政府憑證管理中心

憑證實務作業基準

(Government Certification Authority Certification Practice Statement)

第 2.0 版

主辦機關：國家發展委員會

執行機構：中華電信股份有限公司數據通信分公司

中華民國 110 年 7 月 2 日

政府憑證管理中心憑證實務作業基準版本修訂歷程

版本	生效日期	修訂內容說明
Ver1.3	2010/10/18	加入政府機關所設立的時戳服務機構（Time Stamp Authority，TSA）申請憑證的相關規定
Ver1.4	2012/03/14	1. 修訂憑證收費方式 2. 修訂 GRCA 對外公布之公開資訊類型 3. 增修個人資料處理依據之法令
Ver1.5	2013/06/25	1. 定義逾保存年限資料之處理方式 2. 修訂憑證管理中心金鑰管理方式 3. 新增 SHA-2 演算法 4. 新增密碼模組之標準 5. 修訂安全控管措施
Ver1.6	2014/05/20	1. 行政院研究發展考核委員會組改為國家發展委員會 2. 修訂憑證管理中心金鑰使用期限
Ver1.7	2015/03/18	1. 新增憑證 IC 卡線上屆期換發流程 2. 新增配合組織改造憑證換發流程
Ver1.8	2016/04/19	1. 新增 CA/Browser Forum 所發行之 Baseline Requirements 之規範 2. 新增寫入憑證內之電子郵件驗證 3. 新增網域名稱擁有者識別程序
Ver1.9	2017/12/25	1. 修訂憑證管理中心憑證命名規則 2. 新增個人身分鑑別之程序 3. 修訂網域名稱擁有者識別程序 4. 新增憑證廢止事由 5. 縮短 TLS 類憑證效期 6. 刪除 SHA-1 演算法
Ver2.0	2020/11/3	1. 更版為 RFC3647 架構 2. 刪除有關遵循 CA/Browser Forum 制定之 Baseline Requirements 相關敘述 3. 移除附錄 3。 4. GCA 調整為僅能簽發政府機關內部主機專用之 TLS 憑證。

目　　錄

摘要

政府憑證管理中心憑證實務作業基準之重要事項說明如下：

1、主管機關核定文號：經商字第(待確認)號

2、簽發之憑證：

(1) 種類：

■ 政府機關(構)及單位憑證。

■ 專屬類憑證。

■ 政府非對外系統或網站使用之 TLS 憑證。

(2) 保證等級：政府憑證管理中心依政府機關公開金鑰基礎建設憑證政策保證等級第 3 級運作，簽發憑證政策所定義保證等級第 3 級之憑證。

(3) 適用範圍：本管理中心所簽發之憑證適用於應用服務之身分識別與資料加密，用戶與信賴憑證者須謹慎使用本管理中心所簽發之憑證，並排除本作業基準所限制與禁止之憑證適用範圍。

3、法律責任重要事項：

(1) 用戶或信賴憑證者如未依本作業基準規定之適用範圍使用憑證所引發之後果，本管理中心不負任何法律責任。

(2) 用戶或信賴憑證者如因使用憑證而發生損害賠償事件時，本管理中心之損害賠償責任，以相關法令規定所訂之責任

範圍為限。

(3) 如因不可抗力或其他非可歸責於本管理中心之事由所衍生之損害事件，本管理中心不負任何法律責任。

(4) 註冊中心因執行註冊工作所引發之法律責任，除法令另有規定外，由本管理中心負責。

(5) 用戶提供不正確資料而導致信賴憑證者遭受損害時，相關法律責任應由用戶自行負責。

(6) 用戶之憑證如須暫停使用、恢復使用、廢止或重發，應依照本作業基準相關規定辦理，用戶仍應承擔異動前所有使用該憑證之法律責任。

4、其他重要事項：

(1) 本管理中心如有系統維護、轉換及擴充等需求時，得暫停部分憑證服務，並公告於儲存庫與通知用戶，用戶或信賴憑證者不得以此作為要求本管理中心損害賠償之理由。

(2) 註冊中心如因審驗錯誤，導致用戶或信賴憑證者遭受損害時，註冊中心之損害賠償責任，以相關法令規定所訂之責任範圍為限。

(3) 用戶接受本管理中心所簽發之憑證後，即表示已確認憑證內容資訊之正確性，並依本作業基準相關規定使用憑證，憑證內容資訊如有誤，用戶應主動通知本管理中心。

(4) 用戶與信賴憑證者應慎選安全之電腦環境與可信賴之應用系統，如因電腦環境或應用系統本身因素，導致使用者

權益受損時，應自行承擔責任。

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

(6) 信賴憑證者接受使用本管理中心簽發之憑證時，即表示已了解且同意本管理中心法律責任之條款，並依本作業基準相關規定使用憑證。

(7) 本管理中心之外部稽核作業，係由電子化政府主管機關依政府採購法委託公正第三方辦理外部稽核作業。

(8) 除另有規定外，本作業基準修訂生效後，如修訂之內容與原作業基準牴觸時，以修訂之內容為準；如以附加文件方式修訂，而該附加文件內容與原作業基準牴觸時，以該附加文件內容為準。

1.簡介

政府憑證管理中心憑證實務作業基準(Government Certification Authority Certification Practice Statement，以下簡稱本作業基準)係依政府機關公開金鑰基礎建設憑證政策(Government Public Key Infrastructure Certificate Policy，以下簡稱憑證政策)所訂定，並遵循電子簽章法及其子法「憑證實務作業基準應載明事項準則」相關規定，進行憑證之簽發與管理作業。

本作業基準文件格式參考網際網路工程任務小組(Internet Engineering Task Force, IETF)之徵求修正意見書 RFC 3647 建議之格式。

1.1 總覽

政府憑證管理中心(Government Certification Authority, GCA，以下簡稱本管理中心)係政府機關公開金鑰基礎建設(Government Public Key Infrastructure, GPKI，以下簡稱本基礎建設)之第 1 層下屬憑證機構(Level 1 Subordinate Certification Authority)。

本管理中心負責簽發與管理政府機關(構)及單位憑證、TLS 類憑證及專屬類憑證。

本作業基準係說明本管理中心之憑證簽發與管理作業符合憑證政策所訂定之保證等級第 3 級之規定。本作業基準所載明之實務作業規範僅適用於與本管理中心相關之個體，如本管理中心、註冊中心(Registration Authority, RA)、用戶(Subscriber)、信賴憑證者(Relying Party)及儲存庫(Repository)等。

國家發展委員會(以下簡稱國發會)為本管理中心之主管機關，負責本作業基準之訂定與修訂，本作業基準須經電子簽章法主管機關經濟部核可後施行。本作業基準未授權本管理中心以外之憑證機構使用，其他憑證機構如因引用本作業基準而引發之任何問題，由該憑證機構自行負責。

1.2 文件名稱及識別

1. 文件名稱：政府憑證管理中心憑證實務作業基準
2. 版本：第 2.0 版
3. 公布日期：110 年 XX 月 XX 日(待定)
4. 發布網址：

   https://gca.nat.gov.tw/download/GCA_CPS_v2.0.pdf
5. 憑證政策物件識別碼(Certificate Policy Object Identifier, CP OID)：id-tw-gpki-certpolicy-class3Assurance、{id-tw-gpki-certpolicy 3}。

1.3 主要成員

本管理中心主要成員包括：

1. 本管理中心。
2. 註冊中心。
3. 用戶。
4. 信賴憑證者。

5. 其他相關成員，包括發卡中心及國發會授權管理、建置與系統維運之委外單位。

1.3.1 本管理中心

負責政府機關(構)及單位憑證、TLS 類憑證及專屬類憑證簽發與管理作業。

1.3.2 註冊中心

負責收集、驗證用戶身分及憑證相關資訊之註冊工作。註冊中心由註冊窗口組成，並有憑證註冊審驗人員，負責受理憑證之註冊、暫停使用、恢復使用及廢止等業務。

註冊中心設置註冊中心伺服器，負責驗證憑證註冊審驗人員之身分與管理註冊窗口。註冊中心伺服器由註冊中心管理員負責管理，註冊中心管理員於註冊中心伺服器上設定憑證註冊審驗人員之帳號與權限，並製發憑證註冊審驗人員 IC 卡。註冊中心伺服器上裝設註冊中心之私密金鑰，註冊中心伺服器與本管理中心伺服器間之通訊，由註冊中心之私密金鑰簽章加以保護。

1.3.3 用戶

1. 用戶係指政府機關(構)及單位。

2. 用戶使用之符記(Token)主要採 IC 卡，亦可使用非 IC 卡類硬體密碼模組，每個符記可同時儲存簽章用與加解密用 2 種憑證。

3. 每個用戶僅可申請 1 張正卡，惟可依應用需要申請多張附卡。

4. TLS 憑證及專屬類憑證無正、附卡之區分，憑證之金鑰用途依需求可為簽章用或加解密用。

1.3.4 信賴憑證者

指相信憑證主體名稱與公開金鑰連結關係之個體。

信賴憑證者使用本管理中心所簽發之憑證前，須以本管理中心本身之憑證與憑證狀態資訊，檢驗所使用憑證之有效性。確認憑證有效性後，方可使用憑證識別用戶及其網路伺服器名稱，並與憑證主體間建立安全之通訊管道。

1.3.5 其他相關成員

1.3.5.1 發卡中心

發卡中心進行憑證 IC 卡製作，並負責郵寄予用戶。作業說明如下：

1. IC 卡內部產製金鑰對。
2. 以亂數設定 IC 卡之初始個人識別碼(Personal Identification Number, PIN，以下簡稱 PIN 碼)。
3. 將申請資料與公開金鑰透過安全管道傳送予本管理中心簽發憑證。
4. 將憑證寫入 IC 卡中與印卡等工作。

1.3.5.2 委外服務單位

國發會依照政府採購法委託合格廠商，負責本管理中心之建置與系統維運作業。

1.4 憑證用途

1.4.1 憑證適用範圍

本管理中心所簽發與管理之憑證，包括政府機關(構)及單位憑證、政府非對外系統或網站使用之 TLS(Transport Layer Security)類憑證及專屬類憑證，適用範圍如下：

1. 應用服務所須之身分識別與資料加密。
2. 政府非對外系統或網站使用之 TLS 通訊協定。
3. 專屬伺服器應用系統識別或提供時戳服務。

1.4.3 憑證之禁止使用範圍

1. 犯罪。
2. 軍令戰情與核生化武器管制。
3. 核能運轉設備。
4. 航空飛行與管制系統。

1.4.2 憑證之使用限制

1. 用戶使用私密金鑰時，應慎選安全之電腦環境與可信賴之應用系統，以避免私密金鑰被惡意軟硬體盜取或誤用而引發權益受損。
2. 信賴憑證者使用本管理中心所簽發之憑證前，應確認憑證之類別、正附卡別、保證等級及金鑰用途等符合應用需求。

3. 信賴憑證者應依 X.509 規範處理憑證中之關鍵性與非關鍵性憑證擴充欄位。

4. 信賴憑證者須遵守本作業基準之規定。

1.5 聯絡方式

1.5.1 憑證實務作業基準之制訂及管理機構

1. 本管理中心負責制訂及管理本作業基準。

2. 本作業基準須經電子簽章法主管機關經濟部核可後公布施行。

1.5.2 聯絡資料

本管理中心聯絡方式如下：

- 電子郵件信箱：egov@service.gov.tw
- 憑證問題回報信箱：gca@gca.nat.gov.tw
- 聯絡電話：02-2192-7111
- 郵遞地址：100223 台北市中正區寶慶路 3 號 國家發展委員會

