定回應伺服器收到內含「未分配」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「良好(Good)」。

4.9.11 廢止公告之其他發布形式

為了加速高流量網站的 TLS 憑證之驗證，以完成即時線上 TLS 憑證狀態之驗證作業，HiPKICA 根據 RFC 4366 支援線上憑證狀態協定裝訂(OCSP Stapling)，並透過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 金鑰遭破解時之特殊規定

如果用戶確認私密金鑰遭破解，用戶必須立即通知 HiPKICA 依照本文件第 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。

如果憑證機構確認私密金鑰遭破解，根憑證機構將發布憑證廢止清冊，以向軟體供應商、用戶及信賴憑證者通報私鑰洩露事件。

第三方提交私密金鑰遭破解的證據可接受的方式為：

(1) 由 HiPKICA 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；或

(2) 提交該私密金鑰

4.9.13 憑證暫時停用之情況

HiPKICA 不提供憑證機構憑證與 TLS 憑證之暫時停用與恢復使用服務。

4.9.14 憑證暫時停用之申請者

不適用。

4.9.15 憑證暫時停用之程序

不適用。

4.9.16 憑證暫時停用期間之限制

不適用。

4.9.17 恢復使用憑證之程序

不適用。

4.10 憑證狀態服務

4.10.1 服務特性

HiPKICA 提供憑證廢止清冊，並依簽發憑證機構所提供之服務項目，選擇性提供線上憑證狀態協定查詢服務；其中，憑證廢止清冊或線上憑證狀態協定回應訊息中所註記之憑證廢止資訊，須至該被廢止之憑證已過期後始可移除。

4.10.2 服務可用性

於正常運作情況下，HiPKICA 所提供之憑證廢止清冊下載服務與選擇性提供之線上憑證狀態協定查詢服務，其回應時間均應不超過 10 秒。

HiPKICA 提供全天候(7 x 24)不中斷之儲存庫系統，供應用軟體檢查所有未過期憑證之最新狀態。

HiPKICA 提供全天候(7 x 24)回應機制處理高優先權之憑證問題報告；HiPKICA 可視案件情況向執法當局舉發，並得逕行廢止發生問題之憑證。

4.10.3 可選功能

不做規定。

4.11 訂購終止

訂購終止(End of Subscription)是指用戶之憑證被廢止、到期而不做更新或是用戶約定條款失效而終止。

4.12 私密金鑰託管與回復

4.12.1 金鑰託管與回復之政策與實務

HiPKICA 之私密金鑰不可被託管(Escrowed)。

4.12.2 會議金鑰封裝與回復之政策與實務

HiPKICA 不支援會議金鑰(Session Key)封裝及回復(Encapsulation and Recovery)。

5 憑證機構設施、管理及操作控管

5.1 實體控管

5.1.1 所在位置與結構

HiPKICA 機房位於中華電信資訊技術分公司，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 HiPKICA 之相關設備。

5.1.2 實體存取

HiPKICA 建置採適當之措施管制連接提供 HiPKICA 服務的硬體、軟體和硬體密碼模組。

HiPKICA 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 HiPKICA 系統的惡意軟體。

非 HiPKICA 人員進出機房，須填寫進出紀錄，並由 HiPKICA 相關人員全程陪同。

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

(1)確認設備是否正常運作。

(2)確認機箱門是否關閉。

(3)確認門禁系統是否正常運作。

5.1.3 電源與空調

HiPKICA 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)及不斷電系統(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。

HiPKICA 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

HiPKICA 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 火災防範與保護

HiPKICA 機房具備自動偵測火災預警功能，系統可自動啟動滅火設備，並設置手動開關於各主要出入口處，以供現場人員於緊急情況時以手動方式啟動。

5.1.6 媒體儲存

記錄稽核、歸檔及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 份在異地備援場所。

5.1.7 廢料處理

第 9.3.1 節所記載 HiPKICA 的文件資料在不需使用時，都要經碎紙機處理。任何 HiPKICA 使用過之儲存媒體，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 HiPKICA 機房距離 50 公里以上，備援的內容包括資料與系統程式。

5.2 程序控管

HiPKICA 經由作業程序控管(procedural controls)，以規定執行系統相關作業的各個可信賴角色(trusted role)、每個工作的人員需求數及每個角色的識別與鑑別，以確保系統作業程序的安全。

5.2.1 信賴角色

HiPKICA 為使執行系統相關作業的責任能做適當的區隔分派，以防止某人惡意使用 HiPKICA 系統而不被察覺，對於每項系統存取作業，明確規定那些信賴角色才能執行此項作業。

HiPKICA 指派 7 個不同的 PKI 人員角色，分別為管理員(Administrator)、簽發員(CA Officer)、稽核員(Internal Auditor)、維運員(System Operator)、實體安全控管員(Physical Security Controller)、網路安全專員(Cyber Security Coordinator)和防毒防駭專員(Anti-virus and Anti-hacking Coordinator)，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 7 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 HiPKICA 系統。
- 建立和維護系統之使用者帳號。
- 產製和備份 HiPKICA 之金鑰。
- 啟動/停止憑證管理者相關金鑰。
- 系統軟硬體的更新。
- 系統的備援及復原作業
- 網站的維護。
- 系統之弱點修補作業。

簽發員主要負責：

- 產製和備份 HiPKICA 之金鑰。
- 啟動/停止憑證簽發相關金鑰。
- 啟動/停止憑證廢止相關金鑰。
- 啟動/停止憑證廢止清冊簽發相關金鑰。

稽核員主要負責：

- 產製和備份 HiPKICA 之金鑰。
- 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 HiPKICA 維運是否遵照本文件的規定。
- 稽核主機系統病毒碼與弱點之修補作業。

維運員主要負責：

- 對稽核紀錄的歸檔。
- 系統設備的日常運作維護。
- 儲存媒體的更新。
- 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。
- HiPKICA 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。

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

  需要至少 3 位合格的人員來擔任。

- 簽發員

  需要至少 3 位合格的人員來擔任。

- 稽核員

  需要有 2 位合格的人員來擔任。

- 維運員

  需要至少 2 位合格的人員來擔任。

■ 實體安全控管員

需要至少 2 位合格的人員來擔任。

■ 網路安全專員

需要至少 1 位合格人員擔任。

■ 防毒防駭專員

需要至少 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 HiPKICA 系統	2				1		
建立和維護系統之使用者帳號	1				1		
產製和備份 HiPKICA 之金鑰	2	2	1		1		
啟動/停止憑證簽發、憑證廢止及簽發憑證廢止清冊相關金鑰	2	2			1		
對稽核紀錄的查驗、維護和歸檔			1	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 HiPKICA 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	

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
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(稽核主機)	1		1	1	1		
系統病毒碼與弱點之修補作業(稽核主機以外系統)	1			1	1		

5.2.3 識別與鑑別每個角色

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。

HiPKICA 利用使用者帳號、通行碼和群組之系統帳號管理功能及 IC 卡，識別及鑑別管理員、簽發員、稽核員及維運員等不同角色，並利用中央門禁系統之權限設定功能，識別及鑑別實體安全控管員。

HiPKICA 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

HiPKICA 角色分依照第 5.2.1 節定義的 7 種信賴角色，對人員及角色分配必須符合以下規定：

- 管理員、簽發員、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。
- 任何 1 種信賴角色均不允許執行自我稽核功能。

5.3 人員控管

5.3.1 適任條件與經歷

(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：

- 個人性格之評估。
- 申請者經歷之評估。
- 學術及專業能力及資格之評估。
- 人員身分之確認。
- 人員操守之評估。

(2) 人員之考核管理

HiPKICA 之相關人員在初任時先進行資格審查，以確認其具可信度及工作能力。正式進用後，必須接受適當之教育訓練，並以書面方式簽訂應負之責任，同時每年進行資格複查，如無法通過資格複查則調離現職，改派其他符合資格人選擔任。

(3) 人員之任免遷調管理

如人員之進用、約聘僱條件或契約有所變更，特別是人員離職或約聘僱契約終止時，將遵守維護機密責任之約定。

(4) 機密維護之責任約定

HiPKICA 之相關人員均負維護機密之責任，並簽署維護營業秘密契約書，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

HiPKICA 對於第 5.2.1 節所述之各信賴角色人員，在初任時予以資格審查，以確認其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) HiPKICA 安全認證機制。 (2) HiPKICA 系統安裝、設定及維護之操作程序。 (3) HiPKICA 系統軟硬體的使用與操作程序。 (4) 建立與維護系統用戶帳號之操作程序。 (5) 設定稽核參數操作程序。 (6) 產製和備份 HiPKICA 之金鑰操作程序。 (7) 災後復原以及業務永續經營之程序。
簽發員	(1) HiPKICA 安全認證機制。 (2) 產製和備份 HiPKICA 之金鑰操作程序。 (3) 啟動/停止憑證簽發之操作程序。 (4) 啟動/停止憑證廢止之操作程序。 (5) 啟動/停止憑證廢止清冊簽發服務之操作程序。 (6) 災後復原與業務永續經營之程序。
稽核員	(1) HiPKICA 安全認證機制。 (2) HiPKICA 稽核系統的使用及操作程序。 (3) 產製與備份 HiPKICA 金鑰之操作程序。 (4) 對稽核紀錄的查驗、維護及歸檔程序。 (5) 災後復原及業務永續經營之程序。
維運員	(1) 系統設備日常運作之維護程序。 (2) 儲存媒體之更新程序。 (3) 災後復原以及業務永續經營之程序。 (4) 網路與網站的維護程序。
實體安全控管員	(1) 設定實體門禁權限程序。 (2) 災後復原以及業務永續經營之程序。

角色	教育訓練規定
網路安全專員	(1) 網路與網路設備的維護程序。 (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。 (2) 作業系統與網路之安全機制。

5.3.4 人員再教育訓練之頻率與規定

在 HiPKICA 之軟硬體升級、工作程序改變、設備更換或相關法規改變時，將安排相關人員再教育訓練並記錄受訓情形，以確實瞭解相關作業程序及法規之改變。

5.3.5 工作輪調之頻率與順序

(1) 不得互兼的角色，不可工作調換。

(2) 擔任維運員、網路安全專員或防毒防駭專員滿 2 年，且已接受相關教育訓練及通過審核，可轉任管理員、簽發員、稽核員等工作。

5.3.6 未授權行為之裁罰

HiPKICA 之相關人員，如違反本文件或其他 HiPKICA 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 提供給人員之文件

HiPKICA 提供本文件、HiPKICA 系統操作手冊等文件給 HiPKICA 之相關人員。

5.4 稽核紀錄程序

所有 HiPKICA 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，並遵循第 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

- 憑證機構產製金鑰時。

(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 HiPKICA 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。
- 違反本文件。
- 重設系統時鐘。

5.4.2 紀錄檔處理頻率

HiPKICA 定期檢視稽核紀錄以阻止可能之惡意活動，且對任何重大操作應進一步檢視。檢視工作包括驗證稽核紀錄是否被竄改、檢視所有的紀錄項目及檢查任何警示或異常等，稽核檢視之結果以文件記錄。

5.4.3 稽核紀錄檔保留期限

稽核資料現場保留兩個月，並依第 5.4.4 節、第 5.4.5 節、第 5.4.6 節及第 5.5 節記錄保留管理機制等相關規定辦理。

如稽核紀錄檔的保留期限屆滿，由稽核員負責移除資料，不可由其他人員代理。

5.4.4 稽核紀錄檔之保護

使用簽章、加密技術保存目前與已歸檔之稽核紀錄，並使用 CD-R 或其他無法更改稽核紀錄的媒體儲存，只有授權者才可調閱。

HiPKICA 之稽核系統具有資源控管與身分識別安全機制，由經授權之稽核員執行備份(Backup)及記錄檢視存取，並留存存取稽核紀錄的紀錄檔，以偵測與防止不當的存取與竄改。

