中華電信公開金鑰基礎建設

時戳服務政策

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) 將「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。

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，以下簡稱本基礎建設)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。本基礎建設依照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政策（以下簡稱本時戳政策）主要提供本基礎建設所需時戳服務作業的共同規範，此政策基於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中華電信時戳服務是否可信賴時之確認依據。

本時戳政策主要依據時戳服務需求及相關國際標準所訂定之政策技術文件（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），作為中華電信公開金鑰基礎建設之時戳服務機構（Time Stamp Authority，TSA）於訂定時戳實務作業基準時之依循。

本時戳政策描述時戳服務機構所發行的時戳符記和世界標準時間(Coordinated Universal Time，UTC)同步作業之規範，以及經由時戳單元(Time-Stamping Unit，TSU)簽署數位簽章的政策需求。至於進一步的執行細節，可參考中華電信時戳服務機構的實務作業基準，以瞭解是否符合本時戳政策的需求。

1.2. 時戳政策及實務作業基準之關係

時戳服務機構必須於時戳實務作業基準中說明如何達成本時戳政策之需求。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，詳述於本文件之第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1.75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] 中華電信通用憑證管理中心憑證實務作業基準第1.95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] 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, 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. 時戳服務機構揭露聲明(Disclosure Statement)：時戳服務機構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)：一個由時戳服務機構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)所信任且發行安全的時戳符記之組織稱為時戳服務機構。時戳服務機構必須提供第 4.1 節所講的兩種時戳服務元件。時戳服務機構也必須對那些由一或多個時戳單元所產生及簽章的作業負責任，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。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，但該管理中心必須確保這些團體所提供的服務都能夠根據本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

一般而言，時戳政策主要是在強調時戳服務機構應該堅持哪些原則，而時戳實務作業基準則是在描述如何去實作這些應堅持的事項。

4.4.2. 差異程度

時戳政策在本質上也和時戳實務作業基準不同，一份時戳政策與特定的時戳服務機構之作業環境是彼此獨立的，反之，一份時戳實務作業基準就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。

4.4.3. 途徑

本文件主要是在描述達成時戳服務需求所應該遵循的時戳政策，而各時戳服務機構所定義的時戳實務作業基準則是描述要如何符合這些政策需求的方法。因此一份時戳政策也許可由時戳服務的用戶定義出來，然而時戳服務機構的實務作業基準卻一定是由時戳服務提供者所定義。本文件則是由時戳服務提供者(中華電信)所定義。

5.時戳政策

5.1. 概要

時戳政策就是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。本時戳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，就是每個時戳符記要包含一個

適用政策的識別碼，且必須支援中華電信公開金鑰基礎建設所簽發的憑證，而且發出時間的精準度必須在 UTC 的正負 1 秒以內。時戳服務機構要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

在時戳服務機構給用戶以及信賴方的時戳實務作業基準或揭露聲明中，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。本時戳政策的物件識別碼(Object Identifier)為：id-cht-ePKI-tsapolicy ::= {id-cht-ePKI 5}

其中，id-pen-cht ::= {1 3 6 1 4 1 23459}是本公司在網際網路號碼分配機構(Internet Assigned Numbers Authority, IANA)註冊之私人企業數值(Private Enterprise Number, PEN)。針對不同的簽章演算法，細分為以下之時戳政策識別碼，供時戳服務機構選用:

id-cht-ePKI-tsapolicy-SHA256withRSA2048 ::= {id-cht-ePKI-tsapolicy 1}
id-cht-ePKI-tsapolicy-SHA256withRSA3072 ::= {id-cht-ePKI-tsapolicy 2}
id-cht-ePKI-tsapolicy-SHA256withRSA4096 ::= {id-cht-ePKI-tsapolicy 3}
id-cht-ePKI-tsapolicy-SHA384withRSA2048 ::= {id-cht-ePKI-tsapolicy 4}
id-cht-ePKI-tsapolicy-SHA384withRSA3072 ::= {id-cht-ePKI-tsapolicy 5}
id-cht-ePKI-tsapolicy-SHA384withRSA4096 ::= {id-cht-ePKI-tsapolicy 6}
id-cht-ePKI-tsapolicy-SHA512withRSA2048 ::= {id-cht-ePKI-tsapolicy 7}
id-cht-ePKI-tsapolicy-SHA512withRSA3072 ::= {id-cht-ePKI-tsapolicy 8}
id-cht-ePKI-tsapolicy-SHA512withRSA4096 ::= {id-cht-ePKI-tsapolicy 9}