1.5.3 憑證實務作業基準之審定

本作業基準經行政機關電子憑證推行小組審查後，經電子簽章法主管機關經濟部核定，始得對外提供簽發憑證服務。

1.5.4 憑證實務作業基準變更程序

本作業基準之變更依 1.5.3 節「憑證實務作業基準之審定」規定辦理，憑證政策或總管理中心知憑證實務作業基準如有修訂並公告後，本作業基準應配合修訂。

1.6 名詞定義及縮寫

詳參附錄 **1**「名詞解釋」與附錄 **2**「英文名詞縮寫」。

2.資訊公布及儲存庫責任

2.1 儲存庫

1. 儲存庫應公布資訊如下：

(1) 簽發之憑證、憑證廢止清冊及其他憑證相關資訊。

(2) 憑證政策及本作業基準。

(3) 最新外部稽核結果。

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

2. 儲存庫提供 24 小時服務，網址：

「https://gca.nat.gov.tw/web2/database04.html」。

3. 儲存庫之存取控制依照 2.4 節「存取控制」規定辦理。

4. 儲存庫服務如因故無法正常運作時，須於 2 個工作天內恢復正常運作

2.2 憑證資訊公布

本管理中心採以下方式公布憑證資訊：

1. 本作業基準。

2. 憑證廢止清冊(Certificate Revocation List, CRL)。

3. 提供線上憑證狀態協定(Online Certificate Status Protocol, OCSP)查詢服務。

4. 儲存庫之憑證查詢服務。

2.3 公布頻率或時間

1. 本作業基準審查核定後 10 個工作天內公告於儲存庫。
2. 本管理中心每日至少簽發並公告 1 次憑證廢止清冊。
3. 本憑證實務作業基準所指日數,如未特別標示為"工作天"者,均以日曆天計算。

2.4 存取控制

1. 本管理中心建置資安防護機制，外界無法直接連線至內部主機。
2. 用戶及憑證信賴者透過儲存庫查詢，儲存庫主機透過安全控管連線至本管理中心主機之資料庫。
3. 本管理中心只允許經授權之人員管理儲存庫主機。

3.識別及鑑別程序

3.1 命名

3.1.1 命名種類

1. 憑證主體名稱採用 ITU-T X.500 唯一識別名稱。
2. 用戶憑證主體別名(Subject Alternative Name)擴充欄位須為非關鍵性擴充欄位。

3.1.2 命名須有意義

1. 憑證主體名稱之命名方式應符合政府相關法令規定。
2. 專屬類憑證之唯一識別名稱，包括：
   - 憑證主體名稱：伺服器應用軟體之所有人或經授權之使用人。
   - 一般名稱：伺服器應用軟體名稱。
   - 序號：本管理中心對伺服應用軟體所編訂之識別代號。
3. TLS 憑證說明如下：
   - 一般名稱與憑證主體別名欄位應註記網域名稱。
   - 唯一識別名稱應包含所驗證之組織身分資訊於其組織名稱(Organization Name)欄位屬性。
   - 多網域 TLS 憑證可記載多個用戶能控制之完全吻合網域名稱於 1 張憑證之憑證主體別名欄位。

- 萬用網域 TLS 憑證使用萬用字元(*)放置註記在憑證主體名稱之通用名稱欄位的網域名稱最左邊，以適用於該次網域內的所有網站。

3.1.3 用戶匿名或假名

本管理中心不簽發匿名憑證或假名憑證。

3.1.4 命名形式之解釋規則

1. 依「政府機關公開金鑰基礎建設憑證及憑證廢止清冊格式剖繪」各式命名形式之解釋規則。
2. 依 ITU-T X.520 名稱屬性定義

3.1.5 命名獨特性

1. 憑證機構憑證

憑證機構憑證之 X.500 唯一識別名稱原為：

C=TW，O=行政院，OU=政府憑證管理中心

為便於與國際互通，本管理中心自民國 106 年 12 月 22 日起，新簽發憑證機構憑證之 X.500 唯一識別名稱使用以下格式：

C=TW，O=行政院，CN=政府憑證管理中心 - Gn

其中，n=3,4…

2. 用戶憑證

本管理中心簽發之各類憑證主體名稱格式皆須遵循「政府機關公開金鑰基礎建設憑證及憑證廢止清冊格式剖繪」之規定。

3.1.6 商標之辨識、鑑別及角色

不適用。

3.1.7 命名爭議解決程序

1. 用戶名稱所有權有爭議時，依相關法令規定辦理。
2. 網域名稱或 IP Address 所有權有爭議時，依相關主管機關處理程序辦理。

3.2 初始註冊

3.2.1 證明擁有私密金鑰之方式

1. 用戶使用之符記為 IC 卡時，由本管理中心所信賴之發卡中心產製金鑰對，用戶於申請憑證時不須證明持有私密金鑰。
2. 用戶自行產製金鑰對時，以該金鑰對產製 PKCS#10 憑證申請檔並加以簽章後交予註冊中心，註冊中心使用該用戶之公開金鑰驗證該憑證申請檔之簽章，以證明用戶擁有相對應之私密金鑰。

3.2.2 組織身分之鑑別程序

1. 一般申請

用戶填寫憑證申請書後以公文提出申請，由本管理中心驗證公文之正確性，以證明該機關(構)及單位確實存在且申請獲得授權。

2. 憑證 IC 卡線上屆期換發

憑證 IC 卡將屆期換發者，可持有效之憑證 IC 卡線上申請換發，由註冊中心檢驗其憑證 IC 卡之數位簽章，以鑑別用戶之身分，並檢驗政府目錄服務系統以確認該機關(構)、單位確實存在。

3. 配合政策換發憑證

因政府組織改造、行政區域重新劃分或用戶之上級機關命名規則變更等政策性因素，致須換發憑證者，經本管理中心同意得由用戶之上級機關以公文書方式代為申請，憑證管理中心應檢驗該上級機關公文書之完整性。

4. TLS 類憑證申請

申請 TLS 憑證時可透過以下方式進行身分鑑別：

(1) 用戶填寫憑證申請書後以公文提出申請，由本管理中心驗證公文之正確性，以證明該機關(構)及單位確實存在且申請獲得授權。

(2) 以有效之政府機關(構)及單位憑證 IC 卡線上申請，由註冊中心檢驗其憑證 IC 卡之數位簽章，以鑑別用戶之身分，並確認該機關(構)及單位確實存在。

3.2.3 個人身分之鑑別程序

不適用

3.2.4 未經驗證之用戶資訊

未經驗證之用戶資訊不得寫入憑證。

3.2.5 權責之確認

1. 用戶申請憑證時，應依 3.2.2 節「組織身分之鑑別程序」規定辦理身分鑑別。

2. 用戶申請 TLS 憑證時，除依 3.2.2 節「組織身分之鑑別程序」規定進行組織之身分鑑別外，還須依 3.2.8 節「網域名稱擁有者鑑別之程序」規定鑑別用戶具備網域名稱之擁有權與控制權。

3.2.6 交戶運作標準

不適用。

3.2.7 資通訊設備或伺服器應用軟體鑑別之程序

由設備或應用系統管理者提出憑證申請，本管理中心應依 3.2.2 節「組織身分之鑑別程序」規定進行組織之身分鑑別。

3.2.8 網域名稱擁有者鑑別之程序

1. 用戶若以政府網際服務網(Government Service Network, GSN)註冊之網域(.gov)或 IP Address 申請 TLS 憑證時，本管理中心透過政府中英文網域名稱註冊系統，驗證該網域確實屬該申請者所註冊擁有且用戶具有控制權，並依 3.2.2 節「組織身分之鑑別程序」辦理身分鑑別。

2. 用戶若以教育部管理之網域(.edu)或 IP Address 申請 TLS 憑證時，由國發會授權教育部之審驗窗口驗證該網域確實屬該申請者所註冊擁有且用戶具有控制權，本管理中心依 3.2.2 節「組織身分之鑑別程序」辦理身分鑑別。

3.3 金鑰更換請求之識別及鑑別

3.3.1 例行性金鑰更換識別及鑑別

用戶私密金鑰使用期限屆滿更換金鑰對並重新申請憑證時，本管理中心應依 3.2 節「初始註冊」規定辦理。

3.3.2 憑證廢止之金鑰更換識別及鑑別

用戶因憑證廢止而申請新憑證時，本管理中心應依 3.2 節「初始註冊」規定辦理。

3.3.3 憑證展期之金鑰更換

本管理中心簽發之用戶憑證不得展期。

3.4 憑證廢止申請之識別及鑑別

憑證廢止申請之鑑別依 3.2 節「初始註冊」規定辦理。

3.5 憑證暫時停用與恢復使用之識別及鑑別

用戶提出憑證暫時停用或恢復使用申請時，本管理中心以該用戶之用戶代碼做為身分鑑別之依據。

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

1. 政府機關(構)授權之人員。

2. 電腦、通訊設備或應用軟體等設備，因其在法律上不具行為能力，須由該設備或應用軟體之擁有者或經授權之使用人提出憑證申請。

4.1.2 註冊程序及責任

1. 憑證簽發前註冊中心應確認憑證申請者之身分。

2. 憑證申請者應提供身分識別相關文件。

3. 用戶責任如下：

(1) 遵守本作業基準及用戶約定條款，並確保提供申請資料之正確性。

(2) 確認憑證內容資訊之正確性，並依 4.4 節「接受憑證之程序」規定辦理憑證接受；若憑證內容資訊不正確，應立即通知註冊中心。

(3) 依 1.4.1 節「憑證之適用範圍」規定使用憑證。

(4) 妥善保管與使用其私密金鑰。

(5) 憑證如須暫停使用、恢復使用、廢止或重發，應依第 4 章「憑

證生命週期營運規範」規定辦理，用戶應承擔憑證異動前所有使用該憑證之相關法律責任。

(6) 用戶應確保其電腦環境與應用系統之安全性。

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

4.2 申請憑證之程序

1. 政府機關(構)、單位憑證申請程序

(1)憑證申請人連線至本管理中心網站填寫憑證申請書。

(2)憑證申請人將憑證申請書以公文函送註冊窗口辦理。

2. 憑證 IC 卡線上屆期換發程序

憑證 IC 卡將屆期者，於憑證管理中心網站公告之換發期限內，持有效憑證線上申請屆期換發，註冊中心應依 3.2.2 節「組織身分之鑑別程序」規定辦理身分鑑別，並於驗證數位簽章後簽發憑證，。

3. 由用戶之上級機關代為申請憑證之程序

因配合政府組織改造、行政區域重新劃分或用戶之上級機關命名規則變更等政策性因素，致須換發憑證者，可由用戶之上級機關代為申請憑證，申請程序如下：

(1) 憑證申請人至本管理中心網站填寫憑證申請書。

(2) 本管理中心同意由用戶之上級機關以公文書方式代為申請後，依 3.2.2 節「組織身分之鑑別程序」規定辦理身分鑑別。

4. TLS 憑證及專屬類憑證申請程序

(1) 憑證申請人至本管理中心網站線上提出憑證申請。

(2) 憑證申請人自行產製金鑰對，使用該金鑰對產製 PKCS#10 憑證申請檔後加以簽章，並將憑證申請檔上傳。

(3) 憑證申請人將憑證申請書以公文函送註冊窗口辦理。

(4) 如以機關(構)、單位憑證 IC 卡線上申請 TLS 憑證者，無須以公文函送申請書。

4.2.1 執行識別及鑑別功能

本管理中心依 3.2.2 節「組織身分之鑑別程序」規定辦理識別及鑑別程序，說明如下：

1. 用戶身分識別及鑑別

(1) 憑證審驗人員收到公文後，應依照審驗作業規範進行公文文號與發文單位進行比對，藉此進行身分識別、鑑別並確認該申請有經過授權。

(2) 若以機關(構)、單位憑證 IC 卡線上申請者，註冊中心將驗證其數位簽章做為身分鑑別之依據。

2. 網域擁有者鑑別

本管理中心僅提供政府機關(構)與單位申請 TLS 憑證，並依

3.2.8 節「網域名稱擁有者鑑別之程序」規定辦理網域鑑別。

4.2.2 憑證申請之核准或拒絕

本管理中心完成申請資料審核、身分識別及鑑別作業後，始可核准憑證申請。

本管理中心於以下狀況得拒絕簽發憑證：

1. 未能通過 3.2.2 節「組織身分之鑑別程序」之要求。
2. 申請者曾違反用戶約定條款。
3. 其他經本管理中心認定得拒絕簽發之事項。

4.2.3 處理憑證申請之時間

註冊中心處理憑證申請之時間及本管理中心簽發憑證之時間，視不同憑證類別於用戶約定條款、相關文件或網站揭露。

4.3 簽發憑證之程序

4.3.1 本管理中心於憑證簽發時之作業

本管理中心與註冊中心於收到憑證申請資料後，依本作業基準第3章「識別及鑑別程序」規定進行審核程序，憑證申請審核及簽發程序如下：

4.3.1.1 政府機關(構)及單位憑證

1. 一般申請流程

   憑證註冊審驗人員依 3.2 節「初始註冊」規定對申請用戶進行身分鑑別並檢查憑證申請資料，確認無誤後以註冊審驗人

員之IC卡對憑證申請資料加簽數位簽章，並將相關資料上傳至註冊中心，憑證簽發作業流程因用戶使用之符記不同分為以下兩種程序：

(1) IC卡類符記：

a. 發卡中心於IC卡內部產製金鑰對。

b. 亂數設定IC卡之初始PIN碼。

c. 申請資料及公開金鑰透過安全管道傳送至本管理中心進行憑證簽發並寫入IC卡中。

d. 憑證IC卡印製、包裝及郵寄。

(2) 非IC卡類符記：

本管理中心對審核通過之申請案件進行憑證簽發，憑證簽發後電子郵件方式通知用戶。

2. 憑證IC卡線上屆期換發流程

用戶須使用將屆期憑證IC卡對憑證申請資料簽章，註冊中心驗證其數位簽章且完成身分鑑別後，依上述「一般申請流程」執行發卡作業。

4.3.1.2 專屬類憑證

專屬類憑證之簽發審核程序如下：

1. 憑證註冊審驗人員依3.2.7節「資通訊設備或伺服器應用軟體鑑別之程序」規定進行鑑別程序及申請資料審核。

2. 審核通過之申請案件，由本管理中心簽發憑證後以電子郵件方式通知用戶。

4.3.1.3 TLS 憑證

TLS憑證之簽發審核程序如下：

3. 憑證註冊審驗人員依 3.2.2 節「組織身分之鑑別程序」及 3.2.8 節「網域名稱擁有者鑑別之程序」規定完成機關(構)身分鑑別、網域名稱擁有者鑑別及申請資料審核。

