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 1.4 版

主辦機關：行政院研究發展考核委員會

執行機構：中華電信股份有限公司

中華民國 97 年 3 月 12 日

目　　錄

1 序論

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)係依據電子化政府推動方案(90 至 93 年度)，為健全電子化政府基礎建設環境，建立行政機關電子認證及安全制度所設立。本基礎建設是依照 ITU-T X.509 標準所建置的階層式(Hierarchy)公開金鑰基礎建設，包括公開金鑰基礎建設的信賴起源(Trust Anchor)－政府憑證總管理中心(Government Root Certification Authority，GRCA，以下簡稱總管理中心)及政府機關設立的下屬憑證機構(Subordinate CA)所組成。加入本基礎建設的憑證機構(Certification Authority，CA)必須為目的事業主管機關依據電子化政府電子認證服務分工所建置之憑證機構，簽發之憑證應用於電子化政府的各項應用，以提供更便捷的網路便民服務，提升政府行政效率，促進電子化政府及電子商務的應用發展。

行政院研究發展考核委員會(以下簡稱本會)為本基礎建設的管理機構。本會並設立行政機關電子憑證推行小組(Government Electronic Certification Steering Committee，GECSC)，以協助管理本基礎建設，有關行政機關電子憑證推行小組的工作任務詳如 1.3.1 節。同時，為提供本基礎建設憑證管理的共同規範，並促進本基礎建設對內及對外

的互通性（Interoperability），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，GPKI CP，以下簡稱本憑證政策)。

1.1 概要

1.1.1 憑證政策

本憑證政策係依據電子簽章法規定及相關國際標準（如 IETF RFC 2527 等）所訂定之技術政策文件，以作為本基礎建設憑證機構訂定憑證實務作業基準之依循。為確保公鑰憑證的互通性，加入本基礎建設之政府機關憑證機構均應遵循本憑證政策，不可自訂憑證政策。

本憑證政策共定義 5 種保證等級(Assurance Level)，依次為測試級、第 1 級、第 2 級、第 3 級及第 4 級。其中測試級僅用於測試憑證，其保證等級最低；而第 1 級、第 2 級、第 3 級及第 4 級之等級數字越大者，其保證等級越高。本憑證政策係綜合考量以下 3 個層面來定義不同的保證等級：

(1) 信賴憑證者(Relying Party)能否確信憑證中所記載的憑證主體（Subject）與公開金鑰（Public Key）之連結關係（Binding）。

(2) 信賴憑證者能否確信憑證中所記載的憑證主體確實可以控制

與憑證中所記載的公開金鑰相對之私密金鑰（Private Key）的使用。

(3) 信賴憑證者能否確信憑證機構用來簽發、管理憑證及傳送私密金鑰之系統或程序的安全性。

本基礎建設共註冊 5 個保證等級的憑證政策物件識別碼(CP Object Identifier，CP OID，詳見 1.2 節)，憑證機構在簽發憑證時，可以選擇適當的憑證政策物件識別碼記載在憑證的憑證政策延伸欄位(certificatePolicies Extension)中，信賴憑證者可透過憑證中記載的憑證政策物件識別碼確認該憑證的適用範圍。

此外，本基礎建設所註冊的 5 個保證等級之憑證政策物件識別碼亦可供憑證機構在簽發交互憑證時，於交互憑證的憑證政策對映延伸欄位(policyMappings Extension)中，標示憑證政策對映（Policy Mapping）關係，信賴憑證者可透過成對的憑證政策物件識別碼確認簽發憑證機構與主體憑證機構之間的憑證政策對映關係。

1.1.2 憑證政策及憑證實務作業基準之關係

憑證機構必須於憑證實務作業基準中說明如何達成所引用本憑證政策之保證等級。

1.1.3 憑證機構引用憑證政策物件識別碼

憑證機構引用本基礎建設之憑證政策物件識別碼必須經本會同意。如本基礎建設外的其他憑證機構因引用本憑證政策所引發之任何問題，一律由該憑證機構自行負責。

依據所簽發憑證的適用範圍不同，憑證機構應選擇適當的憑證政策物件識別碼，並記載於憑證的憑證政策延伸欄位中。但總管理中心的自簽憑證(self-signed certificate)在本基礎建設中僅作為信賴起源的資訊物件，信賴憑證者將直接信賴該自簽憑證中所記載的公鑰資訊，因此得不於憑證中標示憑證政策物件識別碼。

總管理中心及非本基礎建設的憑證機構只有在行政機關電子憑證推行小組同意憑證政策對映關係後，才可在憑證政策對映延伸欄位(policyMappings Extension)中引用本基礎建設之憑證政策物件識別碼。

1.2 憑證政策之識別

本憑證政策定義五個保證等級的憑證政策物件識別碼，註冊於id-tw-gpki arc 之下：

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 主要成員及其角色

1.3.1 行政機關電子憑證推行小組

為建立電子化政府電子認證制度，推動電子化政府公鑰基礎建設，加速行政機關網路便民服務之應用發展，本會設立行政機關電子憑證推行小組。行政機關電子憑證推行小組置召集人 1 人，由本會主任委員指派副主任委員 1 人兼任；執行秘書 1 人，由本會資訊管理處處長兼任；委員 15 人至 17 人，由學者專家、業界及機關代表聘兼之，工作任務說明如下：

(1)研議行政機關電子憑證政策及憑證實務作業基準。

(2)研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 政府憑證總管理中心

政府憑證總管理中心為本基礎建設最頂層的憑證機構(Root CA)，主要工作說明如下：

(1)負責下屬憑證機構憑證之簽發及管理。

(2)訂定本基礎建設交互認證(Cross-Certification)程序，以及簽發與管理本基礎建設第 1 層下屬憑證機構憑證、本基礎建設外其他憑證機構的憑證。

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

總管理中心是本基礎建設的信賴起點，基於信賴起點必須具備最高公信力，因此總管理中心必須以保證等級第 4 級運作。總管理中心在經行政機關電子憑證推行小組同意後，才可與本基礎建設外之憑證機構進行交互認證(Cross-Certification)。總管理中心應於憑證實務作業基準中訂定與憑證機構交互認證的程序。

1.3.3 下屬憑證機構

下屬憑證機構為本基礎建設中的另一種憑證機構，主要負責簽發及管理終端個體的憑證，必要時也可依階層式公開金鑰基礎建設的建構方式，由第 1 層下屬憑證機構簽發憑證給第 2 層下屬憑證機構，或

由第 2 層下屬憑證機構簽發憑證給第 3 層下屬憑證機構，依此類推。下屬憑證機構不可以直接與本基礎建設外的憑證機構進行交互認證。

下屬憑證機構應依本憑證政策相關規定進行建置，並設置聯絡窗口。

1.3.4 註冊中心

註冊中心(Registration Authority，RA)主要負責收集及驗證用戶(Subscribers)的身分及相關資料之正確性，以利後續憑證機構將這些資料寫入憑證中及儲存憑證申請資料。

總管理中心應自行擔任註冊中心角色，並依核定之憑證實務作業基準執行註冊中心工作。下屬憑證機構則可另外設立註冊中心，並於憑證實務作業基準中規範其工作內容。

1.3.5 儲存庫

儲存庫提供查詢及下載憑證機構所簽發憑證、憑證廢止清冊及憑證狀態等服務，並公佈憑證政策及憑證實務作業基準等憑證作業相關資訊。

1 個憑證機構至少需有 1 個對外服務的儲存庫，儲存庫可由憑證機構自行維運或委託其他機構維運。憑證機構應在憑證實務作業基準中說明儲存庫的網址，並確保儲存庫之可用性、存取控制及資料完整

性。

1.3.6 終端個體

終端個體(End Entities，EE)包括以下兩類個體：

(1)用戶(Subscriber)。

(2)信賴憑證者(Relying Parties)。

1.3.6.1 用戶

對於簽發給組織及個人的憑證而言，用戶(Subscriber)係指憑證之憑證主體名稱(Subject Name)所識別的個體，該個體並擁有與憑證之公開金鑰相對應之私密金鑰。用戶必須依據憑證所記載的憑證政策物件識別碼合法使用憑證及其相對應之私密金鑰。另外，對於簽發給財產類別(例如應用程式(Application Process)及硬體設備(Device)的憑證而言，由於財產本身並無行為能力，因此用戶為申請憑證的個人或組織。

雖然憑證機構可能會簽發憑證機構憑證給其他憑證機構，但在本憑證政策中並不稱憑證機構憑證之憑證主體名稱所識別的憑證機構為用戶，而稱為主體憑證機構。

1.3.6.2 信賴憑證者

信賴憑證者(Relying Parties)係指相信憑證之憑證主體名稱與公

開金鑰連結關係的個體。信賴憑證者必須依據憑證機構之憑證及憑證狀態資訊，檢驗所使用憑證的有效性。

信賴憑證者可使用憑證來驗證數位簽署訊息的完整性、確認發送訊息者的身分及建立與用戶間的秘密通訊管道。同時，信賴憑證者也可使用憑證中的訊息(例如憑證政策物件識別碼)，檢視此憑證的使用時機是否適當。

1.3.7 其他相關成員

憑證機構可選擇其他機構協助處理憑證作業相關事宜，並在憑證實務作業基準中訂定相關作業程序並說明受託之機構的身分。

1.3.8 適用範圍

本憑證政策依照不同安全需求訂定 5 種保證等級，以因應各種不同應用需要。憑證機構在決定憑證之保證等級時，應依應用範圍審慎評估各種風險，包括環境、潛在危機、弱點及憑證的用途與重要性等。

1.3.8.1 憑證之適用範圍

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

表 1-2 憑證適用範圍

保證等級	適用範圍
測試級	僅供測試(Test)用，對於傳送的資料不負任何法律責任。
第 1 級	基本級(Rudimentary)的保證等級，適合應用於惡意篡改之威脅很低的網路環境，或在無法提供較高保證等級時，識別用戶個體名稱及保證被簽署文件的完整性；不適合應用於需要認證的電子交易。
第 2 級	初級(Basic)的保證等級，適合應用於資訊可能被篡改，但不會有惡意篡改之網路環境(資訊可能被截取但機率不高)；不適合做為重要文件的簽署。
第 3 級	中級(Medium)的保證等級，適合應用於有惡意使用者會截取或篡改資訊、較第 2 級危險之網路環境，傳送的資訊包括電子交易等。
第 4 級	高級(High)的保證等級，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機密的文件等。

1.3.8.2 憑證之使用限制

信賴憑證者應先決定應用上所需的保證等級，然後選擇適合該保證等級的憑證，並依照 6.1.9 節之規定，判別該憑證是否適用於應用上所需的金鑰使用目的。

信賴憑證者應使用符合相關國際標準(如 X.509 標準或 IETF RFC 3280 等)定義之憑證驗證(certificate validation)方法來檢查憑證的有效性（validity）。