5.3. 用戶群體及適用性

本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，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

時戳服務機構應該使用本時戳政策第 5.2 節所述的時戳政策識別碼於其時戳符記上，來表示與這政策的一致性。並且接受定期的內部和外部稽核，以證明時戳服務機構符合本時戳政策第 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 章節所列時戳實務作業基準的需求。

6.義務與責任

6.1. 時戳服務機構的義務

6.1.1. 一般條款

時戳服務機構會確保其時戳實務作業基準需求(如第 7 章所述)，都能夠依據本時戳政策來確實執行。時戳服務機構將會遵守時戳服務參考到的相關政策所定義的義務，也會確保它所有的時戳服務都和它的時戳實務作業基準一致。

6.1.2. 時戳服務機構對用戶的義務

時戳服務機構將依照本時戳政策經營，提供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，並提供時戳服務機構系統的高可用性，但計劃中的技術中斷、時間同步的損失和其他特殊情況下，則不保證可用性；另外，將會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。

6.2. 用戶的義務

本時戳政策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

本時戳政策所謂的信賴方（Relying Party）意指，凡是使用且信賴本時戳政策之時戳符記的組織、個人或程式碼。當信賴方信賴本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。此一驗證程序可應用憑證廢止清冊(Certification Revocation List，CRL)或是線上憑證狀態協定(Online Certificate Status Protocol，OCSP)以確認之。
2. 須根據本時戳政策考量時戳符記使用上的任何限制。
3. 須考量任何其它協議裡面所定義的警告事項。

6.4. 責任

除非是法律適用的情形，時戳服務機構不會承擔任何額外的責任。

7.時戳實務作業基準需求

7.1. 時戳實務作業基準與揭露聲明

7.1.1. 時戳服務機構的實務作業基準

時戳服務機構的實務作業基準應能證明所提供的時戳服務是可靠的，因此它必須符合以下要件：

1. 時戳服務機構應該進行風險的評估，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. 時戳服務機構應該於時戳實務作業基準中明確表達其實作程序與本時戳政策的所有需求之對應(address)關係。
3. 如果時戳服務機構有其他支援時戳服務的外部組織，則應該在時戳實務作業基準中明確指出這些外部組織的義務及相關的政策與準則。
4. 時戳服務機構應確保用戶和信賴方得知時戳實務作業基準及相關的文件，以遵從本時戳政策之規範。
5. 時戳服務機構應該要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)。
6. 時戳服務機構應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。

7. 時戳服務機構的高階管理團隊應確保時戳實務作業基準都是被適當執行的。
8. 對於時戳的實作程序，包括維護時戳實務作業基準的責任，時戳服務機構應該在時戳實務作業基準中定義檢視的程序。
9. 時戳服務機構如果要變更時戳實務作業基準的話，需要經過中華電信憑證政策管理委員會的核准如第 6 項所述，且需使修正過後的時戳實務作業基準能立即符合第 4 項的規定。

7.1.2. 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政策的時戳服務用戶以及信賴方。

1. 時戳機構的時戳實務作業基準須通過中華電信憑證政策管理委員會之審查，並使用中華電信公開金鑰基礎建設所屬之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政策之物件識別碼(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： sha2WithRSAEncryption (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. 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)。

9. 本時戳政策適用的法律責任請參閱第 6.4 節。

10. 有關時戳服務之任何建議請洽相關之時戳服務機構。

本時戳政策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儲存庫(https://eca.hinet.net)中，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

