政府憑證總管理中心

憑證實務作業基準

(Government Root 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

政府憑證總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
Ver1.0	2002/04/18	初版發行
Ver1.1	2003/01/09	將憑證格式詳細內容另外以憑證格式剖繪中說明
Ver1.2	2012/03/14	修訂 GRCA 對外公布之公開資訊類型
Ver1.3	2012/10/25	1. 新增總管理中心簽發憑證種類：自發憑證 (Self-Issued Certificate) 2. 定義外部稽核人員須符合之資格 3. 定義總管理中心私密金鑰用途與有效期限 4. 定義逾保存年限資料之處理方式 5. 新增 SHA-2 演算法 6. 新增密碼模組之標準
Ver1.4	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. 修訂本國政府機關申請憑證機構憑證之相關規定
Ver1.5	2017/12/25	1. 新增憑證機構與瀏覽器論壇所發行之 Baseline Requirements 之規範 2. 修訂總管理中心憑證命名規則 3. 刪除 SHA-1 演算法
Ver2.0	2021/07/02	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。

目　　錄

摘要

政府憑證總管理中心憑證實務作業基準重要事項說明如下：

1. 主管機關核定文號：經商字第 11002418250 號。

2. 簽發之憑證：

(1) 憑證種類：政府憑證總管理中心(以下簡稱總管理中心)之自簽憑證、自發憑證、簽發予下屬憑證機構之下屬憑證機構憑證及簽發予交互認證憑證機構之交互憑證。

(2) 保證等級：依政府機關公開金鑰基礎建設憑證政策(以下簡稱憑證政策)所定義之身份識別保證等級。

(3) 適用範圍：

A. 自簽憑證用以建立政府機關公開金鑰基礎建設信賴之起源。

B. 自發憑證為總管理中心更換金鑰或憑證政策需要時所簽發之憑證，用以建立新舊金鑰間或憑證政策互通憑證信賴路徑。

C. 下屬憑證機構憑證用以建立基礎建設之憑證機構間互相信賴關係，以建構憑證機構互通所需之憑證信賴路徑。

D. 交互憑證用以建立不同公開金鑰基礎建設之憑證機構間互相信賴關係，以建構憑證機構互通所需之憑證信賴路徑。

3. 法律責任重要事項：

(1) 憑證機構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，總管理中心不負任何法律責任。

(2) 與總管理中心交互認證之憑證機構，因簽發憑證或使用憑證致有損害賠償事件時，總管理中心之損害賠償責任，以本作業基準與相關契約所訂之責任範圍為限。

(3) 如因不可抗力或其他非可歸責於總管理中心之事由，所導致之損害事件，總管理中心不負任何法律責任。

4. 其他重要事項：

(1) 總管理中心如有系統維護、轉換及擴充等需求，得暫停部分憑證服務，並公告於儲存庫與通知憑證機構，信賴憑證者、下屬憑證機構或交互認證憑證機構不得以此作為要求總管理中心損害賠償之理由。

(2) 總管理中心直接受理憑證申請與憑證廢止等工作，不另設立註冊中心。

(3) 總管理中心簽發之憑證，依不同保證等級有不同之適用範圍，憑證機構提出憑證申請時，須敘明所申請憑證之保證等級。

(4) 憑證機構須自行產製私密金鑰，並妥善保管與使用。

(5) 憑證機構接受總管理中心所簽發之憑證後，即表示該憑證機構已確認憑證內容資訊之正確性。

(6) 憑證機構如有廢止憑證需求時，應儘速通知總管理中心，並應遵守本作業基準規定程序辦理，惟憑證廢止狀態未被公布之前，應先行採取適當之行動，以減少對憑證機構或信賴憑證者之影響，並承擔所有因使用該憑證所引發之法律責任。

(7) 信賴憑證者使用總管理中心簽發之憑證時，應先確認該憑證之正確性、有效性、保證等級及用途限制。

(8) 國發會依政府採購法規定委託公正第三方，針對總管理中心之運作進行外部稽核作業。

1.簡介

政府憑證總管理中心憑證實務作業基準(Government Root 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(Certificate Policy for the Government Public Key Infrastructure，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。

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

政府憑證總管理中心(Government Root Certification Authority, GRCA，以下簡稱總管理中心)遵照憑證政策執行以下憑證之簽發與管理作業。

1. 自簽憑證(Self-Signed Certificate)。
2. 自發憑證(Self-Issued Certificate)。
3. 下屬憑證機構憑證(Subordinate Certification Authority Certificate)。
4. 交互憑證(Cross-Certificate)。

1.1 總覽

總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)之根憑證機構(Root Certification Authority, Root CA)，亦為本基礎建設之信賴起源(Trust Anchor)，信賴憑證者可直接信賴總管理中心本身之憑證。

總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 4 級之規定。本作業基準所載明之實務作業規範僅適用於與總管理中心相關之個體，如總管理中心、下屬憑證機構(Subordinate Certification Authority)、交互認證憑證機構、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)為總管理中心之主管機關，負責本作業基準之訂定與修訂，本作業基準須電子簽章法主管機關核可後公布施行。本作業基準並未授權總管理中心以外之憑證機構使用，其他憑證機構如引用本作業基準所引發之任何問題，由該憑證機構自行負責。

1.2 文件名稱及識別

1. 文件名稱：「政府憑證總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 7 月 2 日
4. 發布網址：
   https://grca.nat.gov.tw/download/GRCA_CPS_v2.0.pdf
5. 憑證政策物件識別碼(Certificate Policy Object Identifier)：

物件識別碼名稱	物件識別碼
保證等級	
■ 測試級	2.16.886.101.0.3.0
■ 第 1 級	2.16.886.101.0.3.1
■ 第 2 級	2.16.886.101.0.3.2
■ 第 3 級	2.16.886.101.0.3.3
■ 第 4 級	2.16.886.101.0.3.4

1.3 主要成員

總管理中心之主要成員包括：

1. 總管理中心。
2. 下屬憑證機構。
3. 交互認證憑證機構。
4. 信賴憑證者。
5. 其他相關成員。

1.3.1 憑證機構

1.3.1.1 總管理中心

係本基礎建設之根憑證機構，亦為本基礎建設之信賴起源，主要工作說明如下：

1. 負責自簽憑證、自發憑證及下屬憑證機構憑證之簽發與管理。

2. 訂定總管理中心與本基礎建設外之根憑證機構間交互認證(Cross-Certification)之程序，包括交互憑證之簽發與管理。

3. 將簽發之憑證與憑證機構廢止清冊(Certification Authority Revocation List, CARL)公布於儲存庫。

1.3.1.2 下屬憑證機構

下屬憑證機構之工作說明如下：

1. 負責簽發與管理終端個體(End Entity, EE)之憑證。

2. 可依階層式公開金鑰基礎建設之建構方式，由下屬憑證機構簽發憑證予次一層下屬憑證機構，依此原則建構多層次之公開金鑰基礎建設架構。

3. 下屬憑證機構不可直接與本基礎建設外之憑證機構進行交互認證。

4. 下屬憑證機構應依憑證政策相關之規定建置，並設置聯絡窗口，負責與總管理中心及其他下屬憑證機構之互運工作。

1.3.1.3 交互認證憑證機構

本基礎建設外之根憑證機構，可向總管理中心申請成為交互認證憑證機構，須符合憑證政策保證等級安全性規定，並具備公開金鑰基礎建設、數位簽章及憑證簽發技術之建置與管理能力，亦須訂定憑證機構、註冊中心(Registration Authority, RA)及信賴憑證者之相關責任與義務。

1.3.2 註冊中心

總管理中心直接受理憑證申請與憑證廢止等工作，不另設立註冊中心。

1.3.3 用戶

依憑證政策之定義，憑證內主體名稱所識別之個體若為憑證機構，則稱之為主體憑證機構，而非用戶；總管理中心所簽發之憑證主體皆為憑證機構，並未簽發用戶憑證。

1.3.4 信賴憑證者

1. 係指相信憑證主體名稱與公開金鑰間連結關係之個體。
2. 信賴憑證者須檢驗憑證及其憑證串鏈中所有憑證機構憑證，確認憑證狀態有效性後，方可使用憑證進行下述作業：

