中華電信公開金鑰基礎建設

憑證政策

(Certificate Policy for the Chunghwa Telecom ecommerce Public Key Infrastructure)

第 1.1 版

中華電信股份有限公司

中華民國 103 年 12 月 22 日

目　　錄

1 序論

中華電信公開金鑰基礎建設(Chunghwa Telecom ecommerce Public Key Infrastructure, ePKI，以下簡稱本基礎建設)係配合中華電信股份有限公司(以下簡稱本公司) 推動電子化政策，健全電子商務基礎環境，以提供完善的電子認證服務而設立。

本基礎建設是依照ITU-T X.509標準建置的階層式(Hierarchy) 公開金鑰基礎建設，包括公開金鑰基礎建設的信賴起源(Trust Anchor)－中華電信憑證總管理中心(ePKI Root Certification Authority, eCA，以下簡稱 eCA)及本公司所設立的下屬憑證機構(Subordinate CA)所組成，ePKI 所簽發的憑證可適用於電子商務與電子化政府的各項應用，以提供更安全可信賴及便捷的網路服務。

本憑證政策(Certificate Policy, CP)係依據電子簽章法規定及國際相關標準如 Internet Engineering Task Force (IETF) RFC 3647、ITU-T X.509、IETF PKIX Working Group 的 RFC 5280、CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates 訂定之政策文件，以做為 ePKI 各憑證機構訂定憑證實務作業基準(Certification Practice Statement, CPS)之依循。

本憑證政策共定義 5 種保證等級(Assurance Level)，依次為第 1 級、第 2 級、第 3 級、第 4 級和測試級，等級數字越大者，保證程度越高。依照 ITU-T X.509 標準，保證等級必須以憑證政策物件識別碼(CP Object Identifier, CP OID，詳見 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(certificatePolicies)延伸欄位(extension fields)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(參考 1.3.7 節)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) 憑證機構相關系統簽發、管理憑證和傳送私密金鑰（Private Key）之相關作業程序。

(3) 憑證資料中的用戶或主體(Subject)是否能有效控管其憑證中所記載的公開金鑰相對應之私密金鑰，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

載的憑證主體（Subject）與公開金鑰（Public Key）之連結關係（Binding）。

本基礎建設之憑證機構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。本憑證政策訂定之 5 個保證等級僅適用於本基礎建設內的管理及互運，其他公開金鑰基礎建設領域只有在被核定可以政策對等(Equivalent)時，才允許在憑證政策對應延伸欄位(Policy Mapping Extension)使用本基礎建設之憑證政策物件識別碼。

本基礎建設之憑證機構於簽發憑證時，可以選擇適當的憑證政策物件識別碼記載在憑證的憑證政策延伸欄位(certificatePolicies Extension)中，使信賴憑證者可透過憑證中記載的憑證政策物件識別碼確認該憑證的適用範圍。信賴憑證者可透過成對的憑證政策物件識別碼確認簽發憑證機構(Issuing CA)與主體憑證機構（Subject CA）之間的憑證政策對映關係。

本憑證政策訂定的項目及條款係依據相關法令規定，憑證機構一詞在本憑證政策中係指本基礎建設中所有的憑證機構，基於與本國或外國的其他公開金鑰基礎建設互惠原則，eCA 在經本公司核准後，得與本基礎建設外之根憑證機構(Root Certification Authority, 簡稱 Root

CA，中文也有稱為憑證總管理中心或最頂層憑證機構）進行交互認證(Cross-Certification)。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。

1.1 概要

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)。憑證政策是指明某一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。本基礎建設已註冊 5 個保證等級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，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。

eCA 的憑證是自簽(Self-signed)憑證，也是本基礎建設的信賴起源，信賴憑證者應直接信賴 eCA 的憑證。依照國際標準及慣例，eCA 的憑證並無標示憑證政策物件識別碼，因應 eCA 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

憑證機構必須於憑證實務作業基準中說明如何達成所引用憑證

政策之保證等級。

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。憑證機構引用本基礎建設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 憑證政策之識別

本政策之名稱為中華電信公開金鑰基礎建設憑證政策(Certificate Policy for the Chunghwa Telecom ecommerce Public Key Infrastructure)，本版本為第 1.1 版，公布日期為 103 年 12 月 22 日，本憑證政策之最新版本可在以下網頁取得：http://ePKI.com.tw。憑證機構簽發的憑證(不含自簽憑證)必須在憑證政策延伸欄位記載憑證的憑證政策。下表為在 id-cht arc 註冊的憑證政策物件識別碼：

id-cht ::= {2 16 886 1}
id-cht-ePKI ::= {2 16 886 1 100}
id-cht-ePKI-certpolicy::= {id-cht-ePKI 0}

保證等級	物件識別碼名稱	物件識別碼值
測試級	id-cht-ePKI-certpolicy-testAssurance	{id-cht-ePKI-certpolicy 0}
第 1 級	id-cht-ePKI-certpolicy-class1Assurance	{id-cht-ePKI-certpolicy 1}
第 2 級	id-cht-ePKI-certpolicy-class2Assurance	{id-cht-ePKI-certpolicy 2}
第 3 級	id-cht-ePKI-certpolicy-class3Assurance	{id-cht-ePKI-certpolicy 3}

保證等級	物件識別碼名稱	物件識別碼值
第 4 級	id-cht-ePKI-certpolicy- class4Assurance	{id-cht-ePKI-certpolicy 4}

前述物件識別碼其數值自民國 103 年 12 月起將漸進移轉使用於網路通訊協定註冊中心（Internet Assigned Numbers Authority,IANA）註冊之私人企業數值(Private Enterprise Number ,PEN)註冊的 id-pen-cht arc 的憑證政策物件識別碼

id-pen-cht ::= {1 3 6 1 4 1 23459}
id-pen-cht-ePKI ::= {1 3 6 1 4 1 23459 100}
id-pen-cht-ePKI-certpolicy::= { id-pen-cht-ePKI 0}

保證等級	物件識別碼名稱	物件識別碼值
測試級	id-pen-cht-ePKI-certpolicy-testAssurance	{id-pen-cht-ePKI-certpolicy 0}
第 1 級	id-pen-cht-ePKI-certpolicy-class1Assurance	{id-pen-cht-ePKI-certpolicy 1}
第 2 級	id-pen-cht-ePKI-certpolicy-class2Assurance	{id-pen-cht-ePKI-certpolicy 2}
第 3 級	id-pen-cht-ePKI-certpolicy-class3Assurance	{id-pen-cht-ePKI-certpolicy 3}
第 4 級	id-pen-cht-ePKI-certpolicy-class4Assurance	{id-pen-cht-ePKI-certpolicy 4}

本憑證政策在 SSL 憑證之簽發符合在憑證機構與瀏覽器論壇(CA/Browser Forum)網站 http://www.cabforum.org 發行的 Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates 現行正式版本，若有任何本憑證政策或憑證機構之憑證實

務作業基準在 SSL 憑證簽發上與 Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates 現行正式版本不一致的情形，將優先遵循 Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates 的條款。

下屬憑證機構(目前有中華電信通用憑證管理中心)其憑證簽發符合 CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates 並通過 AICPA/CPA WebTrust for Certification Authorities Trust Services Principles and Criteria for Certification Authorities – SSL Baseline Requirements Audit Criteria Version 1.1 外稽標準或其最新版者，下屬憑證機構的憑證及用戶之 SSL 憑證可使用 CA/Browser Forum 之組織鑑別(Organization Validation, OV)與網域鑑別(Domain Validation, DV) SSL 憑證政策物件識別碼：

物件識別碼名稱	物件識別碼值
joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) subject-identity-validated(2)	{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) **1 2 2**}
{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) domain-validated(1)}	{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) **1 2 1**}

1.3 主要成員

1.3.1 政策管理委員會

每個公開金鑰基礎建設都需要有 1 個政策管理機構，以確保此基礎建設的持續及正常運作。以本基礎建設而言，本公司特別設立中華電信公開金鑰基礎建設政策管理委員會(ePKI Policy Management Committee，以下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，以下說明政策管理委員會的組成及工作任務：此委員會置召集人 1 人，由中華電信數據通信分公司副總經理或相當層級 1 人兼任；執行秘書 1 人，由數據通信分公司資通安全處處長兼任；委員 10 人，由中華電信數據通信分公司公司經營規劃處、企業客戶處、行銷處、政府網路處、雲端系統處、智慧聯網處、匯流系統處、資訊處之處長擔任，工作任務說明如下：

(1)監督 ePKI 各憑證管理中心之金鑰產製。

(2)審查 ePKI 憑證政策。

(3)審查 ePKI 相關技術規範。

(4)審查 ePKI 憑證實務作業基準。

(5)審查交互認證憑證機構的互通申請。

(6) 審查及核可加入 ePKI 或是與 ePKI 交互認證憑證機構的憑證政策之對應關係。

(7)監督交互認證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

1.3.2.1 中華電信憑證總管理中心

eCA 為本基礎建設的最頂層憑證機構(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 eCA 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) 訂定與本基礎建設領域外憑證機構間的交互認證(Cross-Certification)程序，包括簽發及管理其他本基礎建設外憑證機構的交互認證憑證。

(3)將簽發的憑證及憑證機構廢止清冊(Certification Authority Revocation List, CARL) 公布於儲存庫(Repository)，並且確保儲存庫之正常運作。

eCA 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與外部憑證機構交互認證的程序。

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 eCA 及其他下屬憑證機構之互運工作。

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(Subscribers)的身分、屬性和聯絡等相關資訊，以便於憑證機構之憑證簽發、廢止、憑證之金鑰更換、變更、展期、停用與復用等管理作業。

eCA 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

對於組織及個人而言，用戶(Subscribers)係指憑證之憑證主體(Subject)所記載的名稱，並擁有與憑證之公開金鑰相對應之私密金鑰的個體。用戶必須依據憑證所記載的憑證政策正確地應用憑證。另外，對於財產類別(例如應用程式(Application Process)、程式碼、伺服軟體(如 Web Server、SSL 伺服器)及硬體設備(Device))而言，由於財產本身並無行為能力，因此憑證用戶為申請憑證的個人或組織。

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，在本憑證政策中並不稱下屬憑證機構為用戶。

1.3.5 信賴憑證者

信賴憑證者(Relying Parties)係指相信憑證之憑證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機構做為協同運作的夥伴，例如稽核機構、屬性憑證機構(Attribute Authority)、時戳服務機構(Time Stamp Authority)、資料存證服務機構(Data Archiving Service)及卡管中心(Card Managenent Center)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。

1.3.7 終端個體

終端個體(End Entities, EE)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)。

1.4 憑證用途

本憑證政策依照不同安全需求訂定 5 種保證等級，以因應各種不同應用需要。憑證機構在決定所要簽發憑證之保證等級時，應依應用

範圍審慎評估各種風險，環境的潛在危機、可能弱點和憑證的用途及應用的重要性，以選擇合乎安全保證等級的方式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

本憑證政策對於各保證等級的憑證適用範圍並不強制規定，也不限定各保證等級所適用的社群對象，建議之適用範圍說明如下：

保證等級	適用範圍
測試級	僅供測試(Test)用，對於傳送的資料不負任何法律責任。
第 1 級	以電子郵件方式確認申請人確實可操作該電子郵件帳號，適合應用於遭到惡意篡改威脅很低的網路環境，或無法提供較高保證等級時，應用於數位簽章時可識別用戶來自於某一個特定電子郵件帳號及保證被簽署文件的完整性；應用於加密時，信賴憑證者可藉由用戶憑證之公鑰加密傳送訊息或對稱式金鑰以保障其隱密性，但不適合應用於需要鑑別身分與不可否認服務的線上交易。
第 2 級	適合應用於資訊可能被篡改，但不會有惡意篡改之網路環境(資訊可能被截取但機率不高)；不適合做為重要文件(與生命及高金額相關的交易之文件)的簽署。例如小額度電子商務交易所需之資料加密與身分認證。
第 3 級	適合應用於有惡意使用者會截取或篡改資訊、並較第 2 級危險之網路環境，傳送的資訊可包括金錢上的線上交易。
第 4 級	適合應用於潛在威脅很高之網路環境、或資訊被篡改後復原的代價很高，傳送的資訊包括高金額的線上交易或極機密的文件。

1.4.2 憑證之使用限制

終端個體應依據應用系統所必須具備的安全需求，選擇使用合適保證等級的憑證。

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，因而權益受損。

信賴憑證者必須依照 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 IETF RFC5280 等）定義之憑證驗證(certificate validation)方法來驗證憑證的有效性(validity)。