1.3.8.3 憑證之禁止使用情形

本基礎建設之憑證機構簽發的憑證禁止使用於以下情形：

(1) 犯罪。

(2) 軍令戰情及核生化武器管制。

(3) 核能運轉設備。

(4) 航空飛行及管制系統。

1.4 聯絡方式

1.4.1 憑證政策之制訂及管理機關

行政院研究發展考核委員會。

1.4.2 聯絡資料

如對本憑證政策有任何建議，請與本會聯繫，聯絡資料請參閱 http://grca.nat.gov.tw/。

1.4.3 憑證實務作業基準之審定

憑證機構應先自行檢查憑證實務作業基準是否符合憑證政策相關規定後，再送行政機關電子憑證推行小組進行審查，審查核定後，憑證機構便可正式引用本基礎建設的憑證政策。

另依據電子簽章法規定，憑證機構訂定之憑證實務作業基準，必須經主管機關經濟部核定後，始得對外提供簽發憑證服務。

本會對於憑證機構是否遵循憑證政策，具有稽核的權利(依照 2.7 節規定)，憑證機構也應定期自行稽核，以證明遵照憑證政策的保證等級進行維運。

2 一般條款

2.1 職責及義務

2.1.1 憑證機構之職責

憑證機構之職責如下：

(1)簽發及公佈憑證。

(2)執行第 3 章規定之鑑別程序。

(3)簽發及公佈憑證機構廢止清冊或憑證廢止清冊,或提供線上憑證狀態查詢服務。

(4)依據第 4 及第 6 章規定提供相關控制。

(5)公佈憑證實務作業基準,並說明對用戶與信賴憑證者所負之責任。

(6)依據第 4、第 5 及第 6 章規定保護私密金鑰。

(7)確實區分憑證機構本身之私密金鑰用途。用於簽發憑證及憑證廢止清冊的私密金鑰不得用於其他用途，例如一般數位簽章、身分認證、資料加密或金鑰加密等。

(8)本基礎建設之各憑證機構所訂定的憑證實務作業基準應遵循本憑證政策。

2.1.2 註冊中心之職責

註冊中心之職責如下：

(1)依據第 4、第 5 及第 6 章規定提供相關控制。

(2)依據第 3 章規定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、註冊中心的義務與責任。

(4) 告知用戶及信賴憑證者，當使用或接受憑證機構簽發之憑證，應遵守之憑證政策相關規定。

(5) 依據第 4、第 5 及第 6 章規定保護私密金鑰。

(6) 確實區分註冊中心本身之私密金鑰用途。註冊中心應依據 6.1.9 節規定使用私密金鑰，未經憑證機構同意，註冊中心本身之私密金鑰不能使用於憑證註冊以外作業。

2.1.3 用戶之義務

接受憑證機構簽發憑證的用戶應負以下義務：

(1) 遵守第 3 及第 4 章規定程序。

(2) 正確地使用憑證。

(3) 妥善地保管及使用私密金鑰。(以保證等級測試級簽發之憑證不做規定)

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

2.1.4 信賴憑證者之義務

使用憑證機構簽發憑證的信賴憑證者應負以下義務：

(1) 熟知憑證之適用範圍及保證等級。

(2) 依憑證之適用範圍使用憑證。

(3) 正確檢驗憑證之有效性。檢驗憑證時應使用符合相關國際標準（如 X.509 標準或 IETF RFC 3280 等）定義之憑證驗證方法完整地檢驗憑證路徑。

(4) 正確查驗憑證廢止及停用清冊。

2.1.5 儲存庫服務之義務

憑證機構的儲存庫服務應負以下義務：

(1) 定期公佈所簽發之憑證。

(2) 定期公佈已廢止及已停用之憑證資訊。

(3) 公佈憑證政策及憑證實務作業基準的最新資訊。

(4) 儲存庫之存取控制必須依照 2.6.3 節規定。

2.2 法律責任

2.2.1 憑證機構之責任

2.2.1.1 保證範圍及其限制條件

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

2.2.1.2 否認聲明及其限制條件

憑證機構得在憑證實務作業基準中載明否認聲明及其限制條件(Disclaimers and Limitations)，以排除上述限制條件以外的責任。但憑證機構不得將因自行疏忽所引起之後果列入排除條件中。

2.2.1.3 其他除外條款

因不可抗拒事件及其他非可歸責於憑證機構之事由，包括天災、意外、突發、特定事件等所導致之損害事件，憑證機構得在憑證實務作業基準中載明其他除外條款，但憑證機構不得將因自行疏忽所引起

之錯誤列入排除條件中。

2.2.2 註冊中心之責任

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

2.2.2.1 保證範圍及限制條件

不做規定。

2.2.2.2 否認聲明及限制條件

不做規定。

2.2.2.3 其他除外條款

不做規定。

2.3 財務責任

2.3.1 對用戶及信賴憑證者之賠償責任

憑證機構之憑證實務作業基準應載明對用戶及信賴憑證者的賠償責任。

2.3.2 行政程序

由憑證機構之主管機關決定憑證機構的行政程序。

2.4 詮釋及施行

當本憑證政策有繁體中文以外語文版本時，若發生其他語文版本

與繁體中文版本不一致情形時，以繁體中文版本為準。

2.4.1 適用法律

本憑證政策依循我國相關法規，如有爭議時，本憑證政策條文之解釋應以我國相關法規為準。

2.4.2 可分割性、存續、合併及公告通知

如本憑證政策的任一章節不正確或無效時，其他章節仍然有效，憑證政策的修訂依照 8.1 節規定。

2.4.3 紛爭之處理程序

當對憑證政策內容之解釋有爭議時，爭議之雙方應儘量自行協商以取得共識。若協商不成，可依本會另訂之爭端解決程序，請求解釋。憑證機構應在憑證實務作業基準中載明紛爭之處理程序。

2.5 費用

2.5.1 憑證簽發、展期費用

不做規定。

2.5.2 憑證查詢費用

不做規定。

2.5.3 憑證廢止、狀態查詢費用

不做規定。

2.5.4 其他服務費用

不做規定。

2.5.5 請求退費之程序

不做規定。

2.6 公佈及儲存庫

2.6.1 憑證機構之資訊公佈

憑證機構應在固定的儲存庫公佈：

(1)憑證實務作業基準。

(2)憑證廢止清冊(或提供線上憑證狀態查詢)。

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

(4)簽發之所有憑證(包括簽發給其他憑證機構之憑證)。

(5)簽發之憑證機構廢止清冊(如憑證機構簽發憑證給其他憑證機構)。

(6)隱私權保護政策。

除上述資訊外，憑證機構應公佈可驗證數位簽章之必要資訊。

憑證機構之憑證實務作業基準應載明儲存庫暫停服務時間之上限。

2.6.2 公佈頻率

憑證廢止清冊之公佈頻率應依照 4.4 節規定辦理。

2.6.3 存取控制

(1) 憑證政策與憑證機構之憑證實務作業基準的取得不需存取控制。

(2)憑證由憑證機構自行決定是否需存取控制。

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

2.6.4 儲存庫

依照 1.3.5 節規定，儲存庫可由憑證機構或其他機構營運，憑證機構之憑證實務作業基準應載明儲存庫之相關資訊。

2.7 稽核方法

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

2.7.1 稽核之頻率

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

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

本會必要時得對與總管理中心互通的下屬憑證機構(含其下屬憑證機構)進行不定期稽核。本會進行不定期稽核時應說明理由。

2.7.2 稽核人員之身分及資格

稽核人員應獨立於被稽核的憑證機構外，可由以下個體擔任：

(1)第三公正人員。

(2)在組織劃分上與被稽核的憑證機構有所區別的另一獨立個體。

稽核人員應提供公正及獨立的評估，其資格認定必須經本會核可，且熟悉憑證機構簽發、管理憑證的相關規定。憑證機構於稽核時應對稽核人員進行身分識別。

2.7.3 稽核人員及被稽核方之關係

依照 2.7.2 節規定，稽核人員應獨立於被稽核的憑證機構外。

2.7.4 稽核之範圍

稽核之範圍如以下規定：

(1)憑證機構是否遵照憑證實務作業基準運作。

(2)憑證機構之憑證實務作業基準是否符合憑證政策之規定。

稽核人員可對憑證機構之相關維運單位如註冊中心進行稽核。

如憑證機構與其下屬憑證機構簽訂交互認證協議書時，則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。

2.7.5 對於稽核結果之因應方式

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

(1)稽核人員應記錄不符合情形。

(2)稽核人員應通知發生不符合情形憑證機構之主管機關，如不符合情形為嚴重缺失，稽核人員應立即通知本會。

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

依不符合情形的種類與嚴重性及完成修正所需時間，本會得暫停總管理中心的營運、廢止總管理中心簽發給下屬憑證機構的憑證或其他配合的行動，相關程序由本會另訂之。

2.7.6 稽核結果公開之範圍

除可能導致系統被攻擊之資訊外，與信賴憑證者信賴該憑證的相關資訊，均應公開提供。

憑證機構應公佈最近 1 次的稽核結果。

2.8 資訊保密之範圍

2.8.1 機密之資訊種類

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

(2)用於憑證機構營運的私密金鑰及通行碼皆為機密資訊，不得公開。

(3)稽核紀錄除 2.7.6 節規定情形外，不得被完整公開。

憑證機構之憑證實務作業基準中應載明機密之資訊種類。

2.8.2 非機密資料之種類

(1)憑證、憑證廢止清冊及廢止或停用資訊不應視為機密資訊。

(2)識別資訊或記載於憑證的資訊，除特別約定外，不應視為機密資訊。

憑證機構之憑證實務作業基準應載明非機密資料之種類。

2.8.3 憑證廢止或暫時停用資訊之公開

憑證廢止或暫時停用資訊屬於非機密資訊，應對外公開。

2.8.4 應司法人員要求釋出資訊

憑證機構之憑證實務作業基準應訂定有關提供司法人員 2.8.1 節機密資訊之相關規定。

2.8.5 應民事訴訟要求釋出資訊

憑證機構之憑證實務作業基準應訂定有關提供民事訴訟 2.8.1 節機密資訊之相關規定。

2.8.6 應用戶要求釋出資訊

憑證機構之憑證實務作業基準應訂定有關提供用戶 2.8.1 節機密資訊之相關規定。

2.8.7 其他資訊釋出之情形

依相關法令規定辦理。

2.9 智慧財產權

本憑證政策之智慧財產權由本會及中華電信股份有限公司(以下簡稱中華電信公司)共同擁有，本會及中華電信公司保有本憑證政策的所有權利。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，必須保證是完整複製，並註明著作權為本會及中華電信公司所擁有。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。本會及中華電信公司對於

不當使用或散布本憑證政策所引發之一切結果，不負任何法律責任。

3 識別及鑑別程序

3.1 初始註冊

3.1.1 命名種類

本基礎建設的憑證主體名稱應為 X.500 唯一識別名稱(Distinguished Name，DN)。

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

3.1.2 命名須有意義

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

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

3.1.3 命名形式之解釋規則

命名形式之解釋規則由本會負責建立，並包含在憑證格式剖繪中。

3.1.4 命名之獨特性

憑證主體名稱在本基礎建設中必須具獨特性，本會負責建立憑證機構使用 X.500 名稱空間(Name Space)相關規範，以確保名稱命名的獨特性，憑證機構必須在憑證實務作業基準中載明如何使用 X.500 名稱空間，同時對於同名的憑證主體在命名時如何確保憑證主體名稱的獨特性(例如同一縣市中同名的兩個人向憑證機構申請憑證，憑證機構如何確保這兩個人各自擁有獨特的憑證主體名稱)。

3.1.5 命名爭議之解決程序

命名所有權依我國相關法令規定之命名規則辦理(例如公司法、姓名法、國民教育法等)，憑證機構應於憑證實務作業基準中訂定命名爭議之解決程序，依照保證等級測試級運作之憑證機構則不做規定。

本會為本基礎建設命名爭議的仲裁機構。

3.1.6 商標之辨識、鑑別及角色

若憑證主體名稱包含商標時，則其命名必須符合我國商標相關法規。

3.1.7 證明擁有私密金鑰之方式

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

不同的金鑰產製者必須採用不同的方法來證明擁有私密金鑰，憑

證政策認可之證明方法有以下 3 種方式：

(1)由憑證機構或註冊中心為用戶產製金鑰對時：

用戶不必證明擁有私密金鑰，但必須依照 3.1.8、3.1.9 及 3.1.10 節規定接受身分鑑別，以取得私密金鑰及啟動資料，且私密金鑰應依照 6.1.2 節規定傳送給用戶。

(2)由可信賴的第三者(例如發卡中心)為用戶產製金鑰對時：

憑證機構或註冊中心必須依照 6.1.3 節規定透過安全管道向可信賴的第三者取得用戶之公開金鑰，用戶不必證明擁有相對應之私密金鑰，但必須依照 3.1.8、3.1.9 及 3.1.10 節規定接受身分鑑別，以取得私密金鑰及啟動資料，且私密金鑰應依照 6.1.2 節規定傳送給用戶。

