HiPKI 憑證政策

(HiPKI Certificate Policy)

第 1.15 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 02 月 22 日	首次發行
1.05	2020 年 3 月 2 日	(1) 依據 Baseline Requirements 第 1.6.7 版修訂第 1.5.2、第 3.2.5、第 4.2.1、第 4.9、第 6.2 及第 9.6 節。 (2) 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。 (3) 依據 Mozilla Root Store Policy 第 2.7 版修訂第 3.2.5 節有關電子郵件地址之控制權或所有權之確認方式與第 4.9 節有關安全電子郵件憑證之廢止規定。 (4) 修訂第 1.1、第 1.6、第 2.3、第 4.8.1、第 6.3.2、第 7.1.3、第 7.1.6、第 7.2.2、第 9.12.2 及第 9.16.1 節。
1.1	2021 年 4 月 13 日	(1) 依據 BR 修訂第 5.5.2 節。 (2) 修訂第 1.1、第 1.4.1、第 1.4.2、第 1.6.1、第 2.3、第 2.4、第 3.2.1、第 3.2.2、第 3.2.3、第 3.2.4、第 3.2.5、第 3.3.1、第 5.7.3、第 6.1.1、第 6.1.2、第 6.2.6、第 6.3、第 6.3.2、第 6.4.2、第 7.1.4、第 9.6.1、第 9.10、第 9.16.1 及第 9.16.5 節。
1.15	2021 年 6 月 17 日	(1) 配合 Google Chrome Root Program Transition，刪除個人、時戳、Code Signing 及 EV Code Signing 憑證等相關描述，使 HiPKI 成為一個純 TLS Root CA/PKI。 (2) 修訂第 1.1、第 1.2、第 1.3.6、第 1.4.1、第 1.6.1、第 1.6.2、第 3.1.2、第 3.1.3、第 3.2.1、第 3.2.2、第 3.2.3、第 3.2.4、第 3.2.5、第 3.3.1、第 4.1.1、第 4.2.1、第 4.4.1、第 4.5.2、第 4.6、第 4.9.1.1、第 4.9.6、第 4.9.7、第 5.4.3、第 5.4.8、第 6.1.7、第 6.2.2、第 6.2.4、第 6.3.2.2、第 6.6.1、第 8、第 8.1、第 9.5、第 9.6.1、第 9.6.3 及第 9.12.1 節。

1 序論

公開金鑰基礎建設(Public Key Infrastructure, PKI)是指由法律、政策、規範、人員、設備、設施、技術、流程、稽核和服務組成之集合，可用於管理憑證及金鑰對。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

本憑證政策(Certificate Policy, CP)係依據最新版之國內法規如：

(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 」

及最新版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)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；

(4) Mozilla Root Store Policy；

(5) Microsoft Trusted Root Program Requirements；

(6) Apple Root Certificate Program 及

(7) Google Root Certificate Policy

所訂定之政策文件，以做為本基礎建設各憑證機構訂定憑證實務作業基準(Certification Practice Statement, CPS)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，本憑證政策多數地方會以 TLS/SSL 憑證表示。

依照 ITU-T X.509 標準，本憑證政策所定義的保證等級(Assurance Level)必須以憑證政策物件識別碼(Object Identifier, OID，詳見第 1.2 節)表示，而這些憑證政策物件識別碼將會記載在憑證的憑證政策擴充欄位(certificatePolicies extension)中。

保證等級係指信賴憑證者(Relying Party)對於以下項目的信任程度：

(1) 憑證機構簽發之憑證，可分為兩種情形，如簽發憑證給終端個體(End Entities, EE)時，憑證政策物件識別碼代表該憑證申請時是依何種保證等級來做身分鑑別及簽發；如簽發憑證給憑證機構時，則該憑證機構的憑證(CA certificate)中可能會有 1 個以上的憑證政策物件識別碼，表示該憑證機構可以簽發符合憑證政策物件識別碼之保證等級的憑證給終端個體。

(2) 憑證之簽發與管理以及私密金鑰(Private Key)之傳送等憑證機構相關作業程序。

(3) 憑證中的用戶(Subscriber)或主體(Subject)是否能有效控管其憑證中所記載的公開金鑰成配對關係之私密金鑰，例如用戶使用軟體或硬體儲存其私密金鑰；亦即信賴憑證者能否確信憑證中所記載的主體與公開金鑰(Public Key)之連結關係(Binding)。

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(Interoperability)，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。

1.1.1 憑證政策

憑證政策是 1 種網路認證資訊科技(Information Technology)的指導原則(Guideline)，用來指明某一憑證所適用之對象或情況所列舉的 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。本基礎建設所使用的憑證政策物件識別碼，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。

HiPKI 憑證總管理中心(HiPKI Root Certification Authority, HiPKI RCA)的憑證是自簽憑證(Self-Signed Certificate)，也是本基礎建設的信賴起源，信賴憑證者應直接信賴 HiPKI RCA 的憑證。依照國際標準及慣例，HiPKI RCA 的憑證並無標示憑證政策物件識別碼，因應 HiPKI RCA 必須具備高公信力，以保證等級第 4 級運作。

1.1.2 憑證政策及憑證實務作業基準之關係

憑證政策用於說明有哪些保證等級可被放入憑證機構所簽發之憑證中，而憑證實務作業基準則說明如何達成所引用憑證政策之保證等級。每個簽發憑證之憑證機構都會有一本相對應的憑證實務作業基準。

1.1.3 憑證機構引用憑證政策物件識別碼

本基礎建設之憑證機構應遵循本憑證政策，不可自訂憑證政策。憑證機構引用本憑證政策之憑證政策物件識別碼必須經本公司同意，如對憑證政策有相關建議，可與本公司聯繫。

1.2 文件名稱及識別

本文件之名稱為 HiPKI 憑證政策(HiPKI Certificate Policy)，核定日期為 110 年 6 月 17 日，本憑證政策之最新版本可在以下網頁取得：https://eca.hinet.net。憑證機構簽發的憑證(不含自簽憑證)必須在憑證政策擴充欄位記載本憑證政策之物件識別碼。本基礎建設之憑證機構可簽發的憑證如下：

(1) 網域驗證(Domain Validation, DV)型 TLS/SSL 憑證

(2) 組織驗證(Organization Validation, OV)型 TLS/SSL 憑證

(3) 延伸驗證(Extended Validation, EV)型 TLS/SSL 憑證

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憑證政策提到的各類憑證及文件所設定之物件識別碼參照表：

物件名稱	物件識別碼
憑證政策	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
第 4 級	1 3 6 1 4 1 23459 200 0 4
Baseline Requirements	
網域驗證型 TLS/SSL 憑證	2.23.140.1.2.1
組織驗證型 TLS/SSL 憑證	2.23.140.1.2.2
EV SSL Certificate Guidelines	
延伸驗證型 TLS/SSL 憑證	2.23.140.1.1 (EV SSL Certificate Guidelines)

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。

若本憑證政策及憑證機構之憑證實務作業基準在 TLS/SSL 憑證簽發上與 Baseline Requirements 之規定有任何不一致的情形，將優先遵循 Baseline Requirements 的條款；若本憑證政策及憑證機構之憑證實務作業基準在延伸驗證型 TLS/SSL 憑證簽發上與 EV SSL Certificate Guidelines 之規定有任何不一致的情形，將優先遵循 EV

SSL Certificate Guidelines 的條款。

簽發網域驗證型 TLS/SSL 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，適用本憑證政策有關保證等級第 1 級之規範；簽發延伸驗證型及組織驗證型 TLS/SSL 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，適用本憑證政策有關保證等級第 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，一律適用本憑證政策有關保證等級第 4 級之規範。

1.3 主要成員

1.3.1 政策管理委員會

本公司特別設立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)以負責本公司對本基礎建設的管理工作，並確保此基礎建設的持續及正常運作。政策管理委員會的組成成員係依照政策管理委員會設置要點：由數據通信分公司總經理指派副總經理或相當層級擔任召集人 1 人，並指派 6 至 9 名委員，執行秘書 1 人由數據通信分公司資訊處處長兼任。工作任務說明如下：

(1) 授權及監督本基礎建設各憑證機構之金鑰產製。

(2) 審查本基礎建設之憑證政策。

(3) 審查本基礎建設之相關技術規範。

(4) 審查本基礎建設之憑證實務作業基準。

(5) 審查交互認證憑證機構(Cross-Certified CA)的互通申請。

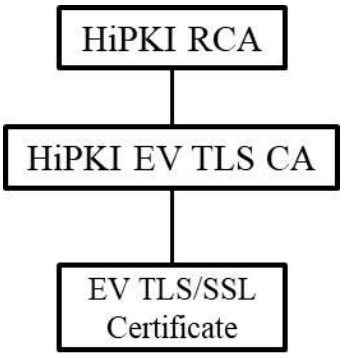
(6) 審查及核可加入本基礎建設或是與本基礎建設交互認證之根

憑證機構的憑證政策之對映關係。

(7) 監督交互認證之根憑證機構對於所允許憑證政策的遵照，以利互通機制持續運作。

1.3.2 憑證機構

本基礎建設是依照 ITU-T X.509 標準建置的階層式(Hierarchy)公開金鑰基礎建設，包括本基礎建設的信賴起源(Trust Anchor)－HiPKI RCA 及本公司所設立的下屬憑證機構(Subordinate CA)。目前本基礎建設僅包含 HiPKI EV TLS CA 一個下屬憑證機構，本基礎建設之架構如下所示：



1.3.2.1 HiPKI RCA

HiPKI RCA 為本基礎建設的根憑證機構(Root Certification Authority, Root CA)，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 HiPKI RCA 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) 將簽發的憑證機構廢止清冊(Certification Authority Revocation

List, CARL，詳見第 1.6.1 節)公布於儲存庫(Repository)，並且確保儲存庫之正常運作。

HiPKI RCA 應於憑證實務作業基準中訂定下屬憑證機構之識別與鑑別程序及外部憑證機構交互認證的程序。HiPKI RCA 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。

HiPKI RCA 之自簽憑證其憑證序號及憑證拇指紋等重要資訊如下：

(1) 第 1 代 HiPKI Root CA 自簽憑證

憑證序號：2d dd ac ce 62 97 94 a1 43 e8 b0 cd 76 6a 5e 60

憑證拇指紋(SHA-1)：6a 92 e4 a8 ee 1b ec 96 45 37 e3 29 57 49 cd 96 e3 e5 d2 60

憑證拇指紋(SHA-256)：f0 15 ce 3c c2 39 bf ef 06 4b e9 f1 d2 c4 17 e1 a0 26 4a 0a 94 be 1f 0c 8d 12 18 64 eb 69 49 cc

憑證效期：2019 年 2 月 22 日 至 2037 年 12 月 31 日

金鑰種類/金鑰長度：RSA 4096 with SHA-256

這些資訊會揭露於外稽報告與管理聲明書，並登錄於 Common CA Database (CCADB)，也會用於申請植入各大應用軟體供應商(Application Software Suppliers，如瀏覽器或作業系統廠商)之 CA 信賴清單。

1.3.2.2 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，必要時也可依階層式公開金鑰基礎建設的建

構方式，由第 1 層下屬憑證機構簽發憑證給第 2 層下屬憑證機構，或由第 2 層下屬憑證機構簽發憑證給第 3 層下屬憑證機構，依此類推而建構 1 個多層次的 PKI。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。

下屬憑證機構之建置應依照憑證政策相關規定，並設置聯絡窗口，負責與 HiPKI RCA 及其他下屬憑證機構之互運工作。

HiPKI EV TLS CA 之憑證機構憑證序號及憑證拇指紋等重要資訊如下：

(1) 第 1 代 HiPKI EV TLS CA 之憑證機構憑證

憑證序號：3c 43 cd cd dc f2 3b 00 4f 0e a0 73 fc 3e a3 89

憑證拇指紋(SHA-1)： 98 7e 11 0f a2 3e 88 82 89 47 65 19 47 2f 40 2f 1e 42 28 37

憑證拇指紋(SHA-256)：2a 8e 6a 86 e7 4d 10 ed b2 02 6c 81 69 3d 64 95 7a 0f 08 1c 16 31 91 2a c9 5e fd fc b5 62 56 57

憑證效期：2019 年 2 月 22 日 至 2037 年 12 月 31 日

金鑰種類/金鑰長度：RSA 4096 with SHA-256

這些資訊除於外稽報告與管理聲明書中揭露外，也登錄於 CCADB。

1.3.2.3 交互認證憑證機構

目前 HiPKI RCA 並無與任何本基礎建設以外之憑證機構進行交互認證。

1.3.3 註冊中心

註冊中心(Registration Authority, RA)主要負責蒐集及驗證用戶的身分、屬性及聯絡等相關資訊，以便於憑證機構之憑證簽發、廢止、金鑰更換、變更、展期、停用及復用等管理作業。