1.4.3 憑證之禁止使用範圍

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) 法令公告禁止適用之範圍

1.5 聯絡方式

1.5.1 憑證政策之制訂及管理機構

中華電信股份有限公司。

1.5.2 聯絡資料

如對本憑證政策有任何建議，請與本公司聯繫：

聯絡電話:0800080365。

郵遞地址：台北市信義路一段 21 號數據通信大樓中華電信憑證總管理中心。

電子郵件信箱：caservice@cht.com.tw。

也可至 http://epki.com.tw 查詢聯絡資料。

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。

另依據我國電子簽章法規定，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)，將中華電信憑證總管理中心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 憑證政策及憑證實務作業基準變更程序

憑證機構之憑證實務作業基準必須遵循相關法令及符合本憑證政策規定，並經中華電信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電子簽章法主管機關經濟部核定。

1.6 名詞定義和縮寫

參見附錄 1 縮寫和定義與附錄 2 名詞解釋。

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說明儲存庫的網址，並確保儲存庫之可用性、適當的存取控制及資料完整性。憑證機構之憑證實務作業基準應載明儲存庫之相關資訊。

憑證機構的儲存庫服務應負以下義務：

(1) 定期公布所簽發之憑證。

(2) 定期公布已廢止及已停用之憑證資訊。

(3) 公布憑證政策及憑證實務作業基準的最新資訊。

(4) 儲存庫之存取控制必須依照 2.3 節規定。

2.2 憑證機構之資訊公布

憑證機構應在固定的儲存庫公布：

(1)憑證政策及憑證實務作業基準。

(2)憑證廢止清冊，包括憑證廢止清冊之簽發時間與效期、憑證廢止時間。

(3)線上憑證狀態查詢協定(Online Certificate Status Protocol, OCSP）服務

(4)憑證機構本身之憑證，至少應使用到該憑證相對應之私密金鑰所簽發的所有憑證效期到期為止。

(5)簽發之所有憑證(包括簽發給其他憑證機構之憑證)。

(6)簽發之憑證機構廢止清冊(如憑證機構簽發憑證給其他憑證機構)。

(7)隱私權保護政策。

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載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載明公布及通知之規定

2.3 公布頻率

憑證廢止清冊之公布頻率請依照 4.9 節規定。憑證政策之公布與後續修訂應於政策管理委員會核准後 7 個日曆天內於 eCA 儲存庫公告。

2.4 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不需存取控制。

(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 識別及鑑別程序

3.1 命名

3.1.1 命名種類

本基礎建設的憑證主體名稱應為 X.500 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

組織及個人之憑證主體名稱必須符合我國相關法令對該主體命名之規定，並且使用正式登記的名稱。

設備或伺服軟體之憑證主體名稱必須為該設備或伺服軟體之管理者的名稱，同時其中的通用名稱(Common Name) 應以易於瞭解為原則，例如是模組的名稱或序號或應用的程序等。

伺服軟體憑證之主體名稱與憑證主體別名依照 CA/Browser Forum 之規範不得使用內部名稱(Internal Name)或保留 IP 位址(Reserved IP Addresses)。

3.1.3 用戶的匿名或假名

第 1 層下屬憑證管理中心可簽發匿名或假名憑證給終端用戶，如果這些憑證不被其所適用之政策（例如憑證種類、保證等級或憑證格式剖繪）禁止且能確保命名空間之唯一性。

3.1.4 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，憑證機構必須在憑證實務作業基準中載明如何使用 X.500 名稱空間，同時對於同名的憑證主體在命名時如何確保憑證主體名稱的獨特性。

3.1.6 商標之辨識、鑑別及角色

當憑證主體名稱可能包含商標時，則其命名必須符合我國商標相關法規。

3.1.7 命名爭議之解決程序

命名所有權依我國相關法令規定之命名規則辦理(例如公司法、姓名法、國民教育法等)，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，依照保證等級測試級運作之憑證機構則不做規定。

本公司為本基礎建設命名爭議的仲裁機構。

3.2 初始註冊

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上的公開金鑰成對。

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有以下 3 種方式：

(1) 由憑證機構或註冊中心為用戶產製金鑰對時：

用戶不必證明擁有私密金鑰，但必須依照 3.2.2 及 3.2.3 節規定接受身分鑑別，以取得私密金鑰及啟動資料，且私密金鑰應依照 6.1.2 節規定傳送給用戶。

(2) 由可信賴的第三者(例如發卡中心)為用戶產製金鑰對時：

憑證機構或註冊中心必須依照 6.1.3 節規定透過安全管道向可信賴的第三者取得用戶之公開金鑰，用戶不必證明擁有相對應之私密金鑰，但必須依照 3.2.2 及 3.2.3 節規定接受身分鑑別，以取得私密金鑰及啟動資料，且私密金鑰應依照 6.1.2 節規定傳送給用戶。

(3) 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 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 組織身分鑑別之程序

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

保證等級	組織身分鑑別之程序
測試級	不做規定。
第 1 級	(1)可不做書面證件核對。 (2)只要申請者具有自己的電子郵件地址即可申請憑證，可不進行鑑別確認程序。 (3)不需臨櫃辦理。
第 2 級	(1)可不做書面證件核對。 (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

保證等級	組織身分鑑別之程序
	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，如代表人無法親自臨櫃申請，得以書面委託書委任代理人代為臨櫃申請，並依 3.2.3 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、本公司對民間組織之專戶經理、專案經理或業務經理)完成符合上述規定之臨櫃識別與鑑別程序，並留下登記或識別與鑑別之佐證資料(例如留下印鑑章圖記或由公證人或本公司對該民間組織之專戶經理、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私法人團體、非法人團體或以上兩者之附屬組織。

保證等級	組織身分鑑別之程序
	(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 中華電信所屬組織必須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構或單位確實存在，並驗證公文書之真確性。 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本基礎建設核發之保證等級第 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： (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

保證等級	組織身分鑑別之程序
	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私法人團體、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 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

3.2.3 個人身分鑑別之程序

對於個人(Individual)身分鑑別之證件數量、鑑別確認程序及是否需臨櫃辦理等，依各保證等級不同有不同之規定，如下表所列：

保證等級	個人身分鑑別之程序
測試級	不做規定。
第 1 級	(1)可不做書面證件核對。

保證等級	個人身分鑑別之程序
	(2)只要申請者具有自己的電子郵件地址即可申請憑證，可不進行鑑別確認程序。 (3)不需臨櫃辦理。
第 2 級	(1)可不做書面證件核對。 (2)用戶提交個人資料，例如個人識別碼(如身分證字號)、姓名等，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	(1) 核對書面證件： 在申請憑證時，用戶至少應出示 1 張被認可並附照片之證件正本(例如國民身分證)，供憑證機構或註冊中心鑑別用戶之身分。 如用戶(例如未成年人)無上述之附照片證件，可使用由政府發給之足以證明用戶身分的書面證明文件(例如戶口名薄)取代，並由 1 位具行為能力之成年人以書面保證用戶之身分；出具書面保證之成年人之身分必須經過上述之鑑別。 (2) 用戶提交之個人資料，例如個人的識別碼(如身分證字號)、姓名及地址(如戶籍地址)等，應與該資料主管機關的登記資料(如戶籍資料)或其它經主管機關認可之可信賴第

保證等級	個人身分鑑別之程序
	三者的登記資料進行比對。 (3)臨櫃辦理： 用戶必須親臨憑證機構或註冊中心證明其身分。若用戶無法親自臨櫃辦理，得以書面委託書委任代理人代為臨櫃申請，但憑證機構或註冊中心必須確認該委託書之真偽(例如比對委託書上之用戶印鑑章)，並依上述規定鑑別代理人之身分。 個人如果事前已經受憑證機構、註冊中心或憑證機構信賴之機構或個人（例如戶政事務所、公證人或本公司經授權之人員）進行過符合上述規定之臨櫃識別與鑑別程序，並且留下該識別與鑑別之佐證資料（例如印鑑證明），則個人不需親臨辦理，憑證機構或註冊中心將驗證該佐證資料。 (4)使用自然人憑證辦理 使用內政部憑證管理中心簽發之保證等級第3級憑證簽章辦理，用戶不需親臨憑證機構或註冊中心證明其身分，憑證機構或註冊中心應驗證其數位簽章是否有效。 (5) 硬體裝置或伺服軟體憑證申請資料透過本基礎建設核發之保證等級第3級個人憑證簽章時，代表人不需親臨辦理，憑證機構或註冊中心將驗證申請

保證等級	個人身分鑑別之程序
	資料之數位簽章。
第 4 級	(1)核對書面證件： 在申請憑證時，用戶應至少出示 1 張被認可並附照片之證件(例如國民身分證)正本，供憑證機構或註冊中心鑑別用戶之身分。 (2)用戶提交之個人資料，例如個人的識別碼(如身分證字號)、姓名及地址等(如戶籍地址)，應與該資料主管機關的登記資料(如戶籍資料)進行比對。 (3)臨櫃辦理，用戶必須親臨憑證機構或註冊中心證明其身分。

3.2.4 沒有驗證的用戶訊息

憑證機構可不需要驗證保證等級第1級或測試級的個人憑證其通用名稱(Common Name)是否為憑證申請者的法定名稱。

3.2.5 授權之確認

當某個個人（憑證申請者）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，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 Authoirty），確認該個人可代表憑證主體，例如：

（1） 藉由第三方之身分認證服務或資料庫驗證、政府機關或有權責及公信力之團體的文書證明組織之存在。

（2） 藉由電話、郵件、電子郵件等聯絡方式或其他相當之程序確認該個人確實任職於該憑證主體（某組織或公司）得到授權代表該憑證主體。

（3） 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。

憑證機構發給組織或個人之憑證，若有記載電子郵件位址於憑證主體別名欄位供安全電子郵件等應用，應於憑證實務作業基準說明註冊中心如何驗證憑證申請者有辦法控制其記載於憑證之電子郵件帳號。

屬於網域驗證型(Domain Valiadition, 簡稱DV)之SSL類應用軟體憑證申請，必須依照CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates所建議之方式鑑別用戶具備網域之控制權，屬於組織驗證型（Organization Validation, 簡稱OV）之SSL類應用憑證申請，除了依照網域驗證型SSL類應用軟體憑證鑑別用戶具備網域之控制權外，尚須依照3.2.2或3.2.3節規定進行組織或個人的身分鑑別。下屬憑證機構若有簽發SSL憑證應於憑證實務作業基準描述網域控制權授權之確認方式。

3.2.6 互運之標準(Criteria of Interoperation)

不做規定。

3.3 金鑰更換請求之識別與鑑別

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。

下屬憑證機構的用戶需要更換金鑰時，需符合下表所列的鑑別要求。

保證等級	對用戶憑證更換金鑰的鑑別要求
測試級	不做規定。
第1級	用戶的身分可使用現行的簽章金鑰進行鑑別或依照3.2節初始註冊之鑑別程序進行鑑別。
第2級	用戶的身分可使用現行的簽章金鑰進行鑑別或依照3.2節初始註冊之鑑別程序進行鑑別，但如與初始註冊時間間隔超過15年時，則應依照3.2節規定重新辦理初始註冊。
第3級	用戶的身分可使用現行的簽章金鑰進行鑑別或依照3.2節初始註冊之鑑別程序進行鑑別，但如與初始註冊時間間隔超過9年時，則應依照3.2節規定重新辦理初始註冊。
第4級	用戶的身分可使用現行的簽章金鑰進行鑑別或依照3.2節初始註冊之鑑別程序進行鑑別，但如與初始註冊時間間隔超過3年時，則應依照3.2節規定重新辦理初始註冊。

3.3.1 憑證展期之金鑰更換的識別與鑑別

憑證機構的憑證不可展期，只有用戶的憑證才可展期，可使用現行的簽章金鑰進行鑑別。

3.3.2 憑證廢止之金鑰更換的識別與鑑別

憑證廢止後，新憑證的簽發應依照3.2節規定，用戶必須重新辦理初始註冊程序。

3.4 憑證廢止申請之識別與鑑別

憑證機構或註冊中心必須對於憑證廢止申請進行鑑別，憑證機構應依照4.9節規定在憑證實務作業基準中載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範

4.1 申請憑證

4.1.1 憑證之申請者

總管理中心之憑證申請者包括 eCA 及本公司所設立之下屬憑證機構或是由本基礎建設外之根憑證機構。

下屬憑證機構之憑證申請者包括組織或個人。

電腦及通訊設備(如路由器、防火牆、負載平衡器等)、伺服軟體(如 Web Server 或 SSL Server)或程式碼，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或程式碼擁有者的身分提出憑證申請。

4.1.2 註冊程序與責任

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與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與鑑別工作。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。(以保證等級測試級簽發之憑證不做規定) 。

