政府機關公開金鑰基礎建設

憑證政策

(Certificate Policy for the Government Public Key Infrastructure)

第 2.0.3 版

主辦機關：數位發展部

執行機構：中華電信股份有限公司企業客戶分公司

中華民國 115 年 06 月 01 日

政府公開金鑰基礎建設憑證政策版本修訂歷程

版本	生效日期	修訂內容說明
Ver1.0	91/04/18	初版發行
Ver1.1	92/01/09	將憑證格式詳細內容另外以憑證格式剖繪中說明
Ver1.2	94/07/28	1. 定義 GPKI CP 之管理機構 2. 定義憑證機構之 CPS 是否符合 GPKI CP 之審查流程
Ver1.3	96/08/01	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	97/03/12	新增憑證展期相關規範
Ver1.5	97/12/31	修訂歸檔紀錄資料中應被歸檔資料之內容
Ver1.6	101/09/07	1. 更改 IETF RFC 3280 為 RFC 5280 2. 新增 GRCA 更換金鑰新簽發自發憑證的程序及 2 張自發憑證的簽發方法 3. 修訂憑證機構金鑰更換時的公告及作法 4. 新增說明憑證中心私密金鑰之安全管理方式 5. 新增 SHA-2 演算法之物件識別碼及改用 SHA-2 演算法之期限 6. 調整各金鑰長度下金鑰使用之年限
Ver1.7	102/01/31	新增政府機關(構)、單位憑證屆期後，可依人事行政總處之資料做為身份鑑別之依據進行憑證申請
Ver1.8	106/01/06	新增修訂組織身分鑑別程序
Ver1.9	106/07/10	1. 新增說明簽發 SSL 憑證之憑證機構另須遵循 CA/Browser Forum 發行之 Baseline Requirements 之規範 2. 新增緊急事件與系統遭破解之處理程序
Ver2.0	107/08/13	更版為 RFC3647 架構
Ver2.0.1	110/12/21	1. 調整憑證適用之符記範圍，新增行動裝置載具 2. 將文中部分「認證」用詞修改為「驗證」 3. 調整憑證管理中心使用之硬體設備範圍，增列虛擬主機
Ver2.0.2	112/10/13	1. 配合 GPKI 憑證相關業務由國家發展委員會移轉至數位發展部，將文件中「國家發展委員會」更改為「數位發展部」，「國發會」更改為「數位部」 2. 調整執行機構「中華電信股份有限公司數據通信分公司」更名為「中華電信股份有限公司企業客戶分公司」 3. 修訂 1.2 節，依此次改版，調整版本資訊、公告日期。 4. 刪除有關遵循 CA/Browser Forum 制定之 Baseline Requirements 相關敘述。 5. 依據電子憑證推行小組委員及經濟部審查委員建議，調整多處內容。
Ver2.0.3	115/06/01	1. 因應量子計算所帶來之安全風險，增訂支援後量子密碼學(Post-Quantum Cryptography, PQC)之規範，並微調現有 RSA 金鑰使用規定，修訂章節包含 6.1.5、6.3.2.1、6.3.2.2 及 7.1.3 節。

		2. 依照 RFC 3647 框架，刪除原 1.4.2、3.1.7、3.2.7、3.3.3、5.7.5 及 6.9 節。 3. 其餘文字修訂章節包含 1、1.1.3、1.2、1.4.2、1.5.1、1.5.4、2.2、3.1.2、3.2.1、3.2.5、3.3.2、4.2、4.2.1、4.7.3、5.3.1、5.4.8、5.7.4、6.1.1、6.1.6、6.2.1、7.3.1、7.3.2、8、8.1、8.2、8.5、9.5、9.10、9.10.1、9.10.2 節及附錄 1。

目　　錄

1 簡介

為健全電子化政府基礎建設環境，我國於民國 94 年依據 ITU-T X.509 標準建立政府機關公開金鑰基礎建設(Government Public Key Infrastructure，以下簡稱 GPKI)，GPKI 係由信賴起源(Trust Anchor)－政府憑證總管理中心(Government Root Certification Authority，以下簡稱總管理中心)及政府機關設立之下屬憑證機構(Subordinate Certification Authority)所組成。加入 GPKI 之憑證機構(Certification Authority) 須為政府機關，其所簽發之憑證(Certificate)可應用於網路服務各項應用。

數位發展部(以下簡稱數發部)為 GPKI 之主責機關，並設有「行政機關電子憑證推行小組」(Government Electronic Certification Steering Committee)提供政策諮詢。為提供 GPKI 憑證管理之共同規範，並促進對內及對外之互通性，特訂定「政府機關公開金鑰基礎建設憑證政策」(Certificate Policy for the Government Public Key Infrastructure，以下簡稱本憑證政策)。

1.1 總覽

1.1.1 憑證政策

本憑證政策係依電子簽章法規定及參考國際標準所訂定，作為各憑證機構訂定憑證實務作業基準(Certification Practice Statement)之依循。為確保公開金鑰憑證之互通性，加入 GPKI 之憑證機構均應遵循本憑證政策。

本憑證政策共定義 5 種保證等級(Assurance Level)，依序為測試級、第 1 級、第 2 級、第 3 級及第 4 級，等級數字越大者，其保證等

級越高。其中測試級僅適用於測試憑證。

GPKI 共註冊 5 個保證等級之憑證政策物件識別碼(Certificate Policy Object Identifier，詳參 1.2 節)，憑證機構於簽發憑證時，可選擇適當之憑證政策物件識別碼，記載於憑證之憑證政策擴充欄位，信賴憑證者(Relying Party)可透過該物件識別碼(Object Identifier)確認憑證適用範圍。

憑證機構須於交互憑證(Cross-Certificate)之憑證政策對應擴充欄位標示憑證政策物件識別碼，信賴憑證者(其定義請參閱 1.3.5 節「信賴憑證者」)可透過該物件識別碼，確認簽發憑證機構(Issuing Certification Authority)與主體憑證機構(Subject Certification Authority)間之憑證政策對應關係。

1.1.2 憑證政策及憑證實務作業基準關係

憑證機構須於憑證實務作業基準中，說明符合本憑證政策保證等級之方法。

1.1.3 憑證機構引用憑證政策物件識別碼

憑證機構引用本憑證政策之憑證政策物件識別碼時須經數發部同意。未經同意引用所衍生之任何問題，一律由該憑證機構自行負責。

憑證機構應依所簽發憑證之適用範圍，選擇適當之憑證政策物件識別碼，並記載於憑證政策擴充欄位中，總管理中心自簽憑證(Self-Signed Certificate)僅作為信賴起源之資訊物件，無須標示憑證政策物件識別碼。信賴憑證者可直接信賴該自簽憑證所記載之公開金鑰資訊。

1.2 文件名稱及識別

(1) 名稱：政府機關公開金鑰基礎建設憑證政策

(2) 版本：2.0.3

(3) 公布日期：115 年 06 月 01 日

本憑證政策定義5個保證等級之憑證政策物件識別碼(詳表 1-1)，註冊於 id-tw-gpki 分支，其物件識別碼說明如下：

id-tw OBJECT IDENTIFIER ::= {2 16 886}

id-tw-gov OBJECT IDENTIFIER ::= {id-tw 101}

id-tw-gpki OBJECT IDENTIFIER ::= {id-tw-gov 0}

id-tw-gpki –certpolicy OBJECT IDENTIFIER ::= {id-tw-gkpi 3}

表 1-1 憑證政策物件識別碼

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

1.3 主要成員

1.3.1 行政機關電子憑證推行小組

行政機關電子憑證推行小組工作任務說明如下：

(1) 審議行政機關電子憑證政策及憑證實務作業基準。

(2) 審議行政機關電子憑證相關技術規範。

(3) 研議行政機關電子憑證體系架構。

(4) 其他行政機關電子憑證管理事項。

1.3.2 憑證機構

1.3.2.1 政府憑證總管理中心

總管理中心為 GPKI 根憑證機構(Root Certification Authority)，以保證等級第 4 級運作，任務說明如下：

(1) 負責自簽憑證、自發憑證(Self-Issued Certificate)、交互憑證及下屬憑證機構憑證之簽發及管理。

(2) 訂定 GPKI 交互認證(Cross-Certification)程序，簽發及管理 GPKI 第 1 層下屬憑證機構憑證、GPKI 外之其他憑證機構憑證。

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

1.3.2.2 下屬憑證機構

下屬憑證機構之任務說明如下：

(1) 負責簽發及管理用戶憑證。

(2) 必要時依階層式公開金鑰基礎建設(Public Key Infrastructure)之建構方式簽發憑證予下屬憑證機構，下屬憑證機構不可直接與 GPKI 外之憑證機構進行交互認證。

(3) 下屬憑證機構應依本憑證政策相關規定進行建置，並設置聯絡窗口。

1.3.3 註冊中心

(1) 註冊中心(Registration Authority)負責蒐集及驗證用戶(Subscriber)身分及相關資料之正確性。

(2) 總管理中心應自行擔任註冊中心角色；下屬憑證機構可另設立註冊中心。

(3) 憑證機構需於憑證實務作業基準中說明註冊中心之運作方式。

1.3.4 用戶

(1) 指憑證主體名稱所識別之個體，該個體擁有與憑證公開金鑰(Public Key)相對應之私密金鑰(Private Key)。

(2) 對簽發予無行為能力之應用程式及硬體設備等類別憑證而言，憑證用戶係指申請憑證之個人或組織。

(3) 交互憑證主體名稱所識別之憑證機構，稱之為主體憑證機構，而非用戶。

1.3.5 信賴憑證者

指相信憑證主體名稱與該主體公開金鑰及私密金鑰連結關係之個人或組織。

1.3.6 其他相關成員

憑證機構得委託其他機構(如金鑰管理中心、發卡中心等)協助處理憑證作業相關事宜，惟應於憑證實務作業基準說明受託之機構身分，並訂定作業程序、管理方式及責任義務。

1.4 憑證用途

信賴憑證者應審慎評估各項風險，選擇適用之憑證。

1.4.1 憑證適用範圍

本憑證政策未強制規定各保證等級之憑證適用範圍及適用對象。惟為使各憑證機構有所依循，各保證等級之適用範圍建議如下表所示：

表 1-2 保證等級適用範圍

保證等級	適用範圍
測試級	僅供測試用，對傳送之資料不負任何法律責任。
第 1 級	適用於惡意篡改之威脅性很低之網路環境，或於無法提供較高保證等級時，作為識別用戶個體名稱及保證被簽署文件之完整性。
第 2 級	適用於資訊可能被篡改，惟無惡意篡改之網路環境(資訊可能被截取之機率不高)。
第 3 級	適用於有惡意使用者截取或篡改資訊、較第 2 級危險之網路環境，傳送之資訊包括電子交易等。
第 4 級	適合應用於潛在威脅很高或資訊被篡改後復原的代價很高之網路環境，傳送的資訊包括高金額的電子交易或極敏感的文件等。