(3)由用戶自行產製金鑰對時：

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

3.1.8 組織身分鑑別之程序

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

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	不做規定。
第 1 級	(1)可不做書面證件核對。 (2)只要申請者具有自己的電子郵件地址即可申請憑證，可不進行鑑別確認程序。 (3)不需臨櫃辦理。
第 2 級	(1)可不做書面證件核對。 (2)用戶提交組織資料，例如組織識別碼(如營利事業統一編號)、組織名稱等，應與憑證機構認可之資料進行比對。 (3)不需臨櫃辦理。
第 3 級	組織身分鑑別分為以下兩種情形： (1)政府機關(構)或單位之身分鑑別 政府機關(構)或單位必須以正式公文書申請憑證，而憑證機構或註冊中心必須確認該機關(構)或單位確實存在，並驗證公文書之真確性。 (2)民間組織之身分鑑別 申請資料應包括組織名稱、所在地及代表人名稱等足以識別該組織之資料。憑證機構或註冊中心除需驗證申請資料及代表人身分的真實性外，並應驗證該代表人有權以該組織之名義申請憑證。申請時應由代表人親臨憑證機構或註冊中心辦理，如代表人無法親自臨櫃申請，得以書面委託書委任代理人代為臨櫃申請，但憑證機構或註冊中心必須確認該委託書之真偽(例如比對委託書上之代表人印鑑章)，並依 3.1.9 節中保證等級第三級之規定鑑別代理人之身分。

保證等級	組織身分鑑別之程序
	民間組織如於申請憑證前已依法完成向主管機關設立登記程序或已於憑證機構、註冊中心或憑證機構信賴之機構或個人（例如公證人）完成符合上述規定之臨櫃識別與鑑別程序，並且留下登記或識別與鑑別之佐證資料（例如留下印鑑章圖記或由公證人在申請書上加蓋認證戳記等），則憑證機構或註冊中心得允許該組織於申請憑證時出示佐證資料來取代上述識別與鑑別方式。憑證機構必須評估採信佐證資料之風險，確認其風險不會大於採用上述識別與鑑別程序之風險，且憑證機構或註冊中心必須具有鑑別佐證資料之能力時，才可接受以佐證資料取代識別與鑑別方式申請憑證。 以上所稱民間組織係指私法人、非法人團體或以上兩者之附屬組織。
第 4 級	組織身分鑑別分為以下兩種情形： (1)政府機關(構)或單位之身分鑑別 政府機關(構)或單位必須以正式公文書指派憑證機構或註冊中心可鑑別之個人，代表該機關(構)或單位親臨憑證機構或註冊中心申請憑證，憑證機構或註冊中心應確認該機關(構)或單位確實存在，並驗證公文書之真確性，並依 3.1.9 節中保證等級第 4 級之規定鑑別代表該機關(構)或單位之個人之身分。 (2)民間組織之身分鑑別 申請資料應包括組織名稱、所在地及代表人名稱等足以識別該組織之資料。憑證機構或註冊中心除需驗證申請

保證等級	組織身分鑑別之程序
	資料及代表人身分的真實性外，並應驗證該代表人有權以該組織之名義申請憑證。申請時應由代表人親臨憑證機構或註冊中心辦理。 以上所稱民間組織係指私法人、非法人團體或以上兩者之附屬組織。

簽發憑證機構對主體憑證機構之識別與鑑別程序應比照上述對組織之識別與鑑別程序，且不得低於主體憑證機構所欲簽發憑證的保證等級。

總管理中心對於政府機關(構)或單位所設立之下屬憑證機構之身分鑑別，至少應依照保證等級第 3 級以上之政府機關(構)或單位之身分鑑別之程序辦理。

3.1.9 個人身分鑑別之程序

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

表 3-2 個人身分鑑別程序

保證等級	個人身分鑑別之程序
測試級	不做規定。
第 1 級	(1)可不做書面證件核對。 (2)只要申請者具有自己的電子郵件地址即可申請憑證，可

保證等級	個人身分鑑別之程序
	不進行鑑別確認程序。 (3)不需臨櫃辦理。
第 2 級	(1)可不做書面證件核對。 (2)用戶提交個人資料，例如個人識別碼(如身分證字號)、姓名等，應與憑證機構認可之資料進行比對。 (3)不需臨櫃辦理。
第 3 級	(1)核對書面證件： 在申請憑證時，用戶至少應出示 1 張被認可並附照片之證件正本(例如國民身分證)，供憑證機構或註冊中心鑑別用戶之身分。 如用戶(例如未成年人)無上述之附照片證件，可使用由政府發給之足以證明用戶身分的書面證明文件(例如戶口名薄)取代，並由 1 位具行為能力之成年人以書面保證用戶之身分；出具書面保證之成年人之身分必須經過上述之鑑別。 (2)用戶提交之個人資料，例如個人的識別碼(如身分證字號)、姓名及地址(如戶籍地址)等，應與該資料主管機關的登記資料(如戶籍資料)或其它經主管機關認可之可信賴第三者的登記資料進行比對。 (3)臨櫃辦理： 用戶必須親臨憑證機構或註冊中心證明其身分。若用戶無法親自臨櫃辦理，得以書面委託書委任代理人代為臨櫃申請，但憑證機構或註冊中心必須確認該委託書之真偽(例如比對委託書上之用戶印鑑章)，並依上述規定鑑別代理人之身分。

保證等級	個人身分鑑別之程序
	個人如於申請憑證前已於憑證機構、註冊中心或憑證機構信賴之機構或個人（例如公證人）完成符合上述規定之臨櫃識別與鑑別程序，並且留下識別與鑑別之佐證資料（例如留下生物識別資料、印鑑章圖記或由公證人在申請書上加蓋認證戳記），則憑證機構或註冊中心得允許該人於申請憑證時出示佐證資料來取代上述識別與鑑別方式。憑證機構必須評估採信佐證資料之風險，確認其風險不會大於採用上述識別與鑑別程序之風險，且憑證機構或註冊中心必須具有鑑別佐證資料之能力時，才可接受以佐證資料取代識別與鑑別方式申請憑證。
第 4 級	(1)核對書面證件： 在申請憑證時，用戶應至少出示 1 張被認可並附照片之證件(例如國民身分證)正本，供憑證機構或註冊中心鑑別用戶之身分。 (2)用戶提交之個人資料，例如個人的識別碼(如身分證字號)、姓名及地址等(如戶籍地址)，應與該資料主管機關的登記資料(如戶籍資料)進行比對。 (3)臨櫃辦理，用戶必須親臨憑證機構或註冊中心證明其身分。

3.1.10 硬體裝置或伺服軟體鑑別之程序

電腦及通訊設備(如路由器、防火牆等)或伺服軟體(如Web Server)，因在法律上不具行為能力，必須由組織或個人以設備管理者

的身分提出憑證申請；對於組織或個人的身分鑑別方式應依照3.1.8或3.1.9節規定辦理。

申請憑證時應提供以下資訊：

(1) 設備或伺服軟體的識別資訊。

(2) 設備或伺服軟體的公開金鑰(依照 6.1.3 節規定提供)。

(3) 設備或伺服軟體的授權及屬性(如授權或屬性需被包含在憑證中才需提供)。

(4) 提出憑證申請之組織或個人之聯絡資訊。

3.2 憑證之金鑰更換及展期

3.2.1 憑證之金鑰更換

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

對於憑證機構的憑證而言，當主體憑證機構申請更換金鑰對時，簽發憑證機構應依照3.1節初始註冊之鑑別程序對主體憑證機構進行識別及鑑別。

對於終端個體的憑證而言，當用戶申請更換金鑰對時，憑證機構應依表3-3之規定對用戶進行識別與鑑別。

3.2.2 憑證展期

憑證展期係指簽發1張與舊憑證具有相同憑證主體名稱、金鑰及相關資訊的新憑證，憑證的有效期限予以展延，並給予1個新的序號。如憑證之金鑰對尚未達到使用期限(依照6.3.2節規定)、私密金鑰無立

即被破解之虞及用戶名稱、屬性沒有改變，則允許申請憑證展期。

對於憑證機構的憑證而言，當主體憑證機構申請憑證展期時，簽發憑證機構應依照3.1節初始註冊之鑑別程序對主體憑證機構進行識別及鑑別。

對於終端個體的憑證而言，當用戶申請憑證展期時，憑證機構應依表3-3之規定對用戶進行識別與鑑別。

表3-3憑證金鑰更換與展期身分鑑別規定

保證等級	對用戶憑證更換金鑰或展期的鑑別要求
測試級	不做規定。
第1級	用戶的身分可使用有效的簽章金鑰進行鑑別或依照3.1節初始註冊之鑑別程序進行鑑別。
第2級	用戶的身分可使用有效的簽章金鑰進行鑑別或依照3.1節初始註冊之鑑別程序進行鑑別，但如與初始註冊時間間隔超過15年時，則應依照3.1節初始註冊之鑑別程序進行鑑別。
第3級	用戶的身分可使用有效的簽章金鑰進行鑑別或依照3.1節初始註冊之鑑別程序進行鑑別，但如與初始註冊時間間隔超過9年時，則應依照3.1節初始註冊之鑑別程序進行鑑別。
第4級	用戶的身分可使用有效的簽章金鑰進行鑑別或依照3.1節初始註冊之鑑別程序進行鑑別，但如與初始註冊時間間隔超過3年時，則應依照3.1節初始註冊之鑑別程序進行鑑別。

3.3 憑證廢止之金鑰更換

憑證廢止後，新憑證的簽發應依照3.1節規定，用戶必須重新辦理初始註冊程序。

3.4 憑證廢止

憑證機構或註冊中心必須對於憑證廢止申請進行鑑別，憑證機構應依照4.4節規定在憑證實務作業基準中載明申請者之身分鑑別方式，以確認申請者為有權提出憑證廢止之申請者。

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

4 營運規範

4.1 申請憑證之程序

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

為確保電子化政府相關時戳服務的互通性及可信賴性，政府機關所設立的時戳服務機構（Time Stamp Authority，TSA）之運作必須符合「政府機關公開金鑰基礎建設時戳政策」的規定，始得向本基礎建設之憑證機構申請時戳類伺服器應用軟體憑證。本基礎建設之憑證機構受理時戳類伺服器應用軟體憑證之申請時，必須先確認其時戳服務實務作業基準（Practice Statement for the Time Stamp Authority）已通過符合「政府機關公開金鑰基礎建設時戳政策」的審核。

總管理中心需接受目的事業主管機關依據電子化政府電子認證服務分工所設立之憑證機構申請憑證，以成為本基礎建設之第 1 層下屬憑證機構，其申請程序由本會另訂之，並公佈於總管理中心之憑證實務作業基準。

本基礎建設外之憑證機構向總管理中心申請交互憑證(Cross-Certificate)的程序由本會另訂之。

本基礎建設中所有層級之下屬憑證機構，除非經其上層憑證機構之同意，否則不得接受其他憑證機構申請成為其下層憑證機構。

4.2 簽發憑證之程序

憑證機構簽發憑證應依照 5.2 節及憑證實務作業基準的規定，由適當人員執行憑證簽發之相關任務，憑證簽發後憑證機構或註冊中心

應以適當方式通知申請者。以保證等級第 1、第 2、第 3 及第 4 級運作之憑證機構，應於憑證實務作業基準中載明憑證簽發後通知申請者的方式。

憑證機構或註冊中心如不同意簽發憑證，應以適當方式通知憑證申請者，並明確告知不同意簽發的理由。除因申請者之身分識別與鑑別之原因外，憑證機構得因其他原因不同意簽發憑證。以保證等級第 1、第 2、第 3 及第 4 級運作之憑證機構，應於憑證實務作業基準中載明不同意簽發憑證之通知方式。

總管理中心應簽發 1 張自簽憑證(Self-Signed Certificate)，此憑證經本會確認內容無誤後，依照 6.1.4 節規定將憑證傳送給信賴憑證者。

4.3 接受憑證之程序

簽發保證等級第 2、第 3 及第 4 級憑證之憑證機構在簽發憑證後，應經憑證申請者審視憑證內容並接受所簽發的憑證後，始得將簽發之憑證公佈到儲存庫上。若憑證申請者審視憑證內容後，拒絕接受所簽發的憑證，則憑證機構應廢止該憑證。以保證等級第 2、第 3 及第 4 級運作之憑證機構，應於憑證實務作業基準中載明以下事項：