(4)當私密金鑰被破解時，應立即通知憑證機構。(以保證等級測試級簽發之憑證不做規定) 。

4.2 申請憑證之程序

憑證機構必須在憑證實務作業基準中載明有關初始註冊、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。

eCA 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 eCA 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。

eCA 簽發交互憑證給本基礎建設外之憑證機構前，應由政策管理委員會與該憑證機構協商以決定是否承認該憑證機構簽發給其他憑證機構的交互憑證。

4.2.1 執行識別和鑑別功能

簽發憑證機構必須確保系統與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 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管理中心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也可被稽核之方式妥善保管。

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，憑證簽發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與鑑別之原因外，憑證機構得因其他原因不同意簽發憑證。憑證簽發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 處理憑證申請的時間

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完成憑證申請之受理。處理憑證申請的時間可記載於憑證實務作業基準或用戶約定條款或與憑證申請者之契約。

4.3 簽發憑證之程序

4.3.1 憑證簽發時憑證機構的作業

憑證機構簽發憑證應依照 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。

eCA 應在每個金鑰生命週期簽發 1 張自簽憑證(Self-Signed Certificate)以建立憑證信賴起源；並得簽發數張自發憑證(Self-Issued Certficate)，以因應本身金鑰及憑證政策的更換。eCA 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 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。

eCA 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 憑證簽發時憑證機構對憑證申請者的通告

以保證等級第 1、第 2、第 3 及第 4 級運作之憑證機構，應於憑證實務作業基準中載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。除因申請者之身分識別與鑑別之原因外，憑證機構得因其他原因不同意簽發憑證。以保證等級第 1、第 2、第 3 及第 4 級運作之憑證機構，應於憑證實務作業基準中載明不同意簽發憑證之通知方式。

4.4 接受憑證之程序

簽發保證等級第 2、第 3 及第 4 級憑證之憑證機構，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。

若憑證申請者(1)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。或(2)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、第 3 及第 4 級運作之憑證機構，應於憑證實務作業基準中載明以下事項：

(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，至少應包括憑證主體名稱。憑證申請者在接受 SSL 類伺服器憑證前尚須審視憑證主體別名欄位。組織或個人憑證之申請者若有安全電子郵件之應用需求而於憑證註記電子郵件位址，也須審視憑證主體別名欄位。

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。

4.4.1 構成接受憑證之事由

憑證申請者預先審視將簽發之憑證內容或審視憑證內容無誤，憑證經憑證機構公布於儲存庫或傳遞給憑證申請者。

4.4.2 憑證機構之憑證發布

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 憑證機構對其他實體的通告

不做規定。

4.5 金鑰對與憑證的用途

4.5.1 用戶私密金鑰與憑證的用途

用戶係指已申請並取得憑證之個體，對組織與個人而言係指憑證主體(Subjct)所記載的名稱，並擁有與憑證之公開金鑰相對應之私密金鑰的個體。對於財產類別（例如應用程式及硬體設備）而言由於財產本身無行為能力，因此憑證用戶為申請憑證的個人或組織。用戶金鑰對的產製應符合本憑證政策 6.1.1 節之規定，並且用戶必須獨自擁有控制憑證相對應私密金鑰的權力與能力，用戶本身不簽發憑證給其他方。用戶應保護其私密金鑰不被他人未經授權的使用或揭露，且只使用其私密金鑰於正確的金鑰用途(於憑證之擴充欄位有註記金鑰用途)。用戶必須依據憑證所記載的憑證政策正確地應用憑證。

4.5.2 信賴憑證者與憑證的用途

信賴憑證者係指相信憑證主體名稱與公開金鑰間連結關係之第三人。信賴憑證者應使用符合 ITU-T X.509、Internet Engineering Task Force (IETF) 的 RFC 、CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates 相關標準或規範的軟體。

信賴憑證者必須依照相對的憑證機構憑證及憑證狀態資訊，以驗證所使用憑證的有效性。在確認憑證的有效性後，才可使用憑證進行以下作業：

(1)驗證具有數位簽章的電子文件之完整性。

(2)驗證文件簽章產生者的身分。

(3)與用戶間建立安全之通訊管道。

前述憑證狀態資訊可透過憑證廢止清冊或憑證線上狀態查詢協定服務取得，憑證廢止清冊散布點（CRL Distribution Point）的位置可在憑證的詳細資訊取得。此外，信賴憑證者也應檢驗簽發憑證機構與用戶憑證之憑證政策，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，只有用戶的憑證才可展期。

4.6.1 憑證展期之事由

用戶憑證即將到期，未停用或廢止且符合以下事由可進行展期：

(1)憑證記載之公開金鑰尚未達到 6.3.2.2 節所規定之使用期限。

(2)用戶及其身分屬性資料仍保持一致。

(3)憑證所記載之公開金鑰其相對應之私密金鑰仍然有效，未遺失或遭破解。

4.6.2 憑證展期之申請者

憑證將到期且為原本之憑證用戶之主體或經授權之代表人。

4.6.3 憑證展期之程序

用戶申請憑證展期時，使用其私密金鑰對憑證申請檔加以簽章，並將該憑證申請檔交給註冊中心，註冊中心將使用該用戶的公開金鑰驗證該憑證申請檔的數位簽章，以識別用戶之身分。

4.6.4 用戶進行憑證展期之注意事項

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

4.6.5 構成接受展期憑證的事由

憑證申請者預先審視將簽發之展期憑證內容或審視展期憑證內容無誤，憑證經憑證機構公布於儲存庫或傳遞給憑證申請者。。

4.6.6 憑證機構之展期憑證發布

憑證機構的儲存庫服務應定期公布所簽發給用戶之展期憑證。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。

4.6.7 憑證機構對其他實體的展期憑證簽發通告

不做規定。

4.7 憑證之金鑰更換

4.7.1 憑證機構之金鑰更換的事由

憑證機構之私密金鑰必須依照 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。舊私密金鑰仍須簽發憑證廢止清冊或線上憑證狀態的回應，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。

如憑證機構本身的憑證被廢止後，其私密金鑰應停止使用，並需更換金鑰對。

eCA 最遲應於其私密金鑰簽發憑證用途的使用期限到期前，更換用來簽發憑證的金鑰對，並簽發 1 張新的自簽憑證及使用新舊私密金鑰相互簽發 1 張自發憑證，此 3 張新憑證的簽發程序依照 4.2 節規定。

下層憑證機構最遲應於其私密金鑰簽發憑證用途的使用期限到期前，更換用來簽發憑證的金鑰對。下層憑證機構更換金鑰對後，應依照 4.2 節規定向上層憑證機構申請新的憑證，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。

與 eCA 交互認證之本基礎建設外憑證機構，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，該憑證機構更換金鑰後是否需要繼續向 eCA 申請交互憑證，則視該憑證機構與本公司之協議或契約而定。若該憑證機構更換金鑰需要繼續向 eCA 申請交互憑證，應依 4.2 節規定辦理，並須保留足夠時間供政策管理委員會及 eCA 處理其交互認證申請，以確保 eCA 能夠在該憑證機構之交互憑證過期前，簽發並公告該憑證機構之新交互憑證。

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，只要是原本之用戶或者經授權之代表人能代表該用戶符合適當的金鑰與憑證生命週期管理負責保管其憑證相對應之私密金鑰。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 憑證之金鑰更換的程序

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，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 3.1、3.2、3.3、4.1 及 4.2 之規定辦理。

4.7.4 用戶進行憑證金鑰更換之注意事項

用戶之私密金鑰必須依照 6.3.2 節規定定期更換。

當用戶的憑證被廢止後，其私密金鑰應停止使用，並於更換金鑰對後，依照 4.2 節規定向憑證機構或註冊中心申請新憑證。

持有保證等級第 2、第 3 及第 4 級之用戶，如其憑證沒有被廢止，憑證機構或註冊中心可於該用戶私密金鑰使用期限到期前 1 個月開始受理其更換金鑰並申請新的憑證，申請新憑證之程序依照 4.2 節規定辦理。

4.7.5 構成接受憑證金鑰更換的事由

憑證機構通知憑證申請者憑證已經簽發、傳遞已經簽發之憑證給申請者或是用戶實際使用憑證皆構成接受憑證金鑰更換的事由。

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。(以保證等級測試級簽發之憑證不做規定) 。

(4) 當私密金鑰被破解時，應立即通知憑證機構。(以保證等級測試級簽發之憑證不做規定) 。

4.7.6 憑證機構之更換金鑰發布

憑證機構的儲存庫服務應定期公布所簽發憑證更換金鑰之憑證。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。

4.7.7 憑證機構對其他實體的通告

不做規定。

4.8 憑證變更

4.8.1 憑證變更之事由

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(例如更新電子郵件位址或其他較不重要之屬性資訊)且符合本憑證政策及憑證實務作業基準之相關規定，新的憑證可能有新的憑證主體公開金鑰或使用原有的主體公開金鑰，但憑證有

效截止日和原有之憑證到期日相同。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 憑證變更的程序

如 4.2 節所述。

4.8.4 申請者進行憑證變更之注意事項

以保證等級第 1、第 2、第 3 及第 4 級運作之憑證機構，應於憑證實務作業基準中載明憑證變更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變更之憑證，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。除因申請者之身分識別與鑑別之原因外，憑證機構得因其他原因不同意簽發憑證。以保證等級第 1、第 2、第 3 及第 4 級運作之憑證機構，應於憑證實務作業基準中載明不同意進行憑證變更之通知方式。

4.8.5 構成接受憑證變更的事由

憑證申請者預先審視將簽發之憑證內容或審視憑證內容無誤，憑證經憑證機構公布於儲存庫或傳遞給憑證申請者。

4.8.6 憑證機構之憑證變更發布

憑證機構的儲存庫服務應定期公布所簽發經憑證變更之憑證。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。

4.8.7 憑證機構對其他實體的通告

不做規定。

4.9 憑證暫時停用及廢止

除以保證等級測試級運作之憑證機構外，其他憑證機構皆應提供憑證廢止服務；憑證機構得依憑證應用範圍及服務品質決定是否提供憑證暫時停用服務。

提供憑證廢止或憑證暫時停用服務的憑證機構應在憑證實務作業基準中規定其提供憑證廢止或暫時停用申請的服務時間。

提供憑證廢止及停用服務之憑證機構應於憑證實務作業基準中載明提供服務方式、憑證廢止申請程序、申辦地點或網址等。

憑證廢止及停用後，憑證機構最遲應於下次預定公布憑證機構廢止清冊或憑證廢止清冊時，將廢止及暫時停用的憑證列入憑證機構廢止清冊或憑證廢止清冊中，並公告於儲存庫上；公告的憑證狀態資訊應包括廢止及暫時停用的憑證，直到這些憑證到期或被恢復使用為止。

對於已過期之憑證，憑證機構得不受理該憑證之廢止或暫時停用申請，亦得不將該憑證之廢止或暫時停用資訊列入憑證機構廢止清冊或憑證廢止清冊中。但對於過期前被廢止或暫時停用之憑證，憑證機構應將其廢止或暫時停用資訊列入憑證機構廢止清冊或憑證廢止清冊中至少 1 次。

4.9.1 廢止憑證之事由

以下 3 種情形必須廢止憑證：

(1) 如用戶的私密金鑰證實或懷疑遭破解(例如用戶儲存私密金鑰的 IC 卡遺失)時，應立即通知憑證機構（以保證等級測試級簽發之憑證不做規定），則該私密金鑰對應之未過期公鑰憑證必須廢止。

(2) 如憑證機構的私密金鑰證實遭破解時，則簽發給該憑證機構的未過期交互憑證必須廢止。

(3) 如憑證主體（Subject）的資料或屬性變更(例如主體名稱變更、主體證號或代碼變更、主體身分因解散或死亡而消失等)足以影響憑證記載資料之正確性時，則該憑證主體之未過期憑證必須廢止。

除以上情形必須廢止憑證外，用戶得於憑證有效期限內，因其他原因提出憑證廢止申請。

如憑證機構或註冊中心證實用戶違反憑證政策或憑證實務作業基準規定之用戶義務時，憑證機構得逕行廢止該用戶之憑證。

如憑證機構證實或懷疑本身的私密金鑰遭破解時，得逕行廢止以該私密金鑰簽發的所有憑證。

如上層憑證機構證實下層憑證機構違反憑證政策或憑證實務作業基準時，得逕行廢止該下層憑證機構的憑證。

如憑證機構證實與其交互認證之憑證機構違反憑證政策或本身

之憑證實務作業基準時，得逕行廢止該憑證機構的交互認證憑證。

如政策管理委員會決定 eCA 的自簽憑證及自發憑證必須廢止時(例如懷疑 eCA 的私密金鑰遭破解)，得逕行廢止 eCA 的自簽憑證及自發憑證。

4.9.2 憑證廢止之申請者

當發生 4.9.1 節規定應廢止憑證或其他情形時，用戶或擁有私密金鑰的個體得於憑證有效期限內，向憑證機構或註冊中心提出憑證廢止申請。

憑證機構依照 4.9.1 節規定，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。

4.9.3 憑證廢止之程序

在收到憑證廢止申請後，憑證機構或註冊中心應依照 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，若身分識別及鑑別無誤，以及憑證廢止的理由合理，例如不得無故選擇憑證機構的金鑰被破解，則便可核准憑證廢止的申請。

