臺灣網路認證股份有限公司

全球憑證管理中心

憑證實務作業基準

(TWCA GLOBAL CA CPS)

(第 1.8 版)

臺灣網路認證股份有限公司
TAIWAN-CA INC.

生效日期：中華民國 112 年 6 月 30 日

Effective Date：2023/6/30

版本變更紀錄

版本	生效日期	發行者	備註
1.0	102/01/22	TWCA PMA	初版發行
1.1	103/07/02	TWCA PMA	新增設備憑證
1.2	105/08/23	TWCA PMA	移除 SSL 伺服器 UCA 的自身憑證中的二個識別名稱
1.3	106/09/26	TWCA PMA	新增法人身分的鑑別程序
1.5	109/01/30	TWCA PMA	(1) 修訂以符合 CABF Baseline Requirement (2) 新增 CA/Browser Forum 政策識別碼 (3) 新增 AATL 憑證
1.6	110/12/21	TWCA PMA	(1) 1.2 節，修改 TLS/SSL 伺服器憑證 OID (2) 1.4.1、3.2.2 節，更新 TLS/SSL 伺服器憑證及設備憑證身分鑑別方式 (3) 3.2.2、4.2.1 節，更新 CAA 之參考文件 (RFC 8659) (4) 3.2.2 節，新增 BR 合法之網域及 IP 驗證方式，並標示已不可使用的驗證方法 (5) 3.3.1、6.3.2 節，更新 TLS/SSL 憑證效期上限更改為 398 天 (6) 4.9.12 節，新增可接受證明金鑰外洩之方式 (7) 新增 TSA 憑證 (8) 3.1.1 節，調整 AATL 憑證命名 (9) 3.2.2 節，修改內容以滿足 CABF Baseline Requirement 1.7.5 之要求 (10) 3.2.2 節，所有 domain 驗證均須進行 Public Suffix 檢查
1.7	111/12/2	TWCA PMA	(1) 設備憑證併入 TLS/SSL 憑證 (2) 2.2、3.2.2、9.15 節，調整 BR 之適用憑證種類 (3) 3.2.2 節，附加內容以滿足 BR 1.7.8 規定 (4) 3.1.1、7.1.4 節，附加內容以滿足 BR 1.7.9 規定 (5) 8.4 節，更新稽核版本 (6) TLS/SSL 憑證名稱與 CP 規範一致 (7) 版面調整
1.8	112/6/30	TWCA PMA	(1) 移除 TLS/SSL 憑證相關內容、商務安全 EC 憑證相關內容

			(2) 移除設備認證相關內容 (3) 資安 UCA 憑證更名為資安憑證 (4) 新增 AATL、S/MIME 相關內容 (5) 調整 OCSP 相關內容 (6) 新增 1.6 節、5.6.1 節、5.6.2 節、8.7 節 (7) 修訂 1.4 節、3.1.1 節、3.2 節、4.3.1 節、5.2.4 節、5.4.2 節、5.4.5 節、6.1.5 節、6.1.6 節、6.3.2 節、6.5.2 節、6.8 節、7.1.3 節、8.2 節、8.6 節、9.2.1 節、9.2.2 節

目 錄

摘要

臺灣網路認證公司全球憑證管理中心憑證實務作業基準之重要事項說明如下：

1. 主管機關核定

本憑證實務作業基準係依據主管機關頒布之「憑證實務作業基準應載明事項準則」規範編撰，經審查後核定之文號為：

民國 112/6/30 數位發展部數位產業署函 產經字第 1124000587 號

2. 簽發之憑證

本憑證管理中心依據本作業基準規範所簽發的全球憑證，其憑證種類、保證等級與適用範圍，詳列如下：

	憑證種類	保證等級	適用範圍
1	資安 UCA 憑證	第三級	金融交易、有價證券交易、電子商務應用、線上身分確認、網路報稅、電子發票、電子通訊投票、線上申請專利商標、短期票券發行交易應用、程式代碼簽署。
		第二級	電子商務應用、線上身分確認、電子郵件應用。
		第一級	電子商務應用、線上身分確認。
		測試級	測試使用。
2	AATL 憑證	第三級	電子商務應用、線上身分確認、電子郵件應用、PDF 文件簽署。
		第二級	電子商務應用、線上身分確認、電子郵件應用、PDF 文件簽署。
3	時戳憑證	第三級	電子文件或訊息之簽章時間證明。
註：憑證保證等級與使用範圍詳述於「1.4 憑證用途」			

3. 法律責任重要事項

(1) 用戶如發生廢止憑證之事由(如私密金鑰資料外洩或遺失)，須立即通知本憑證管理中心，並辦理憑證廢止相關作業，但用戶仍須承擔憑證廢止狀態

未被公布前因使用該憑證所致生之風險與責任。

(2) 本憑證管理中心處理用戶註冊資料及憑證簽發作業，除未遵照本作業基準之規定辦理、違反相關法律規章之規定，或可歸責於本憑證管理中心之故意或過失外，本憑證管理中心不負損害賠償責任。

(3) 本憑證管理中心如因不可抗力之天災事故(例如地震等)，或其他非可歸責於本憑證管理中心之事由(例如戰爭等)，造成用戶損失時，本憑證管理中心不負損害賠償責任。

(4) 本憑證管理中心未善盡保管用戶之註冊及憑證相關資料，而造成相關資訊洩漏、被冒用、竄改或任意使用致造成第三者遭受損害時，本憑證管理中心須負損害賠償責任。

(5) 本憑證管理中心在收到憑證廢止申請後，最遲於 4.9.5 節規定之時限內完成憑證廢止作業，並於作業完成後依據 4.9.7 節規定之頻率簽發憑證廢止清冊及公告於儲存庫。用戶於憑證廢止清冊未被公布之前，須採取適當之行動，以減少對信賴憑證者之影響，並承擔所有因使用該憑證所致生之責任。

(6) 本憑證管理中心與用戶，因簽發憑證或使用憑證而發生損害賠償事件時，雙方須承擔之損害賠償責任，以相關法令規定及合約所定之範圍為責任上限。

(7) 信賴憑證者接受使用本憑證管理中心簽發之憑證時，即表示已了解並同意有關本憑證管理中心法律責任之條款，並依照本作業基準之規定範圍內信賴該憑證。

4. 其他重要事項

(1) 用戶之私密金鑰有遺失或遭破解等不安全之顧慮時，或用戶相關之資訊有異動時，必須依相關作業之規定，向本憑證管理中心辦理申告。

(2) 用戶須妥善產製、保管及使用私密金鑰，並遵守對於金鑰及憑證之使用限制。

(3) 用戶申請憑證時必須提供詳實且正確之資訊，接受本憑證管理中心簽發之憑證時，必須確認憑證內容之正確性，且公開金鑰與私密金鑰為成對之金鑰。

(4) 信賴憑證者驗證憑證時須使用最高層憑證管理中心之自簽憑證，驗證用戶憑證管理中心憑證之數位簽章，並以用戶憑證管理中心之憑證，驗證用戶

憑證之數位簽章是否為用戶憑證管理中心之私密金鑰所簽發，並透過憑證廢止清冊驗證憑證狀態是否已遭廢止。

(5) 信賴憑證者在使用本憑證管理中心簽發之憑證廢止清冊時，須先驗證數位簽章，以確認該憑證廢止清冊是否有效。

(6) 本憑證管理中心至少每半年進行 1 次內部稽核及每年進行 1 次外部稽核，有關稽核作業規範請參閱「8. 稽核及其他評估方法」章節。

1.簡介

1.1 概述

臺灣網路認證股份有限公司(TAIWAN-CA INC.，以下簡稱本公司或 TWCA)係由臺灣證券交易所、臺灣集保決算所、財金資訊股份有限公司、網際威信股份有限公司共同集資設立。

臺灣網路認證股份有限公司全球憑證管理中心憑證實務作業基準(TWCA Global Certification Authority Certification Practice Statement；以下簡稱本作業基準)，係根據臺灣網路認證股份有限公司公開金鑰基礎建設憑證政策(以下簡稱憑證政策)、及遵循電子簽章法主管機關頒布之「憑證實務作業基準應載明事項準則」所訂定。主要為說明臺灣網路認證股份有限公司全球憑證管理中心(以下簡稱本憑證管理中心)，如何遵循憑證政策來進行憑證簽發及管理作業。

為建立安全及可信賴的網路交易環境，確保資訊在網路傳輸過程中不易遭致偽造、竄改或竊取，本公司特規劃建置認證相關安全機制的網際網路認證服務系統，使用公開金鑰密碼機制(public key cryptography)，其安控機制的安全標準符合金融監督管理委員會「金融機構辦理電子銀行業務安全控管作業基準」，具備網路交易訊息的不可否認(non-repudiation)、用戶身分的鑑別(authentication)、訊息完整的驗證(verification)、訊息加密(encryption)的保護及其他機制的安全控管(security control)，可用於網際網路電子銀行、網路下單交易，亦可用於網路報稅、保險、票債券、企業詢價報價、採購與付款交易等網際網路電子商務的應用交易系統。

1.2 文件名稱及識別

本作業基準之名稱為「臺灣網路認證股份有限公司全球憑證管理中心憑證實務作業基準」。

本作業基準依據憑證政策訂定，其所詳述之各種憑證分類，其所對應之物件識別碼分別說明如下：

憑證種類	物件識別碼
資安憑證	2.16.158.3.1.8.5 1.3.6.1.4.1.40869.1.1.23
AATL(Adobe Approved Trust List)憑證	1.3.6.1.4.1.40869.1.1.26
時戳憑證	1.3.6.1.4.1.40869.1.1.27

1.3 成員及適用範圍

「臺灣網路認證股份有限公司全球憑證管理中心」包含以下成員：

(1) 憑證管理中心(Certification Authority，簡稱 CA)。

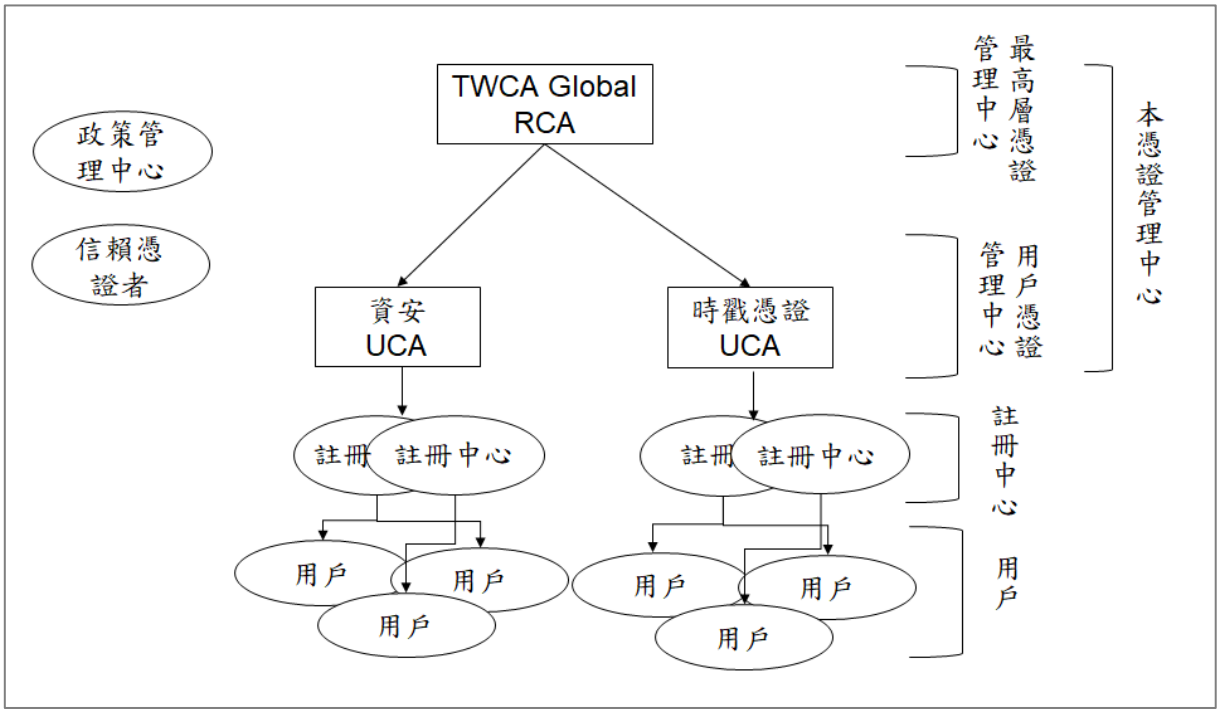
(2) 註冊中心(Registration Authority，簡稱 RA)。

(3) 用戶(Subscribers)。

(4) 信賴憑證者(Relying Party)。

(5) 政策管理中心(Policy Management Authority，簡稱 PMA)。

憑證管理中心依照階層及用途分為「最高層憑證管理中心」(Root CA，簡稱 RCA)與「用戶憑證管理中心」(User CA，簡稱 UCA)，統稱「本憑證管理中心」。成員關係圖如下：



本作業基準將於第三、第四章說明本憑證管理中心如何進行用戶憑證之簽發及管理作業、用戶與信賴憑證者如何申請與使用憑證；於第五章說明最高層憑證管理中心與用戶憑證管理中心之管理準則。

1.3.1 憑證管理中心

1.3.1.1 最高層憑證管理中心

最高層憑證管理中心(RCA)為最高層憑證管理機構，擔任本基礎建設之信賴起源，由本公司負責營運及管理，主要負責以下工作：

(1) 負責用戶憑證管理中心憑證之簽發與管理；不可簽發用戶憑證。

(2) 管理與公告用戶憑證管理中心之憑證、憑證廢止清冊(Certificates Revocation List；CRL)於儲存庫。

(3) 提供線上憑證狀態查詢(Online Certificate Status Protocol；OCSP)服務。

(4) 維持儲存庫的穩定與運作。

(5) 建置於獨立、安全控管的作業環境下，由二位以上經授權的執行人員進行公開金鑰的產生、建置與簽發用戶憑證管理中心憑證的作業，RCA 的憑證為自簽憑證，當新產生或更新憑證時，必須以最迅速的方式遞送予使用者或通知使用者至 RCA 索取。

1.3.1.2 用戶憑證管理中心

用戶憑證管理中心(UCA)由本公司負責營運及管理，主要負責以下工作：

(1) 負責用戶憑證之簽發與管理。

(2) 管理與公告用戶憑證、用戶憑證之憑證廢止清冊(CRL)於儲存庫。

(3) 提供線上憑證狀態查詢(OCSP)服務。

(4) 維持儲存庫的穩定與運作。

1.3.1.3 政策管理中心

「臺灣網路認證股份有限公司」政策管理中心(Policy Management Authority，簡稱 PMA)為設於本公司內部之組織並負責制定下列事項：

(1) 憑證政策。

(2) 本作業基準。

(3) 營運規範。

1.3.2 註冊中心

註冊中心(Registration Authority；RA)主要負責驗證憑證申請者的身分及簽發憑證所需之相關資訊，供本憑證管理中心簽發憑證。

1.3.3 用戶

用戶為憑證中憑證主體(Certificate Subject)名稱所記載之個體，且持有與憑證公開金鑰相對應之私密金鑰者。

本憑證管理中心之用戶為申請憑證之法人與自然人。

1.3.4 信賴憑證者

信賴憑證者係以本憑證管理中心憑證內之公開金鑰，驗證本憑證管理中心用戶憑證之數位簽章訊息有效性之個體。

信賴憑證者依據用戶憑證所記載之身分資訊，用以識別網域主機名稱及所屬用戶資訊。

信賴憑證者須以本憑證管理中心簽發之憑證所記載之資訊，來決定是否可信賴該憑證，或是否可以使用於特定用途。

1.3.5 其他參與者

無規定。

1.4 憑證用途

1.4.1 憑證保證等級

本憑證管理中心依用戶於註冊階段時所使用之身分識別方式的強度，區分不同的憑證保證等級。各憑證保證等級意義如下：

保證等級	保證意義
測試級	本憑證管理中心及註冊中心均未執行任何驗證用戶身分之程序，且僅供測試使用，不可使用於測試以外之任何應用或業務。
第一級	用戶憑證管理中心及註冊中心僅保證用戶識別資訊於本公司資料庫內之唯一性，所有與用戶相關之資訊僅進行有限之查證。
第二級	用戶憑證管理中心及註冊中心保證用戶識別資訊於本公司資料庫內之唯一性，而對於用戶相關資訊，僅提供完成查證而非絕對正確無誤之保證。
第三級	用戶憑證管理中心及註冊中心除保證用戶識別資訊於本公司資料庫內之唯一性外，用戶相關資訊經由多重嚴謹之作業程序，提供類似當面辦理認證強度之身分識別保證。
第四級	用戶憑證管理中心及註冊中心除保證用戶識別資訊於本公司資料庫內之唯一性外，用戶相關資訊經由多重嚴謹之作業程序，提供當面辦理認證強度之身分識別保證。