(1) 憑證申請者確認憑證接受或拒絕的方式。

(2) 憑證申請者在決定接受憑證前應審視的憑證欄位。

(3) 憑證申請者拒絕接受憑證之處理方式。

上述憑證申請者在決定接受憑證前應審視的憑證欄位，至少應包括憑證主體名稱。憑證申請者拒絕接受憑證之處理方式，如涉及收費或退費問題時，應依據消費者保護法及公平交易原則訂定。

總管理中心的自簽憑證必須由本會確認其內容後，始得依照 6.1.4 節規定散佈給信賴憑證者。

4.4 憑證暫時停用及廢止

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

憑證機構對於憑證暫時停用及廢止應符合以下規定：

1. 以保證等級第 1 及第 2 級運作的憑證機構，至少應於政府機關法定上班時間內，提供憑證廢止服務。

2. 以保證等級第 3 及第 4 級運作的憑證機構，提供的憑證暫時停用及廢止服務應符合以下規定之一：

   (1)提供全天候的憑證廢止服務。

   (2)提供全天候的憑證暫時停用服務。

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

提供憑證暫時停用服務之憑證機構應同時提供憑證恢復使用服務，並於憑證實務作業基準中載明憑證暫時停用服務及憑證恢復使用服務之提供方式、憑證暫時停用申請程序、憑證恢復使用申請程序、申辦地點或網址等。

憑證廢止及停用後，憑證機構最遲應於下次預定公佈憑證機構廢止清冊或憑證廢止清冊時，將廢止及停用的憑證列入憑證機構廢止清

冊或憑證廢止清冊中，並公告於儲存庫上；公告的憑證狀態資訊應包括廢止及停用的憑證，直到這些憑證到期或被復用為止。

4.4.1 廢止憑證之事由

以下 3 種情形應廢止憑證：

(1) 如用戶的私密金鑰證實或懷疑遭破解(例如用戶儲存私密金鑰的 IC 卡遺失)。

(2) 如憑證機構的私密金鑰證實遭破解時，則以該私密金鑰簽發的憑證應廢止。

(3) 如憑證的用戶資料或屬性變更(例如用戶名稱變更、用戶證號或代碼變更、用戶身分因解散或死亡而消失等)，但憑證機構的憑證所記載之憑證主體資訊必須變更時，必須由本會評估是否同意廢止該憑證機構的憑證。

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

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

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

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

如憑證機構證實與其交互認證之憑證機構違反憑證政策或本身之憑證實務作業基準時，得逕行廢止該憑證機構的交互認證憑證。

如本會決定總管理中心的自簽憑證必須廢止時(例如懷疑總管理中心的私密金鑰遭破解)，得逕行廢止總管理中心的自簽憑證。

4.4.2 憑證廢止之申請者

當發生 4.4.1 節規定應廢止憑證或其他情形時，用戶或擁有私密金鑰的個體得於憑證有效期限內，向憑證機構或註冊中心提出憑證廢止申請。

憑證機構依照 4.4.1 節規定，得逕行廢止用戶、下屬憑證機構或交互認證憑證機構之憑證。

4.4.3 憑證廢止之程序

在收到憑證廢止申請後，憑證機構或註冊中心應依照 3.4 節及憑證實務作業基準規定，對申請者進行身分識別及鑑別，若身分識別及鑑別無誤，則除憑證機構的金鑰被破解外，原則上憑證機構或註冊中心皆應核准其申請。

如同意憑證廢止申請或決定逕行廢止憑證，則憑證機構或註冊中心應依照 5.2 節及憑證實務作業基準規定，由適當人員執行憑證廢止之相關任務，憑證廢止後憑證機構或註冊中心應以適當的方式通知用戶。以保證等級第 1、第 2、第 3 及第 4 級運作的憑證機構，應於憑證實務作業基準中載明憑證廢止後通知用戶的方式。

如不同意廢止憑證，則憑證機構或註冊中心應以適當方式通知用

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

4.4.4 憑證廢止申請之處理期間

憑證機構應於憑證實務作業基準中載明處理廢止憑證請求之期間。

4.4.5 暫時停用憑證之事由

憑證機構可視需要提供憑證暫時停用服務及憑證恢復使用服務，相關規定應於憑證實務作業基準中載明。

4.4.6 暫時停用憑證之申請者

提供憑證暫時停用服務及憑證恢復使用服務的憑證機構應於憑證實務作業基準中載明憑證暫時停用及憑證恢復使用之申請者資格。

4.4.7 暫時停用憑證之程序

提供憑證暫時停用服務及憑證恢復使用服務的憑證機構應於憑證實務作業基準中載明憑證暫時停用及憑證恢復使用之申請程序。

4.4.8 暫時停用憑證之處理期間及停用期間

提供憑證暫時停用服務及憑證恢復使用服務的憑證機構應於憑證實務作業基準中載明處理憑證暫時停用請求及憑證恢復使用請求之期間及暫時停用憑證之期間。

4.4.9 憑證機構廢止清冊及憑證廢止清冊之簽發頻率

總管理中心應簽發憑證機構廢止清冊(CARL)，下屬憑證機構及交互認證憑證機構應簽發憑證機構廢止清冊或憑證廢止清冊(CRL) 。在簽發憑證機構廢止清冊或憑證廢止清冊前，應檢查其內容，確認資訊之正確性。例如，使用軟體掃瞄憑證機構廢止清冊或憑證廢止清冊，以檢查資料之正確性。憑證機構廢止清冊或憑證廢止清冊應定期發佈，即使憑證狀態沒有改變也要簽發，以確保憑證狀態資訊的即時性。

憑證狀態資訊之公告應在下 1 次憑證狀態資訊更新時完成，如此將有助於離線或遠端作業的應用系統，將憑證狀態資訊儲存成近端快取(Local Cache)。憑證機構應加強與儲存庫間之配合，降低從憑證狀態資訊產生到公告於儲存庫的時間，憑證實務作業基準應規定以那 1 個儲存庫為主，以便用戶可以到該儲存庫取得最新的憑證狀態資訊。

當憑證狀態資訊公告時，過時的憑證狀態資訊應自儲存庫中移除。下表說明憑證機構廢止清冊及憑證廢止清冊之簽發頻率相關規定。

表 4-1 憑證機構廢止清冊及憑證廢止清冊之簽發頻率

保證等級	憑證機構廢止清冊之簽發頻率	憑證廢止清冊之簽發頻率
測試級	不適用	不做規定
第 1 級	不適用	不做規定
第 2 級	不適用	每 3 天至少 1 次

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

4.4.10 憑證機構廢止清冊及憑證廢止清冊之查驗規定

使用保證等級第 2、第 3 及第 4 級憑證的信賴憑證者，必須在使用憑證前查詢目前的憑證機構廢止清冊和憑證廢止清冊，以查驗憑證目前的狀態，同時也必須驗證憑證機構廢止清冊和憑證廢止清冊的真偽和完整性。信賴憑證者必須考量承擔的風險、責任及影響，自行決定間隔多久去取得新的憑證廢止資訊，相關義務依照 2.1.4 節規定。

4.4.11 線上憑證狀態查詢服務

憑證機構除提供憑證機構廢止清冊或憑證廢止清冊服務外，還可選擇性地提供信賴憑證者之線上憑證狀態查詢功能。使用線上憑證狀態查詢之用戶可不需取得或處理憑證機構廢止清冊或憑證廢止清冊。憑證機構應在憑證實務作業基準中載明，是否提供及如何提供線上憑證狀態查詢服務。

4.4.12 線上憑證狀態查詢之規定

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

4.4.13 其他形式廢止公告

不做規定。

4.4.14 其他形式廢止公告之檢查規定

不做規定。

4.4.15 金鑰被破解時之其他特殊規定

金鑰被破解時，請依照 4.4.1、4.4.2 及 4.4.3 節相關規定處理。

4.5 安全稽核程序

以保證等級測試級運作之憑證機構得不具備安全稽核功能，簽發其他保證等級憑證之憑證機構，對於安全相關事件應具備適當的安全稽核紀錄(Audit Log)功能。安全稽核紀錄應儘可能由系統自動產生，如無法由系統自動產生，亦可使用工作記錄本、紙張或其他實體機制。所有安全稽核紀錄不論是電子或非電子的，均應妥善保存，並且在執行稽核時可立即正確取得。安全稽核紀錄之維護應依照 4.6.2 節歸檔保留期限規定辦理。

4.5.1 被記錄事件種類

憑證機構之安全稽核功能，應包括憑證管理系統及憑證管理系統所依存的電腦作業系統(Operation System)的安全稽核。每筆稽核記錄至少應包括以下項目(不論是自動或手動記錄的稽核事件)：

(1) 事件種類。

(2) 引起事件的個體和操作者之身分。

(3) 事件發生之地點或位置

(4) 事件發生之時間和日期。

(5) 憑證機構執行憑證簽發及廢止程序之結果記錄(不論成功或失敗)。

當事件發生時，稽核記錄可由憑證機構自行決定以電子或實體方式記錄，下表說明依各保證等級運作之憑證機構應紀錄的稽核事件，由於這些稽核事件都是需要憑證機構加以記錄或加以回應處理的，所以又被稱為可稽核事件(Auditable Event)：

表 4-2 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的內容等		✓	✓	✓
A.1.2 任何嘗試刪除或修改稽核紀錄檔		✓	✓	✓
A.2 識別與鑑別				
A.2.1 嘗試新角色的設定不論成功或失敗		✓	✓	✓
A.2.2 身分鑑別嘗試的最高容忍次數改變		✓	✓	✓

可稽核事件／保證等級	第 1 級	第 2 級	第 3 級	第 4 級
A.2.3 使用者登入系統時身分鑑別嘗試的失敗次數之最大值		✓	✓	✓
A.2.4 如管理者將已被鎖住的帳號解鎖，而且該帳號是因為多次失敗的身分鑑別嘗試而被鎖住的		✓	✓	✓
A.2.5 管理者改變系統的身分鑑別機制，例如從通行碼改為生物特徵值		✓	✓	✓
A.3 金鑰之產製				
A.3.1 當憑證機構產製金鑰時 (不限制在單次或只限 1 次使用的金鑰產生)	✓	✓	✓	✓
A.4 私密金鑰之載入和儲存				
A.4.1 載入私密金鑰到系統元件中	✓	✓	✓	✓
A.4.2 所有為進行金鑰回復工作，對保存在憑證機構的憑證主體之私密金鑰所做的存取	✓	✓	✓	✓
A.5. 可信賴公開金鑰之新增、刪除及儲存				
A.5.1 所有可信賴公開金鑰之改變，包括新增及刪除	✓	✓	✓	✓
A.6. 私密金鑰之輸出				
A.6.1 私密金鑰之輸出 (不包括只使用在單次或只限	✓	✓	✓	✓

可稽核事件／保證等級	第 1 級	第 2 級	第 3 級	第 4 級
1 次使用之金鑰)				
A.7. 憑證之註冊				
A.7.1 所有憑證之註冊申請過程	✓	✓	✓	✓
A.8. 廢止之憑證				
A.8.1 所有憑證之廢止申請過程		✓	✓	✓
A.9. 憑證狀態改變之核可				
A.9.1 核可或拒絕憑證狀態改變之申請		✓	✓	✓
A.10. 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關之組態設定改變		✓	✓	✓
A.11. 帳號之管理				
A.11.1 加入或刪除角色和使用者	✓	✓	✓	✓
A.11.2 使用者帳號或角色之存取權限修改	✓	✓	✓	✓
A.12. 憑證格式剖繪之管理				
A.12.1 所有憑證格式剖繪之改變	✓	✓	✓	✓
A.13. 憑證機構廢止清冊及廢止清冊格式剖繪之管理				
A.13.1 所有憑證機構廢止清冊及憑證廢止清冊格式剖繪之改變		✓	✓	✓