   (1) 驗證具有數位簽章的電子文件之完整性。

   (2) 驗證電子文件簽章產生者的身分。

   (3) 與憑證主體間建立安全之通訊管道。

1.3.5 其他相關成員

國發會依照政府採購法委託合格廠商，負責總管理中心建置與維運作業。

1.4 憑證用途

1.4.1 憑證之適用範圍

總管理中心簽發之憑證，包括自簽憑證、自發憑證、下屬憑證機

構憑證及交互憑證等 4 種憑證。

1. 自簽憑證

(1) 簽發對象為總管理中心。

(2) 內含總管理中心之公開金鑰，用以驗證自發憑證、下屬憑證機構憑證、交互憑證及憑證機構廢止清冊之數位簽章。

(3) 用以建立政府機關公開金鑰基礎建設信賴之起源。

2. 自發憑證

(1) 總管理中心更換金鑰或憑證政策需要時所簽發之憑證。

(2) 用以建立新舊版本金鑰間或憑證政策互通憑證信賴路徑之用。

3. 下屬憑證機構憑證

(1) 簽發對象為政府公開金鑰基礎建設之下屬憑證機構。

(2) 內含下屬憑證機構之公開金鑰，用以驗證下屬憑證機構所簽發之憑證與憑證廢止清冊之數位簽章。

(3) 用以建立基礎建設之憑證機構間互相信賴關係，以建構憑證機構互通所需之憑證信賴路徑。

4. 交互憑證

(1) 簽發對象為與總管理中心進行交互認證之憑證機構。

(2) 內含交互認證憑證機構之公開金鑰，用以驗證該憑證機構簽發之憑證與憑證廢止清冊之數位簽章。

(3) 用以建立不同公開金鑰基礎建設之憑證機構間互相信賴關係，以建構憑證機構互通所需之憑證信賴路徑。

1.4.2 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。

1.4.3 憑證之使用限制

1. 信賴憑證者應依 6.1.4 節「總管理中心公開金鑰安全傳送予信賴憑證者」之規定，取得總管理中心公開金鑰或自簽憑證。
2. 信賴憑證者應慎選安全之電腦環境與可信賴之應用系統，以避免使用之總管理中心公開金鑰或自簽憑證遭破壞或更換。
3. 信賴憑證者應確認使用之總管理中心公開金鑰或自簽憑證之正確性，始可用以驗證總管理中心簽發之自發憑證、下屬憑證機構憑證、交互憑證及憑證機構廢止清冊之數位簽章。
4. 信賴憑證者應使用符合 ITU-T X.509、RFC5280 或相關國際標準定義之憑證驗證方式，檢查憑證之有效性。
5. 信賴憑證者應依 ITU-T X.509 規範處理憑證中之關鍵性與非關鍵性憑證擴充欄位。

6. 信賴憑證者應確認憑證之保證等級與金鑰用途等符合應用需求。若為交互憑證，則應再檢驗該憑證記載之交互認證層數與所採用之憑證政策與憑證政策間政策對應之關係。

7. 信賴憑證者應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

總管理中心負責制訂及管理本作業基準。

1.5.2 聯絡資料

總管理中心之聯絡電話、郵遞地址及電子郵件信箱，詳參「http://grca.nat.gov.tw/」。

1.5.3 憑證實務作業基準之審定

本作業基準之審定，應符合下列程序：

1. 經行政機關電子憑證推行小組審查。

2. 送電子簽章法主管機關審查核定。

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「憑證實務作業基準之審定」規定辦理；憑證政策如有修訂並公告後，本作業基準應配合修訂。

1.6 名詞定義及縮寫

請詳參附錄 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) 憑證政策與技術規範。

   (2) 本作業基準。

   (3) 總管理中心簽發之憑證。

   - 總管理中心本身之自簽憑證。
   - 總管理中心新舊金鑰互簽之自發憑證。
   - 下屬憑證機構憑證。
   - 交互憑證。

   (4) 憑證機構廢止清冊。

   (5) 最新外部稽核結果。

   (6) 隱私權保護政策。

   (7) 最新消息及其他憑證相關資訊。

2. 儲存庫提供全天候(7x24)服務，網址：
   「https://grca.nat.gov.tw/01-06.html」。

3. 儲存庫之存取控制依照 2.4 節「存取控制」規定辦理。

2.2 憑證資訊公布

總管理中心採以下方式公布憑證資訊：

1. 憑證機構廢止清冊。
2. 線上憑證狀態協定(Online Certificate Status Protocol, OCSP)查詢服務。
3. 儲存庫之憑證下載服務。

2.3 公布頻率或時間

1. 本作業基準之制訂與修訂經電子簽章法主管機關核可後於 10 個工作天內公告於儲存庫。
2. 總管理中心每日至少簽發並公告 1 次憑證機構廢止清冊。
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. 總管理中心建置資安防護機制，儲存庫及外界皆無法直接連線至總管理中心主機。
2. 總管理中心只允許經授權之人員管理儲存庫主機。
3. 總管理中心須公布簽發之憑證與憑證機構廢止清冊時，由總管理中心授權之人員以離線手動方式，將其儲存於可攜式媒體，並複製至儲存庫主機中公布。

4. 下屬憑證機構、交互認證憑證機構及信賴憑證者可透過儲存庫查詢與下載總管理中心公告之資訊。

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. 自簽憑證、自發憑證、下屬憑證機構憑證及交互憑證均使用此唯一識別名稱之格式。

3.1.2 命名須有意義

申請成為下屬憑證機構或交互認證憑證機構之憑證主體名稱應符合該機關(構)或單位據以設立之相關法令規定，且足以代表與識別該憑證機構之名稱。

3.1.3 用戶匿名或假名

總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 ITU-T X.520 名稱屬性定義。

2. 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」訂定。

3.1.5 命名獨特性

1. 自簽憑證

自簽憑證之 ITU-T X.500 唯一識別名稱如下：

(1) 第 1 代與第 2 代自簽憑證

C=TW，O=Government Root Certification Authority

(2) 第 3 代及其後之自簽憑證

自民國 106 年 12 月 25 日起，使用以下名稱格式：

C=TW，O=行政院，CN=Government Root Certification Authority - Gn

其中，n=3,4…

2. 自發憑證

(1) 自發憑證之唯一識別名稱與被簽發之總管理中心自簽憑證之唯一識別名稱相同。

(2) 因第 1 代與第 2 代自簽憑證主體同名造成其相互簽發之自發憑證被瀏覽器誤認為自簽憑證，導致驗證憑證信賴路徑時產生錯誤，故總管理中心產製第 1.5 代金鑰，簽發自發憑證，重新建構第 1 代與第 2 代自簽憑證之信賴路徑，並使用以下名稱格式：

C=TW，O=行政院，CN=Government Root Certification Authority - G1.5

3. 下屬憑證機構憑證與交互憑證

下屬憑證機構或交互認證憑證機構名稱重複時，總管理中心得要求該憑證機構修改名稱。

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

憑證機構之名稱所有權有爭議時，由國發會協調。

3.2 初始註冊

3.2.1 證明擁有私密金鑰之方式

1. 憑證機構自行產製金鑰對，以該金鑰對產製 PKCS#10 憑證申請檔並加以簽章後交予總管理中心。

2. 總管理中心使用該憑證機構之公開金鑰驗證該憑證申請檔之簽章，以證明該憑證機構擁有相對應之私密金鑰。

3.2.2 組織身分之鑑別程序

1. 下屬憑證機構以正式公文提供憑證申請書，由總管理中心驗證公文書之正確性，以證明該機關(構)及單位確實存在且申請獲得授權。

2. 憑證機構經營者如非本國政府機關，應以正式公文提供交互認證申請書，由總管理中心驗證公文書之正確性，以證明該機關(構)及單位確實存在且申請獲得授權。

3.2.3 個人身分之鑑別程序

1. 憑證機構經營者如為本國政府機關時，無須進行個人身分鑑別之程序。

2. 憑證機構經營者如非本國政府機關時，須正式指派代表人(被授權辦理交互認證申請之個人)辦理憑證申請相關作業，其身分鑑別程序如下：

   (1) 代表人須親臨以證明其身分。

   (2) 審查代表人之授權證明書。

   (3) 代表人於申請憑證時，應出示中華民國國民身分證正本或護照，以供總管理中心鑑別其代表人之身分。

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. 透過第三方之身分鑑別服務、具公信力之資料庫、政府機關或有權責及公信力之團體，證明該組織之存在。

2. 藉由申請者親臨核對身分或其他可信賴之方式，確認該憑證申請者獲授權代表該憑證主體

3.2.6 交互運作標準

不予規定。

3.2.7 資通訊設備或伺服器應用軟體鑑別之程序

不適用。

3.2.8 資料正確性

總管理中心應評估資料正確性，評估過程應考慮以下事項：

1. 所提供資料之存在時間。

2. 資料來源之更新頻率。

3. 資料提供者和資料收集之目的。

4. 資料可用性。

5. 資料可公開取得之程度。

6. 偽造或變更資料之相對困難性。

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

1. 總管理中心因私密金鑰使用期限屆滿需更換金鑰對並重新申請憑證時，依 4.2 節「申請憑證之程序」規定辦理。

2. 憑證機構因私密金鑰使用期限屆滿需更換金鑰對並重新申請憑證時，總管理中心依 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

