中華電信公開金鑰基礎建設

時戳實務作業基準

第 1.1 版

中華電信股份有限公司

中華民國 108 年 10 月 9 日

目　錄

文件修訂履歷表

版次	發行日期	修訂內容摘要
1.0	106/4/12	首次發行。
1.1	108/10/9	(1) 修訂參考資料。 (2) 「中華電信公開金鑰基礎建設憑證政策管理委員會」改為「中華電信憑證政策管理委員會」。 (3) 修訂時戳政策物件識別碼。 (4) 依照現況微調第七章時戳服務機構之時戳實務要求。

1.簡介

1.1. 總覽

中華電信公開金鑰基礎建設(Chunghwa Telecom ecommerce Public Key Infrastructure，ePKI)是為了健全電子商務基礎建設環境，以提供完善的電子認證服務而設立。中華電信公開金鑰基礎建設依照ITU-T X.509標準建置一個階層式(Hierarchy)的公開金鑰基礎建設，提供更便捷安全可信賴的網路服務。

中華電信公開金鑰基礎建設時戳實務作業基準（以下簡稱本時戳實務作業基準）描述於中華電信公開金鑰基礎建設內設置中華電信ePKI 時戳服務機構（以下簡稱本時戳服務機構）所提供時戳服務作業的實務，本時戳實務作業基準基於中華電信公開金鑰基礎時戳服務政策、公開金鑰加密演算法、公開金鑰憑證以及可信賴的時間源而組成，並可做為各個獨立的應用機構在評估採用中華電信時戳服務之確認依據。

本時戳實務作業基準主要依據時戳服務需求、中華電信公開金鑰基礎建設時戳政策及相關國際標準（如IETF的RFC 3628、RFC 3161及RFC 5816、ETSI TS 102 023 v1.2.1、ETSI EN 319 421 V1.1.1 (2016-03) 及ETSI EN 319 422 V1.1.1 (2016-03)等）所訂定之政策技術

文件，並經中華電信憑證政策管理委員會審核通過。

本時戳實務作業基準描述本時戳服務機構所發行的時戳符記(Time-Stamp Token, TST)和世界標準時間(Co-ordinated Universal Time, UTC)同步作業之實務，如何符合時戳政策的需求以及經由時戳單元(Time-Stamping Unit, TSU)簽署數位簽章的需求與執行細節。

為使電子交易產生可信賴與可管理的數位證據，因此必須由交易雙方同意之方式針對交易連結時間之資料，之後交易雙方可以互相比對。此證據的品質植基於產生與管理描述此事件和參數資料點連結到真實世界的資料結構。典型之交易為數位簽章之文件，必須證明此數位簽章來自簽署者且其憑證有效。對於數位簽章所實施的時戳證明數位簽章在資料包含時戳前產生。

為了證明數位簽章是在簽署者的憑證有效時產生，數位簽章必須被驗證且以下狀況必須滿足：

1.時戳在簽署者憑證之效期結束前實施。

2.時戳在當簽署者憑證未被廢止或在憑證被廢止前實施。

因此時戳以這種方式證明數位簽章是在簽署者之憑證有效時建立，並證明數位簽章在整個憑證串鏈的有效。涵蓋本節所述之需求是本時戳實務作業基準撰寫的主要理由之一。

1.2. 時戳實務作業基準及時戳政策之關係

本時戳服務機構為達成中華電信公開金鑰基礎建設時戳政策之需求,並支援合格電子簽章使用時戳服務(也就是和 REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC 對齊)，並可能用於需要證明某資料在某一個特定時間之前就已經存在的任何應用而建置與提供服務。有關時戳政策與時戳實務作業基準的定義及其進一步的相互關係,詳述於本時戳實務作業基準之第 4.4 節。

2.參考資料

[1] RFC 3628：”Policy Requirements for Time-Stamping Authorities(TSAs)”

[2] ETSI TS 102 023 v1.2.1：”(ESI) Policy requirements for time-stamping authorities(TSAs)”

[3] FIPS PUB 140-1(1994)：”Security Requirements for Cryptographic Modules”

[4] FIPS PUB 140-2(2001)：”Security Requirements for Cryptographic Modules”

[5] ITU-R Recommendation TF.460-5(1997)：”Standard-frequency and time-signal emissions”

[6] 政府憑證總管理中心憑證實務作業基準第1.5版

[7] 政府機關公開金鑰基礎建設技術規範第1.2版

[8] 政府機關公開金鑰基礎建設憑證政策第2.0版

[9] 中華電信公開金鑰基礎建設憑證政策第1.7版

[10]中華電信通用憑證管理中心憑證實務作業基準第1.95版

[11]中華電信公開金鑰基礎建設時戳政策第1.1版

[12] ETSI EN 319 421 V1.1.1 (2016-03) ：” Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.”

[13] IETF RFC 3161 (2001): "Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP)".