5.4.5 稽核紀錄檔備份程序

(1) HiPKICA 週期性的將稽核紀錄歸檔，電子式稽核紀錄至少每月備份 1 次。

(2) 儲存稽核紀錄之媒體至少一份存放至具有妥善安全管控措施的異地儲存場所。

5.4.6 稽核彙整系統

稽核紀錄彙整系統內建於 HiPKICA 之系統，稽核程序於 HiPKICA 系統啟動時啟用。

自動稽核系統如無法正常運作，同時保護系統資料之完整性、機密性的安全機制處於高風險狀態時，HiPKICA 將暫停憑證簽發服務，直到問題解決後再行提供服務。

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

簽發 TLS 憑證之憑證機構遵照 WebTrust Principles and Criteria for Certification Authorities –Network Security 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。HiPKI OV TLS CA 於認定網路或系統之重大變更，應執行弱點評估，HiPKI OV TLS CA 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。HiPKICA 於滲透測試與弱點評估後進行補強與矯正措施。HiPKICA 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

HiPKICA 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) HiPKICA 本身金鑰對產製、儲存、存取、備援及更換等之重要追蹤紀錄。

(2) 憑證申請、簽發、廢止及重發等之重要追蹤紀錄。

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

5.5.1 歸檔紀錄之種類

HiPKICA 記錄的歸檔資料有：

(1) HiPKICA 被主管機關認證的(Accreditation)資料

(2) 憑證實務作業基準

(3) 重要的契約

(4) 系統與設備組態設定

(5) 系統或組態設定的修改與更新的內容

(6) 憑證申請的資料

(7) 廢止申請的資料

(8) 如第 3.2 節所訂定的用戶身分識別資料

(9) 已簽發或公告的憑證

(10)HiPKICA 金鑰更換的紀錄

(11)已簽發或公告的憑證廢止清冊

(12)所有的稽核紀錄

(13)用來驗證及佐證歸檔內容的其它資料或應用程式

(14)稽核人員所要求的文件

5.5.2 歸檔資料保留期限

HiPKICA 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將維護至所有歸檔資料都不保留後。

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HiPKICA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

HiPKICA 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 HiPKICA 所授權之人員定期整理歸檔。

5.5.5 紀錄之時戳規定

HiPKICA 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 取得與驗證歸檔資料之程序

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

在驗證歸檔資訊時，由稽核員進行驗證的程序，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

HiPKICA 之私密金鑰依照第 6.3.2 節規定定期更換，最遲應於其私密金鑰簽發用戶憑證用途的使用期限到期前，更換用來簽發憑證的金鑰對。下屬憑證機構更換金鑰對後，以新金鑰對向本公司根憑證憑證機構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。根憑證憑證機構更換金鑰對後，應以新私密金鑰簽發 1 張新的自簽憑證及使用新舊私密金鑰相互簽發 1 張新自發憑證。新簽發的自簽憑證依照第 6.1.4 節規定傳送給信賴憑證者，自發憑證公布在儲存庫供信賴憑證者下載。

HiPKICA 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 HiPKICA 本身的憑證被廢止後，其私密金鑰應停止使用，並須更換金鑰對。

5.7 遭破解與災變時之復原

5.7.1 緊急事件與系統遭破解之處理程序

5.7.1.1 事件應變與災難復原計劃

HiPKICA 制定緊急事件與系統遭破解之通報及處理程序，並每年進行演練。

5.7.1.2 大批廢止計畫

HiPKICA 依據 Baseline Requirements 第 5.7.1.2 節之規定，制定並維護一套全面且可實施之憑證大批廢止事件應對計畫。 HiPKICA 每年辦理憑證大批廢止演練，並將演練所得經驗納入前述計畫，以持續提升其應對憑證大批廢止事件之整備能力。

5.7.2 電腦資源、軟體或資料遭破壞

HiPKICA 訂定電腦資源、軟體及資料遭破壞之復原程序，同時每年進行演練。

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

5.7.3 憑證機構私密金鑰遭破解之處理程序

如 HiPKICA 簽章金鑰遭破解，採取以下處理程序：

(1) 公告於儲存庫，通知用戶及信賴憑證者

(2) 廢止 HiPKICA 簽章金鑰憑證及所簽發之用戶憑證。

(3) 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。

HiPKICA 每年至少進行 1 次憑證機構簽章金鑰遭破解之演練。

5.7.4 災變後業務持續營運措施

HiPKICA 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 HiPKICA 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服務

HiPKICA 終止服務時，應依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，HiPKICA 應遵守以下事項：

(1) HiPKICA 於預定終止服務 30 天前，於官網公告並通知用戶；

(2) HiPKICA 終止服務時將採如下措施：

- 對終止當時仍具效力之憑證，安排其他憑證機構承接此業務。並將終止服務及由其他憑證機構承接其業務之事實公告於儲存庫及通知仍具效力之憑證用戶。但無法通知者，不在此限。
- 將所有營業期間之紀錄檔案，移交給承接此業務之其他憑證機構。
- 若無憑證機構願承接 HiPKICA 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，HiPKICA 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，並通知憑證之所有人。HiPKICA 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 HiPKICA 停止其審驗憑證之權利。

6 技術安全控管

6.1 金鑰對產製與安裝

6.1.1 金鑰對之產製

HiPKICA 依照第 6.2.2 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。

HiPKICA 之金鑰產製由相關人員見證及錄影留存，並簽署金鑰啟用見證書(其中記載產製的金鑰對之公開金鑰)，相關人員應包含管理委員會之委員或合格稽核業者(Qualified Auditor)。

6.1.2 將私密金鑰傳送給憑證用戶

HiPKICA 不代用戶產製 TLS/SSL 或下屬憑證機構憑證金鑰對。

6.1.3 將用戶之公開金鑰傳送給憑證機構

用戶自行產製金鑰對時，則用戶必須以 PKCS# 10 憑證申請檔的格式將公開金鑰送給註冊中心，註冊中心依照第 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(Transport Layer Security, TLS)協定或其他相同或更高級之資料加密傳送方式。

6.1.4 將憑證機構之公開金鑰傳送給信賴憑證者

HiPKICA 鼓勵商業瀏覽器或作業系統平台將 HiPKICA 根憑證機構公開金鑰嵌入到它們的根憑證儲存庫與作業系統中。簽發憑證機構於遞交用戶憑證時，會以含有相關憑證機構公開金鑰憑證之憑證串鏈方式交付。信賴憑證者也可透過由 HiPKICA 營運之儲存庫下載相關憑證機構之公開金鑰憑證。除根憑證機構外，HiPKICA 透過已簽發憑

證之憑證機構資訊存取(Authority Information Access, AIA)欄位註記憑證串鏈中之相關公開金鑰憑證下載位置。

6.1.5 金鑰長度

HiPKICA 所使用之金鑰長度說明如下：

(1) 根憑證機構使用金鑰長度為 4096 位元之 RSA 金鑰或符合 NIST P-384 之 ECDSA 金鑰，簽發憑證所需之雜湊函數演算法依其金鑰而定，說明如下：

- RSA 金鑰：SHA-256、SHA-384 或 SHA-512；
- ECDSA 金鑰：使用之橢圓曲線-雜湊對為 P-384 with SHA-384。

(2) 下屬憑證機構與交互認證憑證機構使用金鑰長度為 4096 位元之 RSA 金鑰或符合 NIST P-256/P-384 之 ECDSA 金鑰，簽發憑證所需之雜湊函數演算法依其金鑰而定，說明如下：

- RSA 金鑰：SHA-256、SHA-384 或 SHA-512；
- ECDSA 金鑰：使用之橢圓曲線-雜湊對可為 P-256 with SHA-256 或 P-384 with SHA-384。

(3) 用戶使用金鑰長度至少為 2048 位元之 RSA 金鑰或符合 NIST P-256/P-384 之 ECDSA 金鑰。

(4) 前述之 RSA 金鑰長度(以位元為單位)須可被 8 整除。

6.1.6 公開金鑰參數之產製與品質檢驗

RSA 演算法之公開金鑰參數為空值(Null)。

HiPKICA 根憑證機構與下屬憑證機構選用 RSA 金鑰時，應採用 ANSI X9.31 演算法或 NIST FIPS 186-4 規範產生 RSA 演算法所需之質數，並確保該質數為強質數。

交互認證憑證機構須依所選用之演算法，進行適當之金鑰參數品質檢驗。

用戶金鑰於軟硬體密碼模組中產生 RSA 演算法所需之質數時，得無須保證該質數為強質數，然該金鑰須通過弱金鑰檢查後，始可作為憑證金鑰使用。

HiPKICA 依據 NIST SP 800-89 第 5.3.3 節之規定，確認 RSA 演算法所使用之公開指數值為大於 3 的奇數，且其值介於 $2^{16}+1$ 與 $2^{256}-1$ 之間。同時，模數應具有奇數、非質數的指數次方且沒有小於 752 的因數等性質。

此外，HiPKICA 依據 NIST SP 800-56A Revision 3 之規定，採用橢圓曲線密碼學完整公開金鑰驗證程序(ECC Full Public Key Validation Routine)或橢圓曲線密碼學部分公開金鑰驗證程序(ECC Partial Public Key Validation Routine)，以確保 ECDSA 金鑰之有效性。

6.1.7 金鑰之使用目的

6.1.7.1 憑證機構之金鑰使用目的

HiPKICA 根憑證機構自簽憑證所對應之私密金鑰僅限用於自簽憑證、自發憑證、下屬憑證機構憑證、交互憑證、憑證廢止清冊、線上憑證狀態協定回應伺服器憑證及線上憑證狀態協定回應訊息之簽發。

HiPKICA 根憑證機構簽發之自簽憑證、自發憑證、下屬憑證機構憑證及交互憑證之金鑰用途(Key Usage)擴充欄位與延伸金鑰用途(Extended Key Usage)擴充欄位依第 7.1.2 節之規定辦理。

6.1.7.2 用戶之金鑰使用目的

用戶憑證之金鑰用途擴充欄位與延伸金鑰用途擴充欄位依第 7.1.2 節之規定辦理。

6.2 私密金鑰保護及密碼模組工程控管

6.2.1 密碼模組標準與控管

HiPKICA 使用通過 FIPS 140-2 Level 3、FIPS 140-3 Level 3 或安全強度相當認證之硬體密碼模組。

6.2.2 私密金鑰分持之多人控管

HiPKICA 私密金鑰依第 5.2 節規定採用多人控管程序，並以此做為金鑰啟動與停用以及金鑰分持備份與回復之方式。

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

HiPKICA 私密金鑰不可被託管，HiPKICA 亦不提供金鑰託管服務。

6.2.4 私密金鑰備份

HiPKICA 依第 6.2.2 節私密金鑰分持之多人控管方法備份私密金鑰，並使用具高安全性之 IC 卡做為秘密分持的儲存媒體。HiPKICA 不另提供金鑰備份服務。

6.2.5 私密金鑰歸檔

HiPKICA 私密金鑰不可被歸檔，HiPKICA 亦不對用戶私密金鑰進行歸檔。

6.2.6 私密金鑰匯入、匯出密碼模組

私密金鑰僅於金鑰備份、金鑰回復或更換密碼模組時，始可從密碼模組匯出至備份專用之符記，亦或從備份專用之符記匯入至密碼模

組，其匯入或匯出過程之控管方式應遵照第 6.2.2 節之規定。私密金鑰從密碼模組匯出或於密碼模組間傳輸時，須使用加密或金鑰分持多人控管方式保護，確保私密金鑰不曾以明碼呈現。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。

若 HiPKICA 發現其下屬憑證機構或交互認證憑證機構之私密金鑰洩漏給未授權人員或不屬於該憑證機構之組織的情形，其根憑證機構將廢止與該憑證機構之私密金鑰相關之憑證。