1. 總管理中心因憑證廢止需更換金鑰對並重新申請憑證時，依 4.2 節「申請憑證之程序」規定辦理。

2. 憑證機構因憑證廢止需更換金鑰對並重新申請憑證時，總管理中心依 3.2 節「初始註冊」規定辦理。

3.3.3 憑證展期之金鑰更換識別及鑑別

總管理中心簽發之自簽憑證、自發憑證、下屬憑證機構憑證及

交互憑證不得展期。

3.4 憑證廢止申請之識別及鑑別

1. 自簽憑證與自發憑證之憑證廢止申請依 4.9 節「憑證暫時停用及廢止」規定辦理。

2. 憑證機構憑證廢止申請之鑑別程序與 3.2.2 節「組織身分之鑑別程序」及 3.2.3 節「個人身分之鑑別程序」規定相同。

3.5 憑證暫時停用與恢復使用之識別及鑑別

總管理中心簽發之自簽憑證、自發憑證、下屬憑證機構憑證以及交互憑證不得暫時停用與恢復使用。

4.憑證生命週期營運規範

4.1 憑證申請

4.1.1 憑證之申請者

憑證申請者包含：

1. 總管理中心。
2. 下屬憑證機構。
3. 本基礎建設外之根憑證機構。

4.1.2 註冊程序及責任

4.1.2.1 總管理中心之義務

1. 依憑證政策保證等級第 4 級規定與本作業基準運作。
2. 安全產製並妥善管理總管理中心之私密金鑰。
3. 簽發總管理中心自簽憑證與自發憑證。
4. 訂定下屬憑證機構申請與憑證機構之交互認證申請程序。
5. 受理下屬憑證機構及交互認證憑證機構之憑證申請與廢止申請。
6. 簽發並公布憑證機構憑證。
7. 簽發並公布憑證機構廢止清冊。

4.1.2.2 下屬憑證機構之義務

1. 遵守本作業基準之規定，如未遵守導致信賴憑證者遭受損害時，應負損害賠償責任。

2. 敘明所申請憑證之保證等級。

3. 應依第 6 章「技術性安全控管」規定，自行產製並妥善保管及使用私密金鑰。

4. 應依 4.2 節「申請憑證之程序」規定辦理憑證申請，並確保申請資料之正確性。

5. 總管理中心同意申請並簽發憑證後，下屬憑證機構應於取得憑證後確認憑證內容資訊之正確性，依 4.4 節「接受憑證之程序」規定辦理憑證接受。

6. 應依 4.5 節「金鑰對及憑證之用途」規定使用憑證。

7. 下屬憑證機構如發生私密金鑰資料外洩或遺失等情形致須廢止憑證時，應立即通知總管理中心，並依 4.9 節「憑證暫時停用及廢止」規定辦理。惟下屬憑證機構仍應承擔憑證廢止狀態未被公布前所有使用該憑證之法律責任。

8. 總管理中心如因故無法正常運作時，下屬憑證機構應儘速尋求其他途徑完成與他人應為之法律行為，不得以總管理中心無法正常運作，作為抗辯他人之事由。

4.1.2.3 交互認證憑證機構之義務

交互認證憑證機構之義務與 4.1.2.2 節「下屬憑證機構之義務」

相同。

4.2 申請憑證之程序

1. 總管理中心之憑證申請

   總管理中心之自簽憑證及自發憑證由總管理中心透過公開儀式產製金鑰對及 PKCS#10 憑證申請檔後，經行政機關電子憑證推行小組委員會議同意後，進行憑證簽發。

2. 下屬憑證機構及交互認證憑證機構之憑證申請

   (1) 起始(Initiation)

   A. 憑證機構指派適當人員，代表該憑證機構申請憑證。

   B. 憑證申請人將憑證機構憑證申請書、憑證實務作業基準及 PKCS#10 憑證申請檔等資料，以公文函送總管理中心，如憑證機構遵循之憑證政策，非政府機關公開金鑰基礎建設憑證政策時，應另檢附所遵循之憑證政策。

   (2) 審查申請(Examination)

   總管理中心應對憑證機構提出之申請案進行審查，查驗項目如下：

   - 依 3.2.2 節「組織身分之鑑別程序」規定，對提出申請之憑證機構進行識別與鑑別。
   - 確認憑證機構與總管理中心無技術相容性之問題。

- 檢查憑證機構之憑證實務作業基準是否遵循所引用之憑證政策，若申請交互認證之憑證機構所遵循之憑證政策非政府機關公開金鑰基礎建設憑證政策時，總管理中心應檢查其憑證政策與總管理中心憑證政策之對應關係。

- 檢驗憑證申請者交付之 PKCS#10 憑證申請檔。

總管理中心得要求憑證機構補送資料或拒絕申請，若審查通過，應將審查結果通報國發會，國發會依下列原則進行裁示。

A. 如申請憑證之憑證機構為我國政府機關，審查通過並經國發會確認後，即可進行憑證簽發。

B. 如申請憑證之憑證機構非我國政府機關，審查通過並經國發會確認後，則進入下一階段。

(3) 協議(Arrangement)

國發會召開行政機關電子憑證推行小組委員會議，並通知憑證申請之代表人到場參加，進行以下步驟：

A. 依 3.2.3 節「個人身分之鑑別程序」規定對憑證機構之代表人進行身分識別與鑑別程序。

B. 檢驗憑證機構提交之「授權證明書」，確認該申請有經過授權。

C. 報告憑證機構申請案件之審查結果。

D. 如同意該申請案件，總管理中心將依會議之決議辦理後續憑證簽發程序。

4.2.1 執行識別及鑑別功能

總管理中心依 3.2.2 節「組織身分之鑑別程序」及 3.2.3 節「個人身分之鑑別程序」規定，對提出申請之憑證機構及被授權之代表人進行身分識別與鑑別作業。

4.2.2 憑證申請之批准或拒絕

1. 總管理中心憑證之申請

   總管理中心之憑證申請由行政機關電子憑證推行小組委員會議進行審查，如同意申請時，由總管理中心進行後續之簽發憑證程序。

2. 下屬憑證機構及交互認證憑證機構之申請

   經審查後，如同意申請，總管理中心將進行後續之簽發憑證程序，如不同意申請，總管理中心應以公文通知憑證機構，並敘明未核可之理由。

4.2.3 處理憑證申請之時間

憑證機構提出憑證申請審查通過後，總管理中心應於 7 個工作天內完成憑證之簽發。

4.3 憑證簽發

4.3.1 總管理中心於憑證簽發時之作業

總管理中心依 5.2 節「程序控管」規定，由相關人員執行憑證簽發作業。

4.3.2 總管理中心對憑證申請者之憑證簽發通知

1. 憑證簽發後以公文檢附簽發之憑證通知憑證機構，如不同意申請，應以公文通知憑證機構，並敘明未核可之理由。

2. 總管理中心簽發自簽憑證及自發憑證後以電子郵件或電話通知國發會。

4.4 憑證接受

4.4.1 接受憑證之要件

1. 總管理中心與國發會確認自簽憑證與自發憑證之資訊無誤後，將自簽憑證與自發憑證公布於儲存庫。

2. 憑證機構收到憑證後，應確認憑證內容之正確性，並以公文函復完成憑證接受。

3. 憑證機構如於 30 個工作天內未接受憑證，總管理中心將廢止該憑證，不另行公布。

4.4.2 總管理中心之憑證發布

總管理中心定期將所簽發之憑證公布於儲存庫。

4.4.3 總管理中心對其他個體之憑證簽發通知

1. 總管理中心將所簽發之憑證公布於儲存庫。

2. 總管理中心另依各作業系統、瀏覽器及軟體平台之根憑證計畫(Root Certificate Program)規定，進行新簽發憑證之通知。

4.5 金鑰對及憑證之用途

4.5.1 憑證機構私密金鑰及憑證使用

1. 憑證機構金鑰對之產製應符合 6.1.1 節「金鑰對產製」規定，且憑證機構須有私密金鑰之控制權。

2. 憑證機構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。

3. 憑證機構須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 及網際網路工程任務小組(Internet Engineering Task Force, IETF)之 RFC 相關標準或規範之軟體。

3. 信賴憑證者須驗證憑證有效性，包括憑證及其憑證串鏈中所有的憑證機構憑證；其中，憑證狀態資訊可透過憑證機構廢止清冊或線上憑證狀態協定查詢服務取得。

(1) 憑證機構廢止清冊下載網址註記於憑證之憑證廢止清冊發布點(CRL Distribution Point, CDP)擴充欄位。

(2) 線上憑證狀態協定查詢服務網址註記於憑證之憑證機構資訊存取(Authority Information Access, AIA)擴充欄位。

4. 信賴憑證者確認憑證有效性後方可使用憑證進行下述作業：

(1) 驗證具有數位簽章之電子文件之完整性。

(2) 驗證文件簽章產生者之身分。

(3) 與用戶間建立安全之通訊管道。

5. 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。

6. 信賴憑證者應確認憑證用途。

4.6 憑證展期

憑證機構之憑證不可展期。

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 對憑證機構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 總管理中心對其他個體之憑證簽發通知

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 總管理中心自簽憑證之金鑰更換事由

1. 總管理中心私密金鑰執行簽發憑證用途之使用期限到期。

2. 總管理中心之自簽憑證被廢止。

4.7.1.2 憑證機構之金鑰更換事由

1. 憑證機構用私密金鑰執行簽發憑證用途之使用期限到期。

2. 憑證機構之憑證被廢止。

4.7.2 更換憑證金鑰之申請者

總管理中心、下屬憑證機構或交互認證憑證機構更換憑證金鑰之申請，由經授權之代表人辦理。

4.7.3 憑證之金鑰更換程序

1. 總管理中心之自簽憑證更換金鑰時，依 4.2 節「申請憑證之程序」規定辦理。

2. 憑證機構應依 3.2 節「初始註冊」、3.3 節「金鑰更換請求之識別及鑑別」、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 對憑證機構憑證金鑰更換之簽發通知