[14]IETF RFC 5816: "ESSCertIDV2 update to RFC 3161".

[15] REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

[16]中華電信時戳憑證管理中心憑證實務作業基準第1.0版

[17] ETSI EN 319 422 V1.1.1 (2016-03) Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles

3.定義與縮寫

3.1. 定義

1. 憑證政策(Certificate Policy, CP)：(1)某一憑證所適用之對象或情況所列舉之一套規則，該對象或情況可為特定之社群或具共同安全需求之應用。(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。
2. 憑證實務作業基準(Certificate 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。(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。
3. 時戳服務機構(Time-Stamping Authority, Time Stamp Authority, TSA)：值得信賴並負責簽發時戳符記的機構
4. 時戳服務政策/實務作業基準(TSP/PS)：明示時戳符記適用性的一

套規則，針對特定具有共同安全需求的應用團體或類別。

5. 時戳符記(time-stamp token, TST)：資料物件聯結了數位簽章之特殊時間基準的一種表示法，從而建立數位證據。
6. 時戳單元(time-stamping unit, TSU):以單元方式管理的硬體和軟體之組合，並有單一之時戳符記簽章金鑰在某個時間啟動。
7. 時戳服務機構揭露文件(Disclosure Statement)：時戳服務機構(TSA)需要對用戶及信賴方強調的政策和實務概述。
8. 信賴方(Relying party)：一個由TSA提供信賴時戳符記的實體(個人或組織)。
9. 用戶(Subscriber)：需要由時戳服務機構提供服務，且已同意TSA用戶協議的實體(個人或組織)。
10. 世界標準時間(UTC)：基於秒的時間尺度，由國際電信廣播委員會(ITU-R)之TF.460-5所定義，及大略對應格林威治標準時間(GMT)。

3.2. 縮寫

1. BIPM：國際度量衡局，法文：Bureau international des poids et mesures
2. CP/CPS：憑證政策/憑證實務作業基準，Certificate Policy / Certification Practice Statement

3. CRL：憑證廢止清冊，Certificate Revocation List
4. ePKI：中華電信公開金鑰基礎建設，Chunghwa Telecom ecommerce Public Key Infrastructure
5. ETSI：歐洲電信標準協會，European Telecommunications Standards Institute
6. GMT：格林威治標準時間，Greenwich Mean Time
7. GPKI：政府機關公開金鑰基礎建設，Government Public Key Infrastructure
8. HSM：硬體密碼模組，Hardware Security Modules
9. OID：物件識別碼，object-identifier
10. PKI：公開金鑰基礎建設，Public Key Infrastructure
11. TSA：時戳服務機構，Time-Stamping Authority
12. TSP/PS：時戳服務政策/實務作業基準，Time-stamp Policy / Practice Statement
13. TST：時戳符記，Time-Stamp Token
14. TSU：時戳單元，Time-Stamping Unit
15. UTC：世界標準時間，Coordinated Universal Time

4.一般觀念

4.1. 時戳服務

時戳服務(Time-stamping services)依需求導向之觀點可分為兩種主要的服務元件：

1. 時戳供應元件(Time-stamping provision)：本服務元件負責產生並簽發時戳符記。
2. 時戳管理元件(Time-stamping management)：本服務元件負責監控和管理時戳服務的運作以確保這些服務正是由時戳服務機構所提供的。此服務元件的工作包含監控時戳供應元件的安裝與解安裝以確保其正確性及安全等級。例如，時戳管理元件必須確保時戳服務所提供的時間是經過世界標準時間所正確同步過後的時間值。

4.2. 時戳服務機構

提供時戳符記並被時戳服務使用者(用戶及信賴方)所信任且簽發安全的時戳符記之組織稱為時戳服務機構。本時戳服務機構做為時戳服務機構負責提供第 4.1 節所述的兩種時戳服務元件。本時戳服務機構也必須對那些由一或多個時戳單元(time-stamping unit, TSU)所產生

及簽章的作業負責任，每個時戳單元有不一樣的金鑰對。本時戳服務機構在產生一個時戳符記時也必須同時給予一個識別碼。本時戳服務機構有可能讓某些其他團體提供部分的時戳服務，本時戳服務機構將確保這些團體所提供的服務都能夠根據中華電信公開金鑰基礎建設時戳服務政策之系統技術規範來執行。

4.3. 用戶

用戶(Subscriber)為使用時戳服務並接受時戳服務機構之用戶協議的個體，用戶可能是多個人或一個人所組成的團體，當用戶是一個組織的時候，某些組織的義務必須落實到各個成員身上。無論如何，一個組織當其成員有未盡的義務時，該組織有告知與糾正的責任。當用戶是單一的個人時，如果他有未盡義務的情形，則他必須對自己應盡的義務負責。除非 ePKI 有另外書面特別授權，否則用戶必須使用被認可的方法或軟體工具去產生時戳。