針對不同的保證等級，其註冊階段針對身分識別方式之要求也會有所不同，具體說明於 3.2 節描述。

1.4.2 使用範圍與賠償責任

一、使用範圍

資安憑證、AATL 憑證、時戳憑證使用範圍之代碼共分四段，格式如下：

第一段代碼 ·第二段代碼 ·第三段代碼 ·第四段代碼

各段代碼之意義如下：

第 一 段 [身分認證安全等級]	第 二 段 [用途別]	第 三 段 [用戶身分]	第 四 段 [適用業務範圍]
1. 第一級 2. 第二級 3. 第三級 0. 測試用憑證	1. 單一用途 2. 限定範圍內多用途	1. 法人 2. 自然人	1.金融交易、電子商務應用、網路報稅、電子發票、電子通訊投票、短期票券發行交易應用 2.有價證券交易、電子商務應用、網路報稅、電子發票、電子通訊投票 3.電子商務應用、線上身分確認、網路報稅、電子發票、電子通訊投票、線上申請專利商標、電子郵件應用、程式代碼簽署、PDF 文件簽署、電子文件或訊息之簽章時間證明(Time-Stamp)

(1) 第一段為身分認證安全等級：

區分為(1)第一級、(2)第二級、(3)第三級、(0)測試憑證，安全性係依用戶註冊時身分認證的方式區分等級，請參閱「1.4.1 憑證保證等級」之規範。

(2) 第二段為用途別(Usage)：

區分為(1)單一用途、(2)限定範圍內多用途(例如金控公司範圍內)，說明：

- 單一用途：係指專供某一特殊用途或限制特定交易對象使用，如財產申報專用或網路下單專用或網路銀行專用。此外，憑證內憑證政策(CertificatePolicy)之憑證簽發者的簡要聲明(TerseStatement)欄位會記載憑證專屬之用途及限制之交易對象。
- 限定範圍內多用途：若於憑證中憑證政策之憑證簽發者的簡要聲明欄位有記載代碼者，其限定範圍多用途依其代碼而定；若無記載者，應依本公司簽署之合約或本公司網站之公告為主。

(3) 第三段為用戶身分：

區分為(1)法人、(2)自然人。

(4) 第四段為適用業務範圍(Business Category)：

區分為(1)金融交易、電子商務應用、網路報稅、電子發票、電子通訊投票、短期票券發行交易應用、(2)有價證券交易、電子商務應用、網路報稅、電子發票、電子通訊投票、(3)電子商務應用、線上身分確認、網路報稅、電子發票、電子通訊投票、線上申請專利商標、電子郵件應用、程式代碼簽署、PDF 文件簽署、電子文件或訊息之簽章時間證明；其中金融交易用憑證亦得於符合使用範圍限制之規範或本公司同意下，使用於有價證券交易及電子商務應用、線上身分確認。

例如:網路銀行現行企業憑證之使用範圍代碼為 3.1.1.1 解讀如下：

(3)安全性第三級·(1)單一用途·(1)法人用戶·(1)金融交易使用。

二、憑證交易限額及賠償責任

資安憑證、AATL 憑證、時戳憑證之交易限額及賠償限額說明如下：

(1) 交易限額：依安全性、用途別、客戶身分及適用業務範圍等分別訂定不同之交易限額；用戶進行交易時，其交易金額不可超出該使用範圍代碼所對應之交易限額。

(2) 賠償限額：依安全性、用途別、用戶身分等分別訂定不同之賠償限額；該賠償限額係指對用戶單一憑證之賠償上限，亦即不論交易次數多寡，單一憑證之累積賠償金額均不得超過賠償限額。

(3) 若用戶與本公司訂有合約，另行載明憑證使用範圍、交易限額及賠償限額者，從其約定。

(4) 限定範圍內多用途：用戶憑證的使用範圍，須依本公司簽署之合約或本公司訂定相關的作業管理規範並公告於本公司網站。

憑證使用範圍及賠償責任表如下所示：

〈表一〉 單位：新台幣元

使用範圍代碼	安全等級	用途別	用戶身分	適用業務範圍	交易限額	賠償限額
1.1.1.3	第一級	單一用途	法人	電子商務應用、線上身分確認	3,000	3,000
1.1.2.3	第一級	單一用途	自然人	電子商務應用、線上身分確認	3,000	3,000

2.1.1.3	第二級	單一用途	法人	電子商務應用、線上身分確認、電子郵件應用、PDF 文件簽署	900,000	300,000
2.1.2.3	第二級	單一用途	自然人	電子商務應用、線上身分確認、電子郵件應用、PDF 文件簽署	300,000	100,000
3.1.1.1	第三級	單一用途	法人	金融交易	不限定	2,000,000
3.2.1.1	第三級	限定範圍內多用途	法人	金融交易、電子商務應用、網路報稅、電子發票、電子通訊投票、短期票券發行交易應用	不限定	2,000,000
3.1.2.1	第三級	單一用途	自然人	金融交易	不限定	300,000
3.2.2.1	第三級	限定範圍內多用途	自然人	金融交易、電子商務應用、網路報稅、電子通訊投票、短期票券發行交易應用	不限定	300,000
3.1.1.2	第三級	單一用途	法人	有價證券交易	100,000,000	2,000,000
3.2.1.2	第三級	限定範圍內多用途	法人	有價證券交易、電子商務應用、網路報稅、電子發票、電子通訊投票	100,000,000	2,000,000
3.1.2.2	第三級	單一用途	自然人	有價證券交易	15,000,000	300,000
3.2.2.2	第三級	限定範圍內多用途	自然人	有價證券交易、電子商務應用、網路報稅、電子通訊投票	15,000,000	300,000
3.1.1.3	第三級	單一用途	法人	電子商務應用、線上身分確認、線上申請專利商標、程式代碼簽署、PDF 文件簽署、電子文件或訊息之簽章時間證明	20,000,000	2,000,000
3.2.1.3	第三級	限定範圍內多用途	法人	電子商務應用、線上身分確認、網路報稅、電子發票、電子通訊投票、PDF 文件簽署	20,000,000	2,000,000
3.1.2.3	第三級	單一用途	自然人	電子商務應用、線上身分確認、線上申請專利商標、程式代碼簽署、PDF 文件簽署	2,000,000	300,000

3.2.2.3	第三級	限定範圍內多用途	自然人	電子商務應用、線上身分確認、網路報稅、電子通訊投票、PDF 文件簽署	2,000,000	300,000
註 1：憑證內載明之使用範圍代碼若不在上述表列中，此憑證即不得使用於測試以外之任何應用或業務，且本公司對此憑證不負賠償責任。 註 2：憑證使用範圍代碼載明於憑證內之「憑證政策(Certificate Policy:CP)憑證簽發者的簡要聲明(TerseStatement)」欄位。						

1.4.3 憑證之禁止使用情形

本憑證管理中心所簽發之憑證除使用於上述規定之範圍，不得用於竊聽或攔截第三方通訊，禁止用於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，且禁止使用於電子簽章法、其他相關法令或各事業目的主管機關明訂禁止或排除之應用或業務。

1.5 政策管理

1.5.1 管理單位

本作業基準的制定、修訂、發布等事宜，其權責單位為 PMA。

1.5.2 聯絡窗口

對本作業基準有任何疑義，或相關資安通報(如金鑰外洩疑慮或憑證誤發等)，可將詳細內容與聯絡資訊透過下列窗口進行聯繫：

公司名稱	臺灣網路認證股份有限公司(TAIWAN-CA INC.；TWCA)
聯絡人	客服中心
地址	台北市中正區(100)延平南路 85 號 10 樓 10TH Floor, 85, Yen-Ping South Road, Taipei, Taiwan, R.O.C
電話	886-2-23708886
傳真	886-2-23700728
電子郵箱	ca@twca.com.tw

1.5.3 憑證實務作業基準之核定

本憑證管理中心所訂定之憑證實務作業基準，須經由 PMA 核定。

1.5.4 憑證實務作業基準核定程序

依據電子簽章法規定，本憑證管理中心訂定之憑證實務作業基準，必須經主管機關核定後，始得對外公布本作業基準並提供憑證簽發服務。

1.6 名詞與簡稱

參考附錄二。

2. 公布及儲存庫

2.1 儲存庫

本憑證管理中心之儲存庫提供憑證、憑證廢止清冊、憑證政策及憑證實務作業基準等憑證作業相關資訊之查詢或下載；另亦提供線上憑證狀態查詢(OCSP)服務。

儲存庫的網址為：

https://www.twca.com.tw/repository

CRL 與 OCSP 之儲存庫位址載明於憑證擴充欄位中，詳細資訊參閱第 7 章。

2.2 憑證資訊之公布

本憑證管理中心公布之資訊如下：

(1) 憑證政策及本作業基準。

(2) 本憑證管理中心憑證與相關資訊。

(3) 簽發之憑證。

(4) 憑證廢止清冊(CRL)。

(5) 憑證廢止狀態(OCSP)。

2.3 公布頻率

本作業基準經主管機關核定後即公布於儲存庫。

憑證廢止清冊(CRL)之公布頻率參考 4.9.7 節之規定。

本憑證管理中心須定期檢閱本作業基準，且每年至少修訂本作業基準 1 次。

2.4 儲存庫之存取控制

本作業基準及儲存庫資訊可公開讀取，但為防止惡意攻擊或竄改，於更新儲存庫資訊或流量異常時須進行存取控制。

3.識別與鑑別

3.1 命名

3.1.1 名稱種類

本憑證管理中心簽發以 X.501 命名格式為主體名稱之 X.509 憑證。

一、 本憑證管理中心簽發之用戶憑證識別名稱：

(一)資安憑證

識別名稱(DN)	說明	識別名稱內容範例	是否必要
Country(C)	憑證主體之國別	TW	○
Organization(O)	CA 公司政策的資訊或憑證申請者組織資訊	Information	○
OrganizationUnit(OU)	CA(簽發單位)的資訊或憑證申請者組織單位資訊(1)	TaiCA Information User CA	X
OrganizationUnit(OU)	註冊中心英文識別名稱或憑證申請者組織單位資訊(2)	12345678-RA-Trade	X
OrganizationUnit(OU)	註冊中心應用或服務識別名稱或憑證申請者組織單位資訊(3)	Trade	X
CommonName(CN)	憑證申請者的識別名稱，例如企業的營利事業統一編號或其他可識別之名稱	12345678-01-000	○
註 1：若資安憑證具有 S/MIME 功能，則其增強金鑰使用方法(Extended Key Usage)必須具有 emailProtection、主體別名擴充欄位(Subject Alternative Name)中須記載 Email 識別名稱，且識別名稱之 Organization(O)為非必要。 註 2：本作業基準將資安憑證中具有 S/MIME 功能之憑證簡稱為「S/MIME 憑證」。			

(二) AATL 憑證

識別名稱(DN)	說明	識別名稱內容範例	是否必要
Country(C)	憑證主體之國別	TW	○
Organization(O)	CA 公司政策的資訊或憑證申請者組織資訊	TAIWAN-CA Inc.	○
OrganizationUnit(OU)	CA(簽發單位)的資訊或憑證申請者組織單位資訊(1)	TWCA InfoSec User CA	X
OrganizationUnit(OU)	註冊中心英文識別名稱或憑證申請者組織單位資訊(2)	70759028-RA-AATL	X
OrganizationUnit(OU)	註冊中心應用或服務識別名稱或憑證申請者組織單位資訊(3)	Information Security	X
CommonName(CN)	憑證申請者的識別名稱或其他可識別之名稱或其他經確認之資訊	70759028-AATL	○

(三) 時戳憑證

識別名稱(DN)	說明	識別名稱內容範例	是否必要
Country(C)	憑證機構之國別	TW	○
Organization (O)	憑證機構一般識別名稱	TAIWAN-CA Inc.	○
CommonName(CN)	時戳憑證專屬 CN	70759028-01-TSA	○

二、用戶憑證管理中心自身憑證之識別名稱：

(一) 資安 UCA 的自身憑證

識別名稱(DN)	說明
Country(C)	C=TW
Organization(O)	O=TAIWAN-CA Inc.
OrganizationUnit(OU)	OU=User CA
CommonName(CN)	CN=TWCA InfoSec User CA

(二) 時戳 UCA 的自身憑證

識別名稱(DN)	說明
Country(C)	C=TW
Organization(O)	O=TAIWAN-CA
OrganizationUnit(OU)	OU= Timestamping Sub-CA
CommonName(CN)	CN= TWCA Timestamping Certification Authority

三、最高層憑證管理中心自身憑證之識別名稱：

識別名稱(DN)	說明
Country(C)	C=TW
Organization(O)	O=TAIWAN-CA
OrganizationUnit(OU)	OU=Root CA
CommonName(CN)	CN=TWCA Root Certification Authority

或

識別名稱(DN)	說明
Country(C)	C=TW
Organization(O)	O=TAIWAN-CA
OrganizationUnit(OU)	OU=Root CA
CommonName(CN)	CN=TWCA Global Root CA

或

識別名稱(DN)	說明
Country(C)	C=TW
Organization(O)	O=TAIWAN-CA
OrganizationUnit(OU)	OU=Root CA
CommonName(CN)	CN=TWCA Global Root CA G2

3.1.2 識別名稱之意義

用戶憑證所記載之主體識別名稱，須符合相關法令及規範對於命名之規定，必須足以識別特定之法人單位及自然人，且必須可為信賴憑證者所識別。

3.1.3 用戶之匿名與假名

本作業基準不允許用戶使用匿名、假名、別名或筆名等。

3.1.4 各種名稱的解釋規則

憑證所記載之名稱，其名稱形式之解釋規則依 ITU-T X.520 名稱屬性定義。

3.1.5 名稱的唯一性

本憑證管理中心將審核用戶中、英文名稱及法人識別名稱之唯一性。

3.1.6 識別名稱糾紛的處理

當用戶憑證使用之唯一識別名稱有相同時，本憑證管理中心以先申請註冊並通過組織身分與網域鑑別之用戶優先使用，後申請註冊用戶若較先申請註冊用戶先通過身分資訊確認得優先使用。

如因識別名稱之使用有爭議時，經主管機關/機構合法文件證實為其他申請者所擁有時，本憑證管理中心須註銷已註冊之用戶唯一識別名稱使用權，並廢止已簽發之憑證，且該用戶須負擔相關法律責任。

3.1.7 商標之辨識、鑑別及角色

本憑證管理中心尊重用戶中、英文名稱之註冊商標，於查證後接受用戶使用該中、英文名稱，但不保證用戶註冊商標之認可、驗證與唯一性。若註冊商標發生糾紛時，用戶須自行循法律途徑處理。

3.2 初始驗證

初始驗證目的在於防止偽冒申請，並且申請者提供之身分資料真實性經過確認。為此，註冊中心進行身分驗證時須秉持以下原則：

(1) 對所收集的身分證明資料完成真實性(Authenticity)驗證、有效性(Validation)驗證，以及與申請者之連結性(Linkage)驗證，其驗證強度須與憑證保證等級相匹配。