6.2.7 私密金鑰儲存於密碼模組

依照第 6.1.1 節與第 6.2.1 節規定；硬體密碼模組如不需使用時，須離線並儲存於第 5.1.1 節所述之場所。

6.2.8 啟動私密金鑰之方式

HiPKICA 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 卡分別由管理員與簽發員保管。

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。

6.2.9 停用私密金鑰之方式

HiPKICA 之私密金鑰在不使用時，將依照本文件之規定選擇適當的停用方式將私密金鑰停用。HiPKICA 不提供用戶之私密金鑰停用。

6.2.10 銷毀私密金鑰之方式

為避免憑證機構舊的私密金鑰被盜用，影響簽發憑證之正確性，當憑證機構之私密金鑰生命週期屆滿或不再使用時(不再簽發任何憑證與憑證廢止清冊)，HiPKICA 將會把硬體密碼模組中存放舊的憑證

機構私密金鑰之記憶位置填零(Zeroization)，以銷毀硬體密碼模組中舊的私密金鑰。同時，舊的私密金鑰之金鑰備援的秘密持份 IC 卡也會進行實體銷毀。

倘若硬體密碼模組將不再提供 HiPKICA 所需之服務，但其仍可被存取時，則此硬體密碼模組中所有的私密金鑰(包含曾經使用過或是可能被使用的私密金鑰)皆應被銷毀。在銷毀該硬體密碼模組中的私密金鑰後，須再使用該硬體密碼模組所提供的金鑰管理工具加以檢視，確認前述所有私密金鑰已確實不存在。

下屬憑證機構與交互認證之憑證機構必須依照本文件之規定，選擇適當的私密金鑰銷毀方式；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

6.3.1 公開金鑰歸檔

HiPKICA 依第 5.5 節之規定對其所簽發之憑證進行歸檔作業。

6.3.2 憑證操作與金鑰對之效期

6.3.2.1 憑證機構憑證操作及金鑰對之效期

HiPKICA 簽發憑證機構之憑證及其私密金鑰最長效期如下：

憑證機構	私密金鑰效期	憑證效期
根憑證機構	2025/7/31(含)之前	
	■ 簽發自簽憑證：15 年 ■ 簽發自發憑證：不做規定 ■ 簽發交互憑證：不做規定	25年

	■ 簽發下屬憑證機構憑證：15 年 ■ 簽發憑證廢止清冊、線上憑證狀態協定回應伺服器憑證或線上憑證狀態協定回應訊息：25 年	
	2025/8/1(含)之後	
	■ 簽發自簽憑證：不做規定 ■ 簽發自發憑證：不做規定 ■ 簽發交互憑證：不做規定 ■ 簽發下屬憑證機構憑證：不做規定 ■ 簽發憑證廢止清冊、線上憑證狀態協定回應伺服器憑證或線上憑證狀態協定回應訊息：15.5 年	15.5年
下屬憑證機構	2025/7/31(含)之前	
	■ 簽發用戶憑證：10 年 ■ 簽發憑證廢止清冊、線上憑證狀態協定回應伺服器憑證或線上憑證狀態協定回應訊息：20 年	20年
	2025/8/1(含)之後	
	■ 簽發用戶憑證：2.5 年 ■ 簽發憑證廢止清冊、線上憑證狀態協定回應伺服器憑證或線上憑證狀態協定回應訊息：3 年	3年

根憑證機構自簽憑證之效期至少應為 2922 天(約 8 年)。

根憑證機構簽發之下屬憑證機構憑證或交互憑證之效期不得超過根憑證機構自簽憑證之效期。

根憑證機構新舊金鑰互簽之自發憑證之效期應至根憑證機構舊金鑰簽發之自簽憑證效期到期為止。

簽發憑證機構於其私密金鑰簽發憑證之使用期限到期後，應持續提供憑證廢止清冊、線上憑證狀態協定回應伺服器憑證或線上憑證狀

態協定回應訊息，直至所有憑證皆到期為止。

線上憑證狀態協定回應伺服器之私密金鑰及其憑證最長效期為36 小時；其使用私密金鑰簽發線上憑證狀態協定回應訊息，該回應訊息內含數位簽章與線上憑證狀態協定回應伺服器憑證，可供信賴憑證者驗證該線上憑證狀態協定回應訊息之數位簽章與內容。

6.3.2.2 用戶憑證操作及金鑰對之效期

用戶憑證操作及其私密金鑰最長效期如下：

憑證類型	私密金鑰效期	憑證效期
OV TLS憑證		
• 2025/7/31(含)之前	不做規定	398天
• 2025/8/1(含)至2029/3/15(不含)	不做規定	90天
• 2029/3/15(含)之後	不做規定	47天

6.4 啟動資料

6.4.1 啟動資料之產生與安裝

依據私密金鑰產製時所設定之存取控制群組依序進行多人分持控管 IC 卡保管人員身分確認，並於身分確認完成後將隨機產生的啟動資料寫入硬體密碼模組中。進行前述身分確認時，保管人員須將其多人分持控管 IC 卡插入硬體密碼模組內建之讀卡機，並輸入個人識別碼(Personal Identification Number，以下簡稱 PIN 碼)進行確認。

6.4.2 啟動資料之保護

啟動資料由多人分持控管 IC 卡保護，IC 卡之 PIN 碼由保管人員負責保管，不得記錄於任何媒體上，若 PIN 碼連續輸入錯誤超過 3 次，

該 IC 卡即被鎖住；IC 卡移交時，新保管人員須重新設定 PIN 碼。

6.4.3 啟動資料之其他規範

不做規定。

6.5 電腦軟硬體安全控管措施

6.5.1 特定電腦安全技術需求

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

(1) 具備角色或身分鑑別的登入。

(2) 提供自行定義(discretionary)存取控制。

(3) 提供安全稽核能力。

(4) 對各種憑證服務和PKI信賴角色存取控制的限制。

HiPKICA 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

HiPKICA 憑證伺服器採用通過 Common Criteria EAL 3 或以上認證過的電腦作業系統。

6.6 生命週期技術控管

6.6.1 系統研發控管

HiPKICA 系統遵照軟體工程發展方法之規範進行研發與品質控管。

系統開發環境、測試環境及上線運作環境應獨立運作，以防止未經授權存取或變更之風險。此外，HiPKICA 僅可使用專用且獲得授權之軟硬體。

HiPKICA 註冊中心之軟體須於初次使用或更新版本前檢查是否有惡意程式碼，並定期執行安全性掃描作業，以防止被安裝惡意軟體。

各項交付 HiPKICA 之產品或程式應提供交付清單、測試報告及原始程式碼安全性掃瞄報告，並進行程式版本控管。

6.6.2 安全管理控管

HiPKICA 不得安裝與運作無關之軟硬體或元件。若需安裝軟體時，應先確認版本完整性與正確性，並於每次使用前或定期執行軟體完整性之檢驗。此外，系統之變動均須記錄與控管，同時亦須具備修改系統軟體或組態之偵測機制。

HiPKICA 於風險評鑑、風險處理及安全管理控管措施參考 ISO/IEC 27001、ISO/IEC 27002、ISO/IEC 27005、ISO/IEC 31000、WebTrust Principles and Criteria for Certification Authorities、Baseline Requirements 及 Network and Certificate System Security Requirements 之方法論或規定。

6.6.3 生命週期安全控管

每年至少進行 1 次現行金鑰是否有被破解之風險評估。

6.7 網路安全控管措施

HiPKICA 遵循 CA/Browser Forum 的 Network and Certificate System Security Requirements 實施網路安全控管措施。

HiPKICA 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。

HiPKICA 所簽發的憑證與憑證廢止清冊以數位簽章保護並傳送到儲存庫。HiPKICA 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。

HiPKICA 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。HiPKICA 至少每季進行一次網路與主機弱點掃描，滲透測試至少每年進行一次。修復時間取決於漏洞的嚴重程度，嚴重(Critical)風險之弱點問題會在 96 小時內進行評估，高風險/中等風險之弱點問題會在 45 至 90 天內解決。例外情況會被記錄、評估風險並存檔。

6.8 時戳

為確保下述時間之正確性，HiPKICA 定期依據受信賴之時間源進行系統校時，或於必要時使用自動與手動程序進行系統時間調整；前述之系統校時作業須可被稽核。

(1) 憑證簽發時間。

(2) 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。

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

HiPKICA 所簽發之憑證遵照 ITU-T X.509、Baseline Requirements 及 RFC 5280 正式版之相關規定。

7.1.1 版本

HiPKICA 簽發遵照 RFC 5280 與 ITU-T X.509 v3 版本之憑證。

7.1.2 憑證擴充欄位

參見附錄 3、附錄 3-1 及附錄 3-2 之說明。

7.1.3 演算法物件識別碼

HiPKICA 使用之演算法物件識別碼如下：

類型	演算法	物件識別碼
簽章	sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)}
	sha384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha384WithRSAEncryption(12)}
	sha512WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha512WithRSAEncryption(13)}
	ecdsaWithSHA256	{iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA256(2)}
	ecdsaWithSHA384	{iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA384(3)}

金鑰產製	rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) rsaEncryption(1)}
	ecPublicKey	{iso(1) member-body(2) us(840) ansi-x962(10045) keyType(2) ecPublicKey(1)}

使用上述橢圓曲線密碼演算法產製 ECDSA 金鑰時，其橢圓曲線參數之物件識別碼依金鑰長度設定如下：

金鑰長度	橢圓曲線參數	物件識別碼
P-256	secp256r1	{iso(1) member-body(2) us(840) ansi-x962(10045) curves(3) prime(1) prime256v1(7)}
P-384	secp384r1	{iso(1) identified-organization(3) certicom(132) curve(0) ansip384r1(34)}

7.1.4 命名形式

憑證之主體與簽發者兩個欄位使用 ITU-T X.500 唯一識別名稱，其欄位屬性型態遵照 ITU-T X.509、Baseline Requirements 及 RFC 5280 正式版之相關規定。

7.1.4.1 命名編碼

依據 Baseline Requirements 第 7.1.4.1 節規定，HiPKICA 簽發憑證機構所簽發之憑證，其簽發者欄位的編碼內容須與簽發憑證機構憑證之主體欄位的編碼形式完全相同。此外，前述憑證機構憑證若存在多張主體欄位內容相符之憑證(包含過期與廢止之憑證)，則其主體欄位之編碼內容應皆完全相同。

7.1.4.2 憑證機構憑證之主體資訊

HiPKICA 簽發憑證機構遵照本文件所闡述之程序驗證憑證主體之所有資訊，並確保該資訊正確無誤後，始可簽發憑證。HiPKICA 根憑證機構簽發之自簽憑證與下屬憑證機構憑證之主體名稱包含 3 個

屬性欄位，分別為通用名稱(commonName)、組織名稱(organizationName)及國家名稱(countryName)，說明如下：

(1) 通用名稱：可識別憑證機構之名稱，其為該憑證之唯一識別資訊，可作為與其他憑證機構憑證區分之用。

(2) 組織名稱：憑證機構所屬之正式組織名稱，可依我國認可縮寫方式調整，其組織身分鑑別依第 3.2.2 節規定辦理。

(3) 國家名稱：憑證機構營業地點所在之國家，依 ISO 3166-1 國際標準之規範註記為「TW」。

7.1.4.3 用戶憑證之主體資訊

藉由簽發用戶憑證，表示 HiPKICA 下屬憑證機構與註冊中心在憑證的簽發日期前已遵循第 3.2 節所闡述的程序來作驗證，確保所有記載於憑證之主體資訊的值是準確的。

用戶憑證主體名稱若包含通用名稱屬性欄位時，其僅可註記憑證主體別名擴充欄位之其中 1 個完全吻合網域名稱或萬用網域名稱。此外，憑證主體名稱屬性欄位不得僅註記「.」、「-」及「 」（即空格）等字元，及/或任何暗示該值不存在、不完整或不適用之說明。