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 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，憑證廢止後憑證機構或註冊中心應以適當的方式通知用戶。以保證等級第 1、第 2、第 3 及第 4 級運作的憑證機構，應於憑證實務作業基準中載明憑證廢止後通知用戶的方式。

如不同意廢止憑證，則憑證機構或註冊中心應以適當方式通知用

戶，並明確告知不同意廢止的理由。以保證等級第 1、第 2、第 3 及第 4 級運作的憑證機構，應於憑證實務作業基準中載明不同意廢止憑證之通知方式。

4.9.4 憑證廢止申請的寬限期

用戶或憑證機構如有必須進行廢止憑證的需要，應儘速向簽發其憑證的憑證機構申請。

憑證廢止申請的寬限期是指用戶在憑證廢止事由已經確認而必須提出憑證廢止申請的時間。憑證機構和註冊中心必須在 1 小時內通報其憑證機構或註冊中心私密金鑰疑似遭破解的事由給簽發其憑證的憑證機構。用戶在其私密金鑰遺失或疑似遭破解或已被破解或是憑證所記載之資訊已經過時不正確時，應儘速提出憑證廢止之申請，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的處理期限

除保證等級第 4 級以外，各憑證機構應該在接受憑證廢止申請後於 1 個工作天內完成憑證的廢止作業。

4.9.6 信賴憑證者檢查憑證廢止的要求

使用保證等級第 2、第 3 及第 4 級憑證的信賴憑證者，必須在使用憑證前查詢目前的憑證機構廢止清冊和憑證廢止清冊或是透過憑證線上狀態查詢協定服務，以查驗憑證目前的狀態，同時也必須驗證憑證機構廢止清冊和憑證廢止清冊的真偽和完整性。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 9.6.4 節規定。

4.9.7 憑證機構廢止清冊及憑證廢止清冊之簽發頻率

eCA 應簽發憑證機構廢止清冊(CARL)，下屬憑證機構及交互認證憑證機構應簽發憑證機構廢止清冊或憑證廢止清冊(Certificate Revocation List, CRL) 。在簽發憑證機構廢止清冊或憑證廢止清冊前，應檢查其內容，確認資訊之正確性。例如，使用軟體掃瞄憑證機構廢止清冊或憑證廢止清冊，以檢查資料之正確性。憑證機構廢止清冊或憑證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時完成，如此將有助於離線或遠端作業的應用系統，將憑證狀態資訊儲存成近端快取(Local Cache)。憑證機構應加強與儲存庫間之配合，降低從憑證狀態資訊產生到公告於儲存庫的時間，憑證實務作業基準應規定以那一個儲存庫為主，以便用戶可以到該儲存庫取得最新的憑證狀態資訊。

當憑證狀態資訊公告時，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
測試級	不適用	不做規定
第 1 級	不適用	不做規定
第 2 級	不適用	每 3 天至少 1 次

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 3 級	每天至少 1 次	每天至少 1 次
第 4 級	每天至少 1 次	每天至少 1 次

4.9.8 憑證機構廢止清冊及憑證廢止清冊發布之最大延遲時間

在網際網路正常提供服務的情形下，憑證機構最遲應在憑證機構廢止清冊或憑證廢止清冊所記載之下次更新時間(the nextUpdate)前將憑證機構廢止清冊或憑證廢止清冊公布。

4.9.9 線上憑證狀態查詢協定服務

憑證機構除提供憑證機構廢止清冊或憑證廢止清冊服務外，得選擇性地提供信賴憑證者之線上憑證狀態查詢協定服務。憑證機構所提供之線上憑證狀態查詢服務必須符合 IETF RFC 2560 或 IETF RFC 6960 的規範，且所提供之憑證狀態資訊的更新度（freshness）至少必須等同於憑證機構廢止清冊或憑證廢止清冊之更新度，也就是說其憑證狀態回應的本次更新時間（thisUpdate）至少必須等同於最新之憑證機構廢止清冊或憑證廢止清冊的本次更新時間（thisUpdate）。用戶若使用憑證機構所提供之線上憑證狀態查詢，則可不需取得或處理該憑證機構所公告之憑證機構廢止清冊或憑證廢止清冊。憑證機構應在憑證實務作業基準中載明，是否提供及如何提供線上憑證狀態查詢協定服務。

4.9.10 線上憑證狀態查詢之規定

使用保證等級第 2、第 3 及第 4 級憑證的信賴憑證者，如不查驗憑證機構廢止清冊或憑證廢止清冊，則需採線上查詢憑證狀態的方式以進行憑證狀態的確認。

4.9.11 其他形式廢止公告

不做規定。

4.9.12 金鑰被破解時之其他特殊規定

金鑰被破解時，請依照 4.9.1、4.9.2 及 4.9.3 節相關規定處理。

4.9.13 暫時停用憑證之事由

提供暫時停用憑證服務的憑證機構應於憑證實務作業基準中載明必須或應該暫時停用憑證之事由。

4.9.14 暫時停用憑證之申請者

提供暫時停用憑證服務的憑證機構應於憑證實務作業基準中載明所允許之憑證暫時停用申請者身分。

4.9.15 暫時停用憑證之程序

提供暫時停用憑證服務的憑證機構應於憑證實務作業基準中載明暫時停用憑證之程序。

4.9.16 暫時停用憑證之處理期間及停用期限

提供暫時停用憑證服務的憑證機構應於憑證實務作業基準中載明用戶申請暫時停用憑證之處理期間及停用期限。

4.9.15 恢復使用憑證之程序

提供暫時停用憑證服務的憑證機構應於憑證實務作業基準中載明恢復使用憑證之程序。

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線上憑證狀態查詢協定服務或兩者皆提供的憑證狀態服務。

4.10.2 服務的可用性

憑證機構應提供 7 天 x 24 小時不中斷之憑證狀態服務。

4.10.3 可選功能

不做規定。

4.11 終止服務

終止服務是指憑證用戶終止使用憑證機構的服務，包含憑證到期時終止憑證機構提供用戶的服務或者是用戶憑證廢止而終止服務。

憑證機構應允許用戶藉由廢止憑證或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 私密金鑰託管與回復

4.12.1 金鑰託管與回復政策與實務

簽章用之私密金鑰不可被託管(Escrowed)。

4.12.2 通訊用金鑰封裝與回復政策與實務

憑證機構若有支援通訊用金鑰(Session Key)封裝與回復(Encapsulation and Recovery)應於其憑證實務作業基準描述其實務做法。

5 非技術性安全控管

5.1 實體控管

5.1.1 實體所在及結構

除依照保證等級測試級及第 1 級運作之憑證機構不做規定外，依照保證等級第 2 級以上運作之憑證機構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訊的機房設施水準，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

除依照保證等級測試級及第 1 級運作之憑證機構不做規定外，依照保證等級第 2 級以上運作之憑證機構，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：

依照保證等級第 1 及第 2 級運作之憑證機構之實體控管規定：

(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的可攜式儲存媒體和文件是保存在

安全的場所。

依照保證等級第 3 及第 4 級運作之憑證機構之實體控管規定：

(1)建置全天候人工或電子式監控設備，以防止未經授權之侵入。

(2) 定期維護和檢視存取記錄檔。

(3)進行電腦系統和密碼模組實體控管時，必須至少兩人以上共同執行。

eCA 因為必須簽發所有保證等級憑證，因此設備環境的安全機制依照保證等級第 4 級運作的實體控管規定。對於依照保證等級測試級運作之憑證機構的實體控管則不做規定，但應於憑證實務作業基準中說明。

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、出入門禁)運作正常。

5.1.3 電力及空調

除依照保證等級測試級及第 1 級運作之憑證機構不做規定外，依照保證等級第 2 級以上運作之憑證機構，電力及空調設備必須具備足夠的備援設施，能支援憑證機構的相關系統，以因應外在因素影響時，能正常運作或關機。同時，必須提供不斷電系統，至少 6 小時以上之備用電力，以供儲存庫備援資料(包括已簽發憑證和憑證廢止清冊)。

5.1.4 水災防範及保護

憑證機構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

除依照保證等級測試級及第 1 級運作之憑證機構不做規定外，依照保證等級第 2 級以上運作之憑證機構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

除依照保證等級測試級及第 1 級運作之憑證機構不做規定外，依照保證等級第 2 級以上運作之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，備援的地點與本管理中心機房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) 適當的區隔每種任務，同一任務分派給 1 人以上，以防止 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相關系統，並負責建立和維護系統之用戶帳號及設定稽核參數和產生元件金鑰。

(2)簽發員：簽發憑證和廢止憑證。

(3)稽核員：查驗和維護稽核日誌。

(4)維運員：執行系統備份和故障排除。

5.2.1.1 管理員

管理員主要負責：

(1) 安裝、設定和維護憑證機構相關系統。

(2) 建立和維護系統之使用者帳號。

(3) 設定稽核參數。

(4) 產製和備份憑證機構之金鑰。

5.2.1.2 簽發員

簽發員主要負責：

(1) 登錄新憑證用戶和受理憑證簽發申請。

(2) 核對憑證用戶身分和憑證資訊的正確性。

(3) 審核和執行憑證簽發。

(4) 受理申請、審核和執行憑證廢止。

5.2.1.3 稽核員

稽核員主要負責：

(1) 對稽核記錄的查驗、維護和歸檔。

(2) 執行或監督內部的稽核，以確認憑證機構維運遵照憑證實務作業基準的規定。

5.2.1.4 維運員

維運員主要負責：

(1) 系統的實體安全控管(如機房的門禁管理、防火、防水、空調系統等)。

(2) 系統設備的日常運作維護。

(3) 系統的備援及復原作業。

(4) 儲存媒體的更新。

(5) 系統軟硬體的更新。

(6)網路及網站的維護：建置系統安全與病毒防護機制及網路安全事件的偵測與通報等。

5.2.2 角色分派

憑證機構之角色分派原則如下：

保證等級	角色分派原則
測試級	不做規定。
第1級	不做規定。
第2級	依照5.2.1節規定的4種信賴角色，允許1個人超過1個以上信賴角色，但簽發員和管理員不可相互兼任。
第3級	依照5.2.1節規定的四種信賴角色，允許1個人超過1個以上信賴角色，但簽發員不可以再兼任管理員或稽核員。
第4級	依照5.2.1節規定的4種信賴角色，對人員及角色分派必須符合以下規定： (1)管理員、簽發員和稽核員3種信賴角色不可相互兼任，但可兼任維運員。 (2)任何1個角色均不允許執行自我稽核功能。

5.2.3 每個任務所需之人數

為確保憑證機構設備和維運的安全性達到最佳化，人員角色安排必須依照 5.2.2 節規定，每個任務所需的人數應在憑證實務作業基準中說明。

5.2.4 識別及鑑別每一個角色

除依照保證等級測試級及第 1 級運作之憑證機構不做規定外，依照保證等級第 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。

5.3 人員控管

憑證機構必須確實掌握所有執行憑證機構或註冊中心運作之相關人員，人員任務指派的安全控管必須符合以下規定：

(1) 以書面方式指派工作。

(2) 以法規或契約規定執行任務之條件。

(3) 接受任務之相關訓練。

(4) 以法規或契約規定不可洩漏敏感之憑證機構相關安全資訊及憑證用戶資料。

(5) 指派工作應符合利益迴避原則。

5.3.1 身家背景、資格、經驗及安全需求

憑證機構必須進行人員的識別作業，忠誠、可信賴、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、監督和稽核相關辦法應在憑證實務作業基準中說明。

5.3.2 身家背景之查驗程序

身家背景之查驗程序應在憑證實務作業基準中說明。

5.3.3 教育訓練需求

憑證機構相關人員必須接受以下教育訓練：

(1) 憑證機構及註冊中心之安全認證機制。

(2) 憑證機構系統使用的公開金鑰基礎建設軟體。

(3) 負責執行公開金鑰基礎建設的工作內容。

(4) 災後復原及業務永續經營之程序。

5.3.4 人員再教育訓練之需求及頻率

憑證機構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，憑證機構必須每年進行檢視相關人員之受訓情形。

5.3.5 工作調換之頻率及順序

不做規定。

5.3.6 未授權行動之制裁

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資料，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和懲處。

