時戳 – 電子化社會的時間證明

想像一下實體世界的抽獎活動，主辦單位會告訴觀眾(或聽眾/讀者)朋友截止日期是 X 月 X 日(逾期無效ㄡ)；可是住在偏遠地區的朋友可能需要三到五天才能寄到，而住在市區的朋友則只要一至兩天就能寄到主辦單位，所以當然不能以主辦單位收到的時間爲準，於是只能以觀眾朋友寄出的時間爲準，但是誰來證明這麼多來自四面八方的郵件時間呢 ？ 這就是「郵戳爲憑」！ 也就是大家都相信郵局，當郵差收到這些信件時，在郵票上面蓋上一個戳章，上面有時間日期，這就是實體世界裡的時間證明。

在現今的電子商業(e-Business)世界裡，任何電子交易或文件往來更需要有可信任與安全的基礎，近年來被大家普遍討論與應用的 PKI (Public Key Infrastructure) 就是要建立這樣一個安全的電子商業環境。PKI 主要目的就是要確保電子交易的來源處與目的處的正確無誤、交易內容不會被第三者看見，也不會被竄改，發送者與接收者的不可否認；所以它應該要滿足了下面四點功能:

- 身份確認(Authenticity)
- 資料私密性(Privacy)
- 資料完整性(Integrity)
- 不可否認性(Integrity)

可是誰來證明雙方交易的時間呢 ？ 到底以誰的時間爲準呢 ？ 網路傳輸延遲的時間怎麼辦 ？ 兩邊的電腦時間可能差距好幾分鐘，也可能有人會有意或無意的更動電腦時間 ！ 那到底有沒有一個大家公認的「中原標準時間」呢 ？PKI 顯然少了對於時間證明的機制 ！

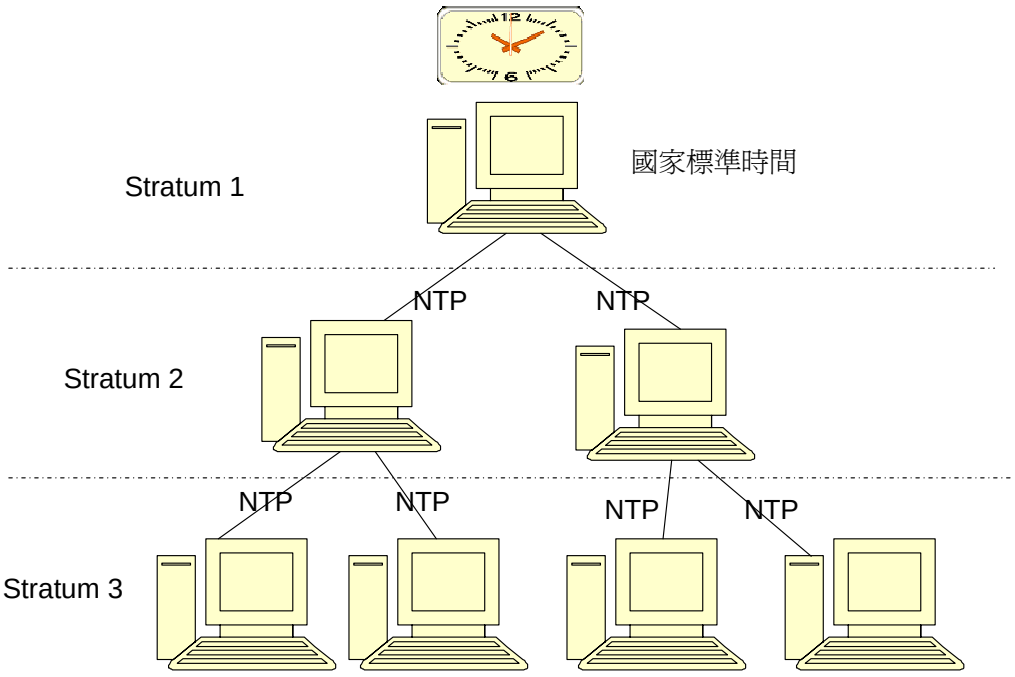
目前現實社會裡，不管有沒有 PKI 的電子交易裡，都是以「聲音大」的一方的時間爲準，於是我們日常生活裡，銀行轉帳就以銀行主機或財金主機爲準，股票下單就以證交所的爲準(萬一券商電子下單主機給你延遲一分鐘，害你損失一些錢，你如何舉證 ？)，網路競標或電子投標都是以「他們」收到的時間爲準，如果你的網路太慢，算你活該倒楣 ！