依 4.3.2 節「總管理中心對憑證申請者之通知」規定辦理。

4.7.5 接受金鑰更換憑證之要件

接受憑證更換金鑰之要件，依 4.4.1 節「接受憑證之要件」規定辦理。

4.7.6 總管理中心之更換金鑰憑證發布

總管理中心將金鑰更換之新憑證公布於儲存庫。

4.7.7 總管理中心對其他個體之憑證簽發通知

總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. 總管理中心或憑證機構變更憑證主體內次要屬性資訊(如更新憑證政策擴充欄位中的憑證政策物件識別碼)

2. 變更之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。憑證變更後，舊憑證應予以廢止。

3. 變更主體名稱等重要身分資料不屬憑證變更，憑證機構須依憑證申請相關規定重新申請憑證，且舊憑證須廢止。

4.8.2 憑證變更之申請者

總管理中心、下屬憑證機構或交互認證憑證機構更換憑證金鑰之申請，由經授權之代表人辦理。

4.8.3 憑證變更之程序

總管理中心依 4.2 節「申請憑證之程序」進行身分識別、鑑別與審查作業，並於憑證變更申請核可後簽發新憑證並廢止舊憑證。

4.8.4 對憑證機構憑證變更之簽發通知

依 4.3.2 節「總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

依 4.4.1 節「接受憑證之要件」規定辦理。

4.8.6 總管理中心之憑證變更發布

總管理中心將金鑰更換之新憑證公布於儲存庫。

4.8.7 總管理中心對其他個體之憑證簽發通知

總管理中心將金鑰更換後之憑證公布於儲存庫。

4.9 憑證暫時停用及廢止

總管理中心提供全天候(7x24)之憑證廢止服務，但不提供憑證暫時停用服務。

4.9.1 廢止憑證之事由

1. 總管理中心廢止憑證之事由(包括但不限於如下情形)：

   (1) 總管理中心私密金鑰遭到破解。

   (2) 總管理中心私密金鑰遺失、遭竊、異動、未經授權之揭露、盜用或其他破壞。

   (3) 憑證不再需要使用。

   (4) 憑證記載內容有誤或需變更。

2. 下屬憑證機構或交互認證憑證機構廢止憑證之事由(包括但不限於如下情形)：

   (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需變更；如變更憑證主體資訊，總管理中心具有廢止憑證之審查權。

(5) 憑證申請未獲得憑證機構授權，且經詢問後憑證機構不願意回溯給予授權。

3. 總管理中心逕行廢止憑證機構憑證之事由(包括但不限於如下情形)：

(1) 總管理中心之私密金鑰或系統遭冒用、偽造或破解。

(2) 憑證機構之私密金鑰遭冒用、偽造或破解。

(3) 憑證機構之私密金鑰不再符合 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。

(4) 憑證記載之內容不實、存在誤導可能性或發生重大改變。

(5) 總管理中心或憑證機構憑證遭誤用。

(6) 總管理中心未依憑證政策或本作業基準規定簽發憑證。

(7) 憑證機構未遵照憑證政策、本作業基準、約定條款或相關法令之規定。

(8) 總管理中心或憑證機構終止服務，且未安排另一個憑證管理中心來提供憑證廢止服務。

(9) 總管理中心或憑證機構已不具簽發憑證之權力，且其亦不再提供儲存庫、憑證機構廢止清冊/憑證廢止清冊或線上憑證狀態協定查詢服務。

(10) 依據憑證政策或本作業基準要求之廢止。

(11) 確認憑證機構私鑰傳送給未獲授權之人或非憑證機構隸屬之機關(構)或單位。

(12) 依我國司法機關、監察機關、治安機關或憑證機構主管機關通知。

(13) 總管理中心簽發憑證後，憑證機構未能於期限內接受憑證。

4.9.2 憑證廢止之申請者

憑證廢止之申請者如下：

1. 下屬憑證機構。

2. 交互認證憑證機構。

3. 下屬憑證機構或交互認證憑證機構之主管機關。

4. 總管理中心。

憑證機構、信賴憑證者、應用軟體供應商及其他第三方組織可針對有問題之憑證向總管理中心提出憑證問題報告(Certificate Problem Report)，如認為須廢止憑證，內容應敘明廢止原因，總管理中心依 4.9.3.3 節「憑證問題回應機制」之規定，確認憑證廢止請求是否成立。

4.9.3 憑證廢止之程序

4.9.3.1 憑證廢止方式

總管理中心依 3.4 節「憑證廢止申請之識別及鑑別」規定完成其及憑證機構之身分識別及鑑別後，始可進行憑證廢止。

1. 總管理中心憑證廢止

   總管理中心廢止自簽憑證及自發憑證時，由總管理中心進行評估後將結果通報國發會，經國發會同意後辦理。

2. 憑證機構憑證廢止

   (1) 由憑證機構指派適當人員提出憑證廢止申請。

   (2) 申請人填寫憑證廢止申請書。

   (3) 以公文書將憑證廢止申請書函送至總管理中心辦理憑證廢止事宜。

   (4) 總管理中心依 3.2.2 節「組織身分之鑑別程序」規定，執行身分識別與鑑別程序。

   (5) 總管理中心於審查憑證廢止申請時，得要求憑證機構補送資料或駁回申請，並將審查結果通報國發會。

   (6) 國發會如同意憑證廢止申請，總管理中心依國發會決議辦理後續作業。否決憑證廢止申請時，將以公文書方式通知該憑證機構，並說明未核可之理由。

3. 總管理中心逕行廢止憑證機構之憑證

   總管理中心逕行廢止憑證機構之憑證時，由總管理中心進行評估後將結果通報國發會，經國發會同意後辦理。

4.9.3.2 公告與通知

1. 廢止之憑證最遲於憑證機構廢止清冊下次更新時間(The nextUpdate)前加入憑證機構廢止清冊，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. 總管理中心以公文書方式通知憑證機構及其主管機關或負責單位憑證廢止申請之結果。

4.9.3.3 憑證問題回應機制

1. 總管理中心提供全天候(7x24)之憑證問題通報受理與憑證問題回應機制。

2. 問題發現者可將憑證問題反應至 1.5.2 節「聯絡資料」所提供之電子郵件信箱。

3. 總管理中心於接收到憑證問題後 24 小時內，提供初步調查報告給憑證機構與問題發現者。

4. 總管理中心與憑證機構及問題發現者共同討論；如須廢止該憑證，總管理中心將依下述準則評估與選定憑證廢止日期：

   (1) 聲稱問題的內容(範圍、內容、嚴重性、重要程度及危害風險)。

(2) 憑證廢止的後果(對憑證機構與信賴憑證者的直接與間接影響)。

(3) 針對該憑證或該憑證機構提出之憑證問題數量。

(4) 提出憑證問題的單位或人員。

(5) 相關的法律條文。

5. 總管理中心受理憑證問題報告或接收到憑證廢止通知之處理期限依 4.9.5 節「總管理中心處理憑證廢止請求之處理期限」規定辦理。

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. 總管理中心或憑證機構如欲廢止其憑證，最遲應於 10 個工作天內向總管理中心提出憑證廢止申請。

2. 如憑證機構因金鑰遭破解或因其他安全事由須廢止憑證時，憑證機構應於事件確認後 30 分鐘內通報總管理中心。

3. 如發生 4.9.1 節「廢止憑證之事由」中，毋須事先取得憑證機構同意，總管理中心得逕行廢止憑證之情形，則總管理中心將於憑證廢止事由確認成立後，逕行提出憑證廢止申請，並通知該憑證機構。

4.9.5 總管理中心處理憑證廢止請求之處理期限

1. 總管理中心於接受憑證廢止申請後 7 個工作天內完成憑證廢止作業。

2. 如遇 4.9.1 節「廢止憑證之事由」所述由總管理中心逕行廢止憑證且毋須事先經過憑證機構同意之事由，則其憑證廢止處理時間將於該事由確認成立後 7 個工作天內完成。

4.9.6 信賴憑證者檢查憑證廢止之要求

信賴憑證者使用總管理中心所簽發之憑證前，應先取得總管理中心公布之憑證機構廢止清冊或線上憑證狀態協定回應訊息並確認其簽章有效後，以此憑證狀態資訊檢驗該憑證之有效性及憑證串鏈之正確性。

4.9.7 憑證機構廢止清冊簽發頻率

1. 憑證機構廢止清冊每日至少簽發 1 次，其有效期限不超過 36 小時。

2. 當有憑證被廢止時，總管理中心於完成憑證廢止作業後的 24 小時內重新簽發憑證機構廢止清冊。

4.9.8 憑證機構廢止清冊發布之最大延遲時間

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

4.9.9 線上憑證廢止/狀態查驗之服務

1. 總管理中心提供憑證下載、憑證機構廢止清冊及線上憑證狀態協定查詢服務。

2. 總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 標準規範之線上憑證狀態協定回應訊息。

3. 總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機構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. 信賴憑證者至少可使用 HTTP GET 方法執行線上憑證狀態協定查詢服務。