可稽核事件／保證等級	第 1 級	第 2 級	第 3 級	第 4 級
A.14. 其他				
A.14.1 安裝作業系統		✓	✓	✓
A.14.2 安裝憑證機構系統		✓	✓	✓
A.14.3 安裝硬體密碼模組			✓	✓
A.14.4 移除硬體密碼模組			✓	✓
A.14.5 銷毀硬體密碼模組		✓	✓	✓
A.14.6 啟動系統		✓	✓	✓
A.14.7 嘗試登入憑證機構的應用作業		✓	✓	✓
A.14.8 硬體及軟體之接收			✓	✓
A.14.9 嘗試設定通行碼		✓	✓	✓
A.14.10 嘗試修改通行碼		✓	✓	✓
A.14.11 憑證機構之內部資料備份		✓	✓	✓
A.14.12 憑證機構之內部資料回復		✓	✓	✓
A.14.13 檔案操作(例如產生、重新命名及移動等)			✓	✓
A.14.14 傳送任何資訊到儲存庫公佈			✓	✓
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		✓	✓	✓

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

可稽核事件／保證等級	第 1 級	第 2 級	第 3 級	第 4 級
A.17.6 設備失效	✓	✓	✓	✓
A.17.7 電力不當			✓	✓
A.17.8 不斷電系統(UPS) 失敗			✓	✓
A.17.9 明顯及重大的網路服務或存取失敗			✓	✓
A.17.10 憑證政策之違反	✓	✓	✓	✓
A.17.11 憑證實務作業基準之違反	✓	✓	✓	✓
A.17.12 重設系統時鐘		✓	✓	✓

4.5.2 紀錄檔處理頻率

稽核紀錄應依據下表進行檢視，並且在稽核報表中對重大事件加以解釋。檢視工作應包括驗證稽核紀錄是否被竄改、檢視所有的紀錄項目及檢查任何警示或異常等。因應稽核檢視之結果所採取的行動亦應以文件記錄。

表 4-3 稽核記錄檔處理頻率

保證等級	紀錄檔之處理頻率
測試級	不做規定
第 1 級	不做規定。
第 2 級	不做規定。
第 3 級	至少每兩個月 1 次。 憑證機構自上次稽核檢視後所發生的重大安全稽核

保證等級	紀錄檔之處理頻率
	紀錄應加以檢視，並且對任何可能之惡意活動應進一步調查。
第 4 級	至少每個月 1 次。 憑證機構自上次稽核檢視後所發生的重大安全稽核紀錄應加以檢視，並且對任何可能之惡意活動應進一步調查。

4.5.3 稽核紀錄檔保留期限

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

以保證等級第 2、第 3 及第 4 級憑證運作的憑證機構，稽核紀錄檔應在憑證機構所在處至少保留兩個月，並依照 4.5.4、4.5.5、4.5.6 及 4.6 節記錄保留管理機制等相關規定辦理。

當稽核紀錄檔的保留期限屆滿時，如須移除該資料，必須由稽核員移除，不可由其他人員代理。

4.5.4 稽核紀錄檔之保護

以保證等級測試級及第 1 級運作的憑證機構，稽核紀錄檔的保護不做規定。

以保證等級第 2、第 3 及第 4 級運作的憑證機構，電子稽核日誌

系統(Electronic Audit Log System)必須包含保護機制，手動的稽核資訊亦應加以保護，以確保不會遭未經授權的閱讀、修改及刪除。

4.5.5 稽核紀錄檔備份程序

表 4-4 稽核紀錄檔備份程序

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

4.5.6 安全稽核系統

稽核系統可以在憑證管理系統之內部或外部。稽核程序應在憑證管理系統啟動時啟用，唯有在憑證管理系統關閉時才停止。

如自動稽核系統無法正常運作，及保護系統資料之完整性、機密性的安全機制處於高風險狀態時，應決定是否暫停憑證管理系統運作，直到問題解決後再行提供服務。

4.5.7 對引起事件者之告知

當事件發生而被稽核系統紀錄時，稽核系統並不需要告知引起該

事件的個體其所引發的事件已經被系統所紀錄。

4.5.8 弱點評估

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

4.6 紀錄歸檔之方法

4.6.1 紀錄事件之類型

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

表 4-5 歸檔記錄資料

應歸檔資料／保證等級	第 1 級	第 2 級	第 3 級	第 4 級
憑證機構被稽核驗證(Accreditation)的資料(假設適用)	✓	✓	✓	✓
憑證實務作業基準	✓	✓	✓	✓
重要契約	✓	✓	✓	✓
系統與設備組態設定	✓	✓	✓	✓
系統或組態設定修改與更新的內容	✓	✓	✓	✓
憑證申請資料	✓	✓	✓	✓
廢止申請資料		✓	✓	✓

應歸檔資料／保證等級	第 1 級	第 2 級	第 3 級	第 4 級
3.1.9 節訂定的用戶身分識別資料		✓	✓	✓
文件的簽收及憑證的接受		✓	✓	✓
符記啟用紀錄		✓	✓	✓
所有已簽發或公告的憑證	✓	✓	✓	✓
憑證機構金鑰更換的紀錄	✓	✓	✓	✓
所有被簽發或公告的憑證機構廢止清冊和憑證廢止清冊		✓	✓	✓
所有稽核記錄	✓	✓	✓	✓
用來驗證及佐證歸檔內容的其它說明資料或應用程式		✓	✓	✓
稽核人員所要求的文件		✓	✓	✓

4.6.2 歸檔之保留期限

歸檔資料的最低保留期限規定如下：

表 4-6 歸檔資料保留期限

保證等級	最低保留期限
測試級	不做規定
第 1 級	3 年
第 2 級	5 年
第 3 級	10 年
第 4 級	20 年

如使用的儲存媒體無法達到上述的保留期限規定，則必須建立定期將歸檔資料轉換到新的儲存媒體之機制。同時用來處理歸檔資料的應用程式也必須被維護一定期間(時間長短由該憑證機構的主管機關決定)。

在歸檔之保留期限屆滿時，憑證機構應提供歸檔資料及處理歸檔資料的應用程式給主管機關。

4.6.3 歸檔之保護

以保證等級測試級及第 1 級運作的憑證機構，歸檔資料之保護不做規定。

以保證等級第 2、第 3 及第 4 級運作的憑證機構，歸檔資料必須儲存在憑證機構以外的地方，並提供適當的保護，保護等級不可低於憑證機構所在處之保護等級。

4.6.4 歸檔備份程序

不做規定。

4.6.5 時戳紀錄之要求

不做規定。

4.6.6 歸檔資料彙整系統

不做規定。

4.6.7 取得及驗證歸檔資料之程序

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

4.7 金鑰更換

4.7.1 憑證機構之金鑰更換

憑證機構之私密金鑰必須依照 6.3.2 節規定定期更換。

如憑證機構本身的憑證被廢止後，其私密金鑰應停止使用，並需更換金鑰對。

總管理中心最遲應於自簽憑證到期前 3 個月，更換用來簽發憑證的金鑰對，並簽發 1 張新的自簽憑證。新的自簽憑證，應由本會確認內容後，依照 6.1.4 節規定傳送給信賴憑證者。

下層憑證機構最遲應於憑證到期前 2 個月，更換用來簽發憑證的金鑰對。下層憑證機構更換金鑰對後，應依照 4.1 節規定向上層憑證機構申請新的憑證。

4.7.2 用戶之金鑰更換

用戶之私密金鑰必須依照 6.3.2 節規定定期更換。

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

持有保證等級第 2、第 3 及第 4 級之用戶，如其憑證沒有被廢止，最遲必須在憑證到期前 1 個月內更換其金鑰對，並依照 4.1 節規定向

憑證機構或註冊中心申請新憑證。

4.8 金鑰遭破解或災變時之復原程序

憑證機構的災後復原工作應優先恢復儲存庫，使憑證狀態資訊能正常提供。

4.8.1 電腦資源、軟體或資料遭破壞之復原程序

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

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

4.8.2 憑證機構之簽章金鑰憑證被廢止之復原程序

以保證等級第 2、第 3 及第 4 級運作之憑證機構，應在憑證實務作業基準或相關的文件中載明憑證機構之簽章金鑰憑證被廢止時之復原程序，以迅速恢復憑證之簽發及管理作業能力。

以保證等級第 3 及第 4 級運作之憑證機構至少每年應進行 1 次憑證機構之簽章金鑰憑證被廢止之演習。

4.8.3 憑證機構之簽章金鑰遭破解之復原程序

以保證等級第 2、第 3 及第 4 級運作之憑證機構，應在憑證實務作業基準中或相關的文件中載明憑證機構之簽章金鑰遭破解時之復原程序，以迅速恢復憑證之簽發及管理作業能力。

以保證等級第3及第4級運作之憑證機構至少每年應進行1次憑證機構簽章金鑰遭破解之演習。

4.8.4 憑證機構安全設施之災後復原工作

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

以保證等級第3及第4級運作之憑證機構至少每年應進行1次災後復原計畫之演習。

4.9 憑證機構之終止服務

應依據電子簽章法相關規定進行憑證機構之終止服務。

5 非技術性安全控管

5.1 實體控管

5.1.1 實體所在及結構

除依照保證等級測試級及第 1 級運作之憑證機構不做規定外，依照保證等級第 2 級以上運作之憑證機構機房的實體所在及結構，必須符合儲存高重要性及敏感性資訊的機房設施水準，結合門禁、保全、入侵偵測及監視錄影等實體安全機制，以防止未經授權存取憑證機構之相關設備。

5.1.2 實體存取

除依照保證等級測試級及第 1 級運作之憑證機構不做規定外，依照保證等級第 2 級以上運作之憑證機構，在安裝及啟用密碼模組後，必須對憑證機構的設備進行實體控管，以防止遭受未經授權之存取。即使在沒有安裝或啟動密碼模組時，亦應對憑證機構的相關設備進行實體控管，以降低設備遭受非法開啟或破壞的風險。

各保證等級之實體控管規定說明如下：

依照保證等級第 1 及第 2 級運作之憑證機構之實體控管規定：

(1) 確保能防止未經授權之侵入。

(2)確保包含敏感性明文資料的可攜式儲存媒體和文件是保存在安全的場所。

依照保證等級第 3 及第 4 級運作之憑證機構之實體控管規定：

(1)建置全天候人工或電子式監控設備，以防止未經授權之侵入。

(2) 定期維護和檢視存取記錄檔。

(3)進行電腦系統和密碼模組實體控管時，必須至少兩人以上共同執行。

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

在離開憑證機構機房時，應查驗以下事項以防止憑證機構機房被未經許可人員接近：

(1) 必須適當地保全安全機箱。

(2) 實體安全系統(例如門鎖、出入門禁)運作正常。

5.1.3 電力及空調

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

5.1.4 水災防範及保護

憑證機構之設置地點必須免於受到水災損害。

5.1.5 火災防範及保護

除依照保證等級測試級及第 1 級運作之憑證機構不做規定外，依照保證等級第 2 級以上運作之憑證機構機房必須具備自動偵測火災預警功能，系統能自動啟動滅火設備，並設置手動開關於各主要出入口處，以供現場人員於緊急情況時以手動方式操作。

5.1.6 媒體儲存

除依照保證等級測試級及第 1 級運作之憑證機構不做規定外，依照保證等級第 2 級以上運作之憑證機構必須保護系統相關的儲存媒體免於遭受意外的損害(如水、火、電磁場等)。

5.1.7 廢料處理

不做規定。

5.1.8 異地備援

除依照保證等級測試級及第 1 級運作之憑證機構不做規定外，依照保證等級第 2 級以上運作之憑證機構相關系統必須定期進行異地備援，全部資料備份必須 1 個星期至少執行 1 次，其他週期排程必須於憑證實務作業基準中說明。

異地備援的地點必須與憑證機構機房距離 30 公里以上，備援的

內容至少包含資料與系統程式。當發生異常狀態時，必須具備恢復正常運作的能力。異地備援系統應與憑證機構系統具備相同的安全等級。

5.2 程序控管

5.2.1 信賴角色

憑證機構必須安排信賴角色負責執行相關任務，以作為憑證機構信賴的基礎，如因意外或人為疏失而未能達到安全目標，則可能降低憑證機構的公正性。憑證機構可採用以下 2 種方法增加安全性：