用戶憑證主體別名擴充欄位至少須註記 1 個完全吻合網域名稱或萬用網域名稱，其內容須符合下述規定：

(1) 依第 3.2.7 節規定完成網域名稱擁有權或控制權之驗證。

(2) 萬用網域名稱須符合第 3.2.8 節之規定。

(3) 不得包含內部名稱。

(4) 自 2026 年 3 月 15 日起，不得包含以 IP 反向區域後綴為結尾之網域名稱。

(5) 完全吻合網域名稱部分須由 P-Labels 或 NR-LDH Labels 所組成，並以句點符號「.」連接。

(6) 不得包含代表網際網路網域名稱系統根區(Root Zone)之零長度網域標籤(Zero-length Domain Label)。

用戶憑證主體名稱使用之屬性欄位如下表所列；未列之屬性欄位不予使用。

屬性欄位名稱	必要性	屬性欄位說明
countryName (C)	MUST	憑證主體所屬國家資訊，採用 ISO 3166-1 alpha-2 代碼表示
localityName (L)	MUST	憑證主體之所在地資訊
organizationName (O)	MUST	憑證主體所屬之正式組織名稱
commonName (CN)	OPTIONAL	若包含此屬性欄位時，其僅可註記憑證主體別名擴充欄位之其中 1 個完全吻合網域名稱或萬用網域名稱。 ■ HiPKI OV TLS CA 自 2025/8/21 起簽發之憑證主體不再包含此屬性欄位 ■ CHT Trust TLS CA 不使用此欄位屬性

7.1.5 命名限制

HiPKICA 簽發之憑證不採用命名限制。對於不受技術約束(Technically Constrained)之自簽憑證、自發憑證、下屬憑證機構憑證及交互憑證，皆予以公開揭露，例如揭露於 CCADB。

7.1.6 憑證政策物件識別碼

HiPKICA 簽發之憑證(不含根憑證機構自簽憑證)須包含憑證政策擴充欄位，此擴充欄位除須依憑證保證等級標示本文件定義之憑證政策物件識別碼，亦應依憑證用途標示本文件引用且適用之 CA/Browser Forum 憑證政策物件識別碼。有關於憑證政策物件識別碼之相關說明請參閱第 1.2 節。

7.1.7 政策限制擴充欄位之使用

HiPKICA 根憑證機構簽發之下屬憑證機構憑證與交互憑證，於必要時將使用政策限制擴充欄位。除前述憑證外，HiPKICA 簽發之憑證不含政策限制擴充欄位。

7.1.8 政策限定元之語法與語意

HiPKICA 簽發之憑證可依其需求於憑證政策擴充欄位中使用憑證政策限定元(Policy Qualifiers)，用於標示本文件公告之網址。

7.1.9 關鍵憑證政策擴充欄位之語意處理

HiPKICA 簽發之憑證所含之憑證政策擴充欄位不註記為關鍵擴充欄位。

7.2 憑證廢止清冊之格式剖繪

HiPKICA 所簽發之憑證廢止清冊遵照 Baseline Requirements 與 RFC 5280 正式版之相關規定，其憑證廢止清冊欄位及擴充欄位說明如下；其中，以 ECDSA 金鑰簽署之憑證廢止清冊，其簽章演算法之選擇與使用應符合 Baseline Requirements 第 7.1.3.2.2 節之規定。

(1) 根憑證機構簽發之憑證廢止清冊

欄位	內容
版本(Version)	v2
簽章演算法	根憑證機構簽發憑證廢止清冊所使用之簽章演算法，其演算法及物件識別碼之對應關係請參見第 7.1.3 節： ■ RSA ➢ sha256WithRSAEncryption ➢ sha384WithRSAEncryption ➢ sha512WithRSAEncryption

	■ ECDSA ➢ ecdsaWithSHA384
簽發者	此欄位之編碼值須與根憑證機構自簽憑證之主體欄位之編碼值完全相同
本次更新時間 (thisUpdate)	憑證廢止清冊之簽發時間
下次更新時間	憑證廢止清冊預計之下次更新時間，其定義依第 4.9.7 節規定辦理
已廢止憑證清單	所有已被根憑證機構廢止之憑證機構憑證清單，至少包含憑證序號及廢止時間；憑證廢止清冊條目擴充欄位依第 7.2.2 節第(2)點之規定定義
憑證廢止清冊擴充欄位	參見第 7.2.2 節第(1)點之說明

(2) 下屬憑證機構簽發之憑證廢止清冊

欄位	內容
版本	v2
簽章演算法	下屬憑證機構簽發憑證廢止清冊所使用之簽章演算法，其演算法及物件識別碼之對應關係請參見第 7.1.3 節： ■ RSA ➢ sha256WithRSAEncryption ➢ sha384WithRSAEncryption ➢ sha512WithRSAEncryption ■ ECDSA ➢ ecdsaWithSHA256 ➢ ecdsaWithSHA384
簽發者	此欄位之編碼值須與下屬憑證機構憑證之主體欄位之編碼值完全相同
本次更新時間	憑證廢止清冊之簽發時間
下次更新時間	憑證廢止清冊預計之下次更新時間，其定義依第 4.9.7 節規定辦理
已廢止憑證清單	所有已被下屬憑證機構廢止之用戶憑證清單，至少包含憑證序號及廢止時間；憑證廢止清冊條目擴充欄位依第 7.2.2 節第(2)點之規定定義
憑證廢止清冊擴充欄位	參見第 7.2.2 節第(1)點之說明

7.2.1 版本

HiPKICA 簽發遵照 RFC 5280 與 ITU-T X.509 v2 版本之憑證廢止清冊。

7.2.2 憑證廢止清冊與憑證廢止清冊條目之擴充欄位

HiPKICA 所簽發之憑證廢止清冊，其憑證廢止清冊擴充欄位(crlExtensions)與憑證廢止清冊條目擴充欄位(crlEntryExtensions)遵照 ITU-T X.509、Baseline Requirements 及 RFC 5280 正式版之相關規定。

HiPKICA 簽發之憑證廢止清冊所使用之憑證廢止清冊擴充欄位與憑證廢止清冊條目擴充欄位說明如下：

(1) 憑證廢止清冊擴充欄位

擴充欄位	必要性	關鍵性	內容
憑證機構金鑰識別碼 (Authority Key Identifier)	MUST	N	此擴充欄位僅含金鑰識別碼欄位，用於註記簽發憑證機構之公開金鑰 SHA-1 雜湊值，其值須與簽發憑證機構憑證之主體金鑰識別碼擴充欄位內容完全相同
憑證廢止清冊數目 (CRL Number)	MUST	N	憑證廢止清冊之序號，須為大於或等於 0 且小於 2^{159} 之非負整數，並應為嚴格遞增之序列
發行發布點 (Issuing Distribution Point)	OPTIONAL	Y	此擴充欄位僅適用於部分憑證廢止清冊(Partitioned CRL)，為必要擴充欄位，其內容如下： ■ 包含發行發佈點欄位，用於註記簽發憑證機構公告之憑證廢止清冊的網址。 ■ 間接憑證廢止清冊與僅限屬性憑證欄位設為 FALSE。 ■ 僅限用戶憑證與僅限憑證機構憑證欄位不可同時設為 TRUE。 ■ 不包含僅限特定廢止原因代碼欄位。

(2) 憑證廢止清冊條目擴充欄位

擴充欄位	必要性	關鍵性	內容
原因代碼 (Reason Code)	OPTIONAL	N	此擴充欄位用於註記與憑證廢止事由相符之廢止原因。用於註記根憑證機構自簽憑證、自發憑證、下屬憑證機構憑證及交互憑證之廢止資訊時，其原因代碼可為： ■ caCompromise(2) ■ affiliationChanged(3) ■ superseded(4) ■ cessationOfOperation(5) ■ privilegeWithdrawn(9) 用於註記用戶憑證之廢止資訊時，其原因代碼及適用情境如下： ■ unspecified(0)：若允許使用此原因代碼時，則該擴充欄位將會被省略 ■ keyCompromise(1)：已知或懷疑用戶私密金鑰已被破解。 ■ affiliationChanged(3)：憑證的主體名稱或其他主體識別資訊已變更，且未有私密金鑰已被破解之疑慮。 ■ superseded(4)：原憑證已由新憑證所取代，可能原因包括(不限於此)： ➢ 用戶申請新憑證； ➢ HiPKICA 有合理證據確認憑證中所註記的完全吻合網域名稱之授權或控制權驗證已不再可信； ➢ 憑證因合規性原因被廢止，例如：不符合 Baseline Requirements 或本文件之規定。 ■ cessationOfOperation(5)：使用該憑證的網站已停止營運或用戶於憑證到期前已不再擁有或控制憑證內註記之網域名稱。

			■ privilegeWithdrawn(9)：用戶有違規行為，惟未導致私密金鑰被破解，例如：憑證申請資料內含不實或誤導性資訊、未履行用戶約定條款中之重大義務。

7.3 線上憑證狀態協定之格式剖繪

若 HiPKICA 提供符合 RFC 6960 與/或 RFC 5019 標準規範之線上憑證狀態協定查詢服務，則其所簽發憑證(不含根憑證機構自簽憑證)應於憑證機構資訊存取擴充欄位中載明簽發憑證機構所提供之線上憑證狀態協定查詢服務的網址。

7.3.1 版本

HiPKICA 可接受之線上憑證狀態協定查詢封包應包含如下資訊:

- 協定版本(Protocol Version)；
- 待查詢憑證識別碼(Target Certificate Identifier)。

線上憑證狀態協定回應伺服器簽發之線上憑證狀態協定回應訊息至少包含線上憑證狀態協定回應訊息狀態欄位，用於說明前述線上憑證狀態協定查詢封包之處理狀態；當狀態為成功時，線上憑證狀態協定回應訊息須再包含下述欄位：

欄位	說明
版本	v1
線上憑證狀態協定回應伺服器 ID(Responder ID)	線上憑證狀態協定回應伺服器之憑證主體名稱
產製時間(Produced Time)	回應訊息簽署時間
待查詢憑證識別碼	包括雜湊函數演算法、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

憑證狀態碼 (Certificate Status)	憑證狀態碼說明如下： ■ 0：表示憑證狀態有效； ■ 1：表示憑證已被廢止。當此欄位註記憑證已被廢止時，尚需提供此憑證之廢止時間與廢止原因，廢止原因應與憑證廢止清冊所註記之原因代碼相符(參見第 7.2.2 節)； ■ 2：表示憑證狀態未知。
效期	此回應訊息建議之效期區間，包括本次更新時間與下次更新時間。
簽章演算法	回應訊息之簽章演算法，可為： ■ sha256WithRSAEncryption ■ ecdsaWithSHA384
簽章	線上憑證狀態協定回應伺服器之簽章
憑證	線上憑證狀態協定回應伺服器之憑證

7.3.2 線上憑證狀態協定擴充欄位

線上憑證狀態協定回應訊息中之 singleExtensions 不得包含憑證廢止清冊條目擴充欄位「原因代碼(reasonCode，其物件識別碼為 2.5.29.21)」。

8 稽核與其他評核

8.1 稽核頻率或評核時機

HiPKICA 接受 1 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 HiPKICA 的運作確實遵循本文件所訂的安全規定與程序。

8.2 稽核人員之身分與資格

HiPKICA 將委外辦理外部稽核作業于熟悉 HiPKICA 運作並經 WebTrust for CA 標章管理單位授權可於中華民國執行相關 WebTrust Principles and Criteria for Certification Authorities 稽核標準之合格外部稽核業者，提供公正客觀的稽核服務。外部稽核人員應為合格授權之資訊系統稽核員(Certified Information System Auditor, CISA)或具同等資格，且具備 2 場次 4 人天以上之憑證機構 WebTrust for CA 標章稽核或 2 場次共計 8 人天憑證機構資訊安全管理稽核相關經驗。HiPKICA 於稽核時應對外部稽核人員進行身分識別。