4.4.時戳政策與時戳服務機構實務作業基準

4.4.1. 目的

本時戳實務作業基準著重於如何實作中華電信公開金鑰基礎時戳服務政策所制訂事項。

4.4.2. 差異程度

一份時戳實務作業基準必須和時戳服務機構的組織架構、作業流程、設備和計算環境息息相關，而時戳政策則可與特定的時戳服務機構之作業環境互為獨立。

4.4.3. 途徑

本文件主要是在描述詳細的時戳實務作業，本時戳服務機構所定義的時戳實務作業基準描述要如何符合中華電信公開金鑰基礎時戳服務政策需求的方法。本文件由時戳服務提供者(中華電信)所訂定。

5.所遵循之時戳政策

5.1. 概要

時戳政策為對於某些團體或應用類型所使用的時戳符記，在應用時需要有的一般安全要求的規則。中華電信公開金鑰基礎建設時戳服務政策定義時戳服務機構於發行時戳符記時所需遵守的基本政策，也就是每個時戳符記要包含一個適用政策的識別碼，且請求服務者必須持有中華電信公開金鑰基礎建設所簽發的憑證或本公司所認可之憑證機構所簽發的憑證，產生時戳符記時間的精準度必須在 UTC 的正負 1 秒以內。中華電信 ePKI 時戳服務機構使用專門保留的私鑰對時戳簽章。請求時戳可以透過傳輸控制協定(TCP)或超文本傳輸協定(HTTP)。

5.2. 識別碼

在本時戳服務機構給用戶以及信賴方的揭露文件（Disclosure Statement）中，須表示此識別碼，而一個時戳服務機構也應該要使用時戳政策的識別碼以指出它的一致性。本時戳服務機構目前使用的時戳政策物件識別碼(Object Identifier)為：

id-cht-ePKI-tsapolicy-SHA256withRSA2048::=1.3.6.1.4.1.23459.100.5.1

。

5.3. 用戶群體及適用性

因中華電信公開金鑰基礎建設時戳政策主要針對時戳電子簽章的長期有效性制訂，用戶要使用時戳服務必須先持有 ePKI 組織、個人或程式碼簽章憑證或本公司認可之憑證機構所簽發的憑證，本服務可應用在任何需要證明特定資料的存在時間上，並且不對其時戳的適用性加以限制。

5.4. 一致性

本時戳服務機構使用第 5.2 節所述的時戳政策物件識別碼於其時戳符記上，來表示與時戳政策的一致性。並且接受定期的內部或外部稽核確保符合 RFC3628 之規定，以證明本時戳服務機構符合中華電信公開金鑰基礎建設時戳政策第 6.1 節時戳服務機構的義務裡面所規定的義務，並有實施適當的控管以符合第 7 章所列時戳實務作業基準的需求。

6.義務與責任

6.1. 中華電信 ePKI 時戳服務機構的義務

6.1.1. 一般條款

本時戳服務機構會確保其時戳實務 (如第 7 章所述)，都能夠依據中華電信公開金鑰基礎建設時戳政策來確實執行。本時戳服務機構遵守時戳服務參考到的相關政策所定義的義務，確保它所有的時戳服務都和它的時戳實務作業基準一致。時戳政策及時戳實務作業基準需求為中華電信、用戶、依賴方間合約不可或缺的一部份。

6.1.2. 中華電信 ePKI 時戳服務機構對用戶的義務

本時戳服務機構保證時戳符記的發行符合下列項目：

- 本時戳服務機構依據相關規則作業
- 時戳單元保持與世界協調時 UTC 在正負 1 秒內的最小時間精準性
- 中華電信接受定期進行內部及外部的稽核，以確保遵守相關法規和內部的政策和程序

本時戳服務機構提供高可用性的時戳服務，當發生下列事件不保證可用性：計劃中的技術中斷、時間同步的損失和其他特殊情況下，則不保證可用性。

6.2. 用戶的義務

本時戳實務作業基準訂定用戶在使用中華電信時戳服務前須接受中華電信時戳服務相關合約，並建議當用戶取得時戳符記的時候，必須驗證這個符記是否被正確的簽署，而且用來簽署這個符記的私密金鑰是否已經廢止或過期，以確保時戳符記的正確性。

6.3. 信賴方的義務

所謂的信賴方（Relying Party）意指，凡是使用且信賴時戳政策之時戳符記的組織、個人或程式碼。當信賴方信賴時戳政策之時戳符記時，信賴方應遵守如下的義務規範：

1. 須驗證時戳符記是否被正確地簽署，而且確保簽署時戳的私鑰在進行驗證時還沒被廢止。
2. 應透過中華電信時戳憑證管理中心所提供憑證廢止清冊(Certification Revocation List, CRL)或是線上憑證狀態協定(Online Certificate Status Protocol, OCSP)來判別時戳單元憑證在

