臺灣網路認證股份有限公司

時戳服務實務作業基準

TWCA Time-stamping Authority

Practice Statement

（第 1.0 版）

生效日期：中華民國 110 年 11 月 8 日

Effective Date：2021/11/8

本作業基準版本變更紀錄：

版 本	生效日期	發 行 者	備 註
V1.0	2021/11/8	TWCA	初版發行

目 錄

1. 簡介

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股份有限公司、財金資訊股份有限公司、臺灣集中保管結算所股份有限公司、網際威信股份有限公司共同集資設立，為一值得信賴的憑證機構。

在現今數位化時代，資料除了使用傳統紙本方式做傳遞或保存，使用數位化的資料不但環保、易保管儲存且傳遞上效率更加，更進一步還可以結合數位簽章機制達到資料的完整性與不可否認性，而為了證明在某個時間點前資料已經存在且被簽署，必須將資料與簽署當下時間做關聯，即使未來簽署憑證過期甚至失效，只要能證明簽署當下的正確性及有效性，則該文件依然具有不可否認性，而這個關聯的時間證據即所謂的時戳（TimeStamp）。

為了證明數位簽章產生的當下簽署者的憑證是有效的，數位簽章必須要被驗證且滿足已下條件：

(1) 首次簽署時戳必須在資料簽署者憑證效期未過期且未被廢止前施用。
(2) 後續簽署時戳必須在前次時戳簽署者憑證效期未過期且未被廢止前施用。

在上述條件下施用時戳才能確保簽署當下簽署者的憑證是有效的。

為了提供一個安全且公正的時戳服務，本公司成立時戳服務機構（Time-stamping authority，TSA），藉此來服務需要時戳證明之應用。本公司之時戳服務機構使用的時戳協定符合 RFC 3161 （Internet X.509 Public Key Infrastructure Time-Stamp Protocol ，簡稱 TSP ），同時本公司也遵照 RFC 3628（Policy Requirements for Time-stamping Authorities ，簡稱 TSAs ）之時戳政策要求，撰寫本時戳服務機構之實務作業基準 （Practice Statement），以下簡稱「本實務作業基準」或「本基準」。

2.總覽

本時戳服務實務作業基準之訂定主要適用於數位簽章之時戳服務，但不限於數位簽章應用，任何需要證明資料在某個時間點存在的應用都可能在本基準適用範圍中。

本實務作業基準主要基於使用公開金鑰密碼學（Public key cryptography）、公開金鑰憑證（Public key certificates）以及可靠的時間源。本基準將使用獨立的章節來確保本公司提供一個可受信任的時戳服務。

本基準將會提到時戳機構所簽發之時戳時間與世界協調時間（UTC）的同步要求，以及時戳單元（TSU）簽署的相關要求。使用時戳的用戶以及信賴者也可以根據本基準清楚的了解本時戳服務機構之實務作業。

本基準之內容及大綱參考 RFC 3628（ Policy Requirements for Time-stamping Authorities ，簡稱 TSAs） 之框架進行撰寫。