用戶憑證使用之符記可為晶片 IC 卡、硬體密碼模組或用戶可信賴之行動裝置等載具，本憑證政策提供 3 種符記驗證保證等級(Authenticator Assurance Level, AAL)供各憑證機構及憑證信賴者有所依循，符記驗證保證等級說明如下表所示：

表 1-3 符記驗證保證等級說明

符記驗證保證等級	說明
第 1 級	對符記控管者是否確實綁定用戶帳號僅提供部分保證，其使用任何可取得的驗證技術來進行單因子或多因子驗證，成功的驗證須可透過一個安全驗證協定來確認該用戶確實擁有且控管該符記。 (1) 允許的符記驗證類型如下： ■ 記憶型秘密：例如：密碼或個人識別碼 ■ 單因子加密軟體 ■ 單因子加密設備 ■ 多因子加密軟體 ■ 多因子加密設備 (2) 符記與驗證器的需求： ■ 加密符記應使用經認可的加密技術，軟體符記可嘗試偵測該終端設備是否有惡意攻擊的可能性(例如有安裝惡意軟體)，若發現時，則終止該驗證作業。 ■ 符記擁有者與驗證器應透過授權且安全加密的管道進行溝通，以避免中間人攻擊。
第 2 級	對符記控管者是否確實綁定用戶帳號提供高信賴度的保證，其須於安全驗證協定的環境下使用兩種驗證因子來進行驗證，其驗證方式應包含經核准的加密技術。 (1) 允許的符記驗證類型：驗證作業應透過多因子驗證或結合兩種單因子驗證。 ■ 當採用多因子驗證時，可使用的符記驗證類型包括： ➢ 多因子加密軟體 ➢ 多因子加密設備 ■ 當採用結合兩種單因子驗證時，則應包含一種

	記憶型秘密驗證，以及下述任一種一次性的驗證： ➢ 單因子加密軟體 ➢ 單因子加密設備 (2) 符記與驗證器的需求： ■ 加密符記應使用經認可的加密技術，政府機關採購的符記應通過 FIPS 140 Level 1 認證，軟體符記亦可嘗試偵測該終端設備是否有惡意攻擊的可能性(例如有安裝惡意軟體)，若發現時，則終止該驗證作業。此外，至少應使用一種具備防止重送攻擊能力之符記，例如動態密碼。 ■ 符記擁有者與驗證器應透過授權且安全加密的管道進行溝通，以避免中間人攻擊。 ■ 若驗證過程中使用如行動裝置等設備時，則該設備原有的解鎖功能(例如：指紋辨識或個人識別碼驗證)不可視為一種驗證因子。
第 3 級	對符記控管者是否確實綁定用戶帳號提供非常高度的信賴保證，其須透過加密協定來驗證用戶金鑰的擁有權，驗證作業應使用硬體符記，且具備防止驗證器被冒充之功能(亦可使用同時具備前述功能的設備)，且於安全驗證協定的環境下使用兩種驗證因子來進行驗證。其驗證方式應包含經核准的加密技術。 (1) 允許的符記驗證類型：可使用下述任一種符記驗證之組合。 ■ 多因子加密設備 ■ 單因子加密設備與記憶型秘密的結合 (2) 符記與驗證器的需求： ■ 符記擁有者與驗證器應透過授權且安全加密的管道進行溝通，以避免中間人攻擊。所有加密設備符記應具備防止驗證器被冒充與重送攻擊之能力。 ■ 符記應為通過 FIPS 140 Level 2(含)以上或符合 Global Platform Trusted Execution Environment 的

	密碼模組。 ■ 若驗證過程中使用如行動裝置等設備時，則該設備原有的解鎖功能(例如：指紋辨識或個人識別碼驗證)不可視為一種驗證因子。

1.4.2 憑證之禁止事項

GPKI 憑證機構所簽發之憑證，禁止使用於下列範圍：

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

(2) 電子簽章法、其他相關法令或各目的事業主管機關明訂禁止或排除之應用或業務。

(3) 其他：由各下屬憑證機構自行規範

1.5 聯絡方式

1.5.1 憑證政策之制訂及管理機構

本憑證政策之制訂及管理機構為數發部。

1.5.2 聯絡資料

如對本憑證政策有任何建議，參考網站 https://grca.nat.gov.tw/。

1.5.3 憑證實務作業基準之審定

憑證機構欲對外提供憑證簽發服務，應符合下列程序：

(1) 憑證機構應檢查憑證實務作業基準是否符合本憑證政策相關規定，經行政機關電子憑證推行小組審查核定。

(2) 憑證實務作業基準送電子簽章法主管機關核定。

1.5.4 憑證政策及憑證實務作業基準核准程序

本憑證政策如有修訂應經行政機關電子憑證推行小組審查後由總管理中心公布。本憑證政策修訂生效並公布後，憑證實務作業基準應配合修訂，並依 1.5.3 節審定程序辦理。

1.6 名詞定義及縮寫

詳參附錄 1「名詞解釋」。

2 資訊公布及儲存庫責任

2.1 儲存庫

各憑證機構至少需提供 1 個網際網路可存取之儲存庫，及確保儲存庫之可用性、存取控制及資料完整性，並於憑證實務作業基準敘明儲存庫之網址；儲存庫之存取控制須依 2.4 節「存取控制」規定辦理。

2.2 憑證資訊公布

憑證機構應在儲存庫公布內容如下：

(1) 簽發之憑證、憑證廢止清冊及其他憑證相關資訊。

(2) 憑證政策及憑證實務作業基準。

(3) 最新外部稽核結果。

(4) 隱私權保護政策。

2.3 公布頻率或時間

(1) 憑證機構廢止清冊或憑證廢止清冊之公布頻率應依 4.9 節「憑證暫時停用及廢止」規定辦理。

(2) 憑證機構應於憑證實務作業基準敘明其作業基準公布頻率或時間。

(3) 總管理中心應於憑證政策修訂內容核准後 7 個日曆天內，於儲存庫中公告。

2.4 存取控制

(1) 憑證機構可決定憑證之存取控制方式。

(2) 憑證機構應保護儲存庫之資訊，以防止遭未授權的篡改。

3 識別及鑑別程序

3.1 命名

GPKI 憑證之命名包括主體名稱及主體別名。

3.1.1 命名種類

(1) 憑證主體名稱應為 X.500 唯一識別名稱。

(2) 用戶申請憑證提出主體別名時，憑證機構具有准駁寫入憑證之權利；憑證中寫入憑證主體別名時，該欄位須標示為非關鍵性擴充欄位。

3.1.2 命名須有意義

(1) 組織及個人之憑證主體名稱須符合我國相關法令規定，並使用正式登記之名稱。

(2) 設備或伺服器應用軟體之憑證主體名稱須為該設備或伺服器應用軟體管理單位之名稱，其名稱應易於瞭解及辨識。

(3) 伺服器應用軟體憑證之主體名稱與主體別名，不得使用保留 IP 位址。

3.1.3 用戶匿名或假名

憑證機構得依需求決定是否允許用戶使用匿名、別名或假名，本憑證政策於此不另行規定。

3.1.4 命名形式之解釋規則

命名格式應於「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」中訂定，並經行政機關電子憑證推行小組審核後頒布。

3.1.5 命名獨特性

對同名之憑證主體，憑證機構應於憑證實務作業基準中敘明使用 X.500 唯一識別方式，以確保獨特性 。

3.1.6 商標之辨識、鑑別及角色

包含商標之憑證主體名稱命名方式須符合我國商標法相關規定。

3.2 初始註冊

3.2.1 證明擁有私密金鑰之方式

用戶申請憑證時，憑證機構應驗證申請者(Applicant)擁有之私密金鑰與公開金鑰是否成對。

本憑證政策認可證明擁有私密金鑰之方式如下：

(1) 憑證機構或註冊中心為用戶產製金鑰對(Key Pair)

用戶不須證明擁有私密金鑰，惟須依 3.2 節「初始註冊」所規定之身分鑑別程序辦理，憑證機構應依 6.1.2 節「私密金鑰安全傳送予用戶」規定，將私密金鑰傳送予用戶。

(2) 可信賴之第三方為用戶產製金鑰對

憑證機構或註冊中心須依 6.1.3 節「公開金鑰安全傳送予憑證機構」規定，透過安全管道向該第三方取得用戶之公開金鑰，用戶不須證明擁有對應之私密金鑰，惟須依 3.2 節「初始註冊」所規定之身分鑑別程序辦理，憑證機構應依 6.1.2 節「私密金鑰安全傳送予用戶」規定，將私密金鑰傳送予用戶。

(3) 用戶自行產製金鑰對

用戶使用私密金鑰產生簽章，並依 6.1.3 節「公開金鑰安全傳送予憑證機構」規定，將該簽章提供憑證機構或註冊中心，憑證機構或註冊中心使用用戶之公開金鑰驗證該簽章或數發部認可之方式，以證明用戶擁有該私密金鑰。

3.2.2 組織身分之鑑別程序

組織身分鑑別依其憑證適用之保證等級採不同程序，各等級之鑑別程序詳如表 3-1 所示。

對憑證機構之識別與鑑別程序，應依表 3-1 進行識別與鑑別程序，且不得低於憑證機構所欲簽發憑證之保證等級。

總管理中心對下屬憑證機構之身分鑑別，應依保證等級第 3 級之規定辦理。

表 3-1 組織身分鑑別程序

保證等級	組織身分鑑別之程序
測試級	憑證機構得自行決定其組織身分鑑別之程序，本憑證政策於此不另行規定。
第 1 級	(1) 可不進行核對書面證件作業。 (2) 申請者提供個人之電子郵件地址即可申請憑證。
第 2 級	(1) 可不進行核對書面證件作業。 (2) 用戶須提交組織資料，包括組織識別碼及組織名稱等，並應與憑證機構認可之資料進行比對。
第 3 級	(1) 公務機關之身分鑑別 ■ 首次申請憑證時，須以正式公文書申請，並經審驗通過。

保證等級	組織身分鑑別之程序
	■ 公務機關憑證使用期限屆期者，憑證機構或註冊中心應確認該機關(構)存在後核發新憑證，其身分鑑別方式應敘明於憑證實務作業基準中。 ■ 公務機關若留有識別與鑑別等資料（例如：可驗證之公開金鑰），憑證機構或註冊中心得允許用戶於申請憑證時以該佐證資料做為已完成識別與鑑別之依據。 (2) 民間組織之身分鑑別 民間組織申請憑證所需驗證之資料應包括組織名稱、所在地及代表人等足以識別該組織之資料。憑證機構或註冊中心除須驗證申請資料及代表人身分之真實性外，並應驗證該代表人已獲授權申請憑證，身分鑑別方式可有以下做法： ■ 申請時應由代表人或以書面委任代理人親臨憑證機構或註冊中心辦理，憑證機構或註冊中心須確認該委託書之真偽，並依 3.2.3 節「個人身分鑑別程序」之保證等級第 3 級規定鑑別代理人之身分。 ■ 民間組織如已依法完成設立登記程序，並留有登記、識別與鑑別等資料（例如：設立登記證明、可驗證之公開金鑰），憑證機構或註冊中心得允許用戶於申請憑證時以該佐證資料做為已完成識別與鑑別之依據，無須臨櫃辦理。 ■ 組織代表人已依 3.2.3 節「個人身分鑑別程序」之保證等級第 3 級規定鑑別身分時，組織代表人得持其自然人憑證線上提出憑證申請，並提出佐證資料進行鑑別。
第 4 級	(1) 公務機關之身分鑑別 公務機關須以正式公文書指派授權代表人親臨申請憑證，並依 3.2.3 節「個人身分鑑別程序」之保證等級第 4 級規定，鑑別該代表人身分。 (2) 民間組織之身分鑑別 申請憑證需親臨且檢附包括組織名稱、所在地及代