4. 審核通過之申請案件，由本管理中心簽發憑證後以電子郵件方式通知用戶。

4.3.2 本管理中心對用戶之憑證簽發通知

1. 憑證 IC 卡簽發後，本管理中心於憑證簽發後以郵寄方式將憑證 IC 卡交予用戶。

2. 非 IC 卡類、專屬類及 TLS 類憑證簽發後，以電子郵件方式通知用戶。

3. 用戶可於憑證管理中心網站查詢憑證申請進度。

4. 如不同意簽發憑證時，應以電子郵件或電話通知用戶，並明確告知不同意簽發之理由。

4.4 接受憑證之程序

1. 用戶於取得憑證並確認憑證內容無誤後，應進行憑證接受，憑證接受程序說明如下：

(1) 憑證 IC 卡

a. 連線至本管理中心網站選擇開卡作業。

b. 檢查憑證主體名稱及憑證內容。

c. 確認憑證內容無誤後依照網頁指示操作並輸入申請憑證時所設定之用戶代碼，表示接受憑證。

d. 進行 IC 卡初始 PIN 碼修改，若因 PIN 碼輸入錯誤多次導致憑證 IC 卡被鎖定無法使用，請至憑證管理中心網站進行線上解鎖。

(2) 非 IC 卡類憑證、專屬類憑證、TLS 憑證

a. 連線至本管理中心網站選擇憑證接受作業。

b. 檢查憑證主體名稱及憑證內容。

c. 確認憑證內容無誤後依照網頁指示操作並輸入申請憑證時所設定之用戶代碼，表示接受憑證。

2. 用戶如發現憑證內容不正確時，應停止憑證接受作業，並立即通知本管理中心或註冊中心。

3. 憑證申請者如於 90 個工作天內未完成憑證接受作業，該憑證自動被停用，不另行公布。

4.4.1 接受憑證之要件

憑證申請者確認憑證內容無誤後，以申請憑證時所設定之用戶代碼做為憑證接受之依據。

4.4.2 本管理中心之憑證發布

本管理中心將所簽發之憑證公布於儲存庫，或以電子郵件、郵遞方式將憑證傳遞用戶。

4.4.3 本管理中心對其他個體之憑證簽發通知

本管理中心將所簽發之憑證公布於儲存庫。

4.5 金鑰對及憑證之用途

4.5.1 用戶私密金鑰及憑證使用

1. 用戶金鑰對之產製應符合 6.1.1 節「金鑰對產製」，且用戶須有私密金鑰之控制權。

2. 用戶私密金鑰不得用於簽發憑證。

3. 用戶應保護私密金鑰不被未經授權之他人使用或揭露，且確保私密金鑰依憑證擴充欄位所註記之金鑰用途使用。

4. 用戶須依憑證政策及本作業基準之規定使用憑證。

4.5.2 信賴憑證者公開金鑰及憑證使用

1. 信賴憑證者使用憑證時須符合本作業基準規定。

2. 信賴憑證者應使用符合 ITU-T X.509、IETF RFC 等相關標準或規範之軟體。

3. 信賴憑證者需驗證憑證有效性，包括憑證及其憑證串鏈中所有憑證機構之憑證。

4. 信賴憑證者應檢驗簽發憑證機構與用戶憑證之憑證政策，以確認憑證之保證等級。

5. 信賴憑證者應確認憑證用途。

4.6 憑證展期

本管理中心不提供憑證展期。

4.6.1 憑證展期之事由

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 接受展期憑證之要件

不適用。

4.6.6 憑證機構之展期憑證發布

不適用。

4.6.7 本管理中心對其他個體之展期憑證簽發通知

不適用。

4.7 憑證之金鑰更換

指重新產生一組公開金鑰及私密金鑰對，並以原有的註冊資訊向憑證機構申請憑證簽發。

4.7.1 憑證之金鑰更換事由

4.7.1.1 本管理中心憑證之金鑰更換事由

1. 私密金鑰執行簽發憑證用途之使用期限到期。

2. 本管理中心憑證被廢止。

4.7.1.2 用戶憑證之金鑰更換事由

1. 用戶私密金鑰使用期限到期。

2. 用戶憑證被廢止。

4.7.2 更換憑證金鑰之申請者

1. 本管理中心憑證之金鑰更換

   由本管理中心授權之人員向總管理中心提出下屬憑證機構憑證之申請。

2. 用戶憑證之金鑰更換

   政府機關(構)授權之人員。

4.7.3 憑證之金鑰更換程序

1. 本管理中心應依總管理中心之憑證實務作業基準相關規定重新申請憑證。

2. 用戶應依 4.1 節「申請憑證」及 4.2 節「申請憑證之程序」規定辦理。

4.7.4 用戶憑證金鑰更換之簽發通知

依4.3.2節「本管理中心對憑證申請者之通知」規定辦理。

4.7.5 接受憑證金鑰更換之要件

1. 本管理中心依總管理中心之憑證實務作業基準 4.7 節「憑證之金鑰更換」相關規定接受金鑰更換之憑證。

2. 用戶依 4.4.1 節「接受憑證之要件」規定接受金鑰更換之憑證。

4.7.6 本管理中心之更換金鑰憑證發布

本管理中心將已完成金鑰更換之憑證公布於儲存庫，或以電子郵件、郵遞方式將憑證傳遞用戶 。

4.7.7 本管理中心更換金鑰後對其他個體之通知

本管理中心將金鑰更換後之憑證公布於儲存庫。

4.8 憑證變更

4.8.1 憑證變更之事由

1. 憑證變更係指同一憑證主體變更憑證內次要屬性資訊(憑證管理中心目前僅提供電子郵件位址變更)時，提供 1 張新憑證，新憑證使用舊憑證主體之公開金鑰，惟新憑證有效截止日與舊憑證之到期日相同。