HiPKI RCA 自行擔任註冊中心角色，並依政策管理委員會核定之憑證實務作業基準執行註冊中心的工作。

下屬憑證機構則可另外設立註冊中心，並於憑證實務作業基準中規範其工作。下屬憑證機構之註冊中心可分為由下屬憑證機構所直接設立與維運，或由本公司簽約之客戶自行建置與維運。無論何種註冊中心都必須遵循本憑證政策與其憑證實務作業基準之規定運作。由本公司簽約之客戶自行建置與維運之註冊中心也可依照其內部需求與規定採用比本憑證政策或其所屬憑證機構之憑證實務作業基準更嚴格之安全控制實務。

1.3.4 用戶

用戶係指不具備憑證簽發能力之憑證主體，並擁有與憑證記載之公開金鑰相對應之私密金鑰的個體。在本憑證政策中並不稱根憑證機構、下屬憑證機構或交互認證憑證機構為用戶，因其具有憑證簽發之能力。

1.3.5 信賴憑證者

信賴憑證者係指相信憑證之主體名稱與某公開金鑰連結關係的個體。信賴憑證者必須依據憑證機構之憑證狀態資訊，檢驗所收到憑證的有效性。

信賴憑證者可使用憑證來驗證數位簽章訊息的完整性、確認發送訊息者的身分，及建立與用戶間的秘密通訊管道。同時，信賴憑證者

也可使用憑證中的訊息(例如憑證政策物件識別碼)，檢視此憑證的使用時機是否適當。

1.3.6 其他相關成員

憑證機構可選擇其他相關提供信賴服務的機構做為協同運作的夥伴，例如稽核機構或資料存證服務機構(Data Archiving Service Authority)等，並應在憑證實務作業基準中訂定相互運作機制及彼此的權利與義務關係，以確保憑證機構服務品質的有效及可靠。

1.4 憑證用途

憑證機構應審慎評估各種風險、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 憑證之適用範圍

本憑證政策對於 TLS/SSL 憑證，其適用範圍之說明如下：

憑證類別	適用範圍
網域驗證型	• 純粹只提供通訊管道之加密及保護(通訊管道之加密是指「促成加密金鑰之交換以達到用戶之瀏覽器和網站之間資訊傳遞的加密」) • 適合下列應用範圍： (1) 為發生惡意行為機率較低的非金錢或非財產交易之環境提供一般認證
組織驗證型	• 通訊管道之加密及保護 • 鑑別網域名稱擁有者屬於哪一個組織 • 適合下列應用範圍： (1) 電子商務交易 (2) 電子化政府 (3) 發生惡意行為機率為中等之環境

延伸驗證型	• 通訊管道之加密及保護 • 鑑別網域名稱擁有者屬於哪一個組織 • 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 • 適合下列應用範圍： (1) 電子商務交易 (2) 電子化政府

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

本基礎建設之憑證機構簽發的憑證禁止使用於以下範圍：

(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 憑證政策之管理機構

中華電信股份有限公司。

1.5.2 聯絡資料

1.5.2.1 憑證政策建議

如對本憑證政策有任何建議，請利用以下資訊與本公司聯繫。

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 憑證總管理中心

電子郵件信箱：caservice@cht.com.tw

也可至 https://eca.hinet.net 查詢聯絡資料。

1.5.2.2 憑證問題報告

憑證機構應於憑證政策實務作業基準敘明憑證問題報告(Certificate Problem Report)之聯絡窗口。

1.5.3 憑證實務作業基準之審定

憑證機構應先自行檢查憑證實務作業基準是否符合憑證政策相關規定後，再送政策管理委員會進行審查及核定。在核定後憑證機構便可正式引用本基礎建設的憑證政策。

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。

本公司對於憑證機構是否遵循憑證政策，具有稽核的權利(依照第 8 章之規定)，憑證機構也應定期自行稽核，以證明遵照引用於本憑證政策的保證等級進行營運。

為使本基礎建設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外稽原則，本基礎建設之憑證機構必須每年提供最新之憑證實務作業基準與外部稽核的結果。

1.5.4 憑證實務作業基準核准程序

憑證機構之憑證實務作業基準必須遵循相關法律及符合本憑證政策規定，並經政策管理委員及電子簽章法主管機關經濟部核定。如本憑證政策修訂公布後，憑證機構之憑證實務作業基準應配合修訂，並送交政策管理委員會及經濟部核定。

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 (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 2

	條第 1 款]
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 2 條第 2 款]
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)	當某個體出示身分時，確認其身分之正確性。
鑑別程序 (Authentication)	(1)建立使用者到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)鑑別是身分的證明程序。 [A Guide to Understanding Identification and Authentication in Trusted Systems] 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 (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：線上憑證狀態協定的服務位址，以及簽發憑證機構之憑證驗證路徑的下載位址等。
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(FQDN)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。
連結、繫結 (Binding)	將兩個相關的資訊元素做連結(結合)的過程。
生物特徵值(Biometric)	人的身體或行為的特徵。
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。
能力成熟度模型整合 (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 (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，內容至少包括： 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. 簽發憑證機構之數位簽章 在本憑證政策中所提及的「憑證」特別指其格式為 X.509 v3，且在其「憑證政策」欄位中明確地引用本憑證政策之物件識別碼的憑證。
憑證遞件核准者 (Certificate Approver)	憑證遞件核准者應為自然人，屬申請人、申請人所聘雇之員工，或有權代表申請人進行意

	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延伸驗證型 TLS/SSL 伺服器憑證申請。
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(或憑證機構廢止清冊)。
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 (Certification Authority Revocation List, CARL)	可供信賴憑證者查詢用之已廢止憑證清冊，該清冊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 (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] (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	(1)由憑證機構對外公告，用以陳述憑證機構

(Certification Practice Statement, CPS)	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、展期及金鑰更換等)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 (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。
憑證金鑰更換 (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 (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。
憑證廢止 (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 (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(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	1 組織，其設立目的為：研議中華電信所經營之公開基礎建設其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

Policy Management Authority，簡稱政策管理委員會)	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 (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。
合約簽署者 (Contract Signer)	申請人、申請人所聘雇之員工、有權代表申請人進行意思表示之授權代理人，或有權代表申請人簽署購買協議的自然人。
交互憑證 (Cross-Certificate)	在兩個根憑證機構(Root CA)之間建立信賴關係的 1 種憑證，屬於 1 種憑證機構憑證，而非用戶憑證。
交互認證協議書 (Cross Certification Agreement, CCA)	根憑證機構與交互認證憑證機構就交互憑證機構申請加入該根憑證機構所在之公開金鑰基礎建設，所必須遵守之事項及個別責任義務歸屬的協議。
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)	保證資料從發文者產製完到被收文者接受都未遭竄改。
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 (Domain Name)	在網域名稱系統分配給一個節點(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(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)	將網域名稱轉換為 IP 位址的網路服務。
網域驗證(Domain Validation, DV)	TLS/SSL 憑證核發過程中，只會驗證用戶之網域擁有權或控制權，但並未識別及鑑別用戶之組織或個人身分。故連結安裝網域驗證型 TLS/SSL 憑證之網站，可提供 TLS 加密通道，但無法知道該網站之擁有者是誰。
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。
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 Validation, EV)	EV SSL Certificate Guidelines 所定義之驗證程序。
聯邦資訊處理標準 (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 (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)及網域名稱兩部分。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)。
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。
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。
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。
金鑰破解	私密金鑰被他人未經授權的使用或揭露。

(Key Compromise)	
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： (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。 (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。
(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)	公開金鑰密碼系統所提供的技術性證據以支援不可否認之安全服務。 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。
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之特別形式的識別碼，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 (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 (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。 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。 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。
組織驗證(Organization Validation, OV)	TLS/SSL 憑證核發過程中，除了驗證用戶之網域擁有權或控制權外，並且依照憑證的保證等級識別及鑑別用戶之組織或個人身分。故連結安裝組織驗證型 TLS/SSL 憑證之網站，可提供 TLS 加密通道，知道該網站之擁有者屬於哪一個組織，並確保資料傳遞之完整性。

特殊安全管道 (Out-of-Band)	不同於現有之線上通訊方式，例如使用實體掛號信與他人進行通訊，此一方式可視為一種特殊安全管道。
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性的金鑰。 (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 (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。
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。
信賴憑證者 (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 (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] (2)包含本憑證政策與憑證相關資訊的資料庫。
徵求修正意見書 (Request for	由 IETF 發行的一系列備忘錄，包含網際網路、UNIX 及網際網路社群之標準、協定及程序

Comments, RFC)	等，並以編號排定。
保留 IP 位址(Reserved IP Addresses)	IANA 設定 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。
根憑證機構 (Root Certification Authority, Root CA)	一個公開金鑰基礎建設中最頂層的憑證機構，負責簽發下屬憑證機構憑證及自簽憑證，也稱為憑證總管理中心。
安全插座層 (Secure Sockets Layer, SSL)	網景公司(Netscape)推出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。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 及 Telnet 等)能直接地建置於 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。
自發憑證 (Self-Issued Certificate)	自發憑證為根憑證機構更換金鑰或憑證政策需要時所簽發之憑證，由兩代(新與舊代)根憑證機構使用其私密金鑰相互簽發，用以建立新舊金鑰間或憑證政策互通時憑證信賴路徑之用。
自簽憑證 (Self-Signed Certificate)	(1)自簽憑證係指憑證的簽發者名稱與憑證的主體名稱相同的一種憑證。亦即使用同一對金鑰對的私密金鑰針對其成配對關係的公開金鑰與其他資訊所簽發的憑證。 (2)一個公開金鑰基礎建設內的自簽憑證可做為憑證信賴路徑的起源，其簽發對象為根憑證機構本身。 (3)可供信賴憑證者用於驗證根憑證機構簽發之自發憑證、下屬憑證機構憑證、交互憑證以及憑證機構廢止清冊的數位簽章。

主體憑證機構 (Subject CA)	對於 1 張憑證機構憑證而言，該憑證的主體中所指的憑證機構即稱為該憑證的主體憑證機構。
下屬憑證機構 (Subordinate CA)	在階層式架構的公開金鑰基礎建設中，憑證由另 1 個憑證機構(上層憑證機構)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) 憑證中所敘明之主體名稱 (b) 擁有與憑證中所載公開金鑰相對應之私密金鑰 (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 (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定時間之存在。
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 (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。

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]
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。
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。[FIPS 140-2]

1.6.2 縮寫

英文縮寫	英文全稱	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
CARL	Certification Authority Revocation List	憑證機構廢止清冊，參見第 1.6.1 節
CCA	Cross-Certification Agreement	交互認證協議書，參見第 1.6.1 節
CMMI	Capability Maturity Model Integration	能力成熟度模型整合，參見第 1.6.1 節
CP	Certificate Policy	憑證政策，參見第 1.6.1 節
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
DV	Domain Validation	網域驗證，參見第 1.6.1 節
EE	End Entities	終端個體
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
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 Protocol	線上憑證狀態協定
OID	Object Identifier	物件識別碼，參見第 1.6.1 節
OV	Organization Validation	組織驗證，參見第 1.6.1 節
PIN	Personal Identification Number	個人識別碼
PKCS	Public Key Cryptography	公開金鑰密碼學標準，參

	Standards	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

2 公布及儲存庫之責任

2.1 儲存庫

儲存庫提供各憑證機構所簽發的憑證、憑證廢止清冊(Certificate Revocation List, CRL)及憑證狀態等資訊的查詢及下載服務，並公布憑證政策及憑證實務作業基準等憑證簽發及管理作業相關資訊。

儲存庫可由憑證機構或其他機構營運，1 個憑證機構不限定只有 1 個儲存庫，但必須至少有 1 個主要對外服務的儲存庫，憑證機構應在憑證實務作業基準中敘明儲存庫之相關資訊，並確保儲存庫之可用性、適當的存取控制及資料完整性。

2.2 憑證機構之資訊公布

憑證機構應負責將以下之資訊公布於其儲存庫：

(1) 憑證政策及憑證實務作業基準

(2) 憑證廢止資訊

(3) 憑證機構本身之憑證(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) 簽發之所有憑證(包括簽發給其他憑證機構之憑證)

(5) 憑證機構廢止清冊

(6) 隱私權保護政策

(7) 最近 1 次之外部稽核結果

(8) 相關最新消息

除上述資訊外，憑證機構應公布可驗證數位簽章之必要資訊。憑證機構之憑證實務作業基準應敘明儲存庫暫停服務時間之上限。憑證機構應於憑證實務作業基準敘明公布及通知之規定。

本基礎建設下簽發 TLS/SSL 憑證的下屬憑證機構應於其憑證實務作業基準載明其 CAA Issuer Domain Name。

2.3 公布之時間或頻率

憑證廢止清冊之公布頻率請依照第 4.9.7 節規定。本憑證政策應每年進行檢視及更新，本憑證政策新版或修訂後之版本應於政策管理委員會核准後儘速於憑證機構之儲存庫公告。憑證機構應於收到主管機關之憑證實務作業基準核准公文後儘速將新版或修訂版本之憑證實務作業基準公布於儲存庫。