3.定義與縮寫

3.1 定義

(1) 信賴者（Relying party）

信賴時戳服務機構且依賴時戳符記進行作業之時戳符記接受方。

(2) 用戶（Subscriber）

需要使用時戳服務機構提供之服務，且已同意相關用戶協議之組織或個人。

(3) 時戳符記（Time-stamp token）

某種資料與時間關聯的物件表示方式，內容包含了某個特定時間點資料已存在之證據。

(4) 時戳服務機構（Time-stamping authority）

簽發時戳符記之機構。

(5) 時戳機構聲明揭露（TSA Disclosure statement）

關於時戳服務機構之政策或實踐的聲明，並揭露給用戶及信賴者。

(6) 時戳機構實務作業基準（TSA practice statement）

時戳服務機構簽發時戳符記所採用的做法聲明。

(7) 時戳系統（TSA system）

由 IT 產品或其他模組組成之系統，為了支持時戳服務。

(8) 時戳政策（time-stamp policy）

針對特定具有共同安全需求的應用或群體，提供一套規則說明時戳符記的適用性。

(9) 時戳單元（Time-stamping unit）

以單元方式管理之軟硬體組合，且在某個時間點具有一把已啟用，用於簽發時戳符記的簽章金鑰。

(10) 世界協調時間（Coordinated Universal Time （UTC） ）

世界協調時間，是最主要的世界時間標準，其以原子時秒長為基礎，在時刻上儘量接近於格林威治標準時間。

3.2 縮寫

(1) TSA Time-stamping Authority

(2) TSU Time-stamping Unit

(3) TST Time-stamp token

(4) UTC Coordinated Universal Time

(5) CA Certification Authority

(6) CC Common Criteria

(7) CP Certificate Policy

(8) CPS Certification Practice Statement

(9) CRL Certificate Revocation List

(10) DN Distinguished Name

(11) FIPS Federal Information Processing Standard

(12) OCSP Online Certificates Status Protocol

(13) OID Object Identifier

(14) PIN Personal Identification Number

(15) PKCS Public Key Cryptography Standards

(16) PKI Public Key Infrastructure

(17) PMA Policy Management Authority

(18) RA Registration Authority

(19) RCA Root Certification Authority

(20) RSA Rivest, Shamir, Adleman （encryption algorithm）

4.一般觀念

4.1 時戳服務

本時戳服務依照需求分類提供以下兩種服務模組：

(1) 時戳生成模組（Time-stamping provision）：本模組負責產生並簽發時戳符記（Time-stamp tokens）。

(2) 時戳管理模組（Time stamping management）：本模組負責監控時戳服務的各項作業以確保該時戳服務是按照 TSA 規範提供服務。本模組同時也負責安裝及卸載時戳生成模組。舉例來說，時戳管理模組必須要確保時戳生成模組所產生之時戳與 UTC 時間同步。

4.2 時戳服務機構

時戳服務機構（Time-stamping authority，TSA） 是指授權簽發時戳符記（Time-stamp tokens）之機構，且受用戶（Subscriber）及信賴者（Relaying parties）所信任。本時戳服務機構有完全的責任針對 4.1 節中所描述的模組提供服務。本時戳服務機構可能包含一個或多個時戳單元（Time-stamping Unit），並且對這些時戳單元負起營運責任，這些時戳單元將代表 TSA 進行時戳之簽署。本時戳服務機構有責任確保簽發之時戳符記具有可識別性。

本時戳服務有可能使用其他組織或單位的系統構建時戳服務的一部分，本時戳服務將具有完全的責任確保這些組織或單位遵守本時戳服務的政策要求。

4.3 用戶

用戶（Subscriber） 可能是個人或是由多人組成的組織。當用戶是組織時，適用於該組

織的義務條款也同樣適用於該組織的用戶。

在任何情況下，如果該組織的用戶沒有正確履行應盡義務，則該組織應承擔責任，同時有責任通知其用戶履行義務。

如果用戶是個人時，當個人用戶未正確履行應盡義務時，則該用戶將自行承擔責任。

4.4 時戳政策與時戳服務機構作業基準

本節說明時戳政策（Time-stamp policy）以及時戳機構實務作業基準（TSA practice statement）。

4.4.1 目的

「時戳政策（Time-stamp policy）」主要規定「要遵守的事項」，而 「時戳機構實務作業基準（TSA practice statement）」主要描述「該如何遵守時戳政策」，例如，如何產生時戳以及如何達到時間的準確性。這兩者之間的關係如同「需求（Requirements）」及「營運（Business）」，而維運單位制訂了如何執行這些政策的程序。

「時戳政策」用以滿足一般對可信任時間戳服務的要求，而「時戳機構實務作業基準」將陳述如何滿足這些要求。

4.4.2 差異程度

「時戳機構實務作業基準」比「時戳政策」更具體。時戳機構實務作業基準主要針對時戳政策中的條款做更詳細的實作描述，並定義了相關的技術以及組織程序來滿足時戳政策的要求。

4.4.2 途徑

「時戳政策」與「時戳機構實務作業基準」是獨立的，本基準將在第 5 章描述「時戳政策」，說明 TSA 應遵守之規則；第 7 章描述「時戳機構實務作業基準」，針對 TSA 組織結構、操作程序、設施以及運行環境作具體聲明，以滿足時戳政策之要求。本基準由時戳服務提供者（臺灣網路認證股份有限公司）所制定之。

5.時戳政策

5.1 總覽

本基準定義了「時戳政策」之規則集合，用於定義時戳符記（Time-stamp token）的適用性，以及一般性安全需求。TWCA 遵循 TSA 簽發時戳的最低要求準則，包含支援公鑰憑證以及時間精度達到 UTC 時間正負 1 秒內。

5.2 識別

TSA 除了要向用戶及信賴者揭露聲明外，同時也需要定義戳政策的識別碼，並指出其一致性。

本時戳政策之物件識別碼（Object Identifier）為「1.3.6.1.4.1.40869.2.1」:

{ISO(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) TWCA(40869) TSA(2) policies(1)}