2. 變更主體名稱等重要身分資料不屬憑證變更，用戶須重新申請憑證，且舊憑證須廢止。

4.8.2 憑證變更之申請者

由政府機關(構)授權之人員，向本管理中心提出申請。

4.8.3 憑證變更之程序

1. 憑證變更之程序說明如下：

(1) 用戶至憑證管理中心網站提出憑證變更申請，使用該憑證之私密金鑰對申請檔加以簽章，並將申請檔傳送至註冊中心。

(2) 註冊中心進行審核程序，並驗證申請檔之數位簽章，以識別用戶之身分。

(3) 註冊中心完成審核作業後，將新憑證申請與舊憑證廢止申請等資料傳送至本管理中心。

(4) 本管理中心於接獲註冊中心提供之新憑證申請與舊憑證廢止申請資料後，簽發新憑證並廢止舊憑證。

2. 本管理中心應於變更之新憑證簽發後 5 天內廢止舊憑證。

4.8.4 對用戶憑證變更之簽發通知

依4.3.2節「本管理中心對憑證申請者之通知」規定辦理。

4.8.5 接受憑證變更之要件

用戶於收到變更之憑證後，應確認憑證記載內容，如發現憑證內容有誤時，應立即通知註冊中心進行處理，未通知者視為接受憑證變

更。

4.8.6 本管理中心之憑證變更發布

本管理中心將變更後之新憑證公布於儲存庫，或以電子郵件、郵遞方式將憑證傳遞用戶。

4.8.7 本管理中心對其他個體之憑證簽發通知

本管理中心將變更後之新憑證公布於儲存庫。

4.9 憑證暫時停用及廢止

1. 本管理中心提供憑證暫時停用及廢止服務。
2. TLS 憑證不得暫時停止使用與恢復使用。

4.9.1 憑證廢止之事由

1. 用戶提出廢止憑證申請之事由如下：

(1) 私密金鑰遭到破解。

(2) 私密金鑰遺失、遭竊、異動、未經授權之揭露、盜用或其他破壞。

(3) 憑證不再使用。

(4) 憑證記載內容有誤或不正確。

(5) 憑證未獲得用戶授權，且經詢問後用戶不願意回溯給予授權。

2. 本管理中心得就下述情形逕行廢止憑證：

(1) 本管理中心之私密金鑰或系統遭冒用、偽造或破解。

(2) 憑證記載之內容不實或發生重大改變。

(3) 用戶憑證遭誤用。

(4) 用戶簽章用之私密金鑰遭冒用、偽造或破解。

(5) 用戶憑證不再符合 6.1.5 節「金鑰長度」與 6.1.6 節「公鑰參數之產製與品質檢驗」之規定。

(6) 用戶之機關(構)或單位裁撤。

(7) 本管理中心未依憑證政策或本作業基準規定簽發用戶憑證。

(8) 用戶未依憑證政策、本作業基準、用戶約定條款或相關法令規定使用憑證。

(9) 註記於憑證的完全吻合網域名稱或 IP Address 喪失合法的使用權。

(10) 本管理中心不具簽發憑證的權力且不再提供儲存庫、憑證廢止清冊或線上憑證狀態協定查詢服務時。

(11) 依據憑證政策或本作業基準要求。

(12) 證實使用可揭露用戶私密金鑰並致使其遭破解或可透過用戶公開金鑰計算取得對應私密金鑰之方法。

(13) 確認金鑰產製方法有瑕疵

(14) 確認用戶私鑰傳送給未經授權之人或非用戶隸屬之機關單

位。

(15) 司法機關或檢調單位通知。

(16) 用戶之上級機關或主管機關通知。

(17) 用戶唯一識別名稱變更(包括其上級機關變更)，如配合組織改造之名稱變更，本管理中心得視實際情況延後逕行廢止該憑證，該憑證廢止之寬限期將另行通知。

4.9.2 憑證廢止之申請者

憑證廢止之申請者如下：

1. 用戶。
2. 用戶之上級機關。
3. 本管理中心(包含註冊中心)。

4.9.3 憑證廢止之程序

4.9.3.1 憑證廢止方式

本管理中心依 3.4 節「憑證廢止申請之識別及鑑別」規定完成用戶身分識別及鑑別後，始可進行憑證廢止。

1. 用戶申請憑證廢止

(1) 用戶至本管理中心網站填寫憑證廢止申請書，並以公文將憑證廢止申請書函送註冊窗口。

(2) 憑證註冊審驗人員依 3.4 節「憑證廢止申請之識別及鑑別」規定完成用戶身分識別及鑑別，並檢查憑證廢止申請書之正

確性。

(3) 憑證廢止申請資料審核通過後，本管理中心於 1 個工作天內完成憑證廢止作業。

2. 本管理中心逕行廢止

須經憑證註冊審驗人員確認後，始可廢止憑證。

4.9.3.2 公告與通知

1. 廢止之憑證最遲於憑證廢止清冊下次更新時間(nextUpdate)前加入憑證廢止清冊中，並將憑證狀態資訊公告於儲存庫，直至該廢止憑證到期為止。

2. 本管理中心得以電子郵件、電話或公文方式通知申請者憑證廢止申請之結果。

4.9.4 憑證廢止申請之寬限期

指憑證廢止事由經確認後必須提出憑證廢止申請的時間。

1. 本管理中心本身之憑證須廢止時，須於 1 小時內通報總管理中心。

2. 用戶憑證須廢止時，最遲應於 10 個工作天內提出憑證廢止申請，本管理中心得視情況延展其憑證廢止之寬限期。

4.9.5 本管理中心處理憑證廢止請求之處理期限

本管理中心原則於接受憑證廢止申請後 5 個工作天內完成憑證廢止作業，但符合下列情事者，則應於 1 個工作天內完成憑證廢止：

1. 用戶向本管理中心提出憑證廢止申請。

2. 用戶通知本管理中心，並告知其原憑證請求未經授權且亦不願意重新授予授權。

3. 本管理中心證實用戶私密金鑰遭冒用、偽造或破解。

4. 本管理中心證實憑證裡記載之完全吻合網域名稱之網域授權或控管的驗證方式不受信賴。

4.9.6 信賴憑證者檢查憑證廢止之要求

信賴憑證者使用本管理中心所簽發之憑證前，應先檢驗本管理中心公布之憑證廢止清冊或線上憑證狀態協定回應訊息，以確認該憑證之有效性及憑證串鏈之正確性。

4.9.7 憑證廢止清冊簽發頻率

1. 憑證廢止清冊每日至少簽發 1 次，其有效期限不超過 36 小時。

2. 本管理中心於完成憑證廢止作業後的 24 小時內須重新簽發憑證廢止清冊。

4.9.8 憑證廢止清冊發布之最大延遲時間

本管理中心最遲於憑證廢止清冊所記載之下次更新時間前發布下一次之憑證廢止清冊。

4.9.9 線上憑證廢止/狀態查驗之服務

1. 本管理中心提供憑證查詢與下載、憑證廢止清冊及線上憑證狀態協定查詢服務。

2. 本管理中心由線上憑證狀態協定回應伺服器(Online Certificate Status Protocol Responder, OCSP Responder)提供符合RFC 6960及RFC 5019標準規範的線上憑證狀態協定回應訊息。

3. 本管理中心簽發線上憑證狀態協定回應伺服器之憑證其安全強度條件如下：

(1) 金鑰長度至少為RSA 2048位元

(2) 使用SHA-256或相同安全等級之雜湊函數演算法

4. 線上憑證狀態協定回應伺服器之憑證須包含符合RFC 6960規範之擴充欄位「id-pkix-ocsp-nocheck」。

4.9.10 線上憑證廢止查驗之規定

1. 信賴憑證者須以憑證廢止清冊或線上憑證狀態協定查詢服務驗證憑證之有效性。

2. 本管理中心線上憑證狀態協定回應伺服器至少可支援符合RFC 6960及RFC 5019標準規範所述之HTTP GET方法。

3. 線上憑證狀態協定查詢服務至少每4天更新1次憑證狀態資訊,其線上憑證狀態協定回應訊息最大效期為10個工作天。

4.9.11 其他形式廢止公告

本管理中心不另提供其他形式之廢止公告。

4.9.12 金鑰被破解時之其他特殊規定

金鑰被破解時，依 4.9.1 節「廢止憑證之事由」、4.9.2 節「憑證廢止之申請者」及 4.9.3 節「憑證廢止之程序」規定辦理。

4.9.13 暫時停用憑證之事由

1. 用戶暫時停用

(1) 私密金鑰遺失或遭盜用時。

(2) 用戶自行認定憑證須暫時停用。

2. 本管理中心逕行停用憑證

(1) 確認用戶私密金鑰遺失或遭盜用時。

(2) 依用戶之上級機關或政府組織之主管機關之通知。

(3) 依據司法機關之通知。

4.9.14 暫時停用憑證之申請者

1. 憑證用戶(政府機關、單位授權之人員) 。
2. 憑證用戶之上級機關或主管機關。
3. 本管理中心。

4.9.15 暫時停用憑證之程序

依用戶使用之符記不同，暫時停用憑證之程序分別說明如下：

1. IC 卡類：

(1) 用戶至本管理中心網站線上填寫憑證卡號及用戶代碼線上辦理暫時停用憑證申請。

(2) 本管理中心檢驗 IC 卡之卡號及用戶代碼無誤後，須於 1 個工作天內完成暫時停用憑證。

2. 非 IC 卡憑證、專屬類憑證、TLS 憑證：

(1) 用戶至本管理中心網站，下載並填寫憑證停用申請書後，以公文函送憑證註冊窗口辦理暫時停用憑證。

(2) 憑證註冊審驗人員依 3.2.2 節「組織身分之鑑別程序」規定辦理身分鑑別並查驗公文真偽後，須於 1 個工作天內完成暫時停用憑證。

4.9.16 暫時停用憑證期間之限制

用戶申請暫時停用最長可停用至該憑證到期。

4.9.17 恢復使用憑證之程序

依用戶使用之符記不同，恢復使用憑證之程序分別說明如下：

1. IC 卡類：

(1) 用戶至本管理中心網站線上填寫憑證卡號及用戶代碼線上辦理恢復使用憑證申請。

(2) 本管理中心檢驗 IC 卡之卡號及用戶代碼無誤後，始可進行恢復使用憑證作業，將憑證狀態更改為有效 (Valid)。

2. 非 IC 卡憑證、專屬類憑證、TLS 憑證：

(1) 用戶至本管理中心網站，下載並填寫憑證停用申請書後，以公文函送憑證註冊窗口辦理恢復使用憑證。

(2) 憑證註冊審驗人員依 3.2.2 節「組織身分之鑑別程序」規定辦理身分鑑別並查驗公文真偽後，始可進行恢復使用憑證作業，將憑證狀態更改為有效 (Valid)。

4.10 憑證狀態服務

4.10.1 服務特性

憑證廢止清冊或線上憑證狀態協定回應訊息中之憑證廢止資訊，須至該被廢止之憑證已過期後始可移除。

4.10.2 服務可用性

1. 本管理中心提供全天候(7 x 24)不中斷之儲存庫服務，憑證狀態查詢服務之回覆時間須在 10 秒內。

2. 儲存庫服務無法正常運作時，須於 2 個工作天內恢復正常運作。

4.10.3 可選功能

不予規定。

4.11 終止服務

指憑證用戶不再使用本管理中心之服務；本管理中心同意用戶終止服務之要件如下：

1. 憑證到期。
2. 用戶廢止憑證。

4.12 私密金鑰託管及回復

4.12.1 金鑰託管及回復政策與實務

1. 本管理中心簽章用之私密金鑰不可被託管。
2. 本管理中心不提供用戶私密金鑰託管與回復。

4.12.2 通訊用金鑰封裝及回復政策與實務

本管理中心不提供通訊用金鑰封裝與回復。

5.基礎設施、安全管理及作業程序控管

5.1 實體控管

5.1.1 實體位置及結構

本管理中心機房位於台北市信義路 1 段 21 號數據通信大樓內之安全機房，具備門禁、保全、入侵偵測及監視錄影等實體安全機制。

5.1.2 實體存取

1. 本管理中心之實體控管符合保證等級第 3 級規定，包含：

(1) 大門及大樓警衛。

(2) 進出管制系統。

(3) 指紋辨識系統。

(4) 機箱監控系統。

2. 可攜式儲存媒體須檢查並確認無電腦病毒及惡意軟體。

3. 非授權人員進出機房時，須填寫進出紀錄，並由本管理中心人員全程陪同。

5.1.3 電力及空調

1. 機房之電力系統包括市電、發電機(滿載油料可連續運轉 6 天)及不斷電系統，可提供至少 6 小時以上備用電力。

2. 機房設有恆溫恆濕空調系統。

5.1.4 水災防範及保護

機房位於建築物第 3 樓層(含)以上，具備防水閘門及抽水機。

5.1.5 火災防範及保護

機房具備自動偵測火災預警功能，系統可自動啟動滅火設備，並於各機房主要出入口設置手動開關。

5.1.6 媒體儲存

稽核紀錄、歸檔及備援資料，除儲存 1 份於主機房外，另將複製 1 份送至異地備援場所儲存。

5.1.7 汰換設備處理

儲存重要資料之媒體不再使用時，須依政府機關資安規定或其他經國發會同意之方式辦理銷毀作業。

5.1.8 異地備援

本管理中心主機房採用雙主機之架構進行同地備援，避免單點失效之風險，此外為了防止憑證管理中心服務中斷，另執行異地備援機制。

1. 異地備援地點位於臺中，與主機房距離 30 公里以上。
2. 備援內容包括資料及系統程式，資料備份至少 1 個月執行 1 次。
3. 異地備援系統與主系統具相同之安全等級。

5.2 程序控管

各信賴角色依工作內容進行識別及鑑別，以確保作業程序之安全。

5.2.1 信賴角色

1. 信賴角色分為管理員、簽發員、稽核員、維運員及實體安全控管員，工作內容說明如下：

(1) 管理員：

- 安裝、設定及維護本管理中心系統。
- 建立及維護本管理中心系統之使用者帳號。
- 設定稽核參數。
- 產製及備份本管理中心之金鑰。

(2) 簽發員：

- 啟動或停止憑證簽發服務。
- 啟動或停止憑證廢止服務。

(3) 稽核員：

- 對稽核紀錄之查驗、維護及歸檔。
- 執行或監督內部稽核。

(4) 維運員：

- 系統及設備之運作維護。

- 系統備份作業。
- 儲存媒體之更新。
- 憑證管理系統外之軟硬體更新。
- 系統異常及網路安全事件之通報等。

(5) 實體安全控管員：

- 系統之實體安全控管。

2. 信賴角色依 5.3 節「人員控管」規定進行人員控管。
3. 各信賴角色可由多人擔任，並設有 1 名主管。

5.2.2 工作內容所需人數

各信賴角色所需之人數如下：

(1) 管理員：至少 3 位。

(2) 簽發員：至少 3 位。

(3) 稽核員：至少 2 位。

(4) 維運員：至少 2 位。

(5) 實體安全控管員：至少 2 位。

各工作內容所需之人數說明如下：

任務名稱	管理員	簽發員	稽核員	維運員	實體安全控管員
安裝、設定及維護本管理中心憑證管理系統	1				1
建立及維護本管理中心憑證管理系統之使用者帳號	1				1
設定稽核參數	1				1
產製及備份本管理中心之金鑰	2		1		1
啟動或停止憑證簽發服務		2			1
啟動或停止憑證廢止服務		2			1
對稽核紀錄之查驗、維護及歸檔			1		1
系統設備之日常運作維護				1	1
系統之備份作業				1	1
儲存媒體之更新				1	1
除本管理中心憑證管理系統外之軟硬體更新				1	1

5.2.3 角色識別及鑑別

1. 以使用者帳號、密碼及 IC 卡等，識別及鑑別管理員、簽發員、稽核員及維運員。

2. 以中央門禁系統，識別及鑑別實體安全控管員。

5.2.4 角色權責劃分

各角色分派須符合規定如下：

1. 管理員、簽發員及稽核員不得相互兼任。
2. 實體安全控管員不得兼任其他信賴角色。
3. 不允許執行自我稽核。

5.3 人員控管

5.3.1 身家背景、資格、經驗及安全需求

1. 人員甄選及進用前須進行安全評估。
2. 人員須定期進行考核管理。
3. 人員須定期進行教育訓練。
4. 人員應遵守並簽訂保密切結。

5.3.2 身家背景之查驗程序

1. 本管理中心工作人員，須由本管理中心及人事相關部門主管依各信賴角色之資格執行實務、經歷及身分背景審查。
2. 每年依各信賴角色之職務特性，執行實務與經歷之審查，確認是否適任。

5.3.3 教育訓練需求

各信賴角色之教育訓練需求如下：

信賴角色	教育訓練需求
管理員	1. 本管理中心之安全認證機制。 2. 本管理中心系統安裝、設定及維護之操作程序。 3. 建立及維護系統用戶帳號之操作程序。 4. 設定稽核參數之操作程序。 5. 產製及備份本管理中心金鑰之操作程序。 6. 災害復原及業務永續經營之程序。
簽發員	1. 本管理中心之安全認證機制。 2. 憑證簽發之操作程序。 3. 憑證廢止之操作程序。 4. 災害復原及業務永續經營之程序。
稽核員	1. 本管理中心之安全認證機制。 2. 本管理中心稽核系統之使用及操作程序。 3. 稽核紀錄查驗、維護及歸檔之程序。 4. 災害復原及業務永續經營之程序。
維運員	1. 系統備份之作業程序。 2. 系統設備日常運作之維護程序。 3. 儲存媒體之更新程序。 4. 災害復原及業務永續經營之程序。
實體安全控管員	1. 設定實體門禁權限程序。 2. 災害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