2.4 儲存庫之存取控制

(1) 憑證政策與憑證機構之憑證實務作業基準的取得只做寫入存取控制。

(2) 憑證由憑證機構自行決定是否需存取控制。

(3) 憑證機構應保護儲存庫的資訊，以防止被惡意的公開散播或修改。公鑰憑證及憑證狀態資訊應經由網際網路公開取得。

3 識別及鑑別

3.1 命名

3.1.1 命名種類

本基礎建設的憑證之主體名稱應為 ITU-T X.500 的唯一識別名稱 (Distinguished Name, DN)。

申請憑證時，憑證機構有權決定是否接受憑證主體別名(Subject Alternative Name)，如憑證機構要求在憑證中附加憑證主體別名時，則該擴充欄位必須標示為非關鍵性的擴充欄位。

3.1.2 命名須有意義

組織驗證型或延伸驗證型 TLS/SSL 憑證的主體名稱必須包含該設備或伺服軟體之擁有組織的名稱，其命名應符合申請組織管轄國家之法律規定。

依照憑證機構與瀏覽器論壇之規範，伺服軟體憑證之主體名稱及憑證主體別名不得使用內部名稱(Internal Name)或保留 IP 位址 (Reserved IP Addresses)。

3.1.3 用戶之匿名或假名

網域驗證型 TLS/SSL 憑證，因主體名稱沒有記載組織或個人資訊，可視為一種匿名憑證。下屬憑證機構只要符合 Baseline Requirements 與憑證格式剖繪，並確保命名空間的唯一性，就可簽發匿名憑證給終端用戶。

3.1.4 不同命名形式之解釋規則

命名形式之解釋規則由本公司負責建立，並包含在憑證格式剖繪中。

3.1.5 命名之獨特性

憑證的主體名稱在本基礎建設中必須具獨特性，本公司負責建立憑證機構使用 X.500 名稱空間(Name Space)相關規範，以確保名稱命名的獨特性，憑證機構應在憑證實務作業基準中敘明如何使用 X.500 名稱空間，同時對於同名的憑證在命名時如何確保主體名稱的獨特性。

命名所有權依中華民國相關法律規定之命名規則辦理(例如公司法)，憑證機構應於憑證實務作業基準中訂定命名爭議之解決程序。

本公司為本基礎建設命名爭議的仲裁機構。

3.1.6 商標之辨識、鑑別及角色

當憑證的主體名稱可能包含商標時，則其命名必須符合中華民國商標相關法規。

3.2 初始身分驗證

3.2.1 證明擁有私密金鑰之方式

憑證機構在憑證申請時，應驗證申請者擁有之私密金鑰與將記載於憑證中的公開金鑰成對。

不同的金鑰產製者必須採用不同的方法來證明擁有私密金鑰，憑證政策認可之證明方法只有以下 1 種方式：

■ 由用戶自行產製金鑰對時：

可由用戶使用私密金鑰產生 1 個簽章，並將該簽章依照第 6.1.3 節規定提供給憑證機構或註冊中心，由憑證機構或註冊中心使用用戶的公開金鑰驗證該簽章，以證明用戶擁有該私密金鑰。憑證政策允許使用其他安全程度相當的方法(例如 RFC 2510 或 RFC 2511 所列的各種方法)證明私密金鑰的擁有。

3.2.2 組織身分鑑別

組織身分鑑別之程序，依保證等級有不同之規定，如下表所列：

保證等級	組織身分鑑別之程序
第 1 級	(1) 可不做證件核對。 (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	(1) 可不做證件核對。 (2) 用戶提交組織資料，例如組織識別碼(如扣繳單位稅籍統一編號)、組織名稱等，應與憑證機構認可之資料進行比對。 (3) 不需臨櫃辦理。
第 3 級	組織身分鑑別分為以下 3 種情形： (1) 民間組織之身分鑑別 申請資料應包括組織名稱、所在地及代表人名稱等足以識別該組織之資料。民間組織必須提供註冊窗口正確且經主管機關或合法授權單位(例如法院)核發之相關證明文件影本(例如公司登記事項表、公司變更登記事項表、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))，憑證機構或註冊中心除需驗證申請資料及代表人身分的真實性外，並應驗證該代表人有權以該組織之名義申請憑證。申請時應由代表人親臨憑證機構或註冊中心辦理，如代表人無法親自臨櫃申請，得以委託書委任代理人代為臨櫃申請，並依第 3.2.3 節中保證等級第 3 級之規定鑑別代理人之身分。 民間組織如於申請憑證前已依法完成向主管機關設立登記程序或已於憑證機構、註冊中心或憑證機構信賴之機構或個人(例如公證人、本公司之專戶經理、專案經理或業務經理)完成符合上述規

保證等級	組織身分鑑別之程序
	定之臨櫃識別與鑑別程序，並留下登記或識別與鑑別之佐證資料(例如留下印鑑章圖記或由公證人或本公司之專戶經理、專案經理或業務經理在申請書上加蓋認證戳記等)，則憑證機構或註冊中心得允許該組織於申請憑證時出示佐證資料來取代上述識別與鑑別方式。憑證機構必須評估採信佐證資料之風險，確認其風險不會大於採用上述識別與鑑別程序之風險，且憑證機構或註冊中心必須具有鑑別佐證資料之能力時，才可以接受以佐證資料取代識別與鑑別方式申請憑證。 以上所稱民間組織係指法人團體、非法人團體或以上兩者之附屬組織。 (2) 政府機關(構)或單位之身分鑑別 政府機關(構)或單位比照前述民間組織之身分鑑別方式，或得以正式公文書申請憑證，而憑證機構或註冊中心必須確認該機關(構)或單位確實存在，並驗證公文書之真確性。 (3) 中華電信所屬組織之身分鑑別 中華電信所屬組織以紙本表單或電子表單申請憑證，註冊窗口必須確認該機構或單位確實存在及名稱之正確性，並驗證申請人有權代表該組織申請憑證。 此外，前述 3 類組織之憑證申請資料透過政府公開金鑰基礎建設核發之保證等級第 3 級憑證簽章時，代表人不需親臨辦理，憑證機構或註冊中心將驗證申請資料之數位簽章。 伺服器軟體憑證申請資料透過中華電信公開基礎建設(ePKI)核發之保證等級第 3 級組織憑證簽章時，代表人不需親臨辦理，憑證機構或註冊中心將驗證申請資料之數位簽章。
第 4 級	組織身分鑑別分為以下兩種情形：

保證等級	組織身分鑑別之程序
	(1) 民間組織之身分鑑別 申請資料應包括組織名稱、所在地及代表人名稱等足以識別該組織之資料。憑證機構或註冊中心除需驗證申請資料及代表人身分的真實性外，並應驗證該代表人有權以該組織之名義申請憑證。申請時應由代表人親臨憑證機構或註冊中心辦理。 以上所稱民間組織係指法人團體、非法人團體或以上兩者之附屬組織。 (2) 中華電信所屬組織之身分鑑別 中華電信所屬組織必須以正式公文書指派憑證機構或註冊中心可鑑別之個人，代表該機構或單位親臨憑證機構或註冊中心申請憑證，憑證機構或註冊中心應確認該機構或單位確實存在，並驗證公文書之真確性，並依第 3.2.3 節中保證等級第 4 級之規定鑑別代表該機構或單位之個人之身分
網域驗證型 TLS/SSL 憑證	適用本節針對保證等級第 1 級之規定。
組織驗證型 TLS/SSL 憑證	適用本節針對保證等級第 3 級之規定，且依情況可利用 Baseline Requirements 第 3.2.2.1 節中所述之可靠來源所提供之文件或與之通訊進行查證。
延伸驗證型 TLS/SSL 憑證	依照 EV SSL Certificate Guidelines 之程序辦理。

3.2.3 個人身分鑑別

本基礎建設下之憑證機構不核發憑證給個人。

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(憑證申請代表人或稱憑證聯絡人)與憑證之主體名稱有關連，進行憑證生命週期活動如憑證申請或廢止請求時，憑證機構應於憑證實務作業基準說明憑證機構或其註冊中心如何進行授權之確認(Validation of Authority)，確認該個人可代表憑證之主體，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主體(某組織或公司)，且得到授權代表該主體

(2) 藉由臨櫃面對面核對身分或其他可信賴的通訊方式確認該個人代表組織

下屬憑證機構應於憑證實務作業基準中描述所簽發之各類型TLS/SSL憑證授權之確認方式：

TLS/SSL憑證類型	授權之確認方式
網域驗證型TLS/SSL憑證	■ 依照Baseline Requirements之規定驗證用戶是否具備網域之擁有權或控制權。
組織驗證型TLS/SSL憑證	■ 依照Baseline Requirements之規定驗證用戶是否具備網域之擁有權或控制權。 ■ 依照Baseline Requirements及下屬憑證機構之憑證實務作業基準第3.2.2或第3.2.3節有關保證等級第3級之規定進行組織的身分之識別、鑑別及憑證申請代表人之授權確認。
延伸驗證型TLS/SSL憑證	■ 依照Baseline Requirements之規定驗證用戶是否具備網域之擁有權或控制權。 ■ 依照EV SSL Certificate Guidelines之規定執行組織身分之識別及鑑別，並執行合約簽署者(Contract Signer)及憑證遞件核准者(Certificate Approver)授權之確認。

3.2.6 互運之準則

憑證機構若有與其他根憑證機構進行交互認證，應於憑證機構實務作業基準中揭露相關資訊。

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，憑證機構應評估此來源的可靠性、正確性和對變更或偽造的抵抗性。憑證機構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) 資料提供者和資料蒐集的目的

(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

由憑證機構、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。

3.3 金鑰更換請求之識別及鑑別

3.3.1 例行性金鑰更換之識別及鑑別

憑證之金鑰更換係指簽發 1 張與舊憑證具有相同特徵及保證等級的新憑證，而新的憑證除有新的、不同的公開金鑰(對應新的、不同的私密金鑰)及不同的序號外，亦可能被指定不同的有效期限。

當下屬憑證機構更換金鑰對時，簽發下屬憑證機構憑證的憑證機構，應依照第 3.2 節規定進行識別及鑑別，簽發新的憑證給下屬憑證機構。

網域驗證型與組織驗證型 TLS/SSL 憑證依照 Baseline Requirements 及本憑證政策第 6.3.2.2 節之規定，金鑰更換之請求如與初始註冊時間間隔超過 398 天，則必須依照第 3.2 節重新辦理初始註冊。延伸驗證型 TLS/SSL 憑證之金鑰更換請求依照 EV SSL Certificate Guidelines 及本憑證政策第 6.3.2.2 節之規定，如與初始註冊時間間隔超過 398 天，必須重新辦理初始註冊。

3.3.2 憑證廢止後金鑰更換之識別及鑑別

憑證廢止後，新憑證的簽發應依照第 3.2 節規定，用戶必須重新辦理初始註冊程序。

3.4 憑證廢止請求之識別及鑑別

憑證機構或註冊中心必須對於憑證廢止申請進行識別及鑑別，憑證機構應依照第 4.9 節規定在憑證實務作業基準中敘明申請者之身分鑑別方式，以確認申請者為有權提出憑證廢止之申請者。

無論私密金鑰是否遭破解，皆可使用私密金鑰之簽章及欲廢止之憑證來鑑別憑證廢止申請者之身分。

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

HiPKI RCA 之憑證申請者包括 HiPKI RCA 本身及本公司所設立之下屬憑證機構或是本基礎建設外之根憑證機構。下屬憑證機構之憑證申請者僅包括組織(或授權代表人)。

電腦及通訊設備(如路由器、防火牆、負載平衡器等)或伺服軟體(如 Web Server 或 Application Server)因在法律上不具行為能力，必須由組織或個人以設備管理者的身分提出憑證申請。

4.1.2 註冊程序及責任

憑證機構負責確保憑證申請者之身分在憑證簽發前依據憑證政策與適用的憑證實務作業基準確認，憑證申請者要負責提供足夠充分與正確的資訊及身分證明文件給憑證機構或其註冊中心在憑證簽發前執行必要的身分識別及鑑別工作。接受憑證機構簽發憑證的用戶應負以下義務：

(1) 遵守第 3 及第 4 章規定程序。

(2) 正確地使用憑證。

(3) 妥善地保管及使用私密金鑰。

(4) 當私密金鑰被破解時，應立即通知憑證機構。

4.2 憑證申請之程序

憑證機構應在憑證實務作業基準中敘明有關初始註冊、憑證展期及憑證之金鑰更換等之申請程序、申辦地點或網址。

HiPKI RCA 可接受本公司所設立之憑證機構申請憑證，以成為本基礎建設之第 1 層下屬憑證機構，其申請程序由政策管理委員會另訂之。本基礎建設外之根憑證機構向 HiPKI RCA 申請交互憑證(Cross-Certificate)的程序由政策管理委員會另訂之。