對於執行 eCA 及儲存庫主機的相關人員，如違反憑證政策或憑證實務作業基準或其他 eCA 公布之程序，必須採取適當的管理和懲處。

5.3.7 聘僱人員之規定

聘僱人員擔任憑證機構相關職務必須符合憑證機構的憑證實務作業基準相關規定。

5.3.8 提供之文件資料

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、政策、契約等相關文件，給憑證機構和註冊中心相關人員。

5.4 安全稽核程序

以保證等級測試級運作之憑證機構得不具備安全稽核功能，簽發其他保證等級憑證之憑證機構，對於安全相關事件應具備適當的安全稽核紀錄(Audit Log)功能。安全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。所有安全稽核紀錄不論是電子或非電子的，均應妥善保存，並且在執行稽核時可立即正確取得。安全稽核紀錄之維護應依照 5.5.2 節歸檔保留期限規定辦理。

5.4.1 被記錄事件種類

憑證機構之安全稽核功能，應包括憑證管理系統及憑證管理系統所依存的電腦作業系統(Operating System)的安全稽核。每筆稽核記錄

至少應包括以下項目(不論是自動或手動記錄的稽核事件)：

(1) 事件種類。

(2) 引起事件的個體和操作者之身分。

(3) 事件發生之地點或位置

(4) 事件發生之時間和日期。

(5) 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)。

當事件發生時，稽核記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紀錄的稽核事件，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		✓	✓	✓

可稽核事件／保證等級	第 1 級	第 2 級	第 3 級	第 4 級
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 如管理者將已被鎖住的帳號解鎖，而且該帳號是因為多次失敗的身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		✓	✓	✓
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，對保存在憑證機構的憑證主體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. 私密金鑰之輸出				

可稽核事件／保證等級	第 1 級	第 2 級	第 3 級	第 4 級
A.6.1 私密金鑰之輸出 (不包括只使用在單次或只限一次使用之金鑰)	✓	✓	✓	✓
A.7. 憑證之註冊				
A.7.1 所有憑證之註冊申請過程	✓	✓	✓	✓
A.8. 廢止之憑證				
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 任何與憑證機構安全相關之組態設定改變		✓	✓	✓
A.11. 帳號之管理				
A.11.1 加入或刪除角色和使用者	✓	✓	✓	✓
A.11.2 使用者帳號或角色之存取權限修改	✓	✓	✓	✓
A.12. 憑證格式剖繪之管理				
A.12.1 所有憑證格式剖繪之改變	✓	✓	✓	✓
A.13. 憑證機構廢止清冊及廢止清冊格式剖繪之管理				
A.13.1 所有憑證機構廢止清冊		✓	✓	✓

可稽核事件／保證等級	第 1 級	第 2 級	第 3 級	第 4 級
及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作業		✓	✓	✓
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 憑證機構之內部資料備份		✓	✓	✓
A.14.12 憑證機構之內部資料回復		✓	✓	✓
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公布			✓	✓
A.14.15 存取憑證機構之內部資料庫			✓	✓

可稽核事件／保證等級	第 1 級	第 2 級	第 3 級	第 4 級
A.14.16 任何憑證被破解之申告		✓	✓	✓
A.14.17 憑證載入符記			✓	✓
A.14.18 符記之傳遞過程			✓	✓
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 軟體檢查完整性失敗		✓	✓	✓
A.17.3 接收不合適訊息			✓	✓

可稽核事件／保證等級	第 1 級	第 2 級	第 3 級	第 4 級
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 (Uninterrupted Power System, UPS) 失敗			✓	✓
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

稽核紀錄應依據下表進行檢視，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警示或異常等。因應稽核檢視之結果所採取的行動亦應以文件記錄。

保證等級	紀錄檔之處理頻率
測試級	不做規定
第 1 級	不做規定。
第 2 級	不做規定。

保證等級	紀錄檔之處理頻率
第 3 級	至少每兩個月 1 次。 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，並且對任何可能之惡意活動應進一步調查。
第 4 級	至少每個月 1 次。 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，並且對任何可能之惡意活動應進一步調查。

5.4.3 稽核紀錄檔保留期限

以保證等級測試級及第 1 級憑證運作的憑證機構，稽核紀錄檔之保留期限不做規定。

以保證等級第 2、第 3 及第 4 級憑證運作的憑證機構，稽核紀錄檔應在憑證機構所在處至少保留兩個月，並依照 5.4.4、5.4.5、5.4.6 及 5.5 節記錄保留管理機制等相關規定辦理。

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

以保證等級測試級及第 1 級運作的憑證機構，稽核紀錄檔的保護不做規定。

以保證等級第 2、第 3 及第 4 級運作的憑證機構，電子稽核日誌系統(Electronic Audit Log System)必須包含保護機制，手動的稽核資

訊亦應加以保護，以確保不會遭未經授權的閱讀、修改及刪除。

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
測試級	不做規定。
第1級	
第2級	稽核記錄檔至少每月應備份1次。
第3級	
第4級	稽核記錄檔至少每月應備份1次，至少每月應異地(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 安全稽核系統

稽核系統可以在憑證管理系統之內部或外部。稽核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 對引起事件者之告知

當事件發生而被稽核系統紀錄時，稽核系統並不需要告知引起該事件的個體其所引發的事件已經被系統所紀錄。

5.4.8 弱點評估

以保證等級第 3 及第 4 級運作之憑證機構，應執行例行的安全控管弱點評估，以保證等級測試級、第 1 及第 2 級憑證運作之憑證機構

則不做規定。

簽發 SSL 憑證之憑證機構應遵照 AICPA/CPA WebTrust SM/TM for Certification Authorities Trust Services Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.0 及 CA/Browser Forum NETWORK AND CERTIFICATE SYSTEM SECURITY REQUIREMENTS Version 1.0 規定之方式與頻率執行弱點評估與滲透測試。

5.5 紀錄歸檔之方法

5.5.1 紀錄事件之類型

依各保證等級的安全需求，應在歸檔時記錄以下資料 (以保證等級測試級運作的憑證機構則不做規定) 。

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	✓	✓	✓	✓
系統與設備組態設定	✓	✓	✓	✓
系統或組態設定修改與更新的內容	✓	✓	✓	✓
憑證申請資料	✓	✓	✓	✓
廢止申請資料		✓	✓	✓

應歸檔資料／保證等級	第 1 級	第 2 級	第 3 級	第 4 級
3.2.3 節訂定的用戶身分識別資料		✓	✓	✓
文件的簽收及憑證的接受		✓	✓	✓
符記啟用紀錄		✓	✓	✓
所有已簽發或公告的憑證	✓	✓	✓	✓
憑證機構金鑰更換的紀錄	✓	✓	✓	✓
所有被簽發或公告的憑證機構廢止清冊和憑證廢止清冊		✓	✓	✓
所有稽核記錄	✓	✓	✓	✓
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 歸檔之保留期限

歸檔資料的最低保留期限規定如下：

保證等級	最低保留期限
測試級	不做規定
第 1 級	不做規定
第 2 級	5 年
第 3 級	10 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(時間長短由該憑證機構的主管機關決定)。

5.5.3 歸檔之保護

以保證等級測試級及第 1 級運作的憑證機構，歸檔資料之保護不做規定。

以保證等級第 2、第 3 及第 4 級運作的憑證機構，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 歸檔備份程序

不做規定。

5.5.5 時戳紀錄之要求

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

憑證機構建立、核對、格式化及封包、移轉及儲存歸檔資料之程序，應在憑證實務作業基準中載明。

5.6 金鑰更換

5.6.1 憑證機構之金鑰更換

憑證機構之私密金鑰必須依照 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。舊私密金鑰仍須簽發憑證廢止清冊或線上憑證狀態的回應，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。

如憑證機構本身的憑證被廢止後，其私密金鑰應停止使用，並需更換金鑰對。

eCA 最遲應於其私密金鑰簽發憑證用途的使用期限到期前，更換用來簽發憑證的金鑰對，並簽發 1 張新的自簽憑證及使用新舊私密金鑰相互簽發 1 張自發憑證，此 3 張新憑證的簽發程序依照 4.2 節規定。

下層憑證機構最遲應於其私密金鑰簽發憑證用途的使用期限到期前，更換用來簽發憑證的金鑰對。下層憑證機構更換金鑰對後，應依照 4.1 節規定向上層憑證機構申請新的憑證，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。

與 eCA 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，該憑證機構更換金鑰後是否需要繼續向 eCA 申請交互憑證，則視該憑證機構與本公司之協議或契約而定。若該憑證機構更換金鑰需要繼續向 eCA 申請交互憑證，應依 4.2 節規定辦理，並須保留足夠時間供政策管理委員會及 eCA 處理其交互認證申請，以確保 eCA 能夠在該憑證機構之交互憑證過期前，簽發並公告該憑證機構之新交互憑證。

5.6.2 用戶之金鑰更換

用戶之私密金鑰必須依照 6.3.2 節規定定期更換。

當用戶的憑證被廢止後，其私密金鑰應停止使用，並於更換金鑰對後，依照 4.1 節規定向憑證機構或註冊中心申請新憑證。

持有保證等級第 2、第 3 及第 4 級之用戶，如其憑證沒有被廢止，憑證機構或註冊中心可於該用戶私密金鑰使用期限到期前 1 個月開始受理其更換金鑰並申請新的憑證，申請新憑證之程序依照 4.1 節規定辦理。

5.7 金鑰遭破解或災變時之復原程序

憑證機構的災後復原工作應優先恢復儲存庫，使憑證狀態資訊能正常提供。

5.7.1 緊急事件與系統遭破解之處理程序

憑證機構應訂定緊急事件和系統遭破解後之通報與處理程序，同時每年進行演練。

5.7.2 電腦資源、軟體或資料遭破壞之復原程序

憑證機構必須以永續經營為目標，依據憑證政策及憑證實務作業基準規定確實做好各種備援措施，儘可能將電腦資源、軟體及資料遭破壞之災害損失減至最低，並迅速恢復憑證之簽發及管理作業。

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演練。

5.7.3 憑證機構之簽章金鑰遭破解之復原程序

以保證等級第 2、第 3 及第 4 級運作之憑證機構，應在憑證實務作業基準中或相關的文件中載明憑證機構之簽章金鑰遭破解時之復原程序，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 次憑證機構簽章金鑰遭破解之演練。

5.7.4 憑證機構安全設施之災後復原工作

以保證等級第 2、第 3 及第 4 級運作之憑證機構應在憑證實務作業基準或相關文件中載明在自然或其他災害後，重新建立憑證機構安全設施的步驟。

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 次災後復原計畫之演練。

5.7.5 憑證機構之簽章金鑰憑證被廢止之復原程序

以保證等級第 2、第 3 及第 4 級運作之憑證機構，應在憑證實務作業基準或相關的文件中載明憑證機構之簽章金鑰憑證被廢止時之復原程序，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 次憑證機構之簽章金鑰憑證被廢止之演練。

5.8 憑證機構或註冊中心之終止服務

應依據電子簽章法相關規定進行憑證機構之終止服務。

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

憑證機構簽發憑證所使用的密碼模組，必須經由中華電信核可之安全等級相當的密碼模組來產製金鑰。

金鑰產製過程中所採用之隨機亂數依照 NIST FIPS 140-2 規範之演算法，其長度及亂度即使提供足夠的資訊和設備，欲計算出相同的亂數序列是不可行的 (Computationally Infeasible)。

儲存在密碼模組內之私密金鑰，應防止其由密碼模組中外洩。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，必須經由中華電信認可。用戶隨機亂數、金鑰對和對稱金鑰之產製，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

測試級	軟體或硬體
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 私密金鑰安全傳送給用戶

如私密金鑰在用戶的密碼模組內被產製及儲存時，無需傳送其私密金鑰。

如由個體(例如憑證用戶或 IC 卡發卡中心)所擁有的符記(Token)直接產製金鑰，或由另一個金鑰產製者產製金鑰後，再傳送金鑰到該個體的符記中，則此個體在私密金鑰產生及接受時，已被視為擁有該私密金鑰。但若上述的個體並不是憑證申請的憑證主體時，則應以安全及可稽核的方法傳送私密金鑰給憑證主體，以完成私密金鑰的轉移。