有效期間內其簽章金鑰的合法性。

3. 若在憑證過期後才進行驗證，信賴方須確保應用的雜湊函數、演算法及加密金鑰長度仍然具安全性。
4. 須根據時戳政策考量時戳符記使用上的任何限制。
5. 須考量任何其它協議裡面所定義的警告事項。

6.4. 責任

中華電信致力於提供高可用性的服務，但不做任何直接或間接的陳述或保證時戳服務不會中斷及時戳服務的精準度。

中華電信只承擔因中華電信因違反法律所造成錯誤導致用戶或信賴方的損失，而中華電信會提供遵守適用法律，法規和規章的證據。

中華電信不對任何利潤損失、間接或直接的損害或資料遺失損失，只在法律合理的範圍內做任何承擔動作。

中華電信不承擔任何因用戶侵權或適用於條款和條件的信賴方所造成的損失。

中華電信因考量商業因素在限定時間內減輕不可抗力因素的影響，任何因不可抗力因素所造成的延遲，不包含在中華電信負責範圍內。

7.時戳服務機構之時戳實務要求

7.1. 時戳實務作業基準與揭露聲明

7.1.1. 本時戳服務機構實務作業基準

1. 本時戳服務機構每年會進行風險評估，以便評價商業資產與其安全上的威脅，來決定必要的安全控管和運作流程。
2. 本時戳服務機構在本時戳實務作業基準中明確指出其他支援時戳服務外部組織的義務及相關的政策與準則。
3. 本時戳服務機構會確保用戶和信賴方得知時戳實務作業基準及相關的文件。
4. 本時戳服務機構對所有用戶以及信賴方公布時戳服務使用上所涉及的項目以及條件(請參閱第 7.2 節)。
5. 本時戳服務機構由中華電信憑證政策管理委員會為其時戳實務作業基準進行最終的核准與授權。
6. 中華電信憑證政策管理委員會應確保本時戳服務機構的時戳實務作業基準都是被適當執行的。
7. 對於時戳的實作程序，包括維護時戳實務作業基準的責任，時戳服務機構定義檢視的程序於時戳實務作業基準之中。

8. 本時戳服務機構欲變更時戳實務作業基準的話，會經過中華電信憑證政策管理委員會的核准如第 6 項所述，且使修正過後的時戳實務作業基準符合第 4 項的規定。

7.1.2. 本時戳服務機構的揭露聲明

下列有關時戳服務的公布項目以及條件，適用於所有符合本時戳實務的時戳服務用戶以及信賴方。

1. 本時戳服務機構的時戳實務作業基準的發行應經過中華電信憑證政策管理委員會之審查，並使用 ePKI 所屬之中華電信時戳憑證管理中心所簽發的時戳憑證。
2. 任何時戳符記均須包含本時戳服務機構所使用之時戳政策物件識別碼(請參閱第 5.2 節)。
3. 雜湊演算法使用 SHA-256 (OID：2.16.840.1.101.3.4.2.1)，簽章演算法為：sha256WithRSAEncryption (OID：1.2.840.113549.1.1.11)，金鑰長度為 RSA 2048 位元。
4. 時戳符記的簽章預期時效為 10 年。
5. 時戳符記中的時間值相對於世界標準時間而言，其精準度為正負 1 秒鐘。
6. 用戶應盡的義務(請參閱第 6.2 節)。

7. 信賴方應盡的義務(請參閱第 6.3 節)。
8. 中華電信可要求使用戶和信賴方遵守符合法律、時戳服務政策及作業基準的終端用戶合約。
9. 中華電信會收取時戳服務提供之費用。
10. 本時戳服務機構保留系統運作的事件紀錄(請參閱第 7.4.11 節)。
11. 本時戳服務機構適用的法律責任請參閱第 6.4 節。
12. 有關時戳服務之任何建議請洽本時戳服務機構（聯絡資訊：timestamp@cht.com.tw）。

本時戳實務作業基準與相關之時戳服務文件以電子檔案型式放置於中華電信公開金鑰基礎建設所屬的中華電信公開金鑰基礎建設儲存庫(https://eca.hinet.net)，公告並提供下載服務。

7.2. 金鑰管理的生命週期

7.2.1. 時戳服務機構的金鑰產製

本時戳服務機構依第7.2.2.1節規定，在通過FIPS 140-2第3級安全認證或同等級的硬體密碼模組內產製時戳單元的金鑰對，採RSA金鑰演算法。本時戳服務機構之時戳單元的私密金鑰於硬體密碼模組內產製金鑰對，採依照NIST FIPS 140-2 規範之演算法與流程，金鑰之匯出與匯入依照中華電信時戳憑證管理中心憑證實務作業基準第6.2.2

與第6.2.6節規定辦理。對時戳單元私密金鑰備份的持份之安全控管，將以n-out-of-m金鑰分持方式來做時戳單元私密金鑰的備份及回復。

時戳單元的金鑰產製演算法、簽章金鑰長度以及用在時戳符記的簽章演算法，應該符合中華電信時戳憑證管理中心憑證實務作業基準第 6.1.5 節金鑰長度的規範或者是符合現有的時戳技術，以便達成時戳服務機構簽發時戳符記的目的。