1. 各信賴角色每年進行 1 次教育訓練。

2. 軟硬體升級、工作程序改變、設備更換或相關法規改變時。

5.3.5 工作調換之頻率及順序

1. 管理員調離原職務滿 1 年後，方可轉任簽發員或稽核員。

2. 簽發員調離原職務滿 1 年後，方可轉任管理員或稽核員。

3. 稽核員調離原職務滿 1 年後，方可轉任管理員或簽發員。

4. 維運員滿 2 年，且已接受相關教育訓練及通過審核，方可轉任管理員、簽發員或稽核員。

5.3.6 未授權行動之懲處

人員如違反相關規定，應接受適當之管理及懲處，如情節重大致造成損害者，本管理中心得採取法律行動追究其責任。

5.3.7 聘僱人員之規定

聘僱人員須簽訂保密協定，並依規定進行作業。

5.3.8 提供之文件資料

本管理中心提供之文件包括憑證政策、技術規範、本作業基準、系統操作手冊及電子簽章法等相關文件。

5.4 稽核記錄程序

1. 安全相關事件均保存安全稽核紀錄(Audit Log)，且於執行稽核時可立即取得。
2. 安全稽核紀錄可為系統自動產生或人工紙本紀錄方式。

5.4.1 事件記錄之類型

1. 安全稽核
   - 重要稽核參數之改變。
   - 嘗試刪除或修改稽核紀錄。

2. 識別及鑑別

- 嘗試設定新角色。
- 管理者調整身分鑑別嘗試之最高容忍次數。
- 登入系統失敗。
- 帳號解鎖。
- 改變系統之身分鑑別機制。

3. 本管理中心產製金鑰時(不包括單次使用之金鑰產製)。
4. 本管理中心私密金鑰之存取
5. 公開金鑰之新增、刪除及儲存
6. 除單次使用之金鑰外，其餘私密金鑰之匯出。
7. 憑證註冊、廢止及狀態改變之申請過程。
8. 安全相關之組態設定改變。
9. 帳號之新增、刪除及存取權限修改
10. 憑證格式剖繪之改變
11. 憑證廢止清冊格式剖繪之改變
12. 本管理中心之伺服器設定改變
13. 實體存取及場所之安全
14. 異常事件

5.4.2 紀錄處理頻率

本管理中心每月檢視 1 次稽核紀錄，並追蹤調查重大事件。

5.4.3 稽核紀錄保留期限

稽核紀錄至少保留6個月，保留期限屆滿時，由稽核員移除資料，不可由其他人員代理。

5.4.4 稽核紀錄之保護

1. 使用簽章、加密技術保存之稽核紀錄，應使用無法更改或刪除紀錄之媒體儲存。
2. 簽署事件紀錄之私密金鑰不可使用於其他用途。
3. 稽核系統之私密金鑰應有安全保護措施。
4. 稽核紀錄須存放於安全場所。

5.4.5 稽核紀錄備份程序

1. 電子式稽核紀錄每月備份 1 次。
2. 稽核系統以每日、每星期及每月等周期將稽核紀錄自動歸檔。

5.4.6 稽核紀錄彙整系統

稽核紀錄彙整系統內建於本管理中心之系統，稽核程序於管理中心系統啟動時啟用。

自動稽核系統如無法正常運作，且系統資料處於高風險狀態時，本管理中心將暫停憑證簽發服務，直至問題解決後再行提供服務。

5.4.7 對引起事件者之告知

稽核系統不須告知引起事件之個體，其引發之事件已被系統紀錄。

5.4.8 弱點評估

本管理中心每年進行 1 次風險評鑑，對作業系統、實體設施、憑證管理系統及網路進行評估。

5.5 紀錄歸檔之方法

5.5.1 歸檔紀錄之類型

1. 本管理中心向總管理中心申請憑證之相關資料。
2. 憑證實務作業基準。
3. 重要契約。
4. 系統或設備組態設定。
5. 系統或組態設定之修改或更新之內容。
6. 憑證申請資料。
7. 廢止申請資料。
8. 憑證接受之確認紀錄。
9. 符記啟用紀錄。
10. 已簽發或公告之憑證。
11. 本管理中心金鑰更換之紀錄。

12. 已簽發或公告之憑證廢止清冊。

13. 稽核紀錄。

14. 用以驗證及佐證歸檔內容之其他說明資料或應用程式。

15. 稽核人員所要求之文件。

16. 依 3.2.2 節「組織身分之鑑別程序」規定所定之組織身分鑑別資料。

5.5.2 歸檔紀錄保留期限

1. 歸檔紀錄及處理歸檔紀錄之應用程式,其保留期限為 10 年。

2. 歸檔紀錄逾保留期限後，書面資料應以安全方式銷毀；電子形式之資料檔得另備份至其他儲存媒體並提供適當保護，或以安全方式銷毀。

5.5.3 歸檔紀錄之保護

1. 不允許新增、修改或刪除歸檔紀錄。

2. 歸檔紀錄移至另一個儲存媒體，其保護等級不得低於原保護等級。

3. 歸檔紀錄應存放於安全場所。

5.5.4 歸檔紀錄備份程序

1. 電子式紀錄定期備份至異地備援中心。

2. 紙本紀錄將由本管理中心授權之人員定期整理歸檔。

5.5.5 歸檔紀錄之時戳要求

1. 歸檔之電子式紀錄內容應包含日期及時間資訊，並經適當之數位簽章保護，用以檢測紀錄中之日期及時間資訊是否遭篡改。

2. 電子式紀錄中之日期及時間資訊，係為電腦作業系統之日期及時間，非第三方所提供之電子式時戳資料。

3. 本管理中心所有電腦系統均定期進行校時。

4. 歸檔之書面紀錄亦記載日期資訊，必要時得記載時間資訊。紀錄之日期及時間紀錄如有更改時須由稽核人員簽名確認。

5.5.6 歸檔紀錄彙整系統

本管理中心無歸檔紀錄彙整系統。

5.5.7 取得及驗證歸檔紀錄之程序

1. 歸檔紀錄須以書面申請並經同意後方可取得。

2. 稽核員負責驗證歸檔紀錄，書面文件須驗證文件簽署者及日期等之真偽；電子檔須驗證歸檔紀錄之數位簽章。

5.6 金鑰更換

1. 本管理中心私密金鑰於簽發憑證用途之使用期限到期前，應完成用以簽發憑證之金鑰對更換作業，並取得總管理中心核發之下屬憑證機構憑證。

2. 用戶之私密金鑰依 6.3.2 節「公開金鑰及私密金鑰之使用期限」規定定期更換，用戶更換金鑰並申請憑證時，應依 4.2 節「申請憑證之程序」規定辦理。

5.7 破解或災害時之復原程序

5.7.1 緊急事件及系統遭破解之處理程序

本管理中心訂定緊急事件及系統遭破解之通報與處理程序，每年依該程序進行演練。

5.7.2 電腦資源、軟體或資料遭破壞之復原程序

本管理中心訂定電腦資源、軟體或資料遭破壞之復原程序，且每年依該程序進行演練。

電腦設備遭破壞無法運作時，須優先回復儲存庫之運作，並迅速重建憑證簽發及管理之能力。

5.7.3 本管理中心簽章金鑰遭破解之復原程序

本管理中心訂有簽章金鑰遭破解之復原程序，且每年依該程序進行演練。

5.7.4 本管理中心安全設施之災害復原工作

1. 本管理中心每年對安全設施之災害復原工作進行演練。
2. 當發生災害時，將啟動災害復原程序，優先回復本管理中心儲存庫之運作，並迅速重建憑證簽發及管理的能力。

5.7.5 本管理中心簽章金鑰憑證被廢止之復原程序

本管理中心訂有簽章金鑰憑證被廢止之復原程序，且每年依該程序進行演練。

5.8 本管理中心之終止服務

1. 除無法通知者外，管理中心於預定終止服務 3 個月前，應通知所有未廢止及未過期憑證之用戶，並公告於儲存庫。
2. 廢止全部有效憑證，並進行檔案紀錄之保管及移交工作。

6.技術性安全控管

6.1 金鑰對產製及安裝

6.1.1 金鑰對產製

6.1.1.1 本管理中心金鑰對之產製

1. 本管理中心依 6.2.1 節「密碼模組標準及控管」規定於硬體密碼模組內產製金鑰對，其金鑰產製過程採用符合 NIST FIPS 140-2 規範之亂數產生機制與 RSA 金鑰演算法。

2. 私密金鑰之匯出與匯入依 6.2.2 節「金鑰分持多人控管」與 6.2.6 節「私密金鑰與密碼模組間傳輸」規定進行。

3. 金鑰產製須準備與遵循金鑰產製腳本，於本管理中心相關人員見證下進行，且金鑰產製過程須錄影留存。

6.1.1.2 政府機關(構)、單位憑證之金鑰對產製

1. 使用之符記為 IC 卡時，其金鑰對由本管理中心所信賴之發卡中心代為產製。發卡中心須採用通過 FIPS 140 等級 2 認證或安全強度相當之 IC 卡，並於 IC 卡內部產製金鑰對，且金鑰對產製完畢後，其私密金鑰將無法由 IC 卡中匯出。

2. 使用其他符記時，其金鑰對由用戶自行產製。

3. 產製金鑰對之公開金鑰須符合 6.1.5 節「金鑰長度」與 6.1.6 節「公鑰參數之產製與品質檢驗」之規定，且私密金鑰不可為弱金鑰。。

6.1.1.3 TLS 憑證及專屬類憑證之金鑰對產製

用戶申請 TLS 憑證或專屬類憑證時，須自行產製金鑰對，且該金鑰對之公鑰須符合 6.1.5 節「金鑰長度」與 6.1.6 節「公鑰參數之產製與品質檢驗」之規定。

6.1.2 私密金鑰安全傳送予用戶

使用之符記為 IC 卡時，依 6.1.1.1 節「政府機關(構)、單位憑證之金鑰對產製」規定，其私密金鑰由本管理中心所信賴之發卡中心代為產製，發卡中心於本管理中心簽發憑證後，將存有私密金鑰之 IC 卡掛號郵寄予用戶。

用戶於收到 IC 卡後，若確認接受，則應連線至本管理中心網站進行開卡作業。

6.1.3 公開金鑰安全傳送予本管理中心

1. 本管理中心代為產製用戶金鑰

   由註冊中心透過安全管道將用戶之公開金鑰傳送予本管理中心。該安全管道係指以使用傳輸層安全性協定、專屬通訊協定或資料簽章與加密等傳送方式。例如以憑證管理協定(Certificate Management Protocol)簽章封包、憑證註冊審驗人員簽章等傳送方式，將用戶之公開金鑰傳送予本管理中心。

2. 用戶自行產製金鑰對

   用戶以 PKCS# 10 憑證申請檔之格式將公開金鑰傳送至註冊中心，註冊中心依照 3.2.1 節「證明擁有私密金鑰之方式」規定，檢驗用戶確實擁有相對應之私密金鑰後，再以傳輸層

安全協定或安全強度相同之資料加密傳送方式將用戶之公開金鑰傳送至管理中心。

6.1.4 本管理中心公開金鑰安全傳送予信賴憑證者

本管理中心之公鑰憑證由總管理中心簽發，並公布於總管理中心及本管理中心之儲存庫，供用戶及信賴憑證者直接下載與使用。

6.1.5 金鑰長度

1. 本管理中心使用金鑰長度至少為 2048 位元之 RSA 金鑰，並以 SHA-256、SHA-384 或 SHA-512 雜湊函數演算法簽發憑證。

2. 用戶使用之金鑰可為以下 2 種：

(1) 長度至少須為 2048 位元之 RSA 金鑰，並以 SHA-256、SHA-384 或 SHA-512 雜湊函數演算法簽發憑證。

(2) 使用符合 NIST P-280、P-384 或 P-521 金鑰長度之橢圓曲線密碼演算法(Elliptic Curve Cryptography, ECC)簽發憑證。