5.3 用戶群體及適用性

本時戳服務機構所簽發之時戳主要用於電子文件或訊息之簽章時間證明，更進一步提供電子文件的長效期驗證（Long Term Validation，LTV），以證明該文件在某一時點就已存在，即使未來文件簽署憑證狀態已經失效，仍不改變該文件在該時刻其文件簽署憑證有效的事實。

本時戳服務所使用的憑證為 TWCA 所簽發之時戳憑證，任何個人或組織若有「由一個可信任的第三方機構來提供資料在某一特定時間點已存在的證據」之需求，均適用於本時戳服務機構所規範之時戳政策。

5.4 一致性

本時戳服務機構之時戳政策物件識別碼定義於 5.2 節中，與時戳機構所簽發之時戳符記（Time-stamp token）中之物件識別碼 （TSAPolicyId，定義於 RFC 3161） 一致，用來表示與時戳政策之一致性。

6.義務與責任

6.1 時戳服務機構義務

6.1.1 一般條款

本時戳服務機構確保依照實務作業基準（如第 7 章所述）之要求提供服務。本時戳服務機構遵守時戳服務所參考之相關政策所定義的義務，確保本時戳服務與時戳實務作業基準一致。本基準為本時戳服務機構、用戶、信賴者之間合約不可或缺的一部分。

6.1.2 時戳服務機構對用戶之義務

以下為本時戳服務機構之義務：

(1) 本時戳服務機構應遵守本時戳服務實務作業基準。

(2) 本時戳服務機構遵守相關法律及法規。

(3) 本時戳服務機構應盡到相關合約及作業規範告知之義務。

(4) 本時戳服務機構應盡到妥善保管簽署時戳私鑰之義務。當私鑰有洩漏之疑慮時，應盡到告知用戶之義務。

(5) 本時戳服務機構所使用簽署時戳之私鑰僅限於簽署時戳之用途。

(6) 本時戳服務機構致力於提供時間精準度保持與 UTC 時間落差正負 1 秒內。

(7) 本時戳服務機構定期執行稽核，確保其遵守相關法規、內部政策及程序。

6.2 用戶的義務

以下為使用時戳服務之用戶的義務：

(1) 使用本時戳服務機構之用戶應了解並同意本時戳服務作業基準，合法且正確的使用

時戳符記（Time-stamp token）於相關的業務系統，且無任何違反相關法律的規定與侵害第三者的權利。

(2) 使用本時戳服務機構之用戶應審視 TWCA 提供之相關合約及作業規範要求，並於接受合約及作業規範要求為前題下，方可使用本時戳服務機構所提供之服務。

(3) 使用本時戳服務機構之用戶應遵循 RFC 3161 之要求，針對時戳單元（Time-stamping Unit）所簽發之時戳符記進行檢查，包含時戳符記的正確性和有效性、時戳憑證的正確性和有效性以及其他相關檢核要求。

6.3 信賴者的義務

以下為使用時戳服務之信賴者的義務：

(1) 使用本時戳服務機構之信賴者應了解並同意本時戳服務作業基準，合法且正確的使用時戳符記（Time-stamp token）於相關的業務系統，且無任何違反相關法律的規定與侵害第三者的權利。

(2) 使用本時戳服務機構之信賴者應遵循 RFC 3161 之要求，針對時戳單元（Time-stamping Unit）所簽發之時戳符記進行檢查，包含時戳符記的正確性和有效性、時戳憑證的正確性和有效性、簽署內容的完整性，以及其他相關檢核要求。

(3) 使用本時戳服務機構之信賴者應透過憑證廢止清冊（Certification Revocation List，CRL）或是線上憑證狀態協定（Online Certificate Status Protocol，OCSP），確保簽署時戳之時戳憑證於驗證當下有效且尚未被廢止。

(4) 使用本時戳服務機構之信賴者應根據本基準考量時戳符記使用上的任何限制。

(5) 使用本時戳服務機構之信賴者應考量本時戳服務機構公告之相關注意事項。

6.4 責任

以下為本時戳服務機構之責任：

(1) 本時戳服務機構致力於提供高可用性之時戳服務。

(2) 本時戳服務機構若因為違反政府法律或作業人員故意或過失，導致用戶及信賴者的損失，本時戳服務機構將依照與用戶合約及相關適用法律規章執行損害賠償責任。

(3) 本時戳服務機構對於用戶或信賴者不當使用本基準所引發之一切結果，不負任何法律責任。

(4) 本時戳服務機構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時戳服務機構之事由（例如戰爭等），本時戳服務機構不負損害賠償責任。