時戳服務機構應該確保任何加密簽章的金鑰是在安全控管的環境下產製。

7.2.1.1. 時戳單元的簽章金鑰其產製過程應該在雙重控制下由受信任角色(請參閱第 7.4.3 節)的人員在實體安全環境(請參閱第 7.4.4

節）中進行。那些被授權去實行此一產製金鑰的人員，應限於根據時戳實務作業基準要求的人員。

7.2.1.2. 產製時戳單元簽章金鑰的密碼模組應該符合下列的任一條件：

1. 符合 FIPS 140-2 Level 3 以上的需求，或是
2. 符合 CEN Workshop Agreement 14167-2[CWA 14167-2]的需求，或是
3. 必須為確實根據 ISO 15408 的 EAL 4 或相同安全等級的規範所實作的可信賴系統。如果是依據此項條件的話，密碼模組應該要基於風險分析和實體及其他非技術性的考量，提出安全標的或保護剖繪(Protection Profile)，以達到本時戳政策的安全需求。

7.2.1.3. 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，應該符合中華電信公開金鑰基礎建設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。

7.2.2. 時戳單元私鑰的保護

時戳服務機構應該要確保時戳單元的私鑰其機密性以及完整

性，特別是：

1. 時戳單元的簽章私密金鑰應該採用第 7.2.1.2 節所描述之密碼模組的安全條件，執行其保存及使用作業。
2. 如果時戳單元的簽章私鑰有進行備份的話，那麼此私鑰應該要由實體安全環境雙重管制制度下所信任的人來進行複製、儲存、和復原的動作。
3. 任何時戳單元之簽章私密金鑰的備份在儲存到外部裝置之前，都應該經由密碼模組執行加密保護作業以確保它的機密性。

7.2.3. 時戳單元公開金鑰的散布

在把公開金鑰散布給信賴方的時候，時戳服務機構應該要確保時戳單元公鑰的完整性和真實性，而且應該注意：

1. 時戳單元的簽章驗證用公開金鑰應該要讓信賴方能在其公開金鑰憑證裡面取得。
2. 時戳單元的簽章驗證用憑證應該是由中華電信公開金鑰基礎建設之憑證管理中心根據其憑證政策所簽發出來的，而這個憑證政策的安全等級要跟時戳政策的安全等級一樣或更高。

7.2.4. 時戳單元金鑰的更新

時戳單元的憑證有效期間不應該比所選用的演算法及金鑰長度的安全期間還長，因此時戳單元的金鑰也要因應這些需求而做更新的動作。有關時戳單元的金鑰使用效期應該考慮：

1. 當時戳單元的金鑰停用以後，已簽發的時戳服務相關資料起碼要保存一年以上。因此金鑰的使用期間愈長的話，則須保存的時戳服務資料就愈多。(請參閱第 7.4.11 節)
2. 如果時戳單元的私密金鑰被破解，那麼它的使用期間愈長的話，則受到影響的時戳符記就愈多。

7.2.5. 時戳單元金鑰生命週期的結束

時戳服務機構應該確保時戳單元的簽章私密金鑰在它的生命週期結束後不被使用，特別是：

1. 在時戳單元的金鑰過期時，必須確保依據標準作業程序所產生的新金鑰被放置到適當的地方。
2. 過期之時戳單元的私鑰或者是私鑰的任何部分，及其任何的備份都應該被銷毀，以防止私鑰被取得。
3. 如果簽章私鑰效期已過期，那麼時戳符記的產製系統應該拒絕其任何產製時戳符記的嘗試。

7.2.6. 時戳簽章之密碼模組的生命週期管理

時戳服務機構應該要確保密碼模組的簽章硬體在它的生命週期內之安全性。特別是：

1. 簽章時戳符記之密碼模組在運送過程中沒有遭到破壞。
2. 簽章時戳符記之密碼模組在儲存過程中沒有遭到破壞。
3. 當安裝、啟動、複製密碼模組的簽章金鑰時，應該在具備實體安全的環境裡，由雙重管制制度中所信任的角色來執行。
4. 應該要確保簽章時戳符記之密碼模組各項功能正常。
5. 當密碼模組報廢的時候，儲存於其內的時戳單元金鑰應該被確實銷毀。