3. 線上憑證狀態協定查詢服務至少每 12 個月更新自發憑證、下屬憑證機構憑證及交互憑證之狀態資訊，線上憑證狀態協定

回應訊息的最大效期為 36 小時；若前述憑證被廢止，則於該憑證廢止後 24 小時內更新憑證狀態資訊。

4. 線上憑證狀態協定回應伺服器接收到查詢尚未簽發之憑證的狀態請求，不可回覆其狀態為「正常(Good)」。總管理中心會監督線上憑證狀態協定回應伺服器對於這類請求之回覆是否符合上述安全回應程序。

4.9.11 其他形式廢止公告

總管理中心依據 RFC 4366 規範支援線上憑證狀態協定裝訂(OCSP Stapling)。

4.9.12 金鑰被破解時之其他特殊規定

憑證機構之私密金鑰如被破解，總管理中心將於公布之憑證機構廢止清冊中註明該憑證廢止之原因為金鑰被破解。

4.9.13 暫時停用憑證之事由

總管理中心不提供暫時停用憑證服務。

4.9.14 暫時停用憑證之申請者

不適用。

4.9.15 暫時停用憑證之程序

不適用。

4.9.16 暫時停用憑證期間之限制

不適用。

4.10 憑證狀態服務

4.10.1 服務特性

憑證機構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過期後始可移除。

4.10.2 服務可用性

1. 總管理中心提供全天候(7 x 24)不中斷之儲存庫服務。

   (1) 儲存庫提供憑證機構廢止清冊與線上憑證狀態協定查詢服務;正常運作時,憑證狀態查詢回覆時間須在 10 秒內。

   (2) 儲存庫無法正常運作時，須於 2 個工作天內恢復正常。

2. 總管理中心提供全天候(7 x 24)回應機制處理高優先權之憑證問題報告，並視情況向執法當局舉發及廢止該憑證。

4.10.3 可選功能

不予規定。

4.11 終止服務

終止服務係指憑證機構終止使用總管理中心之服務；總管理中心同意憑證機構終止服務之要件如下：

1. 憑證到期時終止總管理中心提供憑證機構之服務。

2. 憑證機構廢止憑證而終止服務。

3. 因交互認證約定條款或相關規定失效而終止服務。

4.12 私密金鑰託管及回復

4.12.1 金鑰託管及回復政策及實務

1. 總管理中心簽章用之私密金鑰不可被託管。

2. 總管理中心不提供憑證機構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

總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

總管理中心機房位於台北市信義路一段 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. 總管理中心之實體控管符合保證等級第 4 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，並由總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

總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、設定及維護總管理中心系統。
- 建立及維護總管理中心系統之使用者帳號。
- 設定稽核參數。
- 產製及備份總管理中心之金鑰。
- 公布憑證機構廢止清冊於儲存庫。

(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：

工作內容	管理員	簽發員	稽核員	維運員	實體安全控管員
安裝、設定及維護總管理中心憑證管理系統	1				1
建立及維護總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
產製及備份總管理中心之金鑰	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
公布憑證機構廢止清冊於儲存庫	1				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
除總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

各角色分派須符合下列規定：

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. 總管理中心工作人員，須由總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. 總管理中心之安全認證機制。 2. 總管理中心系統安裝、設定及維護之操作程序。 3. 建立及維護系統使用者帳號之操作程序。 4. 設定稽核參數之操作程序。 5. 產製及備份總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. 總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. 總管理中心之安全認證機制。 2. 總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一次教育訓練。

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，總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

總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記錄方式。

5.4.1 事件記錄之類型

1. 安全稽核

   (1) 重要稽核參數之改變。

   (2) 嘗試刪除或修改稽核紀錄。

2. 識別及鑑別

(1) 嘗試設定新角色。

(2) 管理者調整身分鑑別嘗試之最高容忍次數。

(3) 登入系統失敗。

(4) 帳號解鎖。

(5) 改變系統之身分鑑別機制。

3. 總管理中心產製金鑰時(不包括單次使用之金鑰產製)。

4. 總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. 憑證機構廢止清冊格式剖繪之改變

12. 總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

總管理中心每月檢視 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總管理中心之系統，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，總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記錄。

5.4.8 弱點評估

1. 總管理中心每年進行一次風險評鑑，對作業系統、實體設施、憑證管理系統及網路進行評估。

2. 總管理中心遭遇重大資安事件時，應進行風險評鑑。

5.5 紀錄歸檔之方法

5.5.1 歸檔紀錄之類型

1. 總管理中心被主管機關認證過程及結果資料。

2. 憑證實務作業基準。

3. 交互認證協議。

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. 已簽發或公告之憑證。

10. 總管理中心金鑰更換之紀錄。

11. 已簽發或公告之憑證機構廢止清冊。

12. 稽核紀錄。

13. 用以驗證及佐證歸檔內容之其他說明資料或應用程式。

14. 稽核人員所要求之文件。

15. 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 20 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 1 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. 紙本紀錄將由總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. 總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

總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. 總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，並簽發 1 張新自簽憑證及 2 張自發憑證。新簽發之自簽憑證依 6.1.4 節「總管理中心公開金鑰安全傳送予信賴憑證者」規定傳送予信賴憑證者；自發憑證公布於儲存庫供信賴憑證者下載。

2. 交互認證憑證機構之私密金鑰依 6.3.2 節「公開金鑰及私密金鑰之使用期限」規定定期更換，交互認證憑證機構更換金鑰並申請憑證時，依 4.1 節「申請憑證」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

總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

1. 總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。

2. 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 總管理中心簽章金鑰遭破解之復原程序

總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 總管理中心安全設施之災害復原工作

1. 總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，優先回復總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 總管理中心簽章金鑰憑證被廢止之復原程序

總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 總管理中心之終止服務

1. 除無法通知者外，總管理中心於預定終止服務 3 個月前，應通知交互認證憑證機構，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 總管理中心金鑰對之產製

1. 總管理中心依 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，於總管理中心相關人員、行政機關電子憑證推行小組委員及合格稽核業者(Qualified Auditor)見證下進行，金鑰產製過程須錄影留存，並簽署金鑰啟用見證書(其中記載金鑰對之公開金鑰)。

4. 合格稽核業者應出具金鑰產製典禮見證報告，確認總管理中心金鑰產製過程依循其金鑰產製腳本與管控措施，確保金鑰對之完整性及機密性。

6.1.1.2 下屬憑證機構與交互認證憑證機構金鑰對之產製

1. 下屬憑證機構與交互認證憑證機構須依憑證政策規定自行產製金鑰對。

2. 總管理中心於簽發下屬憑證機構憑證與交互憑證時檢查憑證申請檔中之公開金鑰，確認該憑證機構公開金鑰之唯一性。

6.1.2 私密金鑰安全傳送予下屬憑證機構與交互認證憑證機構

不適用。

6.1.3 公開金鑰安全傳送予總管理中心

憑證機構申請憑證時，須以 PKCS#10 憑證申請檔之格式將公開金鑰安全傳送予總管理中心，總管理中心將依照 3.2.1 節「證明擁有私密金鑰之方式」規定，檢驗該憑證機構確實擁有相對應之私密金鑰。

6.1.4 總管理中心公開金鑰安全傳送予信賴憑證者

總管理中心公開金鑰或其自簽憑證(內含公開金鑰)之安全散布方式如下，可供信賴憑證者透過安全管道取得。

1. 總管理中心於遞交下屬憑證機構憑證或交互憑證時，一併將其自簽憑證或公開金鑰遞交予該憑證機構，該憑證機構再以符記儲存總管理中心自簽憑證或公開金鑰，並透過安全方式傳送予該憑證機構之用戶或信賴憑證者。

2. 於可信賴第三方所發行之軟體中存放總管理中心自簽憑證

3. 於大量發行之光碟中放置總管理中心自簽憑證。

4. 透過媒體公告總管理中心金鑰啟用見證書。

6.1.5 金鑰長度

1. 總管理中心使用金鑰長度為 4096 位元之 RSA 金鑰。

   (1) 第 1 代總管理中心

   - 現今僅使用 SHA-256 雜湊函數演算法簽發憑證。
   - 使用 SHA-1 與 SHA-256 雜湊函數演算法簽發憑證機構廢止清冊。其中，SHA-1 雜湊函數演算法之憑證機構廢止清冊提供至其使用 SHA-1 雜湊函數演算法簽發之所有憑證機構憑證效期到期或所有憑證機構不再提供憑證與憑證廢止清冊之簽發服務。

   (2) 第 1.5 代總管理中心起使用 SHA-256、SHA-384 或 SHA-512 雜湊函數演算法簽發憑證與憑證機構廢止清冊。

2. 下屬憑證機構與交互認證憑證機構依憑證政策之規定選擇適當之金鑰長度，總管理中心於簽發該憑證機構之憑證前，審查其金鑰長度之恰當性。

3. 若使用橢圓曲線密碼演算法(Elliptic Curve Cryptography, ECC)簽發憑證將使用符合 NIST P-256、P-384 或 P-521 之金鑰長度。

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. 總管理中心與下屬憑證機構之簽章用金鑰對採用 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. 交互認證憑證機構須依所選用之演算法進行適當之金鑰參數品質檢驗。