保證等級	組織身分鑑別之程序
	表人等足以識別該組織之資料。憑證機構或註冊中心除須驗證申請資料及代表人身分之真實性外，並應驗證該代表人已獲授權申請憑證。

3.2.3 個人身分之鑑別程序

個人身分鑑別依其憑證適用之保證等級採不同之鑑別程序，詳如表 3-2 所示。

表 3-2 個人身分鑑別程序

保證等級	個人身分鑑別程序
測試級	憑證機構得自行決定其個人身分鑑別之程序，本憑證政策於此不另行規定。
第 1 級	用戶提供自己之電子郵件地址，即可申請憑證。
第 2 級	用戶須提供身分證字號、姓名等個人資料，並經審核通過。
第 3 級	(1) 用戶須提供身分證字號、姓名及具照片之個人身分證件正本或由政府發給足以證明用戶身分之書面文件，採臨櫃或以書面委任代理人臨櫃申請。 (2) 用戶申請或廢止憑證需本人親自辦理。 (3) 憑證機構或註冊中心須驗證申請資料之真實性，並應與該資料主管機關登記資料或經主管機關認可之可信賴第三方登記資料進行比對。 用戶如已向憑證機構、註冊中心、憑證機構信賴之機構，完成符合上述規定之臨櫃識別與鑑別程序，並留有識別與鑑別之佐證資料（例如：生物識別資料、可驗證之公開金鑰、其他具公信力之佐證資料），憑證機構或註冊中心得允許該用戶於申請憑證時，以該佐證資料做為已完成識別與鑑別之依據。
第 4 級	其身分鑑別程序同第三級，惟用戶須親臨辦理。

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

憑證機構應於憑證實務作業基準中敘明申辦者已被授權可代表憑證主體之作法，驗證方式應符合以下原則：

(1) 透過第三方身分驗證服務、資料庫、政府機關或有權責及公信力團體之文書，證明該組織確實存在。

(2) 透過親臨、電話、紙本郵件或電子郵件等管道，確認該個人確實任職於該憑證主體，並獲授權代表該憑證主體。

憑證主體別名欄位記載電子郵件位址並用於安全電子郵件應用時，憑證機構應於憑證實務作業基準中敘明驗證申請者可控制該電子郵件帳號之方式。

憑證機構若提供 TLS 憑證申請，應於憑證實務作業基準中敘明確認網域控制權授權之方式。

3.2.6 交互運作標準

憑證機構得視需求自行定義交互運作之標準，本憑證政策於此不另行規定。

3.3 金鑰更換請求之識別及鑑別

主體憑證機構申請更換金鑰對時，簽發之憑證機構應依3.2節「初始註冊」進行主體憑證機構之識別及鑑別作業。

當終端個體(End Entity)之用戶申請更換金鑰對時，憑證機構應依表3-3規定進行用戶之識別與鑑別作業。

表3-3憑證金鑰更換之身分鑑別規定

保證等級	用戶憑證更換金鑰之身分鑑別規定
測試級	憑證機構得自行決定用戶憑證更換金鑰之身分鑑別規定，本憑證政策於此不另行規定。
第1級	用戶身分可使用有效之簽章金鑰進行鑑別，或依3.2節「初始註冊」進行鑑別作業。
第2級	(1) 用戶身分可使用有效之簽章金鑰進行鑑別，或依 3.2 節「初始註冊」之身分鑑別程序辦理。 (2) 如與初始註冊時間間隔超過 15 年時，則須依 3.2 節「初始註冊」之身分鑑別程序重新辦理。
第3級	(1) 用戶身分可使用有效之簽章金鑰進行鑑別，或依 3.2 節「初始註冊」之身分鑑別程序辦理。 (2) 如與初始註冊時間間隔超過 9 年時，則須依 3.2 節「初始註冊」之身分鑑別程序重新辦理。
第4級	(1) 用戶身分可使用有效之簽章金鑰進行鑑別，或依 3.2 節「初始註冊」之身分鑑別程序辦理。 (2) 惟如與初始註冊時間間隔超過 3 年時，則須依 3.2 節「初始註冊」之身分鑑別程序重新辦理。

3.3.1 例行性金鑰更換識別及鑑別

當憑證機構進行例行性金鑰更換時，簽發之憑證機構應依3.2節「初始註冊」規定，對憑證機構進行識別及鑑別作業。

當終端個體之用戶進行例行性金鑰更換時，憑證機構應依3.3節表3-3規定進行用戶之識別與鑑別作業。

3.3.2 憑證廢止後金鑰更換之識別及鑑別

用戶於憑證廢止後，申請新憑證之簽發時，應依3.2節「初始註冊」程序規定重新辦理。

3.4 憑證廢止申請之識別及鑑別

(1) 憑證機構或註冊中心須對憑證廢止申請進行鑑別，並依 4.9 節「憑證暫時停用及廢止」規定辦理。

(2) 憑證機構應於憑證實務作業基準中敘明申請者之身分鑑別方式。

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

憑證申請者包含：

(1) 下屬憑證機構。

(2) 下屬憑證機構之憑證申請者，包括組織或個人。

4.1.2 註冊程序及責任

憑證機構應於憑證實務作業基準中敘明憑證申請者身分識別與鑑別程序及憑證用戶應負義務。

4.2 申請憑證之程序

(1) 總管理中心應於其憑證實務作業基準中敘明下屬憑證機構之申請程序。

(2) 下屬憑證機構憑證之申請，須經其上層憑證機構之同意。

(3) 憑證機構應於憑證實務作業基準中敘明初始註冊、憑證展期及憑證金鑰更換等程序、申辦地點或網址。

(4) GPKI 外之憑證機構與總管理中心申請交互憑證程序，由數發部另訂之。

4.2.1 執行識別及鑑別功能

簽發憑證之機構須依本憑證政策 3.2 節「初始註冊」之規定執行，確保系統與程序足以鑑別用戶身分。

簽發 TLS 憑證之憑證機構應於憑證實務作業基準中，敘明授權憑證機構簽發憑證檢視及確認網域名稱系統資源紀錄之程序。

4.2.2 憑證申請之核准或拒絕

憑證簽發機構完成及確認身分驗證後，可核准憑證申請。

憑證機構可於以下狀況拒絕憑證簽發：

(1) 未通過身分驗證。

(2) 其他經憑證機構認定之原因。

4.2.3 處理憑證申請之時間

憑證機構及註冊中心應於憑證實務作業基準中記載完成受理憑證申請作業之時間。

4.3 簽發憑證之程序

4.3.1 憑證機構之作業

憑證機構簽發憑證應依本憑證政策第 5.2 節「程序控管」及憑證實務作業基準規定，由適當人員執行憑證簽發作業，且憑證機構或註冊中心應以適當方式通知申請者。

4.3.2 憑證機構對憑證申請者之通知

以保證等級第 1 級(含)以上運作之憑證機構，應於憑證實務作業基準中敘明下列事項：

(1) 同意憑證簽發後通知申請者之方式。

(2) 不同意憑證簽發之原因及通知方式。

4.4 接受憑證之程序

以保證等級第 2 級(含)以上運作之憑證機構應經憑證申請者審視憑證內容並接受憑證後，始得將該憑證公布於儲存庫；若憑證申請者不接受憑證，憑證機構應廢止該憑證。

以保證等級第 2 級(含)以上運作之憑證機構，應於憑證實務作業基準中敘明下列事項：

(1) 憑證申請者接受或拒絕憑證之方式。

(2) 憑證申請者接受憑證前應審視之憑證欄位(至少應包括主體名稱)。

(3) 憑證申請者拒絕接受憑證之後續處理方式。

總管理中心應於憑證實務作業基準中敘明自簽憑證及自發憑證接受程序。

4.4.1 接受憑證之要件

憑證申請者於收到憑證後，應確認憑證記載內容是否正確，並了解憑證使用相關規定，方可使用憑證。

4.4.2 憑證機構之憑證發布

憑證機構應定期將所簽發之憑證公布於儲存庫。

憑證機構得委託註冊中心或其他機構將憑證傳遞予用戶。

4.4.3 憑證機構對其他個體之憑證簽發通知

憑證機構得自行決定其對其他個體之憑證簽發通知，本憑證政策於此不另行規定。

4.5 金鑰對及憑證之用途

4.5.1 用戶私密金鑰及憑證使用

(1) 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) 私密金鑰不得用於簽發憑證。

(3) 應保護私密金鑰不被未經授權之他人使用或揭露。

(4) 確保私密金鑰依憑證擴充欄位所註記之金鑰用途使用。

(5) 須依憑證所記載之憑證政策使用憑證。

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各憑證機構之憑證實務作業基準規定。

(2) 須確認憑證有效性後方可使用憑證進行下述作業：

- 驗證電子文件數位簽章之完整性。
- 驗證文件簽章者之身分。
- 建立與用戶間安全通訊管道。

(3) 各憑證機構應於憑證實務作業基準敘明憑證驗證之方式。

4.6 憑證展期

憑證機構如提供憑證展期，則應至少符合下述規定：

(1) 憑證機構之憑證不可展期。

(2) 除已廢止之用戶憑證不得展期外，餘均可視憑證機構之需求提供憑證展期服務。

(3) 用戶憑證展期期限依 6.3.2.2 節「用戶公開金鑰及私密金鑰之使用期限」規定辦理。

4.6.1 憑證展期之事由

由各憑證機構於憑證實務作業基準中敘明是否提供憑證展期。

4.6.2 憑證展期之申請者

憑證機構如提供憑證展期，應於憑證實務作業基準中敘明憑證展期之申請者資格。如申請者資格不符，應明確告知資格不符之理由。

4.6.3 憑證展期之程序

憑證機構如提供憑證展期，應於憑證實務作業基準中敘明憑證展期之程序。

4.6.4 對用戶憑證展期之簽發通知

憑證機構於完成用戶憑證展期後，應依照 4.3.2 節「憑證機構對憑證申請者之通知」規定通知用戶。如憑證機構不同意展期或該憑證無法展期，應明確告知未能展期之理由。

4.6.5 接受展期憑證之要件

憑證申請者於收到展期憑證後，應確認憑證記載內容是否正確，方可使用憑證。

4.6.6 憑證機構之展期憑證發布

憑證機構應定期將展期之憑證公布於儲存庫。

憑證機構得委託註冊中心或其他機構將展期憑證傳遞予用戶。

4.6.7 憑證機構對其他個體之展期憑證簽發通知

憑證機構得自行決定其對其他個體之展期憑證簽發通知，本憑證政策於此不另行規定。

4.7 憑證之金鑰更換

4.7.1 憑證機構金鑰更換事由

(1) 憑證機構應依照 6.3.2.1 節「憑證機構公開金鑰及私密金鑰之使用期限」規定更換金鑰對。

(2) 憑證機構本身之憑證被廢止後，其私密金鑰應停止使用，並須更換金鑰對。

4.7.2 更換憑證金鑰之申請者

更換憑證金鑰之申請者須為該憑證用戶或經授權代表該用戶且負責保管憑證相對應私密金鑰之代表人。

4.7.3 憑證之金鑰更換程序

憑證機構應依照第 4.1 及第 4.2 之規定辦理；憑證機構得要求憑證申請者提供額外資訊以驗證用戶身分。

4.7.4 用戶憑證金鑰更換之簽發通知

憑證機構於完成用戶憑證金鑰更換後，應依照 4.3.2 節「憑證機構對憑證申請者之通知」規定通知用戶，如憑證機構不同意金鑰更換或無法進行用戶憑證金鑰更換，應明確告知未能進行用戶憑證金鑰更換之理由。