爲什麼不能有一個公正機構，就像郵局提供郵戳一樣，提供一個足夠安全並被大家所信任的「時間」證明呢 ？

有人就提出，只要把彼此電腦的時間同步，不就好了嗎 ？ 即使有的電腦時鐘會走偏，只要將「對時」的頻率增加，例如每一個小時「校時」一次，就能將所有電腦的時間偏差縮小到可接受的程度。企業內部可以規定所有電腦都向某一指定

電腦校時，那跨企業間呢 ？ 當然也可以依據大家公認的機構來校時，於是我們理論上就可能讓所有電腦都有一個誤差值很小的標準時間。那電腦與電腦之間怎麼校時呢 ？ 當然不可能由人工來做，因爲所有電腦都可以接上網路，於是就有人提出網路校時的方法，這就是 NTP (Network Time Protocol)的產生。

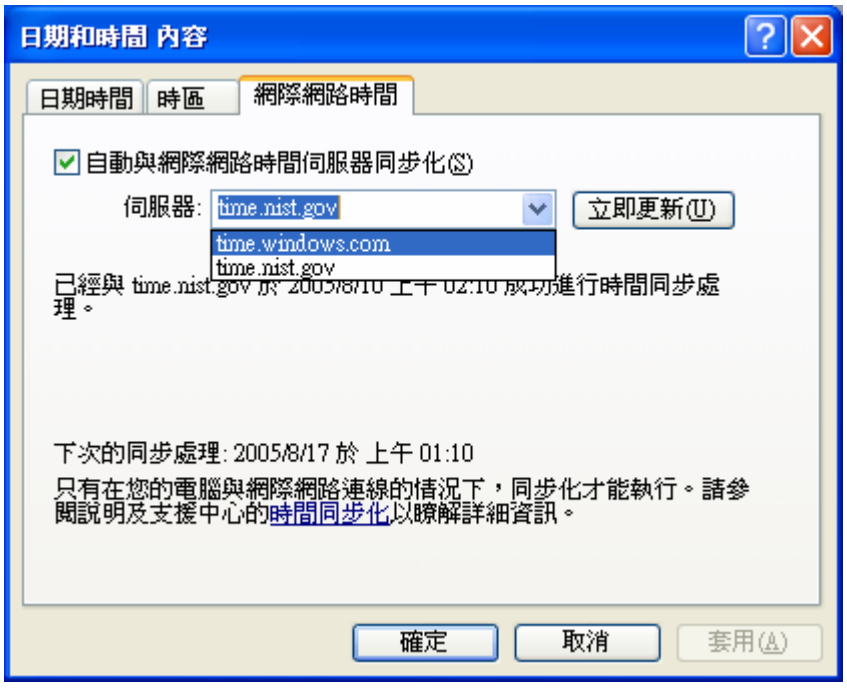
NTP 是由美國德拉瓦大學的 D.L.Mills 教授於 1985 年提出，可以量測封包在網路上來回往返的時間延遲和估算電腦時鐘偏差，達到在網路上實現高精準度電腦校時的目的。NTP 伺服器以階層式架構形成時間追溯體系。位於階層最頂層的伺服器直接追溯到國家標準時間，階層 2 伺服器則透過階層 1 伺服器間接追溯到國家標準時間。每台伺服器均以本身的時鐘來維持某精準度的時間，並自行於適當校時週期主動向上一階層伺服器發出校時請求。



NTP 可提供電腦間時間誤差在幾個 ms (百分之一秒)內，所以這對於標準時間的發佈及電腦時間準確性有很大的助益。

關於NTP校時，網路上有很多軟體可以讓你的電腦隨時同步標準時間，例如:
http://www.symmttm.com/software_download.asp?ID=download_symmtime.asp,
台灣地區國家時間與頻率標準實驗室也提供網路校時軟體:
http://www.stdtime.gov.tw/chinese/home.htm