(2) 若申請者委託代理人辦理，須具備可驗證之授權機制以完成代理人之身分及授權驗證。

(3) 最後登錄之身分資料須由申請者進行確認，以確保擬登錄之資料與申請人提交時的一致，且為申請人之正確資訊。

3.2.1 證明擁有私密金鑰的方式

憑證內公開金鑰及對應之私密金鑰須由用戶自行產製，並提供 PKCS#10 憑證申請檔且以私密金鑰簽章後交付本憑證管理中心，作為擁有私密金鑰之證明。本憑證管理中心將以用戶之公開金鑰，驗證用戶對 PKCS#10 憑證申請檔之簽章訊息，來確認用戶為私密金鑰擁有者、公開金鑰與私密金鑰成對及用戶身分資訊之完整性。

3.2.2 法人身分的鑑別

法人身分的鑑別方式依照其所申請之憑證保證等級(定義於 1.4.1 節)而有所不同，具體驗證方式描述如下：

保證等級	法人身分識別方式
測試級	測試級無須驗證，參閱 1.4.1 說明。
第一級	1. 法人用戶以自我主張之身分資訊進行註冊。 2. 註冊中心須檢核該資訊之唯一性並進行有限之查證。
第二級	1. 須滿足前述第一級相關檢核。 2. 法人用戶須提交證據證明其法人身分資訊。 3. 註冊中心須檢核該證據的存在性和有效性。
第三級	1. 須滿足前述第二級相關檢核。 2. 代表人或持有授權文件之代理人，須提供足以識別法人身分之證明文件。 3. 註冊中心須以類似於當面辦理認證強度的方式辦理，並查詢信賴的第三方權威資訊(例如工商登記查詢)，檢查法人用戶主張

	之身分資訊或只有該法人用戶所知的資訊。
第四級	1. 須滿足前述第三級相關檢核。 2. 註冊中心須以當面認證的方式辦理。

若申請憑證種類為 S/MIME 憑證，除以上法人查驗外，須進行「電子郵件位址查驗」，以確認申請者是否為合法之法人組織，以及確認憑證申請者具有該電子郵件信箱之所有權或控制權。

下列針對「電子郵件位址查驗」之查驗方式進行描述：

- 電子郵件位址查驗：本憑證管理中心(以下簡稱本中心)至少使用一項下述之查驗作業程序，對申請者欲於憑證內申請之電子郵件位址進行使用權或所有權之查驗：

  1. 本中心使用電子郵件傳遞一個具有 24 小時效期之亂數值給指定收件人，其中該收件人為未來簽發之 S/MIME 憑證的主體別名(Subject Alternative Name；SAN)中指定之收件人，再由本中心驗證該亂數值。

  2. 本中心使用網域名稱查驗確認電子郵件位址的所有權，其中網域名稱為完整電子郵件位址於"@"後之網域名稱，驗證方式可使用以下「網域名稱查驗」中所定義之任一驗證方式。

- 網域名稱查驗：本憑證管理中心(以下簡稱本中心)至少依一項下述由 CA/Browser Forum 公布之「Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates」(以下簡稱為 SSL BR) 3.2.2.4 節所定義之查驗作業程序，對申請者欲於憑證內申請之網域名稱進行使用權、所有權之查驗：

  (1) 本中心使用電子郵件、傳真、簡訊、郵遞等方式傳遞一個唯一且效期 30 天之亂數值給網域聯絡人(Domain Contact)，再由本中心驗證該亂數值。其中網域聯絡人之定義遵循 SSL BR 1.6.1 節之定義。查驗方式遵循 SSL BR 3.2.2.4.2 節。

  (2) 本中心使用電子郵件傳遞一個唯一且效期 30 天之亂數值給指定收件人，再由本中心驗證該亂數值，其中收件人電子郵件地址限定：admin 或 administrator 或 webmaster 或 hostmaster 或 postmaster 等名稱再接續"@"及欲驗證網域名稱。查驗方式遵循 SSL BR 3.2.2.4.4 節。

  (3) 申請單位於欲驗證網域 DNS 服務內之 CNAME、TXT 或 CAA 等資源紀錄中以欲驗證網域名稱或欲驗證網域名稱前放置以底線符號(Underscore)開頭之標籤值(Label)命名之，再於其中放置一個唯一之 Request Token 值後，由本中心確認之。查驗方式遵循 SSL BR 3.2.2.4.7

節。

(4) 本中心使用電子郵件傳遞一個唯一且效期 30 天之亂數值給指定收件人，再由本中心驗證該亂數值，其中收件人電子郵件地址來自欲驗證網域名稱之 DNS CAA 資源紀錄中的聯絡人 Email，且該 CAA 資源紀錄須以 RFC 8659 Section 3 所定義之搜尋演算法取得之。查驗方式遵循 SSL BR 3.2.2.4.13 節。

(5) 本中心使用電子郵件傳遞一個唯一且效期 30 天之亂數值給指定收件人，再由本中心驗證該亂數值，其中收件人電子郵件地址來自欲驗證網域名稱之 DNS TXT 資源紀錄中的聯絡人 Email。查驗方式遵循 SSL BR 3.2.2.4.14 節。

(6) 本中心致電給網域聯絡人(Domain Contact)，並取得其對該網域名稱之授權確認。其中網域聯絡人之定義遵循 SSL BR 1.6.1 節之定義。查驗方式遵循 SSL BR 3.2.2.4.15 節。

(7) 本中心致電給聯絡人，並取得其對該網域名稱之授權確認，其中聯絡人電話來自欲驗證網域名稱之 DNS TXT 資源紀錄中的聯絡人電話。查驗方式遵循 SSL BR 3.2.2.4.16 節。

(8) 本中心致電給聯絡人，並取得其對該網域名稱之授權確認，其中聯絡人電話來自欲驗證網域名稱之 DNS CAA 資源紀錄中的聯絡人電話，且記載該聯絡人之 CAA 資源紀錄須以 RFC 8659 Section 3 所定義之搜尋演算法取得之。查驗方式遵循 SSL BR 3.2.2.4.17 節。

上述查驗方式，須搭配參考 public suffix list 資訊，應用於網域名稱查驗。

3.2.3 個人用戶身分的鑑別

個人用戶身分的鑑別方式依照其所申請之憑證保證等級(定義於 1.4.1 節)而有所不同，具體驗證方式描述如下：

保證等級	個人身分識別方式
測試級	測試級無須驗證，參閱 1.4.1 說明。
第一級	1. 個人用戶以自我主張之身分資訊進行註冊。 2. 註冊中心須檢核該資訊之唯一性並進行有限之查證。
第二級	1. 須滿足前述第一級相關檢核。 2. 個人用戶須提交證據證明其個人身分資訊(例如個人身分證影本)。 3. 註冊中心須檢核該證據的存在性和有效性。

第三級	1. 須滿足第二級相關要求。 2. 本人或持有授權文件之代理人,須提供足以識別個人身分之證明文件。 3. 註冊中心須以類似於當面認證強度的方式辦理,並查詢信賴的第三方權威資訊(例如內政部身分確認服務),檢查用戶主張之身分資訊或只有該用戶所知的資訊。
第四級	不適用。

若申請憑證種類為 S/MIME 憑證，須進行「電子郵件位址查驗」以確認憑證申請者具有該電子郵件信箱之所有權或控制權。其驗證方式同「3.2.2 法人身分的鑑別：電子郵件位址查驗」。

3.2.4 未驗證之用戶資訊

本憑證管理中心對所有用戶資訊皆須進行驗證。

3.2.5 權限之驗證

法人之代表人、代理人及法人(下稱該等人)之身分證明文件，須為官方核發之證明文件(下稱該文件)；註冊中心須確認代理人授權文件之真偽，該等人須具結該文件為真實。

3.2.6 相互溝通方式

無規定。

3.3 金鑰更新之識別與鑑別

3.3.1 憑證例行性金鑰更新

隨著金鑰使用時間增加，其可能遺失或遭破解之風險增加，用戶須定期更新金鑰以確保金鑰之安全性。

當用戶金鑰(即憑證)的生命效期訂定為一年，於一年後到期時必須更新，即是用戶憑證的有效期限為一年,在有效期限屆滿前的憑證更新期內(例如,屆滿前一個月),用戶必須自己重新產生一組公開金鑰及私密金鑰對，並向本憑證管理中心/註冊中心申請新憑證的簽發，此為憑證及私密金鑰的更新(Rekey)。

資安憑證、AATL 憑證的用戶憑證有效期限最長為 39 個月(私密金鑰的有效期限與憑證相同)，惟 S/MIME 憑證之有效期限上限為 825 天。

資安憑證、AATL 憑證的用戶，於憑證有效期限屆滿前，將新產生的公開金鑰憑證申請訊息以使用中有效的私密金鑰簽章後，傳遞至註冊中心申請新憑證簽發。

資安憑證、AATL 憑證於憑證有效期限屆滿後用戶執行憑證及私密金鑰的更新時，用戶必須以 3.2 節規定之身分鑑別方式向註冊中心申請憑證更新，待取得註冊中心的憑證更新申請時之身分認證識別資料後，用戶將帶有新私密金鑰簽章的憑證申請訊息與用戶身分認證識別資訊，依註冊中心作業規範至本憑證管理中心/註冊中心申請新憑證簽發；註冊中心於收妥用戶憑證申請訊息時，除驗證私密金鑰擁有的合法性外，並驗證用戶憑證申請訊息的合法性與完整性。

時戳憑證私密金鑰有效期限最長為 15 個月，時戳憑證有效期限最長為 135 個月。

時戳私密金鑰於有效期限屆滿前，須重新產製金鑰對並申請新的時戳憑證。

3.3.2 憑證廢止後之金鑰更新

用戶之憑證廢止後，必須重新進行如 3.2 節規定之初始驗證方式或其他能有效確認用戶身分的方式，重新申請新憑證。

3.4 憑證廢止請求

當用戶提出憑證廢止請求時，本憑證管理中心將對憑證廢止請求進行鑑別，作業程序如 4.9.3 節。

4. 憑證生命週期管理

4.1 憑證申請

4.1.1 憑證申請者

欲申請憑證之法人機構，以代表人或其代理人為憑證申請者。

自然人本身即為憑證申請者。

4.1.2 註冊申請程序及責任

用戶須向註冊中心申請憑證的簽發，申請憑證前必須向註冊中心完成用戶註冊申請。

(1) 註冊中心必須向用戶詳細說明憑證申請單與合約書上之權利與義務規範，相關業務運作的作業流程與提供使用說明與操作文件，且須由用戶同意並確認。

(2) 用戶須正確且詳實的填寫相關申請單與提供相關證明文件，註冊中心依身分認證安全等級的作業規範，驗證用戶身分與證明文件無誤後，設定用戶身分識別代碼與保護密碼，完成用戶註冊申請作業。

4.2 憑證申請程序

4.2.1 識別與鑑別程序

各安全等級的身分鑑別程序如 1.4.1 節。身分識別與鑑別程序如 3.2 節。

4.2.2 接受或拒絕憑證申請

完成 4.2.1 節識別與鑑別程序後，視為憑證申請通過；如未能完成識別與鑑別程序，須拒絕憑證申請。

4.2.3 憑證申請處理時間

以用戶與本公司所簽合約為準。

4.3 憑證簽發

4.3.1 憑證機構簽發憑證

資安 UCA 憑證、AATL 憑證、時戳憑證之憑證核發程序如下：

(1) 用戶至少經過身分識別碼及密碼的檢核驗證，登入至註冊中心，將產生的憑證申請訊息經由用戶私密金鑰簽章後傳送至註冊中心。

(2) 註冊中心驗證用戶身分識別碼及密碼正確無誤後，檢核用戶憑證申請訊息的完整性，正確無誤後，將用戶憑證申請訊息以註冊中心的私密金鑰簽章，經加密保護後傳送至本憑證管理中心。

(3) 本憑證管理中心之審查人員透過雙因子驗證登入憑證管理網站進行 3.2 節定義之驗證程序，並由另一審查人員進行覆核程序，確定資料皆無誤後，即可簽發憑證並傳送至註冊中心。

(4) 註冊中心檢核本憑證管理中心傳回之用戶憑證回覆訊息的合法性與完整性，正確無誤後，將用戶憑證傳送予申請人。

(5) 本憑證管理中心簽發之用戶憑證中的憑證起始日不回溯過去時間，即憑證起始日不會早於憑證簽發之當下時間。

註冊中心或本憑證管理中心為安全管控措施的考量，得將憑證申請與私密金鑰產生的軟體，以可信賴且具安全管控措施的方式遞送予用戶，且該軟體必須經由註冊中心或本憑證管理中心適當的安全評估與驗證。

4.3.2 憑證機構簽發憑證通知用戶

即時線上申請簽發之用戶，於本憑證管理中心於完成憑證簽發作業後即可得知簽發結果。

非即時線上申請簽發之用戶，於本憑證管理中心於完成憑證簽發作業後以電話或電子郵件方式通知用戶。

4.4 憑證接受

4.4.1 憑證接受之程序

用戶於收到本憑證管理中心簽發之憑證後，須進行以下程序：

(1) 確認憑證內容與申請時之一致性，且為用戶之正確資訊。

(2) 檢查憑證內之公開金鑰，是否與 PKCS#10 憑證申請檔內之公開金鑰資訊相同。

(3) 用戶必須驗證該憑證之憑證鏈，檢驗其內每張憑證的正確性、完整性與有效性，並確認憑證是否已廢止、憑證有效期限是否已結束、是否確為本憑證管理中心所簽發。

(4) 當發現憑證有誤時，須立即告知註冊中心廢止憑證，並得重新進行 4.3 節憑證簽發程序。

(5) 用戶於收到所申請之憑證後，必須確認已充分了解並同意其使用憑證之權利及義務，若不同意則視為拒絕接受憑證，用戶須告知註冊中心廢止憑證。

本憑證管理中心僅接受用戶於憑證核發後 7 天內，向本憑證中心提出憑證變更請求。

4.4.2 憑證機構公布憑證

本憑證管理中心於用戶完成接受之程序後，即將簽發之用戶憑證公布於儲存庫。

4.4.3 憑證機構通知其他機構憑證簽發

無規定。

4.5 金鑰對及憑證用途

4.5.1 用戶私密金鑰及憑證的使用

用戶憑證的用途、適用範圍及限制，如 1.4 節之規定。

用戶須妥善保護其私密金鑰，若有被冒用、曝露或遺失等不安全疑慮時，必須向註冊中心辦理申告。

4.5.2 信賴憑證者使用公開金鑰及憑證

信賴憑證者於信賴本憑證管理中心簽發之用戶憑證前，至少須進行以下必要之程序以決定是否信賴該憑證：

(1) 透過適當及安全之管道，取得本憑證管理中心之最高層憑證管理中心自簽憑證。

(2) 檢查最高層憑證管理中心自簽憑證、用戶憑證管理中心憑證及用戶憑證是否已過期。

(3) 以最高層憑證管理中心自簽憑證之公開金鑰，驗證用戶憑證管理中心憑證之數位簽章是否有效且並未被廢止。

(4) 以用戶憑證管理中心憑證之公開金鑰，驗證用戶憑證之數位簽章是否有效。

(5) 檢查用戶憑證未遭用戶憑證管理中心廢止。

如未能通過前述驗證，表示信賴憑證者取得之用戶憑證非本憑證管理中心所簽發，或憑證已失效，信賴憑證者不可信賴該用戶憑證。

4.6 憑證展期

憑證展期(renewal)係指用戶識別資訊不變之情況下，重新簽發一張與原有憑證具相同金鑰、不同序號、以及效期延長之憑證。

本憑證管理中心不提供憑證展期服務。

4.7 憑證更新

憑證更新係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 憑證更新之事由

如 3.3.1 節之規定。

4.7.2 有權更新憑證者

用戶有權更新憑證。

4.7.3 憑證更新程序

- 依照 3.3 節之規定對用戶進行身分識別與鑑別。
- 依照 4.3 節之規定簽發憑證。

4.7.4 憑證更新簽發之通知

依 4.3.2 節之規定。

4.7.5 更新後憑證接受之程序

依 4.4 節之規定。

4.7.6 憑證機構公布更新憑證

依 4.4.2 節之規定。

4.7.7 更新憑證後對其他機構之通知

依 4.4.3 節之規定。

4.8 憑證變更

憑證變更係指憑證之公開金鑰不變，但其所記載之用戶名稱識別資訊須變更時，重新簽發憑證予用戶。

本憑證管理中心不接受用戶進行憑證變更，如用戶之識別資訊或其他記載於憑證之資訊須變更時須依 4.9 節之規定廢止憑證後，依 4.1、4.2、4.3、4.4 節規定重新申請憑證簽發。