時戳單元的簽章金鑰產製由中華電信憑證政策管理委員會的委員及內部的稽核員見證，過程經錄影留存。

7.2.2. 時戳單元私鑰的保護

7.2.2.1.密碼模組標準

使用通過FIPS 140-2第3級安全認證密碼模組，控管IC卡使用通過FIPS 140-2第2級安全認證或相當安全強度的IC卡。

7.2.2.2.金鑰分持之多人控管

對時戳單元私密金鑰備份的持份之安全控管，將以n-out-of-m金鑰分持方式來做時戳單元私密金鑰的備份及回復。

7.2.2.3.私密金鑰託管

時戳單元的簽章用私密金鑰不可被託管（Escrow）。

7.2.2.4.私密金鑰備份

依照第7.2.2.2 金鑰分持之多人控管方法備份本服務中心私密金鑰，並使用通過FIPS 140-2第2級安全認證或相當安全強度的IC卡做為秘密分持的儲存媒體。

7.2.2.5.私密金鑰歸檔

本時戳服務機構時戳單元簽章用私密金鑰不可被歸檔(Archive)。

7.2.2.6.私密金鑰輸入至密碼模組

在下述情況時做私密金鑰輸入密碼模組中：

(1)時戳單元金鑰產製及更換密碼模組時。

(2)金鑰持份備援的回復時。在此情況是以秘密持份(*n-out-of-m* control)的方式來做時戳單元私密金鑰的回復，經由私密金鑰秘密持份IC卡的回復後，便即時將完整的私密金鑰寫入到硬體密碼模組中。

(3)更換密碼模組時，私密金鑰輸入方式採加密方式以確保輸入過程中不得將金鑰明碼暴露於密碼模組之外，私密金鑰輸入完成後，須將輸入過程產製之相關機密參數完全銷毀。

7.2.2.7.私密金鑰之啟動方式

本時戳服務機構時戳單元的私密金鑰之啟用是由n-out-of-m控管IC卡組來控制，不同用途的控管IC卡由管理員或簽發員所保管。

本時戳服務機構之時戳單元的私密金鑰啟動資料由n-out-of-m控管IC卡組保護，IC卡的PIN碼由保管人員自行記憶，不得紀錄於任何媒體上，如登入的失敗次數超過3次，則鎖住此IC卡。IC卡移交時新的保管人員必須重新設定PIN碼。

本時戳服務機構之簽章時戳符記用的密碼模組在匯入時戳單元的私密金鑰後，需透過金鑰產製見證書上之公開金鑰數值比對公鑰值，以確認產製之時戳單元的金鑰對其公鑰值與匯入時戳單元的金鑰對其公鑰值相符，才能讓系統進行運作。

7.2.2.8.私密金鑰之停用方式

如時戳單元的私密金鑰需要停用時，必須由簽發員及管理員藉由由n-out-of-m控管IC卡組透過金鑰管理程式停用。本時戳服務機構之時戳單元的私密金鑰生命週期結束時，須將舊私密金鑰停用，之後依照第7.2.2.9節進行私密金鑰之銷毀。

7.2.2.9.私密金鑰之銷毀方式

為避免本時戳服務機構過期的時戳單元的舊私密金鑰被盜用，影響整個本時戳服務機構資料之真確性，本時戳服務機構於時戳單元的舊私密金鑰不再簽發任何時戳符記後，依照 FIPS 140-2 第 3 級金鑰零值化（Key Zeroization）的規定銷毀時戳單元的舊私密金鑰。

7.2.3. 時戳單元公開金鑰的散布

由中華電信時戳憑證管理中心提供用戶下載所簽發的時戳單元的公鑰憑證、憑證廢止清冊及憑證狀態等資訊的查詢及下載服務。

7.2.4. 時戳單元金鑰的更新

時戳單元的憑證其金鑰對依照中華電信時戳憑證管理中心第 6.3.2 節規定定期更換，以時戳單元的新私密金鑰取代舊私密金鑰簽署時戳符記，並應適時對信賴本時戳服務機構的個體公告。

7.2.5. 時戳單元金鑰生命週期的結束

依照第 7.2.2.9 節私密金鑰之銷毀方式進行私密金鑰銷毀。時戳憑證所記載之公開金鑰在其憑證到期或憑證廢止時結束其生命週期。

7.2.6. 時戳簽章之密碼模組的生命週期管理

時戳單元所採用的硬體密碼模組其運送、存放與點收、查檢程式與韌體更新、維護與送修硬體密碼模組或私密金鑰於硬體密碼模組之移轉遵照內部硬體密碼模組管理程序辦理，以確保時戳簽章的硬體密碼模組之完整性。例如時戳單元之硬體密碼模組在運送過程前需由系統管理員進行妥善包裝，以讓硬體密碼模組有基本保護措施。在運送過程中經由多重角色控管，例如管理員負責搬運，實體控管員、稽核員、產品經理或主管至少其中之一陪同監督，以確認在運送過程中沒有遭到破壞。