4.7.5 接受憑證金鑰更換之要件

憑證申請者於收到更換之憑證後，應確認憑證記載內容是否正確，方可使用憑證。

4.7.6 憑證機構之更換金鑰發布

憑證機構應定期將已完成金鑰更換之憑證公布於儲存庫。

憑證機構得委託註冊中心或其他機構將更換之憑證傳遞予用戶。

4.7.7 憑證機構對其他個體之憑證簽發通知

憑證機構得自行決定其對其他個體之憑證簽發通知，本憑證政策於此不另行規定。

4.8 憑證變更

4.8.1 憑證變更之事由

憑證機構應於憑證實務作業基準中敘明憑證變更之事由。

4.8.2 憑證變更之申請者

憑證變更之申請者為該憑證用戶或經授權代表該用戶且負責保管憑證相對應私密金鑰之代表人。

4.8.3 憑證變更之程序

憑證變更之程序依 4.2 節「申請憑證之程序」規定辦理。

4.8.4 對用戶憑證變更之簽發通知

憑證機構於完成用戶憑證變更後，應依照 4.3.2 節「憑證機構對憑證申請者之通知」規定通知用戶，如憑證機構不同意憑證變更或該憑證無法變更，應明確告知未能完成憑證變更之理由。

4.8.5 接受憑證變更之要件

憑證申請者於收到更換之憑證後，應確認憑證記載內容是否正確，方可使用憑證。

4.8.6 憑證機構之憑證變更發布

憑證機構應定期將已完成變更之憑證公布於儲存庫。

憑證機構得委託註冊中心或其他機構將變更之憑證傳遞予用戶。

4.8.7 憑證機構對其他個體之憑證簽發通知

憑證機構得依其作業需求決定對其他個體之憑證簽發通知，本憑證政策於此不另行規定。

4.9 憑證暫時停用及廢止

(1) 以保證等級第 1 級(含)以上運作之憑證機構均應提供憑證廢止服務，並得自行決定是否提供憑證暫時停用之服務。

(2) 若憑證機構提供憑證廢止服務，則：

- 其應於憑證實務作業基準中敘明憑證廢止服務之服務時間、提供服務方式、憑證廢止申請程序、申辦地點或網址等資訊。如其亦提供憑證暫時停(復)用服務，則亦應於憑證實務作業基準中敘明前述資訊。
- 憑證廢止及停用後，其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，將廢止及停用之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，直至該憑證到期或被復用為止；公告之憑證狀態資訊應包括廢止及停用之憑證。

4.9.1 廢止憑證之事由

憑證機構應於憑證實務作業基準中敘明廢止憑證之事由，內容至少包含以下事由：

(1) 私密金鑰遺失、證實或懷疑遭破解(Compromise)。

(2) 憑證記載之憑證主體資訊須變更時得由憑證機構評估後決定。

4.9.2 憑證廢止之申請者

憑證廢止申請者至少包括以下:

(1) 憑證機構。

(2) 1.3.4 節所定義之「用戶」。

4.9.3 憑證廢止之程序

憑證機構或註冊中心依本憑證政策 3.4 節「憑證廢止申請之識別與鑑別」，完成身分識別及鑑別後，應核准憑證廢止申請。

若憑證機構之金鑰證實被破解，憑證機構憑證及所簽發之憑證無須進行識別及鑑別程序即逕行廢止。

以保證等級第 1 級(含)以上運作之憑證機構，應於憑證實務作業基準中敘明廢止憑證之通知方式。

4.9.4 憑證廢止申請之寬限期

憑證機構如懷疑、已確認金鑰遭破解或因其他安全事由須廢止憑證時，須於 1 小時內通報上層憑證機構。

用戶如懷疑、已確認金鑰遭破解或有其他安全事由須廢止憑證時，應儘速提出憑證廢止申請。

4.9.5 憑證機構處理憑證廢止請求之處理期限

憑證機構應於憑證實務作業基準中敘明處理廢止憑證請求之期限。

4.9.6 信賴憑證者檢查憑證廢止之要求

使用保證等級第 2 級(含)以上憑證之信賴憑證者，於使用憑證前須查詢目前憑證機構廢止清冊及憑證廢止清冊，或透過線上憑證狀態協定查詢服務查驗憑證。

信賴憑證者須考量風險、責任及影響，自行決定擷取憑證廢止資訊之時間。

憑證機構應於憑證實務作業基準中敘明信賴憑證者檢查憑證機構廢止清冊或憑證廢止清冊之要求。

4.9.7 憑證機構廢止清冊及憑證廢止清冊簽發頻率

憑證機構廢止清冊或憑證廢止清冊應定期發布，即使憑證狀態無改變亦要發布，以確保憑證狀態資訊即時性。

憑證機構廢止清冊及憑證廢止清冊之簽發頻率規定如表 4-1 所示：

表 4-1 憑證機構廢止清冊及憑證廢止清冊簽發頻率

簽發頻率 / 保證等級	憑證機構廢止清冊	憑證廢止清冊
測試級	憑證機構得依需求自訂	憑證機構得依需求自訂
第 1 級	憑證機構得依需求自訂	憑證機構得依需求自訂
第 2 級	憑證機構得依需求自訂	每 3 天至少 1 次
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