在 Windows 裡也有一個 NTP 自動校時的功能，請按下螢幕右下角,「調整時間與日期」功能，選擇「網際網路時間」之頁，如下圖，



你可以在伺服器右方欄位內選擇或輸入你希望與之對時的 NTP 伺服器網址，按下右邊「立即更新」，你的電腦時間就會與網際網路上這台伺服器時間同步。

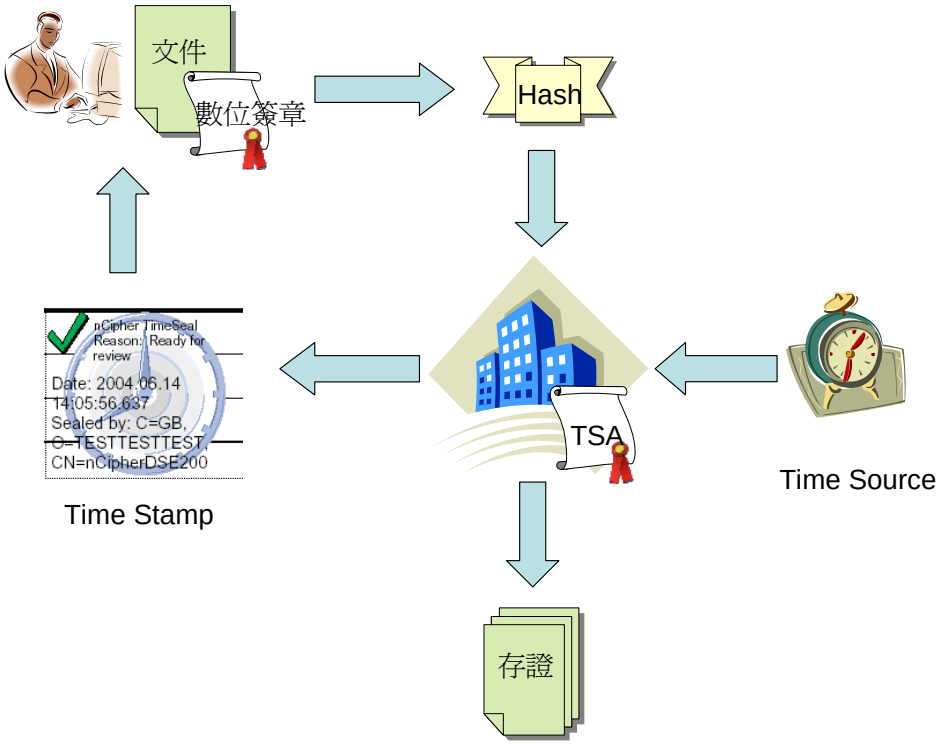
讓我們再回到電子交易的環境來，我們已經知道 PKI 機制能夠讓雙方確認身份、保護資料內容隱私及不被竄改，當然還有不可否認的功能；假設雙方電腦的時間也經由 NTP 與上層標準時間校時過，是否這樣就足以讓雙方相信對方的時間呢? 我怎麼相信你說你寄出這份文件的時間? 你會相信我說我是一個小時後才真的收到嗎 ？ 有沒有可能你 NTP 校時錯誤(誤上賊船，連到假的 NTP Server)？有人能幫你證明你確實在幾點幾分到正確的標準時間源校時嗎? 有沒有可能有人在兩次校時之間改了你的電腦時間 ？.....

顯然 NTP 無法去除時間安全性的問題，我們需要有一個公正的第三者來證明這個時間的正確性與安全性，就正如 PKI 裡公正的機構(Certificate Authority, CA)來給你發一個身份證明(Certificate，憑證)，你用這個憑證來證明你的身份,來保護你的資料。對方因爲相信這個公正的機構，所以相信這個憑證，也相信你的身份與資料。而電子時戳(Time-Stamp)就是一份由公正第三者發出來爲電子文件或交易做的時間證明，而這公正第三者我們稱爲 TSA (Time-Stamping Authority)。對方因爲相信這個 TSA 的公正性與其時間的正確性，所以相信你這份文件或交易的時間。

時戳可以爲任何電子文件或網路交易提供準確的時間證明，並且驗出文件或交易的內容自蓋上時戳後是否曾被人修改過。電子時戳就如一個值得信賴的第三者或

公證人，爲你提供可靠的時間確認和核實服務。所有電子數據或資料，不論是什麼樣的格式或內容，都可以蓋上電子時戳。這個可靠的時間核證服務可應用於網路交易、電子郵件、加密訊息、保障知識產權和其他需要準確時間證明的事務。

時戳的技術如同 PKI 一樣用到密碼學、公鑰、私鑰、簽章等技術，比較不同的是時戳需要一個正確的時間來源, 所以 TSA 的時間必須要正確、安全才能保障時戳的被信任。