8.3 稽核人員與被稽核方之關係

本公司將委託公正之第三方，就 HiPKICA 的運作進行稽核。

8.4 稽核項目

稽核採用的標準為 WebTrust Principles and Criteria for Certification Authoritie、WebTrust Principles and Criteria for Certification Authorities – TLS Baseline 與 WebTrust Principles and Criteria for Certification Authorities – Network Security。

稽核項目如下所述：

(1) HiPKICA是否遵照本文件運作，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，且對HiPKICA之實務作業而言是否允當。

(2) 確認註冊中心是否遵照本文件及相關程序運作。

HiPKICA 有權執行以下項目的查核或調查，以確保 HiPKICA 之公信力：

(1) 若有事件造成HiPKICA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本文件。

(2) 在符合性查核有不完整或特殊發現下，HiPKICA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，HiPKICA必須執行相關之查核或調查。

HiPKICA 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 HiPKICA 和執行稽核或調查的人員充分而合理之合作。

8.5 對於稽核結果之因應方式

如外部/內部稽核人員發現HiPKICA 或註冊中心之建置與維運不符合本文件規定時，採取以下行動：

(1) 記錄不符合情形。

(2) 將不符合情形通知HiPKICA。

(3) 對於不符合規定之項目，HiPKICA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，HiPKICA 將公布合格外部稽核業者所提供之應公開說明資訊。稽核結果以 WebTrust for Certification Authorities 、 WebTrust for Certification Authorities – Baseline Requirements 及 WebTrust for Certification Authorities – Network Security 標章之方式呈現於 HiPKICA 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，HiPKICA 將提供合格外部稽核業者簽署之解釋函。

8.7 自我稽核

HiPKICA 由內部稽核員依據 Baseline Requirements 及 WebTrust for Certification Authorities – TLS Baseline，至少每季針對簽發 TLS 憑證的註冊中心，自前 1 次抽樣後，隨機選擇簽發數量的至少 3%(若不足 1 張視為 1 張)執行持續性之內部稽核。

9 其他業務與法律事項

9.1 費用

9.1.1 憑證簽發或展期費用

HiPKICA 與用戶之間的憑證申請、簽發等計費架構，於相關業務契約條款中訂定。

9.1.2 憑證查詢費用

若有收費，應於相關業務契約條款中訂定。

9.1.3 憑證廢止或狀態查詢費用

用戶下載查詢憑證廢止清冊不收費；線上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。

9.1.4 其他服務費用

不做規定。

9.1.5 退費規定

HiPKICA 所收取之憑證簽發收費，如因 HiPKICA 之過失致用戶憑證無法使用，經 HiPKICA 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，HiPKICA 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

9.2.1 保險涵蓋範圍

HiPKICA 由本公司營運，其財務責任由本公司負責。

9.2.2 其他資產

HiPKICA 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，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。HiPKICA 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，流動資產與流動負債比符合 CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates 要求不低於 1.0 的要求，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

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 HiPKICA 或註冊中心產生、接收或保管之資料，均視為機密資訊。

(1) 營運相關的私密金鑰及通行碼(passphrase)。

(2) 金鑰分持的保管資料。

(3) 用戶之申請資料。

(4) 產生或保管之可供稽核及追蹤之紀錄。

(5) 稽核人員於稽核過程中產生之稽核紀錄及報告。

(6) 列為機密等級的營運相關文件。

HiPKICA 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) HiPKICA 儲存庫公布之簽發憑證、已廢止憑證及憑證廢止清冊資訊不視為機密資訊。

9.3.3 保護機密資訊之責任

HiPKICA 依照 WebTrust Principles and Criteria for Certification Authorities 相關稽核標準、Baseline Requirements 及個人資料保護法與其相關子法處理 HiPKICA 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

HiPKICA 於網站公告個人資料保護與隱私權聲明。HiPKICA 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 視為隱私之資訊

(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或指紋特徵

(4) 保密協定或契約之個人資訊。

HiPKICA 及註冊中心實施安控措施防止可識別之個人資料遭未經授權的揭露、洩漏或破壞。

9.4.3 非隱私之資訊

(1) 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。

(2) 儲存庫公布之簽發憑證、已廢止憑證及憑證廢止清冊資訊非隱私資訊。

9.4.4 保護隱私資訊之責任

配合 HiPKICA 運作所需之個人資料，無論紙本或是電子之形式，HiPKICA 依照個人資料保護法及其相關子法暨隱私權聲明處理用戶申請資料。HiPKICA 並與註冊中心協議保護隱私資訊的責任。

9.4.5 利用隱私資訊之告知與同意

遵循個人資料保護法及其相關子法，非經用戶同意或個人資料保護與隱私權聲明與本文件另有規範，不做特定目的外之利用。用戶得查詢第 9.3.1 節第(3)款用戶本身之申請資料；惟 HiPKICA 保留向申請查詢之用戶收取合理費用之權利。

9.4.6 應司法或管理程序提供資訊

司法機關、監察機關或治安機關如因下列之一之條件，必須查詢第 9.3.1 節機密資訊時，依法定程序辦理：

(1) 政府法令之規定並經由權責管理單位合法之授權。

(2) 法院處理因使用憑證產生的糾紛與仲裁而合法之申請需求。

否則憑證用戶之註冊基本資料與身分識別相關資料絕不任意提供予權責管理單位，或其他任何人知悉使用。

9.4.7 其他資訊提供之情況

HiPKICA 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 HiPKICA 之智慧財產:

(1) 因執行 HiPKICA 憑證管理作業而撰寫的相關文件或研發之系統。

(2) HiPKICA 所簽發的憑證及憑證廢止清冊。

(3) 本文件。

本文件可由 HiPKICA 儲存庫自由下載，或依著作權法相關規定合理使用。本文件得為合理之使用，不收取費用，對於不當使用或散布本文件之侵害，HiPKICA 將依法予以追訴。

9.6 聲明與擔保

9.6.1 憑證機構之聲明與擔保

HiPKICA 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，係遵照本文件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

於憑證簽發時，HiPKICA 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文件(參見第 3.2 節)。

(2) 憑證授權

於憑證簽發時，HiPKICA 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文件(參見第 3.2.5 節)。

(3) 資訊正確性

於憑證簽發時，HiPKICA 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文件(參見第 3.2.2、第 3.2.3 及第 3.2.9 節)。

(4) 無誤導資訊

於憑證簽發時，HiPKICA 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文件(參見第 3.2.2、第 3.2.3 及第 3.2.9 節)。

(5) 申請者的身分

若憑證中包含主體身分資訊，HiPKICA 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文件。

(6) 用戶協議

若 HiPKICA 與用戶非隸屬同一組織，則用戶與 HiPKICA 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 HiPKICA 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

HiPKICA 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

HiPKICA 將根據 Baseline Requirements 中所規定的任何理由廢止憑證(參見第 4.9.1 節)。

9.6.2 註冊中心之聲明與擔保

HiPKICA 所簽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。

註冊中心聲明以下責任及確保以下責任會被承擔：

(1) 對於憑證註冊審驗，係遵照本文件之規定

(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文件之規定

(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 用戶之聲明與擔保

為了 HiPKICA 及憑證受益人之明確利益，申請者應擔保憑證簽發前，HiPKICA 會收到：

(1) 申請者同意的用戶協議；或

(2) 申請者對用戶條款的確認。

申請者(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)應聲明以下責任及確保以下責任會被承擔：

(1) 安全地產製其私密金鑰並避免遭受破解

(2) 提供 HiPKICA 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 HiPKICA、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) 憑證只用於符合本文件及用戶約定條款之合法及經授權的使用目的，例如只安裝 TLS 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

信賴憑證者應聲明以下責任及確保以下責任會被承擔：

(1) 使用憑證或查詢 HiPKICA 儲存庫時，必須遵守本文件之相關規定

(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 HiPKICA 簽發之憑證廢止清冊或線上憑證狀態協定查驗 HiPKICA 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) HiPKICA 如因不可抗拒之故而無法正常運作時，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 HiPKICA 無法正常運作，作為抗辯他人之事由

(7) 接受 HiPKICA 簽發之憑證時，即視為已了解並同意有關 HiPKICA 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

除法律或本文件另有規範禁止之範圍外，HiPKICA 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本文件或 Baseline Requirements 之適用範圍使用憑證所引發之損失，HiPKICA 不負任何賠償責任。若屬可歸咎於 HiPKICA 之責任，其賠償金額上限依照本文件第 9.9 節規範。

9.9 賠償

9.9.1 HiPKICA 之賠償責任

HiPKICA 處理用戶憑證相關作業，若故意或過失未遵照本文件、相關法律規定及 HiPKICA 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 HiPKICA 負賠償責任。用戶得依與 HiPKICA 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。HiPKICA 對每一用戶或信賴憑證者之賠償總金額限制如下表所示，如用戶或信賴憑證者與 HiPKICA 訂有合約，另行規範憑證使用範圍與交易賠償限額者，從其約定。

憑證保證等級	賠償總金額上限(新台幣:元)
第 1 級	3,000
第 2 級	100,000
第 3 級	3,000,000
第 4 級	5,000,000

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

9.9.2 註冊中心之賠償責任

註冊中心處理用戶憑證註冊作業，若故意或過失未遵照本文件、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，屬 HiPKICA 建置之註冊中心由 HiPKICA 負賠償責任，賠償上限遵循第 9.9.1 節規定，其餘非 HiPKICA 建置之註冊中心，由該註冊中心負賠償責任。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

本文件於政策管理委員會核定通過後，於 HiPKICA 儲存庫公布後即生效。

9.10.2 終止

本文件新版本經政策管理委員會核定後公布，現有版本即告終止。

9.10.3 終止與保留之效力

本文件之效力，維持至遵循本文件所簽發之最後一張憑證到期或廢止為止。

9.11 主要成員間之個別告知與溝通

HiPKICA、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

本文件每年定期評估是否需要修訂，以維持其保證等級。如 Baseline Requirements 規範修訂時，本文件將配合修訂，且以適當之版本編號代表本文件有進行修訂，並依據第 2.3 節規定進行公告。

9.12.2 通知之機制與期限

重大變更項目及修訂之本文件新版生效後將公告於 HiPKICA 儲存庫。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 HiPKICA 考量相關意見，評估變更項目與回覆。

本文件重新排版時，不另作通知。

9.12.3 物件識別碼必須更改之情況

本文件之修訂會影響其聲明之憑證用途或保證等級時，憑證政策物件識別碼應作相對應之變更。

9.13 爭議解決

用戶或註冊中心與 HiPKICA 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 HiPKICA 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

依據本文件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

本文件所約定者，係主要成員(憑證機構、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

本文件所敘述的主要成員之間的權利或責任，不能在未通知 HiPKICA 下以任何形式轉讓給其他方。

9.16.3 可分割性

本文件的任一條款不正確或無效時，其他條款仍然有效，直到本文件修改為止。

本文件遵循 Baseline Requirements 規定，惟 Baseline Requirements 相關規定若與本文件所依循之本國相關法律或法規產生衝突時，本文件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 CA/Browser Forum；若本國法律或法規已不再適用時，或 Baseline Requirements 修訂相關內容使其規定可相容於本國法律時，則本文件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文件相關規定，致 HiPKICA 受有損害時，HiPKICA 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。

HiPKICA 未向違反本文件相關規定者主張權利，不代表 HiPKICA 對於其繼續或未來違反本文件情事，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 HiPKICA 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，HiPKICA 不負任何法律責任。HiPKICA 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。