憑證機構最遲應於憑證機構廢止清冊或憑證廢止清冊下次更新時間欄位所記載之時間前公布。

4.9.9 線上憑證廢止/狀態查驗之服務

憑證機構應提供憑證機構廢止清冊或憑證廢止清冊，進行憑證狀態查驗，憑證機構應於憑證實務作業基準中敘明是否提供線上憑證狀態協定查詢服務。

4.9.10 線上憑證廢止查驗之規定

憑證機構須於憑證實務作業基準中敘明信賴憑證者線上憑證廢止查驗之方式。

4.9.11 其他形式廢止公告

憑證機構得依作業考量提供其他形式之廢止公告，本憑證政策於此不另行規定。

4.9.12 金鑰被破解時之其他特殊規定

憑證機構於金鑰被破解時如有其他特殊規定，應於憑證實務作業基準中敘明。

4.9.13 憑證暫時停用及復用之事由

各憑證機構於憑證實務作業基準中敘明是否提供憑證暫時停用及復用之服務。

4.9.14 憑證暫時停用及復用之申請者

申請者為該憑證用戶或經授權代表該用戶且負責保管憑證相對應私密金鑰之代表人。

4.9.15 憑證暫時停用及復用之程序

憑證機構應於憑證實務作業基準中敘明憑證暫時停用及復用之程序。

4.9.16 暫時停用憑證期間之限制

憑證機構應於憑證實務作業基準中敘明處理憑證暫時停用期間之限制。

4.10 憑證狀態服務

4.10.1 服務特性

憑證機構應提供憑證機構廢止清冊或憑證廢止清冊、線上憑證狀態協定查詢服務，或二者均提供之憑證狀態服務。

4.10.2 服務可用性

憑證機構應提供 7 x 24 小時查詢憑證狀態服務可用性。

4.10.3 可選功能

憑證機構得自行決定憑證狀態服務之可選功能，本憑證政策於此不另行規定。

4.11 終止服務

用戶不再使用憑證機構之服務時，憑證機構應同意用戶終止服務。

4.12 私密金鑰託管及回復

4.12.1 金鑰託管及回復政策與實務

簽章用之私密金鑰不允許被託管於憑證機構。

4.12.2 通訊用金鑰封裝及回復政策與實務

憑證機構如支援通訊用金鑰封裝與回復，應於憑證實務作業基準敘明作法。

5 基礎設施、安全管理及作業程序控管

除有特別規定外，本章節適用於保證等級第 2 級(含)以上運作之憑證機構

5.1 實體控管

5.1.1 實體位置及結構

機房實體所在及結構須結合門禁、保全、入侵偵測、監視錄影等實體安全機制，以防止遭受未經授權之進入。

5.1.2 實體存取

(1) 保證等級第 2 級運作之憑證機構，其實體控管規定如下：

- 應防止未經授權之侵入。
- 儲存機敏性資料之儲存媒體及文件應保存於安全場所。

(2) 保證等級第 3 及第 4 級運作之憑證機構，其實體控管規定如下：

- 應建置 24 小時人工或電子式監控設備。
- 應定期維護及檢視存取紀錄檔。
- 進行電腦系統與密碼模組實體控管時，至少須 2 人(含)以上共同執行。

5.1.3 電力及空調

憑證機構須具備足夠之電力、空調，並提供不斷電系統及至少 6 小時(含)以上之備用電力。

5.1.4 水災防範及保護

憑證機構設置地點須考量避免受到水災侵害。

5.1.5 火災防範及保護

憑證機構須具備自動偵測火災預警，並啟動滅火功能。

5.1.6 媒體儲存

憑證機構須保護相關儲存媒體避免遭受意外損害。

5.1.7 廢料處理

憑證機構得自行規範廢料處理之方式，本憑證政策於此不另行規定。

5.1.8 異地備援

憑證機構須定期進行相關系統異地備援作業，並於憑證實務作業基準中敘明備援、備份週期及地點。

異地備援系統應與正式系統具備相同之安全等級。

5.2 程序控管

5.2.1 信賴角色

憑證機構考量憑證之安全性及有效性，須提供信賴角色執行相關任務，並適當區隔各項任務，同一任務至少須配置 2 人(含)以上。

憑證機構須於憑證實務作業基準中敘明信賴角色之定義。

5.2.2 個別任務所需之人數

個別任務之執行不得由單一人員完成操作，憑證機構應於憑證實務作業基準中敘明信賴角色之任務，及各任務之人數配置。

5.2.3 角色識別及鑑別

信賴角色於執行任務前，須進行身分識別及鑑別作業。

5.2.4 角色權責劃分

憑證機構須於憑證實務作業基準中敘明信賴角色之權責劃分。

5.3 人員控管

憑證機構須確實掌握憑證作業相關人員。

5.3.1 適任條件與經歷

憑證機構須進行作業相關人員之識別作業，並於憑證實務作業基準中敘明人員之資格、遴選、監督及稽核相關辦法。

5.3.2 身家背景之查驗程序

憑證機構應於憑證實務作業基準中敘明作業相關人員身家背景之查驗程序。

5.3.3 教育訓練需求

憑證機構人員須接受相關教育訓練，內容至少包括：

(1) 憑證機構之安全驗證機制。

(2) 憑證機構系統使用之軟硬體。

(3) 負責執行之工作內容。

(4) 災後復原及營運持續計畫。

5.3.4 人員再教育訓練之需求及頻率

憑證機構於法規變更、軟硬體升級或工作程序改變等重大變更時，應進行人員再教育訓練，並於憑證實務作業基準中敘明需求及頻率。

5.3.5 工作調換之頻率及順序

憑證機構得依作業規範定義工作調換之頻率及順序，本憑證政策於此不另行規定。

5.3.6 未授權行動之懲處

憑證機構應於憑證實務作業基準中敘明人員違反規定之懲處方式。

5.3.7 聘僱人員之規定

憑證機構應於憑證實務作業基準中敘明聘僱人員擔任憑證機構相關職務之規定。

5.3.8 提供之文件資料

憑證機構應於憑證實務作業基準中敘明提供憑證機構相關人員執行業務所須之文件資料。

5.4 稽核記錄程序

保證等級第 1 級(含)以上運作之憑證機構，應具備適當之稽核記錄功能，憑證機構應於憑證實務作業基準中敘明稽核記錄程序。

5.4.1 事件記錄之類型

憑證機構應記錄之稽核事件至少包括下列項目：

(1) 事件種類。

(2) 引發事件之個體或操作者。

(3) 事件發生之地點或位置

(4) 事件發生之日期及時間。

(5) 憑證簽發或廢止作業之成功或失敗紀錄。

憑證機構應記錄之稽核事件如表 5-1 所示。

表 5-1 稽核事件記錄規定

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之內容等		✓	✓	✓
A.1.2 任何嘗試刪除或修改稽核紀錄(Audit Log)		✓	✓	✓
A.2 識別與鑑別				
A.2.1 嘗試新角色之成功或失敗設定		✓	✓	✓
A.2.2 身分鑑別嘗試之最高容忍次數改變		✓	✓	✓
A.2.3 使用者登入系統時身分鑑別嘗試之失敗次數之最大值		✓	✓	✓
A.2.4 管理者身分鑑別失敗而被鎖住之帳號解鎖		✓	✓	✓
A.2.5 管理者改變系統之身分		✓	✓	✓

可稽核事件／保證等級	第 1 級	第 2 級	第 3 級	第 4 級
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	✓	✓	✓	✓
A.4 私密金鑰之載入及儲存				
A.4.1 載入私密金鑰至系統元件中	✓	✓	✓	✓
A.4.2 為進行金鑰回復，對憑證主體之私密金鑰存取之所有作業	✓	✓	✓	✓
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新增、刪除及儲存等改變	✓	✓	✓	✓
A.6. 私密金鑰之匯出				
A.6.1 除單次使用之金鑰外，其餘私密金鑰之匯出	✓	✓	✓	✓
A.7. 憑證之註冊				
A.7.1 憑證之註冊申請過程	✓	✓	✓	✓
A.8. 廢止之憑證				
A.8.1 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. 總管理中心或下屬憑證機構之組態設定				
A.10.1 任何與憑證機構安全相		✓	✓	✓

可稽核事件／保證等級	第 1 級	第 2 級	第 3 級	第 4 級
關之組態設定改變				
A.11. 帳號之管理				
A.11.1 新增、刪除角色或使用者	✓	✓	✓	✓
A.11.2 使用者帳號或角色存取權限修改	✓	✓	✓	✓
A.12. 憑證格式剖繪之管理				
A.12.1 憑證格式剖繪之改變	✓	✓	✓	✓
A.13. 憑證機構廢止清冊及憑證廢止清冊格式剖繪之管理				
A.13.1 憑證機構廢止清冊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 嘗試登入憑證機構之應用作業		✓	✓	✓
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		✓	✓	✓

可稽核事件／保證等級	第 1 級	第 2 級	第 3 級	第 4 級
備份				
A.14.12 憑證機構之內部資料回復		✓	✓	✓
A.14.13 產生、重新命名或移動檔案等操作			✓	✓
A.14.14 傳送任何資訊至儲存庫			✓	✓
A.14.15 存取憑證機構之內部資料庫			✓	✓
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 (Zeroize)		✓	✓	✓
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		✓	✓	✓
A.15.5 安全格式剖繪			✓	✓
A.16. 實體存取及場所之安全				
A.16.1 人員進出憑證機構機房			✓	✓
A.16.2 存取憑證機構伺服器			✓	✓

可稽核事件／保證等級	第 1 級	第 2 級	第 3 級	第 4 級
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 接收不正確之訊息			✓	✓
A.17.4 非正常路由之訊息			✓	✓
A.17.5 網路攻擊		✓	✓	✓
A.17.6 設備失效	✓	✓	✓	✓
A.17.7 電力不當			✓	✓
A.17.8 不斷電系統失敗			✓	✓
A.17.9 明顯及重大網路服務或存取失敗			✓	✓
A.17.10 違反憑證政策	✓	✓	✓	✓
A.17.11 違反憑證實務作業基準	✓	✓	✓	✓
A.17.12 重設系統時間		✓	✓	✓

5.4.2 紀錄處理頻率

憑證機構應依表 5-2 規定於憑證實務作業基準中敘明紀錄處理頻率。

表 5-2 紀錄處理頻率

保證等級	紀錄處理頻率
第 2 級	憑證機構得自行決定紀錄處理之頻率，本憑證政策於此不另行規定。
第 3 級	憑證機構應至少每 2 個月檢視自前次稽核檢視後所發生之重大安全稽核紀錄，且對任何可能之惡意活動應進一步調查。
第 4 級	憑證機構應至少每個月檢視自前次稽核檢視後所發生之重大安全稽核紀錄，且對任何可能之惡意活動應進一步調查。

5.4.3 稽核紀錄保留期限

憑證機構稽核紀錄應於所在處至少保留 2 個月，並依第 5.4.4、5.4.5、5.4.6 及 5.5 節規定辦理。

稽核紀錄保留期限屆滿時須由稽核員移除，不可由其他人員代理。

5.4.4 稽核紀錄之保護

憑證機構應採取適當之機制保護稽核紀錄，以避免遭未經授權之存取。

憑證機構應於憑證實務作業基準中敘明稽核紀錄之保護方式。

5.4.5 稽核紀錄備份程序

憑證機構應依表 5-3 之規定於憑證實務作業基準中敘明稽核紀錄備份作法。

表 5-3 稽核紀錄備份作法

保證等級	稽核記錄之備份作法
第2級	每月至少應本地備份1次。

保證等級	稽核記錄之備份作法
第3級	
第4級	每月至少應本地及異地備份1次。

5.4.6 稽核紀錄彙整系統

稽核系統應於憑證系統啟動時持續運作至憑證管理系統關閉為止。

5.4.7 對引起事件者之告知

稽核系統不需告知引起事件之個體。

5.4.8 弱點評估

保證等級第 3 及第 4 級運作之憑證機構，應定期執行弱點及修補評估。

5.5 紀錄歸檔之方法

5.5.1 歸檔紀錄之類型

憑證機構應歸檔之紀錄如表 5-4 所示。

表 5-4 歸檔記錄資料

應歸檔紀錄／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驗證過程及結果之資料	✓	✓	✓	✓
憑證實務作業基準	✓	✓	✓	✓

應歸檔紀錄／保證等級	第 1 級	第 2 級	第 3 級	第 4 級
重要契約	✓	✓	✓	✓
系統或設備組態設定	✓	✓	✓	✓
系統或設備組態設定之修改或更新內容	✓	✓	✓	✓
憑證申請資料	✓	✓	✓	✓
廢止申請資料		✓	✓	✓
用戶身分識別資料		✓	✓	✓
文件簽收及憑證接受		✓	✓	✓
符記啟用紀錄		✓	✓	✓
已簽發或公告憑證	✓	✓	✓	✓
憑證機構金鑰更換紀錄	✓	✓	✓	✓
被簽發或公告之憑證機構廢止清冊及憑證廢止清冊		✓	✓	✓
所有稽核記錄	✓	✓	✓	✓
用以驗證及佐證歸檔內容之其它說明資料或應用程式		✓	✓	✓
稽核人員所要求之文件		✓	✓	✓

5.5.2 歸檔紀錄保留期限

除測試級外，歸檔紀錄保留期限不得低於簽發之憑證效期(Duration)。

憑證機構應於憑證實務作業基準中敘明歸檔之保留期限屆滿時，歸檔紀錄之處理方式。

5.5.3 歸檔紀錄之保護

(1) 已歸檔紀錄不可進行異動及刪除。

(2) 歸檔紀錄須儲存於具安全管控措施且對儲存媒體無害之地點。

(3) 歸檔紀錄於用戶授權同意下得提供其他個人或組織。

5.5.4 歸檔紀錄備份程序

憑證機構得依需求自行決定歸檔紀錄備份程序，本憑證政策於此不另行規定。

5.5.5 歸檔紀錄之時戳要求

憑證機構得依需求自行決定歸檔紀錄之時戳要求，本憑證政策於此不另行規定。

5.5.6 歸檔紀錄彙整系統

憑證機構得自行決定其欲使用之歸檔紀錄彙整系統，本憑證政策於此不另行規定。

5.5.7 取得及驗證歸檔紀錄之程序

憑證機構應於憑證實務作業基準中敘明取得及驗證歸檔紀錄之程序。

5.6 金鑰更換

5.6.1 憑證機構之金鑰更換

(1) 憑證機構須依第 6.3.2 節「公開金鑰及私密金鑰之使用期限」規定定期更換私密金鑰並進行公告。

(2) 舊私密金鑰仍須簽發憑證機構廢止清冊、憑證廢止清冊或線上憑證狀態協定之回應訊息，並持續維護至以舊私密金鑰簽發之所有用戶憑證到期為止。

(3) 憑證機構本身之憑證如被廢止，其私密金鑰應停止使用，並更換金鑰對。

(4) 總管理中心最遲應於自簽憑證到期前 3 個月，更換用以簽發下屬憑證機構憑證之金鑰對，並簽發 1 張新自簽憑證，及使用新舊私密金鑰相互簽發 1 張自發憑證，新憑證之簽發程序依 4.3 節「簽發憑證之程序」規定辦理。