本基礎建設中所有層級之下屬憑證機構，除非經其上層憑證機構之同意，否則不得接受其他憑證機構申請成為其下層憑證機構。HiPKI RCA 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與 HiPKI RCA 協商以決定是否承認 HiPKI RCA 簽發給其他根憑證機構的交互憑證。

4.2.1 執行識別及鑑別

簽發憑證機構必須確保系統及程序足以鑑別用戶身分以符合憑證政策與憑證實務作業基準之規定。初始註冊程序依照本憑證政策第 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。於申請過程中之聯繫以及由憑證申請者申請憑證時提供之資訊，必須由憑證機構與註冊中心依憑證政策及憑證實務作業基準之規定以安全及可被稽核之方式妥善保管。

憑證機構應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。

核發憑證前，對於註記在憑證之 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 規範之授權憑證機構簽發憑證(Certification Authority Authorization, CAA)網域名稱系統資源紀錄(DNS Resource

Record)。

本基礎建設的 CAA 發布者網域名稱(Issuer Domain Names)包括 pki.hinet.net、tls.hinet.net 及 eca.hinet.net。憑證機構應於憑證實務作業基準清楚指定當申請者之完全網域名稱於 CAA 紀錄屬於"issue"或"issuewild"狀態時，允許簽發 TLS/SSL 憑證的發布者網域名稱列表。

4.2.2 憑證申請之批准或拒絕

如果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，簽發憑證機構可以批准憑證之申請。若各項驗證身分的工作無法成功完成，憑證機構得以拒絕憑證之申請。

除因申請者之身分識別及鑑別之原因外，憑證機構得因其他原因不同意簽發憑證。簽發憑證機構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

在申請者提交的資料齊全且符合憑證政策及憑證實務作業基準的要求下，憑證機構及註冊中心應於合理時間內驗證完申請者之資料並完成憑證之核發。處理憑證申請之時間可記載於憑證實務作業基準、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

憑證機構簽發憑證應依照第 5.2 節及憑證實務作業基準的規定，由適當人員執行憑證簽發之相關任務，憑證簽發後憑證機構或註冊中心應以適當方式通知申請者。

HiPKI RCA 應在每個金鑰生命週期簽發 1 張自簽憑證以建立憑

證信賴起源；並得簽發數張自發憑證，以因應本身金鑰及憑證政策的更換。HiPKI RCA 的自簽憑證及自發憑證簽發前必須由政策管理委員會確認其內容，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。

HiPKI RCA 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 憑證機構對用戶之憑證簽發通知

本基礎建設內之憑證機構，應於憑證實務作業基準中敘明憑證簽發後通知申請者的方式。

憑證機構或註冊中心如不同意簽發憑證，應以適當方式通知憑證申請者，並明確告知不同意簽發的理由，並於憑證實務作業基準中敘明不同意簽發憑證之通知方式。

4.4 憑證接受

4.4.1 構成接受憑證之事由

以保證等級第 2 級(含)以上憑證運作或簽發 TLS/SSL 憑證之憑證機構，應經憑證申請者 1)預先審視將簽發之憑證內容；或 2)在簽發憑證後審視憑證內容，代表接受所簽發的憑證後，始得將簽發之憑證公布到儲存庫上並傳遞給憑證申請者。若憑證申請者審視將簽發之憑證內容後，拒絕接受所註記於憑證之資訊，則憑證不予簽發；若憑證申請者審視已經簽發之憑證內容後，拒絕接受所簽發的憑證，則憑證機構應廢止該憑證。

以保證等級第 2 級以上憑證運作或簽發 TLS/SSL 憑證之憑證機構，應於憑證實務作業基準中敘明以下事項：

(1)憑證申請者確認憑證接受或拒絕的方式。

(2)憑證申請者在決定接受憑證前應審視的憑證欄位。

(3)憑證申請者拒絕接受憑證之處理方式。

上述憑證申請者在決定接受憑證前應審視的憑證欄位，至少應包括憑證的主體名稱。憑證申請者在接受 TLS/SSL 憑證前尚須審視憑證之主體別名欄位。

憑證申請者拒絕接受憑證之處理方式，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訂定。

4.4.2 憑證機構對簽發憑證之發布

憑證機構的儲存庫服務應定期公布所簽發之憑證。註冊中心得與憑證機構協議將憑證透過註冊中心傳遞給用戶。

4.4.3 憑證機構對其他個體之憑證簽發通知

不做規定。

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

用戶金鑰對的產製應符合本憑證政策第 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之權力與能力，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)。用戶必須依據憑證所記載的憑證政策正確地使用憑證。

4.5.2 信賴憑證者公開金鑰及憑證之用途

信賴憑證者應使用符合 ITU-T X.509、IETF RFC、Baseline Requirements 或 EV SSL Certificate Guidelines 之相關標準或規範的軟體驗證憑證路徑中所有憑證之簽章完整性與特定欄位正確性，並透過憑證廢止清冊(或憑證機構廢止清冊)或線上憑證狀態協定(Online Certificate Status Protocol, OCSP)查詢服務確認所有憑證之有效性，其後始可使用憑證路徑中之 TLS/SSL 憑證鑑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。

此外，信賴憑證者也應檢驗簽發憑證機構憑證與 TLS/SSL 憑證之憑證政策，確認憑證之保證等級。

4.6 憑證展期

憑證機構的憑證不可展期；過期、停用、廢止之憑證不得展期。本基礎建設不提供 TLS/SSL 憑證之展期，請用戶重新產生金鑰對申請新憑證。

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

(1) 用戶之私密金鑰必須依照第 6.3.2 節規定定期更換。

(2) 金鑰更換包括但不限於以下的情況：

(a) 憑證因金鑰遭到破解而廢止

(b) 憑證到期，且其金鑰效期也過期

4.7.2 更換憑證金鑰之申請者

憑證機構可接受更換憑證金鑰之請求，只要是符合金鑰與憑證生命週期管理及負責保管該憑證相對應之私密金鑰的原本用戶或經授權之代表人。更換憑證金鑰所提供之憑證請求檔必須包含新的公開金鑰。

4.7.3 憑證金鑰更換之程序

憑證機構在處理金鑰更換時得要求憑證申請者提供額外之資訊或是重新驗證用戶之身分，包含先前曾驗證過之身分資訊，並透過適當的挑戰與回應機制進行身分鑑別。相關程序必須依照第 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

如第 4.3.2 節所述。

4.7.5 構成接受金鑰更換之憑證的事由

如第 4.4.1 節所述。

4.7.6 憑證機構對金鑰更換之憑證的發布

如第 4.4.2 節所述。

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，其記載資訊和舊的憑證有些許不同，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憑證到期日相同。

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

如第 4.2 節所述。

4.8.4 對用戶憑證變更之簽發通知

如第 4.3.2 節所述。

4.8.5 構成接受變更之憑證的事由

如第 4.4.1 節所述。

4.8.6 憑證機構對變更之憑證的發布

如第 4.4.2 節所述。

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 憑證廢止及停用

憑證機構應於憑證實務作業基準中敘明憑證廢止請求及憑證問題報告之受理及回應的機制，並依憑證應用範圍及服務品質決定是否提供憑證停用服務。

對於已過期之憑證，憑證機構得不受理該憑證之廢止或停用申請，亦得不將該憑證之廢止或停用資訊列入憑證廢止清冊(或憑證機構廢止清冊)中。但對於過期前被廢止或停用之憑證，憑證機構應將其廢止或停用資訊列入憑證廢止清冊(或憑證機構廢止清冊)中，待憑證效期到期或被恢復使用後始可移除。

4.9.1 憑證廢止之情況

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，並且不回溯授予授權；

(3) 憑證機構證實用戶之私密金鑰遭破解或疑似金鑰遭破解，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；或

(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 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受理註冊機構(Domain Name Registrar)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憑證政策或憑證實務作業基準之規定程序簽發時；

(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) 憑證政策或憑證實務作業基準所規定應廢止項目；或

(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，憑證機構應於 7 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；

(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) 憑證未依憑證機構之憑證政策或憑證實務作業基準之規定程序簽發時；

(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；或

(9) 憑證機構之憑證政策或憑證實務作業基準所規定應廢止項目

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

用戶或擁有私密金鑰的個體得於憑證有效期限內向簽發其憑證之憑證機構或註冊中心提出憑證廢止請求。用戶、信賴憑證者、應用軟體供應商及其他第三方可向憑證機構提出憑證問題報告告知合理之原因以廢止憑證。

4.9.3 憑證廢止之程序

憑證機構應於憑證實務作業基準中敘明 7 天 x 24 小時不中斷之

對憑證廢止及憑證問題報告的受理及回應機制。在收到憑證廢止申請或憑證問題報告後，憑證機構或註冊中心應依照第 4.9 節及憑證實務作業基準規定，對申請者進行身分識別及鑑別。

憑證機構應於憑證實務作業基準中敘明通知用戶有關是否廢止憑證之決策結果的方式，如同意憑證廢止申請或決定逕行廢止憑證，則憑證機構或註冊中心應依照第 5.2 節及憑證實務作業基準規定，由適當人員執行憑證廢止之相關任務。

4.9.4 憑證廢止請求之寬限期

用戶於憑證廢止事由已經確認後，應儘速提出憑證廢止申請。若憑證機構及註冊中心之私密金鑰疑似遭破解，必須在 1 小時內通報該事由給簽發其憑證的憑證機構。憑證機構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

憑證機構應於收到憑證憑證問題報告後 24 小時內，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回報者。

憑證機構應於其憑證實務作業基準敘明在接收到憑證廢止申請或憑證問題報告後，確認該憑證廢止請求是否成立之準則及程序，其處理期限依第 4.9.1 節所規定之合理的時間範圍來辦理。

4.9.6 信賴憑證者檢查憑證廢止之規定

信賴憑證者於使用憑證前須透過憑證廢止清冊(或憑證機構廢止清冊)或是線上憑證狀態協定查詢服務查驗憑證的狀態。同時也必須驗證憑證廢止清冊(或憑證機構廢止清冊)或是線上憑證狀態協定回應訊息的真偽、完整性及有效性。

憑證機構廢止清冊或憑證廢止清冊下載網址應可於憑證的憑證

廢止清冊發布點(CRL Distribution Point, CDP)擴充欄位中取得。信賴憑證者必須考量承擔的風險、責任及影響，自行決定間隔多久去取得新的憑證廢止資訊，相關義務依照第 9.6.4 節規定。

4.9.7 憑證廢止清冊之簽發頻率

簽發憑證廢止清冊(或憑證機構廢止清冊)前，憑證機構應檢查其內容，確認資訊之正確性。憑證廢止清冊(或憑證機構廢止清冊)應定期發布，即使憑證狀態沒有改變也要簽發，以確保憑證狀態資訊的即時性。憑證狀態資訊之公告應在下一次憑證狀態資訊更新前完成，過時的憑證狀態資訊應自儲存庫中移除。下表說明憑證機構廢止清冊及憑證廢止清冊之簽發頻率相關規定。

保證等級	憑證機構廢止清冊之簽發頻率	憑證廢止清冊之簽發頻率
第 1 級	不適用	每 7 天至少 1 次
第 2 級	不適用	每 3 天至少 1 次
第 3 級	不適用	每天至少 1 次
第 4 級	每天至少 1 次	每天至少 1 次

4.9.8 憑證廢止清冊發布之最大延遲時間

憑證機構最遲應在憑證廢止清冊(或憑證機構廢止清冊)所記載之下次更新時間(nextUpdate)前將憑證廢止清冊(或憑證機構廢止清冊)公布於儲存庫上。

4.9.9 線上憑證廢止及狀態查驗之可用性

憑證機構應提供憑證廢止清冊(或憑證機構廢止清冊)，進行憑證狀態查驗，憑證機構應於憑證實務作業基準中敘明是否提供線上憑證

狀態協定查詢服務；若提供時，則其線上憑證狀態協定查詢服務須符合 RFC 6960 與 RFC 5019 的規範。

4.9.10 線上憑證廢止查驗之規定

憑證機構除提供憑證廢止清冊(或憑證機構廢止清冊)服務外，得選擇性地提供信賴憑證者線上憑證狀態協定查詢服務進行憑證狀態的確認。信賴憑證者若使用憑證機構所提供之線上憑證狀態協定查詢服務，則可不需取得或處理該憑證機構所公告之憑證廢止清冊(或憑證機構廢止清冊)。

憑證機構若有提供線上憑證狀態協定查詢服務，則該服務應支援符合 RFC 6960 與 RFC 5019 標準規範所述之 HTTP-based 的 GET 或 POST 方法，並於憑證實務作業基準中敘明線上憑證狀態協定查詢服務更新憑證狀態之頻率與其接收到線上憑證狀態協定查詢封包後之回覆規則。

4.9.11 廢止公告之其他發布形式

簽發 TLS/SSL 憑證之憑證機構應支援線上憑證狀態協定裝訂(OCSP Stapling)運作。

憑證機構可使用其他發布形式進行憑證廢止公告，替代方法必須滿足以下規定：

(1) 替代方法應敘明於憑證機構已被核准之憑證實務作業基準中
(2) 替代方法應提供與將廢止憑證之保證等級相當之鑑別與完整度服務
(3) 替代方法應滿足第 4.9.7 及第 4.9.8 節對於憑證廢止清冊之簽發及延遲的規定