4.9 憑證廢止及暫時停用

當廢止狀況發生時，相關憑證須被廢止並加入 CRL/OCSP，遭廢止之憑證必須包含於之後所公布的 CRL/OCSP，直到憑證到期為止。

4.9.1 憑證廢止之事由

於憑證仍然為有效期間內，當有下述情況時必須執行憑證廢止：

(1) 用戶：

- 用戶欲廢止該憑證的使用，例如：公司員工的職務異動或離職時，為控管措施的安全考量，或用戶擬不繼續使用憑證而廢止。
- 憑證內容及用戶註冊相關資訊有更動時，例如：公司的整合與合併，或因特殊原因而更新公司的註冊名稱及註冊相關資料。
- 與憑證相關的私密金鑰有毀損、遺失、曝露、被篡改，或有為第三者竊用之慮時。

(2) 本憑證管理中心得逕行廢止用戶憑證：

- 因憑證系統的金鑰異動變更、或不適用、或憑證系統的整合需求。
- 憑證機構的業務結束營運管理而必須移轉至其他憑證機構的需求。
- 用戶使用憑證而為註冊中心(本憑證管理中心)宣告未依據合約或作業規範履行應盡義務(如費用)，或不當使用憑證而違反政府法令、規章、或業務使用規範時。
- 憑證內容的用戶相關資訊，不符合憑證政策、本作業基準或業務使用規範時，例如用戶憑證內容與註冊資料不符，或因註冊資料輸入的疏忽或憑證申請未獲正當授權。

(3) 權責單位：

- 主管機關或法院，因業務之需求依照正式合法作業程序申請。

針對 S/MIME 憑證，當有下述情況時必須執行憑證廢止：

(1) 用戶告知原始憑證申請未獲得授權。

(2) 用戶憑證關聯的私密金鑰經證實或懷疑遭破解、毀損、遺失、曝露、被竄改時。

(3) 用戶將憑證使用於用戶合約之外的用途。

(4) 用戶違反主管機關之法令、憑證政策、本憑證實務作業基準或用戶合約時。

(5) 用戶已不再使用憑證中記載之 Email。

(6) 憑證中所記載之用戶資訊異動。

(7) 憑證未依本憑證管理中心之憑證政策或憑證實務作業基準之規定程序簽發時。

(8) 憑證中所記載之資訊不正確。

(9) 本憑證管理中心簽發憑證的權力已逾期、被廢止或被中止；除非已安排繼續維護 CRL 與 OCSP 服務。

(10) 本憑證中心使用之金鑰經證實或懷疑遭破解、毀損、遺失、曝露、被竄改時。

(11) 憑證政策規定須廢止項目。

(12) 簽發憑證時違反本作業基準或 MRSP(Mozilla Root Store Policy)之規定時。

當上述狀況發生時，相關憑證應被廢止並加入憑證廢止清冊。遭廢止之憑證必須包含於之後所公布的憑證廢止清冊，直到憑證到期為止。

4.9.2 有權請求廢止憑證者

與用戶有關的註冊中心或本憑證管理中心、主管機關或合法授權的第三者及用戶皆有權申請憑證的廢止。

(1) 用戶：

- 用戶可依照其需求，依註冊中心作業規範申請廢止用戶憑證。

(2) 註冊中心(本憑證管理中心)：

- 註冊中心(本憑證管理中心)申請廢止用戶憑證時，必須依照「4.9.3 憑證廢止程序」處理，且必須依註冊中心與用戶間的合約與相關作業規範辦理。

(3) 有權責的第三者：

- 公司授權人員於公司合法授權下，廢止用戶憑證。
- 用戶財產合法繼承人的申請，註冊中心必須依相關作業規範，驗證用戶的死亡與合法繼承人的身分。

- 法院因訴訟與仲裁經註冊中心的申請，但必須符合本公司的相關作業規範。
- 主管機關，並符合相關法令與規範的申請。

4.9.3 憑證廢止程序

(1) 人工申請：

用戶提出憑證廢止請求，經本憑證管理中心檢核用戶身分無誤後，由作業人員執行憑證廢止作業。

(2) 網際網路申請：

用戶登入註冊中心憑證系統的網頁，經註冊中心檢核用戶身分無誤後，由本憑證管理中心憑證系統執行憑證廢止作業。

註冊中心收到本憑證管理中心的用戶廢止憑證回覆訊息時，檢核回覆訊息的合法性與完整性，正確無誤後回覆予申請的用戶。

主管機關、法院與訴訟仲裁單位及其他有權責者，須以書函方式向註冊中心提出申請。

4.9.4 憑證廢止請求提出期限

用戶於憑證廢止事由發生後，須於一般商業運作慣例之合理期限內提出憑證廢止請求，本作業基準不強制規定期限。如懷疑或證實金鑰遭破解或有其他安全事項須廢止憑證，用戶須於 24 小時內提出。

本憑證管理中心提供線上 24 x 7 受理憑證廢止申請及憑證不當使用回報，接受後處理機制如 4.9.5 節。

4.9.5 憑證機構處理憑證廢止請求時限

註冊中心(或本憑證管理中心)收到用戶憑證廢止請求或不當使用回報訊息時，於營運或上班時間必須立刻處理，且至多於 1 個工作天內完成。

4.9.6 信賴憑證者憑證廢止驗證規定

信賴憑證者須根據其風險、責任及可能導致之後果，自行決定透過 CRL 或 OCSP 來確認本憑證管理中心簽發憑證之狀態，並決定查詢頻率。

若信賴憑證者透過本憑證管理中心簽發之 CRL 檢查憑證狀態，使用前須驗證 CRL 是否為本憑證管理中心簽發，包含驗證 CRL 數位簽章之正確性與有效性，其他驗證注意事項須滿足 RFC 5280 相關要求。

若信賴憑證者透過本憑證管理中心簽發之 OCSP 訊息檢查憑證狀態，使用前須驗證 OCSP 是否為本憑證管理中心之 OCSP Responder 簽發，包含驗證 OCSP 訊息之數位簽章是否正確與有效，其他驗證注意事項須滿足 RFC 6960 相關要求。OCSP 相關內容請參閱 4.9.9、4.9.10、7.3 節。

4.9.7 憑證廢止清冊簽發頻率

本憑證管理中心每 24 小時至少更新並簽發 1 次憑證廢止清冊。

4.9.8 憑證廢止清冊最大潛在因素

不做規範。

4.9.9 線上憑證廢止/狀態查詢服務

本憑證管理中心僅對 S/MIME 憑證提供 OCSP 服務，支援以 HTTP GET 或 POST 方式查詢 OCSP 服務，其回應訊息符合 RFC 6960 之規範，內容包含對該訊息之數位簽章。

本憑證管理中心每 24 小時更新 OCSP 服務提供之憑證狀態資訊，效期最長為 4 天，其他相關內容請參閱 7.3 節。

4.9.10 線上廢止/狀態查詢驗證規定

信賴憑證者於決定信賴本憑證管理中心簽發之憑證前，必須透過本憑證管理中心簽發之 CRL 來檢查其憑證狀態。

若信賴 S/MIME 憑證者未使用本憑證管理中心簽發之 CRL 來檢查憑證狀態，則必

須以 4.9.9 節規定之方式，透過 OCSP 服務來檢查憑證狀態。

4.9.11 其他形式之廢止公告

不做規範。

4.9.12 金鑰遭破解之特殊規定

若金鑰疑似遭到破解，通報者可將證明資訊以合法之管道聯繫本憑證管理中心之適當窗口，本憑證管理中心接受以下方式證明金鑰疑似遭到破解：

提供以疑似遭到破解金鑰簽發之 CSR(使用標準 PKCS#10 格式)進行證明，其中 CSR 之 common name 必須為「Proof of Key Compromise for TWCA」，以供本憑證中心驗證其真偽。

本憑證管理中心之簽章金鑰遭破解時，須依照以下程序辦理：

(1) 產生新的簽章用金鑰對及相對應的新憑證。

(2) 廢止所有已簽發之憑證，使用新的簽章金鑰簽發憑證廢止清冊，憑證廢止清冊包含所有已簽發之未到期憑證資訊(含金鑰遭破解前簽發之已廢止憑證)。

(3) 告知用戶。

(4) 安全地遞送新憑證予用戶。

(5) 使用新的簽章用金鑰來簽發新憑證予用戶。

用戶之金鑰被懷疑或證實遭破解，須於知悉該事實 24 小時內告知本憑證管理中心廢止憑證。

4.9.13 憑證暫時停用之事由

一、資安憑證

用戶憑證暫時停用的作業方式悉遵照本憑證管理中心與註冊中心的業務需求與作業規範辦理，若有提供憑證暫時停用服務者，用戶於憑證有效期間內，當有下述情況時可執行憑證的暫時停用：

(1) 用戶：

- 憑證的私密金鑰有可能遺失、洩露的不安全疑慮時，為保留用戶的憑證使用權利而不申請廢止憑證時,用戶欲暫時停用該憑證的使用。
- 用戶欲暫時停止使用該憑證一段時間。

(2) 註冊中心/本憑證管理中心：

- 用戶使用憑證而為註冊中心/本憑證管理中心宣告未履行應盡義務(例如：費用)，或不當使用憑證而有可能違反政府法律、規章、本作業基準或業務使用規範的疑慮時。

(3) 權責單位：

- 主管機關或法院，因業務之需求依照作業程序申請。

二、AATL 憑證

AATL 憑證不提供憑證暫時停用服務。

三、時戳憑證

時戳憑證不提供憑證暫時停用服務。

4.9.14 有權請求憑證暫時停用者

一、資安憑證

與用戶有關的註冊中心或本憑證管理中心、主管機關或合法授權的第三者及用戶皆有權執行憑證的暫時停用。

(1) 用戶：

- 用戶可依照其需求，依註冊中心作業規範申請暫時停用用戶憑證。

(2) 註冊中心(本憑證管理中心)：

- 註冊中心(本憑證管理中心)申請暫時停用用戶憑證時，必須依照「4.9.15 憑證暫時停用程序」處理，且必須依註冊中心與用戶間的合約與相關作業規範辦理。

(3) 有權責的第三者：

- 公司人員於公司合法授權下，申請暫時停用用戶憑證。
- 法院因訴訟與仲裁經註冊中心的申請，但必須符合本憑證管理中心的相關作業規範。
- 主管機關，符合相關法令與規範的申請。

二、AATL 憑證

AATL 憑證不適用。

三、時戳憑證

時戳憑證不適用。

4.9.15 憑證暫時停用程序

一、資安憑證

(1) 當面辦理：

用戶提出憑證暫時停用請求，經本憑證管理中心檢核用戶身分無誤後，由作業人員執行憑證暫時停用作業。

(2) 非當面辦理：

用戶登入註冊中心憑證系統的網頁，經註冊中心檢核用戶身分無誤後，由本憑證管理中心憑證系統執行憑證暫時停用作業。

註冊中心收到本憑證管理中心的用戶憑證暫時停用回覆訊息時，檢核回覆訊息的合法性與完整性，正確無誤後回覆予申請的用戶。

主管機關、法院與訴訟仲裁單位及其他有權責者，須以書函方式向註冊中心提出申請。

暫時停用憑證於限制之原因解除後，憑證用戶擬繼續使用該張憑證，且憑證之有效期限尚未到期時，憑證用戶可向註冊中心申請憑證之解禁，使憑證成為有效且可以使用。

二、AATL 憑證

AATL 憑證不適用。

三、時戳憑證

時戳憑證不適用。

4.9.16 憑證暫時停用期間限制

一、資安憑證

用戶執行憑證暫時停用完成後，於憑證有效期間終止前，如未執行憑證的解禁，則此張憑證皆存在廢止憑證清冊中，為無法使用的憑證。

憑證暫時停用時效為，當用戶憑證經完成暫時停用後存放至憑證廢止清冊中，至用戶申請憑證解禁完成，而憑證從憑證廢止清冊中移轉成有效憑證為止的期間，是為憑證的暫時停用時效，此段期間如至超過憑證有效期限仍未執行憑證解禁時，則此張憑證即為過期憑證(與廢止憑證同為無法使用的憑證)。

憑證暫時停用的時效最長為本憑證管理中心簽發用戶憑證的有效期限。

二、AATL 憑證

AATL 憑證不適用。

三、時戳憑證

時戳憑證不適用。

4.10 憑證狀態服務

4.10.1 服務特性

用戶透過本憑證管理中心提供之 CRL、OCSP 服務查詢憑證狀態。已廢止憑證之憑證廢止資訊，在該憑證效期屆滿後，才會自 CRL 和 OCSP 服務中移除。

4.10.2 服務之可用性

本憑證管理中心提供線上 24x7 之儲存庫供信賴憑證者查詢所有未過期憑證之憑證狀態。

本憑證管理中心所簽發之用戶憑證皆可透過 CRL 查詢其憑證狀態；S/MIME 憑證亦可透過 OCSP 服務查詢憑證狀態。

在網路正常運作之情況下，本憑證管理中心提供之 CRL、OCSP 服務的回應時間在 10 秒以內。

本憑證管理中心提供 24x7 之投訴機制，用以回應重大憑證問題(例如憑證遭冒名申請或誤發)之投訴，投訴經確認後，將遭投訴之憑證逕行廢止，若有違法事件將轉知執法機構。本憑證管理中心之聯繫窗口參考 1.5.2 節。

4.10.3 附加功能

參閱 4.9.9, 4.9.11 節之規定。

4.11 憑證終止使用

當本憑證管理中心簽發之憑證效期屆滿、憑證廢止或本憑證管理中心結束營運時，已簽發之憑證即告失效。

4.12 金鑰託管及復原

4.12.1 金鑰託管及復原政策與施行

本憑證管理中心及用戶的金鑰不得進行金鑰託管。

4.12.2 加密期間金鑰封裝及復原政策與施行

不做規範。

5.實體、管理及作業流程控管

本憑證管理中心之安全控管遵循 CA/Browser Forum 公布之「NETWORK AND CERTIFCATE SYSTEM SECURITY REQUIREMENTS」規範。

5.1 實體控管

5.1.1 建築物與位置

本憑證管理中心機房位於本公司，符合儲存高重要性及敏感性資訊的機房設施水準，並結合門禁、保全、入侵偵測及監視錄影等實體安全機制，以防止未經授權者存取本憑證管理中心之相關設備。

5.1.2 實體進出管制

本憑證管理中心機房之進出管制措施如下：

(1) 3 道門禁之身分查核(以智慧卡或指紋識別)識別管制，其中至少 2 道必須同時兩人以上經過身分鑑別後才可進入；具備 24 小時 CCTV 位移監控錄影設備、及紅外線防入侵警報系統，以記錄進出機房之狀況及預防未經授權者進入機房。

(2) 本憑證管理中心運作之私密金鑰備份相關資料，皆妥善安全地存放於設有監控錄影系統保護之保險櫃內。憑證管理系統運作之相關作業人員，須 2 人以上方可執行憑證管理作業，且皆有監控錄影設備之監測。

(3) 軟硬體及硬體密碼模組等設備，皆置於有監控錄影系統保護之環境下，須 2 人以上方可執行金鑰管理相關作業。

5.1.3 電力與空調

本憑證管理中心機房設有柴油發電機及不斷電系統(Uninterruptible Power Supply；UPS)，當一般供電系統異常時，會自動切換至柴油發電機供電，切換過程由 UPS 提供穩定之電力。

具備獨立之空調系統，確保系統運作的穩定與提供最佳之工作環境，並定期執行維護與測試。

5.1.4 防水處理

本憑證管理中心之機房為密閉式建築物，除內部可進出之出入門外，外部皆為混凝土建築物，且樓層地板裝置高架地板無進水之顧慮。

5.1.5 防火

本憑證管理中心機房建置之材質為防火材質並配置具有中央監控系統之滅火設備，於偵測到火災發生時，能自動啟動滅火功能。

5.1.6 媒體儲存

本憑證管理中心之媒體儲存環境，可避免媒體意外損毀，對磁性媒體具有防磁、防靜電干擾之設備與環境；重要資料備份媒體儲存於具防火功能之保險櫃，其中 1 份備份資訊之媒體儲存於具有安全管控措施之異地備援地點。