(1)保證擔任每種角色的人員已接受適當訓練且可充分信賴。

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

規定之信賴角色如下：

(1)管理員：安裝、設定和維護憑證機構相關系統，並負責建立和維護系統之用戶帳號及設定稽核參數和產生元件金鑰。

(2)簽發員：簽發憑證和廢止憑證。

(3)稽核員：查驗和維護稽核日誌。

(4)維運員：執行系統備份和故障排除。

5.2.1.1 管理員

管理員主要負責：

(1) 安裝、設定和維護憑證機構相關系統。

(2) 建立和維護系統之使用者帳號。

(3) 設定稽核參數。

(4) 產製和備份憑證機構之金鑰。

5.2.1.2 簽發員

簽發員主要負責：

(1) 登錄新用戶和受理憑證簽發申請。

(2) 核對用戶身分和憑證資訊的正確性。

(3) 審核和執行憑證簽發。

(4) 受理申請、審核和執行憑證廢止。

5.2.1.3 稽核員

稽核員主要負責：

(1) 對稽核記錄的查驗、維護和歸檔。

(2)執行或監督內部的稽核，以確認憑證機構維運遵照憑證實務作業基準的規定。

5.2.1.4 維運員

維運員主要負責：

(1)系統的實體安全控管(如機房的門禁管理、防火、防水、空調

系統等)。

(2) 系統設備的日常運作維護。

(3) 系統的備援及復原作業。

(4) 儲存媒體的更新。

(5) 系統軟硬體的更新。

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

5.2.2 角色分派

憑證機構之角色分派原則如下：

表5-1角色分派原則

保證等級	角色分派原則
測試級	不做規定。
第1級	不做規定。
第2級	依照5.2.1節規定的4種信賴角色，允許1個人超過1個以上信賴角色，但簽發員和管理員不可相互兼任。
第3級	依照5.2.1節規定的4種信賴角色，允許1個人超過1個以上信賴角色，但簽發員不可以再兼任管理員或稽核員。
第4級	依照5.2.1節規定的4種信賴角色，對人員及角色分派必須符合以下規定： (1)管理員、簽發員和稽核員3種信賴角色不可相互兼任，但

保證等級	角色分派原則
	可兼任維運員。 (2)任何1個角色均不允許執行自我稽核功能。

5.2.3 每個任務所需之人數

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

5.2.4 識別及鑑別每 1 個角色

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

5.3 人員控管

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

(1) 以書面方式指派工作。

(2) 以法規或契約規定執行任務之條件。

(3) 接受任務之相關訓練。

(4)以法規或契約規定不可洩漏敏感之憑證機構相關安全資訊及用戶資料。

(5) 指派工作應符合利益迴避原則。

5.3.1 身家背景、資格、經驗及安全需求

憑證機構必須進行人員的識別作業，忠誠、可信賴、正直和中華民國國民是遴選信賴角色人員的必備條件，人員的資格、遴選、監督和稽核相關辦法應在憑證實務作業基準中說明。

5.3.2 身家背景之查驗程序

身家背景之查驗程序應在憑證實務作業基準中說明。

5.3.3 教育訓練需求

憑證機構相關人員必須接受以下教育訓練：

(1) 憑證機構及註冊中心之安全認證機制。

(2) 憑證機構系統使用的公開金鑰基礎建設軟體。

(3) 負責執行公開金鑰基礎建設的工作內容。

(4) 災後復原及業務永續經營之程序。

5.3.4 人員再教育訓練之需求及頻率

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

新進人員也必須比照辦理，憑證機構必須每年進行檢視相關人員之受訓情形。

5.3.5 工作調換之頻率及順序

不做規定。

5.3.6 未授權行動之制裁

憑證機構應訂定適當的管理辦法，以防止人員未經授權存取資料，並將相關規定公佈在憑證實務作業基準中。對於違反憑證政策或憑證實務作業基準相關規定的人員，憑證機構必須採取適當的管理和懲處。

對於執行總管理中心及儲存庫主機的相關人員，如違反憑證政策或憑證實務作業基準或其他總管理中心公佈之程序，必須採取適當的管理和懲處。

5.3.7 聘僱人員之規定

聘僱人員擔任憑證機構相關職務必須符合憑證機構的憑證實務作業基準相關規定。

5.3.8 提供之文件資料

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

6 技術性安全控管

6.1 金鑰對之產製及安裝

6.1.1 金鑰對之產製

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

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

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

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

6.1.2 私密金鑰安全傳送給用戶

如私密金鑰在用戶的密碼模組內被產製及儲存時，無需傳送其私密金鑰。

如由個體(例如用戶或 IC 卡發卡中心)所擁有的符記(Token)直接產製金鑰，或由另一個金鑰產製者產製金鑰後，再傳送金鑰到該個體

的符記中，則此個體在私密金鑰產生及接受時，已被視為擁有該私密金鑰。但若上述的個體並不是憑證申請的憑證主體時，則應以安全及可稽核的方法傳送私密金鑰給憑證主體，以完成私密金鑰的轉移。

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

如私密金鑰由憑證機構或註冊中心或可信賴的第三者代為產製，則此密碼模組必須安全傳送至用戶，用戶必須作收受私密金鑰的確認。密碼模組的存放位置及狀態之追溯紀錄必須被妥善保存，至少到用戶確認接受該密碼模組為止。

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

6.1.3 公開金鑰安全傳送給憑證機構

在憑證機構對用戶做身分鑑別時，用戶必須將其公開金鑰傳送給憑證機構，傳送的方式包括：

(1) 由註冊中心代為發出憑證申請的電子訊息。

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

(3) 可經由其它安全的電子化機制來完成。

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

6.1.4 憑證機構公開金鑰安全傳送給信賴憑證者

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

(1) 憑證機構以符記儲存總管理中心之自簽憑證或公開金鑰，並以安全方式傳送至信賴憑證者。

(2) 透過特殊安全的管道(out-of-band)傳送總管理中心之自簽憑證或公開金鑰。

(3) 透過特殊安全的管道(out-of-band)傳送總管理中心之自簽憑證或公開金鑰之雜湊值或指紋，供使用者比對(與憑證一起在線上公佈(in-band) 的雜湊值或指紋，不被視為是合格的安全管道)。

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

(5) 其他本會核可之方式。

以上所述之特殊安全管道應在總管理中心的憑證實務作業基準中說明。

總管理中心簽發的下屬憑證機構憑證需公佈在該憑證機構的儲存庫中。

6.1.5 金鑰長度

表 6-1 金鑰長度規定

保證等級	對稱金鑰	公開金鑰
測試級	至少必須具備 3-DES (3 Keys)或安全強度相當的其他種類金鑰(例如AES 128位元)。	至少必須使用1024位元的RSA金鑰或安全強度相當的其他種類金鑰(例如ECC 161位元)。
第1級		
第2級		
第3級		
第4級		至少必須使用2048位元的RSA金鑰或安全強度相當的其他種類金鑰(例如ECC 224位元)。

6.1.6 公鑰參數之產製

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

6.1.7 金鑰參數品質之檢驗

對於RSA演算法而言，不必做參數品質的檢驗，但必須做質數的測試，憑證機構應於憑證實務作業基準中說明如何執行相關測試。

對於其他演算法而言，則依相關的國際標準，並應包括質數的測試。

6.1.8 金鑰經軟體或硬體產製

任何被用於金鑰產製的隨機亂數，必須經由本會認可。用戶隨機亂數、金鑰對和對稱金鑰之產製，使用軟體或硬體之相關規定如下表所列：

表6-2金鑰產製機制

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

6.1.9 金鑰之使用目的

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

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

憑證給予用戶，一做為資料加密用；一做為數位簽章與身分認證用。

6.2 私密金鑰保護

6.2.1 密碼模組標準

本會應決定密碼模組驗證的相關標準，其中密碼模組之安全需求主要是參考FIPS 140系列或安全強度相當的標準。相關標準的採用由本會發佈。密碼模組必須依據相關的驗證標準進行安全等級相當的驗證。另外，本會得對總管理中心所使用密碼模組的相關技術文件進行檢視。

下表列出密碼模組的最低要求，亦可使用更高的安全等級，而表中所列的等級係參考FIPS 140系列的定義。

表6-3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	不做規定	不做規定	不做規定
第1級	不適用	等級1 (硬體或軟體)	等級1 (硬體或軟體)	不做規定
第2級	不適用	等級2 (硬體或軟體)	等級1 (硬體或軟體)	等級1 (硬體或軟體)
第3級	不適用	等級2(硬體)	等級2(硬體)	等級1 (硬體或軟體)
第4級	等級3(硬體)	等級3(硬體)	等級2(硬體)	等級2(硬體)

6.2.2 金鑰分持之多人控管

簽發保證等級第3及第4級憑證的憑證機構之簽章用私密金鑰，必須符合第5章規定的多人控管程序。

6.2.3 私密金鑰託管

簽章用之私密金鑰不可被託管(Escrowed)。

6.2.4 私密金鑰備份

6.2.4.1 憑證機構簽章用私密金鑰備份

以保證等級第3級及第4級運作之憑證機構，其簽章用私密金鑰，應在多人控管程序下進行備份，並保存在備援場所；金鑰備份的程序必須在憑證實務作業基準中說明。

6.2.4.2 用戶簽章用私密金鑰備份

保證等級第1、第2及第3級憑證，用戶簽章用私密金鑰可做備份或拷貝，但是必須由用戶控制。

保證等級第4級憑證，用戶簽章用私密金鑰不可以備份或拷貝。

6.2.5 私密金鑰歸檔

簽章用私密金鑰不可以被歸檔(Archival)。

6.2.6 私密金鑰輸入至密碼模組

依照 6.1.1 節規定。

6.2.7 私密金鑰之啟動方式

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

已啟動的私密金鑰不應沒人看管或是容許未經授權的存取。

6.2.8 私密金鑰之停用方式

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

6.2.9 私密金鑰之銷毀方式

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

6.3 用戶金鑰對管理之其他規定

將單一金鑰對同時用於簽章和加密，雖然在技術上可行，但除非符合6.1.9節規定之舊版應用系統，否則不論任何保證等級，建議都應簽發兩種金鑰對憑證給予用戶，一種做為資料加密用；另一種則使用於數位簽章與身分認證。

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

6.3.1 公開金鑰之歸檔

在憑證歸檔後，得不必再進行公開金鑰之歸檔。

6.3.2 公開金鑰及私密金鑰之使用期限

6.3.2.1 憑證機構公開金鑰及私密金鑰之使用期限

憑證機構之公開金鑰及私密金鑰依金鑰強度等級不同，使用期限說明如下：

(1) RSA 4096位元或安全強度相當之其他種類的公開金鑰對(例如ECC 300位元)：私密金鑰使用期限至多為15年；公鑰憑證有效期限至多為30年。

(2) RSA 2048位元或安全強度相當之其他種類的公開金鑰對(例如ECC 224位元)：私密金鑰使用期限至多為10年；公鑰憑證有效期限至多為20年。

(3) RSA 1024位元或安全強度相當之其他種類的公開金鑰對(例如ECC 161位元)：私密金鑰使用期限至多為5年；公鑰憑證有效期限至多為10年。

總管理中心用來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的一半，其自簽憑證生命週期不超過30 年。

總管理中心簽發給下屬憑證機構之憑證，其憑證生命週期，加上總管理中心用來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。

6.3.2.2 用戶公開金鑰及私密金鑰之使用期限

用戶之金鑰使用期限依據其金鑰長度而訂，若有展期考量，從其規定，說明如下：

(1)若金鑰為與 RSA 1024 位元安全強度相當，則私密金鑰使 用期限原則上至多為 5 年。另憑證機構得經評估適法性、便民性、安全性、成本效益之需要，而將 RSA 1024 位元金鑰之展期不得超過 3 年，但展延後的使用期限至多到民國 102 年 12 月 31 日(含)為止。