4.9.12 金鑰被破解時之特殊規定

依照第 4.9.1、第 4.9.2 及第 4.9.3 節之相關規定辦理。

4.9.13 憑證停用之情況

依照 Baseline Requirements 第 4.9.13 節之規定，不得提供 TLS/SSL 憑證停用之服務。憑證機構應於憑證實務作業基準中敘明是否提供憑證停用及復用之服務。

4.9.14 憑證停用之申請者

針對 TLS/SSL 憑證不適用。

4.9.15 憑證停用之程序

針對 TLS/SSL 憑證不適用。

4.9.16 憑證停用期間之限制

針對 TLS/SSL 憑證不適用。

4.10 憑證狀態服務

4.10.1 操作特性

憑證機構應提供憑證廢止清冊(或憑證機構廢止清冊)或線上憑證狀態協定查詢服務，亦或兩者皆提供的憑證狀態服務。公告的憑證狀態資訊應包括廢止與停用的憑證，待廢止憑證效期到期或停用憑證被恢復使用後始可加以移除。

4.10.2 服務可用性

憑證機構應提供 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。

憑證機構應提供 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

訂購終止是指憑證用戶終止使用憑證機構的服務，憑證機構應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

憑證機構之私密金鑰及用戶之簽章用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

憑證機構若有支援會議金鑰(Session Key)之封裝及回復(Encapsulation and Recovery)應於其憑證實務作業基準描述其實務做法。

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

憑證機構之機房的實體所在及結構，必須符合儲存高重要性及敏感性資料的機房設施水準，結合門禁、保全、入侵偵測及監視錄影等實體安全機制，以防止未經授權存取憑證機構之相關設備。

5.1.2 實體存取

憑證機構在安裝及啟用密碼模組後，必須對憑證機構的設備進行實體控管，以防止遭受未經授權之存取。即使在沒有安裝或啟動密碼模組時，亦應對憑證機構的相關設備進行實體控管，以降低設備遭受非法開啟或破壞的風險。各保證等級之實體控管規定說明如下：

- 保證等級第 1 及第 2 級：
  (1) 確保能防止未經授權之侵入
  (2) 確保包含敏感性明文資料之可攜式儲存媒體及文件是保存在安全的場所
- 保證等級第 3 及第 4 級：
  (1) 建置全天候人工或電子式監控設備，防止未經授權之侵入
  (2) 定期維護及檢視存取記錄檔
  (3) 進行電腦系統及密碼模組實體控管時，必須至少兩人以上共同執行

HiPKI RCA 因為必須簽發所有保證等級憑證，因此憑證機構設置之場所的安全機制應比照保證等級第 4 級運作的實體控管規定。

在離開憑證機構機房時，應查驗以下事項以防止憑證機構機房被

未經許可人員接近：

(1)必須適當地保全安全機箱。

(2)實體安全系統(例如門鎖或出入門禁)運作正常。

5.1.3 電力及空調

憑證機構之電力及空調設備必須具備足夠的備援設施，如不斷電系統(Uninterrupted Power System, UPS)，支援憑證機構的相關系統運作，以因應外在因素所引起之不正常關機。同時，不斷電系統必須提供至少 6 小時以上之備用電力，以供儲存庫備援資料(包括已簽發憑證及憑證廢止清冊(或憑證機構廢止清冊))。

5.1.4 水災防範

憑證機構設備之設置地點必須免於受到水災損害。

5.1.5 火災防範及保護

憑證機構之機房必須具備自動偵測火災預警功能，系統能自動啟動滅火設備，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操作。

5.1.6 媒體儲存

憑證機構必須保護系統相關的儲存媒體免於遭受意外的損害(如水、火、電磁場等)。

5.1.7 廢料處理

不做規定。

5.1.8 異地備援

憑證機構應於憑證實務作業基準敘明有無異地備援、備援的地點與憑證機構主機房之距離以及備援的項目。

5.2 程序控管

5.2.1 信賴角色

憑證機構及註冊中心必須安排信賴角色負責執行相關任務，以作為憑證機構信賴的基礎，如因意外或人為疏失而未能達到安全目標，則可能降低憑證機構及註冊中心的公正性。憑證機構可採用以下兩種方法增加安全性：

(1) 保證擔任每種角色的人員已接受適當訓練且可充分信賴。

(2) 適當的區隔任務，同一任務分派給 1 人以上，以防止單獨 1 個人有機執行惡意活動。

規定之信賴角色如下：

(1) 管理員：安裝、設定和維護憑證機構軟體，包括系統及用戶帳號、稽核參數及產生元件金鑰。

(2) 簽發員：啟動/停止硬體密碼模組之憑證簽發/廢止服務。

(3) 稽核員：查驗與維護稽核日誌及執行內部稽核。

(4) 維運員：執行系統備份和故障排除。

(5) 實體安全控管員：實體安全控管。

(6) 網路安全專員：網路及網路設備之安全防護。

(7) 防毒防駭專員：提供防毒防駭、防惡意軟體等威脅之技術或措施。

(8) 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。

5.2.2 每項任務所需之人數

每項任務所需的人數應在憑證實務作業基準中說明。

5.2.3 識別及鑑別每個角色

除以保證等級第 1 級運作之憑證機構不做規定外，以保證等級第 2 級以上運作之憑證機構其相關人員在執行角色分派任務前，必須識別和鑑別是否為本人。

5.2.4 需要職責分離之角色

為確保憑證機構設備及維運之安全性達到最佳化，憑證機構之角色需要進行職責分離的規定如下：

保證等級	規定
第1級	不做規定。
第2級	憑證機構之相關人員應依第5.2.1節規定指定擔任信賴角色，但必須符合以下規定： (1) 管理員、簽發員、稽核員和網路安全專員不得相互兼任 (2) 管理員、簽發員、稽核員可兼任維運員 (3) 實體安全控管員不得兼任管理員、簽發員、稽核員及維運員 (4) 註冊審驗人員不得兼任管理員、稽核員及維運員 (5) 任何1個角色均不允許執行自我稽核功能。
第3級	同第2級之規定。
第4級	同第2級之規定。

5.3 人員控管

5.3.1 資格、經驗及清白規定

憑證機構於正職員工或是約聘人員任職前，都必須對該人員之身分及可信度進行驗證。忠誠、正直和中華民國國民是遴選信賴角色人員的必備條件，人員的資格、遴選、監督及考核相關辦法應在憑證實務作業基準中說明。

5.3.2 背景調查程序

憑證機構應於憑證實務作業基準中載明背景之調查程序。

5.3.3 教育訓練規定

憑證機構有義務提供相關人員以下之技能訓練：

(1) 公開金鑰基礎架構基本知識

(2) 憑證政策或憑證實務作業基準中載明之鑑別及審驗程序

(3) 憑證申請資訊驗證過程常見之威脅，包含釣魚或其他社交工程手法

(4) 災後復原及業務永續經營之程序

(5) 憑證機構及註冊中心之安全認證機制

(6) Baseline Requirements (只針對簽發 TLS/SSL 憑證之憑證機構)

憑證機構應要求註冊審驗人員通過憑證機構所提供有關 Baseline Requirements 對於資訊驗證規定之測驗，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。憑證機構應以文件證明註冊審驗人員具備某項任務所需之技能。

5.3.4 人員再教育訓練之頻率及規定

擔任信賴角色之相關人員必須熟悉憑證機構相關工作程序及法規的改變，在任何重大變動時，例如憑證機構的軟體或硬體升級、工作程序改變及設備更換等，必須再接受教育訓練並記錄受訓情形。

新進人員也必須比照辦理，憑證機構必須每年檢視相關人員之受訓情形。

5.3.5 工作輪調之頻率及順序

不做規定。

5.3.6 未授權行為之裁罰

憑證機構應訂定適當的管理辦法，以防止人員未經授權存取或不恰當之行為，並將相關規定公布在憑證實務作業基準中。對於違反憑證政策或憑證實務作業基準相關規定的人員，憑證機構必須採取適當的管理及懲處。

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

憑證機構必須提供憑證政策、憑證實務作業基準及其他規定、契約等相關必要之文件給憑證機構和註冊中心相關人員。

5.4 稽核紀錄程序

5.4.1 被記錄事件種類

憑證機構之稽核紀錄應包括憑證管理系統及憑證管理系統所依存的作業系統(Operating System)。每筆稽核記錄至少應包括以下項目：

(1) 事件種類(CA 金鑰生命週期管理、CA 與用戶憑證生命週期管理或安全相關)

(2) 引起事件的個體和/或操作者之身分

(3) 事件所針對之目標的身分

(4) 事件發生之時間和日期

(5) 事件發生之原因

(6) 憑證機構執行憑證簽發及廢止程序之結果記錄(不論成功或失

敗)

稽核紀錄應儘可能由系統自動產生，如無法由系統自動產生，亦可使用工作記錄本、紙張或其他實體機制，當事件發生時，稽核紀錄可由憑證機構自行決定以電子或實體方式記錄。下表說明依各保證等級運作之憑證機構應記錄的稽核事件，由於這些稽核事件都是需要憑證機構加以記錄或加以回應處理的，所以又被稱為可稽核事件(Auditable Event)：

可稽核事件／保證等級	第 1 級	第 2 級	第 3 級	第 4 級
A.1 安全稽核				
A.1.1 任何重要稽核參數之改變，如稽核頻率、稽核事件型態及新舊參數的內容等		✓	✓	✓
A.1.2 任何嘗試刪除或修改稽核紀錄檔		✓	✓	✓
A.2 識別與鑑別				
A.2.1 嘗試新角色的設定不論成功或失敗		✓	✓	✓
A.2.2 身分鑑別嘗試的最高容忍次數改變		✓	✓	✓
A.2.3 使用者登入系統時身分鑑別嘗試的失敗次數之最大值		✓	✓	✓
A.2.4 管理者將已被鎖住的帳號解鎖，而且該帳號是因為多次失敗的身分鑑別嘗試而被鎖住的		✓	✓	✓
A.2.5 管理者改變系統的身分鑑別機制，例如從通行碼改為生物特徵值		✓	✓	✓

可稽核事件／保證等級	第 1 級	第 2 級	第 3 級	第 4 級
A.3 金鑰之產製				
A.3.1 當憑證機構產製金鑰時(不限制在單次或只限一次使用的金鑰產生)	✓	✓	✓	✓
A.4 私密金鑰之載入和儲存				
A.4.1 載入私密金鑰到系統元件中	✓	✓	✓	✓
A.4.2 所有為進行金鑰回復工作，對保存在憑證機構之私密金鑰所做的存取	✓	✓	✓	✓
A.5 可信賴公開金鑰之新增、刪除及儲存				
A.5.1 所有可信賴公開金鑰之改變，包括新增及刪除	✓	✓	✓	✓
A.6 私密金鑰之匯出				
A.6.1 私密金鑰之匯出(不包括只使用在單次或只限一次使用之金鑰)	✓	✓	✓	✓
A.7 憑證註冊				
A.7.1 所有憑證之註冊申請過程	✓	✓	✓	✓
A.8 憑證廢止				
A.8.1 所有憑證之廢止申請過程		✓	✓	✓
A.9 憑證狀態改變之核可				
A.9.1 核可或拒絕憑證狀態改變之申請		✓	✓	✓
A.10 憑證機構之組態設定				
A.10.1 任何與憑證機構之組態設定改變		✓	✓	✓
A.11 帳號之管理				

可稽核事件／保證等級	第 1 級	第 2 級	第 3 級	第 4 級
A.11.1 加入或刪除角色和使用者	✓	✓	✓	✓
A.11.2 角色或使用者帳號之存取權限修改	✓	✓	✓	✓
A.12 憑證格式剖繪之管理				
A.12.1 任何憑證格式剖繪之改變	✓	✓	✓	✓
A.13 憑證機構廢止清冊及憑證廢止清冊格式剖繪之管理				
A.13.1 任何憑證機構廢止清冊或憑證廢止清冊格式剖繪之改變		✓	✓	✓
A.14 其他				
A.14.1 安裝作業系統		✓	✓	✓
A.14.2 安裝憑證機構系統		✓	✓	✓
A.14.3 安裝硬體密碼模組			✓	✓
A.14.4 移除硬體密碼模組			✓	✓
A.14.5 銷毀硬體密碼模組		✓	✓	✓
A.14.6 啟動系統		✓	✓	✓
A.14.7 嘗試登入憑證機構的應用程式		✓	✓	✓
A.14.8 硬體及軟體之接收			✓	✓
A.14.9 嘗試設定通行碼		✓	✓	✓
A.14.10 嘗試修改通行碼		✓	✓	✓
A.14.11 憑證機構之資料備份		✓	✓	✓
A.14.12 憑證機構之資料回復		✓	✓	✓
A.14.13 檔案操作(例如產生、重新命名及移動等)			✓	✓
A.14.14 傳送任何資訊到儲存庫			✓	✓
A.14.15 存取憑證機構之內部資			✓	✓