7.3. 時戳

7.3.1. 時戳符記

時戳服務機構應該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. 時戳符記應該包含有關時戳政策的識別碼。
2. 每一個時戳符記都應該具有唯一的識別。
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應該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，也應達到此精準度需求。
5. 假如時戳提供者的時間值已經被偵測出無法達到規定的精準度，那麼時戳服務機構就不應該簽發時戳符記。
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. 時戳符記應該由專門用以簽署時戳符記的金鑰進行簽章。
8. 時戳符記應該包含：
   - 時戳服務機構的識別碼。
   - 時戳單元的識別碼。
   - 如果可行的話，也應該包含一個代表時戳服務機構所在國家的地區識別碼。

7.3.2. 與世界標準時間同步

時戳服務機構應該要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. 時戳單元的時間值應該持續微調以確保不會低於所宣稱的精準度。
2. 時戳單元之時間被保護在硬體密碼模組內，每日須與參考世界標準時間源重新校時。
3. 應該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)，這些將會導致時間值的精準度超出所宣稱的誤差範圍。
4. 假如用在時戳符記的時間值和世界標準時間同步的時間值有所偏移的話，時戳服務機構應該要能夠偵測出來，並通知信賴方(請參閱第 7.4.8 節)。
5. 如果時戳單元之時間漂移至聲明的準確性之外，且重新校時失敗，時戳服務機構將不會發出時戳，直到恢復正確的時間。
6. 時戳服務機構也應該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，而且當閏秒產生的時候，事件紀錄也要精確地記錄此一事件，以保持閏秒調整作業的正確性。
7. 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。

7.4. 時戳服務機構的管理與運作

7.4.1. 安全控管

根據最佳實務和相關標準的要求，時戳服務機構對於文件，實作，及保持適當的安全條款，並設計主動安全管理方案。中華電信憑證政策管理委員會負責整體時戳服務政策及做法的制定，提供時戳服務的系統和資訊資產應被記錄在案，並且對實施設備依安全控制和操作規則實施和維護。明確規定的協力廠商的責任。須保留並披露相關做法及所有各方的責任。

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，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

為提高運作的可信度，時戳服務機構保持適當的人事作業，以符合安全最佳實務和相關標準的要求。

尤其是：

1. 時戳服務機構聘僱具備專業知識，經驗和必要資格之人員，以提供服務及適當的工作職能。
2. 應於時戳服務機構的安全性原則中明確定義時戳服務機構的操作中可信賴的安全角色和責任，並應記錄在工作描述中。
3. 時戳服務機構人員須具有職責分離和以最小權限的角度定義的工作說明，基於職責和存取層級決定職位敏感度，背景審查和員工培訓和意識。
4. 時戳服務機構人員須行使符合時戳服務機構資訊安全政策之行政及管理程序和流程。

以下額外控管須適用於時戳管理：

1. 聘僱之管理人員應具有：
   - 時戳技術知識；
   - 數位簽章技術知識；
   - 對於時戳單元時間校準或同步與世界標準時間機制的知識；
   - 熟悉安全責任人員的安全程序；
   - 資訊安全和風險評估之經驗。
2. 所有在受信任角色的時戳服務機構人員須避免可能有損公正性的時戳服務機構操作之利益衝突。
3. 受信任角色包括下列角色職責：

- 安全人員：全面負責管轄安全作法的實施。
- 系統管理員：授權安裝、配置和維護時戳服務機構信賴系統的時戳管理。
- 系統操作員：負責日常時戳服務機構信賴系統的基礎操作。授權執行系統備份和復原。
- 系統稽核員:授權查看時戳服務機構信賴系統的檔案和稽核。

4. 時戳服務機構人員須由由主責之科長正式任命為信任角色。
5. 時戳服務機構不得委任受信任或管理角色於已有任何嚴重犯罪或其他影響適合這個職位之罪行的人。在完成所有必要的檢查前，人員不得存取受信任的功能。

7.4.4. 實體與環境安全

根據中華電信的安全控管規範，應確保對關鍵服務的實際存取控制和資產實際風險最小化。尤其是：

1. 對時戳供應與時戳管理：
   - 對與時戳服務有關的設施之實際存取,限於適當授權的個人；
   - 執行控管，以避免損失，損害或洩漏資產和中斷商務活動；
   - 執行控管，以避免資訊和資訊處理設施的洩漏或被盜竊。
2. 對密碼模組的存取控制，需滿足條款第 7.2.1 和第 7.2.2 節所述之