(2)若金鑰為與 RSA 2048 位元安全強度相當，則私密金鑰使用期限至多為 10 年。

基於金鑰安全強度的需求，憑證機構最晚必須在民國 99 年 12 月 31 日停止簽發與 RSA 1024 位元安全強度相當的憑證，但在此之前簽發的憑證，仍可使用到效期到期日為止。

6.4 啟動資料之保護

6.4.1 啟動資料之產生

用來解開憑證機構或用戶私密金鑰的啟動資料，與其他相關存取控制機制，必須適當的保護。對於以保證等級第1、第2及第3級運作之憑證機構，其啟動資料得由使用者自行選擇。對於以保證等級第4級運作之憑證機構，必須能接受使用者的生物特徵資料，或由密碼模組強化的安全機制。若以通行碼(Password)做為啟動資料時，通行碼的產生必須符合行政院及所屬各機關資訊安全管理要點及規範規定。如果啟動資料必須傳送，應透過適當的安全管道。

6.4.2 啟動資料之保護

用來解開私密金鑰的啟動資料，必須使用結合密碼和存取控制的安全機制加以保護以防止揭露。啟動資料得以生物特徵或記憶方式保存。若需留下紀錄，必須使用與該資料安全等級相當的密碼模組來保護，以確保其安全。若登入的失敗次數超過憑證實務作業基準規定的最大預設值時，保護機制必須能即時鎖住此帳號或終止應用程式。

6.4.3 其他啟動資料之規定

不做規定。

6.5 電腦軟硬體安控措施

6.5.1 特定電腦安全技術需求

依證保證等級第3及第4級運作之憑證機構，和其相關輔助系統必須包含以下功能，這些電腦安全功能可由作業系統，或結合作業系統、軟體和實體的保護措施提供。

(1) 具備身分鑑別的登入。

(2) 提供自行定義(Discretionary)存取控制。

(3) 提供安全稽核能力。

(4) 對各種憑證服務和公開金鑰基礎建設信賴角色存取控制的限制。

(5) 具備公開金鑰基礎建設信賴角色和相關身分的識別和鑑別。

(6) 以密碼技術確保每次通訊和資料庫安全。

(7) 具備公開金鑰基礎建設信賴角色和相關身分識別的安全及可信賴的管道。

(8) 具備程序完整性及安全控管保護。

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

6.5.2 電腦安全評等

不做規定。

6.6 生命週期技術控管措施

6.6.1 系統研發控管措施

憑證機構的系統研發控管措施說明如下:

表6-4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	不做規定。
第1級	不做規定。
第2級 第3級 第4級	(1) 憑證機構所使用的軟體，必須依良好的軟體工程發展方法開發，如採用Capability Maturity Model(CMM)方法。 (2) 憑證機構之硬體和軟體必須是專用的，不得安裝與運作無關的其他應用系統(包括硬體裝置、網路連接或元件軟體)。 (3) 必須防止惡意軟體安裝在憑證機構設備

	上。憑證機構的運作僅能使用獲得安全政策授權的元件。 (4) 對於註冊中心之硬體和軟體，必須在初次使用時檢查是否有惡意程式碼並定期掃瞄。

6.6.2 安全管理控管措施

表 6-5 安全管理控管規定

保證等級	安全管理控管措施
測試級 第1級 第2級 第3級	必須記錄和控管憑證機構相關系統的組態及任何修正與功能升級，並具備偵測未經許可修改憑證機構之軟體或組態的機制。在首次安裝憑證機構軟體時，必須確認是由供應商提供且未被修改過，且為正確的版本。
第4級	必須記錄和控管憑證機構相關系統的組態以及任何修正與功能升級，並具備偵測未經許可修改憑證機構之軟體或組態的機制。在首次安裝憑證機構軟體時，必須確認是由供應商提供且未被修改過，且為正確的版本。 憑證機構必須至少每月1次驗證憑證機構軟體的完整性。

6.6.3 生命週期安全評等

不做規定。

6.7 網路安全控管措施

總管理中心主機和內部儲存庫不得與任何外部網路連接。總管理中心外部儲存庫則連接到網際網路(Internet)上，以提供不中斷服務(除必要之維護或備援外)。內部儲存庫資訊以手動方式，從內部儲存庫傳送到外部儲存庫，而且所有資訊(憑證與憑證機構廢止清冊)都以數位簽章保護。外部儲存庫透過系統修補程式的更新、弱點掃描、入侵偵測系統、防火牆、過濾路由器(Filtering Router)等加以保護，以防範阻絕服務和入侵等攻擊。

6.8 密碼模組安全控管措施

依照 6.1及6.2 節規定。

7 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 版本的憑證，其版本序號(Version Numbers)的欄位值為 2。

7.1.2 憑證擴充欄位

在憑證格式剖繪中訂定憑證擴充欄位(Certificate Extensions)的使用、處理方式及欄位值設定等規定。透過憑證格式剖繪對憑證的基礎架構進行適當控制，以提供足夠的彈性來符合不同憑證機構及社群的要求。

總管理中心簽發的憑證必須遵循「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」的規定，其下屬憑證機構簽發的憑證若屬保證等級第 3 級，也必須遵循憑證及憑證廢止清冊格式剖繪的規定；若屬保證等級第 1 及第 2 級，則須遵循 RFC 3280 的規定。若必須使用自行擴充欄位時，應在憑證實務作業基準中說明，同時關鍵的(Critical)自行擴充欄位，在應用服務上必須能與其社群達到互運。

7.1.3 演算法物件識別碼

簽發的憑證必須於簽章時使用下述之演算法的物件識別碼(OID)：

sha-1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}

簽發的憑證必須使用下述之物件識別碼來識別產製主體金鑰的演算法：

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

7.1.4 命名形式

憑證的主體及簽發者兩個欄位值，必須使用 X.500 的唯一識別名稱(Distinguished Name)，且此名稱的屬性型態必須遵循 RFC 3280 的規定。

7.1.5 命名限制

不做規定。

7.1.6 憑證政策物件識別碼

簽發的憑證必須引用憑證政策的物件識別碼，同時憑證政策的物件識別碼必須與憑證的保證等級相符。

7.1.7 政策限制擴充欄位之使用

不做規定。

7.1.8 政策限定元之語法及語意

簽發的憑證不得包含政策限定元(Policy Qualifiers)。

7.1.9 關鍵憑證政策擴充欄位之語意處理

簽發的憑證所使用之關鍵憑證政策的擴充欄位之語意處理，必須遵循憑證及憑證廢止清冊格式剖繪的規定。

7.2 憑證機構廢止清冊及憑證廢止清冊之格式剖繪

7.2.1 版本序號

簽發的憑證機構廢止清冊(CARL)及憑證廢止清冊(CRL)必須符合 X.509 v2 的規定。

7.2.2 憑證機構廢止清冊及憑證廢止清冊擴充欄位

在憑證機構廢止清冊及憑證廢止清冊(CARL/CRL)的格式剖繪中，規定每 1 個擴充欄位皆必須遵循憑證及憑證廢止清冊格式剖繪的規定。

8.憑證政策及憑證實務作業基準之維護

8.1 變更程序

本會至少每年應檢視本憑證政策 1 次，憑證機構至少每年應檢視憑證實務作業基準 1 次，以維持其保證度。憑證政策的修改不影響憑證政策所聲明的憑證使用目的與保證度時，憑證政策之物件識別碼不需修改，憑證政策之物件識別碼變更，憑證實務作業基準應作相對應之變更。

8.1.1 變更時不另作通知之變更項目

憑證政策及憑證實務作業基準重新排版時，不另作通知。

8.1.2 應通知之變更項目

憑證機構應於憑證實務作業基準載明應通知之變更項目。

8.1.2.1 變更項目

憑證政策由本會評估項目的變更對用戶或信賴憑證者影響程度：

(1)影響程度大者，應先公告 30 個日曆天，始得修訂。

(2)影響程度小者，應先公告 15 個日曆天，始得修訂。

8.1.2.2 通知機制

本會及憑證機構應將對用戶可能產生重大影響的變更項目，分別公告於總管理中心及憑證機構之儲存庫，憑證機構應於憑證實務作業

基準載明變更項目通知機制。

8.1.2.3 意見之回覆期限

對於 8.1.2.1 節之變更項目有意見者，其回覆期限為：

(1)依照 8.1.2.1 節之(1)影響程度大者之回覆期限為自公告日起 15 個日曆天內。

(2)依照 8.1.2.1 節之(2)影響程度小者之回覆期限為自公告日起 7 個日曆天內。

憑證機構應於憑證實務作業基準載明意見之回覆期限。

8.1.2.4 處理意見機制

本會負責處理本憑證政策相關意見，憑證機構應於憑證實務作業基準載明處理意見機制。

8.1.2.5 最後公告期限

憑證政策公告之變更項目應依照 8.1.2.2 及 8.1.2.3 節規定進行修訂，公告期限應依照 8.1.2.1 節規定至少公告 15 個日曆天，直到憑證政策修訂生效，憑證機構應於憑證實務作業基準載明最後公告期限。

8.2 公告及通知之規定

憑證政策之公佈與後續修訂應於本會核准後 7 個日曆天內於總管理中心儲存庫公告，憑證機構應於憑證實務作業基準載明公告及通知之規定。

8.3 憑證實務作業基準變更程序

憑證機構之憑證實務作業基準必須遵循相關法令及符合本憑證政策規定，並經本會及電子簽章法主管機關經濟部核定。如本憑證政策修訂公佈後，憑證機構之憑證實務作業基準應配合修訂，並送交本會及電子簽章法主管機關經濟部核定。

附錄：名詞解釋

存取(Access)	運用系統資源處理資訊的能力。
存取控制 (Access Control)	對於授權的使用者、程式、程序或其他系統給予資訊系統資源存取權限的處理過程。
啟動資料 (Activation Data)	在存取密碼模組時(例如用來開啟私密金鑰以進行簽章或解密)，除金鑰外所需的隱密資料。
申請者(Applicant)	向憑證機構申請憑證，而尚未完成憑證作業程序的用戶。
歸檔(Archive)	實體上(與主要資料存放處)分隔的長期資料儲存處，可用來支援稽核服務、可用性服務或完整性服務等用途。
保證(Assurance)	據以信賴該個體已符合特定安全要件之基礎。(憑證實務作業基準應載明事項準則第 1 章第 2 條第 1 項)
保證等級 (Assurance Level)	具相對性保證層級中之某 1 級數。(憑證實務作業基準應載明事項準則第 1 章第 2 條第 2 項)
屬性憑證管理中心(Attribute Authority)	依據目的業務職掌，有權驗證某個體與某些屬性相關聯的主體。
稽核(Audit)	評估系統控制的是否恰當、確保符合既定的政策及營運程序、並對現有的控制、政策及程序建議必要的改善而進行的獨立檢閱及調查。
稽核紀錄 (Audit Data)	依照發生時間順序之系統活動紀錄，可用以重建或調查事件發生的順序及某個事件中的變化。
鑑別(Authenticate)	當某個體出示身分時，確認其身分之正確性。
鑑別程序	用以建立資料傳送、訊息、來源者之安全措施，

(Authentication)	或是驗證個人接收特定種類資訊權限之方法。
備份(Backup)	將資料或程式複製，必要時可供復原之用。
連結、繫結 (Binding)	將兩個相關的資訊元素做連結(結合)的過程。
生物特徵值 (Biometric)	人的身體或行為的特徵。
憑證機構憑證(CA Certificate)	簽發給憑證機構的憑證。
憑證(Certificate)	(1)指載有簽章驗證資料，用以確認簽署人身分、資格之電子形式證明。(電子簽章法第二條第六款) (2)資訊之數位呈現，內容包括： A.簽發的憑證機構。 B.用戶之名稱或身分。 C.用戶的公開金鑰。 D.憑證之有效期間。 E.憑證機構數位簽章。 在本憑證政策中所提及的“憑證”特別指其格式為 X.509 v.3，且在其“憑證政策”欄位中明確地引用本憑證政策之物件識別碼的憑證。
憑證機構 (Certification Authority, CA)	(1)簽發憑證之機關、法人。(電子簽章法第 2 條第 5 款) (2)為使用者所信任之權威機構，其業務為簽發並管理 X.509 格式之公開金鑰憑證及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)	經簽署及蓋時戳之清單，清單中為已被廢止之憑證機構公開金鑰憑證(包括交互憑證)之序號。