7.時戳服務機構之實務要求

7.1 實務作業基準與聲明揭露

7.1.1 時戳服務機構實務作業聲明

(1) 本時戳服務機構每年會進行風險評估，藉由評估結果識別相關資訊資產之威脅，並確保必要的安全控制及作業程序正確執行。

(2) 本時戳服務實務作業基準（以下簡稱本基準）訂定之各項程序滿足時戳政策之要求。

(3) 本基準針對參與角色描述其義務與責任（請參閱第 6 章）。

(4) 本時戳服務機構（以下簡稱本機構）確保所有參與者可取得本基準及相關文件。

(5) 本機構針對所有聲明做揭露（請參閱 7.1.2 節）。

(6) 本機構之管理機構為「臺灣網路認證股份有限公司」政策管理中心（Policy Management Authority，PMA），具有本基準的最終決定權。

(7) 本機構確保整體服務及營運依照本基準內容施行。

(8) 本基準由 PMA 負責管理及維護。

(9) 當本機構欲變更本基準之內容，必須由 PMA 進行審核後發佈及公告。

7.1.2 時戳服務機構揭露事項

本機構揭露事項如下：

(1) 本基準的制定、修訂、發布等事宜，其權責單位為「臺灣網路認證股份有限公司」政策管理中心（Policy Management Authority，PMA）。

(2) 本機構之時戳政策物件識別碼定義於 5.2 節中，任何由本機構所簽發之時戳符記均須包含此物件識別碼。

(3) 本機構使用之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)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)11}
簽章	ECDSAWithSHA256	{iso(1)member-body(2)us(840)ansi-X9-62(10045)signatures(4)ecdsa-with-SHA2(3)2}
簽章	ECDSAWithSHA384	{iso(1)member-body(2)us(840)ansi-X9-62(10045)signatures(4)ecdsa-with-SHA2(3)3}
雜湊	SHA256	{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithms(4) hashalgs(2) sha256(1)}
雜湊	SHA384	{joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) hashAlgs(2) sha384(2)}

(4) 本機構簽發之時戳符記，其簽章效期最長為 135 個月。

(5) 本機構使用之時間精準度與 UTC 時間落差正負 1 秒內。

(6) 用戶應盡的義務（請參閱 6.2 節）。

(7) 信賴者應盡的義務（請參閱 6.3 節）。

(8) 本機構保留系統運作之相關事件紀錄（請參閱 7.4.11 節）。

(9) 本機構適用之法律責任（請參閱 6.4 節）。

(10) 本機構可要求用戶遵守法律、時戳服務政策、時戳服務實務作業基準、以及合約之規範。

(11) 本機構使用之時戳憑證由 TWCA 時戳憑證機構所簽發。

(12) 本機構使用之時戳憑證，其私密金鑰效期小於 15 個月，其憑證效期小於 135 個月。

(13) 本機構使用之時戳協定遵循 RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol （TSP）。

(14) 本機構視業務類型收取相關之服務費用。

(15) 對於本基準有任何修改建議或有任何意外事件發生時，請將詳細的建議、說明文件與聯絡資訊，電話、E-mail 或郵寄至下述的聯絡窗口：

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

(16) 本基準公布於官網（www.twca.com.tw）儲存庫供下載。

7.2 金鑰管理生命週期

7.2.1 時戳單元金鑰產製

本機構之金鑰對由二位以上金鑰管理人員，同時登入 （Log-in） 至硬體密碼模組（HSM），由硬體密碼模組 （HSM） 直接產生，任何人絕無法單獨一人執行金鑰對的產生作業，且私密金鑰於硬體密碼模組 （HSM） 內產生後，直接經亂碼保護後儲存在設備內。

7.2.2 時戳單元私鑰保護

本機構使用滿足 CNS 15135、ISO 19790 或 FIPS 140-2 等級 3 硬體密碼模組（HSM）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。

7.2.2.1 密碼模組標準

本時戳服務機構使用 CNS 15135、ISO 19790 或 FIPS 140-2 等級 3 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。

7.2.2.2 私密金鑰分持控管

本機構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，分別由不同管理人員管控，並儲存於具安全管控措施之環境。

7.2.2.3 私密金鑰託管

本時戳服務機構之私密金鑰不允許託管。

7.2.2.4 私密金鑰的備份

(1) 本機構之私密金鑰儲存於硬體密碼模組內，且依照 7.2.2.2 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 份存放於本機構內之安全地點，另一份存放於具安全管控之異地備援地點。