6.1.6 公鑰參數之產製與品質檢驗

1. RSA 演算法之公鑰參數為空值。

2. 本管理中心簽章用金鑰對採用 ANSI X9.31 演算法或 NIST FIPS 186-4 規範產生 RSA 演算法所需之質數，並確保該質數為強質數。

3. 用戶於軟硬體密碼模組以 RSA 演算法產製金鑰程序中的質數，需確保該質數為強質數。

4. 本管理中心依據 NIST SP 800-89 第 5.3.3 節之規定，確認該金鑰之公開指數值為大於 3 的奇數，且其值介於 $2^{16}+1$ 與 $2^{256}-1$ 之間。此外，模數應具有奇數、非質數的指數次方且沒有小於 752 的因數等性質。

5. 若使用橢圓曲線密碼演算法簽發憑證，本管理中心將遵照 NIST SP 800-56A Revision 3 之規定，確認所有使用 ECC Full Public Key Validation Routine 與 ECC Partial Public Key Validation Routine 的金鑰之效期。

6.1.7 金鑰使用目的

1. 本管理中心簽章用私密金鑰僅用於簽發憑證及憑證廢止清冊。

2. 用戶使用之符記為 IC 卡者，其金鑰用途為簽章用與加解密用；簽章用憑證金鑰用途擴充欄位設定為 digitalSignature，加解密用憑證金鑰用途擴充欄位設定 keyEncipherment 與 dataEncipherment。

3. 用戶使用之符記為非 IC 卡者，其金鑰用途可為簽章用或加解密用，亦可同時包含簽章及加解密之用途；簽章用憑證金鑰用途擴充欄位設定為 digitalSignature，加解密用憑證金鑰用途擴充欄位設定 keyEncipherment 與 dataEncipherment。

4. 專屬類憑證之金鑰用途可為簽章用或加解密用，亦可同時包含簽章及加解密之用途；簽章用憑證金鑰用途擴充欄位設定為 digitalSignature，加解密用憑證金鑰用途擴充欄位設定 keyEncipherment 與 dataEncipherment。

5. TLS 憑證之金鑰用途擴充欄位設定為 digitalSignature 與 keyEncipherment，其延伸金鑰用途擴充欄位包含 serverAuth 與 clientAuth。

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

1. 本管理中心使用通過 FIPS 140-2 安全等級第 3 級認證之硬體密碼模組產製亂數與金鑰對。

2. 用戶金鑰對之儲存媒體可為通過 FIPS 140 等級 2 認證或安全強度相當之 IC 卡或其他載具。

6.2.2 金鑰分持多人控管

1. 本管理中心之金鑰分持多人控管採 m-out-of-n 方法。

(1) m-out-of-n 方法係一種完全秘密分享的方式，其 m 與 n 皆須為大於或等於 2 的數值，且 m 必須小於或等於 n。

(2) 本管理中心使用此方法做為做為金鑰分持備份、啟動及回復之方式

2. 本管理中心於金鑰產製後，採用上述之多人控管方式進行金鑰分持，分別存放於不同之安全地點。

6.2.3 私密金鑰託管

1. 本管理中心簽章用之私密金鑰不可被託管。

2. 本管理中心不提供用戶私密金鑰託管。

6.2.4 私密金鑰備份

本管理中心採用金鑰分持之多人控管方法備份私密金鑰，並使用通過高安全性之 IC 卡做為秘密分持之儲存媒體。

6.2.5 私密金鑰歸檔

1. 本管理中心簽章用私密金鑰不可被歸檔。
2. 用戶簽章用私密金鑰，本管理中心不進行歸檔。

6.2.6 私密金鑰及密碼模組間傳輸

本管理中心於下列情況進行私密金鑰輸入密碼模組作業：

1. 金鑰產製。
2. 金鑰持份備援之回復。
3. 更換密碼模組。

6.2.7 私密金鑰儲存於密碼模組

1. 私密金鑰依規定儲存於密碼模組內。
2. 密碼模組如不需使用時，須離線並儲存於安全場所。

6.2.8 私密金鑰之啟動方式

本管理中心私密金鑰之啟動是由多人控管 IC 卡控制，IC 卡組分別由管理員與簽發員保管。

6.2.9 私密金鑰之停用方式

本管理中心私密金鑰之停用以多人控管方式進行。

6.2.10 私密金鑰之銷毀方式

1. 本管理中心私密金鑰之銷毀方式說明如下：

(1) 舊私密金鑰不再使用時，本管理中心將硬體密碼模組中存放舊私密金鑰之記憶位址進行零值化(Zeroization)處理，以銷毀硬體密碼模組中舊私密金鑰，同時將對應之金鑰備援秘密持份 IC 卡進行實體銷毀。

(2) 硬體密碼模組汰除時，硬體密碼模組中所有的私密金鑰皆應被銷毀，並於銷毀後使用該硬體密碼模組之金鑰管理工具確認所有私密金鑰已銷毀。

2. 用戶之私密金鑰銷毀方式，不另做規定。

6.2.11 密碼模組評等

密碼模組評等方式依憑證政策 6.2.1 節「密碼模組標準及控管」規定辦理。

6.3 金鑰對管理之其他規定

本管理中心不負責保管用戶之私密金鑰。

6.3.1 公開金鑰之歸檔

本管理中心依 5.5 節「紀錄歸檔之方法」規定進行用戶憑證之歸檔，不另對公開金鑰進行歸檔。

6.3.2 公開金鑰及私密金鑰之使用期限

6.3.2.1 本管理中心公開金鑰及私密金鑰之使用期限

1. 本管理中心公開金鑰與私密金鑰使用期限至多為 20 年
2. 以私密金鑰執行簽發用戶憑證用途之使用期限至多為 10 年
3. 私密金鑰執行簽發用戶憑證用途之使用期限到期後，仍須簽發憑證廢止清冊或線上憑證狀態協定回應伺服器憑證，持續至該私密金鑰簽發之所有用戶憑證到期為止。

6.3.2.2 用戶公開金鑰及私密金鑰之使用期限

用戶之公開金鑰憑證之使用期限至多為 9 年，私密金鑰之使用期限至多為 9 年。

6.4 啟動資料之保護

6.4.1 啟動資料之產生

本管理中心私密金鑰之啟動資料由硬體密碼模組亂數產生並寫入硬體密碼模組後，再寫入至多人分持控管 IC 卡中。

6.4.2 啟動資料之保護

1. 本管理中心之啟動資料由多人分持控管 IC 卡保護，須透過硬體密碼模組內建之讀卡機存取，並於硬體密碼模組內建之鍵盤上輸入 IC 卡個人識別碼(以下簡稱為 PIN 碼)。
2. 上述 IC 卡之 PIN 碼不得記錄於任何媒體上。
3. 登入之失敗次數如超過 3 次時，該 IC 卡即被鎖住。

4. IC 卡移交時，保管人員須重新設定 PIN 碼。

6.4.3 啟動資料之其他規範

不予規定。

6.5 電腦軟硬體安控措施

6.5.1 特定電腦安全技術需求

本管理中心提供安全控管功能說明如下：

1. 具備身分鑑別之登入。
2. 提供自行定義存取控制。
3. 提供安全稽核能力 。
4. 對各種憑證服務與信賴角色存取控制之限制。
5. 具備信賴角色與相關身分之識別及鑑別。
6. 以密碼技術確保每次通訊與資料庫之安全。
7. 具備信賴角色與相關身分識別之安全與可信賴管道。
8. 具備程序完整性與安全控管保護。

6.5.2 電腦安全評等

本管理中心採用安全強度與 C2(TCSEC)、E2(ITSEC)或 EAL3(CC,ISO/IEC 15408)等級相當之電腦作業系統，且系統及運作環境符合 WebTrust for CA 之安全控管原則。

6.6 生命週期技術控管措施

6.6.1 系統研發控管措施

1. 依憑證管理中心主管機關(國發會)認可之軟體工程發展方法與品質管理規範進行開發與品質控管

2. 系統開發環境、測試環境及正式環境應獨立運作，以防止未經授權存取或變更之風險。

3. 使用專用且獲得授權之軟硬體。

4. 各項交付本管理中心之產品或程式應提供交付清單、測試報告、原始程式碼掃描報告，並進行程式版本控管，軟體之原始程式碼須定期掃描。

6.6.2 安全管理控管措施

1. 不得安裝與運作無關之軟硬體或元件。

2. 軟體安裝時應確認版本完整性及正確性，並每日自動檢查軟體之完整性。

3. 系統組態之變動均須紀錄與控管。

4. 須具備修改系統軟體或組態之偵測機制。

6.6.3 生命週期安全控管措施

本管理中心每年至少進行 1 次現行金鑰是否有被破解之風險評估。

6.7 網路安全控管措施

1. 本管理中心之主機與儲存庫透過資安防護設備進行隔離。
2. 儲存庫置於資安防護設備對外服務區，連接至網際網路。
3. 本管理中心之儲存庫係透過系統修補程式之更新及資安系統加以保護，以防範阻絕服務與入侵等攻擊。
4. 本管理中心應配合資通安全管理法規定辦理相關資安防護作業。

6.8 時戳

為確保下述時間之正確性，本管理中心定期依據受信賴之時間源進行系統校時，且系統校時作業須可被稽核。

1. 用戶憑證簽發時間。
2. 用戶憑證廢止時間。
3. 憑證廢止清冊之簽發時間。
4. 系統事件之發生時間。

6.9 密碼模組安全控管措施

密碼模組安全控管措施，依 6.1 節「金鑰對產製及安裝」與 6.2 節「私密金鑰保護及密碼模組安全控管措施」規定辦理。

7.憑證、憑證廢止清冊及線上憑證狀態協定格式剖繪

7.1 憑證之格式剖繪

本管理中心簽發之憑證遵照 ITU-T X.509 與 IETF PKIX Working Group 的 RFC 5280 或其最新版相關之規定，其格式剖繪依本基礎建設技術規範相關規定。

本管理中心透過密碼安全偽亂數產生器(Cryptographically Secure Pseudorandom Number Generator, CSPRNG)產生其所簽發之憑證的憑證序號，此憑證序號為長度至少 64 位元且非循序之正整數。

7.1.1 版本序號

本管理中心簽發遵照 RFC5280 與 ITU-T 規範之 X.509 v3 版本之憑證。

7.1.2 憑證擴充欄位

1. 憑證擴充欄位遵照 ITU-T X.509、IETF PKIX Working Group RFC 5280 及本基礎建設技術規範相關規定。

2. 憑證所使用之必要擴充欄位與該擴充欄位的關鍵性與內容於「政府機關公開金鑰基礎建設憑證及憑證廢止清冊格式剖繪」中敘明。

3. 其他選擇性擴充欄位依情況不同使用時，其使用方式遵照前述標準之規定。

4. 本管理中心不允許簽發下述兩種情境之憑證：

(1) 憑證的擴充欄位內含無法應用於公眾網路的設定。

(2) 憑證的內容包含可能誤導信賴憑證者相信該憑證資訊已經由本管理中心驗證之語意。

7.1.3 演算法物件識別碼

1. 本管理中心使用之演算法之物件識別碼(Object Identifier)如下：

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

(OID：1.2.840.113549.1.1.11)

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

(OID：1.2.840.113549.1.1.12)

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

(OID：1.2.840.113549.1.1.13)

2. 本管理中心所簽發憑證之主體公鑰，其演算法之物件識別碼說明如下：

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

(OID：1.2.840.113549.1.1.1)

7.1.4 命名形式

憑證之主體與簽發者兩個欄位使用 X.500 之唯一識別名稱，其欄位屬性型態係遵照 ITU-T X.509、IETF PKIX Working Group RFC5280 等相關規定。

7.1.4.1 簽發者資訊

依據RFC 5280名稱串鏈之規定，本管理中心所簽發之用戶憑證，其簽發者唯一識別名稱欄位(Issuer Distinguished Name)內容須與本管理中心本身憑證之主體唯一識別名稱欄位(Subject Distinguished Name)內容相同。

7.1.4.2 用戶憑證之主體資訊

本管理中心所簽發用戶憑證主體唯一識別名稱欄位、主體別名擴充欄位與其他必要擴充欄位的關鍵性與格式，於「政府機關公開金鑰基礎建設憑證及憑證廢止清冊格式剖繪」中敘明。

7.1.4.3 本管理中心之主體資訊

本管理中心之憑證機構憑證主體唯一識別名稱欄位中各屬性的格式與必要性，於「政府機關公開金鑰基礎建設憑證及憑證廢止清冊格式剖繪」中敘明，憑證主體名稱欄位說明參考 3.1.5 節「命名獨特性」。