附錄 1：縮寫及定義

縮寫	全稱	中文名詞或定義
AIA	Authority Information Access	憑證機構資訊存取，參見附錄 2。
CA	Certification Authority	憑證機構，參見附錄 2。
CAA	Certification Authority Authorization	授權憑證機構簽發憑證，參見附錄 2。
CPA	Chartered Professional Accountants Canada	加拿大會計師公會，參見附錄 2。
CP OID	CP Object Identifier	憑證政策物件識別碼。
CPS	Certification Practice Statement	憑證實務作業基準，參見附錄 2。
CRL	Certificate Revocation List	憑證廢止清冊，參見附錄 2。
DN	Distinguished Name	唯一識別名稱。
DNS	Domain Name System	網域名稱系統，參見附錄 2。
EE	End Entities	終端個體，參見附錄 2。
FIPS	(US Government) Federal Information Processing Standard	(美國)聯邦資訊處理標準，參見附錄 2。
FQDN	Fully Qualified Domain Name	完全吻合網域名稱，參見附錄 2。
IANA	Internet Assigned Numbers Authority, IANA	網際網路號碼分配機構，參見附錄 2。
IDN	Internationalized Domain Name	國際化域名，參見附錄 2。
IETF	Internet Engineering Task Force	網際網路工程任務小組，參見附錄 2。

縮寫	全稱	中文名詞或定義
NIST	(US Government) National Institute of Standards and Technology	(美國)國家標準和技術研究院，參見附錄 2。
OCSP	Online Certificate Status Protocol	線上憑證狀態協定。
OID	Object Identifier	物件識別碼，參見附錄 2。
OV	Organization Validation	組織驗證，參見附錄 2。
PIN	Personal Identification Number	個人識別碼。
PKCS	Public-Key Cryptography Standard	公開金鑰密碼學標準，參見附錄 2。
PKI	Public Key Infrastructure	公開金鑰基礎建設，參見附錄 2。
QGIS	Qualified Government Information Source	合格的政府資訊來源，參見附錄 2。
QTIS	Qualified Government Tax Information Source	合格的政府稅收資訊來源，參見附錄 2。
RA	Registration Authority	註冊中心，參見附錄 2。
RFC	Request for Comments	徵求修正意見書，參見附錄 2。
SSL	Secure Sockets Layer	安全插座層，參見附錄 2。
TLS	Transport Layer Security	傳輸層安全，參見附錄 2。
UPS	Uninterrupted Power System	不斷電系統，參見附錄 2。

附錄 2：名詞解釋

存取(Access)	運用系統資源處理資訊的能力。
存取控制 (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 (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(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。
歸檔(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(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 1 章第 2 條第 1 項]
保證等級 (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 1 章第 2 條第 2 項]
稽核(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。
稽核紀錄 (Audit Data)	依照發生時間順序之系統活動紀錄，可用以重建或調查事件發生的順序及某個事件中的變化。
鑑別(Authenticate)	(1) 驗證某個聲稱的身分是合法的且屬於提出此聲稱者的程序。[A Guide to Understanding Identification and Authentication in Trusted Systems, National Computer Security Center] (2) 當某個體出示身分時，確認其身分之正確性。
鑑別程序 (Authentication)	(1) 建立使用者或資訊系統身分信賴程度的程序。[NIST.SP.800-63-2 Electronic Authentication Guideline]。 (2) 用以建立資料傳送、訊息、來源者之安全措施，或是驗證個人接收特定種類資訊權限之方法。

	(3) 鑑別是識別的證明。[A Guide to Understanding Identification and Authentication in Trusted Systems] 而所謂的相互鑑別(Mutual Authentication, National Computer Security Center)是指發生在進行通訊活動的兩方彼此進行鑑別。
憑證機構資訊存取(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。微軟之視窗作業系統中文版將此名詞翻譯為授權存取資訊。
經授權網域名稱(Authorization Domain Name)	用於取得對某一個特定完全吻合網域名稱之憑證簽發的授權之網域名稱。 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(Base Domain Name)	申請的完全吻合網域名稱(FQDN)之一部分，是註冊表控制(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或公開字尾(例如「example.co.uk」或「example.com」)。完全吻合網域名稱(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。
基本要求(Baseline Requirements)	由 CA/Browser Forum 所發行的「The Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates」以及對這份文件所作的任何修訂。

連結、繫結 (Binding)	將兩個相關的資訊元素做連結(結合)的過程。
憑證機構憑證 (CA Certificate)	簽發給憑證機構的憑證。
憑證機構金鑰對 (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。
憑證(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] (2) 資訊之數位呈現，內容包括： A.簽發的憑證機構。 B.用戶之名稱或身分。 C.用戶的公開金鑰。 D.憑證之有效期間。 E.憑證機構數位簽章。 在本文件中所提及的「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物件識別碼的憑證。
憑證機構 (Certification Authority, CA)	(1) 簽發憑證之機關、法人。[電子簽章法第 2 條第 5 款] (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)取得授權幫該網域名稱簽發憑證。發布 CAA DNS Resource Record 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]
憑證政策 (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 1 章第 2 條第 3 項]

	(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(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] (2) 宣告某憑證機構對憑證之作業程序(包括簽發、停用、廢止及存取等)符合特定需求(需求載明於憑證政策或其他服務契約中)之聲明。
憑證格式剖繪 (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 (Certificate Problem Reports)	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。
憑證廢止清冊 (Certificate Revocation List, CRL)	(1) 憑證機構以數位方式簽章，並可供信賴憑證者使用之已廢止憑證表列。[憑證實務作業基準應載明事項準則第 1 章第 2 條第 8 項] (2) 由憑證機構維護之清單，清單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。
加拿大會計師公會(Chartered Professional Accountants Canda, CPA)	與美國會計師公會共同訂頒 The Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy 系列標準之單位，並為 WebTrust for CA、SSL Baseline Requirement & Network Security 標章之管理單位。加拿大會計師公會之前英文名稱為 Canadian Institute of Chartered Accountants，縮寫為 CICA。

破解 (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 (Confidentiality)	資訊不會遭受未經授權的個體或程序獲知或取用。
交互憑證 (Cross-Certificate)	在兩個憑證根憑證機構(Root CA)之間建立信賴關係的一種憑證，屬於一種憑證機構憑證，而非用戶憑證。
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。
資料完整性(Data Integrity)	資料未遭受未經授權或意外的更改、破壞或遺失的性質。
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(Domain Name Registrant)、技術聯絡人(technical contact)、或管理聯絡人(administrative contract)(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(Domain Name Registrar)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：(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(a national Domain Name authority/registry), 或(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)	用來自動轉換 IP 位址與網域名稱的分散式資料庫。
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。
終端個體 (End Entity)	在本基礎建設中包括以下兩類個體： (1) 負責保管及應用憑證的私密金鑰擁有者。 (2) 信賴本基礎建設憑證機構所簽發憑證的第三者(不是私密金鑰擁有者，也不是憑證機構)，亦即終端個體為用戶及信賴憑證者，包括人員、組織、客戶(Account)、裝置或站台(Site)。
終端個體憑證 (End-Entity Certificate)	簽發給終端個體的憑證。
中華電信 HiPKI	本公司配合 Chrome Root Certificate 政策規範，依照 ITU-T X.509 標準建置的階層式公開金鑰基礎建設，此基礎建設中之下屬憑證機構只會簽發應用於傳輸層安全(Transport Layer Security, TLS)通訊協定之設備或應用軟體用 TLS 憑證。
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)	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憑證政策/憑證實務作業基準文件及電子憑證體系架構、接受下屬憑證機構與交互證認證憑證機構的互運申請及其所提供之憑證政策/憑證實務作業基準文件。

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。
聯邦資訊處理標準(Federal Information Processing Standard, 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)，FIPS 140-2 將密碼模組區分為 11 類安全需求，每一個安全需求類別再分成 4 個安全等級。
防火牆(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(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。完全吻合網域名稱包含主機名稱(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)。完全吻合網域名稱的開頭一定是主機名稱。 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)。
高風險憑證請求(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。
識別(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] 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、電子郵件。

完整性(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。
國際化域名(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(Alphabetic 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。官方網站位於 https://www.ietf.org/，其願景是藉由產製高品質之技術文件影響人類設計、使用與管理網際網路，使得網際網路運作更順暢。
IP 反向區域後綴(IP Reverse Zone Suffix)	由網域標籤「in-addr.arpa」或「ip6.arpa」所構成之兩個完全吻合網域名稱之一。此兩個完全吻合網域名稱分別作為網際網路協定第 4 版(IPv4)及第 6 版(IPv6)反向對應(Reverse Mapping)命名空間之根節點。其中，「in-addr.arpa」為 IPv4 反向對應命名空間之根節點，「ip6.arpa」則為 IPv6 反向對應命名空間之根節點。
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。
金鑰託管(Key Escrow)	將用戶的私密金鑰及依據用戶必須遵守的託管協議(或類似的契約)所規定的相關資訊進行存放，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，依據協議的規定，擁有用戶的金鑰。
金鑰交換(Key Exchange)	交換彼此金鑰以建立安全通訊的處理過程。
金鑰對(Key Pair)	兩把數學上有相關性的金鑰，具有下列特性： (1) 其中 1 把金鑰用來做訊息加密，而此加密訊息只有用成配對關係的另 1 把金鑰可以解密。

	(2) 從其中 1 把金鑰要推出另 1 把金鑰(從計算的角度而言)是不可行的。
Linting	用以檢查數位簽章資料(例如預簽憑證 [RFC 6962]、憑證、憑證廢止清冊或 OCSP response)或待簽章資料物件(例如 tbsCertificate (參考 RFC 5280 第 4.1.1.1 節))的內容是否符合這些要求中定義的剖繪和要求的流程。
不可否認性(Non-Repudiation)	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任者(信任之一方)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；本文件修訂時，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 1 章第 2 條第 4 項] (2) 向國際標準化組織(ISO)註冊的特別形式的數碼，當提及某物件或物件類別時，可以引用此唯一的數碼做辨識。例如在公開金鑰基礎架構中，可以此數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(Online Certificate Status Protocol, OCSP)	線上憑證狀態協定(Online Certificate Status Protocol)是 1 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 (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 憑證狀態請求擴展欄位(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。

	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 CA 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 CA 詢問其 TLS 憑證狀態，因此減輕 CA 的負擔。 此種機制藉由 TLS 網站轉發 CA OCSP 回應伺服器定期簽發之 TLS 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。
特殊安全管道 (Out-of-Band)	不同於一般的傳送訊息管道的傳送方式。例如使用電子線上傳送的情形，可稱使用實體的掛號信為特殊安全管道。
組織驗證 (Organization Validation, OV)	TLS 憑證簽發過程中，除了識別與鑑別用戶之網域名稱控制權外並且依照憑證的保證等級識別與鑑別用戶之組織身分。故連結安裝組織驗證型 TLS 憑證之網站，可提供 TLS 加密通道，知道該網站之擁有者是誰並確保傳遞資料之完整性。
持久性網域控管權 TXT 紀錄 (Persistent DCV TXT Record)	依據 Baseline Requirements 第 3.2.2.4.22 節，用於識別申請者之 DNS TXT 紀錄。
私密金鑰 (Private Key)	(1) 在簽章金鑰對中，用以產生數位簽章的金鑰。 (2) 在加解密金鑰對中，用以對機密資訊解密的金鑰。 在這兩種情境中，此金鑰皆須保密。
公開金鑰 (Public Key)	(1) 在簽章金鑰對中，用以驗證數位簽章有效的金鑰。 (2) 在加解密金鑰對中，用以對機密資訊加密的金鑰。 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。

公開金鑰密碼學標準(Public-Key Cryptography Standard, 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。
公開金鑰基礎建設(Public Key Infrastructure, PKI)	由法律、政策、規範、人員、設備、設施、技術、流程、稽核和服務之集合，在廣泛尺度上發展與管理非對稱式密碼學及公鑰憑證。
合格稽核業者(Qualified Auditor)	符合基本要求(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(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。CA/Browser Forum 之 Guidelines For The Issuance and Management of Extended Validation Certificates 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、美國的國稅局(IRS)。
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。
註冊中心(Registration Authority, RA)	(1) 負責確認憑證申請者之身分或其他屬性，但不簽發憑證亦不管理憑證。註冊中心是否需為其行為負責及其應負責任之範圍，依所適用之憑證政策或協議訂之。 (2) 1 個體，負責對憑證主體做身分識別及鑑別，但不做憑證簽發。