7.2.2.5 私密金鑰歸檔

本機構之私密金鑰不進行歸檔。

7.2.2.6 私密金鑰自密碼模組輸入或輸出

本機構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 7.2.2.4 節規定辦理。

7.2.2.7 私密金鑰儲存於密碼模組

本機構之私密金鑰係以加密型態儲存於密碼模組。

7.2.2.8 私密金鑰啟動方式

儲存於密碼模組內的私密金鑰必須經管理人員使用晶片卡登入管理網站後，手動開啟成為啟用狀態，金鑰方可啟動。

7.2.2.9 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管理人員使用晶片卡登入管理系統後手動關閉成為停用狀態，以避免私密金鑰遭非法使用。

7.2.2.10 私密金鑰銷毀

本時戳服務機構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進行刪除，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。

7.2.2.11 密碼模組等級

本機構使用之硬體密碼模組等級，必須為 CNS 15135、ISO 19790 或 FIPS 140-2 等級

3。

7.2.3 時戳單元公鑰散布

本機構提供用戶或信賴者下載時戳憑證及其完整憑證鏈、憑證廢止清冊等相關資訊。

7.2.4 時戳金鑰更新

本機構之時戳金鑰定期做更換,時戳金鑰對應之時戳憑證透過 TWCA 時戳憑證機構(TSA Certificate Authority）所簽發，相關的憑證更新程序由 TWCA 時戳憑證機構規範。

7.2.5 時戳單元金鑰生命週期結束

本機構之時戳金鑰生命週期結束時，依照 7.2.2.9 節之停用方式進行停用，當金鑰必須執行銷毀時，依照 7.2.2.10 節之規範進行。

7.2.6 簽署時戳密碼模組之生命週期管理

本機構使用之硬體密碼模組（HSM）由協力廠商提供及維護，相關作業流程及生命週期管理不在本基準中描述。

7.3 時戳

7.3.1 時戳符記

本機構確保所簽發之時戳符記是安全的，且包含正確的時間：

(1) 時戳符記內包含時戳政策識別碼（請參閱 5.2 節）。

(2) 每一個時戳符記具有唯一識別性（RFC 3161 2.4.2 Response Format 章節所定義之 serialNumber 資訊）。

(3) 時戳符記所使用的時間為 UTC 時間，該時間值取自於我國「國家時間與頻率標準實驗室」、其他世界標準時間實驗室，或其他時間源設備。

(4) 時戳符記中記載之時間與 UTC 時間同步，且其時間精準度定義於時戳政策中或是定義於該時戳符記中（RFC 3161 2.4.2 Response Format 章節所定義之 Accuracy 資訊）。

(5) 若本時戳服務機構使用之時間源，其時間精準度不符 7.1.2 節（5）中所聲明之時間精準度，則將不允許簽發時戳符記。

(6) 時戳符記中將包含由時戳需求者提供之關聯資料雜湊值（其相關內容定義於 RFC 3161 2.4.1 Request Format 章節中）。

(7) 本機構用於簽發時戳符記之私鑰，其金鑰用途僅限於簽發時戳符記。

(8) 時戳符記內容包含 TSU 之識別碼，同（1）。

7.3.2 與世界標準時間同步

本機構確保其所使用之時間源與 UTC 時間同步：

(1) 本機構從時間源取得之時間將會進行正確性檢核，避免時間源發生非預期之錯誤，使其時間精準度超過所允許範圍。

(2) 本時戳服務之各項軟硬體設施均受到高安全強度之保護，避免時間資訊遭到竄改。

(3) 同（1），當時戳單元從時間源取得之時間資訊其時間落差遠超過本時戳政策之容忍值，時戳單元將告警並立即停止服務。

(4) 本機構確保當潤秒產生時，依然可以與 UTC 時間同步，所有索取時間源之相關紀錄均會記載於資料庫中。

7.4 時戳服務機構的管理與維運

7.4.1 安全控管

本機構之營運機房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機構之相關設備。其他人員控管及實體環境安全部分，分別描述於 7.4.3 節以及 7.4.4 節。

7.4.2 資產分類與管理

為保護本公司各類資訊資產，以防止因人為疏失、蓄意或自然災害等風險所造成之傷害。

(1) 為使組織內資產得到應有的保護及維護，本公司將組織內重要資產造冊列帳，明定權責單位（Owner）/保管單位的權利義務；並指定權責單位（Owner）/保管單位，負責資訊資產之維護。

(2) 為使組織內資訊資產受到應有程度的保護。資訊的敏感程度和關鍵程度各不相同，本公司對資訊分類，指明其需要、優先順序和保護級別。使用資訊分類系統定義合適的保護級別，並解釋對特別處理手段的需要。