7.1.5 命名限制

本管理中心簽發之憑證不採用命名限制(nameConstraints)。

7.1.6 憑證政策物件識別碼

本管理中心所簽發憑證之憑證政策擴充欄位使用本基礎建設之憑證政策物件識別碼。

7.1.7 政策限制擴充欄位之使用

本管理中心簽發之憑證不含政策限制擴充欄位(policyConstraints)。

7.1.8 政策限定元之語法及語意

本管理中心簽發之憑證不含政策限定元(policyQualifiers)。

7.1.9 關鍵憑證政策擴充欄位之語意處理

本管理中心簽發之憑證，其所含之憑證政策擴充欄位，須依「政府機關公開金鑰基礎建設憑證及憑證廢止清冊格式剖繪」之規定，進行關鍵性之註記。

7.2 憑證廢止清冊格式剖繪

7.2.1 版本序號

本管理中心簽發 ITU-T X.509 v2 版本之憑證廢止清冊。

7.2.2 憑證廢止清冊與憑證廢止清冊條目擴充欄位

本管理中心簽發的憑證廢止清冊、憑證廢止清冊擴充欄位(crlExtensions)及憑證廢止清冊條目擴充欄位(crlEntryExtensions)會遵照 ITU-T X.509 與 IETF PKIX Working Group 的 RFC 5280 或其最新版相關之規定。

憑證廢止清冊之擴充欄位內容均詳述於「政府機關公開金鑰基礎建設憑證及憑證廢止清冊格式剖繪」。

7.3 線上憑證狀態協定格式剖繪

1. 本管理中心提供符合 RFC 6960 與 RFC 5019 標準規範之線上憑證狀態協定查詢服務，並於憑證之憑證機構存取資訊擴充欄位中註明本管理中心線上憑證狀態協定之服務網址。

2. 本管理中心線上憑證狀態協定查詢服務之線上憑證狀態協定查詢封包，應包括資訊如下：

- 版本序號
- 待查詢憑證識別碼，包括：雜湊演算法、憑證簽發者名稱、憑證簽發者公開金鑰及待查詢憑證之憑證序號等。

3. 本管理中心線上憑證狀態協定回應訊息基本欄位說明如下：

欄位	說明
版本序號(Version)	v.1　(0x0)
線上憑證狀態協定回應伺服器 ID(Responder ID)	線上憑證狀態協定回應伺服器之主體名稱
產製時間(Produced Time)	回應訊息簽署時間
待查詢憑證識別元(Identifier)	包括雜湊演算法、憑證簽發者名稱、憑證簽發者公開金鑰及待查詢憑證之憑證序號等
憑證狀態碼(Certificate Status)	憑證狀態對應碼(0:有效/1:廢止/2:未知)
效期(ThisUpdate/NextUpdate)	此回應訊息建議之效期區間,包括生效時間(ThisUpdate) 與下次更新時間
簽章演算法(Signature Algorithm)	回應訊息之簽章演算法，可為 sha256WithRSAEncryption
簽章(Signature)	線上憑證狀態協定回應伺服器之簽章
憑證(Certificates)	線上憑證狀態協定回應伺服器之憑證

7.3.1 版本序號

版本序號以 RFC 5019 及 RFC 6960 規定為依據。

7.3.2 線上憑證狀態協定擴充欄位

1. 線上憑證狀態協定擴充欄位會依照 ITU-T X.509、RFC 5019 及 RFC 6960 之規定。

2. 線上憑證狀態協定回應訊息應包括線上憑證狀態協定伺服器之憑證機構金鑰識別碼(Authority Key Identifier)。

3. 憑證狀態協定查詢封包有隨機數欄位時，線上憑證狀態協定回應訊息亦須包括相同之隨機數欄位。

7.3.3 線上憑證狀態協定服務運轉規範

本管理中心線上憑證狀態協定服務運轉作業說明如下：

1. 可以處理與接受 HTTP GET/POST 方法所傳送線上憑證狀態協定用戶端之線上憑證狀態協定查詢封包。

2. 線上憑證狀態協定回應伺服器使用短效期憑證，由本管理中心定期簽發與更新。

8.稽核方法

8.1 稽核頻率或評估事項

1. 本管理中心每年執行 2 次內部稽核。
2. 本管理中心每年接受 1 次外部稽核，且查核區間不可超過 12 個月。
3. 稽核採用之標準為 WebTrust Principles and Criteria for Certification Authorities。

8.2 稽核人員之身分及資格

1. 稽核方須經 WebTrust 認證標章管理單位授權可於我國執行 WebTrust Principles and Criteria for Certification Authorities 稽核標準之合格稽核業者。
2. 稽核人員應通過國際電腦稽核師(Certified Information Systems Auditor, CISA)認證或具同等資格。
3. 本管理中心於稽核時應對稽核人員進行身分識別。

8.3 稽核人員及被稽核方之關係

稽核人員應獨立於被稽核之憑證管理中心，為獨立且公正之第三方人員。

8.4 稽核之範圍

1. 本作業基準是否符合憑證政策及總管理中心憑證實務作業基準之規定。

2. 本管理中心及註冊中心是否遵照本作業基準運作。

8.5 對於稽核結果之因應方式

1. 本管理中心對不符合規定之項目進行改善，並於完成後通知原稽核人員進行複核。

2. 依不符合情形之種類、嚴重性及修正所需時間，本管理中心得採取必要措施。

8.6 稽核結果公開之範圍

除可能導致系統安全風險及依 9.3 節「業務資訊保密」規定外，本管理中心應於儲存庫公布最近 1 次外部稽核結果。

9.其他業務與法律事項

9.1 費用

暫不收費。

9.1.1 憑證簽發、展期費用

暫不收費。

9.1.2 憑證查詢費用

暫不收費。

9.1.3 憑證廢止、狀態查詢費用

暫不收費。

9.1.4 其他服務費用

暫不收費。

9.1.5 請求退費程序

不適用。

9.2 財務責任

本管理中心之營運由政府編列預算維持，未向保險公司投保，財務責任依政府法令規定辦理。

9.2.1 保險範圍

不適用。

9.2.2 其他資產

不予規定。

9.2.3 對終端個體之保險或保固責任

不適用。

9.3 業務資訊保密

9.3.1 重要資訊之範圍

1. 本管理中心營運之私密金鑰與通行碼。
2. 本管理中心金鑰分持之相關資料。
3. 未經同意公開之用戶資料。
4. 本管理中心產生或保管之可供稽核與追蹤之紀錄。
5. 稽核人員於稽核過程中產生之稽核紀錄與發現，不得被完整公開者。
6. 本管理中心列為不得公開之營運相關文件。
7. 其他經法令規定不得公開之資料。

9.3.2 一般資訊之範圍

非 9.3.1 節「重要資訊之範圍」規定之資訊，原則皆屬一般資訊。

9.3.3 保護重要資訊之責任

本管理中心依電子簽章法、Trust Service Principles and Criteria for Certification Authorities 標準及個人資料保護法等規定，處理本管理中

心之重要資料。

9.4 個人資訊之隱私性

9.4.1 隱私保護計畫

1. 本管理中心於網站公告隱私權保護政策。
2. 本管理中心實施隱私衝擊分析與個資風險評鑑等措施。

9.4.2 隱私資料之種類

1. 憑證申請時記載之個人資訊。
2. 本管理中心運作所取得之個人資訊。

9.4.3 非隱私資料之種類

非 9.4.2 節「隱私資料之種類」規定之資訊，原則皆屬非隱私資料。

9.4.4 保護隱私資料之責任

依網站公告之隱私權保護政策、WebTrust Principles and Criteria for Certification Authorities 標準及個人資料保護法等相關規定進行隱私資料保護。

9.4.5 使用隱私資訊之公告與同意

1. 隱私權保護政策公告於網站。
2. 使用個人隱私資訊須經用戶同意。

9.4.6 應司法或管理程序釋出資訊

司法機關或檢調單位如應依法調查或蒐集證據需要，須查詢重要資訊時，本管理中心依法辦理，不另通知用戶。

9.4.7 其他資訊釋出之情形

依相關規定法令辦理。

9.5 智慧財產權

除個人資料外，本管理中心產製之文件(含電子檔案)，其智慧財產權皆屬本管理中心所有，重製、散布或公開傳輸須依網站公布之著作權聲明規定辦理。

9.6 職責與義務

9.6.1 本管理中心之職責與義務

1. 依憑證政策保證等級第 3 級規定與本作業基準運作。
2. 執行憑證申請之識別及鑑別程序。
3. 簽發、公布、廢止憑證。
4. 簽發與公布憑證廢止清冊。
5. 提供線上憑證狀態協定查詢服務。
6. 產製及管理本管理中心之私密金鑰。
7. 公布憑證實務作業基準。

9.6.2 註冊中心之職責與義務

1. 提供憑證申請服務。

2. 執行憑證申請之識別及鑑別程序。

3. 管理註冊中心之私密金鑰，且不得用於憑證註冊以外作業。

9.6.3 用戶之義務

1. 提供正確完整之資訊。

2. 遵守本作業基準相關規定。

3. 妥善管理與使用私密金鑰。

4. 私密金鑰遭冒用、破解或遺失時，應立即通知本管理中心廢止憑證，惟用戶仍應承擔異動前所有使用該憑證之法律責任。

5. 安全產製其私密金鑰並避免遭受破解。

6. 用戶應慎選安全之電腦環境與可信賴之應用系統，如因電腦環境或應用系統本身因素，導致信賴憑證者權益受損時，用戶應自行承擔責任。

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

8. 本管理中心所簽發之專屬類憑證，係以標的物為憑證主體，並以該標的物之所有人或經授權之使用人為用戶。如標的物

之財產所有權或使用權發生移轉時，用戶應廢止原憑證並重新申請憑證。

9.6.4 信賴憑證者之義務

1. 遵守本作業基準相關規定。
2. 正確檢驗憑證數位簽章、有效性及金鑰用途。
3. 信賴憑證者應確保憑證使用環境之安全，如非可歸責於本管理中心之事由導致權益受損時，應自行承擔責任。
4. 本管理中心如因故無法正常運作時，信賴憑證者應儘速尋求其他途徑完成與他人應為之法律行為，不得以本管理中心無法正常運作，作為抗辯他人之事由。

9.6.5 其他參與者之義務

9.6.5.1 發卡中心之義務

1. 依本作業基準 6.1.1.1 節「政府機關(構)、單位憑證之金鑰對產製」規定產製用戶之金鑰對。
2. 執行憑證寫入及製卡作業，並以亂數設定 IC 卡之初始 PIN 碼。
3. 寄送用戶之 IC 卡。

9.6.5.2 委外方式提供認證服務機構之義務

本管理中心由國發會依政府採購法規定辦理委外服務，承商依契約規定辦理。

9.7 免責聲明

用戶或信賴憑證者如未依本作業基準相關規定申請、管理及使用憑證，產生因不可抗力或其他非可歸責於本管理中心之事由，而造成之損害，由用戶或信賴憑證者自行負責，本管理中心不負任何法律責任。

9.8 責任限制

1. 本管理中心如因系統維護、轉換及擴充等事由，須暫停部分憑證服務時，得於 3 日前公告於儲存庫。用戶或信賴憑證者不得以此作為要求本管理中心損害賠償之理由。

2. 用戶如有廢止憑證事由時，應依 4.9 節「憑證暫時停用及廢止」規定提出憑證廢止申請。廢止憑證申請核定後，本管理中心將於 1 個工作天內完成憑證廢止作業、簽發憑證廢止清冊與公告於儲存庫。