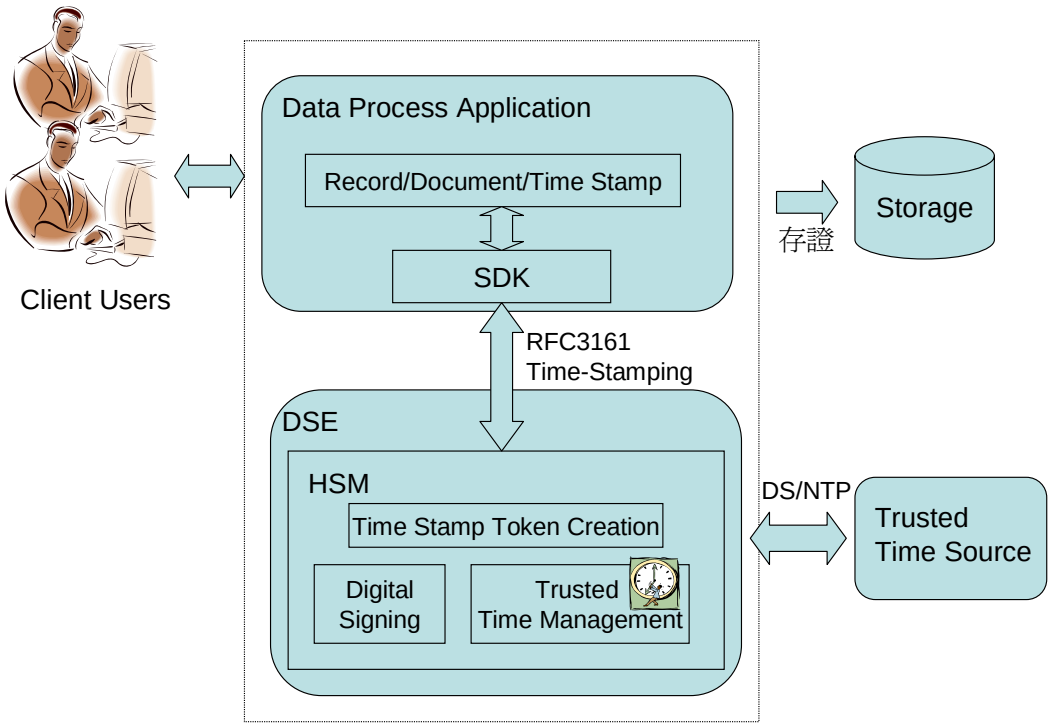
上圖中, 電子文件主人將其文件與簽章, 產生 Hash Value 送到 TSA, TSA 產生時戳交回給文件主人, 並存證記錄。同樣的, 想要驗證這份文件的時戳, 也可將文件與時戳送到 TSA 連驗證是否無誤。這整個過程十分簡單清楚。但這裡面最重要關鍵點就是 TSA 的時間來源(Time Source)，這就牽涉到標準時間來源的問題了。標準時間是以全球各國時間實驗室(大約 50 個, 台灣是中央標準局委託中華電信研究所)所提供的時間分別乘以不同的加權比重後的平均值做爲標準時間, 而各國的時間實驗室的標準時間源則爲高精準的原子鐘。到這裡, 我們可以認定這些標準時間源是可以當成大家信賴的 Time Source。

讓我們回到 NTP 來, TSA 的時間來源可能經由 NTP 往上層 Server 取得標準時間, 這過程中就有安全性的考量, 例如如何確保「Time Source」是真的 ? 如何避免 DNS Spoofing (僞冒網址) ? 稽核與事後追蹤如何做 ? 當交易雙方對時間有爭執時, TSA 能拿出夠公信力的證明嗎 ? 其實 TSA 透過網路 NTP 與 Time Source 的連線就向我們的電腦流覽器(Browser)與網站伺服器(Web)連線一樣, 如何確認雙

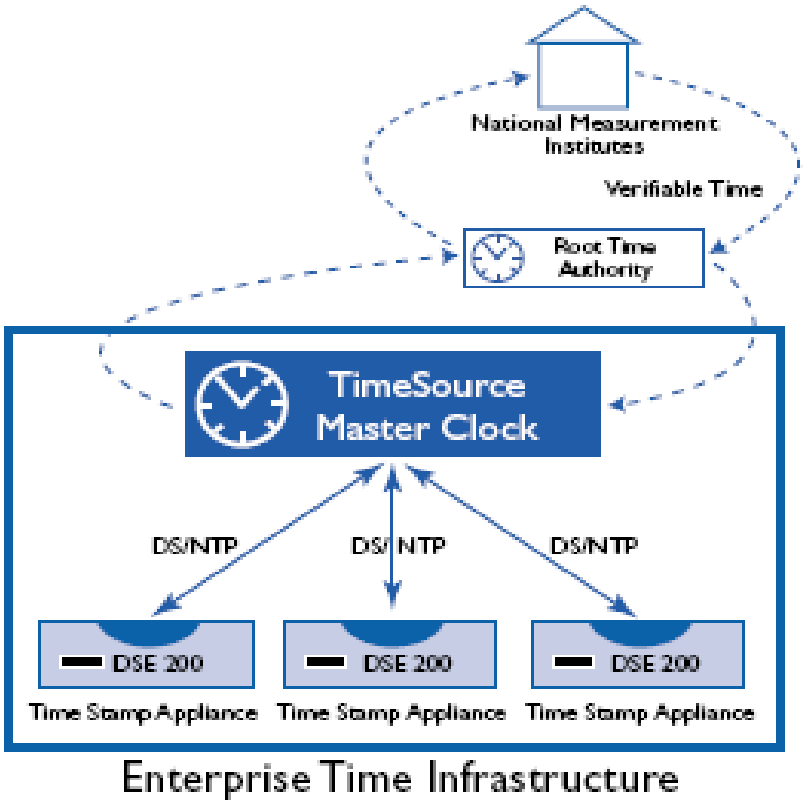
方身份 ? 所以 TSA 與 Time Source 的連線(上下階層的 TSA)需要比 NTP 更爲安全的連線方式。國外已有先進廠商提出 DS/NTP 的 Protocol 了, DS/NTP 基本上是結合 NTP 與 TLS (Transport Layer Security, SSL 的接班人)的概念, 在網路上增加互相辨識真僞(Authenticate), 提供時間的稽核與追蹤 (Time Auditing and Tracking)的功能。在 DS/NTP 環境下, 你不用擔心 TSA 的時間來源會有問題, 交易雙方有爭執時, TSA 可以提供必要的證據。