(3) 其他相關內容參考本公司「ISMS-02-002 資訊資產分類與分級控管程序書」。

7.4.3 人員控管

7.4.3.1 背景、適任條件與經歷

本公司執行各種業務的作業人員，必須具備忠實、可信賴及工作的熱誠度，無影響本公司作業的其他兼職工作，無本公司作業上因工作的疏失、不盡責的缺失紀錄，無違法犯紀的不良紀錄。

(1) 作業人員：

具備時戳服務機構作業的實務經驗，或經過時戳服務機構相關作業訓練者。此職務本公司因人力資源不足時，可以委由外包人員擔任。

(2) 管理人員與監督人員：

具備時戳服務機構作業的實務經驗，或具有電腦系統規劃、開發、營運管理經驗者。此職務必須由公司選派適當人員擔任，不可以委由外包人員擔任。

7.4.3.2 背景審核程序

時戳服務系統運作的人員，由人事管理相關部門依監督人員、管理人員、作業人員所訂定的審核規範，執行身分背景安全的審查，以及本公司部門相關作業的實務與經歷的審查通過後，始可任職，且每年必須依各種作業人員的職務特性，執行安全、實務與經歷的審查，該員是否適任相關的工作以做為執行工作調整或調派的依據。

7.4.3.3 教育訓練

時戳服務系統運作的人員，皆依照其職務，施予時戳服務系統運作所應具備的軟硬體功能、作業程序、安控程序、災變備援作業規範、PKI 公開金鑰作業及時戳服務政策與時戳服務機構實務作業基準與其他資訊安全相關作業規範的訓練，時戳服務系統有異動或有新系統的加入時，亦需給予適當的教育訓練。

本公司需訂定一套時戳服務系統有關硬軟體、應用系統與安全管理系統之完整的教育訓練規範，於新進人員及時戳服務系統或有異動時，施行相關技能的教育訓練。教育訓練完成後有詳實的成果紀錄，做為相關作業人員工作委任的參考。

7.4.3.4 教育訓練的頻率與需求

時戳服務系統運作的相關人員，其執行時戳服務系統運作的相關知識與技能，每年至

少檢討一次，並給予適當的再教育的訓練。

時戳服務系統功能的更新、新系統的加入，或相關知識與技術的進步與更新，皆需對系統運作的相關人員執行教育訓練。

7.4.3.5 職務的輪調

配合系統運作的需求與相關作業人員工作的適任性，本公司會選派適任的人選輪調至適合的工作歷練，但調派前必須施以適當知識與技能的教育訓練。

7.4.3.6 非授權作業的處罰

時戳服務系統運作的相關作業人員，因故意或疏失而執行非自己職務上的作業時，無論造成或未造成時戳服務系統安全的問題，皆應即刻呈報監督管理者，依照相關作業之規範處理。

7.4.3.7 委外人員需求

因人力資源不足而委由外包人員擔任操作人員時，除必須依照業務的工作內容簽訂相關的保密合約外，該委外人員的權利與義務與本公司之內部操作人員相同，必須施以職務上知識與技能的教育訓練，且遵守相關作業規範與法律規範。

7.4.3.8 作業文件需求

為使時戳服務系統的運作正常及順暢，必須提供相關作業人員執行系統運轉的作業文件，至少包含如下：

(1) 硬體、軟體作業平台的操作文件、網路系統與網站相關的操作文件、硬體密碼模組（HSM） 的操作文件。
(2) 時戳服務系統的相關操作文件。

(3) 時戳服務機構實務作業基準、時戳服務政策及相關作業規範文件。

(4) 時戳服務系統內部作業文件，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。

7.4.4 實體與環境安全

7.4.4.1 建築物與位置

本時戳服務機構所在機房，具備防震、防水、防火、門禁保全系統、防入侵門禁監視與防破壞警報系統，符合儲存高重要性及敏感性資訊的機房設施水準，以防止未經授權者存取本時戳服務機構之相關設備。

7.4.4.2 實體進出管制

作業人員欲進入時戳服務機構機房必須通過三道 IC 卡門禁管制，其中至少一道門禁具備生物特徵鑑別裝置（包含但不限於指紋、臉部或掌形）；時戳服務機構電腦主機所在位置至少具備須兩人以上經身分驗證之實體控管措施；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。

本時戳服務機構運作的相關私密金鑰與備份資料皆妥善、安全的存放於本中心設有監控錄影系統保護的保險櫃內，時戳服務系統運作的相關作業人員，執行時戳服務管理作業時，皆有監控錄影設備的監測。

本時戳服務機構運作的硬軟體及硬體密碼模組 （HSM） 皆置於有監控錄影系統保護的環境下，時戳服務系統安全控管人員，執行金鑰管理相關作業時，皆有監控錄影設備的監測。