3. 用戶於憑證廢止狀態未被公布前，應採取適當之行動，以減少對信賴憑證者之影響，並承擔所有因使用該憑證所引發之責任。

9.9 賠償

9.9.1 本管理中心之賠償責任

本管理中心如未依本作業基準及相關法令規定導致利害關係人權益損害時，由本管理中心負賠償責任；用戶及信賴憑證者得依相關法律規定請求損害賠償。

9.9.2 註冊中心之賠償責任

註冊中心如未依本作業基準及相關法令規定導致利害關係人權益損害時，由註冊中心負賠償責任；用戶及信賴憑證者得依相關法律規定請求損害賠償。

9.10 有效期限與終止

9.10.1 有效期限

本作業基準由總管理中心核定並公告後生效，直至被新版本取代前仍然有效。

9.10.2 終止

本作業基準之終止須由行政機關電子憑證推行小組委員決議，並經電子簽章法主管機關核定。

9.10.3 終止與存續之效力

1. 本作業基準效力終止之說明，應公告於本管理中心儲存庫。
2. 本作業基準終止後，其效力須維持至所簽發之最後一張憑證失效為止。

9.11 對參與者之個別通知及溝通

本管理中心、註冊中心、用戶及信賴憑證者間得採網站公告、儲存庫、公文、書信、電話、傳真、電子郵件等方式建立通知與聯絡管道。

9.12 修訂

本管理中心每年定期檢視及評估本作業基準，本作業準修訂方式如下：

1. 直接修訂本作業基準之內容。
2. 以附加文件方式增修。

9.12.1 修訂程序

本作業基準之修訂經行政機關電子憑證推行小組委員審查，並經電子簽章法主管機關經濟部核定後頒布。

9.12.2 通知機制與期限

本作業基準之修訂，經電子簽章法主管機關核定後須於 10 個工作天內公告，所有變更項目將公告於儲存庫。

9.12.3 須修改憑證政策物件識別碼之事由

憑證政策修訂或其物件識別碼如有變更時，本作業基準須配合修訂。

9.13 紛爭之處理程序

用戶與本管理中心如有爭議時，雙方應本誠信原則先進行協商，由本管理中心就本作業基準相關條文提出解釋。

9.14 管轄法律

依我國相關法令規定辦理。

9.15 適用法律

依我國相關法令規定辦理。

9.16 雜項條款

9.16.1 完整協議

本作業基準所約定者，構成主要成員間最終且完整之約定，主要成員包括本管理中心、註冊中心、用戶及信賴憑證者等。主要成員間就同一事項縱使以口頭或書面進行其他表示，最終仍應以本作業基準之約定為準。

9.16.2 轉讓

本作業基準所敘述之主要成員間權利或責任，不可於未通知本管理中心下以任何形式轉讓予其他方。

9.16.3 可分割性

本作業基準之任一章節不適用而須修正時，其他章節仍屬有效。

9.16.4 契約履行

用戶或憑證信賴者違反本作業基準相關規定，致本管理中心遭受損害，如可歸責於用戶或憑證信賴者之故意或過失時，本管理中心除得請求損害賠償外，亦得向可歸責之一方請求支付處理該爭議或訴訟之律師費用。

9.16.5 不可抗力

因不可抗力或其他非可歸責於本管理中心所導致之損害事件，本

管理中心不負任何法律責任。

9.17 其他條款

不予規定。

附錄 1：名詞解釋

◆ A

- **啟動資料(Activation Data)**：存取密碼模組時(例如用以開啟私密金鑰以進行簽章或解密)，除金鑰外所需之隱密資料。

- **申請者(Applicant)**：向憑證機構申請憑證，而尚未完成憑證作業程序之用戶。

- **歸檔(Archive)**：實體上(與主要資料存放處)分隔之長期資料儲存處，可用以支援稽核服務、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。

- **保證等級(Assurance Level)**：具相對性保證層級中之某一級數。

- **稽核(Audit)**：評估系統控制是否恰當，以確保符合既定之政策與營運程序，並對現有之控制、政策與程序等，建議必要之改善所進行之獨立檢閱與調查。

- **稽核紀錄(Audit Log)**：依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之順序與某個事件中之變化。

- **鑑別(Authenticate)**：驗證某個聲稱的身分是合法且屬於提出此聲稱者的程序。

- **鑑別程序(Authentication)**

  - 建立使用者或資訊系統身分信賴程度的程序。
  - 用以建立資料傳送、訊息、來源者之安全措施，或是驗證個人接收特定種類資訊權限之方法。

◆ **C**

- **憑證(Certificate)**
  - 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。
  - 資訊之數位呈現內容包括：
    - ✓ 簽發之憑證機構。
    - ✓ 用戶之名稱或身分。
    - ✓ 用戶之公開金鑰。
    - ✓ 憑證之有效期間。
    - ✓ 憑證機構數位簽章。

- **憑證政策(Certificate Policy, CP)**：係為透過憑證管理執行之電子交易所訂定具專門格式之管理政策。憑證政策中包括與數位憑證相關之生成、產製、傳送、稽核、被破解後復原及其管理等各項議題。憑證政策與其相關技術可提供特定應用所需之安全服務。

- **憑證廢止清冊(Certificate Revocation List, CRL)**
  - 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。
  - 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於到期日前被廢止之憑證。

- **憑證機構(Certification Authority, CA)**
  - 簽發憑證之機關。

- 為使用者所信任之權威機構，其業務為簽發並管理 X.509 格式之公開金鑰憑證、憑證機構廢止清冊及憑證廢止清冊。

- **授權憑證機構簽發憑證(Certification Authority Authorization , CAA)**：根據 RFC 6844 規定，授權憑證機構簽發憑證網域名稱系統資源紀錄(The Certification Authority Authorization 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。發布授權憑證機構簽發憑證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風險。

- **憑證變更(Certificate Modification)**：係指對同一憑證主體提供一張新憑證取代原憑證，惟新憑證有效截止日須與舊憑證到期日相同，憑證變更後，舊憑證應予以廢止。

- **憑證實務作業基準(Certification Practice Statement, CPS)**
  - 由憑證機構對外公告，用以陳述憑證機構據以簽發憑證與處理其他認證業務之作業準則。
  - 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)符合特定需求之聲明(需求敘明於憑證政策或其他服務契約中)。

- **破解(Compromise)**：資訊洩漏予未經授權人士或違反資訊安全政策，造成物件未經授權蓄意、非蓄意洩漏、修改、毀壞或遺失。

- **交互憑證(Cross-Certificate)**：在兩個根憑證機構之間建立信賴關係的一種憑證，屬於一種憑證機構憑證，而非用戶憑證。

- **密碼模組(Cryptographic Module)**：一組硬體、軟體、韌體或前述之組合，用以執行密碼之邏輯或程序(包含密碼演算法)，且被包含於此模組之密碼邊界內。

◆ **D**

- **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。

- **憑證效期(Duration)**：憑證欄位，由有效期限起始時間與有效期限截止時間二個子欄位所組成。

◆ **E**

- **終端個體(End Entity, EE)**：在 GPKI 中包括以下兩類個體：
  - 負責保管與應用憑證的私密金鑰擁有者。
  - 信賴 GPKI 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與信賴憑證者，包括人員、組織、客戶、裝置或站台。

◆ **F**

- **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，所有政府機構與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。

- **G**

  - **政府憑證總管理中心(Government Root Certification Authority)**：GPKI 根憑證機構，在此階層式公開架構中最頂層之憑證機構，其公開金鑰為信賴之起源。

- **I**

  - **網際網路工程任務小組(Internet Engineering Task Force, IETF)**：負責網際網路標準之開發與推動，其願景係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。(官方網站：https://www.ietf.org)

  - **簽發憑證機構(Issuing CA)**：對一張憑證而言，簽發該憑證之憑證機構即稱為該憑證之簽發憑證機構。

- **K**

  - **金鑰託管(Key Escrow)**：依用戶須遵守之託管協議(或類似契約)所規定相關資訊，將用戶之私密金鑰進行存放，此託管協議條款要求一個或以上之代理機構，基於有益於用戶、雇主或另一方之前提下，依協議規定擁有用戶之金鑰。

  - **金鑰對(Key Pair)**：兩把數學上有相關性之金鑰，其特性如下：
    - 其中一把金鑰用以進行訊息加密，而此加密訊息僅有另一把可解密。
    - 從其中一把金鑰要推出另一把金鑰(從計算之角度而言)是不可行。

◆ O

- **物件識別碼(Object Identifier, OID)**
  - 一種以字母或數字組成之唯一識別碼，該識別碼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。
  - 向國際標準機構(International Organization for Standardization)註冊之特別形式數碼，當提及某物件或物件類別時，可以引用此唯一之數碼進行辨識。例如於公開金鑰基礎架構中以此數碼指明使用之憑證政策與使用之密碼演算法。

- **線上憑證狀態協定(Online Certificate Status Protocol, OCSP)**：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)。

- **組織驗證(Organization Validation, OV)**：TLS 憑證核發過程中，除了識別及鑑別用戶之網域名稱控制權外，並且依照憑證的保證等級識別及鑑別用戶之組織或個人身分。故連結安裝組織驗證型 TLS 憑證之網站，可提供 TLS 加密通道，知道該網站之擁有者是誰，並確保傳遞資料之完整性。

◆ P

- **私密金鑰(Private Key)**：下述二情況下此金鑰均須保密。
  - 簽章金鑰對中用以產生數位簽章之金鑰。
  - 加解密金鑰對中用以對敏感性資訊解密之金鑰。

- **公開金鑰(Public Key)**：下述二情況下此金鑰均須公開可得(一般以數位憑證形式)。

- 簽章金鑰對中用以驗證數位簽章有效之金鑰。
- 加解密金鑰對中用以對敏感性資訊加密之金鑰。

- **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、稽核及服務之集合，在廣泛尺度上發展與管理非對稱式密碼學及公鑰憑證。

◆ **R**

- **註冊中心(Registration Authority, RA)**
  - 負責確認憑證申請人之身分或其他屬性，惟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。
  - 負責對憑證主體做身分識別及鑑別，惟不做憑證簽發。

- **金鑰更換(Re-key a Certificate)**：憑證金鑰更換係指簽發一張與舊憑證具有相同特徵與保證等級之新憑證，新憑證除具有全新、不同之公開金鑰(對應新且不同之私密金鑰)及不同序號外，亦可被指定不同之有效期限。

- **信賴憑證者(Relying Party)**
  - 信賴所收受之憑證與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) 與憑證所載公開金鑰之對應關係者。
  - 個人或機構收到包含憑證與數位簽章之資訊，且可能信賴這些資訊(此數位簽章可藉由憑證上所列之公開金鑰做驗證)。

- **憑證展期(Renew a Certificate)**：係指簽發一張與舊憑證具有相同憑證主體名稱、金鑰及相關資訊之新憑證，使憑證之有效期限予以展延，並付予一個新序號。

- **儲存庫(Repository)**
  - 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)。
  - 包含憑證政策、憑證實務作業基準及憑證相關資訊之資料庫。

- **憑證廢止(Revoke a Certificate)**：在憑證之有效期間內，提前終止憑證之運作。

- **根憑證機構(Root Certification Authority, Root CA)**：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供應商負責散布。亦可稱為憑證總管理中心或最頂層憑證機構。

◆ **S**

- **自簽憑證(Self-Signed Certificate)**：自簽憑證係指憑證的簽發者名稱與憑證主體的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。一個公開金鑰基礎建設內的自簽憑證，可做為憑證路徑信賴的起源，其簽發對象為總管理中心本身，內含總管理中心的公開金鑰，且憑證簽發者名稱與憑證主體名稱相同，可供信賴憑證者用於驗證總管理中心簽發之自發憑證、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。

- **下屬憑證機構(Subordinate Certification Authority)**：階層架構之公開金鑰基礎建設中，憑證由另一個憑證機構所簽發，且其活動受限於此另一憑證機構之憑證機構。

- **用戶(Subscriber)**
  - 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。
  - 具下列特性之個體，包括(但不限於)個人、機構或網路裝置：
    - ✓ 簽發憑證上所敘明之主體。
    - ✓ 擁有與憑證上所列公開金鑰對應之私密金鑰。
    - ✓ 本身不簽發憑證予其他方。

◆ **T**

- **可信賴系統(Trustworthy System)**：具有下列性質之電腦硬體、軟體與程序：
  - 對於入侵與誤用有相當之保護功能。
  - 提供合理之可用性、可靠度及正確操作。
  - 適當地執行預定功能。
  - 與一般為人所接受之安全程序一致。

◆ **Z**

- **零值化(Zeroize)**：清除電子式儲存資料之方法，藉由改變資料儲存，以防止資料被復原。

附錄 2：英文名詞縮寫

縮寫	全稱
AIA	Authority Info Access
CA	Certification Authority
CAA	Certification Authority Authorization
CP	Certificate Policy
CP OID	Certificate Policy Object Identifier
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
DNS	Domain Name System
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
IETF	Internet Engineering Task Force
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OV	Organization Validation
PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standard
PKI	Public Key Infrastructure
RA	Registration Authority
RFC	Request for Comments
SSL	Security Socket Layer
TLS	Transport Layer Security