可稽核事件／保證等級	第 1 級	第 2 級	第 3 級	第 4 級
料庫				
A.14.16 憑證破解之通知		✓	✓	✓
A.14.17 憑證載入符記(Token)			✓	✓
A.14.18 符記之傳遞			✓	✓
A.14.19 符記之零值化		✓	✓	✓
A.14.20 憑證機構之金鑰更換	✓	✓	✓	✓
A.15 憑證機構之伺服器設定改變				
A.15.1 硬體		✓	✓	✓
A.15.2 軟體		✓	✓	✓
A.15.3 作業系統		✓	✓	✓
A.15.4 修補程式(Patches)		✓	✓	✓
A.15.5 安全格式剖繪			✓	✓
A.16 實體存取及場所之安全				
A.16.1 人員進出憑證機構之機房			✓	✓
A.16.2 存取憑證機構之伺服器			✓	✓
A.16.3 得知或懷疑違反實體安全規定		✓	✓	✓
A.17 異常				
A.17.1 軟體錯誤		✓	✓	✓
A.17.2 軟體完整性檢查失敗		✓	✓	✓
A.17.3 接收不合適訊息			✓	✓
A.17.4 非正常路由之訊息			✓	✓
A.17.5 網路攻擊(懷疑或確定)		✓	✓	✓
A.17.6 設備失效	✓	✓	✓	✓
A.17.7 電力不當			✓	✓
A.17.8 不斷電系統失敗			✓	✓

可稽核事件／保證等級	第 1 級	第 2 級	第 3 級	第 4 級
A.17.9 明顯及重大的網路服務或存取失敗			✓	✓
A.17.10 憑證政策之違反	✓	✓	✓	✓
A.17.11 憑證實務作業基準之違反	✓	✓	✓	✓
A.17.12 重設系統時鐘		✓	✓	✓

5.4.2 紀錄檔處理頻率

憑證機構應依據下表定期檢視稽核紀錄，並且在稽核報表中對重大事件加以解釋。檢視工作應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異常或不正常行為等。

保證等級	處理頻率
第 1 級	不做規定。
第 2 級	不做規定。
第 3 級	(1) 至少每兩個月 1 次。 (2) 憑證機構自上次稽核檢視後所發生的重大安全稽核紀錄應加以檢視。 (3) 憑證機構對任何確認之惡意活動應進一步調查，而因應稽核檢視之結果所採取的行動亦應以文件記錄。
第 4 級	(1) 至少每個月 1 次。 (2) 憑證機構自上次稽核檢視後所發生的重大安全稽核紀錄應加以檢視。 (3) 憑證機構對任何確認之惡意活動應進一步調查，而因應稽核檢視之結果所採取的行動亦應以文件記錄。

5.4.3 稽核紀錄檔保留期限

憑證機構其稽核紀錄檔之保留期限應依第 5.5.2 節之規定辦理。

稽核紀錄檔應在憑證機構所在處應至少保留兩個月，再移至適當場所儲存。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。當稽核紀錄檔的保留期限屆滿時，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

憑證機構應保護稽核紀錄在保留期限前不會遭未經授權的存取、修改及破壞。

5.4.5 稽核紀錄檔備份程序

保證等級	稽核記錄檔之備份程序
第1級	不做規定
第2級	稽核記錄檔應至少每月備份1次。
第3級	
第4級	稽核記錄檔應至少每月備份及異地(off-site)備援1次。異地備援相關程序應於憑證實務作業基準中規定。

5.4.6 稽核彙整系統

稽核彙整系統可以設置在憑證管理系統之內部或外部。稽核紀錄程序應在憑證管理系統啟動時啟用，唯有在憑證管理系統關閉時才停止。

5.4.7 對引起事件者之通知

不做規定。

5.4.8 弱點評估

簽發 TLS/SSL 憑證之憑證機構應遵照 WebTrust Principles and Criteria for Certification Authorities － SSL Baseline with Network Security(簡稱 WebTrust for CA－SSL BR)及 Network and Certificate System Security Requirements 規定之方式及頻率執行弱點評估及滲透測試。

5.5 紀錄歸檔

5.5.1 歸檔紀錄之種類

依各保證等級的安全需求，憑證機構應在歸檔時記錄以下資料。

應歸檔資料／保證等級	第 1 級	第 2 級	第 3 級	第 4 級
憑證機構被主管機關認證(Accreditation)的資料(假設適用)	✓	✓	✓	✓
憑證實務作業基準	✓	✓	✓	✓
重要契約	✓	✓	✓	✓
系統及設備組態設定	✓	✓	✓	✓
系統或組態設定修改及更新的內容	✓	✓	✓	✓
憑證申請資料	✓	✓	✓	✓
憑證廢止資料		✓	✓	✓
身分識別資料		✓	✓	✓
文件的簽收或憑證的接受		✓	✓	✓
符記啟用紀錄		✓	✓	✓
已簽發或公告的憑證	✓	✓	✓	✓
金鑰更換的紀錄	✓	✓	✓	✓

應歸檔資料／保證等級	第 1 級	第 2 級	第 3 級	第 4 級
已簽發或公告的憑證機構廢止清冊和憑證廢止清冊		✓	✓	✓
稽核記錄	✓	✓	✓	✓
用來驗證及佐證歸檔內容的其它說明資料或應用程式		✓	✓	✓
稽核人員所要求的文件		✓	✓	✓

5.5.2 歸檔資料保留期限

歸檔資料的最低保留期限依各保證等級規定如下：

保證等級	最低保留期限
第 1 級	2 年
第 2 級	2 年
第 3 級	2 年
第 4 級	20 年

如使用的儲存媒體無法達到上述的保留期限規定，則必須建立定期將歸檔資料轉換到新的儲存媒體之機制。同時用來處理歸檔資料的應用程式也必須被維護一定期間，直到歸檔資料被銷毀或轉換到新的儲存媒體。

5.5.3 歸檔資料之保護

憑證機構之歸檔資料必須儲存在憑證機構以外的地方，並提供適當的保護，保護等級不可低於憑證機構所在處之保護等級。

5.5.4 歸檔資料備份程序

不做規定。

5.5.5 記錄之時戳規定

不做規定。

5.5.6 歸檔資料彙整系統

不做規定。

5.5.7 取得及驗證歸檔資料之程序

憑證機構應於憑證實務作業基準中敘明取得及驗證歸檔資料之程序。

5.6 憑證機構之金鑰更換

憑證機構之私密金鑰必須依照第 6.3.2 節規定定期更換，以新私密金鑰取代舊私密金鑰簽發憑證，並應適時對信賴該憑證機構憑證的所有個體公告。

HiPKI RCA 最遲應於其私密金鑰簽發憑證機構憑證的使用期限到期前，更換金鑰對。HiPKI RCA 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，此 3 張新憑證的簽發程序依照第 4.3 節規定。

下層憑證機構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。下層憑證機構更換金鑰對後，應依照第 4.1 節規定向上層憑證機構申請新的憑證機構憑證，上層憑證機構必須於下層憑證機構憑證到期前，簽發並公告下層憑證機構的新憑證機構憑證。

與 HiPKI RCA 交互認證之本基礎建設外的根憑證機構，其金鑰更換時間由該憑證機構自行依其所遵循之憑證政策決定。該根憑證機構更換金鑰對後，是否需要繼續向 HiPKI RCA 申請交互憑證，則視該根憑證機構與本公司之協議或契約而定。若該根憑證機構需要繼續

向 HiPKI RCA 申請交互憑證，應依第 4.3 節規定辦理，並須保留足夠時間供政策管理委員會及 HiPKI RCA 處理其交互認證申請，以確保 HiPKI RCA 能夠在該根憑證機構之交互憑證過期前，簽發並公告該根憑證機構之新交互憑證。

若舊私密金鑰仍須簽發憑證廢止清冊(或憑證機構廢止清冊)或線上憑證狀態協定的回應，則維持及保護該舊私密金鑰至以舊私密金鑰簽發的所有用戶憑證到期為止。

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

憑證機構應訂定緊急事件及系統遭破解後之通報與處理程序，必要之文件包括事件回應計畫(Incident Response Plan)及持續營運計畫(Business Continuity Plan)，同時至少每年進行演練、審視及更新。

憑證機構應確保其事件回應計畫及持續營運計畫可於合格稽核業者執行外部稽核時取得。

5.7.2 電腦資源、軟體或資料遭破壞

憑證機構必須依據憑證政策及憑證實務作業基準規定定期做好各種備援措施，儘可能將電腦資源、軟體或資料遭破壞時之災害損失減至最低。在確認憑證機構系統的完整性後，憑證機構應優先恢復儲存庫，使憑證狀態資訊能正常提供。

以保證等級第 3 及第 4 級運作之憑證機構至少每年應進行 1 次電腦資源、軟體及資料遭破壞之復原程序演練。

5.7.3 憑證機構私密金鑰遭破解之處理程序

以保證等級第 2 級以上憑證運作之憑證機構，應在憑證實務作業

基準中敘明憑證機構之私密金鑰遭破解時之處理程序及採取之適當行動，以迅速恢復憑證之簽發及管理作業能力。

以保證等級第 3 及第 4 級運作之憑證機構至少每年應進行 1 次憑證機構私密金鑰遭破解之演練。

憑證機構私密金鑰遭破解時，應立即通知應用軟體供應商、用戶及信賴憑證者。

5.7.4 災變後業務持續營運能力

以保證等級第 2 級以上憑證運作之憑證機構應在憑證實務作業基準敘明在災變後，恢復憑證機構設施運作的步驟。

以保證等級第 3 及第 4 級運作之憑證機構至少每年應進行 1 次災變後復原計畫之演練。

5.8 憑證機構或註冊中心之終止

憑證機構應依據電子簽章法相關規定進行終止服務。

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

金鑰對產製應於符合 FIPS 140-2 規範之密碼模組內完成，採用之演算法及金鑰長度應依第 6.1.5 及第 6.1.6 節規定辦理。

如私密金鑰在密碼模組內產製，該金鑰應一直保存在該密碼模組中或加密儲存於主機中。如私密金鑰在密碼模組外產製，該金鑰應在不離開金鑰產製的環境下匯入密碼模組中，該環境應保證沒有人員可用任何方法，在不被偵測的情形下取得已經產製的私密金鑰，當私密金鑰儲存在密碼模組後，該金鑰應立即由金鑰產製的環境中刪除。

憑證機構應採取適當的措施來確保用戶的公開金鑰在該憑證機構所轄之公開金鑰基礎建設領域內是唯一的。

任何被用於金鑰產製的隨機亂數，必須經由本公司認可。用戶隨機亂數與金鑰對之產製，使用軟體或硬體之相關規定如下表所列：

保證等級	金鑰產製機制
第1級	軟體或硬體
第2級	軟體或硬體
第3級	軟體或硬體
第4級	只限硬體

6.1.2 私密金鑰傳送給用戶

如用戶私密金鑰由可信賴的第三者代為產製，則產製金鑰之個體必須透過密碼模組將私密金鑰安全地傳送至用戶手上，而用戶必須作收受私密金鑰的確認。當使用任何秘密共享的機制於私密金鑰啟用時，