密碼模組安全需求。

3. 下列附加之控管適用於時戳管理：

- 時戳管理設施的操作須在實體保護的環境中，以避免對系統或資料的未授權之存取而造成服務洩漏。
- 時戳管理之實體保護是透過建立明確的安全邊界之實現（即實體障礙）。任何與其他組織共享的部分，皆處於此邊界之外。
- 實行實體與環境安全之控管以保護容納系統資源之設施，系統資源本身，及該設施是用於支援其運作。
- 時戳服務機構資訊安全政策（包括關於時戳管理之系統）說明其實體存取控管、消防安全因素、公用設施之失效（如電力，電信）、防範盜竊、闖入和災難復原。
- 實行控管以防止涉及時戳相關的設備、資訊、媒體及軟體未經授權帶離現場。

7.4.5. 操作管理

時戳服務機構應確保時戳服務機構系統元件的安全和正確操作，將失敗的風險降至最低，時戳服務機構制定並執行內控機制

1. 系統和資訊的完整性保護

2. 事故回報和應變程序
3. 媒體應安全處理
4. 應制訂與安全角色相關之程序並實施
5. 執行資訊分類計畫，當媒體不再需要時，對包含敏感性資料媒體的安全處置
6. 容量需求進行監測
7. 事故報告和回應

時戳服務機構透過內部和外部稽核以達成有效之控管。

7.4.6. 系統存取的管理

時戳服務機構對受影響之設施，硬體，系統及資訊，保持適當的實體及邏輯存取控管。

7.4.7. 信賴系統的部署和維持

時戳服務機構使用之資訊系統有防止修改之安全機制。時戳服務機構系統之部署與維護控管，需根據時戳服務機構之安全機制，若有軟體的變更，應當遵循標準化的變更控制程序。

7.4.8. 時戳服務的對策

萬一時戳單元私鑰遭到破解，時戳服務機構將遵循程序，廢止相關憑證並將其加至憑證廢止清冊。若私鑰無效，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，時戳單元將不會發出時戳，直到完成回復時間校準之步驟。時戳服務機構需維護相關稽核軌跡。

7.4.9. 時戳服務機構終止

在時戳服務機構終止的情況下，將遵循時戳服務機構終止程序。包括在最低限度通知，終止任何有關代表時戳服務機構執行發行時戳符記的授權，廢止時戳單元憑證，轉移責任至可靠方以維持事件日誌和稽核檔案，以及時戳單元私鑰(包括備份副本)應使用私鑰無法被回收的方式予以銷毀。

7.4.10. 遵守法律的要求

時戳服務機構應符合適用的法律要求，如：電子簽章法，以及個人資料保護法的要求。對個人資料須採取適當的技術和組織措施，以防止未經授權或非法之處理，及個人資料之意外遺失或破壞或損壞。除非使用者同意或法院命令或其他法律的規定，使用者貢獻時戳服務

機構之資訊須完全防止遭披露。

7.4.11. 關於時戳服務操作資訊的紀錄

時戳服務機構維持 10 年的所有相關的資訊操作紀錄。相關紀錄保護時戳資料之完整性，並移至受保護的存儲伺服器且隨後歸檔。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。

在用戶的要求或是法院命令或其他法律要求之下，有關的時戳服務的操作紀錄是可取得的。該時戳服務機構保持包括精確的時間之記錄：

1. 時戳請求和建立時戳。
2. 有關時戳服務機構的管理事件(包括憑證管理、金鑰管理和時間同步)。
3. 有關時戳單元私鑰和憑證之生命週期的事件。

7.5. 組織

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。這意味著時戳安全性取決於負責簽發時戳單元憑證和提供準確廢止狀態資訊的 CA 本身安全性。每一次驗證時戳符記，必須確認當下的時戳單元憑證廢止清冊狀態資訊。

時戳是在給定的時間點驗證為有效，這並不意味著時間點驗證以後必然保持有效。每一個時戳符記被驗證在時戳單元憑證的有效期間，必須再反復去驗證廢止狀態的資訊，在時戳單元金鑰遭破解的情況下，所有由該時戳單元產生的時間符記將變成無效。

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。