對於所有保證等級，如存放金鑰的硬體傳送給用戶時，應確保將正確的符記及其啟動資料(Activation Data)傳送給用戶。憑證機構必須維護 1 份確認用戶已收到該符記的紀錄。當使用任何包含秘密共享(如密碼或 PIN 碼)的機制，則該機制必須確保只有申請者及 eCA 或下屬憑證機構是唯一擁有該秘密的個體。

如私密金鑰由憑證機構或註冊中心或可信賴的第三者代為產製，則此密碼模組必須安全傳送至用戶，用戶必須作收受私密金鑰的確認。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。

在任何情況下，除了用戶外，其他人皆不能取得或控制簽章用私密金鑰。任何替用戶產製簽章用之私密金鑰的個體，也不可保留該金鑰的備份。

6.1.3 公開金鑰安全傳送給憑證機構

在憑證機構對用戶做身分鑑別時，用戶必須將其公開金鑰傳送給憑證機構，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) 可經由其它安全的電子化機制來完成。

(4) 可透過安全的非電子化方式來完成，這些方法包含(但不限)經由掛號郵件或快遞傳送軟式磁碟片(或其他儲存媒體)。

6.1.4 憑證機構公開金鑰安全傳送給信賴憑證者

eCA 之公開金鑰必須隨時可取得。下屬憑證機構必須以可信賴的方式將 eCA 自簽憑證或公開金鑰傳遞給使用者。可信賴之憑證傳送方式包括以下幾種：

(1) 憑證機構以符記儲存 eCA 之自簽憑證或公開金鑰，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 eCA 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 eCA 之自簽憑證或公開金鑰之雜湊值或指紋，供使用者比對(與憑證一起在線上公

布(in-band) 的雜湊值或指紋，不被視為是合格的安全管道)。

(4) 由具有同等級或更高安全保證等級的網站下載 eCA 自簽憑證或公開金鑰。

(5) 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eCA的憑證實務作業基準中說明。eCA簽發的下屬憑證機構憑證需公布在該憑證機構的儲存庫中。

6.1.5 金鑰長度

保證等級	公開金鑰
測試級	至民國102年12月31日(含)之前至少必須使用RSA 1024位元的金鑰或安全強度相當的其他種類金鑰。 到民國119年12月31日(含)之前必須使用RSA 2048 位元金鑰或安全強度相當的其他種類金鑰 超過民國119年12月31日者，應使用RSA 3072 位元金鑰或安全強度相當的其他種類金鑰。
第1級	
第2級	
第3級	
第4級	至少必須使用RSA 4096位元的金鑰或安全強度相當的其他種類金鑰。

6.1.6 公鑰參數之產製與品質檢驗

對於RSA演算法而言，公鑰參數必須為空的(Null)；對於其他演算法而言，公開金鑰參數則依相關的國際標準。

對於RSA演算法而言，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，則依相關的國際標準，並應包括參數品質的測試。

6.1.7 金鑰之使用目的

對於憑證中所認證的公開金鑰必須在ITU-T X.509憑證之keyUsage擴充欄位註明其金鑰用途(簽章或加密)。作為數位簽章(包括鑑別)的憑證必須設定digitalSignature位元；作為加密用的憑證必須設定 keyEncipherment或dataEncipherment位元。憑證機構本身的憑證必須設定兩個金鑰使用位元：cRLSign 和keyCertSign。

保證等級測試級、第1、第2及第3級憑證，可將單一金鑰同時使用於加密與簽章，以支援某些舊版的安全電子郵件(Secure Multipurpose Internet Mail Extensions, S/MIME)應用軟體。除非憑證政策有特別註明，此種雙重用途(Dual-Use)之憑證必須依照簽章用途憑證的規定來產生及管理，不得設定不可否認金鑰用途(Non-Repudiation Key Usage) 之位元，而且不得用於重要資料的簽章驗證。對於下屬憑證機構，不論任何種保證等級，應簽發兩種金鑰對憑證給予用戶，一做為資料加密用；一做為數位簽章與身分認證用。

6.2 私密金鑰保護及密碼模組安全控管措施

6.2.1 密碼模組標準及控管

政策管理委員會應決定本基礎建設所使用的密碼模組驗證的標準，其中密碼模組之安全需求是遵照(Compliance)美國FIPS 140-2系列或安全強度相當的標準，憑證機構用於簽發憑證的密碼模組應通過上列的安全認證標準。

對於本基礎建設的各個個體中，除了用戶可以必須盡可能遵照

外，其餘的個體應依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)係參照美國FIPS 140-2系列的定義。

個體 \保證等級	eCA	下屬憑證機構	註冊中心	用戶
測試級	不適用	不做規定	不做規定	不做規定
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 (硬體或軟體)	等級1 (硬體或軟體)	等級1 (硬體或軟體)
第3級	不適用	等級2(硬體)	等級2(硬體)	等級1 (硬體或軟體)
第四級	等級3(硬體)	等級3(硬體)	等級2(硬體)	等級2(硬體)

6.2.2 金鑰分持之多人控管

簽發保證等級第3及第4級憑證的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

簽章用之私密金鑰不可被託管(Escrowed)。

6.2.4 私密金鑰備份

6.2.4.1 憑證機構簽章用私密金鑰備份

以保證等級第3級及第4級運作之憑證機構，其簽章用私密金鑰，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。

6.2.4.2 用戶簽章用私密金鑰備份

保證等級第1、第2及第3級憑證，用戶簽章用私密金鑰可做備份

或拷貝，但是必須由用戶控制。

保證等級第4級憑證，用戶簽章用私密金鑰不可以備份或拷貝。

6.2.5 私密金鑰歸檔

簽章用私密金鑰不可以被歸檔(Archival)。

6.2.6 私密金鑰與密碼模組間傳輸

依照 6.1.1 節規定產製金鑰。憑證管理中心與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，只有在執行憑證管理中心或註冊中心金鑰備份回復及更換密碼模組時，才可將私密金鑰輸入至密碼模組中，並應以6.2.2節之規定採多人控管方式進行私密金鑰輸入至密碼模組中，私密金鑰輸入方式可為加密或金鑰分持，且必須確保加密金鑰不致外洩，以確保輸入過程中不得將私密金鑰明碼暴露於密碼模組之外。私密金鑰輸入完成後，須將輸入過程產製之相關機密參數完全銷毀。

6.2.7 私密金鑰儲存於密碼模組

依照 6.1.1 節及6.2.1節規定。

6.2.8 私密金鑰之啟動方式

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(Personal Identification Number, PIN)或生物識別。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 私密金鑰之停用方式

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 私密金鑰之銷毀方式

當簽章用私密金鑰及其備份不再需要、或憑證到期、或被廢止時，簽章用私密金鑰必須被銷毀。對於軟體密碼模組而言，必須將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6.2.1節。

6.3 金鑰對管理之其他規定

將單一金鑰對同時用於簽章和加密，雖然在技術上可行，但除非符合6.1.7節規定之舊版應用系統，否則不論任何保證等級，建議都應簽發兩種金鑰對憑證給予用戶，一種做為資料加密用；另一種則使用於數位簽章與身分認證。

用戶用於簽章與身分鑑別的私密金鑰絕不可被託管、歸檔或備份；用戶所屬的憑證機構得要求託管、歸檔或備份職務上用來加密的私密金鑰。

6.3.1 公開金鑰之歸檔

在憑證歸檔後，得不必再進行公開金鑰之歸檔。

6.3.2 公開金鑰及私密金鑰之使用期限

6.3.2.1 憑證機構公開金鑰及私密金鑰之使用期限

憑證機構之公開金鑰及私密金鑰依金鑰強度等級不同，使用期限說明如下：

(1) RSA 4096位元或安全強度相當之其他種類的公開金鑰對：公開金鑰與私密金鑰有效期限至多為30年；惟以私密金鑰簽發憑證用途，其使用期限不得超過15年。

(2) RSA 3072位元或安全強度相當之其他種類的公開金鑰對：公開金鑰與私密金鑰有效期限至多為30年；惟以私密金鑰簽發憑證用途，其使用期限不得超過15年。

(3) RSA 2048位元或安全強度相當之其他種類的公開金鑰對：公開金鑰與私密金鑰有效期限至多為20年；惟以私密金鑰簽發憑證用途，其使用期限不得超過10年。

前述3種情形但憑證機構的簽章私密金鑰用以簽發簽發憑證機構廢止清冊或憑證廢止清冊、憑證線上狀態查詢協定服務伺服器憑證或憑證線上狀態查詢協定服務回應訊息之用途則不受前述私密金鑰簽發憑證用途的期限限制，會使用至其下屬憑證機構憑證（若憑證機構為根憑證機構時）或憑證機構所發用戶憑證效期皆到期為止。

eCA自簽憑證生命週期不超過30年。

eCA簽發給下屬憑證機構之憑證，其憑證生命週期，加上 eCA用來簽署憑證之簽章用私密金鑰生命週期，合計不得超過 eCA自簽

憑證生命週期。

eCA因應其簽章用金鑰更換時所簽發的2張自發憑證，它們的憑證生命週期之期限不超過舊自簽憑證的效期。

6.3.2.2 用戶公開金鑰及私密金鑰之使用期限

用戶之金鑰使用期限依據其金鑰長度而訂，若金鑰為與RSA 1024位元安全強度相當，則私密金鑰使用期限至多為5年，原則上其使用期限至多到民國102年12月31日止；若金鑰為與RSA 2048位元安全強度相當，則私密金鑰使用期限至多為10年。憑證的總有效期限(包括展期)至多與金鑰使用期限相同。RSA 1024位元之SSL憑證至民國102年12月31日以後禁止使用，必須廢止。

6.3.2.3 SHA-1 雜湊函數演算法有效期限

依據國際間密碼學之安全評估及 CA/Browser Forum 在 Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates v.1.2.1 版之規定，105 年 1 月 1 日起憑證機構不能再使用 SHA-1 雜湊函數演算法簽發任何新的用戶憑證或下屬憑證機構憑證。直到 106 年 1 月 1 日，憑證機構仍可使用 SHA-1 雜湊函數演算法簽發驗證憑證線上狀態查詢協定（OCSP）服務回應訊息的憑證(亦即可使用 SHA-1 雜湊函數演算法簽發 OCSP 伺服器之憑證)。憑證機構可以繼續使用其現有存在之 SHA-1 根憑證機構憑證或交互認證憑證。SHA-2 SSL 憑證不應由 SHA-1 下屬憑證機構憑證對應的簽章私密金鑰簽發。自 104 年 1 月 16 日起，憑證機構不應該使用 SHA-1 雜

湊函數演算法簽發憑證到期日超過 106 年 1 月 1 日之 SSL 或 Code Signing 憑證，因為應用軟體提供者正在從其軟體不贊成和/或移除 SHA-1 雜湊函數演算法，並且已經與憑證機構和用戶溝通繼續使用 SHA-1 憑證必須自己承擔風險。

憑證機構應採取相關措施確保用戶選擇適當的應用軟體以及淘汰 SHA-1 憑證。

6.4 啟動資料之保護

6.4.1 啟動資料之產生

憑證機構或憑證用戶私密金鑰的啟動資料與其他相關存取控制機制必須適當的保護。對於以保證等級第1、第2及第3級運作之憑證機構，其啟動資料得由使用者自行選擇。對於以保證等級第4級運作之憑證機構，必須能接受使用者的生物特徵資料，或由密碼模組強化的安全機制。如果啟動資料必須傳送，應透過適當的安全管道。

6.4.2 啟動資料之保護

用來解開私密金鑰的啟動資料，必須使用結合密碼和存取控制的安全機制加以保護以防止揭露。啟動資料得以生物特徵或記憶方式保存。若需留下紀錄，必須使用與該資料安全等級相當的密碼模組來保護，以確保其安全。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 其他啟動資料之規定

不做規定。

6.5 電腦軟硬體安控措施

6.5.1 特定電腦安全技術需求

依照保證等級第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功能，這些電腦安全功能可由作業系統，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) 對各種憑證服務和公開金鑰基礎建設信賴角色存取控制的限制。

(5) 具備公開金鑰基礎建設信賴角色和相關身分的識別和鑑別。

(6) 以密碼技術確保每次通訊和資料庫安全。

(7) 具備公開金鑰基礎建設信賴角色和相關身分識別的安全及可信賴的管道。

(8) 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。

6.5.2 電腦安全評等

不做規定。

6.6 生命週期技術控管措施

6.6.1 系統研發控管措施

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
測試級	不做規定。
第1級	不做規定。
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（Capability Maturity Model, CMM）方法。 (2) 必須防止惡意軟體安裝在憑證機構設備上。憑證機構的運作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和軟體，必須在初次使用時檢查是否有惡意程式碼並定期掃瞄。 (4) 系統開發環境與測試環境與上線環境應有所區隔。 (5) 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