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

5. 未來若使用橢圓曲線密碼演算法簽發憑證，總管理中心將遵照 NIST SP800-56A Revision 3 之規定，確認所有使用 ECC Full Public Key Validation Routine 與 ECC Partial Public Key Validation Routine 之金鑰效期。

6.1.7 金鑰使用目的

1. 總管理中心自簽憑證相對應之私密金鑰，僅限用於簽發自簽憑證、自發憑證、下屬憑證機構憑證、交互憑證、線上憑證狀態協定回應伺服器憑證及憑證機構廢止清冊。

2. 第 2 代總管理中心起簽發之自簽憑證須含金鑰用途擴充欄位，其內容設定為 keyCertSign 與 cRLSign

3. 自發憑證之金鑰用途擴充欄位內容與被簽發之總管理中心自簽憑證之金鑰用途擴充欄位相同。

4. 下屬憑證機構憑證與交互憑證之金鑰用途擴充欄位設定為 keyCertSign 與 cRLSign。

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. 總管理中心使用通過 FIPS140-2 安全等級第 3 級認證之硬體密碼模組。

2. 下屬憑證機構與交互認證憑證機構須依憑證政策之規定選擇適當之密碼模組;總管理中心於簽發該憑證機構憑之憑證前，審查其密碼模組安全等級之恰當性。

6.2.2 金鑰分持多人控管

1. 總管理中心之金鑰分持多人控管採 m-out-of-n 方法，做為金鑰分持備份、啟動及回復之方式。

   (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) 總管理中心使用此方法做為金鑰啟動、停用、備份及回復之方式。

2. 保證等級第 3 級與第 4 級憑證之憑證機構須依憑證政策規定採用多人控管程序管理其簽章用私密金鑰；總管理中心於簽發該憑證機構之憑證前，審查其多人控管程序之恰當性。

6.2.3 私密金鑰託管

1. 總管理中心簽章用私密金鑰不可被託管。

2. 總管理中心不提供下屬憑證機構與交互認證憑證機構簽章用私密金鑰託管。

6.2.4 私密金鑰備份

1. 總管理中心採用 6.2.2 節「金鑰分持多人控管」之金鑰分持多人控管方法備份私密金鑰，並使用通過 FIPS 140-2 安全等級第 2 級認證(含以上)驗證之 IC 卡做為秘密分持之儲存媒體。

2. 下屬憑證機構與交互認證之憑證機構須依憑證政策之規定選擇適當之私密金鑰備份方法；總管理中心於簽發該憑證機構憑證之憑證前，審查其私密金鑰備份方法之恰當性。

3. 總管理中心不負責保管下屬憑證機構與交互認證憑證機構之私密金鑰備份。

6.2.5 私密金鑰歸檔

1. 總管理中心簽章用私密金鑰不可被歸檔，但相對應之公開金鑰依 5.5 節「紀錄歸檔之方法」規定，以憑證檔案格式進行歸檔。

2. 總管理中心不對下屬憑證機構與交互認證憑證機構簽章用私密金鑰進行歸檔。

6.2.6 私密金鑰及密碼模組間傳輸

1. 總管理中心於下列情況進行私密金鑰匯入或匯出密碼模組作業，其過程依 6.2.2 節「金鑰分持多人控管」規定辦理。

   (1) 金鑰產製。

   (2) 金鑰備份與回復。

   (3) 更換密碼模組。

2. 私密金鑰與密碼模組間傳輸需使用加密或金鑰分持等方式保護，確保私密金鑰不曾以明碼呈現。私密金鑰匯入完成後，將匯入過程產製之相關機密參數完全銷毀。

3. 下屬憑證機構與交互認證之憑證機構須依憑證政策之規定選擇適當之私密金鑰輸入方法；總管理中心於簽發該憑證機構之憑證前，審查其私密金鑰輸入方法之恰當性。

4. 若總管理中心發現下屬憑證機構或交互認證憑證機構私密金鑰洩漏給未授權人員或不屬於該憑證機構之組織等情形，總管理中心將廢止與該憑證機構私密金鑰相關之憑證。

6.2.7 私密金鑰儲存於密碼模組

1. 總管理中心之私密金鑰依 6.1.1 節「金鑰對產製」與 6.2.1 節「密碼模組標準及控管」規定儲存於密碼模組。

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

1. 總管理中心私密金鑰之啟動是由符合 6.2.2 節「金鑰分持多人控管」規定之多人控管 IC 卡組控制，不同用途之 IC 卡組分別由管理員與簽發員保管。

2. 下屬憑證機構與交互認證憑證機構須依憑證政策之規定選擇適當之私密金鑰啟動方式；總管理中心於簽發該憑證機構之憑證前，審查其私密金鑰啟動方式之恰當性。

6.2.9 私密金鑰之停用方式

1. 總管理中心私密金鑰未使用時皆保持於停用狀態。

2. 每次完成憑證與憑證機構廢止清冊之簽發及相關管理作業後，私密金鑰將採 6.2.2 節「金鑰分持多人控管」規定之方式進行停用。

3. 下屬憑證機構與交互認證憑證機構須依憑證政策之規定選擇適當之私密金鑰停用方式；總管理中心於簽發該憑證機構之憑證前，審查其私密金鑰停用方式之恰當性。

6.2.10 私密金鑰之銷毀方式

1. 總管理中心私密金鑰之銷毀說明如下：

   (1) 舊私密金鑰不再使用時，總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. 下屬憑證機構與交互認證憑證機構須依憑證政策之規定選擇適當之私密金鑰銷毀方式；總管理中心於簽發該憑證機構之憑證前，審查其私密金鑰銷毀方式之恰當性。

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

1. 下屬憑證機構與交互認證憑證機構須自行管理金鑰對。

2. 總管理中心不負責保管下屬憑證機構憑證與交互認證憑證機構之私密金鑰。

6.3.1 公開金鑰之歸檔

總管理中心依 5.5 節「紀錄歸檔之方法」規定進行其簽發憑證之歸檔，不另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 總管理中心公開金鑰與私密金鑰之使用期限

1. 總管理中心之金鑰對長度為 RSA 4096 位元。

(1) 公開金鑰或其自簽憑證之使用期限至多為 30 年。

(2) 私密金鑰之使用期限：

- 用於簽發下屬憑證機構憑證或交互憑證時，使用期限至多為 15 年。
- 用於簽發自發憑證時，使用期限不得超過公開金鑰或其自簽憑證之使用期限。
- 用於簽發憑證機構廢止清冊或線上憑證狀態協定回應伺服器憑證時，使用期限至總管理中心簽發之自發憑證、下屬憑證機構憑證及交互憑證效期到期為止。

2. 總管理中心自簽憑證效期應考量涵蓋與憑證之公開金鑰相對應之私密金鑰簽發的所有憑證效期到期為止。

3. 總管理中心新舊金鑰互簽之自發憑證之效期應至其舊金鑰簽發之自簽憑證效期到期為止。

6.3.2.2 下屬憑證機構與交互認證憑證機構公開金鑰及私密金鑰之使用期限

1. 下屬憑證機構與交互認證憑證機構之金鑰對長度至少為 RSA 2048 位元。

   (1) 公開金鑰或其自身憑證之使用期限至多為 20 年。

   (2) 私密金鑰之使用期限：

   - 用於簽發用戶憑證時，使用期限至多為 10 年。
   - 用於簽發憑證廢止清冊或線上憑證狀態協定回應伺服器憑證之用途則不在此限。

2. 下屬憑證機構憑證或交互憑證之效期不得超過總管理中心自簽憑證之效期。

6.4 啟動資料

6.4.1 啟動資料之產生及安裝

1. 總管理中心之啟動資料產生與安裝方式如下：

   (1) 由硬體密碼模組產生，再寫入至多人控管 IC 卡組中。

   (2) IC 卡中之啟動資料由硬體密碼模組內建之讀卡機直接存取，IC 卡之 PIN 碼於硬體密碼模組內建之鍵盤上輸入。

2. 下屬憑證機構與交互認證憑證機構須依憑證政策之規定選擇適當之啟動資料產生方式；總管理中心於簽發該憑證機構之憑證前，審查其啟動資料產生與安裝方式之恰當性。

6.4.2 啟動資料之保護

1. 總管理中心之啟動資料保護方式如下：

   (1) 由多人控管 IC 卡組保護，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 碼由保管人員負責保存，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，新任保管人員須重新設定新 PIN 碼。

2. 下屬憑證機構與交互認證憑證機構須依憑證政策之規定選擇適當之啟動資料保護方式；總管理中心於簽發該憑證機構之憑證前，審查其啟動資料保護方式之恰當性。

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

總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。
9. 有權簽發憑證之帳號均應使用多因子認證方式驗證身分。

6.5.2 電腦安全評等

總管理中心採用安全強度與 C2(TCSEC)、E2(ITSEC)或 EAL3(CC)等級相當之電腦作業系統，且系統及運作環境符合 WebTrust Principles and Criteria for Certification Authorities 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. 各項交付總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，每次使用時應檢驗軟體之完整性，且每個月至少執行 1 次軟體完整性驗證作業。