金鑰更換(Re-key (a certificate))	改變在密碼系統應用程式中所使用之金鑰之值。通常必須藉由對新的公開金鑰簽發新的憑證來達成。
信賴憑證者 (Relying Party)	(1) 信賴所收受之憑證及可用憑證中所載之公開金鑰加以驗證之數位簽章者，或信賴憑證中所命名主體之身分(或其他屬性)及憑證所載公開金鑰之對應關係者。[憑證實務作業基準應載明事項準則第 1 章第 2 條第 6 項] (2) 個人或機構收到包含憑證及數位簽章(此數位簽章可藉由憑證上所列之公開金鑰做驗證)之資訊，並且可能信賴這些資訊。
儲存庫 (Repository)	(1) 用以儲存與檢索憑證或其他憑證相關資訊之可信賴系統(Trustworthy System)。[憑證實務作業基準應載明事項準則第 1 章第 2 條第 7 項] (2) 包含本文件與憑證相關資訊的資料庫。
請求符記 (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。 請求符記應結合用於憑證請求之公開金鑰。 請求符記可包含時戳以指出何時產製。 請求符記可包含其他資訊以確保其唯一性。 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。 包含時戳的請求符記如果其時戳是在未來則應視為無效。 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。 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。
所要求的網站內容(Required Website Content)	隨機值或請求符記其中之一，加上由憑證機構指定可唯一識別用戶之額外資訊。
保留 IP 位址 (Reserved IP Addresses)	IANA 設定為保留的 IPv4 或 IPv6 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
憑證廢止(Revoke a Certificate)	在憑證的有效期間內，提前終止憑證的運作。
徵求修正意見書(Request for Comments, RFC)	由網際網路工程任務小組(IETF)發行的一系列備忘錄。包含網際網路、UNIX 和網際網路社群的規範、協定、流程等的標準檔案，以編號排定。
安全插座層(Secure Sockets Layer)	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。 安全插座層協定的優勢在於它與應用層協定獨立無關。高層的應用層協定(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 TLS(Transport Layer Security)協定。
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： (a)憑證中所載明之主體 (b)擁有與憑證上所列公開金鑰相對應之私密金鑰。 (c)本身不簽發憑證給其他方。
技術上的不可否認性(Technical 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。
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(Inside Threat)與外部威脅(Outside Threat)。內部威脅是指利用授與之權限，可能透過資料的破壞、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。
頂級網域名稱 (Top-Level Domain)	依據 RFC 8499(https://tools.ietf.org/html/rfc8499)之定義，頂級網域名稱係指位於根網域下一層之區域，例如「com」或「jp」。
時戳(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 協定制訂為 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 (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 (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。
可信賴系統 (Trustworthy System)	具有下列性質之電腦硬體、軟體及程序： (1)對於入侵及誤用有相當的保護功能。 (2) 提供合理的可用性、可靠度及正確操作。 (3)適當地執行預定功能。 (4)與一般為人所接受的安全程序一致。
不斷電系統 (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(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]
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(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。

附錄 3：HiPKICA 憑證基本欄位及擴充欄位說明

HiPKICA 簽發之憑證所使用之基本欄位及擴充欄位，遵照 ITU-T X.509、Baseline Requirements 及 RFC 5280 正式版之相關規定。

HiPKICA 不允許簽發下述情境之憑證：

(1) 憑證之擴充欄位內含無法應用於公眾網路的設定；

(2) 憑證之內容包含可能誤導信賴憑證者相信該憑證資訊已經由HiPKICA驗證之語意；

(3) 憑證主體名稱欄位之通用名稱或憑證主體別名擴充欄位內含內部名稱或保留IP位址。

HiPKICA 下屬憑證機構可使用符合 RFC 6962 之「X.509 v3 擴充欄位」，以支援憑證透明度(Certificate Transparency, CT)，做法如下：

(1) 下屬憑證機構傳送符合RFC 6962所定義且尚未封裝已簽憑證時戳之預簽憑證至數個憑證透明度日誌伺服器，待其個別回覆已簽憑證時戳；

(2) 將已取得且數量符合規定之已簽憑證時戳封裝至預簽憑證之特定X.509 v3擴充欄位，並對該預簽憑證進行簽章與封裝，完成該憑證之簽發作業；

(3) 前述作業所提及之預簽憑證僅用於憑證透明度之「X.509 v3 擴充欄位」方法，其不可視為符合RFC 5280規定之憑證。

附錄 3-1：憑證機構憑證

HiPKICA 簽發之憑證機構憑證包含根憑證機構自簽憑證與自發憑證、下屬憑證機構憑證及交互憑證，其基本欄位及擴充欄位說明如下；其中，以 ECDSA 金鑰簽署之憑證，其簽章演算法之選擇與使用應符合 Baseline Requirements 第 7.1.3.2.2 節之規定。未於本附錄中提及之擴充欄位，其使用方式應依附錄 3 之規定辦理。

(1) 根憑證機構自簽憑證

■ 憑證基本欄位

欄位	內容
版本	v3
序號	憑證序號，其為大於 0 且小於 2^{159}之非連續數值，且該值至少包含由密碼學安全偽隨機數產生器(Cryptographically Secure Pseudorandom Number Generator, CSPRNG)所產生之 64 位元輸出
簽章演算法	根憑證機構簽發憑證所使用之簽章演算法，其演算法及物件識別碼之對應關係請參見第 7.1.3 節： ■ RSA ➢ sha256WithRSAEncryption ➢ sha384WithRSAEncryption ➢ sha512WithRSAEncryption ■ ECDSA ➢ ecdsaWithSHA384
簽發者	此欄位之編碼值須與主體欄位之編碼值完全相同
效期	憑證效期包含起始時間及截止時間；其規定依第 6.3.2.1 節辦理
主體	用於載明根憑證機構自簽憑證之主體資訊，相關說明請參見第 7.1.4.2 節
主體公開金鑰資訊	用於載明憑證主體之公開金鑰及其所使用之演算法，其演算法及參數之物件識別碼對應關係請參見第 7.1.3 節：

	■ RSA：rsaEncryption ■ ECDSA：ecPublicKey ➢ 橢圓曲線參數：secp384r1(NIST P-384)

■ 憑證擴充欄位

擴充欄位	必要性	關鍵性	內容
憑證機構金鑰識別碼	OPTIONAL	N	此擴充欄位若存在，則僅可含金鑰識別碼欄位，其值須與主體金鑰識別碼擴充欄位內容完全相同
主體金鑰識別碼 (Subject Key Identifier)	MUST	N	根憑證機構之公開金鑰 SHA-1 雜湊值(160 位元)
基本限制 (Basic Constraints)	MUST	Y	Subject Type=CA Path Length Constraint=None
金鑰用途	MUST	Y	此擴充欄位內容包含： ■ keyCertSign(必要) ■ cRLSign(必要) ■ digitalSignature(可選)

(2) 根憑證機構自發憑證

■ 憑證基本欄位

欄位	內容
版本	v3
序號	憑證序號，其為大於 0 且小於 2^{159}之非連續數值，且該值至少包含由密碼學安全偽隨機數產生器所產生之 64 位元輸出
簽章演算法	新(舊)根憑證機構簽發憑證所使用之簽章演算法，其演算法及物件識別碼之對應關係請參見第 7.1.3 節： ■ RSA ➢ sha256WithRSAEncryption ➢ sha384WithRSAEncryption ➢ sha512WithRSAEncryption ■ ECDSA ➢ ecdsaWithSHA384

簽發者	此欄位之編碼值須與新(舊)根憑證機構自簽憑證之主體欄位之編碼值完全相同
效期	憑證效期包含起始時間及截止時間；其規定依第 6.3.2.1 節辦理
主體	用於載明根憑證機構自發憑證之主體資訊，此欄位之編碼值須與舊(新)根憑證機構自簽憑證之主體欄位之編碼值完全相同
主體公開金鑰資訊	用於載明憑證主體之公開金鑰及其所使用之演算法，其演算法及參數之物件識別碼對應關係請參見第 7.1.3 節： ■ RSA：rsaEncryption ■ ECDSA：ecPublicKey ➢ 橢圓曲線參數：secp384r1(NIST P-384)

■ 憑證擴充欄位

擴充欄位	必要性	關鍵性	內容
憑證機構金鑰識別碼	MUST	N	此擴充欄位僅含金鑰識別碼欄位，用於註記新(舊)根憑證機構之公開金鑰 SHA-1 雜湊值，其值須與新(舊)根憑證機構自簽憑證之主體金鑰識別碼擴充欄位內容完全相同
主體金鑰識別碼	MUST	N	舊(新)根憑證機構之公開金鑰 SHA-1 雜湊值(160 位元)
憑證廢止清冊發布點 (CRL Distribution Points)	MUST	N	新(舊)根憑證機構公告之憑證廢止清冊的下載網址
憑證機構資訊存取	MUST	N	此擴充欄位至少包含下述任一資訊： ■ 新(舊)根憑證機構自簽憑證之下載網址(可選) ■ 新(舊)根憑證機構所提供之線上憑證狀態協定查詢服務的網址(可選)
憑證政策 (certificate Policies)	MUST	N	此擴充欄位須包含下述憑證政策物件識別碼資訊，並可視憑證需求使用政策限定元，用於標示本文件公告之網址。

擴充欄位	必要性	關鍵性	內容
			■ 本文件引用之所有 CA/Browser Forum 定義之憑證政策物件識別碼 ■ 本文件定義之所有憑證政策物件識別碼
延伸金鑰用途	MUST	N	此擴充欄位內容包含： ■ id-kp-serverAuth(必要) ■ id-kp-clientAuth(可選；自 2025/6/15 起簽發之憑證不得包含)
金鑰用途	MUST	Y	此擴充欄位內容應與舊(新)根憑證機構自簽憑證之金鑰用途擴充欄位相同。
基本限制	MUST	Y	Subject Type=CA Path Length Constraint=None

(3) 下屬憑證機構憑證

■ 憑證基本欄位

欄位	內容
版本	v3
序號	憑證序號，其為大於 0 且小於 2^{159}之非連續數值，且該值至少包含由密碼學安全偽隨機數產生器所產生之 64 位元輸出
簽章演算法	根憑證機構簽發憑證所使用之簽章演算法，其演算法及物件識別碼之對應關係請參見第 7.1.3 節： ■ RSA ➢ sha256WithRSAEncryption ➢ sha384WithRSAEncryption ➢ sha512WithRSAEncryption ■ ECDSA ➢ ecdsaWithSHA384
簽發者	此欄位之編碼值須與根憑證機構自簽憑證之主體欄位之編碼值完全相同

效期	憑證效期包含起始時間及截止時間；其規定依第 6.3.2.1 節辦理
主體	用於載明下屬憑證機構憑證之主體資訊，相關說明請參見第 7.1.4.2 節
主體公開金鑰資訊	用於載明憑證主體之公開金鑰及其所使用之演算法，其演算法及參數之物件識別碼對應關係請參見第 7.1.3 節： ■ RSA：rsaEncryption ■ ECDSA：ecPublicKey ➢ 橢圓曲線參數：secp256r1(NIST P-256) ➢ 橢圓曲線參數：secp384r1(NIST P-384)