	告與管理手冊、版本控管與憑證管理中心。

6.6.2 安全管理控管措施

保證等級	安全管理控管措施
測試級	(1)憑證機構不得安裝與運作無關的其他應用系統(包括硬體裝置、網路連接或元件軟體)。 (2)必須記錄和控管憑證機構相關系統的組態及任何修正與功能升級，並具備偵測未經許可修改憑證機構之軟體或組態的機制。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，且為正確的版本。
第1級	
第2級	
第3級	

第4級	(1)憑證機構之硬體和軟體必須是專用的，不得安裝與運作無關的其他應用系統(包括硬體裝置、網路連接或元件軟體)。 (2)必須記錄和控管憑證機構相關系統的組態以及任何修正與功能升級，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，且為正確的版本。 (4)憑證機構必須至少每月1次驗證憑證機構軟體的完整性。 （5）遵循AICPA/CPA Trust Service Principles and Criteria for Certification Authorities之規定執行安控措施。

6.6.3 生命週期安全評等

憑證機構應於憑證實務作業基準揭露金鑰生命週期安全評等的頻率。

6.7 網路安全控管措施

eCA主機不得與任何外部網路連接。eCA儲存庫則連接到網際網路(Internet)上，以提供不中斷服務 (除必要之維護或備援外)。eCA主機所簽發的憑證與憑證機構廢止資訊以手動方式，從與外部網際網路

實體隔離的eCA主機傳送到儲存庫，而且所有資訊(憑證與憑證機構廢止清冊)都以數位簽章保護。儲存庫透過系統修補程式的更新、弱點掃描、入侵偵測系統、防火牆、過濾路由器(Filtering Router)等加以保護，以防範阻絕服務和入侵等攻擊。

6.8 時戳

憑證機構應定期以受信賴時間源進行校時，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）憑證機構廢止清冊或憑證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需可被稽核。

7 憑證、憑證廢止清冊及憑證線上狀態查詢協定服務格式剖繪

7.1 憑證之格式剖繪

7.1.1 版本序號

憑證機構須簽發 ITU-T X.509 v3 版本的憑證，其版本序號(Version Numbers)的欄位值為 3。

7.1.2 憑證擴充欄位

eCA 及其下屬憑證機構簽發的憑證必須遵循 ITU-T X.509、CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates 及 IETF PKIX Working Group 的 5280 或其最新版相關規定。若必須使用自行擴充欄位時，應在憑證實務作業基準中說明，並註明哪些屬於關鍵的(Critical)自行擴充欄位，在應用服務上必須能與其社群達到互運。

7.1.3 演算法物件識別碼

eCA 及其下屬憑證機構簽發的憑證必須於簽章時使用下述之演算法的物件識別碼(OID)：

sha-1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
sha384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12}
sha512WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 13}

eCA 及其下屬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) 1}

7.1.4 命名形式

eCA 及其下屬憑證機構所簽發之憑證的主體及簽發者兩個欄位值，必須使用 ITU-T X.500 的唯一識別名稱(Distinguished Name)，且此名稱的屬性型態必須遵循 ITU-T X.509、CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates 及 IETF PKIX Working Group 的 RFC 5280 或其最新版的規定。

7.1.5 命名限制

不做規定。

7.1.6 憑證政策物件識別碼

eCA 其下屬憑證機構所簽發的憑證必須引用憑證政策的物件識

別碼，同時憑證政策的物件識別碼必須與憑證的保證等級相符。

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

eCA 其下屬憑證機構所簽發的憑證不得包含政策限定元(Policy Qualifiers)。

7.1.9 關鍵憑證政策擴充欄位之語意處理

eCA 及其下屬憑證機構簽發的憑證所使用之關鍵憑證政策的擴充欄位之語意處理，必須遵循 ITU-T X.509、CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates 及 IETF PKIX Working Group 的 RFC 5280 或其最新版的規定。

7.2 憑證機構廢止清冊及憑證廢止清冊之格式剖繪

7.2.1 版本序號

eCA 簽發的憑證機構廢止清冊(CARL)及 eCA 其下屬憑證機構簽發的憑證廢止清冊(CRL)必須符合 ITU-T X.509 v2 的規定。

7.2.2 憑證機構廢止清冊及憑證廢止清冊擴充欄位

在 ePKI 內各憑證機構的憑證機構廢止清冊及憑證廢止清冊(CARL/CRL)的格式，每一個擴充欄位皆必須遵循 ITU-T X.509、CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates 及 IETF PKIX Working Group 的 RFC 5280 或其最新版的規定。

7.3 線上憑證狀態查詢協定服務之格式剖繪

憑證機構若提供線上憑證狀態查詢協定 (OCSP)服務，應於其憑證實務作業基準揭露線上憑證狀態查詢協定服務版本序號及擴充欄位所採用的標準。

7.3.1 版本序號

憑證機構的線上憑證狀態查詢協定(OCSP) 服務應符合 IETF PKIX Working Group 的 RFC 5019 及 RFC 6960 標準規範。

7.2.2 線上憑證狀態查詢協定服務擴充欄位

憑證機構提供之線上憑證狀態查詢協定(OCSP)服務其擴充欄位應遵循 ITU-T X.509、CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates 及 IETF PKIX Working Group 的 RFC 5019、RFC 6960 或其最新版相關之規定。

8. 稽核方法

簽發保證等級第 2、第 3 及第 4 級憑證之憑證機構，應建立公正之稽核(Compliance Audit)機制，以確保其運作遵照憑證實務作業基準與憑證政策之規定。

8.1 稽核之頻率

憑證機構應接受定期稽核，依照保證等級第 3 及第 4 級運作之憑證機構至少每年 1 次，且查核期間不可超過 12 個月。依照保證等級第 2 級運作之憑證機構至少每兩年 1 次。依照保證等級測試級及第 1 級運作之憑證機構則不做規定。

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。

8.2 稽核人員之身分及資格

稽核人員應獨立於被稽核的憑證機構外，可由以下個體擔任：

(1)第三公正人員。

(2)在組織劃分上與被稽核的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 標章管理單位授權可於中華民國執行 Trust Service Principles and Criteria for Certification Authorities Version 2.0 之稽核業者，提供公正客觀的稽核服務。稽核人員應為合格授權之資訊系統稽核員(Certified Information System Audit，CISA)或具同等資

格，且具備 2 場次 4 人天以上之憑證機構 WebTrust for CA 標章稽核或 2 場次共計 8 人天憑證機構資訊安全管理稽核相關經驗，且熟悉憑證機構簽發、管理憑證的相關規定。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 8.2 節規定，稽核人員應獨立於被稽核的憑證機構外。

8.4 稽核之範圍

稽核之範圍如以下規定：

(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)稽核人員可對憑證機構之相關營運單位如註冊中心進行稽核。

如憑證機構與其下屬憑證機構簽訂交互認證協議書時，稽核之範圍應涵蓋下屬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)稽核人員應記錄不符合情形。

(2)稽核人員應通知發生不符合情形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 稽核結果公開之範圍

除可能導致系統被攻擊以及 9.3 節規定之範圍外，憑證機構應公布與信賴憑證者信賴該憑證機構有關的最近 1 次稽核結果。

9. 其他業務和法律事項

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 請求退費之程序

不做規定。

9.2 財務責任

9.2.1 保險涵蓋範圍

不做規定。

9.2.2 其他資產

不做規定。

9.2.3 對終端個體之賠償責任

對終端個體（用戶及信賴憑證者）之賠償責任不做規定。

9.3 業務資訊之保密

9.3.1 機密資訊之範圍

由憑證機構產生、接收或保管之資料，現職及曾任職於憑證機構之人員與各類稽核人員對於機密資訊均負保密責任。機密資訊至少包括：

(1)任何在憑證申請時記載之個人或組織資訊皆為機密資訊，未經用戶同意或依法令規定不得公開。

(2)用於憑證機構營運的私密金鑰及通行碼皆為機密資訊，不得公開。

(3)稽核紀錄除 8.6 節規定情形外，不得被完整公開。

憑證機構之憑證實務作業基準中應載明機密之資訊種類。

9.3.2 非機密資料之範圍

(1) 憑證、憑證廢止清冊及廢止或停用資訊不應視為機密資訊。憑證廢止或暫時停用資訊屬於非機密資訊，應對外公開。

(2) 識別資訊或記載於憑證的資訊，除特別約定外，不應視為機密資訊與隱私資訊。

憑證機構之憑證實務作業基準應載明非機密資料之種類。

9.3.3 保護機密資訊之責任

憑證機構應實施安控措施防止機密資訊遭洩漏或破壞。

9.4 個人資訊之隱私性

9.4.1 隱私保護計畫

憑證機構應於網站公告個人資料保護與隱私權聲明。憑證機構宜實施隱私衝擊分析、個資風險評估等措施以訂定隱私保護計畫。

9.4.2 隱私資料之種類

任何在憑證申請時記載之個人資訊皆為隱私資訊，未經用戶同意或依法令規定不得公開。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、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與指紋特徵、保密協定或契約之個人資訊等應視為隱私資料加以保護，憑證機構及註冊中心應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 非隱私資訊

識別資訊或記載於憑證的資訊與憑證，除特別約定外，不應視為機密資訊與隱私資訊。

儲存庫公布之簽發憑證、已廢止憑證或暫時停用資訊及憑證廢止清冊不視為機密與隱私資訊。

9.4.4 保護隱私資訊的責任

配合憑證機構運作所需之個人資料必須安全存放與受到保護，符合電子簽章法、Trust Service Principles and Criteria for Certification

Authorities 標準及個人資料保護法相關規定。憑證機構並需與註冊中心協議保護隱私資訊的責任。

9.4.5 使用隱私資訊的公告與同意

非經用戶同意或個人資料保護與隱私權聲明與本憑證政策另有規範，不會將個人資料用於其他地方。憑證機構之憑證實務作業基準應訂定有關提供 9.3.1 節機密資訊第(3)款之相關規定。

9.4.6 應司法或管理程序釋出資訊

除非經本憑證政策允許，或經法律或政府規章要求或配合司法審判，憑證機構不應揭露隱私資訊給任何第三方。憑證機構之憑證實務作業基準應訂定有關提供司法人員 9.4.2 節隱私資訊之相關規定。

9.4.7 其他資訊釋出之情形

依相關法令規定辦理。憑證機構之憑證實務作業基準應訂定有關提供用戶 9.3.1 節機密資訊之相關規定。

9.5 智慧財產權

本政策為本公司之智慧財產，本政策可依著作權法相關規定重製或散布，但必須保證是完整複製，並註明著作權為本公司所擁有。重製或散佈本政策者，不得向他人收取費用，對於不當使用或散佈本政策之侵害，本公司將依法予以追訴。

9.6 法律責任

9.6.1 憑證機構之責任

如憑證機構在簽發的憑證中，引用憑證政策所訂的任何保證等級之物件識別碼，即表示該憑證機構保證其所簽發憑證之內容資訊已遵守憑證政策之規定。除非憑證機構確實遵守憑證政策之規定，否則不得在所簽發的憑證中引用憑證政策所訂的任何保證等級之憑證政策物件識別碼。

9.6.2 註冊中心之責任

憑證機構應承擔註冊中心因代理憑證機構執行註冊中心工作所引發的所有責任，註冊中心之責任應依其與憑證機構間的權利義務而定。憑證機構得在憑證實務作業基準或與註冊中心之契約或協議中載明註冊中心之責任。

9.6.3 用戶之責任

用戶應負以下之責任：

(1)安全地產製其私密金鑰並避免遭受破解。

(2)提供憑證機構與註冊中心正確與完整的資訊。

(3)遵守第 3 及第 4 章規定程序。

(4)於使用憑證前確認憑證資料的正確性。

(5)妥善地保管及使用私密金鑰。(以保證等級測試級簽發之憑證不做規定) 。

(6)當私密金鑰被破解時，應立即通知憑證機構。(以保證等級測試級簽發之憑證不做規定) 。

(7)適當地停止使用憑證並通知憑證機構，包括(a)如果提供給憑證機構之資訊或是記載於憑證中的資訊已經變更有可能誤導(b)有任何實際或懷疑的憑證所記載之公鑰其相對應的私密金鑰遭誤用或破解

(8)正確地使用憑證，只使用於符合憑證實務作業基準與用戶接受條款的合法與經授權的使用目的，包含只安裝 SSL 憑證於憑證中所註記之完全吻合網域名稱的伺服器、不使用程式碼簽章憑證相對應之私密金鑰簽署惡意軟體。