如密碼或個人識別碼，則必須確保只有用戶及產製金鑰之個體是唯一擁有該秘密的個體。

產製金鑰之個體應進行以下工作：

(1) 保護私密金鑰在傳送的過程中不會被啟動、破解或竄改

(2) 私密金鑰在傳送給用戶後不應留有備份

(3) 確保將正確之符記及啟動資料傳送給正確之用戶

(4) 維護 1 份用戶確認收到符記的紀錄

(5) 密碼模組的存放位置及狀態之追溯紀錄必須被妥善保存，至少到用戶確認接受該密碼模組為止

如私密金鑰在用戶之密碼模組內被產製及儲存時，無需傳送其私密金鑰。

6.1.3 公開金鑰傳送給簽發憑證機構

用戶必須將其公開金鑰傳送給憑證機構以進行身分鑑別，傳送的方式包括：

(1) 由註冊中心代為發出憑證申請的電子訊息

(2) 由第三者產製金鑰時，憑證機構或註冊中心必須透過可稽核之安全管道，取得用戶之公開金鑰

(3) 其它安全的電子化機制

(4) 安全的非電子化方式，如經由掛號郵件或快遞傳送儲存用戶公開金鑰之媒體

6.1.4 憑證機構公開金鑰傳送給信賴憑證者

根憑證機構(HiPKI RCA)之公開金鑰必須隨時可被信賴憑證者取得，憑證機構必須以可信賴的方式將根憑證機構之自簽憑證或公開金鑰傳送給信賴憑證者，包括：

(1)憑證機構將根憑證機構之自簽憑證或公開金鑰以符記儲存，並以安全方式傳送至信賴憑證者。

(2)透過特殊安全的管道(Out-of-Band)傳送根憑證機構之自簽憑證或公開金鑰。

(3)透過特殊安全的管道(Out-of-Band)傳送根憑證機構之自簽憑證或公開金鑰之雜湊值或指紋，供使用者比對

(4)其他政策管理委員會核可之方式。

以上所述之特殊安全管道應在根憑證機構的憑證實務作業基準中說明。根憑證機構簽發的下屬憑證機構憑證須公布在其儲存庫中。

6.1.5 金鑰長度

本基礎建設內之憑證必須滿足以下演算法與金鑰長度之規定：

(1)根憑證機構之憑證

雜湊函數演算法	SHA-256、SHA-384或SHA-512
RSA模數最少位元數	4096
ECC演算法	NIST P-384

(2)下屬憑證機構之憑證

雜湊函數演算法	SHA-256、SHA-384或SHA-512
RSA模數最少位元數	4096
ECC演算法	NIST P-256或P-384

(3)用戶之憑證

雜湊函數演算法	SHA-256、SHA-384或SHA-512
RSA模數最少位元數	2048
ECC演算法	NIST P-256或P-384

6.1.6 公開金鑰參數之產製及品質檢驗

對於RSA演算法而言，公開金鑰參數必須為空的(Null)，且不必做參數品質的檢驗，但必須做質數的測試，憑證機構應於憑證實務作業基準中說明如何執行相關測試。

對於其他演算法而言，憑證機構應依相關國際標準(如NIST SP 800-89)進行公開金鑰參數的設定與參數品質的測試。

6.1.7 金鑰之使用目的

憑證機構本身憑證之金鑰用途擴充欄位至少須設定兩個金鑰用途位元，分別為cRLSign與keyCertSign。

憑證機構簽發之TLS/SSL憑證之金鑰用途擴充欄位須依其金鑰對產製所使用之演算法與金鑰用途設定所需之金鑰用途位元，但不可包含cRLSign與keyCertSign。

6.2 私密金鑰保護及密碼模組工程控管

憑證機構應提供實體與邏輯保護措施，以防止未經授權的憑證簽發。憑證機構之私密金鑰若存在於密碼模組之外，則其應採用實體安全機制、加密或兩者的結合等方式保護，避免憑證機構私密金鑰遭洩漏。憑證機構應使用具備防範密碼分析攻擊之演算法與金鑰長度來加密其私密金鑰。

6.2.1 密碼模組標準及控管

政策管理委員會應確認本基礎建設所使用的密碼模組之安全需求符合FIPS 140-2系列或安全強度相當的國際標準。

對於本基礎建設的各個個體，除了用戶必須盡可能遵照外，其餘

的個體應參照下表做為密碼模組的最低安全要求，亦可使用更高的安全等級，此表中所列的等級(Level)係參照FIPS 140-2系列的定義。

個體 / 保證等級	HiPKI RCA	下屬憑證機構	註冊中心	用戶
第1級	不適用	等級1 (硬體或軟體)	等級1 (硬體或軟體)	不做規定
第2級	不適用	等級2 (硬體)	等級1 (硬體或軟體)	等級1 (硬體或軟體)
第3級	不適用	等級3 (硬體)	等級2 (硬體)	等級1 (硬體或軟體)
第4級	等級3 (硬體)	等級3 (硬體)	等級2 (硬體)	等級2 (硬體)

6.2.2 私密金鑰分持之多人控管

憑證機構之簽章用私密金鑰必須符合第5章規定的多人控管程序。

6.2.3 私密金鑰託管

憑證機構與用戶簽章用之私密金鑰不可被託管(Escrow)。

6.2.4 私密金鑰備份

憑證機構之簽章用私密金鑰應在多人控管程序下進行備份，並保存在備援場所；金鑰備份的程序必須在憑證實務作業基準中說明。

6.2.5 私密金鑰歸檔

憑證機構與用戶簽章用私密金鑰不可以被歸檔。

6.2.6 私密金鑰匯入、匯出密碼模組

依照第6.1.1節規定產製金鑰後，憑證機構及其註冊中心不應允許

其私密金鑰於硬體密碼模組外以明文形式存在。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並匯入至備份專用之符記，亦或從備份專用之符記匯入至密碼模組，其過程應遵循第6.2.2節規定多人控管方式。私密金鑰從密碼模組匯出或於密碼模組間傳輸時，憑證機構及其註冊中心應使用加密或金鑰分持等方式保護，以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。

若上層憑證機構發現有下層憑證機構之私密金鑰洩漏給未授權人員或不屬於下層憑證機構之組織的情形，上層憑證機構應將與該私密金鑰相關之憑證廢止。

6.2.7 私密金鑰儲存於密碼模組

依照第6.1.1與第6.2.1節規定。

6.2.8 啟動私密金鑰之方式

儲存在密碼模組中的私密金鑰在啟動時必須對啟動者做身分鑑別，可接受的鑑別方式包含(但不限於)通行詞組(Pass-Phrase)、個人符記、個人識別碼或生物特徵值，但輸入的啟動資料必須避免被洩露(不應被顯示出來)。

已啟動的私密金鑰不應沒人看管或是容許未經授權的存取。

6.2.9 停用私密金鑰之方式

密碼模組不需要使用時必須停止運作；透過手動的登出程序，或經過一段時間沒有運作後(時間的長度在憑證實務作業基準中訂定)自動停止運作。如硬體密碼模組不再使用時，必須與主機分離並儲存至安全場所。

6.2.10 銷毀私密金鑰之方式

當簽章用私密金鑰及其備份不再需要或是憑證到期或被廢止時，此私密金鑰必須被銷毀。對於軟體密碼模組而言，必須將亂數資料複寫至原簽章用私密金鑰佔用的記憶體或儲存媒體；對於硬體密碼模組而言，必須執行零值化(Zeroize)動作，但不需做實體銷毀。

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

在憑證歸檔後，得不必再進行公開金鑰之歸檔。

6.3.2 憑證操作及金鑰對之效期

6.3.2.1 憑證機構憑證操作及金鑰對之效期

本基礎建設內之憑證機構的憑證及其私密金鑰之效期如下：

憑證機構	私密金鑰效期	憑證效期
根憑證機構	■ 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 ■ 簽發下屬憑證機構憑證：15年 ■ 簽發憑證機構廢止清冊、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：30年	30年
下屬憑證機構/交互認證憑證機構	■ 簽發終端個體憑證：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

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。

6.3.2.2 用戶憑證操作及金鑰對之效期

本基礎建設內之TLS/SSL憑證及其私密金鑰效期如下：

憑證類別	私密金鑰效期	憑證效期
網域驗證型TLS/SSL	不做規定	398天
組織驗證型TLS/SSL	不做規定	398天
延伸驗證型TLS/SSL	不做規定	398天

TLS/SSL憑證之有效期限不得超過其簽發憑證機構之憑證效期。

6.4 啟動資料

6.4.1 啟動資料之產生及安裝

憑證機構應產生足夠保護其私密金鑰之啟動資料，並交由適任之信賴角色人員管理。如果啟動資料必須傳送，其傳送方法必須保持啟動資料之機密性與完整性。

6.4.2 啟動資料之保護

用來啟動私密金鑰的啟動資料，必須使用結合密碼與存取控制機制加以保護，以防止揭露。若啟動私密金鑰時之啟動資料須記錄留存，則該紀錄須使用具有不可偽造與竄改之密碼機制保護，確保其資料完整性。若登入的失敗次數超過憑證實務作業基準規定的最大預設值時，保護機制必須能即時鎖住此帳號或終止應用程式。

6.4.3 啟動資料之其他規範

不做規定。

6.5 電腦安全控管

6.5.1 特定電腦安全技術規定

以保證等級第3及第4級運作之憑證機構和其相關輔助系統必須包含以下特定電腦之安全功能，這些功能可由作業系統，或結合作業系統、軟體和實體的保護措施提供：

(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) 以密碼技術確保每次通訊及資料庫安全

(5) 具備程序完整性及安全控管保護

憑證機構設備必須建構在經過安全評估的作業平臺上，且憑證機構相關系統(硬體、軟體、作業系統)必須在經過安全評估的組態下運作。憑證機構應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

不做規定。

6.6 生命週期技術控管

6.6.1 系統研發控管

憑證機構的系統研發控管措施說明如下：

保證等級	系統研發控管措施
第1級	不做規定。

保證等級	系統研發控管措施
第2級 第3級 第4級	(1)憑證機構所使用的軟體，必須依良好的軟體工程發展方法開發，如採用能力成熟度模型整合(Capability Maturity Model Integration, CMMI)方法。 (2)必須防止惡意軟體安裝在憑證機構設備上，僅能使用獲得安全政策授權的元件。 (3)對於註冊中心之硬體與軟體，必須在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。 (4)系統開發與測試環境應與上線環境有所區隔。 (5)憑證機構之系統研發單位應善盡良善管理責任，諸如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、測試報告及管理手冊。

6.6.2 安全管理控管

憑證機構的安全管理控管措施說明如下：

保證等級	安全管理控管措施
第1級 第2級 第3級	(1)憑證機構不得安裝與運作無關的其他應用程式、硬體裝置、網路連接或元件軟體。 (2)必須記錄與控管憑證機構相關系統的組態、任何修正及功能升級，並具備偵測未經許可修改憑證機構之軟體或組態的機制。 (3)在首次安裝憑證機構軟體時，必須確認是由供應商提供且未被修改過之正確的版本。
第4級	(1)憑證機構之硬體與軟體必須是專用的，不得安裝與運作無關的其他應用程式、硬體裝置、網路連接或元件軟體。 (2)必須記錄與控管憑證機構相關系統的組態、任何修正及功能升級，並具備偵測未經許可修改憑證機構之軟體或組態的機制。 (3)在首次安裝憑證機構軟體時，必須確認是由供應商提供且未被修改過之正確的版本。 (4)憑證機構必須至少每月驗證1次憑證機構軟體的完整

保證等級	安全管理控管措施
	性。 (5) 遵循WebTrust for CA之規定執行安全管理控管措施。

6.6.3 生命週期安全控管

憑證機構得依需求自行決定生命週期之安全控管措施，並於憑證實務作業基準中規定。

6.7 網路安全控管

憑證機構主機不得與任何外部網路連接，而其儲存庫則必須連接到網際網路(Internet)上，以提供不中斷服務(除必要之維護或備援外)。憑證機構須於憑證實務作業基準中敘明網路安全控管措施。

6.8 時戳

憑證機構之系統應定期與受信賴時間源進行同步，以維持系統時間正確性，並確保以下時間之正確性：

(1) 憑證簽發時間

(2) 憑證廢止時間

(3) 憑證廢止清冊(或憑證機構廢止清冊)之簽發時間

(4) 系統事件之發生時間

憑證機構系統校時動作為可稽核事件(參見第5.4.1節)。

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

憑證機構須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

憑證機構須簽發 ITU-T X.509 版本 3 的憑證。

7.1.2 憑證擴充欄位

憑證機構須遵循 ITU-T X.509、Baseline Requirements 及 RFC 5280 規定使用憑證擴充欄位。若須另訂欲使用之擴充欄位時，應在憑證實務作業基準中說明，並註明哪些屬於關鍵的(Critical)擴充欄位，使得在應用服務上能與其社群達到互運。

7.1.3 演算法物件識別碼

本基礎建設內憑證機構應採用 SHA-256 或更高安全強度的雜湊函數演算法。

憑證機構簽發的憑證必須於簽章時使用下述演算法之物件識別碼：

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

憑證機構簽發的憑證必須使用下述之物件識別碼來識別產製主體金鑰的演算法：

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)}

若憑證機構簽發的憑證使用 ECC 演算法產製主體金鑰時，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)}
secp384r1	{iso(1) identified-organization(3) certicom(132) curve(0) ansip384r1(34)}

7.1.4 命名形式

憑證機構所簽發之憑證的主體與簽發者兩個欄位值，必須使用

ITU-T 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、Baseline Requirements 及 RFC 5280 規定。

依據 RFC 5280，根憑證機構(如 HiPKI RCA)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簽發者欄位，其編碼內容須與該根憑證機構自簽憑證之主體欄位的編碼形式完全相同；下屬憑證機構簽發之用戶憑證簽發者欄位，其編碼內容須與該下屬憑證機構憑證之主體欄位的編碼形式完全相同。

7.1.5 命名限制

不做規定。

7.1.6 憑證政策物件識別碼

當憑證機構簽發的憑證引用第 1.2 節中所訂之憑證政策物件識別碼時，則應表示該憑證已遵照該憑證政策物件識別碼規範之規定進行簽發與管理。

7.1.7 政策限制擴充欄位之使用

不做規定。

7.1.8 政策限定元之語法及語意

不做規定。

7.1.9 關鍵憑證政策擴充欄位之語意處理

憑證機構簽發的憑證所使用之關鍵憑證政策擴充欄位之語意處理，必須遵循 ITU-T X.509、Baseline Requirements 及 RFC 5280 之規定。