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

總管理中心每年至少進行 1 次現行金鑰被破解之風險評估作業。

6.7 網路安全控管措施

1. 總管理中心之主機不與外部網路連接。
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. 總管理中心簽發之憑證與憑證機構廢止清冊由總管理中心授權之人員採手動方式將其儲存於可攜式媒體，並複製至儲存庫主機中。
4. 總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。
5. 總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

為並確保下述時間之正確性，總管理中心定期依據受信賴之時間源進行系統校時，其系統校時作業可採自動或手動調整，且系統校時動作須可被稽核。

1. 憑證簽發時間。
2. 憑證廢止時間。

3. 憑證機構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

總管理中心之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

1. 總管理中心簽發之憑證遵照 ITU-T X.509、RFC 5280 及本基礎建設技術規範相關規定。

2. 總管理中心透過密碼學安全偽亂數生成器(Cryptographically Secure Pseudorandom Number Generator, CSPRNG)產生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

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

7.1.2 憑證擴充欄位

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

2. 自簽憑證、自發憑證、下屬憑證機構憑證以及交互憑證所使用之必要擴充欄位及其欄位關鍵性與內容皆詳述於「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」文件。

   (1) 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。

(2) 如須新增憑證擴充欄位，須修正「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」，新增此擴充欄位之關鍵性、處理方式及欄位值設定等資訊。

3. 總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總管理中心驗證之語意。

4. 總管理中心不提供用戶憑證之簽發作業，亦不執行 RFC 6962 所定義之預簽憑證(Pre-certificate)的簽發。

7.1.3 演算法物件識別碼

總管理中心使用之演算法物件識別碼(Object Identifier)如下。

類型	演算法	演算法物件識別碼
簽章	sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)}
	sha384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha384WithRSAEncryption(12)}
	sha512WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha512WithRSAEncryption(13)}
金鑰產製	rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) rsaEncryption(1)}

7.1.4 命名形式

1. 憑證之主體與簽發者欄位皆使用 X.500 之唯一識別名稱，其屬性型態遵照 ITU-T X.509 及 RFC5280 或最新版相關規定。

2. 自簽憑證之簽發者與主體欄位內容相同，自發憑證、下屬憑證機構憑證及交互憑證之簽發者欄位內容與簽發該憑證之總管理心自簽憑證之主體欄位內容相同。

3. 自民國 106 年 12 月 25 日起，總管理心自簽憑證主體唯一識別名稱包含 3 個屬性，分別為一般名稱(commonName)、組織名稱(organizationName)與國家代碼(countryName)，說明如下：

   (1) 一般名稱：可識別總管理中心之名稱，此名稱為此憑證的唯一識別碼，可作為與其他憑證區分之用。

   (2) 組織名稱：總管理中心所屬的正式組織名稱。

   (3) 國家代碼：總管理中心營業地點所在之國家，依 ISO 3166-1 國際標準之規範註記為「TW」。

4. 總管理中心藉由簽發自發憑證、下屬憑證機構憑證與交互憑證，表示其於憑證的簽發日期前已遵循憑證政策與/或本作業基準所闡述的程序來作驗證，確保所有記載於憑證之主體資訊之準確性。

7.1.5 命名限制

總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

1. 自簽憑證不含憑證政策擴充欄位。

2. 自發憑證、下屬憑證機構憑證或交互憑證，其憑證政策擴充欄位應包含憑證證策定義之憑證政策物件識別碼。

7.1.7 政策限制擴充欄位之使用

總管理中心簽發之下屬憑證機構憑證與交互憑證，必要時將使用政策限制擴充欄位。

7.1.8 政策限定元之語法及語意

總管理中心簽發之憑證不含政策限定元(Policy Qualifiers)。

7.1.9 關鍵憑證政策擴充欄位之語意處理

總管理中心簽發之憑證，其憑證政策擴充欄位依「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」之規定進行關鍵性與否之註記。

7.2 憑證機構廢止清冊格式剖繪

7.2.1 版本序號

總管理中心簽發遵照 RFC 5280 與 ITU-T 規範之 X.509 v2 憑證機構廢止清冊。

7.2.2 憑證機構廢止清冊與憑證機構廢止清冊條目擴充欄位

1. 憑證機構廢止清冊擴充欄位(crlExtensions)及憑證機構廢止清冊條目擴充欄位(crlEntryExtensions)依照 ITU-T X.509 及 RFC 5280 或其最新版之規定辦理。

2. 憑證機構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. 總管理中心提供符合 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總管理中心線上憑證狀態協定查詢服務之網址。

2. 總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：

   (1) 版本序號。

   (2) 待查詢憑證識別元，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. 總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(NextUpdate)
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擴充欄位包括線上憑證狀態協定伺服器之憑證機構金鑰識別元(Authority Key Identifier)。

3. 線上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。

8.稽核方法

8.1 稽核頻率或評估事項

1. 總管理中心每年執行 2 次內部稽核
2. 總管理中心每年接受 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. 總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. 總管理中心是否遵照本作業基準運作。

2. 本作業基準是否符合憑證政策之規定。

8.5 對於稽核結果之因應方式

1. 總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，總管理中心得採取必要措施。

8.6 稽核結果公開之範圍

1. 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，本管理中心應於查核區間結束後 3 個月內將最近 1 次外部稽核報告與管理聲明書公布於儲存庫，若延遲公布，應提供合格稽核業者簽署之解釋函。

2. 稽核結果以 WebTrust Principles and Criteria for Certification Authorities 認證標章之方式呈現於本管理中心網站首頁，點選認證標章後可閱覽外稽報告與管理聲明書。

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 其他服務之費用

暫不收費。

9.1.5 請求退費程序

不適用。

9.2 財務責任

總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. 總管理中心營運之私密金鑰與通行碼。
2. 總管理中心金鑰分持之相關資料。
3. 未經同意公開之憑證機構資料
4. 總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. 總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

總管理中心依電子簽章法、WebTrust Principles and Criteria for Certification Authorities 及個人資料保護法等規定，處理總管理中心之重要資訊。

9.4 個人資訊之隱私性

9.4.1 隱私保護計畫

1. 總管理中心於網站公告隱私權保護政策。

2. 總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 隱私資訊之種類

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 非隱私資訊之種類

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 保護隱私資訊之責任

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因調查或蒐集證據需要，須查詢重要資訊時，總管理中心依法辦理，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)，其智慧財產權皆屬總管理中心所有，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 憑證機構之職責與義務

9.6.1.1 總管理中心之職責與義務

1. 依憑證政策保證等級第 4 級規定與本作業基準運作。

2. 訂定下屬憑證機構憑證申請程序及憑證機構交互認證申請程序。

3. 執行憑證申請之識別及鑑別程序。

4. 簽發、公布、廢止憑證。

5. 簽發與公布憑證機構廢止清冊。

6. 簽發及提供線上憑證狀態協定查詢服務。

7. 產製及管理總管理中心之私密金鑰。

8. 執行總管理中心自簽憑證金鑰更換及自發憑證簽發。

9.6.1.2 下屬憑證機構及之職責與義務

1. 提供正確完整之資訊。

2. 遵守憑證政策及本作業基準相關規定。

3. 敘明所申請憑證之保證等級。

4. 安全產製其私密金鑰並避免遭受破解。

5. 妥善管理與使用私密金鑰

6. 總管理中心如因故無法正常運作時，下屬憑證機構應儘速尋求其他途徑完成與他人應為之法律行為，不得以總管理中心無法正常運作，作為抗辯他人之事由。

9.6.1.3 交互認證憑證機構之承諾與擔保

1. 提供正確完整之資訊。

2. 遵守憑證政策、本作業基準及交互認證協議之相關規定。

3. 敘明所申請憑證之保證等級。

4. 安全產製其私密金鑰並避免遭受破解。

5. 妥善管理與使用私密金鑰

6. 總管理中心如因故無法正常運作時，下屬憑證機構應儘速尋求其他途徑完成與他人應為之法律行為，不得以總管理中心無法正常運作，作為抗辯他人之事由。

9.6.2 註冊中心之職責與義務

總管理中心不設置註冊中心。

9.6.3 用戶之義務

總管理中心不簽發用戶憑證。

9.6.4 信賴憑證者之義務

1. 遵守本作業基準相關規定。

2. 透過 6.1.4 節「總管理中心公開金鑰安全傳送予信賴憑證者」規定所述之安全散布管道，取得總管理中心之公開金鑰或自簽憑證。

3. 正確檢驗憑證數位簽章、有效性及金鑰用途。

4. 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。

5. 總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，不得以總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 委外方式提供認證服務機構之義務

總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

憑證機構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總管理中心之事由，而造成之損害，由憑證機構或信賴憑證者自行負責，總管理中心不負任何法律責任。

9.8 責任限制

1. 總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，得提前公告於儲存庫並通知憑證機構。憑證機構或信賴憑證者不得以此作為要求總管理中心損害賠償之理由。

2. 憑證機構如有廢止憑證事由時，應依 4.9 節「憑證暫時停用與廢止」規定提出憑證廢止申請。廢止憑證申請核定後，總管理中心最遲於 10 個工作天內完成憑證廢止作業、簽發憑證機構廢止清冊與公告於儲存庫。