7.3. 時戳

7.3.1. 時戳符記

本時戳服務機構確保時戳符記產製過程的安全性，以及時戳時間值的正確性，特別是：

1. 時戳符記包含有關時戳政策的識別碼。
2. 每一個時戳符記具有唯一的識別性。
3. 時戳單元所使用在時戳符記的時間值，應該可至少追溯到我國國家時間與頻率標準實驗室，或再加上其他的世界標準時間實驗室所發佈出來的時間值。

4. 時戳符記裡面包含的時間值依據世界標準時間值進行同步至時戳政策所定義的精準度以內，如果時戳符記本身有包括時間精準度資訊，也會達到此精準度需求。
5. 當時戳單元無法與時間源同步時，將停止簽發時戳符記
6. 時戳符記應該包含一個由服務要求者所提供，可代表欲進行時戳資料的唯一值(例如：雜湊值)。
7. 時戳符記由專門用以簽署時戳符記的金鑰進行簽章。

7.3.2. 與世界標準時間同步

本時戳服務機構確保它的時間和世界標準時間同步至所宣稱的精準度以內，特別是：

1. 時戳單元之時間被保護在時戳計時卡內，以 IEEE 1344 與國家標準時間訊號保持同步並且維持時間之精準度。
2. 保護時戳單元的時間值免於某些威脅(例如：非授權人士的存取或電磁波影響)，這些會導致時間值的精準度超出所宣稱的誤差範圍。
3. 當時戳單元無法與時間源同步時，將停止簽發時戳符記，並在時戳符記中回應通知用戶方直到時間恢復同步。
4. 本時戳服務機構確保當閏秒產生的時候，時間值仍然可以和世界

標準時間同步，在潤秒修正前的 24 小時會以接收衛星的方式，收到由 BIPM(國際度量衡局)發佈的閏秒修正通知，而且當閏秒產生的時候，透過重複出現兩次該秒數，例如 23:59:59 UTC (07:59:59 本地時間)，以保持閏秒調整作業的正確性，以上步驟皆會記錄在設備的 Log 檔裡面可供查詢。

5. 時戳單元時間的手動管理則需依規定的授權人員進行處理，手動管理可能情形為，時戳設備故障或需以 IRIG-B 1344 作為優先參考來源時，需要手動關閉衛星(GNSS)的接收。

7.4. 本時戳服務機構的管理與運作

7.4.1. 安全控管

本時戳服務機構機房位於中華電信股份有限公司數據通信分公司，符合儲存高重要性及敏感性資訊的機房設施水準，並具備門禁、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本時戳服務機構之相關設備。

本時戳服務機構依照中華電信股份有限公司資訊安全管理規範與實施細則及其規定之安全設定技術文件設定作業系統安全性設定。

7.4.2. 資產分類與管理

為確保資訊和其他資產獲得適當的安全保障，本時戳服務機構維護所有資產清單，並且將這些資產依風險分析分類，並對應到相對的保護等級。

7.4.3. 人員控管

7.4.3.1.身家背景、資格、經驗及安全需求

(1) 人員甄選及進用之安全評估

A. 個人性格之評估。

B. 申請者經歷之評估。

C. 學術、專業能力及資格之評估。

D. 人員身分之確認。

E. 人員操守之評估。

(2) 人員之考核管理

本時戳服務機構之相關人員在進用前先進行資格審查，以確認其資格及工作能力。正式進用後，必須接受適當之教育訓練，並以書面方式簽定應負之責任，同時每年進行資格複查，如無法通過資格複查將調離現職，改派其他符合資格人員擔任。

(3) 人員之任免及遷調管理

如人員之進用、約聘僱條件或契約有所變更，特別是人員離職或約聘僱契約終止時，將遵守維護保密責任之約定。

(4) 維護保密責任之約定

本時戳服務機構之相關人員均負維護保密之責任，並簽署保密切結書，不得以口頭、影印、借閱、交付、文章發表或其他方法洩漏機敏性資訊。

7.4.3.2.身家背景之查驗程序

本時戳服務機構對於第 7.4.3.3 節所述之各種信賴角色人員，在進用前予以資格審查，以確認其身分資格相關證明文件是否屬實。

7.4.3.3.教育訓練需求

信賴角色	教育訓練需求
管理員	1、本時戳服務機構之安全認證機制。 2、本時戳服務機構安裝、設定和維護之操作程序。 3、建立和維護系統之用戶帳號操作程序。 4、設定稽核參數操作程序。