7.2 憑證廢止清冊之格式剖繪

7.2.1 版本序號

HiPKI RCA 簽發的憑證機構廢止清冊及其下屬憑證機構簽發的憑證廢止清冊必須符合 ITU-T X.509 版本 2 的規定。

7.2.2 憑證廢止清冊及憑證廢止清冊條目之擴充欄位

憑證機構簽發之憑證廢止清冊(或憑證機構廢止清冊)，其憑證廢止清冊擴充欄位與憑證廢止清冊條目擴充欄位皆須遵循 ITU-T X.509、Baseline Requirements 及 RFC 5280 之規定。

7.3 線上憑證狀態協定之格式剖繪

憑證機構若提供線上憑證狀態協定查詢服務，應於其憑證實務作業基準敘明線上憑證狀態協定版本序號與擴充欄位所採用的標準，其查詢服務網址應可於憑證的憑證機構資訊存取(Authority Information Access, AIA)擴充欄位中取得。

7.3.1 版本序號

憑證機構的線上憑證狀態協定查詢服務應符合 RFC 5019 與 RFC 6960 規範標準。

7.3.2 線上憑證狀態協定擴充欄位

憑證機構提供之線上憑證狀態協定擴充欄位應遵循 ITU-T X.509、Baseline Requirements、RFC 5019 及 RFC 6960 之相關規定。

8 稽核及其他評核

憑證機構應執行 WebTrust for CA 之稽核，以確保其運作遵照憑證政策及憑證實務作業基準之規定。簽發組織驗證型與網域驗證型 TLS/SSL 憑證之憑證機構另須執行 WebTrust for CA－SSL BR 稽核。簽發延伸驗證型 TLS/SSL 憑證之憑證機構除須執行前述兩種稽核外，另須執行 WebTrust Principles and Criteria for Certification Authorities－Extended Validation SSL(簡稱 WebTrust for CA－EV SSL)稽核。

若憑證機構未執行過上述之任一項稽核，則該憑證機構在核發 TLS/SSL 憑證前須通過準備度稽核(point-in-time readiness assessment)。

8.1 稽核頻率或評核事項

憑證機構應接受定期稽核，至少每年 1 次，且查核期間不可超過 12 個月。

憑證機構得對其下屬憑證機構及註冊中心進行定期及不定期稽核，以確認下屬個體遵照憑證實務作業基準運作。

簽發 TLS/SSL 憑證之憑證機構另須安排稽核員依據 Baseline Requirements 及 WebTrust for CA－SSL BR 之規定，自前 1 次抽樣後至少每季，隨機選擇 3% 或至少 1 張 TLS/SSL 憑證執行內部稽核。

8.2 稽核人員之身分及資格

稽核人員應獨立於被稽核之憑證機構外，可由以下個體擔任：

(1) 第三公正人員。

(2) 組織劃分上與被稽核之憑證機構有所區別的另一獨立個體。

稽核人員應提供公正及獨立的評估。本公司委託熟悉憑證機構運

作並經 WebTrust for CA 系列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 系列標章稽核或 2 場次共計 8 人天憑證機構資訊安全管理稽核相關經驗，且熟悉憑證機構簽發及管理憑證的相關規定。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。憑證機構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

依照第 8.2 節規定，稽核人員應獨立於被稽核之憑證機構外。

8.4 稽核項目

稽核項目如下所述：

(1) 憑證機構是否遵照憑證實務作業基準運作

(2) 憑證機構之憑證實務作業基準是否符合憑證政策之規定

(3) 註冊中心是否遵照憑證政策及憑證實務作業基準運作

(4) 憑證機構與其他根憑證機構簽訂交互認證協議書(Cross Certification Agreement, CCA)時，稽核之項目應涵蓋該根憑證機構是否符合交互認證協議書之規定

8.5 對於稽核結果之因應方式

當稽核人員發現憑證機構之建置及維運不符合憑證政策或交互認證協議書之規定時，必須採取以下行動：

(1) 記錄不符合情形。

(2) 將不符合情形通知憑證機構之維運管理單位，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。

發生不符合情形之憑證機構，應依據稽核報告及憑證政策或交互認證協議書之規定，執行修正。

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，憑證機構應公布及信賴該憑證機構之信賴憑證者有關的最近 1 次外部稽核結果。稽核結果由憑證機構依照其適用的標準懸掛 WebTrust for CA 標章、WebTrust for CA－SSL BR 標章或 WebTrust for CA－EV SSL 標章呈現於憑證機構網站首頁，點選標章後可閱覽近期的外稽報告及管理聲明書。最近 1 次的外稽報告及管理聲明書亦應於查核區間結束後 3 個月內公布於憑證機構之儲存庫。若因故延遲公布最近 1 次稽核結果，憑證機構應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

不做規定。

9.1.2 憑證查詢費用

不做規定。

9.1.3 憑證廢止、狀態查詢費用

不做規定。

9.1.4 其他服務費用

不做規定。

9.1.5 退費

不做規定。

9.2 財務責任

9.2.1 保險涵蓋範圍

簽發延伸驗證型 TLS/SSL 憑證的憑證機構應於其憑證實務作業基準揭露其所投保之保險種類與理賠涵蓋範圍或是於第 9.2.2 節說明其他資產之擔保，說明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 規範。

簽發其他類別憑證之憑證機構不做規定。

9.2.2 其他資產

參見第 9.2.1 節

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

憑證機構應於憑證實務作業基準中敘明機密資訊之範圍。

9.3.2 非機密之資訊

憑證機構應於憑證實務作業基準敘明非機密資訊之範圍。

9.3.3 保護機密資訊之責任

憑證機構應於憑證實務作業基準中敘明保護機密資訊之責任。

9.4 個人資訊之隱私

9.4.1 隱私保護計畫

憑證機構應依網站公告之個人資料保護及隱私權政策，實施個人資料保護。

9.4.2 隱私之資訊

憑證機構應於憑證實務作業基準敘明隱私資訊之範圍。

9.4.3 非隱私之資訊

憑證機構應於憑證實務作業基準敘明非隱私資訊之範圍。

9.4.4 保護隱私資訊之責任

憑證機構應於憑證實務作業基準敘明保護隱私資訊之責任。

9.4.5 使用隱私資訊之告知與同意

憑證機構應於憑證實務作業基準敘明使用隱私資訊之相關規定。

9.4.6 應司法或管理程序釋出資訊

憑證機構應於憑證實務作業基準敘明有關提供司法人員隱私資訊之相關規定。

9.4.7 其他資訊釋出之情況

憑證機構應於憑證實務作業基準敘明提供其他資訊之相關規定，並依相關法律規定辦理。

9.5 智慧財產權

本憑證政策可由儲存庫自由下載，或依著作權法相關規定合理使用。散布本憑證政策者，不得向他人收取費用，對於不當使用或散布本憑證政策之侵害，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

簽發憑證機構應向憑證之受益人(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，係遵照本憑證政策及/或簽發憑證機構之憑證政策實務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，簽發憑證機構會(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憑證政策及/或簽發憑證機構之憑證實務作業基準(參見第 3.2 節)。

(2) 憑證授權

於憑證核發時，簽發憑證機構會(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憑證政策及/或簽發憑證機構之憑證實務作業基準(參見第 3.2.5 節)。

(3) 資訊正確性

於憑證核發時，簽發憑證機構會(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憑證政策及/或簽發憑證機構之憑證實務作業基準(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，簽發憑證機構會(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憑證政策及/或簽發憑證機構之憑證實務作業基準(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，簽發憑證機構會(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憑證政策及/或簽發憑證機構之憑證實務作業基準。

(6)用戶協議

若簽發憑證機構與用戶非隸屬同一組織，則用戶與簽發憑證機構是符合 Baseline Requirements 要求之合法有效且可執行用戶協議的當事方；若簽發憑證機構與用戶隸屬同一組織，則由申請代表人對使用條款表示確認。

(7)狀態

簽發憑證機構應維護一個 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

簽發憑證機構將根據 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，簽發憑證機構應向用戶、信賴憑證者及應用軟體供應商聲明，其係遵照 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

註冊中心應聲明及擔保：

(1)對於憑證管理，係遵照本憑證政策及簽發憑證機構之憑證實務作業基準之規定

(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簽發憑證機構憑證實務作業基準之規定

(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

為了簽發憑證機構及憑證受益人之明確利益，申請人應擔保憑證核發前，簽發憑證機構會收到：

(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)應向簽發憑證機構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)提供憑證機構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)立即通知簽發憑證機構、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)憑證只用於符合本憑證政策、簽發憑證機構之憑證政策實務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

信賴憑證者在信賴或使用某個憑證前，必須依照憑證實務作業基準及信賴憑證者協議中所規定之程序進行聲明表達。

9.6.5 其他參與者之聲明及擔保

不做規定。

9.7 免責聲明

除非在憑證實務作業基準中另有敘明或受法律限制，本基礎建設不承擔任何與此憑證政策有關之擔保及義務。如本基礎建設外的其他憑證機構因引用本憑證政策而引發之任何問題，概由該憑證機構自行負責。

9.8 責任限制

憑證機構應於憑證實務作業基準中敘明責任限制。

9.9 賠償

依據電子簽章法第十四條，「憑證機構對因其經營或提供認證服務之相關作業程序，致當事人受有損害，或致善意第三人因信賴該憑證而受有損害者，應負賠償責任。但能證明其行為無過失者，不在此限。憑證機構就憑證之使用範圍設有明確限制時，對逾越該使用範圍所生之損害，不負賠償責任。」。

憑證機構之憑證實務作業基準應敘明對用戶及信賴憑證者的賠償責任，例如：

(1)於用戶約定協議要求用戶因於憑證申請時之虛假或欺詐的陳述，造成憑證機構簽發了不正確的憑證之損失的賠償條款。

(2)於信賴憑證者約定協議要求信賴憑證者若使用憑證時沒有適當檢查憑證廢止資訊或逾越憑證機構憑證之使用範圍，造成憑證機構之損害或損失的賠償條款。

9.10 本文件之生效與終止

9.10.1 生效

本憑證政策於 HiPKI RCA 儲存庫公布後即生效。

9.10.2 終止

本憑證政策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

本憑證政策之效力，維持至遵循本憑證政策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

本公司接受有關憑證政策之意見以安全電子郵件或書面進行告知(notice)，透過本憑證政策第 1.5.2 節之聯絡資料可將這些意見送至 HiPKI RCA。告知在發文者收到有效(使用數位簽章)之回執時才有效，如果回執在 5 天內沒有收到，可改採書面並以快遞或掛號方式執行。

憑證機構可在其憑證實務作業基準中敘明對主要成員之個別告知及溝通的方式，如組織架構有重大變更時。

9.12 修訂

9.12.1 修訂程序

政策管理委員會至少每年應檢視本憑證政策 1 次，憑證機構至少每年應檢視憑證實務作業基準 1 次，並依據第 2.3 節規定進行公告。

9.12.2 通知之機制及期限

對用戶可能產生重大影響之變更項目，憑證機構應公告於網站，並於憑證實務作業基準敘明變更項目通知機制及公告期限。

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及保證度時，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

當對憑證政策內容之解釋有爭議時，爭議之雙方應儘量自行協商以取得共識，若協商不成，可向本公司另請求解釋。憑證機構應在憑證實務作業基準中敘明爭議之解決條款。

9.14 管轄法律

牽涉本憑證政策或協議之解釋及實施，以及本基礎建設所簽發之憑證的合法性及任何爭議皆由中華民國相關法律管轄。

9.15 適用法律

依據憑證政策所進行之所有憑證機構之操作，必須遵循中華民國相關法律及規定。

9.16 雜項條款

9.16.1 完整協議

本憑證政策所約定者，係主要成員(如第 1.3 節所述)間最終且完整的約定。

憑證機構應透過合約或協議要求註冊中心符合憑證政策及可適用之業界標準及指引。憑證機構應透過協議要求用戶及信賴憑證者依照協議內容使用產品或服務。

9.16.2 轉讓

本憑證政策所敘述的主要成員之權利或義務，不能在未通知本公司就以任何形式轉讓給其他方。

9.16.3 可分割性

如本憑證政策的任一條款不正確或無效時，其他條款仍然有效。

本憑證政策遵循 Baseline Requirements 及 EV SSL Certificate Guidelines 對憑證機構之要求，惟 Baseline Requirements 及 EV SSL Certificate Guidelines 相關規定若與本憑證政策所依循之本國相關法律產生衝突時，本憑證政策得調整相關作法以滿足該法律之要求，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，則本憑證政策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政策相關規定，致本基礎建設受有損害時，本基礎建設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。本基礎建設未向違反本憑證政策相關規定者主張權利，不代表本基礎建設對於其繼續或未來違反本憑證政策情事，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憑證機構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，憑證機構不負任何法律責任。憑證機構得在憑證實務作業基準中敘明其他除外條款，但憑證機構不得將因自行疏忽所引起之錯誤列入排除條件中。

9.17 其他條款

不做規定。