(5) 下屬憑證機構最遲應於憑證到期前 2 個月，更換用以簽發憑證之金鑰對。下屬憑證機構更換金鑰對後，應依 4.2 節「申請憑證之程序」規定申請新憑證。

5.6.2 用戶金鑰更換

(1) 用戶之私密金鑰須依 6.3.2 節「公開金鑰及私密金鑰之使用期限」規定定期更換。

(2) 用戶憑證被廢止後，其私密金鑰應停止使用，如需申請新憑證，須依 4.2 節「申請憑證之程序」規定辦理。

(3) 憑證機構應於憑證實務作業基準中敘明用戶金鑰更換之規定。

5.7 金鑰遭破解或災害時之復原程序

憑證機構之災後復原工作應優先恢復儲存庫，俾正常提供憑證狀態資訊。

5.7.1 緊急事件及系統遭破解之處理程序

憑證機構應於憑證實務作業基準敘明緊急事件及系統遭破解後之通報、處理及復原程序，並每年須依該程序進行演練作業。

5.7.2 電腦資源、軟體或資料遭破壞之復原程序

憑證機構應於憑證實務作業基準敘明電腦資源、軟體或資料遭破壞之復原程序。

保證等級第 3 及第 4 級運作之憑證機構，每年至少須依該程序進行演練作業。

5.7.3 憑證機構簽章金鑰遭破解之復原程序

憑證機構應於憑證實務作業基準敘明憑證機構簽章金鑰遭破解之復原程序。

保證等級第 3 及第 4 級運作之憑證機構，每年至少須依該程序進行演練作業。

5.7.4 憑證機構災變後業務持續營運措施

憑證機構應於憑證實務作業基準敘明憑證機構災後持續營運作業。

保證等級第 3 及第 4 級運作之憑證機構，每年至少須依該程序進行演練作業。

5.8 憑證機構或註冊中心終止服務

憑證機構或註冊中心終止服務應依電子簽章法相關規定辦理。

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

(1) 憑證機構簽發憑證所使用之密碼模組，須符合 FIPS 140-2、FIPS 140-3 規範或經總管理中心同意。

(2) 已產製之私密金鑰應確保無法被非授權人員或未被紀錄之狀態下取得。

(3) 憑證機構應採取適當之措施，確保該用戶之公開金鑰具唯一性。

(4) 代替用戶產製簽章用私密金鑰之個體，不得保留該金鑰備份。

(5) 保證等級第 4 級運作之憑證機構，用戶隨機亂數、金鑰對及對稱金鑰限使用硬體產製。

6.1.2 私密金鑰安全傳送予用戶

(1) 私密金鑰除產製及儲存於用戶之密碼模組外，產製金鑰之個體應以安全及可稽核之方法傳送私密金鑰予憑證主體。

(2) 憑證機構應於憑證實務作業基準中敘明私密金鑰安全傳送予用戶及用戶確認接受之方式。

6.1.3 公開金鑰安全傳送予憑證機構

憑證機構應於憑證實務作業基準中敘明公開金鑰安全傳送予憑證機構之方式。

6.1.4 憑證機構公開金鑰安全傳送予信賴憑證者

憑證機構應於憑證實務作業基準中敘明憑證機構公開金鑰安全傳送予信賴憑證者之方式。

6.1.5 金鑰長度

(1) 憑證機構應使用 RSA 2048 位元(含以上)或安全強度相當之金鑰，並搭配 SHA-256、SHA-384 或 SHA-512 雜湊函數演算法進行憑證簽發。

(2) 用戶使用金鑰長度至少 2048 位元之 RSA 金鑰。

(3) 若支援後量子密碼學(Post-Quantum Cryptography, PQC)，則金鑰與演算法建議符合下列 NIST PQC 標準所定義之安全性類別(Security Category)：

- 憑證機構金鑰：至少須符合安全性類別 3 之安全強度。
- 用戶簽章金鑰：至少須符合安全性類別 2 之安全強度。
- 用戶加解密金鑰:至少須符合安全性類別 1之安全強度。

6.1.6 公開金鑰參數之產製與品質檢驗

使用 RSA 演算法之公開金鑰參數須遵循相關國際標準進行產製，並辦理適當之金鑰品質檢驗。

憑證機構應於憑證實務作業基準中敘明 RSA 公開金鑰品質檢驗之原則。

6.1.7 金鑰使用目的

憑證之公開金鑰須遵循 X.509 標準，於憑證之金鑰用途擴充欄位註記其金鑰用途。

憑證機構應於憑證實務作業基準中敘明金鑰使用目的。

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

密碼模組應符合 FIPS 140-2 或 FIPS 140-3 標準，或於受平台或設備型態限制情形下，經憑證機構依其權責評估並確認具同等安全強度之密碼模組；表 6-1 所列為總管理中心、下屬憑證機構、註冊中心及用戶於密碼模組使用時至少應達成之安全強度要求。

表6-1密碼模組標準規定

保證等級	總管理中心	下屬憑證機構	註冊中心	用戶
測試級	不適用	可自行決定	可自行決定	可自行決定
第1級	不適用	等級1	等級1	可自行決定
第2級	不適用	等級2	等級1	等級1
第3級	不適用	等級2	等級2	等級1
第4級	等級3	等級3	等級2	等級2

※本表參考 FIPS 140-2 及 FIPS 140-3 標準

6.2.2 金鑰分持多人控管

簽發保證等級第 3 或第 4 級憑證之憑證機構，其簽章用私密金鑰分持須符合多人控管(Multi-Person Control)原則。

憑證機構須於憑證實務作業基準中敘明金鑰分持之多人控管程序。

6.2.3 私密金鑰託管

簽章用之私密金鑰不可被託管。

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(含)以上運作之憑證機構，其簽章用私密金鑰應於多人控管程序下進行備份，並保存於安全場所。

憑證機構須於憑證實務作業基準中敘明金鑰備份之程序。

6.2.4.2 用戶簽章用私密金鑰備份

保證等級第 1 級至第 3 級憑證用戶，可由用戶自行備份或複製其簽章用私密金鑰。

保證等級第 4 級憑證用戶，其簽章用私密金鑰不可備份或複製。

6.2.5 私密金鑰歸檔

簽章用私密金鑰不可被歸檔。

6.2.6 私密金鑰及密碼模組間傳輸

(1) 金鑰產製應依 6.1.1 節「金鑰對產製」規定辦理。

(2) 憑證機構除金鑰備份回復、金鑰更換及更換密碼模組外，不得進行私密金鑰與密碼模組間之傳輸。

(3) 憑證機構之私密金鑰與密碼模組間之傳輸可採加密或金鑰分持方式，且不得以明文形式存在於密碼模組外，並應依 6.2.2 節「金鑰分持多人控管」規定進行私密金鑰輸入於密碼模組中。

(4) 憑證機構之私密金鑰輸入完成後，須將過程中產製之參數完全銷毀。

6.2.7 私密金鑰儲存於密碼模組

私密金鑰須符合前述規定儲存於密碼模組內，憑證機構之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

啟動密碼模組中之私密金鑰前，須對啟動者進行身分鑑別並確保資訊安全；已啟動之私密金鑰須進行安全控管。

6.2.9 私密金鑰之停用方式

憑證機構之私密金鑰不需使用時須停止運作；憑證機構應於憑證實務作業基準中敘明私密金鑰之停用方式。

6.2.10 私密金鑰之銷毀方式

憑證機構之簽章用私密金鑰銷毀時須連同備份一併銷毀，銷毀方式如下：

(1) 軟體密碼模組：須將資料複寫至原簽章用私密金鑰佔用之記憶體或儲存媒體。

(2) 硬體密碼模組：硬體密碼模組進行實體銷毀，或執行零值化動作。

6.2.11 密碼模組等級

密碼模組等級依 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

金鑰對不得同時用於簽章與加密；憑證機構應於憑證實務作業基準中敘明金鑰對管理之規定。

6.3.1 公開金鑰之歸檔

憑證歸檔時已進行公開金鑰歸檔，無須再進行公開金鑰歸檔。

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

(1) 總管理中心用以簽署憑證之簽章用私密金鑰，其金鑰生命週期不得超過自簽憑證生命週期之一半。

(2) 總管理中心簽發予下屬憑證機構之憑證生命週期，加上總管理中心用以簽署憑證之簽章用私密金鑰生命週期，合計不得超過總管理中心自簽憑證生命週期。

(3) 總管理中心因應其簽章用金鑰更換時所簽發之自發憑證，其憑證生命週期不得超過舊憑證之效期。

(4) 憑證機構之公開金鑰及私密金鑰使用期限如下：

- RSA 4096 位元或其他安全強度相當之金鑰對：公開金鑰及私密金鑰有效期限至多為 30 年；如該私密金鑰係用於簽發憑證，其使用期限至多為 15 年。
- RSA 2048 位元或其他安全強度相當之金鑰對：公開金鑰與私密金鑰有效期限至多為 20 年；如該私密金鑰係用於簽發憑證，其使用期限至多為 10 年。
- 若支援後量子密碼學時，安全強度至少符合 NIST PQC 標準所定義之安全性類別 3 或其他經評估具相當安全強度之金鑰對：公開金鑰及私密金鑰有效期限至多為 30 年；如該私密金鑰係用於簽發憑證，其使用期限建議至多為 15 年。

- 為因應量子計算對現行公開金鑰密碼技術(包含簽章與加密機制)之潛在威脅，自 2035 年 1 月 1 日(或視技術發展情況調整之期限)起，憑證機構所使用之 RSA 金鑰對建議不再使用；於前述期限前簽發之憑證，其有效期限建議不宜超過該期限；如已簽發且有效期限超過該期限者，應依憑證機構另行公告之過渡處理原則辦理。如前述期限因應政策、技術或國際標準發展而有所變動，憑證機構應另行公告過渡處理原則，並於適當期間內，視風險評估結果，通知相關憑證提前終止使用或辦理可選用演算法之更換，以確保持續符合憑證政策之安全性要求。

6.3.2.2 用戶公開金鑰及私密金鑰之使用期限

(1) 用戶所使用之公開金鑰與私密金鑰使用期限至多為 10 年。

(2) 為因應量子計算對現行公開金鑰密碼技術(包含簽章與加密機制)之潛在威脅，自 2035 年 1 月 1 日(或視技術發展情況調整之期限)起，用戶所使用之 RSA 金鑰對建議不再使用，並配合相關公告之規定，辦理金鑰對之汰換，以確保持續符合憑證政策之安全性要求。

6.4 啟動資料之保護

6.4.1 啟動資料之產生

(1) 保證等級第 1 至第 3 級運作之憑證機構及用戶，其啟動資料(Activation Data)得由使用者自行選擇。

(2) 保證等級第 4 級運作之憑證機構及用戶，應採使用者生物特徵值或密碼模組之安全機制。

(3) 憑證機構如以通行碼做為啟動資料時，須符合行政院及所屬各機關資訊安全管理要點及相關資安規定。

6.4.2 啟動資料之保護

用以解開私密金鑰之啟動資料，須評估風險後採用適當安全機制加以保護；啟動資料如須傳送時應透過適當之安全管道。

憑證機構須於憑證實務作業基準中敘明啟動資料之保護機制。

6.4.3 其他啟動資料之規定

憑證機構得自行定義其對其他啟動資料之規定，本憑證政策於此不另行規定。

6.5 電腦軟硬體安控措施

6.5.1 特定電腦安全技術需求

(1) 特定電腦：指儲存私密金鑰之設備。

(2) 特定電腦設備須建構於通過安全評估之作業平台。

(3) 保證等級第 3 級(含)以上運作之憑證機構，其特定電腦安全技術需求如下：

- 具備身分鑑別之登入。
- 須定義存取控制方式。
- 提供安全稽核能力。
- 確保每次通訊及資料庫安全。
- 具備程序完整性及安全控管保護。

6.5.2 電腦安全評等

憑證機構得依需求定義其電腦安全評等之最低標準；憑證機構整體電腦系統及運作環境應符合 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