9.9 賠償

9.9.1 總管理中心之賠償責任

總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，由總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 下屬憑證機構與交互認證憑證機構之賠償責任

下屬憑證機構與交互認證憑證機構於下述情形造成直接損害時，總管理中心得依相關法律規定請求損害賠償：

1. 憑證機構於憑證申請時，提供虛假或欺詐之陳述，造成總管理中心簽發不正確之憑證機構憑證或交互認證憑證。

2. 憑證機構未妥善保管其私密金鑰，導致私密金鑰遭破解、揭露、修改或未經授權之使用。

3. 憑證機構違反電子簽章法、憑證政策、本作業基準或交互認證協議之規定。

4. 憑證機構違背總管理中心參與各作業系統、瀏覽器及軟體平台之根憑證計畫所簽署之協議，甚至影響總管理中心於上述應用軟體供應者已植入或即將申請植入之憑證機構信賴清單。

9.10 有效期限與終止

9.10.1 有效期限

本作業基準由電子簽章法主管機關核定並公告後生效，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，應公告於總管理中心網站與儲存庫。

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

總管理中心、下屬憑證機構、交互認證憑證機構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

總管理中心每年定期檢視並評估本作業基準是否需要修訂，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

本作業基準之修訂由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核定後公告。

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

憑證政策修訂或物件識別碼有變更時，本作業基準須配合修訂。

9.13 紛爭之處理程序

憑證機構與總管理中心如有爭議時，雙方應本誠信原則先進行協商，由總管理中心就憑證政策或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，主要成員包括總管理中心、下屬憑證機構、交互認證憑證機構及信賴憑證者。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，不可於未通知總管理中心下以任何形式轉讓予其他方。

9.16.3 可分割性

本作業基準之任何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

憑證機構或信賴憑證者違反本作業基準相關規定，致總管理中心遭受損害，如可歸責於憑證機構或憑證信賴者之故意或過失時，總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總管理中心所導致之損害事件，總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。

- **憑證問題報告(Certificate Problem Report)**：金鑰遭破解、憑證被誤用、或憑證遭偽造、破解、濫用或不當使用之投訴。

- **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。

- **憑證機構廢止清冊(Certification Authority Revocation List, CARL)**：可供信賴憑證者使用之已廢止憑證表列，該表列中記載由憑證機構簽發且在到期日前被廢止之憑證(主要包括自發憑證、下屬憑證機構憑證、或交互憑證)及廢止時間與原因等資訊，由憑證機構以數位簽章的方式確保其完整性與不可否認性。

- **憑證實務作業基準(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)。

- **國際電腦稽核師(Certified Information Systems Auditor, CISA)**：國際電腦稽核協會(Information Systems Audit and Control Association, ISACA)於 1978 年推出之稽核認證，其以資訊系統的觀點檢視營運流程，為現今電腦稽核、控管、確認與安全等專業領域之資格標準。需通過國際電腦稽核協會之考試並滿足維持證照有效性之要求始可獲證。

- **資訊技術安全評估共同準則(Common Criteria for Information Technology Security Evaluation)**：簡稱為「共同準則」(Common Criteria, CC)，為美國、英國、德國、法國及

加拿大等國家所制訂之資安產品評估及驗證規範，於 1999 年 8 月正式成為 ISO 國際標準(ISO/IEC 15408)，其經過標準評估的產品可獲得「評估保證等級」(Evaluation Assurance Level, EAL)，用於說明該產品安全規範檢測之結果與界定之安全等級，可分為 7 個安全評估等級，最低等級為 EAL 1，最高等級為 EAL 7，為現今多數國家認定之經第三方實驗室驗證、最高層級的 IT 產品安全性認證，可作為資訊產品使用者採購及使用的依據。

- **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。

- **交互認證(Cross-Certification)**：由一個公開金鑰基礎建設下的憑證機構簽發公開金鑰憑證給另一個公開金鑰基礎建設下的憑證機構之行為或程序。

- **交互認證協議(Cross Certification Agreement, CCA)**：總管理中心與下屬憑s證機構就下屬憑證機構申請加入GPKI所須遵守之事項與個別責任義務歸屬協議。

- **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。

- **密碼學安全偽亂數生成器(Cryptographically Secure Pseudorandom Number Generator, CSPRNG)**：用於加密系

統之亂數生成器。

◆ **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**

- **資訊技術安全評估準則(Information Technology Security Evaluation Criteria, ITSEC)**：於 1991 年由英、法、德、荷等歐洲國家提出，為歐洲安全評估準則，其定義了 7 種安全評估等級，分別為 E0 至 E6。與可信賴電腦系統安全評估準則不同，其僅說明技術安全之要求，將機密性作為安全增強功能，同時，強調對資訊安全之機密性、完整性及可用性的重要性。

- **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)。

- **線上憑證狀態協定回應伺服器(Online Certificate Status Protocol Responder, OCSP Responder)**：由憑證管理中心授權維運之線上伺服器，其連接至儲存庫，以處理憑證狀態查詢請求。

- **線上憑證狀態協定裝訂(OCSP Stapling)**
  - 一種 TLS/SSL 憑證狀態請求擴充欄位，可替代線上憑證狀態協定成為另一種檢查 X.509 憑證狀態的方法。其運作機制如下：

- ✓ 網站向線上憑證狀態協定回應伺服器取得具有「時間限制」之線上憑證狀態協定回應訊息，並暫存之。
- ✓ 於每次 TLS 連線初始過程中，網站將此暫存之線上憑證狀態協定回應訊息傳送給用戶(通常為瀏覽器)，用戶僅需驗證該回應訊息之有效性，無需向憑證機構發送線上憑證狀態協定查詢封包。

- 此機制可透過網站轉發線上憑證狀態協定回應伺服器定期簽發之 TLS/SSL 憑證有效性訊息，減少用戶向憑證機構查詢 TLS/SSL 憑證狀態之頻率，減輕憑證機構之負擔。

- **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名稱控制權外，並且依照憑證的保證等級識別與鑑別用戶之組織或個人身分。故連結安裝組織驗證型 SSL 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與公鑰憑

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與鑑別，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)及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)。

- 包含本憑證政策與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

- **自發憑證(Self-Issued Certificate)**：自發憑證為根憑證機構更換金鑰或憑證政策需要時所簽發之憑證，由兩代根憑證機構使用其私密金鑰相互簽發，用以建立新舊金鑰間或憑證政策互通憑證信賴路徑之用。

- **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。

- **安全插座層(Secure Sockets Layer, SSL)**：由網景公司(Netscape)所設計，主要用於全球資訊網(Web)之安全通訊協定，其可於傳輸層進行網路通信之加密，確保傳送之資料完整性，並可對伺服器端與用戶端進行身分驗證。其應用獨立於應用層協定，故應用層通訊前，即可透過此安全通訊協定完成加密演算、通信密鑰之協商及伺服器認證作業。現今最新版本為 SSL 3.0，其於 2014 年 10 月經 Google 發現設計缺陷並建議禁用，現多改採用 TLS 1.3 版安全通訊協定。

◆ **T**

- **傳輸層安全(Transport Layer Security, TLS)**：為一種安全通訊協定，1999 年網際網路工程任務小組將 SSL 進行標準化，公告第一版 TLS 標準(即為 RFC 2246)，隨後陸續公布 RFC 4346、RFC 5246 與 RFC 6176 等更新版本，分別說明 TLS 1.1 與 TLS 1.2 版，現今最新版本為 2018 年網際網路工程任務小組公告之 RFC 8446，即為 TLS 1.3，其移除許多過時或不安全的功能(包括 MD5 與 SHA-224 加密功能)，新增對 ChaCha20、Poly1305、Ed25519、Ed448 、x25519 及 x448 之支援，同時，支援 1-RTT、0-RTT，以減少伺服器端與用戶端連結之延遲時間。

- **信賴起源(Trust Anchor)**：信賴路徑之起始憑證，為信賴憑證者所信賴，且經由安全可靠之傳送方式取得，又稱為信賴起點。

- **可信賴電腦系統安全評估準則(Trusted Computer System Evaluation Criteria,TCSEC)**：為電腦系統安全評估的第一個正式標準，於 1970 年由美國國防科學委員會提出，1985 年由美國國防部公布，其將電腦系統之安全劃分為四個等級與七種安全等級，主要著重於作業系統的安全性，非強調系統之整體性。

- **可信賴系統(Trustworthy System)**：具有下列性質之電腦硬體、軟體及程序：
  - 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(Zeroization)**：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
CARL	Certification Authority Revocation List
CC	Common Criteria for Information Technology Security Evaluation
CISA	Certified Information Systems Auditor
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSPRNG	Cryptographically Secure Pseudorandom Number Generator
DN	Distinguished Name
EE	End Entities
FIPS	(US Government) Federal Information Processing Standard
IETF	Internet Engineering Task Force
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standard
PKI	Public Key Infrastructure
RA	Registration Authority
RFC	Request for Comments
SSL	Security Sockets Layer
TCSEC	Trusted Computer System Evaluation Criteria

縮寫	全稱
TLS	Transport Layer Security