5.1.7 廢棄處理

本憑證管理中心所使用之硬體設備、磁碟機與密碼設備等，於廢棄不使用時，其所儲存之商業敏感性及隱密性資訊必須經過安全之清除與銷毀，且須經由稽核單位之驗證，並留存查核文件。

文件與媒體若有儲存商業敏感性及隱密性資訊者，於廢棄處理時必須經過安全之清除與銷毀，使該資訊無法回復與存取使用，且須經由稽核單位之驗證，並留存查核文件。

5.1.8 異地備援

本憑證管理中心設置有異地備援機房，並設置備援設備，當日常營運之設備因外力因素無法正常運作時，備援設備可提供本憑證管理中心持續營運的能力。

本憑證管理中心運作所須之相關媒體資訊與文件，經備份後儲存於具備溫濕度管控、防磁、防靜電干擾，且具有監控攝影機監控錄影，與人員進出須經過授權之高度安全管控異地備援環境。

本憑證管理中心之備份紀錄檔，皆儲存於具高度安全管控之異地備援機房。

5.2 作業程序控管

5.2.1 信賴角色

本憑證管理中心於公開金鑰基礎建設(PKI)的架構下，憑證管理作業必須在具備嚴密性、安全性的作業流程下進行。為使職務與權責之區分，及職務之備援不危及整體系統之安全性及營運之完整性，本憑證管理中心之信賴角色及其分工如下：

(1) 系統管理人員(Administrator)負責系統安裝、管理作業及環境參數設定。

(2) 憑證主管人員(Officer)負責憑證簽發及憑證廢止。

(3) 稽核人員(Auditor)負責進行內部稽核、檢視並維護稽核紀錄。

(4) 操作人員(Operator)負責例行性維護作業，如備份、還原、網站資料維護等。

5.2.2 作業人員需求人數

各種信賴角色的作業人數需求如下：

(1) 系統管理人員(Administrator)至少 2 名。

(2) 憑證主管人員(Officer)至少 2 名。

(3) 稽核人員(Auditor)至少 1 名。

(4) 操作人員(Operator)至少 2 名。

5.2.3 角色的識別與鑑別

本憑證管理中心執行憑證管理作業之系統管理人員、憑證主管人員、稽核人員與操作人員，於系統資源之使用上皆有依業務區分，並使用唯一之身分識別碼、智慧卡及相關之身分識別驗證密碼，以達到信賴角色之身分識別與鑑別。

相關作業人員依業務需求執行之作業功能，每筆皆有詳細之紀錄，確保系統資源使用之可稽核性，並可評估系統安全威脅及風險。

5.2.4 角色隔離

角　色	憑證主管人員	系統管理人員	稽核人員	操作人員
憑證主管人員	O	X	X	X
系統管理人員	X	O	X	O
稽核人員	X	X	O	X
操作人員	X	O	X	O

5.3 人員控管

5.3.1 背景、適任條件與經歷

(1) 本憑證管理中心之作業人員，必須具備忠實、可信賴及工作之熱誠，無影響憑證作業之其他兼職工作，且無違法及信用不良之紀錄。

(2) 憑證主管人員至少具備憑證作業之實務經驗，或經過憑證相關作業之訓練而通過測驗者。

(3) 系統管理人員至少具備憑證作業之實務經驗，並具有電腦系統規劃及營運管理之經驗。

5.3.2 背景審核程序

本憑證管理中心工作人員，須由人事管理相關部門依背景審核規範，執行身分背景安全審查，並由相關作業部門執行實務與經歷審查，審查通過後始可任職。每年必須依各種作業人員之職務特性，執行實務與經歷之審查，作為該員是否適任相關之工作或作為執行工作調整之依據。

5.3.3 教育訓練

本憑證管理中心作業人員，皆依照其職務，施予本憑證管理中心系統運作所須具備之軟硬體功能、作業程序、憑證核發審驗程序、安控程序、災變備援作業規範、金鑰管理作業及憑證政策與本作業基準與其他資訊安全相關作業規範之教育訓練，

憑證系統有異動或有新系統加入時，亦須給予適當之教育訓練。

針對憑證管理系統相關硬軟體、應用系統與安全管理系統，本憑證管理中心制定有完整之教育訓練規範，於新進人員雇用或本憑證管理中心系統有異動時，均施行相關技能之教育訓練，教育訓練完成後有詳實之成果紀錄，作為相關作業人員工作委任之參考。

5.3.4 教育訓練的頻率與需求

針對憑證管理系統運作相關人員，本憑證管理中心將就其執行憑證管理系統運作之相關知識與技能，每年至少進行 1 次檢討，並給予適當之教育訓練；憑證管理系統功能之更新、或新系統之加入、或公開金鑰基礎建設相關知識與技術之進步與更新，皆對系統運作之相關人員進行教育訓練。

5.3.5 職務的輪調

(1) 系統管理人員調離原職務滿 1 年後，才可轉任憑證主管人員或稽核人員。

(2) 憑證主管人員調離原職務滿 1 年後，才可轉任系統管理人員或稽核人員。

(3) 稽核人員調離原職務滿 1 年後，才可轉任系統管理人員或憑證主管人員。

(4) 擔任操作人員滿 2 年，且已接受相關教育訓練並通過審核後，才可轉任系統管理人員、憑證主管人員及稽核人員。

5.3.6 非授權作業的處罰

本憑證管理中心憑證管理系統運作之相關作業人員，因故意或過失而執行非自己職務上之作業時，無論是否造成憑證管理系統安全之問題，皆須即刻呈報監督管理者，並依照相關作業之規範處理。

5.3.7 委外人員需求

若本憑證管理中心因人力資源不足而委由外包人員擔任操作人員時，本憑證管理中心必須對其進行如 5.3.2 節之背景審查程序後，施以如 5.3.3 節職務上知識與技能之教育訓練，該外包人員除須簽訂與工作內容相關之保密合約外，並須遵守相關作業規範與法律規範；該外包人員之權利義務與本憑證管理中心內部操作人員相同。

5.3.8 作業文件需求

為使憑證管理系統正常運作，本憑證管理中心必須提供相關作業人員執行系統運轉之作業文件，至少包含如下：

(1) 硬體、軟體作業平台之操作文件、網路系統與網站相關之操作文件、密碼系統之操作文件。

(2) 本憑證管理中心憑證管理系統之相關操作文件。

(3) 本憑證作業基準、憑證政策及相關作業規範文件。

(4) 本憑證管理中心憑證管理系統內部作業文件，例如：系統備援與回復作業文件、異地災變備援與回復作業文件、例行工作作業文件。

5.4 稽核紀錄程序

5.4.1 事件紀錄類型

本憑證管理中心的每筆稽核紀錄，無論是採自動或手動方式紀錄，均包含下列項目：

(1) 事件類型。

(2) 事件發生日期及時間。

(3) 事件成功或失敗之結果。

(4) 引發此事件之個體或人員。

(5) 事件內容描述。

以下是本憑證管理中心所記錄的稽核事件種類：

(1) 安全稽核

- 任何重要稽核參數之改變，如稽核事件型態、新舊參數的內容等。
- 任何嘗試刪除或修改稽核紀錄檔。

(2) 人員及信賴角色管理、識別及鑑別

- 新角色的設定不論成功或失敗。

- 身分鑑別嘗試的最高容忍次數改變。
- 使用者登入系統時身分鑑別嘗試的失敗次數之最大值。
- 管理者將已被鎖住的帳號解鎖。
- 管理者改變系統的身分鑑別機制，例如從通行密碼改為生物特徵值。

(3) 金鑰作業程序

- 產製金鑰。
- 銷毀金鑰。

(4) 私密金鑰之載入和儲存

- 載入私密金鑰到系統元件中。

(5) 可信賴公開金鑰之新增、刪除及儲存

- 可信賴公開金鑰之改變，包括新增、刪除及儲存。

(6) 私密金鑰之輸出

- 私密金鑰之輸出(不包括只用在單次或只限 1 次使用之金鑰)。

(7) 憑證之註冊/簽發

- 憑證之註冊申請過程。
- 憑證之發行。

(8) 廢止憑證

- 憑證之廢止申請過程。
- CRL 產製記錄。
- OCSP 服務簽章記錄。

(9) 憑證狀態改變之核可

- 核可或拒絕憑證狀態改變之申請。

(10) 組態設定

- 安全組態相關設定之改變。

(11) 帳號之管理

- 加入或刪除角色和使用者。

- 修改使用者帳號或角色之存取權限。

(12) 憑證剖繪之管理

- 憑證剖繪之改變。

(13) 憑證廢止清冊剖繪之管理

- 憑證廢止清冊剖繪之改變。

(14) 系統安裝及營運重要事件

- 安裝作業系統。
- 安裝憑證管理系統。
- 安裝硬體密碼模組。
- 移除硬體密碼模組。
- 銷毀硬體密碼模組。
- 啟動系統。
- 嘗試登入憑證管理系統。
- 硬體及軟體之接收。
- 嘗試設定通行密碼。
- 嘗試修改通行密碼。
- 本憑證管理中心之內部資料備份。
- 本憑證管理中心之內部資料回復。
- 檔案操作(例如產生、重新命名及移動等)。
- 傳送任何資訊到儲存庫。
- 存取本憑證管理中心之內部資料庫。
- 金鑰被破解。
- 本憑證管理中心之金鑰更換。

(15) 改變本憑證管理中心伺服器之設定

- 硬體。
- 軟體。
- 作業系統。
- 修補程式(Patches)。
- 安全剖繪。

(16) 實體存取及場所之安全。

- 人員進出本憑證管理中心之機房。
- 存取本憑證管理中心之伺服器。
- 知悉或懷疑違反實體安全規定。

(17) 異常事件

- 軟體錯誤。
- 軟體檢查完整性失敗。
- 接收錯誤格式之訊息。
- 非正常路由之訊息。
- 網路攻擊(懷疑或確定)。
- 設備失效。
- 電力不當。
- 不斷電系統失效。
- 明顯及重大的網路服務或存取失敗。
- 違反本作業基準。
- 重設系統時鐘。

5.4.2 紀錄處理頻率

本憑證管理中心至少每月會檢視 1 次稽核紀錄，追蹤調查發生的事件。檢視工作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，並加以解釋及提出相對預防再發生的方案。

5.4.3 稽核紀錄保留期限

本憑證管理中心相關稽核紀錄報表與媒體資料至少保留 7 年且不得早於相關金鑰銷毀、憑證過期、廢止後 2 年。

5.4.4 稽核紀錄的保護

(1) 確保只有經授權人員可以讀取稽核紀錄，只有經授權人員可以備份稽核紀錄。

(2) 使用簽章或加密技術保存目前和已歸檔之電子式稽核紀錄，並儲存於不可覆

寫光碟片或其他無法更改稽核紀錄的媒體。

(3) 保護事件紀錄的金鑰不能再使用於其他用途。

(4) 紙張及實體的稽核紀錄存放於安全場所。

5.4.5 稽核紀錄備份程序

電子式稽核紀錄每月至少備份 1 次，並儲存於本憑證管理中心外，並依 ISO 或相關標準所選定之備援地點。

5.4.6 稽核紀錄彙整系統

稽核系統內建於本憑證管理中心憑證管理系統中，稽核程序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，保護系統資料完整性、機密性的安全機制處於高風險狀態時，本憑證管理中心將暫停憑證簽發服務，直到問題解決後再行提供服務。

5.4.7 對引發事件者之告知

如因發生事件而被稽核系統紀錄，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紀錄。

5.4.8 脆弱性評鑑

每年進行 1 次以下所列的各種脆弱性評鑑：

(1) 識別可預見的內部和外部威脅，這些威脅可能導致未經授權存取，資訊洩露，資訊濫用，資料遭竄改或破壞任何憑證資料或憑證管理流程。

(2) 評鑑威脅發生的可能性，以及發生時憑證資料和憑證管理流程可能的損害。

(3) 評鑑本憑證管理中心目前適用之資訊安全政策、管理程序、資訊技術以及其他防護措施，是否足以防禦威脅。

5.5 紀錄歸檔

5.5.1 歸檔紀錄類型

本憑證管理中心歸檔紀錄包含以下種類：

(1) 被稽核驗證(Accreditation)資料。

(2) 憑證實務作業基準。

(3) 用戶合約。

(4) 系統與設備組態設定。

(5) 系統或組態設定修改與更新的內容。

(6) 憑證申請資料。

(7) 廢止申請資料。

(8) 憑證接受的確認文件。

(9) 已簽發或公告的憑證。

(10) 本身金鑰更換的紀錄。

(11) 已簽發或公告的憑證廢止清冊。

(12) 稽核紀錄。

(13) 用來驗證及佐證歸檔內容的其它說明資料或應用程式。

(14) 公正稽核人員要求的文件。

(15) 用戶身分鑑別資料。

5.5.2 歸檔紀錄保存期限

本憑證管理中心之歸檔資料至少保留 7 年且不得早於相關金鑰銷毀、憑證過期、廢止後 2 年。

5.5.3 歸檔紀錄的保護

已歸檔資料不可進行寫入、修改或刪除的動作；屬於用戶之個別已歸檔資料，允許對該用戶或其他法規允許之機構釋出。

歸檔資料必須保存 1 份於本憑證管理中心所在地外，具安全管控措施，且對儲存媒體具備損壞預防措施之異地備援地點。

5.5.4 歸檔紀錄的備份程序

金鑰、憑證、交易資料等相關資料，依照備份與備援回復的作業程序，每日、週、月的整理歸檔及備份，1 份儲存於本公司具安全管控措施的環境下，且 1 份保存資料儲存於具安全管控措施的異地備援環境，當憑證系統異常無法開啟時，依系統備份與回復作業手冊，以保存的備份資料執行憑證系統的回復作業。

5.5.5 歸檔紀錄之時戳要求

歸檔之電子式紀錄(例如憑證、憑證廢止清冊及稽核紀錄等)包含日期與時間資訊，且這些紀錄皆經過適當的數位簽章或加密演算保護，可用以檢測紀錄中的日期與時間資訊是否遭到竄改。惟此電子式紀錄中的日期與時間資訊並非公正第三者所提供之電子式時戳資料，而是電腦作業系統的日期與時間。

本憑證管理中心的所有電腦系統都會定期進行校時，以確保電子式紀錄中日期與時間資訊的準確性與可信度。

歸檔的書面紀錄也將記載日期資訊，必要時並將記載時間資訊。書面紀錄的日期與時間紀錄不可任意更改，如須更改必須由稽核人員簽名確認。

5.5.6 歸檔紀錄彙整系統

本憑證管理中心作業相關的歸檔紀錄資訊，皆由本公司內部的作業人員執行，於具有資源權責獨立及安全的管控措施下產生；稽核紀錄蒐集的保存資訊亦是由內部的管控系統所產生，憑證管理系統運作的相關文件歸檔紀錄，由權責的業務相關人員蒐集與管理。

5.5.7 取得及驗證歸檔紀錄之程序

必須以書面申請獲得正式授權後，才可取得歸檔資料；歸檔資料由稽核人員負責驗證，書面文件必須驗證文件簽發者及日期等之真偽，電子檔則驗證歸檔資料的數位簽章或以密碼學方式驗證。

5.6 金鑰更新

為降低本憑證管理中心簽章用金鑰遭破解的風險，簽章用金鑰必須定期進行更新。

用戶憑證管理中心進行金鑰更新時，會產製一對新的金鑰對，交由最高層憑證管理中心簽發憑證後，依照 6.1.4 節規定供信賴憑證者查詢下載。

用戶之金鑰效期，須考慮金鑰長度、保護方式、控制方式及其他各種因素，且不可違反 6.1.5 節之規定。

5.6.1 用戶憑證管理中心金鑰更新

用戶憑證管理中心簽發用戶憑證之金鑰，其有效期間等同於對應憑證之生命週期，不得超過 10 年。

用戶憑證管理中心進行金鑰更新時，會產製一對新的金鑰對，交由最高層憑證管理中心簽發憑證後，依照 6.1.4 節規定供信賴憑證者查詢下載。

用戶憑證管理中心金鑰使用有效期限結束時，可以產生新金鑰對向最高層憑證管理中心申請新憑證的簽發，並即刻通知註冊中心，完成後以新私密金鑰簽發用戶憑證，舊金鑰將繼續簽發 CRL，直至該舊金鑰的生命週期結束。