憑證政策 (Certificate Policy, CP)	(1)某 1 憑證所適用之對象或情況所列舉之 1 套規則，該對象或情況可為特定之社群或具共同安全需求之應用。(憑證實務作業基準應載明事項準則第 1 章第 2 條第 3 項) (2)憑證政策係為透過憑證管理執行的電子交易所訂定之具專門格式的管理政策。憑證政策中包括與數位憑證相關之生成、產製、傳送、稽核、被破解後的復原以及其管理等各項議題。憑證政策亦可間接地控制運用憑證之安全系統，以保護通訊系統所進行的交易。藉由控制關鍵的憑證擴充欄位方式，憑證政策及其相關技術可提供特定應用所需的安全服務。
憑證實務作業基準(Certification Practice Statement, CPS)	(1)由憑證機構對外公告，用以陳述憑證機構據以簽發憑證及處理其他認證業務之作業準則。(電子簽章法第 2 條第 7 款) (2)宣告某憑證機構對憑證之作業程序(包括簽發、停用、廢止、展期及存取等)符合特定需求(需求載明於憑證政策或其他服務契約中)之聲明。
憑證廢止清冊 (Certificate Revocation List, CRL)	(1)憑證機構以數位方式簽章，並可供信賴憑證者使用之已廢止憑證表列。(憑證實務作業基準應載明事項準則第 1 章第 2 條第 8 項) (2)由憑證機構維護之清單，清單中記載由此憑證機構所簽發且在到期日之前被廢止之憑證。
元件私密金鑰 (Component Private Key)	與憑證簽發設備功能相關聯的私密金鑰，相對於與操作員或管理者相關聯的私密金鑰。
破解 (Compromise)	資訊洩漏給未經授權的人士或違反資訊安全政策造成物件未經授權蓄意、非蓄意的洩漏、修改、毀壞或遺失。
機密性 (Confidentiality)	資訊不會遭受未經授權的個體或程序獲知或取用。

交互憑證 (Cross-Certificate)	由 1 個憑證機構簽發給另 1 個憑證機構，用以建立兩個憑證機構之間信賴關係的憑證。交互憑證是 1 種憑證機構憑證(CA Certificate)。
密碼模組 (Cryptographic Module)	1 組硬體、軟體、韌體或前述的組合，用以執行密碼的邏輯或程序(包含密碼演算法)，並且被包含在此模組的密碼邊界之內。
金鑰效期 (Cryptoperiod)	每個金鑰設定之有效期限。
資料完整性(Data Integrity)	資料未遭受未經授權或意外的更改、破壞或遺失的性質。
數位簽章 (Digital Signature)	將電子文件以數學演算法或其他方式運算為一定長度之數位資料，以簽署人之私密金鑰對其加密，形成電子簽章，並得以公開金鑰加以驗證者。(電子簽章法第 2 條第 3 款)
雙用憑證(Dual Use Certificate)	可用於數位簽章及資料加密兩種服務的憑證。
憑證效期 (Duration)	1 憑證欄位，由“有效期限起始時間”(notBefore)及“有效期限截止時間”(notBefore)兩個子欄位所組成。
電子商務 (E-commerce)	使用網路科技(特別是網際網路)以提供買賣貨物及相關服務。
加密憑證 (Encryption Certificate)	1 憑證，包含用以加密電子訊息、檔案、文件或資料的公開金鑰，此金鑰亦可用來建立或交換以上各項加密用途的短期密鑰。
終端個體 (End Entity)	信賴憑證者及用戶，包括人員、組織、客戶(Account)、裝置或站台(Site)。
終端個體憑證 (End-Entity Certificate)	簽發給終端個體的憑證。

防火牆 (Firewall)	符合近端(區域)安全政策而對網路之間做接取限制的閘道器。
內部威脅 (Inside Threat)	利用授與之權限，可能透過資料的破壞、揭露、篡改或拒絕服務等方式造成對資訊系統的損害。
完整性 (Integrity)	對資訊的保護，使其不受未經授權的修改或破壞。資訊從來源產製後，經傳送、儲存到最終被收受方接收的期間中都維持不被篡改的一種狀態。
金鑰託管 (Key Escrow)	將用戶的私密金鑰及依據用戶必須遵守的託管協議(或類似的契約)所規定的相關資訊進行存放，此託管協議的條款要求 1 個或 1 個以上的代理機構基於有益於用戶、雇主或另一方的前提下，依據協議的規定，擁有用戶的金鑰。
金鑰交換 (Key Exchange)	交換彼此金鑰以建立安全通訊的處理過程。
金鑰產製原料 (Key Generation Material)	用於產製金鑰的隨機亂數、擬隨機亂數及其他密碼參數。
金鑰對(Key Pair)	兩把數學上有相關性的金鑰，具有下列特性： (1) 其中 1 把金鑰用來做訊息加密，而此加密訊息只有另 1 把可以解密。 (2) 從其中 1 把金鑰要推出另 1 把金鑰(從計算的角度而言)是不可行的。
交互認證協議書 (Cross Certification Agreement, CCA)	政府憑證總管理中心與下屬憑證機構就下屬憑證機構申請加入政府機關公開金鑰基礎建設所必須遵守之事項及個別責任義務歸屬的協議。
簽發憑證機構 (Issuing CA)	對於 1 張憑證而言，簽發該憑證的憑證機構即稱為該憑證的簽發憑證機構。

相互鑑別(Mutual Authentication)	發生在進行通訊活動的兩方彼此進行鑑別時。(參閱鑑別的解釋)
命名機構(Naming Authority)	一權責單位，負責指定唯一識別名稱並確保每個唯一識別名稱有意義且在其領域內為唯一。
不可否認性(Non-Repudiation)	對資料傳送方提供傳送證明以及對資料收受方提供傳送方的身分之保證，因而兩方在事後皆無法否認曾經處理過此項資料。技術上的不可否認性是指對信任者(信任之一方)而言，如果某個公開金鑰可用以驗核某個數位簽章，保證此簽章必定是由相對應的私密金鑰所簽署。在法律上，不可否認性是指建立私密簽章金鑰之擁有或控管機制。
物件識別碼(Object Identifier, OID)	(1)1 種以字母或數字組成之唯一識別碼，該識別碼必須依國際標準組織所訂定之註冊標準加以註冊，並可被用以識別唯一與之對應之憑證政策；憑證政策修訂時，其物件識別碼不必然隨之變更。(憑證實務作業基準應載明事項準則第 1 章第 2 條第 4 項) (2)向國際認可之標準機構(ISO)註冊的特別形式的數碼，當提及某物件或物件類別時，可以引用此唯一的數碼做辨識。例如在公開金鑰基礎架構中，可以此數碼來指明使用的憑證政策及使用的密碼演算法。
特殊安全管道(Out-of-Band)	不同於一般的傳送訊息管道的傳送方式。例如使用電子線上傳送的情形，可稱使用實體的掛號信為特殊安全管道。
外部威脅(Outside Threat)	1 來自外部未經授權，且對資訊系統具有潛在破壞能力(包括對資料的毀壞、篡改、洩漏，或是造成拒絕服務)的個體。
行政機關電子憑證推行小組	1 組織，其設立目的為：研議行政機關電子憑證政策及憑證實務作業基準、相關技術規範、電子憑證體系架構及其他電子憑證管理事項。

私密金鑰(Private Key)	(1) 在簽章金鑰對中，用以產生數位簽章的金鑰。 (2) 在加解密金鑰對中，用以對機密資訊解密的金鑰。 在這兩種情況裡，此金鑰皆須保密。
公開金鑰(Public Key)	(1) 在簽章金鑰對中，用以驗證數位簽章有效的金鑰。 (2) 在加解密金鑰對中，用以對機密資訊加密的金鑰。 在這兩種情裡，此金鑰皆須(一般以數位憑證的形式)公開可得。
註冊中心 (Registration Authority, RA)	(1)負責確認憑證申請人之身分或其他屬性，但不簽發憑證亦不管理憑證。註冊中心是否需為其行為負責及其應負責任之範圍，依所適用之憑證政策或協議訂之。 (2)1 個體，負責對憑證主體做身分識別及鑑別，但不做憑證簽發。
金鑰更換(Re-key (a certificate))	改變在密碼系統應用程式中所使用之金鑰之值。通常必須藉由對新的公開金鑰簽發新的憑證來達成。
信賴憑證者 (Relying Party)	(1)信賴所收受之憑證及可用憑證中所載之公開金鑰加以驗證之數位簽章者，或信賴憑證中所命名主體之身份(或其他屬性)及憑證所載公開金鑰之對應關係者。(憑證實務作業基準應載明事項準則第 1 章第 2 條第 6 項) (2)個人或機構收到包含憑證及數位簽章(此數位簽章可藉由憑證上所列之公開金鑰做驗證)之資訊，並且可能信賴這些資訊。
憑證展期(Renew (a certificate))	藉由簽發新的憑證，以延展公開金鑰憑證所連結資料有效性的程序。
儲存庫	(1)用以儲存與檢索憑證或其他憑證相關資訊之

(Repository)	可信賴系統。(憑證實務作業基準應載明事項準則第 1 章第 2 條第 7 項) (2)包含本憑證政策與憑證相關資訊的資料庫。
憑證廢止(Revoke a Certificate)	在憑證的有效期間內，提前終止憑證的運作。
政府憑證總管理中心(Government Root CA)	在階層式公開金鑰基礎建設架構中最頂層的憑證機構，其公開金鑰為信賴之起源。
秘密金鑰 (Secret Key)	在對稱式密碼系統中“共持的秘密”，使用者之身分鑑別是藉由 password、PIN 或與遠端主機(或伺服器)共享的其他秘密。 單一的金鑰由兩方共持：傳送方用以加密傳送訊息，而收受方用以解密此訊息。此共持的金鑰由兩方在事前所協議的演算法生成。
簽章憑證 (Signature Certificate)	公開金鑰憑證包含用以驗證數位簽章(而非用於加密資料或其他密碼功用)之公開金鑰。
簽發憑證機構 (Subject CA)	對於 1 張憑證機構憑證(CA Certificate)而言，該憑證的憑證主體(Subject)所指的憑證機構即稱為該憑證的主體憑證機構。
下屬憑證機構 (Subordinate CA)	在階層架構的公開金鑰基礎建設中，憑證由另 1 個憑證機構所簽發，且其活動受限於此另 1 憑證機構的憑證機構。
用戶 (Subscriber)	(1)指憑證中所命名或識別之主體，且其持有與憑證中所載公開金鑰相對應之私密金鑰者。(憑證實務作業基準應載明事項準則第 1 章第 2 條第 5 項) (2)具下列特性之個體，包括(但不限於)個人、機構或網路裝置： (a)簽發憑證上所載明之主體。 (b)擁有與憑證上所列公開金鑰對應之私密金鑰。

	(c)本身不簽發憑證給其他方。
技術上的不可否認性(Technical Non-Repudiation)	公開金鑰機制所提供的技術性證據以支援不可否認之安全服務。
威脅(Threat)	對資訊系統可能造成損害(包括損毀、揭露、惡意修改資料或拒絕服務)的任何狀況或事件。
憑證信賴清冊(Trust List)	可信賴憑證之清單，信賴憑證者用以鑑別憑證。
可信賴憑證(Trusted Certificate)	為信賴憑證者所信賴且經由安全可靠之傳送方式取得的憑證。此類憑證中所包含的公開金鑰用於信賴路徑之起始，又稱為信賴起點。
可信賴時戳(Trusted Timestamp)	由可信賴的權威機構以數位方式簽署，證明某特定數位物件在某特別時間之存在。
可信賴系統(Trustworthy System)	具有下列性質之電腦硬體、軟體及程序： (1) 對於入侵及誤用有相當的保護功能。 (2) 提供合理的可用性、可靠度及正確操作。 (3) 適當地執行預定功能。 (4) 與一般為人所接受的安全程序一致。
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。