好了, 我們已經說明了標準時間 TimeSource 是沒有問題的, 也簡單提出使用較安全的 DS/NTP 通道來確保 TSA 的時間來源是可靠的。但是,，TSA 本身如何證明它是安全與準確無虞的 ? 如前所述, TSA 的目的是提供時戳, 簡單來說, Input 是需求者的押時戳的文件或其 Hash Value, 當然拉, 還有 TSA 的時間, Output 則是一份電子時戳, 這過程就是一些複雜的數學公式、運算與規定, 這些規定與標準就定在 RFC 3161 裡, 有興趣的讀者可以在網路上找到相關資料。無論這些運算多複雜, 電腦都可以解決, 於是你會想到, TSA 就是一台伺服器, 它接受網路上的 Request, 以 DS/NTP 或 NTP 與上一層的 TSA 或 TimeSource 取得或校正標準時間, 再加上一些執行 FRC3161 的程式碼, 當然還得要有憑證 (Certificate), 不就是一台「時戳伺服器」嗎 ? 沒錯, 但是沒有人會相信這台「時戳伺服器」的, 因爲, 可能有人會在兩次校時之間去變更電腦時間, 而且所有產生時戳的運算過程全部在電腦記憶體裡, 稍懂程式設計的人都知道你的金鑰(Key)曝光了，還有更多留後門的可能。

所以, TSA 的建置絕對馬虎不得, 應該要將上述過程全部在獨立的硬體及晶片裡全部做完, 沒有人可以任意更動時間, 金鑰不容許曝光, 絕無留後門的可能。它就是一個黑盒子, 它接受你的 Input (要產生時戳的內容或驗證時戳), 它就回給你要的東西, 過程中沒有人可以偷窺、篡改，並且都有記錄可查與追蹤。我們姑且稱這黑盒子爲 Document Sealing Engine (DSE)。以下是 DSE 的示意圖



到此，我們已經完整的走過甚麼是標準時間來源，爲甚麼需要 NTP 來同步時間，NTP 仍需要更進一步的安全與稽核機制，到如何建置時戳伺服器，每一個環結都要確保安全無慮。TSA 提供的時戳服務基本上是要收費的，對於有大量電子交易或電子文件需要時戳證明的企業，是否可以自行建立 TSA？，當然可能，只要其 TSA 俱有「公信力」即可，企業對外的電子文件或交易都可以在自家的 TSA 押上時戳，對方可以驗證其真僞。企業也可用這台 TSA 做爲其內部公文、電子郵件的時間依據。 企業建置 TSA 如下圖。



最後談到時戳的應用範圍，舉凡需要時間證明的電子文件或交易行爲都需要時戳，下面是一些隨手舉來的例子:

- 電子商務
- 保護智慧財產權
- 股票買賣
- 電子投標／報價／拍賣
- 簽署合約／文件
- 結束會計賬目
- 電子病歷
- 訂立遺囑

電子化的虛擬世界裡，人與人之間缺乏面對面的互動與互信，更需要完整的安全基礎與環境，時戳是安全環境裡很重要的一環，本文儘量避開了艱深的技術名詞，試圖以淺顯易懂的方式介紹了時戳的意義與應用、建置安全與受信賴的時戳伺服環境時應考量的事項，希望對讀者们有些許的幫助。