7.4.4.3 電力與空調

本機構機房設有發電機及不斷電系統 （Uninterruptible Power Supply; UPS），當一般供電系統異常時，會自動切換至發電機供電，切換過程由 UPS 提供穩定之電力。

本機構機房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。

7.4.4.4 防水處理

本機構機房的房屋為密閉式建築物，除內部可進出的出入門外，外部皆為混凝土建築物，雨水無法進入，且樓層地板裝置高架地板無進水之顧慮。

7.4.4.5 防火處理

本機構之機房建築物的材質為防火材質並配置具有中央監控系統的滅火設備，於偵測到發生火災時，能自動啟動滅火功能，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。

7.4.4.6 媒體儲存

媒體儲存環境，具有對磁性媒體防磁、防靜電干擾的設備與環境，重要資料媒體則儲存具高度防火功能的保險櫃，其中一份備份資訊的媒體儲存於具有安控措施的異地處所，備份及保存資訊的儲存媒體，定期執行測試與驗證資訊的有效性與可使用性。

7.4.4.7 廢棄處理

本機構於時戳服務系統所使用的硬體設備、磁碟機與硬體密碼模組 （HSM） 等，於廢棄不使用時，商業敏感性及機密性資訊必須經過安全的清除與銷毀，且經由稽核單位的驗證，並留存查核文件。

文件與媒體資訊儲存有商業敏感性及機密性資訊時，於廢棄處理時必須經安全的銷毀，該資訊皆無法回復與存取使用，且經由稽核單位的驗證，並留存查核文件。

7.4.4.8 異地備援

時戳服務系統運作所須的相關媒體資訊、文件規範，備份後儲存於具備中央恆溫、恆濕空調系統、防磁、防靜電干擾，且具有中央監控攝影機監控錄影，與人員進出存取需經過合法授權之高度安全控管的異地備援環境。

時戳服務系統每日的交易備份紀錄檔，每週完整的系統備份紀錄檔，皆備份後儲存於高度安全控管的異地。備份及保存資訊的儲存媒體與文件，定期執行測試與驗證資訊的有效性與可使用性。

7.4.5 操作管理

本機構之維運或管理人員依照本基準及相關作業規範文件進行操作。

7.4.6 系統存取管理

本機構具有獨立的作業管理系統，且需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。

時戳服務系統需經授權後由業務相關之作業人員才可以執行管理作業。為防範網路入侵與破壞，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。

時戳服務系統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驗證，確認係經授權之人員或系統方可存取。

時戳服務系統的儲存庫透過系統修補程式的更新、系統弱點掃描、入侵防禦系統、防火牆系統等加以保護，以防範阻絕服務及入侵等攻擊。

7.4.7 信賴系統的部署與維運

時戳服務系統所使用自行開發之軟體於上線佈署前均需通過弱點掃描檢測，系統進行各項作業變更時，均依照變更作業程序進行。時戳服務系統主機會定期進行主機弱點修補，以確保維運環境的安全。

7.4.8 時戳服務對策

7.4.8.1 金鑰遭破解及緊急應變處理程序

若時戳服務機構金鑰疑遭破解或遺失(雖尚未確定是否遭破解)，則須進行下列程序：

(1) 時戳服務機構中斷服務，停止時戳符記之簽發。

(2) 向簽發時戳憑證之 CA 提出憑證廢止請求。

(3) 儘快以電子郵件、書面或其他方式，通知所有用戶。

(4) 重新產製金鑰並向 CA 申請新的時戳憑證。

(5) 確保所有復原作業流程均完成後，重新啟動時戳服務。

(6) 針對已簽發之時戳符記進行重新簽署時戳之動作。

時戳服務機構必須調查，並向政策管理中心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。

7.4.8.2 電腦資源、軟體及資料損毀之處理程序

時戳服務系統使用的電腦軟體資源、或時戳服務系統運作相關的資料有異常毀損時，依照系統備份與回復作業手冊，可以由內部備份媒體資料、或移送異地的備份媒體資料執行時戳服務系統的復原作業，使系統能繼續且正常營運。

7.4.8.3 災變後之營運持續能力

時戳服務系統運作所使用的相關安全設施，於天災與地變時毀損時：

(1) 如果在回復使用的相關安全設施至正常運轉之前，不會影響時戳服務系統的運作，則儘速修護或更新至正常運轉狀態，不至於影響時戳服務系統的正常運作。
(2) 當足以造成時戳服務系統運作的危害時，必須立刻緊急關閉時戳服務系統的運作，且儘速修護或更新相關安全設施至正常運轉狀態後，才開啟時戳服務系統的運作。如果於作業規範的時間內無法修護或更新相關的安全設施時，則必須執行異地災變復原計劃，於異地正式開啟時戳服務系統的營運作業。
(3) 如發生的災變已嚴重損害時戳服務系統運作使用的相關安全設施時，則必須立即執行異地災變復原計劃，回復時戳服務系統的運作功能。