當用戶憑證管理中心舊金鑰有不安全顧慮且有效期限尚未結束時，必須先向最高憑證管理中心申請廢止舊憑證，才可以產生新金鑰對並簽發新憑證，完成後以新私密金鑰簽發用戶憑證與 CRL，並即刻通知用戶與註冊中心，先前使用用戶憑證管理中心之舊私密金鑰所簽發的用戶憑證與 CRL 皆失效，用戶必須重新產生新金鑰對向用戶憑證管理中心申請新憑證的簽發。

5.6.2 最高層憑證管理中心金鑰更新

最高層憑證管理中心簽發下屬憑證之金鑰，其有效期間等同於對應憑證之生命週

期，不得超過 25 年。

最高層憑證管理中心於金鑰使用有效期限結束前，產製一對新金鑰對及自簽憑證，並立即公告此新自簽憑證，且即刻通知下屬憑證管理中心。原舊金鑰繼續簽發 CRL，直至該舊金鑰的生命週期結束。

當最高層憑證管理中心憑證有效期限尚未結束之金鑰有不安全疑慮時，必須先廢止憑證，才可以產生新金鑰對及自簽憑證，並即刻通知下屬憑證管理中心，此時，下屬憑證管理中心的憑證皆已無效，必須重新產生新金鑰對向最高層憑證管理中心申請新憑證的簽發。

當最高層憑證管理中心私密金鑰遭破解時，須廢止全部下屬憑證管理中心的憑證，並通知下屬憑證管理中心，逕行廢止全部用戶的憑證，且通知業務應用系統停止使用下屬憑證管理中心所簽發的憑證。

5.7 金鑰遭破解及災變復原程序

5.7.1 金鑰遭破解及緊急應變處理程序

若用戶憑證管理中心金鑰遭破解或遺失(雖尚未確定是否可能遭破解)，則須進行下列程序：

(1) 必須儘快透過安全電子郵件或書面方式，通知所有用戶及最高層憑證管理中心。

(2) 依 6.1 節的規定產生新的金鑰對並交由最高層憑證管理中心簽發新憑證。

(3) 廢止所有已簽發之憑證，使用新的簽章金鑰簽發憑證廢止清冊，憑證廢止清冊包含所有已簽發之未到期憑證資訊(含金鑰遭破解前簽發之已廢止憑證)。

(4) 依 4.3 節的程序，簽發新的憑證給各用戶。

(5) 將事故資訊通報並揭露給信賴憑證者及各 Root CA 信賴清單維護組織。

若最高憑證管理中心金鑰遭破解或遺失，則須進行下列程序：

(1) 必須儘快透過安全電子郵件或書面方式，通知所有下屬憑證管理中心，逕行廢止全部用戶的憑證。

(2) 廢止所有已簽發之憑證。

(3) 依 6.1 節的規定產生新的金鑰對與自簽憑證。

(4) 簽發新的憑證給下屬憑證管理中心。

(5) 將事故資訊通報並揭露給信賴憑證者及各 Root CA 信賴清單維護組織。

本憑證管理中心必須調查，並向 PMA 報告金鑰遭破解或遺失之原因，以及採取何種措施以避免發生相同狀況。

本憑證管理中心訂定有緊急應變處理程序和災難復原計畫，以書面記載業務持續計畫與災變復原程序，內容包含當發生災難、安全性遭破解以及營運中斷事件時，對軟體商(例如瀏覽器廠商)、用戶及信賴憑證者之告知程序；以上程序本憑證管理中心將每年定期檢視或修訂。

若本憑證管理中心誤發或未依本作業基準簽發 S/MIME 用戶憑證時，亦會將事故揭示於 Bugzilla 中。

5.7.2 電腦資源、軟體及資料損毀之處理程序

本憑證管理中心訂定電腦資源、軟體及資料遭破壞之復原程序，同時每年進行演練。

如本憑證管理中心的電腦設備遭破壞或無法運作，但簽章金鑰並未損毀，則優先回復儲存庫之運作，並迅速重建憑證簽發、廢止及管理的功能。

5.7.3 個體金鑰遭破解之處理程序

用戶之金鑰懷疑遭破解時，須依 4.9.3 節之方式辦理。

5.7.4 災變後之營運持續能力

在發生自然災害或其他災變，以致於無法在 24 小時內恢復憑證狀態服務時，將啟用異地備援機房之設施，並於啟用後 24 小時內恢復提供憑證狀態服務。

5.8 憑證機構終止服務

本憑證管理中心終止服務時，將依電子簽章法相關規定辦理。

本憑證管理中心因故結束其系統營運時，須對系統運作之影響減少至最低程度，而將相關憑證業務安全地轉移至其他憑證機構繼續運作。

於業務正常結束、或合約終止、或公司重整而無安全之考量因素時：

(1) 於終止服務之日 30 天前通知主管機關。

(2) 於終止服務之日 3 個月前，將終止服務及由其他憑證機構承接相關業務之事實通知用戶並公布於儲存庫。

(3) 於無安全顧慮之作業環境下，將結束之本憑證管理中心相關私密金鑰與憑證，移轉至承接之憑證機構。

(4) 將憑證政策、憑證實務作業基準、憑證機構相關作業手冊文件、用戶合約與註冊資料、稽核紀錄、歸檔資料、憑證狀態資料及其他業務承接所必須的相關文件，移轉至承接的憑證機構。

(5) 將本憑證管理中心之相關私密金鑰完全清除，並向用戶正式宣告，憑證業務已移轉至承接的憑證機構繼續營運。

於業務異常結束時(法院宣告破產、或不合法)，本憑證管理中心必須儘早向用戶告知事實，且必須執行業務正常結束時的作業程序，將影響減少至最低程度。

本憑證管理中心結束業務時，相關權利義務亦將依照用戶合約辦理。

6.技術安全控管

6.1 金鑰對的產製及安裝

6.1.1 金鑰對的產生

本憑證管理中心產製自身金鑰對：

(1) 制定並遵循金鑰產製腳本。

(2) 本憑證管理中心依照 6.2.1 節規定，使用至少符合 CNS 15135、ISO 19790、FIPS 140-2 Level 3 或 FIPS 140-3 Level 3 之硬體密碼模組產製金鑰對，私密金鑰在硬體密碼模組內產製後一直儲存在其中而不外洩。

(3) 金鑰產製過程在第三方公正人士見證下進行，金鑰產製程序全程錄影，金鑰產製後由公正人士簽署金鑰產製見證書，以昭公信。

用戶產製金鑰對：

若用戶申請 AATL 憑證，則金鑰儲存載具必須為硬體裝置，相關硬體規格須滿足「Adobe Approved Trust List Technical Requirements」。

6.1.2 私密金鑰遞送至用戶

用戶私密金鑰由憑證用戶自行產製，故無遞送之需求。

6.1.3 公開金鑰遞送至憑證簽發者

公開金鑰是以 PKCS#10 憑證申請檔傳送給本憑證管理中心，其傳送方式須以受安全保護的管道傳送。並且依 3.2.1 節所述之方式完成私密金鑰擁有的驗證程序。

6.1.4 憑證機構公開金鑰遞送至信賴憑證者

本憑證管理中心須將其簽發的憑證公布至儲存庫，供用戶及信賴憑證者查詢下載。

6.1.5 金鑰長度

本憑證管理中心的 RSA 公開金鑰長度至少為 2048 位元，且位元長度必可整除 8；ECC 公開金鑰使用之曲線其安全強度至少為 P-256。

用戶的 RSA 公開金鑰長度至少為 2048 位元，且位元長度必可整除 8；ECC 公開金鑰使用之曲線其安全強度至少為 P-256。

6.1.6 公開金鑰參數的產生及參數品質檢驗

RSA：本憑證管理中心採用 RSA 演算法，質數產生器是採用 ANSI X9.31 演算法產生 RSA 演算法所需的質數，此方法可保證該質數為強質數(Strong Prime)。其中指數(exponent)須包含以下特性：大於等於 3 的奇數且介於 2^16+1 與 2^256-1 之間；模數(modulus)須包含以下特性：奇數、不是質數乘冪且無小於 752 之因數。

ECC：本憑證管理中心使用 ECC 完整公開金鑰驗證程序(ECC Full Public Key Validation Routine)或 ECC 部分公開金鑰驗證程序(ECC Partial Public Key Validation Routine)來確保所有金鑰的有效性。

6.1.7 金鑰使用目的

本憑證管理中心簽發給用戶作為簽章及加密或其他用途使用的憑證，該憑證使用於安控措施用途上的種類區分，用戶必須依照本作業基準與業務應用系統的規範使用，且訂定於 X.509 v3 憑證的標準擴充欄位的金鑰用途欄位(key Usage)，用戶必須依憑證的用途使用於相關的業務系統。

除簽章及加密憑證的需求外，用戶如果有其他用途的憑證需求時，本憑證管理中心得簽發該種用途的金鑰憑證予用戶使用。。

6.2 私密金鑰保護措施及密碼模組工程控管

6.2.1 密碼模組標準

本憑證管理中心使用至少符合 CNS 15135、ISO 19790、FIPS 140-2 Level 3 或 FIPS 140-3 Level 3 之硬體密碼模組來做為私密金鑰的保護設備，並具備多人控管功能。

根據「Adobe Approved Trust List Technical Requirements」要求，AATL 憑證用戶之私密金鑰須產製並儲存於至少符合 FIPS 140-2 Level 2 或 FIPS 140-3 Level 2 或安全等級相當之硬體密碼模組。

6.2.2 私密金鑰分持控管

本憑證管理中心之私密金鑰啟動資料是採 m-out-of-n 的方式由多人分持控管，為一種完全隱密(Perfect Secret)的秘密分享(Secret Sharing)方式，可做為私密金鑰安全啟用、備份及回復方法。

保護私密金鑰相關資訊之智慧卡與個人通行密碼，分別由職務獨立之不同管理人員管控，並儲存於具安全管控措施之環境。

6.2.3 私密金鑰託管

本憑證管理中心之私密金鑰不允許託管，亦不提供憑證用戶私密金鑰託管服務。

6.2.4 私密金鑰的備份

(1) 本憑證管理中心之私密金鑰儲存於硬體密碼模組內，且依照 6.2.2 節以分持控管方法將私密金鑰加密後進行備份，並將加密金鑰分持資訊儲存於高安全性之智慧卡中。

(2) 儲存加密金鑰分持資訊之智慧卡，存放於經雙重控管之安全環境內，由安全控管人員密封保管。

(3) 加密金鑰之分持資訊至少保留 2 份，1 份存放於本憑證管理中心內之安全地點，另一份存放於具安全管控之異地備援地點。

6.2.5 私密金鑰歸檔

本憑證管理中心之私密金鑰不進行歸檔。

6.2.6 私密金鑰自密碼模組輸入或輸出

本憑證管理中心之私密金鑰是在硬體密碼模組中產生及儲存，並且只有在進行金鑰備份回復時，才能將私密金鑰輸入至另一個硬體密碼模組中；自密碼模組輸出時，

依 6.2.4 節規定辦理。

6.2.7 私密金鑰儲存於密碼模組

本憑證管理中心之私密金鑰係以加密型態儲存於密碼模組。

6.2.8 私密金鑰啟動方式

儲存於密碼模組內的私密金鑰必須由 2 人以上之授權憑證主管人員，經身分鑑別後啟動，啟動之方式係透過智慧卡鑑別憑證主管人員身分，且啟動之程序控管措施必須符合 5.2 節之規定。

6.2.9 私密金鑰停用方式

私密金鑰在啟動後，其停用方式是將密碼模組經身分鑑別後以手動關閉或指定時間內無動作後自動登出成為停用狀態，以避免私密金鑰遭非法使用。

6.2.10 私密金鑰銷毀

本憑證管理中心在私密金鑰效期屆滿後，將會把硬體密碼模組中存放之舊私密金鑰的記憶位置零值化(Zeroization)，以銷毀硬體密碼模組中舊的私密金鑰。

除了銷毀硬體密碼模組中之舊私密金鑰外，該舊私密金鑰之備份副本(保留三代)，也將於備份過期時進行實體銷毀，惟遇到必須以金鑰備份副本進行還原時，如還原之金鑰中有已過期之金鑰時，將立即進行刪除。

6.2.11 密碼模組等級

本憑證管理中心使用之硬體密碼模組等級，必須至少符合 CNS 15135、ISO 19790、FIPS 140-2 Level 3 或 FIPS 140-3 Level 3。

6.3 金鑰對管理的其他事項

6.3.1 公開金鑰歸檔

本憑證管理中心所簽發憑證生命週期到期時，將會進行憑證歸檔，並將公開金鑰同時歸檔。

6.3.2 公開金鑰與私密金鑰的有效期限

本憑證管理中心公開金鑰與私密金鑰之有效期限相同。

(1) 最高層管理中心之金鑰對有效期限上限為 25 年。

(2) 用戶憑證管理中心之金鑰對有效期限上限為 10 年。

(3) 資安憑證、AATL 憑證用戶之金鑰對有效期限上限為 39 個月；惟 S/MIME 憑證之金鑰對有效期限上限為 825 天。

(4) 時戳憑證用戶之金鑰對有效期限，私密金鑰上限為 15 個月，公開金鑰效期與憑證效期相同，上限為 135 個月。

6.4 啟動資料

6.4.1 啟動資料產製及安裝

啟動簽章用私密金鑰的啟動資料由多張智慧卡個別產生，並使用多人控管的權限分離(Duty Separation)機制，智慧卡中的啟動資料由讀卡機存取，並以智慧卡的個人識別碼(以下簡稱 PIN 碼)做為啟動資料存取身分鑑別之用。

6.4.2 啟動資料的保護

啟動資料由控管智慧卡組保護，智慧卡的 PIN 碼由保管人員負責保存，不得記錄於任何媒體上，如登入的失敗次數超過 3 次，則鎖住此智慧卡；智慧卡移交時，新的保管人員必須重新設定新的 PIN 碼。

6.4.3 啟動資料的其他考量

無規定。

6.5 電腦安全控管

6.5.1 電腦安全技術需求

本憑證管理中心和相關輔助系統透過作業系統，或結合作業系統、軟體和實體的保護措施提供以下安全控管功能：

(1) 具備身分鑑別與多因子的登入。

(2) 提供自行定義存取控制。

(3) 提供安全稽核能力。

(4) 對於各種憑證服務和信賴角色存取控制的限制。

(5) 具備信賴角色及身分的識別和鑑別。

(6) 確保通訊和資料庫之安全。

(7) 具備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。

6.5.2 電腦系統安全等級

本憑證管理中心使用之電腦作業系統，其安全等級至少需具備 EAL3[ISO / IEC 15408 Common Criteria]或 C2[TCSEC]或 E2[ITSEC]等級的安全標準。