憑證機構使用之軟體須遵循系統研發控管措施如下表。

表6-2系統研發控管措施規定

保證等級	系統研發控管措施
測試級	憑證機構得自行決定，本憑證政策不另行規定
第1級	憑證機構得自行決定，本憑證政策不另行規定
第2級	(1) 須確保使用之軟體係依軟體工程發展方法開發。 (2) 憑證機構使用專用之實體或虛擬主機及獲授權之軟體，不得安裝與運作無關之軟硬體。 (3) 須防止被安裝惡意軟體。 (4) 軟體於初次使用時須進行惡意程式碼檢查作業，並定期掃瞄。
第3級	
第4級	

6.6.2 安全管理管控措施

憑證機構使用之軟體須遵循安全管理措施如下表。

表 6-3 安全管理措施

保證等級	安全管理控管措施
測試級	(1) 須記錄及控管相關系統組態及系統修訂歷程。

保證等級	安全管理控管措施
第1級	(2) 具備偵測未經許可修改憑證機構之軟體或組態機制。 (3) 安裝軟體時，須確認該軟體為正確版本且未被竄改。
第2級	
第3級	
第4級	(1) 須記錄及控管相關系統組態及系統修訂歷程。 (2) 具備偵測未經許可修改憑證機構之軟體或組態機制。 (3) 安裝軟體時，須確認該軟體為正確版本且未被竄改。 (4) 每月至少 1 次驗證憑證機構軟體之完整性。

6.6.3 生命週期安全管控措施

憑證機構得依需求自行決定生命週期安全之管控措施，本憑證政策於此不另行規定。

6.7 網路安全控管措施

總管理中心除外部儲存庫主機外，其他主機不得與任何外部網路連接。

憑證機構須於憑證實務作業基準中敘明網路安全控管措施。

6.8 時戳

憑證機構得依需求自行決定時戳之相關規定，本憑證政策於此不另行規定。

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

7.1.1 版本序號

憑證機構須簽發 X.509 v3 版本之憑證。

7.1.2 憑證擴充欄位

保證等級第 3 級(含)以上憑證機構簽發之憑證須遵循「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」規定；保證等級第 1 級及第 2 級之憑證機構，須遵循 RFC 5280 標準之規定。

憑證格式剖繪中應訂定憑證擴充欄位之使用、處理方式及欄位值設定等規定。

憑證機構如須新增擴充欄位，應於憑證實務作業基準中敘明該新增欄位之關鍵性。

7.1.3 演算法物件識別碼

憑證機構簽發之憑證可使用之演算法物件識別碼如下：

表7-1演算法物件識別碼

類型	演算法	演算法物件識別碼
金鑰產製	rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) rsaEncryption(1)}
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)}

若支援後量子密碼學，則可使用之演算法物件識別碼如下：

類型	演算法	演算法物件識別碼
簽章金鑰產製	id-ml-dsa-44	{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) sigAlgs(3) id-ml-dsa-44(17)}
	id-ml-dsa-65	{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) sigAlgs(3) id-ml-dsa-65(18)}
	id-ml-dsa-87	{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) sigAlgs(3) id-ml-dsa-87(19)}
	id-MLDSA44-RSA2048-PSS-SHA256	{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) algorithms(6) id-MLDSA44-RSA2048-PSS-SHA256(37)}
	id-MLDSA44-RSA2048-PKCS15-SHA256	{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) algorithms(6) id-MLDSA44-RSA2048-PKCS15-SHA256(38)}
	id-MLDSA65-RSA3072-PSS-SHA512	{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) algorithms(6) id-MLDSA65-RSA3072-PSS-SHA512(41)}
	id-MLDSA65-RSA3072-PKCS15-SHA512	{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) algorithms(6) id-MLDSA65-RSA3072-PKCS15-SHA512(42)}
	id-MLDSA65-RSA4096-PSS-SHA512	{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) algorithms(6) id-MLDSA65-RSA4096-PSS-SHA512(43)}
	id-MLDSA65-RSA4096-PKCS15-SHA512	{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) algorithms(6) id-MLDSA65-RSA4096-PKCS15-SHA512(44)}
	id-MLDSA87-RSA3072-PSS-SHA512	{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) algorithms(6) id-MLDSA87-RSA3072-PSS-SHA512(52)}
	id-MLDSA87-RSA4096-PSS-SHA512	{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) algorithms(6) id-MLDSA87-RSA4096-PSS-SHA512(53)}

加解密金鑰產製	id-alg-ml-kem-512	{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) kems(4) id-alg-ml-kem-512(1)}
	id-alg-ml-kem-768	{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) kems(4) id-alg-ml-kem-768(2)}
	id-alg-ml-kem-1024	{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) kems(4) id-alg-ml-kem-1024(3)}
	id-MLKEM768-RSA2048-SHA3-256	{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) algorithms(6) id-MLKEM768-RSA2048-SHA3-256(55)}
	id-MLKEM768-RSA3072-SHA3-256	{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) algorithms(6) id-MLKEM768-RSA3072-SHA3-256(56)}
	id-MLKEM768-RSA4096-SHA3-256	{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) algorithms(6) id-MLKEM768-RSA4096-SHA3-256(57)}
	id-MLKEM1024-RSA3072-SHA3-256	{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) algorithms(6) id-MLKEM1024-RSA3072-SHA3-256(62)}
簽章	id-ml-dsa-44	{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) sigAlgs(3) id-ml-dsa-44(17)}
	id-ml-dsa-65	{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) sigAlgs(3) id-ml-dsa-65(18)}
	id-ml-dsa-87	{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) sigAlgs(3) id-ml-dsa-87(19)}
	id-MLDSA44-RSA2048-PSS-SHA256	{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) algorithms(6) id-MLDSA44-RSA2048-PSS-SHA256(37)}
	id-MLDSA44-RSA2048-PKCS15-SHA256	{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) algorithms(6) id-MLDSA44-RSA2048-PKCS15-SHA256(38)}

	id-MLDSA65-RSA3072-PSS-SHA512	{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) algorithms(6) id-MLDSA65-RSA3072-PSS-SHA512(41)}
	id-MLDSA65-RSA3072-PKCS15-SHA512	{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) algorithms(6) id-MLDSA65-RSA3072-PKCS15-SHA512(42)}
	id-MLDSA65-RSA4096-PSS-SHA512	{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) algorithms(6) id-MLDSA65-RSA4096-PSS-SHA512(43)}
	id-MLDSA65-RSA4096-PKCS15-SHA512	{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) algorithms(6) id-MLDSA65-RSA4096-PKCS15-SHA512(44)}
	id-MLDSA87-RSA3072-PSS-SHA512	{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) algorithms(6) id-MLDSA87-RSA3072-PSS-SHA512(52)}
	id-MLDSA87-RSA4096-PSS-SHA512	{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) algorithms(6) id-MLDSA87-RSA4096-PSS-SHA512(53)}

7.1.4 命名形式

主體及簽發者 2 個欄位值，須使用 X.500 唯一識別名稱，且屬性型態須遵循 RFC 5280 規定。

7.1.5 命名限制

憑證機構得依需求決定憑證是否使用命名限制，本憑證政策於此不另行規定。

7.1.6 憑證政策物件識別碼

憑證須記載憑證政策物件識別碼，該物件識別碼須與憑證保證等級相符。

7.1.7 政策限制擴充欄位之使用

憑證機構得依需求決定憑證是否使用「政策限制」擴充欄位，本憑證政策於此不另行規定。

7.1.8 政策限定元之語法及語意

憑證不得包含「政策限定元」 。

7.1.9 關鍵憑證政策擴充欄位之語意處理

關鍵憑證政策擴充欄位之語意處理須遵循「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」規定。

7.2 憑證機構廢止清冊及憑證廢止清冊格式剖繪

7.2.1 版本序號

憑證機構廢止清冊及憑證廢止清冊須符合 X.509 v2 之規定。

7.2.2 憑證機構廢止清冊及憑證廢止清冊擴充欄位

每個擴充欄位均須於「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」中定義。

7.3 線上憑證狀態協定格式剖繪

憑證機構如提供線上憑證狀態協定查詢服務，應於憑證實務作業基準敘明服務版本序號及擴充欄位所採用之標準；回應訊息應加上數位簽章。

7.3.1 版本序號

線上憑證狀態協定版本序號應符合 RFC 6960 規定

7.3.2 線上憑證狀態協定擴充欄位

線上憑證狀態協定查詢之擴充欄位應符合 RFC 6960 規定。

8 稽核方法

簽發保證等級第 2 級(含)以上憑證之憑證機構，應建立公正之稽核機制，以確保其運作遵照憑證實務作業基準與憑證政策之規定。

數發部具有稽核憑證機構之權利，以確保該憑證機構遵循憑證政策規定進行各項維運作業。憑證機構應定期自行稽核，以確保其遵照憑證政策之保證等級進行維運作業。

8.1 稽核頻率或評估事項

憑證機構應接受定期稽核，並符合表 8-1 憑證機構稽核頻率規定。

表8-1 憑證機構稽核頻率

保證等級	稽核頻率
測試級	憑證機構得自行決定，本憑證政策不另作規定
第1級	憑證機構得自行決定，本憑證政策不另行規定
第2級	至少每兩年 1 次
第3級	至少每年 1 次
第4級	至少每年 1 次

憑證機構應於憑證實務作業基準載明其定期稽核所採用之稽核標準，並應對其下屬憑證機構及註冊中心，進行定期及不定期稽核，以確認其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之憑證機構外，可由下述個體擔任：

(1) 第三方公正人員。

(2) 在組織劃分上，與被稽核之憑證機構有所區別之另一獨立個體。

稽核人員應提供公正及獨立之評估，其資格認定須經數發部核可，且熟悉憑證機構簽發、管理憑證之相關規定。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

稽核人員應獨立於被稽核之憑證機構外，其資格依 8.2 節「稽核人員之身分及資格」規定辦理。

8.4 稽核之範圍

稽核之範圍規定如下：

(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。

稽核人員應對憑證機構之註冊中心等相關維運單位進行稽核，憑證機構與其下屬憑證機構如簽訂交互認證協議書(Cross Certification Agreement)時，稽核範圍應涵蓋該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，須採取行動如下：