信賴角色	教育訓練需求
	5、產製和備份本時戳服務機構之時戳單元金鑰操作程序。 6、災後復原及業務永續經營之程序。
簽發員	1、本時戳服務機構之安全認證機制。 2、本時戳服務機構系統軟硬體的使用及操作程序。 3、時戳單元金鑰的啟動操作程序。 4、時戳單元金鑰的停止操作程序。 5、災後復原及業務永續經營之程序。
稽核員	1、本時戳服務機構之安全認證機制。 2、本時戳服務機構系統軟硬體的使用及操作程序。 3、產製和備份本時戳服務機構之時戳單元金鑰操作程序。 4、稽核紀錄的查驗、維護和歸檔程序。 5、災後復原及業務永續經營之程序。
維運員	1、本時戳服務機構之安全認證機制。 2、系統設備的日常運作維護程序。

信賴角色	教育訓練需求
	3、儲存媒體之更新程序。 4、災後復原及業務永續經營之程序。 5、網路和網站的維護程序。
實體安全控管員	1、設定實體門禁權限程序。 2、災後復原以及業務永續經營之程序。

7.4.3.4.人員再教育訓練之需求及頻率

在本時戳服務機構之軟硬體升級、工作程序改變、設備更換或相關法規改變時，將安排相關人員再教育訓練並記錄受訓情形，以確實瞭解相關作業程序及法規之改變。

7.4.3.5.工作調換之頻率及順序

(1) 管理員調離原職務滿 1 年後，才可轉任簽發員或稽核員。

(2) 簽發員調離原職務滿 1 年後，才可轉任管理員或稽核員。

(3) 稽核員調離原職務滿 1 年後，才可轉任管理員或簽發員。

(4) 擔任維運員滿 2 年，且已接受相關教育訓練及通過審核，才可轉任管理員、簽發員及稽核員。

7.4.3.6.未授權行動之制裁

本時戳服務機構之相關人員，如違反中華電信公開金鑰基礎建設時戳政策與本作業基準或其他本時戳服務機構公布之程序，將接受適當的管理與懲處，如情節重大而造成損害者，將採取法律行動追究其責任。

7.4.3.7.聘雇人員之規定

本時戳服務機構任職之聘雇人員須具備足夠的知識技能與道德規範，遵守本作業基準相關規定，並依循本作業基準相關規定及簽定之相關保密協定進行作業。

7.4.3.8.提供之文件資料

本時戳服務機構提供憑證政策、技術規範、本實務作業基準、系統操作手冊等相關文件給本管理中心之相關人員。

7.4.4. 實體與環境安全

7.4.4.1.實體所在及結構

本時戳服務機構機房位於中華電信股份有限公司數據通信分公司，符合儲存高重要性及敏感性資訊的機房設施水準，並具備門禁、

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本時戳服務機構之相關設備。

7.4.4.2. 實體存取

本時戳服務機構以保證等級第 3 級的實體控管規定運作。機房共有 4 層門禁，第 1 層和第 2 層分別為全年無休的大門及大樓警衛，第 3 層為樓層讀卡機進出管制系統，第 4 層為機房人員指紋辨識進出管制系統，指紋辨識器採用 3 度空間指紋取樣，可以判別辨識物的紋深、色澤及是否為活體。

除門禁系統可限制不相干人員接近機房外，機箱之監控系統可控制機箱之開啟，以防止未經授權存取硬體、軟體和硬體密碼模組等相關設備。

任何可攜式儲存媒體帶進機房，需檢查並確認沒有電腦病毒及任何可能危害本時戳服務機構系統的惡意軟體。

非本時戳服務機構人員進出機房，須填寫進出紀錄，並由本時戳服務機構相關人員全程陪同。

本時戳服務機構相關人員離開機房時，將進行以下之查驗工作並記錄，以防止未授權人員進入機房：

(1) 確認設備是否正常運作。

(2) 確認機箱門是否關閉。

(3)確認門禁系統是否正常運作。

7.4.4.3.電力及空調

本時戳服務機構的電力系統，除市電外，另設有發電機（滿載油料可連續運轉 6 天）及不中斷電源系統（UPS），並具有市電及發電機的電源自動切換功能，可提供至少 6 小時以上備用電力，供儲存庫備援資料。

本時戳服務機構機房設有恆溫恆濕空調系統，以控制環境的溫度及濕度，使機房保持最佳運作環境。

7.4.4.4.水災防範及保護

本時戳服務機構機房設置在基地墊高建築物的第 3 樓層(含)以上，該建築物具備防水閘門和抽水機，且沒有因為水災造成重大損害紀錄。

7.4.4.5.火災防範及保護

本時戳服務機構機房具備自動偵測火災預警功能，系統可自動啟動滅火設備，並設置手動開關於各機房主要出入口，以供現場人員於緊急情況時以手動方式啟動。

7.4.4.6.媒體儲存

稽核紀錄、歸檔和備援資料的儲存媒體於本時戳服務機構機房儲存，另將複製 1 份送至異地備援場所儲存。

7.4.4.7.廢料處理

本時戳服務機構機敏性資訊，文件資料部分在不需使用時，將經碎紙機處理；磁帶、硬碟、磁碟及其他形式的記憶體，在報廢前，將經格式化程序清除儲存的資料，光碟將被實體銷毀。