6.6 生命週期技術控管

6.6.1 系統開發控管

本憑證管理中心的系統開發遵循 ISO 27001 的規範。

本憑證管理中心之硬體和軟體僅能使用符合安全政策的元件，不安裝與運作無關的硬體裝置、網路連接或元件軟體，並且在每次使用時會檢查是否有惡意程式碼。

6.6.2 安全管理控管

本憑證管理中心的軟體在首次安裝時，將確認是由開發人員提供正確的版本且未被修改。系統安裝後，每次啟動時驗證軟體的完整性。

本憑證管理中心將記錄和控管系統的組態與功能變更。

6.6.3 生命週期的安全等級

無規定。

6.7 網路安全控管

最高層憑證管理中心憑證系統為離線(Off-Line)、獨立的作業管理系統，且須經授權後由業務相關的作業人員才可以人工方式執行作業。

本憑證管理中心之憑證管理系統須經授權後由業務相關之作業人員才可以執行管理作業，於執行管理作業時，憑證管理系統將對作業人員進行身分鑑別，通過後方可允許執行作業。

為防範網路入侵與破壞，本憑證管理中心之各主機安裝及建置有防火牆、入侵防禦與防毒系統等以增進網路安全，並定期執行系統修補程式更新、系統弱點掃描以加強防護。

本憑證管理中心的主機和內部資料庫僅與內部網路連接並以防火牆隔離，僅允許內部主機連線且必須經過身分鑑別，確認係經授權之人員或系統方可存取。

儲存庫連接到網際網路(Internet)上，提供不中斷之憑證、CRL 及 OCSP 查詢服務(必要之維護或備援狀況除外)。

6.8 時間戳記

本憑證管理中心定時透過信賴時間源進行校時，確保本憑證管理中心各項作業時間值之準確性，包含但不限於以下時間值：

(1) 憑證簽發時間。

(2) 憑證廢止時間。

(3) CRL 簽發時間。

(4) OCSP 簽發時間。

本憑證管理中心簽發之時戳憑證提供本公司之時戳服務機構(Time-stamping authority；TSA)作為簽署文件時戳之用，本公司之時戳服務機構使用的時戳協定滿足 RFC 3161 之要求，同時本公司也遵照 RFC 3628 之規範撰寫時戳實務作業基準，並公開於儲存庫中。

7.憑證、憑證廢止清冊及線上憑證狀態查詢剖繪

7.1 憑證剖繪

7.1.1 版本

本憑證管理中心之憑證及簽發予用戶之憑證版本為 X.509 v3。

7.1.2 憑證擴充欄位

擴充欄位之使用符合 RFC 5280 標準。其憑證各欄位詳細內容請見本憑證管理中心憑證及憑證廢止清冊剖繪。

本憑證管理中心所簽發之 S/MIME 用戶憑證具備以下特性：

(1) 必定具有主體名稱擴充欄位(SAN)記載 Email 識別名稱，其值必須為 rfc822Name 或 otherName 形式。

(2) 增強金鑰使用方法(EKU)必須具有 emailProtection(1.3.6.1.5.5.7.3.4)。

(3) OCSP 服務網址可於憑證機構資訊存取(authorityInfoAccess)擴充欄位中取得。

7.1.3 演算法物件識別碼

本憑證管理中心簽發憑證時使用的演算法物件識別碼如下：

演算法類型	演算法(Algorithm)	物件識別碼(OID)
金鑰	rsaEncryption	{iso(1) member-body(2) us{840} rsadsi(113549) pkcs(1) pkcs-1(1) rsaEncryption(1)}
金鑰	ecPublicKey	{iso(1) member-body(2) us(840) ansi-X9-62(10045) keyType(2) ecPublicKey(1)}
簽章	sha256WithRSAEncryption	{iso(1) member-body(2) us{840} rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)}

簽章	sha384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha384WithRSAEncryption(12)}
簽章	ECDSAWithSHA256	{iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA256(2)}
簽章	ECDSAWithSHA384	{iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA384(3)}

7.1.4 識別名稱格式

本憑證管理中心及用戶之憑證，其憑證主體與發行者名稱皆符合 X.500 唯一識別名稱(Distinguished Name；DN)之命名方式，此名稱的屬性型態遵循 RFC 5280 相關規定。

7.1.5 識別名稱限制

本憑證管理中心簽發之憑證，皆無使用「名稱限制」(nameConstraints)擴充欄位。

7.1.6 憑證政策物件識別碼

本憑證管理中心所簽發之憑證，在憑證內的「憑證政策」(certificatePolicies)擴充欄位中，使用憑證政策所定義的憑證政策物件識別碼。

7.1.7 憑證政策限制擴充欄位的使用

本憑證管理中心所簽發之憑證可視需要包含「政策限制」(policyConstraints)擴充欄位。

7.1.8 憑證政策限定元語法與語意

本憑證管理中心所簽發之憑證皆可視需要包含「政策限定元」(policyQualifier)語法。

7.1.9 憑證政策擴充欄位語意必要的處理

無規定。

7.2 憑證廢止清冊剖繪

可於用戶憑證之 CRL 發布點(cRLDistributionPoints)擴充欄位中取得服務網址。本憑證管理中心簽發 CRL 之頻率如 4.9.7 節規定。

7.2.1 版本

本憑證管理中心簽發 X.509 v2 格式的憑證廢止清冊。

7.2.2 憑證廢止清冊與憑證廢止清冊擴充欄位

各欄位詳細內容請見本憑證管理中心憑證及憑證廢止清冊剖繪。

7.3 線上憑證狀態查詢剖繪

本憑證管理中心提供之 OCSP 服務具有以下特性：

(1) 回覆訊息使用之簽章憑證禁止使用 SHA-1 演算法且此憑證由本憑證管理中心簽發。

(2) 回覆訊息之簽章值禁止使用 SHA-1 演算法。

(3) 回覆訊息之憑證狀態支援：正常(good)、已廢止(revoked)、未知(unknown)。

(4) 當接收到非本憑證管理中心簽發憑證之狀態查詢請求時，將會回覆憑證狀態未知(unknown)之訊息。

(5) 其餘內容參考 4.9.9 節規定。

7.3.1 版本

本憑證管理中心之線上憑證狀態查詢版本為 1.0，符合 RFC6960 規範。

7.3.2 線上憑證狀態查詢擴充欄位

本憑證管理中心之線上憑證狀態查詢，其擴充欄位的使用符合 RFC 6960 規範。

8. 稽核及其他評估方法

8.1 稽核頻率或評估事項

本憑證管理中心至少每年進行 1 次外部稽核及每半年進行 1 次內部稽核。

本憑證管理中心所屬註冊中心，除僅被授權核發特定群組之憑證的外部註冊中心可自行稽核外，其餘註冊中心須接受本憑證管理中心或本憑證管理中心委託的外部稽核進行稽核。

8.2 稽核人員之識別及資格

本憑證管理中心執行內部和外部稽核作業之稽核人員至少必須具備憑證機構、資訊系統安全稽核之知識，有 2 年以上之稽核相關經驗或憑證實務作業經驗，且須熟悉本作業基準之運作規範，以及具有應用系統之作業及電腦硬軟體系統之相關知識與經驗。若主管機關就稽核人員之適任條件有相關規範時，以該規範為準據。

進行外部稽核作業時，委託之稽核業者須符合 MRSP(Mozilla Root Store Policy)之規定且具有國家稽核人員正式資格或國際上認可之稽核資歷，以提供公正客觀的稽核服務。本憑證管理中心於進行稽核時，會先對稽核人員進行資格確認，完成稽核後，稽核報告中亦會條列稽核人員之稽核資歷、具備之稽核證照。

8.3 稽核者與受稽核者之關係

本憑證管理中心執行稽核作業之內部稽核人員與被稽核單位的權責為獨立分工，無任何利害關係足以影響稽核之客觀性，並以獨立、公正、客觀之態度執行查核評估。

本憑證管理中心之外部稽核作業，將委託稽核業者就本憑證管理中心之運作進行稽核。

8.4 稽核項目

稽核內容包括下列項目：

(1) 是否訂定與公告憑證實務作業基準及相關作業規範，包括依憑證實務作業基

準所訂定之作業規範。

(2) 是否依照憑證實務作業基準及相關作業規範執行憑證管理等相關作業，以符合憑證服務之完整性及本憑證管理中心環境之安全控管等相關需求。

(3) 憑證實務作業基準是否符合憑證政策之規定。

本憑證管理中心的稽核規範遵循以下標準：

- WebTrust for CAs v2.2.1 或更新版本。
- WebTrust for CAs SSL Baseline with Network Security v2.5 或更新版本。

8.5 稽核結果之因應

本憑證管理中心的運作經詳細查核評估後，若有不符合憑證實務作業基準的規範時，稽核者須依缺失嚴重等級詳細條列，並將稽核結果通知本憑證管理中心，本憑證管理中心必須依缺失提出矯正與預防措施，並追蹤後續改善情形。

若稽核發現 S/MIME 憑證作業事故，本憑證管理中心會主動將重大缺失揭示於 Bugzilla。

8.6 稽核結果之公開

本憑證管理中心將於儲存庫公布歷次 WebTrust 稽核報告，同時本公司於官網記載取得之國際標章，點擊標章圖示亦可閱覽 WebTrust 稽核報告。

8.7 內部稽核

本憑證管理中心監督其是否遵循憑證政策及憑證實務作業基準，每半年至少進行 1 次內部查核來嚴格控制服務品質。

9. 其他業務及法律規定

9.1 收費

9.1.1 憑證簽發及更新費用

本憑證管理中心簽發憑證予用戶，由本憑證管理中心向用戶收取憑證費用；憑證費用規範於憑證申請表單，或公布於本憑證管理中心網站。

9.1.2 憑證查詢費用

不收費。

9.1.3 憑證廢止及狀態查詢費用

不收費。

9.1.4 其他服務費用

無規定。

9.1.5 退費

用戶於完成憑證申請，但憑證尚未簽發前申請退費者，扣除新臺幣 3 千元的處理工本費後，餘無息退還予用戶；於完成憑證簽發後用戶始申請退費時，按比例扣除使用月份之費用後，再扣除新臺幣 3 千元的處理工本費，餘無息退費。

9.2 賠償責任

9.2.1 賠償責任

(1) 本憑證管理中心處理用戶註冊資料及憑證簽發作業，除未遵照本作業基準、憑證政策及相關作業規範的規定辦理而造成用戶的損失，且可歸責於本憑證管理

中心之過失外，本憑證管理中心不負損害賠償責任。

(2) 本憑證管理中心如因不可抗力的天災事故(例如地震等)，或其他非可歸責於本憑證管理中心之事由(例如戰爭等)，造成用戶損失時，本公司不負損害賠償責任。

(3) 本憑證管理中心如因作業人員故意或過失、未遵照本作業基準、憑證政策及相關作業規範的規定，辦理註冊、憑證的簽發與廢止作業，或違反相關法律規範而造成用戶的損害時，本憑證管理中心須依規定賠償用戶的損害。

(4) 本憑證管理中心或其他有權者提出廢止用戶憑證之要求後，至本憑證管理中心實際公布廢止該用戶憑證(記載於CRL)為止之期間內，如因使用該用戶憑證而產生法律糾紛時，本憑證管理中心如依據本作業基準與相關的作業規範執行處理作業者，則不負損害賠償責任。

(5) 用戶使用非法假造、錯誤的憑證而造成損害時，本憑證管理中心不負損害賠償責任。

(6) 用戶的損害賠償請求權時效期間，依相關法律的規範辦理，雙方須承擔之損害賠償責任，以相關法令規定及合約所定之範圍為責任上限。

9.2.2 其他資產

本憑證管理中心執行憑證業務有關財務運作的稽核作業，每年定期委由公正、客觀的第三機構執行財務運作的查核。

於憑證管理作業有關的風險管理，除已投保建築物與硬體設施的地震及火險外，為分散業務的營運風險，已投保 200 萬美元之一般責任險和 500 萬美元之專業責任險。

9.2.3 對用戶及信賴憑證者之賠償責任

依 9.2.1 節之規定。

9.3 機密資訊

9.3.1 機密資訊的種類

機密資訊包括：

(1) 用於本憑證管理中心營運的私密金鑰及通行密碼。

(2) 控管本憑證管理中心私密金鑰之分持資料。

(3) 用戶申請憑證時，擔任憑證申請者代表人及代理人之個人資料。

(4) 本憑證管理中心產生或保管之可供稽核及追蹤之紀錄。

(5) 稽核人員於稽核過程中產生之稽核紀錄及文件。

(6) 列為機密等級的營運相關文件。

9.3.2 非機密資訊種類

憑證政策、本作業基準、本憑證管理中心簽發之憑證、本憑證管理中心簽發之憑證廢止清冊、外部稽核結果等皆為可公開之資訊。

9.3.3 保護機密資訊之責任

除非符合下列條件之一，否則用戶之註冊基本資料與身分驗證相關資料絕不任意提供予權責管理單位，或其他任何人知悉：

(1) 依法令之規定並經由權責管理單位依法定程序授權。

(2) 具有合法司法管轄權之訴訟仲裁機構處理因憑證產生之糾紛與仲裁，而依法定程序申請之需求。

9.4 個人資訊隱私

9.4.1 隱私保護計畫

本憑證管理中心依照「個人資料保護法相關規範」，及其他政府單位相關的規範運作。

9.4.2 個人資訊隱私種類

依 9.4.1 節之規定。

9.4.3 非個人資訊隱私種類

無規定。

9.4.4 個人資訊隱私保護責任

依相關法令規定辦理。

9.4.5 使用個人資訊隱私之告知與同意

依相關法令規定辦理。

9.4.6 因行政法令或司法要求之揭露

依 9.3.3 節之規定。

9.4.7 其他資訊公開情形

依 9.3.3 節之規定。

9.5 智慧財產權

(1) 本憑證管理中心產製之金鑰對及金鑰分持，其產出為本公司之智慧財產。

(2) 本憑證管理中心所簽發之憑證及憑證廢止清冊為本公司之智慧財產。

(3) 用戶的金鑰對為用戶之智慧財產，但其公開金鑰經本憑證管理中心簽發成憑證時，該憑證為本公司之智慧財產。

(4) 本憑證管理中心將確保用戶名稱之正確性，但不保證記載於用戶憑證主體識別名稱之智慧財產權歸屬。

(5) 本憑證管理中心因執行憑證管理作業而撰寫的相關文件，其智慧財產權為本公司擁有。

(6) 本作業基準之智慧財產權由本公司擁有。

(7) 本作業基準可由本憑證管理中心儲存庫自由下載，或經本公司授權後依著作權法相關規定合理使用。

(8) 合理使用本作業基準者，不得向他人收取費用。

(9) 本憑證管理中心對於不當使用本作業基準所引發之一切結果，不負任何法律責任。

9.6 職責及義務

9.6.1 憑證機構之職責

(1) 訂定、公告與管理憑證業務範圍內的憑證實務作業基準與憑證政策，及憑證運作的相關作業規範。

(2) 確認本憑證管理中心與註冊中心的權責關係，且註冊中心的實務作業必須依本作業基準與憑證政策及相關的規範運作。

(3) 確認憑證系統作業人員(含合約委外人員)的選用與系統運作符合憑證實務作業基準的規範。

(4) 作業人員必須善盡保管用戶註冊與憑證資料及相關訊息之責任，避免相關資訊洩漏、被冒用、篡改及任意使用。

(5) 依照憑證實務作業基準的規範，接受用戶(註冊中心)憑證的申請、更新、暫時停用、廢止、查詢及有關註冊申請訊息，確認註冊中心及用戶發送至本憑證管理中心之相關交易訊息的正確性與完整性，並執行憑證簽發作業及將相關回覆訊息正確且安全的遞送至用戶。

(6) 依據憑證作業規範將用戶與本公司的憑證及廢止憑證清冊正確且安全的遞送至儲存庫。

(7) 必須於與用戶的合約或相關作業文件，詳細說明憑證申請、更新、暫時停用、廢止、註冊與使用的作業規範，及相關的權利與義務關係。

(8) 本憑證管理中心的私密簽章金鑰只可用於用戶憑證與廢止憑證的簽發，如有訊息加密或其他簽章的需求時，必須使用不同且獨立的私密金鑰。

本憑證管理中心審查並擔保下列內容：

- 使用網域或 IP 位址之權利：參考第 3.2.2 節內容。
- 申請憑證之授權：參考第 3.2.2 節內容。

- 資訊的正確性：參考第 3.2.2 節內容。
- 沒有誤導性之資訊：參考第 3.2.2 節內容。
- 申請者的身分：參考第 3.2.2 節內容。

9.6.2 註冊機構之職責

(1) 依本作業基準、憑證政策及註冊中心的作業規範，確認註冊中心與用戶的權責關係，執行用戶註冊身分認證及憑證申請、更新、暫時停用、與廢止相關作業時，申請訊息合法性與完整性的驗證。