(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主管機關，如不

符合情形為嚴重缺失，稽核人員應立即通知數發部。

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

對於不符合稽核標準要求之憑證機構，數發部得要求限期改善或採取其他必要措施。

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，與信賴憑證者信賴該憑證之相關資訊均應公開提供。

憑證機構應公布最近 1 次之稽核結果。

9 其他業務與法律事項

9.1 費用

憑證機構得依業務需求決定是否收取憑證相關作業之費用，本憑證政策不另行規定。

9.1.1 憑證簽發、展期費用

憑證機構得自行決定憑證簽發與憑證展期之費用，本憑證政策於此不另行規定。

9.1.2 憑證查詢費用

憑證機構得自行決定憑證查詢之費用，本憑證政策於此不另行規定。

9.1.3 憑證廢止、狀態查詢費用

憑證機構得自行決定憑證廢止與憑證狀態查詢之費用，本憑證政策於此不另行規定。

9.1.4 其他服務費用

憑證機構得自行決定其他服務之費用，本憑證政策於此不另行規定。

9.1.5 請求退費程序

憑證機構得自行決定請求退費之程序，本憑證政策於此不另行規定。

9.2 財務責任

憑證機構得依業務考量規劃其財務保險之責任，本憑證政策不另行規定。

9.2.1 保險範圍

憑證機構得自行決定其憑證服務之財務保險範圍，本憑證政策於此不另行規定。

9.2.2 其他資產

憑證機構得自行決定其他資產之財務責任，本憑證政策於此不另行規定。

9.2.3 對終端個體之保險或保固責任

憑證機構得自行決定其對終端個體之保險或保固責任，本憑證政策於此不另行規定。

9.3 業務資訊保密

9.3.1 機敏性資訊之範圍

憑證機構應於憑證實務作業基準中敘明機敏性資訊範圍及種類，並依照相關法令規定辦理。

9.3.2 非機敏性資料之範圍

憑證機構應於憑證實務作業基準中敘明非機敏性資訊範圍及種類。

9.3.3 保護機敏性資訊之責任

憑證機構應於憑證實務作業基準中敘明保護機敏性資訊之責任。

9.4 個人資訊之隱私性

9.4.1 隱私保護計畫

憑證機構應於憑證實務作業基準敘明個人資料保護與隱私權聲明。

9.4.2 隱私資料之種類

憑證機構應於憑證實務作業基準或網站敘明隱私資料之種類。

9.4.3 非隱私資訊

憑證機構應於憑證實務作業基準敘明非隱私資料之種類。

9.4.4 保護隱私資訊之責任

憑證機構應於憑證實務作業基準敍明保護隱私資訊之責任。

9.4.5 使用隱私資訊之公告與同意

憑證機構應於憑證實務作業基準敍明使用隱私資訊之規定。

9.4.6 應司法或管理程序提供資訊

憑證機構應於憑證實務作業基準敘明提供司法人員隱私資訊之相關規定。

9.4.7 其他資訊提供之情形

憑證機構應於憑證實務作業基準敍明提供其他資訊之相關規定，並依相關法令規定辦理。

9.5 智慧財產權

本憑證政策之智慧財產權由數發部擁有，相關資料可由總管理中心儲存庫自由下載，或依著作權法相關規定重製或散布，惟須保證係完整複製，並註明著作權之擁有。另外，重製或散布本憑證政策者，不得向他人收取費用，亦不得拒絕任何人請求取得。數發部對不當使用或散布本憑證政策所衍生之任何問題，不負任何法律責任。

9.6 職責與義務

9.6.1 憑證機構職責與義務

憑證機構之職責與義務至少包括下列事項：

(1) 遵守本憑證政策之規定。

(2) 執行憑證申請之識別與鑑別程序。

(3) 簽發及公布憑證。

(4) 廢止憑證。

(5) 簽發及公布憑證機構廢止清冊或憑證廢止清冊。

(6) 簽發及提供線上憑證狀態協定查詢服務回應訊息。

(7) 執行憑證機構人員之識別與鑑別程序。

(8) 安全產製憑證機構之私密金鑰。

(9) 保護憑證機構之私密金鑰。

(10) 公布憑證實務作業基準，並說明對用戶與信賴憑證者所負之責任。

9.6.2 註冊中心職責與義務

註冊中心之職責與義務至少包括下列事項：

(1) 提供憑證申請服務。

(2) 對憑證申請進行識別及鑑別。

(3) 告知用戶及信賴憑證者關於憑證機構、註冊中心之義務與責任。

(4) 執行憑證註冊審驗人員之識別與鑑別程序。

(5) 管理註冊中心之私密金鑰。

(6) 註冊中心未經其上層憑證機構同意，不得將註冊中心私密金鑰使用於憑證註冊以外作業。

9.6.3 用戶之義務

用戶之義務至少包括下列事項：

(1) 提供正確完整之資訊。

(2) 遵守本憑證政策及憑證實務作業基準相關規定。

(3) 妥善保管及使用私密金鑰。

(4) 私密金鑰遭冒用、破解或遺失時應立即通知憑證機構並停用憑證。

(5) 安全產製其私密金鑰並避免遭受破解。

9.6.4 信賴憑證者義務

信賴憑證者之義務至少包括下列事項：

(1) 依憑證及保證等級及適用範圍使用憑證。

(2) 依照憑證政策或憑證實務作業基準規定正確檢驗憑證數位簽章、有效性及金鑰用途。

(3) 應確保憑證使用環境之安全，如非可歸責於憑證機構之事由，應自行承擔責任。

(4) 憑證管理中心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。

9.6.5 其他參與者義務

憑證機構得自行決定其他參與者之義務，本憑證政策於此不另行規定。

9.7 免責聲明

憑證機構應於憑證實務作業基準中敘明免責聲明及其限制條件，惟不得將因自行疏忽所引起之後果列入免責聲明中。

9.8 責任限制

憑證機構應於憑證實務作業基準中敘明責任限制。

9.9 賠償

憑證機構應於憑證實務作業基準中敘明對用戶及信賴憑證者的賠償責任，且應符合電子簽章法及相關法規。

9.10 文件之生效與終止

憑證機構應於憑證實務作業基準中敘明文件生效與終止之情況。

9.10.1 生效

本憑證政策及附件公告於 GPKI 網站與儲存庫後即生效。

9.10.2 終止

本憑證政策新版本經行政機關電子憑證推行小組委員核定後公布，現有版本即告終止。

9.10.3 終止及存續之效力

本憑證政策終止後，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

應以適當方式對參與者進行個別通知及溝通。

9.12 修訂

每年應至少檢視本憑證政策 1 次，憑證機構每年至少應檢視憑證實務作業基準 1 次。

9.12.1 修訂程序

本憑證政策之修訂經行政機關電子憑證推行小組審查通過後頒布。

9.12.2 通知機制與期限

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

憑證實務作業基準之修訂，經電子簽章法主管機關核定後須於 10 個日曆天內公告。

9.12.3 須修改憑證政策物件識別碼之事由

憑證政策物件識別碼須進行變更之事由如下：

(1) 本憑證政策定義之保證等級變更時。

(2) 因應國際環境變遷或規範變更，經評估須進行修改。

9.13 紛爭之處理程序

憑證機構應於憑證實務作業基準中敘明紛爭之處理程序。

9.14 管轄法律

GPKI 執行相關業務，依中華民國管轄法律為主。

9.15 適用法律

GPKI 執行業務應依相關法令規定辦理，憑證機構應於憑證實務作業基準中敘明適用之法律。

9.16 雜項條款

9.16.1 完整協議

憑證機構得自行決定與其憑證實務作業基準所約定者間之完整協議，本憑證政策於此不另行規定。

9.16.2 轉讓

憑證機構應於憑證實務作業基準中敘明主要成員之權利或責任轉讓之規定。

9.16.3 可分割性

本憑證政策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憑證政策相關規定，致總管理中心受有損害，如可歸責於用戶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。

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

因不可抗力及其他非可歸責於憑證機構所導致之損害事件，憑證機構不負任何法律責任。

憑證機構得於憑證實務作業基準中敘明排除條款，惟不得將因自行疏忽所衍生之錯誤列入排除條款中。

9.17 其他條款

憑證機構得依需求自行定義其他條款，本憑證政策於此不另行規定。

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及營運程序，並對現有之控制、政策及程序等，建議必要之改善所進行之獨立檢閱及調查。
- **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及某個事件中之變化。
- **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。憑證政策及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序號(包括下屬憑證機構憑證交互憑證)。
- **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及處理其他身分識別業務之作業準則。
  - 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)。
- **加拿大會計師公會(Chartered Professional Accountants Canada, CPA)**:與美國會計師公會共同訂頒 The Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy 系列標準之單位，並為 WebTrust for CA、SSL Baseline Requirement & Network Security 標章之管理單位。加拿大會計師公會之前英文名稱為 Canadian Institute of Chartered Accountants，縮寫為 CICA。
- **破解(Compromise)**：資訊洩漏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。
- **交互認證協議書(Cross Certification Agreement, CCA)**：總管理中心與下屬憑證機構就下屬憑證機構申請加入 GPKI 所須遵守之事項及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。

◆ **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及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：
  - 負責保管及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及信賴憑證者，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。

◆ **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。

◆ **M**

- **多人控管(Multi-Person Control)**：由二人或以上之人員對同一流程或事項進行操作與管理，為一種完全秘密分享(Perfect Secret Sharing)之控管方式，例如：LaGrange 多項式內插法(LaGrange Polynomial Interpolation)的 n-out-of-m。
- **相互鑑別(Mutual Authentication)**：發生於進行通訊活動之兩方彼此進行鑑別時。

◆ **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及使用之密碼演算法。
- **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 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

- **個人標識號(Personal Identification Number, PIN)**：由一串數字構成的通行碼，用來認證使用者身份，授權他進入系統。
- **後量子密碼學(Post-Quantum Cryptography, PQC)**：指為抵抗量子電腦運算攻擊所設計之密碼學技術，其安全性建立於量子電腦目前難以有效解決之數學問題（例如格問題、雜湊函數問題、多變量多項式問題等）之上，以確保於量子電腦環境下，相關資訊系統仍能維持其機密性、完整性及安全性。
- **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機敏性資訊解密之金鑰。
- **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機敏性資訊加密之金鑰。
- **公開金鑰加密標準(Public Key Cryptography Standards, PKCS)**：由 RSA 資訊安全公司旗下的 RSA 實驗室針對金鑰技術的使用，設計與發佈一系列的公開金鑰密碼編譯標準。
- **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開金鑰

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及保證等級之新憑證，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。
  - 個人或機構收到包含憑證及數位簽章之資訊，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。

- **請求意見稿（Request for Comments,RFC）**：由網際網路工程任務小組(IETF)發布的一系列備忘錄。檔案收集了有關網際網路相關資訊，以及 UNIX 和網際網路社群的軟體檔案，以編號排定。

- **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廠商負責散布。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。

- **主體憑證機構(Subject Certification Authority)**：對憑證機構憑證(CA Certificate)而言，該憑證之憑證主體(Subject)所指之

憑證機構，即稱為該憑證之主體憑證機構。

- **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**

- **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。

- **可信賴系統(Trustworthy System)**：具有下列性質之電腦硬體、軟體及程序：
  - 對於入侵及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。