為避免因天災與地變而造成時戳服務系統運作的停頓，本公司建置一套於異地的業務回復作業計劃，及異地災變備援的復原系統，將時戳服務系統運作所需要硬軟體系統與設施、時戳訊相關的媒體與文件、及作業規範與業務系統回復文件，於離開本公司營運系統適當距離處的異地備援中心，建置系統與儲存媒體與文件。

異地災變備援的業務復原系統，依業務需求每年至少執行一次災變復原計劃的人員訓練與測試演練，並配合實際作業環境隨時更新作業規範與業務系統回復文件，與留存測試紀錄文件以備稽核作業的查核。在發生自然災害或其他災變，以致於無法在 24 小時內恢復時戳服務時，將啟用異地備援機房之設施，並於啟用後 24 小時內恢復提供時戳服務。

7.4.9 時戳服務終止

本公司因故結束任一系統營運時，需對業務系統運作的影響減少至最低程度，而將相關業務穩定的轉移至安全且公正客觀的其他時戳服務機構繼續運作。

於業務正常結束、或合約終止、或公司重整而無安全的考量因素時：

(1) 終止服務日之三十日前，將終止服務或由其他時戳服務機構承接相關業務之事實通知用戶。

(2) 於高度安全且無安全顧慮的作業環境下，將結束系統營運之時戳服務機構全部的憑證進行廢止。

(3) 若有承接的時戳服務機構時，將時戳服務機構政策、本作業基準、本公司相關作業手冊文件、用戶合約與註冊資料、稽核紀錄、歸檔資料及其他業務承接所必須的相關文件，移轉至承接的時戳服務機構，至少妥善安全的保存，保留期限須滿足 7.4.11 所定義之期限。

(4) 將結束系統營運時戳服務機構之相關私密金鑰完全清除乾淨，並向用戶正式宣告。若時戳業務已移轉至承接的時戳服務機構繼續營運，且儘可能的協助接任者執行時戳業務的進行。

(5) 於業務異常結束（法院宣告破產、或不合法）時，本公司必須儘早向用戶公告事實，且必須執行如業務正常結束時的作業程序，將對用戶業務系統運作的影響減少至最低程度。

7.4.10 遵守法律要求

本作業基準依據政府相關法律的規範而訂定，受中華民國相關法律規範的管轄與督導，接受主管機關相關法律規範，例如電子簽章法與相關施行細則，如有跨國或跨區域的業務整合需求時，除配合業務整合規範所需之外，仍以中華民國相關法律規範為管轄依據。

7.4.11 時戳服務操作記錄

除配合主管機關訂定的資訊保存期限規範，本公司訂定時戳服務系統運作有關資訊的保存期限如下：

(1) 時戳服務實務作業基準、相關作業手冊、及用戶的申請表單相關合約條款、證明文件等資料，保留期限為十年。

(2) 時戳請求交易訊息紀錄，保留期限為十年。

(3) 時戳管理相關作業紀錄，保留期限為十年。

7.5 組織

本時戳服務機構為確保其組織的可靠，時戳服務機構的運作依據相關政策、程序及作業基準，內部程序文件只能在嚴格控管的條件下提供。

8. 安全考量

當驗證者執行時戳符記驗證時，必須確保時戳憑證是由 TWCA 之時戳憑證機構（TSA Certificate Authority）所簽發，且憑證尚未被廢止。這意味著時戳的安全性取決於 TWCA 時戳憑證機構的安全性，包含時戳憑證的簽發，以及提供準確的憑證廢止狀態資訊。

當驗證者在時戳憑證效期區間內驗證時戳符記時，還需要檢查時戳憑證的廢止狀態，一旦時戳憑證之私鑰被破解（時戳憑證被廢止），則所有由此私鑰所簽發之時戳符記也都將失效。

當應用程式在使用時戳符記時，還需要考慮其它的安全性，尤其是當需要確保文件的完整性時，驗證者應該要檢查文件之雜湊值與時戳符記中之雜湊值的一致性。

9. 參考

(1) [RFC 3161] Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)

(2) [RFC 3628] Policy Requirements for Time-Stamping Authorities (TSAs)

(3) 臺灣網路認證股份有限公司公開金鑰基礎建設憑證政策 V2.3

(4) 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 V1.6