(2) 確認註冊中心憑證系統作業人員(含合約委外人員)的選用與系統運作符合憑證實務作業基準、與註冊中心的作業規範。

(3) 註冊中心必須確認用戶於註冊申請時，確實了解且同意申請書與合約書上的權利與義務，及業務相關作業規範的內容，並於用戶親自辦理下簽名確認〈或法人戶的合法授權代理人員之親自辦理下簽名確認〉，或於依據用戶註冊時身分認證安全等級的作業規範，由用戶簽名確認。

(4) 接受用戶註冊、憑證申請、更新、暫時停用、查詢與憑證廢止申請之作業。

(5) 用戶申請註冊時必須驗證用戶身分的合法性與正確性，於用戶申請憑證時，驗證用戶身分的合法性與正確性，完成後通知本憑證管理中心簽發憑證予用戶，並將本憑證管理中心傳回的正確回復訊息安全的遞送予用戶。

(6) 註冊中心與其作業人員必須善盡保管用戶註冊資料及相關訊息之責任、避免相關資訊洩漏、被冒用、篡改及任意使用。

(7) 註冊中心與用戶的合約或相關作業文件，須詳細說明憑證申請、更新、暫時停用、廢止、查詢、註冊與使用的作業規範，及相關的權利與義務關係。

(8) 註冊中心與憑證相對應的私密金鑰有被冒用、曝露及遺失等不安全的顧慮時，或憑證內註冊中心相關的資訊有異動時，必須依相關作業的規定，即刻向簽發該憑證之本憑證管理中心辦理申告與處理。

(9) 註冊中心負責用戶註冊管理作業相關的權責義務，本憑證管理中心負責由註冊中心委託的憑證簽發管理作業相關的權責義務，註冊中心必須提供上述權責義務關係之資訊予用戶及信賴憑證者。

9.6.3 用戶之義務

(1) 用戶向註冊中心申請註冊時，必須提供詳細且正確的身分證明文件與資料。

(2) 用戶向註冊中心申請註冊時，必須確實了解並同意申請書與合約書上的權利與義務，及憑證申請、更新、暫時停用、廢止、註冊與使用的作業規範內容，並且於接受該規範的規定下始可簽名確認。

(3) 用戶必須依本作業基準規範的規定，確實且妥善安全的產製與保護其私密金鑰及私密金鑰保護密碼，除本人外絕無其他任何人知悉與使用。

(4) 用戶於接受本公司所簽發的用戶憑證時，必須驗證用戶及本憑證管理中心身分的合法性，及憑證訊息的完整性與有效性。

(5) 用戶必須了解且同意憑證實務作業基準相關作業規範的規定，合法且正確的使用私密金鑰與憑證於相關的業務系統，無任何違反相關法律的規定與侵害第三者的權利。

(6) 與憑證相對應的私密金鑰有被冒用、曝露及遺失等不安全的顧慮時，或憑證內用戶相關的資訊有異動時，或不再使用該憑證時，用戶必須依相關作業的規定，即刻向註冊中心辦理申告與處理。

9.6.4 信賴憑證者義務

(1) 憑證的使用，信賴憑證者必須了解且同意憑證實務作業基準，與使用之業務系統相關作業規範權利與義務的規定，且依憑證內容所規定的業務範圍，及本作業基準的規範使用於相關的業務系統，無任何違反相關法律的規定與侵害第三者的權利。

(2) 憑證的使用，必須依憑證實務作業基準、應用業務系統作業規範的規定、X.509 憑證標準的規範，由憑證鏈逐一驗證該憑證的正確性及有效性，透過 CRL 或 OCSP 服務驗證憑證狀態是否已遭廢止。若使用 OCSP 服務查詢 S/MIME 憑證時，須先檢查 OCSP 回應之數位簽章。

(3) 驗證交易訊息的有效性時，除驗證用戶憑證的有效性與合法性外，必須依憑證實務作業基準與業務系統相關規範的規定，驗證交易限額、賠償限額、使用業務範圍、及法律的權責關係。

9.6.5 其他成員義務

無規定。

9.7 除外責任

(1) 本憑證管理中心處理用戶註冊資料及憑證簽發作業，除未遵照本作業基準之規定辦理，或違反相關法律規章之規定，或可歸責於本憑證管理中心之過失外，本憑證管理中心不負損害賠償責任。

(2) 本憑證管理中心如因不可抗力之天災事故(例如地震等)，或其他非可歸責於本憑證管理中心之事由(例如戰爭等)，造成用戶及信賴憑證者損失時，本憑證管理中心不負損害賠償責任。

(3) 本憑證管理中心未善盡保管用戶之註冊及憑證相關機密資料，而造成相關資訊洩漏、被冒用、竄改或任意使用致造成第三者遭受損害時，本憑證管理中心須負損害賠償責任。

(4) 本憑證管理中心在收到憑證廢止申請後，最遲於 4.9.5 節規定之時限內完成憑證廢止作業，並於作業完成後依據 4.9.7 節規定之頻率簽發憑證廢止清冊及公告於儲存庫。用戶於憑證廢止清冊未被公布之前，應採取適當之行動，以減少對信賴憑證者之影響，並承擔所有因使用該憑證所引發之責任。

9.8 責任限制

用戶及信賴憑證者，因簽發憑證或使用憑證而發生損害賠償事件時，本憑證管理中心須承擔之損害賠償責任如 1.4.2 節。

9.9 賠償

如 9.2.1 節之規定。

9.10 本文件生效與終止

9.10.1 生效

本作業基準於主管機關依電子簽章法核定通過後，於本憑證管理中心儲存庫公布後即生效。

9.10.2 終止

本作業基準新版本經主管機關核定後公布，原有版本即告終止。

9.10.3 終止及存續之效力

本作業基準之效力，維持至遵循本作業基準所簽發之最後一張憑證到期或廢止為止。

9.11 通知與聯絡方式

本憑證管理中心將以適當的方式，與用戶建立聯絡管道，包括但不限以下方式：電話、傳真或 Email。

9.12 變更及公告

9.12.1 變更程序

(1) 本作業基準之權責管理單位為 PMA，每年至少檢視本作業基準 1 次。修訂方式包括以附加文件方式修訂或直接修訂本作業基準的內容。

(2) 如憑證政策修訂或物件識別碼變更時，本作業基準將配合修訂。

(3) 如因法律規範改變、國際標準更新等因素而須變更時，本作業基準亦將做相對應的變更。

(4) 本作業基準之修訂經主管機關審查核定後，將依照第 2 章規定公布於儲存庫。

9.12.2 變更聯絡機制

(1) 對本作業基準有建議更新時，請將詳細的建議文件郵寄或 Email 至 1.5.2 節的聯絡窗口，交由 PMA 審議。

(2) 本作業基準之修訂經主管機關審查核定後，公布於本憑證管理中心之儲存庫供下載。

(3) 除另有規定外，本憑證管理中心以 9.11 節規定之方式，做為與用戶間之變更

聯絡機制。

9.12.3 物件識別碼變更條件

本作業基準引用之憑證政策物件識別碼，於本作業基準內容變更時不會更動，僅增加本作業基準之版本識別代碼。

9.13 爭議處理程序

用戶對本憑證管理中心服務或其簽發憑證之使用如有爭議時，依以下規定辦理：

(1) 爭議之雙方須本誠信原則，於合理的方式下雙方盡力協商解決之。

(2) 爭議之雙方如無法於30天內合理的協商解決爭議，則必須指派具適任能力的公正第三協調者，以進行協調並解決爭議，且雙方必須同意協調者的協商與裁決。

(3) 爭議之雙方如無法於60天內同意協調者的協商與裁決，雙方同意以臺北地方法院為第一審管轄法院。

(4) 於爭議協商、訴訟處理過程所發生的費用分擔，依據協商或相關的法律規範處理。

(5) 如遇跨國或跨區域之爭議，無法以上述的處理方式解決時，則必須依照相關的跨國或跨區域的糾紛仲裁規範處理。

9.14 政府管理法規

本作業基準訂定的內容與本憑證管理中心相關業務的執行與釋義，皆遵循主管機關之相關法令規定辦理，且遵循中華民國之相關法律規範。

9.15 法規之符合性

本作業基準及本憑證管理中心應符合電子簽章法及其施行細則之規定。

9.16 各項條款

9.16.1 完整合約

無規定。

9.16.2 轉讓

無規定。

9.16.3 存續性

本作業基準的某些章節規定有不適用而必須修正時，其他條文的規定仍屬有效，不受該項不適用之規定影響，直到新版之本作業基準更新完成並公告。

本作業基準之更新依 9.12 節規定辦理。

9.16.4 施行

無規定。

9.16.5 不可抗力

本憑證管理中心如因不可抗力之天災事故(例如地震等)或其他不可歸責於本憑證管理中心之事由(例如戰爭等)，本憑證管理中心不負損害賠償責任。

9.17 其他條款

無規定。

附錄一 詞彙(Glossary)

(1).網際網路(Internet)

許多不同的電腦網路相互連結，經過標準的通訊協定，得以相互交換資訊。

(2).(電子)訊息((Electronic)Message)

指文字、聲音、影像、符號或其他資料，以電子、磁性或人之知覺無法直接認識之方式，所製成足以表示其用意之紀錄，而供電子處理之用者。

(3).RSA 演算法(RSA Algorithm)

是一種非對稱加密演算法，由 Ron Rivest、Adi Shamir 和 Leonard Adleman 於 1977 年提出，其安全強度建構於針對大數做質因數分解的困難性上。

(4).橢圓曲線密碼學(Elliptic Curve Cryptography；ECC)

是一種基於橢圓曲線數學的公開密鑰加密演算法，由 Neal Koblitz 和 Victor Miller 於 1985 年提出，其安全強度建構於解決橢圓曲線離散對數問題的困難性上。

(5). ECC P-256 曲線 (ECC P-256 Curve)

由 NIST 於 FIPS 186-3 中所制定之橢圓曲線標準，其定義了橢圓曲線之相關參數 p, a, b, G, n, h，其中曲線之基點 G 的 x、y 座標長度分別為 256 bits。

(6).電子簽章(Electronic Signature)

指以電子型式存在之資料訊息，依附在電子文件可用以辨識及確認電子文件簽署人身分及簽署人以數位、聲音、指紋、或其他生物光學技術的特性產生的訊息，其依附在電子訊息上，具有與簽名同等的效力，可用以辨識及確認電子文件簽署人的身分，及辨識簽署訊息的完整性。

(7).加密(Encrypt/Encipher)

指利用數學演算法或其他方法，將電子文件以亂碼方式處理，以確保資料傳輸的安全。

(8).解密(decrypt/Decipher)

將經加密後形成人無法辨識其代表意義的訊息，以相關的數學演算法或其他方法將

該訊息還原為人可以辨識其代表意義的訊息。

(9).數位簽章(Digital Signature)

數位簽章為電子簽章的一種，係指採用非對稱型的密碼演算法(Asymmetric Cryptosystem)及雜湊函數(Hash Function)，對一定長度的數位訊息壓縮後再以簽署人的私密金鑰予以加密，其相對應的公開金鑰可以驗證此加密後的數位訊息，形成一可供辨識簽署人身分及電子文件真偽之資料訊息。

(10).私密金鑰(Private Key)

指用以製作及驗證數位簽章具有配對關係之一組數位資料而由簽署人保有者，該數位資料除作為製作數位簽章之用外，尚可用作電子訊息解密之用。

(11).公開金鑰(Public Key)

於非對稱型密碼演算法之數位簽章，指用以製作及驗證數位簽章之一組具有配對關係之數位資料中對外公開者;其可用以執行驗證簽署人簽章過的訊息資料的正確性，於執行訊息隱密性功能時可以將傳遞訊息加密。

(12).<公開金鑰>憑證或電子憑證(<Public Key>Certification or Certificate)

一筆以電腦為媒介基礎由憑證機構簽發之數位式的紀錄，內含申請者的註冊識別名稱、公開金鑰、該公開金鑰的有效期限、憑證機構的註冊識別名稱與簽章，及其他用以識別的相關訊息，用以確認簽署人之身分，並證明其擁有相配對之公開金鑰及私密金鑰。

(13).認證中心/憑證機構 (Certification Authority or Certificates Authority；CA)

指提供數位簽章製作及電子認證服務之機構，亦即係指居於公正客觀地位，查驗憑證申請人身分資料之正確性，及其與待驗證公開金鑰及私密金鑰間之關連性與合法性，並據以簽發公開金鑰憑證之單位。

(14).憑證實務作業基準 (Certification Practice Statement；CPS)

憑證機構向所服務的對象公告其執行憑證簽發、廢止、查詢等管理的作業規範及申請程序，內含憑證運作的公開金鑰架構與安全機制、作業規範與程序、憑證機構軟硬體施行的安全機制、權責的管理及相關的規範。

(15).非對稱型的密碼演算法(亂碼系統)(Asymmetric Cryptosystem)

以電腦為媒介基礎的一種數學演算法，可以產生及使用一組數學運算上相關連的安

全金鑰對。其中私密金鑰用以對訊息作簽章，對應的公開金鑰則用以對簽章後的訊息作驗證；公開金鑰亦可用以對訊息作加密，而對應的私密金鑰則用以對加密後的訊息作解密。

(16).雜湊函數(Hash Function)

一種可以將一長串的位元訊息轉換成固定長度位元訊息的數學演算法。相同的訊息輸入經由壓縮函數運算產生輸出結果必定相同，且決無法由輸出產生的結果推算出輸入的訊息。

(17).自動憑證更新環境(Automated Certificate Management Environment；ACME)

一種通訊協議，用於自動化執行憑證機構(CA)與其用戶端 Web 伺服器之間的憑證相關管理作業(例如憑證申請)，允許用戶以極低的成本自動化部署公鑰基礎設施。該協議主要透過 HTTPS 傳輸格式化之 JSON 訊息，相關標準定義於 RFC 8555 中。

(18).憑證簽名請求(Certificate Signing request；CSR)

一種經過編碼的檔案，讓憑證申請者透過標準化的方式，把公開金鑰、憑證相關資訊(例如網域名稱)傳給憑證機構進行憑證簽發。該檔案可具體證明申請者為私鑰之擁有者。

(19).簽發憑證(電子認證)(Issue a Certificate)

係指認證中心(憑證機構)依憑證實務作業基準，審驗公開金鑰憑證申請人之身分資格、相關文件，並驗證其公開金鑰及私密金鑰之配對關係後，簽發公開金鑰憑證或其他憑證。

(20).公用後綴列表(Public Suffix List；PSL)

由 Mozilla 創建的公共資源，列表位於 https://publicsuffix.org/，該列表由兩部分組成：一部分是由 ICANN 提供的 TLD(Top Level Domain，頂級域名)列表，一部分是由個人或機構提供的 PRIVATE 列表。

(21).Bugzilla

由 Mozilla 維護之瀏覽器問題的追蹤管理網路程式，當 CA 發生重大缺失時，必須回報於此處。位於 https://bugzilla.mozilla.org/home。

(22).安全的多用途 Internet 郵件擴充(Secure Multipurpose Internet Mail Extensions；S/MIME)

是一種 Internet 標準，它在安全方面對 MIME 協定進行了擴充，可以將 MIME 實體(比如數位簽章和加密資訊等)封裝成安全物件，為電子郵件應用增添了訊息真實性、完整性和保密性服務。

附錄二 名詞與簡稱(Acronyms and Abbreviations)

ACME Automated Certificate Management Environment

ANSI American National Standard Institute

CA Certification Authority

CC Common Criteria

CP Certificate Policy

CPS Certification Practice Statement

CRL Certificate Revocation List

CSR Certificate Signing request

DN Distinguished Name

ECC Elliptic Curve Cryptography

FIPS Federal Information Processing Standard

ISO/IEC the International Organization for Standardization, The International Electrotechnical Commission

ITSEC Information Technology Security Evaluation Criteria

OCSP Online Certificates Status Protocol

OID Object Identifier

MRSP Mozilla Root Store Policy

PMA Policy Management Authority

PIN Personal Identification number

PKCS Public Key Cryptography Standard

PKI Public Key Infrastructure

RA Registration Authority

RCA Root Certification Authority

RSA Rivest, Shamir, Adleman (encryption algorithm)

TCSEC Trusted Computer System Evaluation Criteria

URL Universal Resources Location