■ 憑證擴充欄位

擴充欄位	必要性	關鍵性	內容
憑證機構金鑰識別碼	MUST	N	此擴充欄位僅含金鑰識別碼欄位，用於註記根憑證機構之公開金鑰 SHA-1 雜湊值，其值須與根憑證機構自簽憑證之主體金鑰識別碼擴充欄位內容完全相同
主體金鑰識別碼	MUST	N	下屬憑證機構之公開金鑰 SHA-1 雜湊值(160 位元)
憑證廢止清冊發布點	MUST	N	根憑證機構公告之憑證廢止清冊的下載網址
憑證機構資訊存取	MUST	N	此擴充欄位至少包含下述任一資訊： ■ 根憑證機構自簽憑證之下載網址(可選) ■ 根憑證機構所提供之線上憑證狀態協定查詢服務的網址(可選)
憑證政策	MUST	N	此擴充欄位用於標示下屬憑證機構經根憑證機構核准並允許使用之憑證政策物件識別碼，可視憑證需求使用政策限定元，用於標示本文件公告之網址。憑證政策物件識別碼包含： ■ 本文件引用之 CA/Browser Forum 定義之憑證政策物件識別碼，必

擴充欄位	必要性	關鍵性	內容
			須與用戶憑證類型相關，且僅可註記 1 個(必要) ■ 本文件定義之憑證政策物件識別碼(可選)
延伸金鑰用途	MUST	N	此擴充欄位內容包含： ■ id-kp-serverAuth(必要) ■ id-kp-clientAuth(可選；自 2025/6/15 起簽發之憑證不得包含)
金鑰用途	MUST	Y	此擴充欄位內容包含： ■ keyCertSign(必要) ■ cRLSign(必要) ■ digitalSignature(可選)
基本限制	MUST	Y	Subject Type=CA Path Length Constraint=0

(4) 交互憑證

交互憑證之簽發對象為根憑證機構，該憑證機構不直接簽發用戶憑證。

■ 憑證基本欄位

欄位	內容
版本	v3
序號	憑證序號，其為大於 0 且小於 2^{159}之非連續數值，且該值至少包含由密碼學安全偽隨機數產生器所產生之 64 位元輸出
簽章演算法	根憑證機構簽發憑證所使用之簽章演算法，其演算法及物件識別碼之對應關係請參見第 7.1.3 節： ■ RSA ➢ sha256WithRSAEncryption ➢ sha384WithRSAEncryption ➢ sha512WithRSAEncryption ■ ECDSA ➢ ecdsaWithSHA384

簽發者	此欄位之編碼值須與根憑證機構自簽憑證之主體欄位之編碼值完全相同
效期	憑證效期包含起始時間及截止時間；其規定依第 6.3.2.1 節辦理
主體	用於載明交互憑證之主體資訊，此欄位之編碼值須與交互認證憑證機構之既有憑證機構憑證之主體欄位編碼值完全相同
主體公開金鑰資訊	用於載明憑證主體之公開金鑰及其所使用之演算法，其演算法及參數之物件識別碼對應關係請參見第 7.1.3 節： ■ RSA：rsaEncryption ■ ECDSA：ecPublicKey ➢ 橢圓曲線參數：secp256r1(NIST P-256) ➢ 橢圓曲線參數：secp384r1(NIST P-384)

■ 憑證擴充欄位

擴充欄位	必要性	關鍵性	內容
憑證機構金鑰識別碼	MUST	N	此擴充欄位僅含金鑰識別碼欄位，用於註記根憑證機構之公開金鑰 SHA-1 雜湊值，其值須與根憑證機構自簽憑證之主體金鑰識別碼擴充欄位內容完全相同
主體金鑰識別碼	MUST	N	交互認證憑證機構之公開金鑰 SHA-1 雜湊值(160 位元)
憑證廢止清冊發布點	MUST	N	根憑證機構公告之憑證廢止清冊的網址
憑證機構資訊存取	MUST	N	此擴充欄位至少包含下述任一資訊： ■ 根憑證機構自簽憑證之下載網址(可選) ■ 根憑證機構所提供之線上憑證狀態協定查詢服務的網址(可選)
憑證政策	MUST	N	此擴充欄位用於標示交互認證憑證機構經根憑證機構核准並允許使用之憑證政策物件識別碼，可視憑證需求使用政策限定元，用於標示本

擴充欄位	必要性	關鍵性	內容
			文件公告之網址。憑證政策物件識別碼包含： ■ 本文件引用之 CA/Browser Forum 定義之憑證政策物件識別碼，須與此憑證間接簽發之用戶憑證類型相關，且至少註記 1 個(必要) ■ 本文件定義之憑證政策物件識別碼(可選)
延伸金鑰用途	MUST	N	此擴充欄位內容包含： ■ id-kp-serverAuth(必要) ■ id-kp-clientAuth(可選；自 2025/6/15 起簽發之憑證不得包含)
金鑰用途	MUST	Y	此擴充欄位內容包含： ■ keyCertSign(必要) ■ cRLSign(必要) ■ digitalSignature(可選)
基本限制	MUST	Y	Subject Type=CA Path Length Constraint=依交互認證憑證機構所需之憑證路徑長度限制設定之，亦可不設定。

附錄 3-2：用戶憑證

HiPKICA 下屬憑證機構簽發之 TLS 憑證，其基本欄位及擴充欄位說明如下；其中，以 ECDSA 金鑰簽署之憑證，其簽章演算法之選擇與使用應符合 Baseline Requirements 第 7.1.3.2.2 節之規定。未於本附錄中提及之擴充欄位，其使用方式應依附錄 3 之規定辦理。

■ 憑證基本欄位

欄位	內容
版本	v3
序號	憑證序號，其為大於 0 且小於 2^{159}之非連續數值，且該值至少包含由密碼學安全偽隨機數產生器所產生之 64 位元輸出
簽章演算法	下屬憑證機構簽發憑證所使用之簽章演算法，其演算法及物件識別碼之對應關係請參見第 7.1.3 節： ■ RSA ➢ sha256WithRSAEncryption ➢ sha384WithRSAEncryption ➢ sha512WithRSAEncryption ■ ECDSA ➢ ecdsaWithSHA256 ➢ ecdsaWithSHA384
簽發者	此欄位之編碼值須與下屬憑證機構憑證之主體欄位之編碼值完全相同
效期	憑證效期包含起始時間及截止時間；其規定依第 6.3.2.2 節辦理
主體	用於載明 TLS 憑證之主體資訊，相關說明請參見第 7.1.4.3 節
主體公開金鑰資訊	用於載明憑證主體之公開金鑰及其所使用之演算法，其演算法及參數之物件識別碼對應關係請參見第 7.1.3 節： ■ RSA：rsaEncryption ■ ECDSA：ecPublicKey ➢ 橢圓曲線參數：secp256r1(NIST P-256) ➢ 橢圓曲線參數：secp384r1(NIST P-384)

■ 憑證擴充欄位

擴充欄位	必要性	關鍵性	內容
憑證機構金鑰識別碼	MUST	N	此擴充欄位僅含金鑰識別碼欄位，用於註記下屬憑證機構之公開金鑰 SHA-1 雜湊值，其值須與下屬憑證機構憑證之主體金鑰識別碼擴充欄位內容完全相同
主體金鑰識別碼	OPTIONAL	N	用戶之公開金鑰 SHA-1 雜湊值(160 位元)
憑證政策	MUST	N	此擴充欄位用於標示下屬憑證機構使用之憑證政策物件識別碼，可視憑證需求使用政策限定元，用以標示本文件公告之網址。憑證政策物件識別碼包含： ■ 本文件引用之 CA/Browser Forum 定義之憑證政策物件識別碼，必須與用戶憑證類型相關，且僅可註記 1 個(必要) ■ 本文件定義之憑證政策物件識別碼(可選)
憑證廢止清冊發布點	MUST	N	下屬憑證機構公告之憑證廢止清冊的網址
憑證機構資訊存取	MUST	N	此擴充欄位包含： ■ 下屬憑證機構憑證之下載網址(必要) ■ 下屬憑證機構所提供之線上憑證狀態協定查詢服務的網址(可選)
主體別名	MUST	N	此擴充欄位用於標示 1 個或多個完全吻合網域名稱或萬用網域名稱
基本限制	OPTIONAL	Y	Subject Type=End Entity Path Length Constraint=None
金鑰用途	MUST	Y	若憑證記載之公開金鑰為 RSA 公開金鑰時，其包含： ■ digitalSignature(必要) ■ keyEncipherment(依下列 CA 規定)

			➢ HiPKI OV TLS CA 自 2026 年 3 月起簽發之憑證不得包含 ➢ CHT Trust TLS CA 不得包含 若憑證記載之公開金鑰為 ECDSA 公開金鑰時，其包含： ■ digitalSignature
延伸金鑰用途	MUST	N	此擴充欄位內容包含： ■ id-kp-serverAuth(必要) ■ id-kp-clientAuth(依下列 CA 規定) ➢ HiPKI OV TLS CA 已停止包含，且自 2027/3/15 起簽發之憑證不得包含 ➢ CHT Trust TLS CA 不得包含
已簽憑證時戳清單 (Signed Certificate Timestamp List)	OPTIONAL	N	此擴充欄位若存在，則用於記載符合 RFC 6962 規範之已簽憑證時戳清單

附錄 4：HiPKICA 憑證機構憑證列表

請造訪 https://chtca.hinet.net/assets/download/CACertlist.pdf 查看 HiPKICA 的 CA 憑證列表。

附錄 5：BRs-Section 1.2.1 Revisions 參照表

本文件最新版修訂所參照之 Baseline Requirements 版本至 2.2.4 版。

Ver.	Ballot	Description	Adopted	Effective*
2.0.6	SC75	Pre-sign linting	28-Jun-2024	6-Aug-2024
2.0.7	SC67	Require Multi-Perspective Issuance Corroboration	2-Aug-2024	6-Sep-2024
2.0.8	SC77	Update WebTrust Audit name in Section 8.4 and References	2-Sep-2024	2-Oct-2024
2.0.9	SC78	Subject organizationName alignment for DBA / Assumed Name	2-Oct-2024	8-Nov-2024
2.1.0	SC76	Clarify and improve OCSP requirements	26-Sep-2024	14-Nov-2024
2.1.1	SC79	Allow more than one Certificate Policy in a Cross-Certified Subordinate CA Certificate	30-Sep-2024	14-Nov-2024
2.1.2	SC80	Strengthen WHOIS lookups and Sunset Methods 3.2.2.4.2 and 3.2.2.4.15	7-Nov-2024	16-Dec-2024
2.1.3	SC83	Winter 2024-2025 Cleanup Ballot	23-Jan-2025	24-Feb-2025
2.1.4	SC84	DNS Labeled with ACME Account ID Validation Method	28-Jan-2025	1-Mar-2025
2.1.5	SC81	Introduce Schedule of Reducing Validity and Data Reuse Periods	11-Apr-2025	16-May-2025
2.1.6	SC085v2	Require Validation of DNSSEC (when present) for CAA and DCV Lookups	19-Jun-2025	21-Jul-2025
2.1.7	SC089	Mass Revocation Planning	23-Jul-2025	25-Aug-2025
2.1.8	SC092	Sunset Precertificate Signing CAs	03-Oct-2025	04-Nov-2025
2.1.9	SC088	DNS TXT Record with Persistent Value DCV Method	09-Oct-2025	10-Nov-2025
2.2.0	SC086	Sunset the Inclusion of Address and Routing Parameter Area Names	2025-11-13	2026-12-15
2.2.1	SC091	(1) Sunset 3.2.2.5.3 Reverse Address Lookup Validation (2) new DNS-based validation using Persistent DCV TXT Record for IP addresses	2025-11-13	2026-12-16
2.2.2	SC090	Gradually sunset remaining email-based, phone-based, and 'crossover' validation methods	2025-11-20	2026-01-12
2.2.3	SC094	DNSSEC exception in email DCV methods	2026-01-15	2026-02-16
2.2.4	SC096	Carve-out for DNSSEC verification logging requirements	2026-01-14	2026-02-17
2.2.5	SC097	Sunset all remaining use of SHA-1 signatures in Certificates and CRLs	2026-02-24	2026-02-25
2.2.6	SC095	Clean-up 2025	2026-02-27	2026-03-31

2.2.7	SC099	Improve Recording of Validation Method	2026-04-18	2026-05-19