7.4.4.8.異地備援

異地備援的地點在臺中，與本時戳服務機構機房距離30公里以上。備援的內容包括資料與系統程式。本時戳服務機構之資料與系統程式將依照備份程序，以複製方式定期備份至儲存媒體存放，及定期放至異地存放。

7.4.5. 操作管理

本時戳服務機構提供時戳政策、本實務作業基準、系統操作手冊等相關文件給本時戳服務機構之相關人員，相關人員依照上述文件進行操作管理。

7.4.6. 系統存取的管理

本時戳服務機構主機建置於防火牆內部，外界無法直接連線。時戳主機透過防火牆系統控管，連線至本時戳服務機構主機之資料庫，擷取時戳簽署資訊或查詢時戳簽署資訊。

本時戳服務機構公布的資訊，主要提供用戶或信賴憑證者查詢之用，因此開放提供閱覽存取，並將維持其可接取狀態及可用性。

同時為保障時戳主機之安全應進行存取控制，設定存取權限，有授權者方可存取。

7.4.7. 信賴系統的部署和維持

本時戳服務機構的軟體在首次安裝時，將確認是由供應商提供正確的版本且未被修改。系統安裝後，本時戳服務機構每天自動檢驗軟體的完整性。

本時戳服務機構將記錄和控管系統的組態及任何修正與功能提升，同時偵測未經許可修改系統之軟體或組態。

7.4.8. 時戳服務的對策

萬一時戳單元金鑰遭到破解，本時戳服務機構將遵循程序，向申請時戳單元憑證的憑證中心申請廢止憑證。時戳單元憑證無效，時戳

單元將不會發出時戳。若時間遠離所參考世界標準時間聲明的準確性之外，時戳單元也將不會發出時戳，直到完成回復時間校準之步驟。本時戳服務機構將留存相關稽核軌跡。

7.4.9. 本時戳服務機構終止服務

本時戳服務機構終止服務時，將依據本時戳服務機構下述相關規定辦理。

本時戳服務機構遵守以下事項，以為確保終止服務對用戶與信賴憑證者所造成之影響最小：

(1) 本時戳服務機構於預定終止服務 3 個月前，將通知所有使用本時戳服務機構服務用戶（但無法通知者，不在此限），並公告於時戳網站上。

(2) 本時戳服務機構終止服務時必須：

A. 依電子簽章法相關規定進行檔案紀錄之保管及移交。

B. 針對使用本時戳服務機構時戳之用戶，依合約或所付金額比例合理退還其所繳費用，最高以其所繳費用 80%為上限。

本時戳服務機構結束業務時，對用戶或信賴憑證者，除依前項規定退費外，不負任何賠償責任。

7.4.10. 遵守法律的要求

本時戳服務機構因執行時戳簽署及管理作業需要，所簽署的相關協議之解釋及合法性，遵循我國相關法令規定辦理。

7.4.11. 關於時戳服務操作資訊的紀錄

本時戳服務機構歸檔資料之保留期限為 10 年，用來處理歸檔資料的應用程式也將維護 10 年。

歸檔資料逾保留期限後，得以安全方式銷毀，但電子型式資料檔如涉及未來法律舉證需求者得備份至其他媒體並提供適當保護。所有紀錄被視為機密。有關記錄用戶的任何信息都應保密，除非取得用戶同意公開。

司法機關、監察機關或治安機關如因調查或蒐集證據需要，必須查詢時戳服務機構機敏性資訊，依法定程序辦理，不對用戶另作通知；惟本時戳服務機構保留向申請查詢之機關收取合理費用之權利。

1. 用戶得查詢本時戳服務機構機敏性資訊；本時戳服務機構以掛號信件或電子郵件通知用戶，惟本時戳服務機構保留向申請查詢之用戶收取合理費用之權利。

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

驗證時戳符記時，驗證程式需確保時戳單元憑證是受信任且為未廢止的狀態。這意味著時戳安全取決於負責簽發時戳單元憑證的憑證管理中心本身的安全性，和提供準確的廢止狀態資訊。每一次驗證時戳符記，必須藉由中華電信時戳憑證管理中心所提供的憑證廢止清冊或線上憑證狀態協定查詢服務確認當下的時戳單元憑證狀態資訊。且必須循憑證串鍊驗證中華電信時戳憑證管理中心之憑證機構憑證的狀態資訊。

在應用程式取得時戳時，需要有確認時戳正確及完整性的安全的考量。時戳請求者必須真正確保在資料的雜湊值與時戳符記中包含的雜湊值是一致的才能使用。