(9)於憑證到期後合宜地停止使用憑證與其對應之私密金鑰。

9.6.4 信賴憑證者之責任

使用憑證機構簽發憑證的信賴憑證者應負以下之責任：

(1)熟知憑證之應用範圍及保證等級。

(2)依憑證之適用範圍使用憑證。

(3)正確檢驗數位簽章。

(4)正確查驗憑證廢止清冊以確認憑證是否有效。(以保證等級測試級簽發之憑證不做規定)

(5)應確認憑證所記載之金鑰用途。

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

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

(8)接受使用憑證管理中心簽發之憑證時,即表示已了解同意有關憑證管理中心法律責任之條款,依照憑證實務作業基準所規定範圍使用憑證。

9.6.5 其他參與者之責任

不做規定。

9.7 免責聲明

憑證機構得在憑證實務作業基準中載明否認聲明及其限制條件(Disclaimers and Limitations),以排除不屬憑證機構責任之錯誤。但憑證機構不得將因自行疏忽所引起之後果列入排除條件中。

9.8 有限責任

憑證機構得在憑證實務作業基準中載明責任上限。

9.9 賠償

憑證機構之憑證實務作業基準應載明對用戶及信賴憑證者的賠償責任。

9.10 有效期限與終止

9.10.1 有效期限

本憑證政策和附件當公告於 eCA 網站與儲存庫時生效，且直到被新的版本取代前仍然有效。

9.10.2 終止

本憑證政策和附件直到被新的版本取代前仍然有效。

9.10.3 效力的終止與保留

透過 eCA 網站與儲存庫溝通憑證政策效力終止的狀況和影響。此溝通將強調憑證政策效力終止的保留情形，最起碼保護機密資訊的相關責任在憑證政策終止後仍將保留。

9.11 對參與者的個別通告與溝通

本公司接受對於有關憑證政策之意見以數位簽章電子郵件或書面通告（notice）於本政策 1.5.2 節之地址。通告在發文者收到有效與數位簽章之回執時才有效，如果回執在 5 天內沒有收到，可改採書面以快遞或掛號方式執行。

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，以維持其保證度。

9.12.2 通知機制和期限

9.12.2.1 通知機制

政策管理委員會及憑證機構應將對用戶可能產生重大影響的變更項目，分別公告於 eCA 及憑證機構之儲存庫，憑證機構應於憑證實務作業基準載明變更項目通知機制。

9.12.2.2 變更項目

憑證政策由政策管理委員會評估項目的變更對用戶或信賴憑證者影響程度：

(1)影響程度大者，應先公告 15 個日曆天，始得修訂。

(2)影響程度小者，應先公告 7 個日曆天，始得修訂。

9.12.2.3 意見之回覆期限

對於 9.12.2.2 節之變更項目有意見者，其回覆期限為：

(1)依照 9.12.2.2 節之(1)影響程度大者之回覆期限為自公告日起 7 個日曆天內。

(2)依照 9.12.2.2 節之(2)影響程度小者之回覆期限為自公告日起 3 個日曆天內。

憑證機構應於憑證實務作業基準載明意見之回覆期限。

9.12.2.4 處理意見機制

對於憑證政策變更項目有意見者，於意見回覆期限截止前，以總管理中心儲存庫公告之回覆方式傳送給總管理中心，總管理中心將考量相關意見，評估變更項目。

憑證機構應於憑證實務作業基準載明處理意見之機制。

9.12.2.5 最後公告期限

本憑證政策公告之變更項目依照 9.12.1 及 9.12.2 節規定進行修訂，公告期限依照 9.12.2.3 節規定至少公告 15 個日曆天，直到本憑證政策修訂生效。

9.12.3 必須修改憑證政策物件識別碼之事由

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

9.13 紛爭之處理程序

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，可依中華電信另訂之爭端解決程序，請求

解釋。憑證機構應在憑證實務作業基準中載明紛爭之處理程序。

9.14 管轄法律

牽涉本基礎建設所簽發之憑證的任何爭議由中華民國相關法令規定管轄。

9.15 適用法律

依據憑證政策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令規定。

9.16 一般條款

9.16.1 完整協議

憑證機構應透過合約或協議賦予註冊中心符合憑證政策和可適用的業界標準與指引。

憑證機構對於用戶和信賴憑證者應透過合約或協議提供憑證政策相關條款。

9.16.2 轉讓

本憑證政策內所敘述的成員不能未經本公司事先書面同意轉讓其權利或責任，除非在合約敘明，本公司不提供轉讓權利或責任的通知。

9.16.3 可分割性

如本憑證政策的任一章節不正確或無效時，其他章節仍然有效。

9.16.4 強制執行(律師費用與拋棄權利)

因可歸責於用戶或憑證信賴者之故意或過失違反本憑證政策相關規定，致總管理中心受有損害時，總管理中心除得請求損害賠償以外，並得向可歸責之一方請求支付為處理該爭議或訴訟之律師費用。總管理中心未向違反本憑證政策相關規定者主張權利，不代表總管理中心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，包含但不限於天災、戰爭、恐怖攻擊、電信網路中斷或天然災害等事件，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載明其他除外條款，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。

附錄 1：縮寫和定義

英文縮寫	英文全稱	中文名詞或定義
AIA	Authority Info Access	憑證機構存取資訊，參見附錄 2。
AICPA	American Institute of Certified Public Accountants	美國會計師公會，參見附錄 2。
CA	Certification Authority	憑證機構，參見附錄 2。
CCA	Cross Certification Agreement	交互認證協議書，參見附錄 2。
CARL	Certification Authority Revocation List	憑證機構廢止清冊，參見附錄 2。
CMM	Capability Maturity Model	能力成熟度模型，參見附錄 2。
CP	Certificate Policy	憑證政策，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。
CARL	Certificate Authorty Revocation List	憑證機構廢止清冊，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。
DV	Domain Validation	網域驗證，參見附錄 2。
eCA	ePKI Root Certification Authority	中華電信憑證總管理中心，參見附錄 2。
EE	End Entities	終端個體，參見附錄 2。
ePKI	Chunghwa Telecom ecommerce	中華電信公開金鑰基

	Public Key Infrastructure	礎建設，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。
IANA	Internet Assigned Numbers Authority, IANA	網路通訊協定註冊中心，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。
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	線上憑證狀態查詢協定。
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。
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	Security Socket Layer	安全插座層協定，參見附錄 2。
TLS	Transport Layer Security	傳輸層安全協定，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)，除金鑰外所需的隱密資料。
美國會計師公會 (American Institute of Certified Public Accountants, AICPA)	與加拿大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。
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)	當某個體出示身分時，確認其身分之正確性。而所謂的相互鑑別(Mutual Authentication)是指發生在進行通訊活動的兩方彼此進行鑑別。
鑑別程序	用以建立資料傳送、訊息、來源者之安全措施，

(Authentication)	或是驗證個人接收特定種類資訊權限之方法。
憑證機構存取資訊(Authority Info Access, AIA)	記載有關存取憑證機構資訊的擴充欄位，內容可包含：線上憑證狀態查詢協定(OCSP)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。
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。
能力成熟度模型(Capability Maturity Model, CMM)	由美國卡內基美隆大學（Carnegie Mellon University, CMU）的軟體工程研究所（Software Engineering Institute, SEI）以軟體流程評鑑（Software Process Assessment, SPA）與軟體能力評估（Software Capability Evaluation, SCE）為基礎的框架，協助軟體開發業者找出軟體開發流程需要改善之處。
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。 在本憑證政策中所提及的“憑證”特別指其格式為 X.509 v.3，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機構廢止清冊或憑證廢止清冊。
憑證機構廢止清冊(Certification Authority Revocation List, CARL)	經簽署及蓋時戳之清單，清單中為已被廢止之憑證機構公開金鑰憑證(包括下屬憑證機構憑證或交互憑證)之序號。
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、展期及存取等)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。
元件私密金鑰(Component Private Key)	與憑證簽發設備功能相關聯的私密金鑰，相對於與操作員或管理者相關聯的私密金鑰。
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)	在兩個憑證總管理中心(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(CA Certificate)，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。
金鑰效期(Cryptoperiod)	每個金鑰設定之有效期限。
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	將電子文件以數學演算法或其他方式運算為一

(Digital Signature)	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)
雙重用途憑證 (Dual-Use Certificate)	可用於數位簽章及資料加密兩種服務的憑證。
憑證效期 (Duration)	1 憑證欄位，由“有效期限起始時間”(notBefore)及“有效期限截止時間”(notBefore)兩個子欄位所組成。
網域驗證(Domain Valiadition, DV)	SSL 憑證之核發，鑑別用戶之網域控制權但並未鑑別用戶之組織或個人身分。故連結安裝網域驗證型 SSL 憑證之網站，可提供 SSL 加密通道，但無法知道該網站之擁有者是誰。
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。
加密憑證 (Encryption Certificate)	1 憑證，包含用以加密電子訊息、檔案、文件或資料的公開金鑰，此金鑰亦可用來建立或交換以上各項加密用途的短期密鑰。
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。
中華電信公開金鑰基礎建設（Chunghwa	中華電信股份有限公司為推動電子化政策，健全電子商務基礎環境，依照 ITU-T X.509 標準建置的階層式公開金鑰基礎建設，可適用於電子

Telecom ecommerce Public Key Infrastructure, ePKI）	商務與電子化政府的各項應用。
中華電信公開金鑰基礎建設政策管理委員會(ePKI Policy Managemet Committee，簡稱政策管理委員會)	1 組織，其設立目的為：研議本基礎建設憑證政策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他如審議憑證實務作業基準等電子憑證管理事項。
中華電信憑證總管理中心(ePKI Root CA, eCA)	中華電信公開金鑰基礎建設的根憑證機構(Root Certification Authority, 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。
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。
金鑰產製原料 (Key Generation Material)	用於產製金鑰的隨機亂數、擬隨機亂數及其他密碼參數。
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 把金鑰要推出另 1 把金鑰(從計算的角度而言)是不可行的。
交互認證協議書 (Cross Certification Agreement, CCA)	總管理中心與交互認證憑證機構就交互憑證機構申請加入本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。
網路通訊協定註冊中心（Internet Assigned Numbers Authority, IANA）	網際網路位址指派機構，負責管理國際網際網路中使用的 IP 位址、網域名稱和許多其它參數
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。
命名機構(Naming Authority)	負責指定唯一識別名稱並確保每個唯一識別名稱有意義且在其領域內為唯一的權責單位。
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。其所制訂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)	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；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 1 章第 2 條第 4 項) 。 (2)向國際認可之標準機構(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。
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)	SSL 憑證核發過程中，除了識別與鑑別用戶之網域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或個人身分。故連結安裝組織驗證型 SSL 憑證之網站，可提供 SSL 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。
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。
註冊中心(Registration Authority, RA)	(1)負責確認憑證申請人之身分或其他屬性，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份(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。
憑證展期(Renew (a certificate)	藉由簽發新的憑證，以延展公開金鑰憑證所連結資料有效性的程序。
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)包含本憑證政策與憑證相關資訊的資料庫。
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。
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，除了簽發下屬 CA 憑證與自簽憑證外，其自簽憑證由應用軟體提供者負責散布，中文也有稱為憑證總管理中心或最頂層憑證機構。
安全插座層 (Secure Socket 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。
秘密金鑰 (Secret Key)	在對稱式密碼系統中“共持的秘密”，使用者之身分鑑別是藉由 password、PIN 或與遠端主機(或伺服器)共享的其他秘密。 單一的金鑰由兩方共持：傳送方用以加密傳送訊息，而收受方用以解密此訊息。此共持的金鑰由兩方在事前所協議的演算法生成。

簽章憑證 (Signature Certificate)	公開金鑰憑證包含用以驗證數位簽章(而非用於加密資料或其他密碼功用)之公開金鑰。
簽發憑證機構 (Subject CA)	對於 1 張憑證機構憑證(CA Certificate)而言，該憑證的憑證主體(Subject)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)	(1)指憑證中所命名或識別之主體，且其持有與憑證中所載公開金鑰相對應之私密金鑰者。(憑證實務作業基準應載明事項準則第 1 章第 2 條第 5 項) (2)具下列特性之個體，包括(但不限於)個人、機構、伺服器軟體或網路裝置： (a)簽發憑證上所載明之主體。 (b)擁有與憑證上所列公開金鑰對應之私密金鑰。 (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。
時戳	由可信賴的權威機構以數位方式簽署，證明某

(Time stamp)	特定數位物件在某特別時間之存在。
傳輸層安全協定 (Transport Layer Security, TLS)	由網際網路工程任務小組(IETF)將 SSL 協定制訂為 RFC 2246，並將其稱為 TLS (Transport Layer Security)，其最新版本是 RFC 5246，亦即 TLS 1.2 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。
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。