Time Stamp Server

全球首創硬體電子時戳伺服器

實體世界裡有「郵戳為憑」來證明信件的時間，在網路世界裡如何來證明電子文件或交易的時間? 「時戳」可以為任何電子文件或電子交易提供準確的時間證明，並且驗證其內容自蓋上時戳後是否曾被人修改過。nCipher領先全球的時戳服務設備可以快速的為大至整個政府，小至企業部門建置安全與可信任的時戳服務中心。

時間的重要性

使用標準與可信任的時間是現今商業系統與流程正確性的基本，在一個愈趨緊密連接的世界裡，網路系統與工具必須使用共同與準確的時間以保運作順暢，電腦時間的差異可能造成交易記錄順序的混亂，甚至造成金錢方面的爭執或損失。

網路上的時間問題

每一台電腦設備的時間可能都不同, 到底以誰的時間為準? 雖然有NTP (Network Time Protocol)可做網路校時, 可是在駭客肆虐的網路上如何保證時間來源安全無疑, 又如何避免電腦時間被任意變更 ?

時戳的重要性

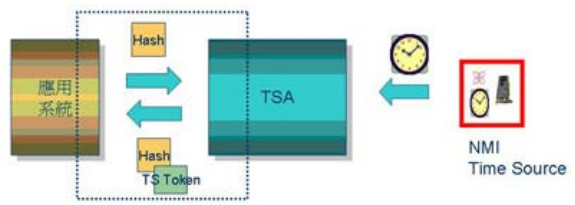
越來越多的法律與規範要求電子資料與文件必須有時間證明，稽核的要求也凸顯了驗證資料完整性的重要。時戳已成為公鑰基礎建設(PKI)裡重要的一環，它提供不可否認性與確保未來一段長時間裡的資料正確性的驗證。「時戳」可以連結時間與數位簽章，可以用來鑑識資料的完整性、驗證簽章，即使其簽章憑證已失效，仍可長期確保文件正效性的驗證。以上都須依靠建立下述的信任時間基礎上：

- 準確的時間：時鐘須維持精確的時間值
- 標準時間源：時間值能與國際認可的「中原標準時間」同步/對時
- 時間的完整性：時間不能被竄改或操縱
- 時間的驗證：可追溯至信任的時間源

時戳服務機構(TSA)

時戳服務機構(Time Stamp Authority, TSA)扮演一個可信任的第三者來提供資料在某一特定時間前即已存在的證據, TSA通常需要建置一個安全的, 可被信任的時戳伺服器(Time Stamp Server), TSA面臨的問題：

- 如何安全地取得標準時間源
- 如何確保時間不被篡改
- 如何保證「押時戳」的過程是安全的
- 如何提供高效能與可稽核的時戳服務



最佳方案

用軟體來實現時戳服務是充滿了安全的漏洞, 例如人為的更改系統時間、金鑰保護與運算過程都暴露在風險中，這樣的TSA是無法俱備公信力與法律基礎的。最佳方案應該是：

- 增強NTP的安全性，消除時間傳遞過程中的風險，並增加時間的稽核與追蹤功能
- 公正機構為其傳遞的時間「掛保證」，以夠正確與安全的設備做為TSA的時間源
- 時戳伺服器以FIPS認證過的HSM來實現
- 時間都放在HSM裡, 無法任意修改

nCIPHER™

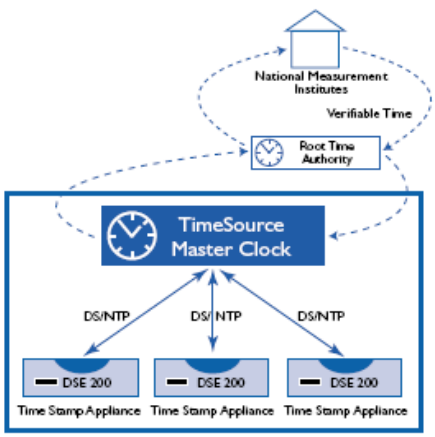
Time Stamp Solution by nCipher

nCipher以其領先全球的HSM(硬體加密模組)技術與產品,率先推出完整的時戳服務解決方案,以DS/NTP取代NTP,以TSMC做為時間源與傳遞設備,確保標準時間來源的正確性與可追溯性,以DSE做為時戳伺服器,提供快速與安全的文件簽章與時戳服務

TSMC(TimeSource Master Clock)保證時間的準確性與完整性

由於電腦時間容易竄改,且時間在網路傳輸上的易被破壞與偽裝,標準的NTP協定不夠安全。所以在實務運作上需要一個安全與可驗明正身的管道來傳遞正確的標準時間。TSMC 使用下列機制來確保時間值的完整性:

- 內含精密的銣原子鐘,可確保時間的精確度。
- 使用安全的傳遞管道--DS/NTP,整合互相認證與資料加密,與DSE及外部標準時間單位建立安全的連線,認證與加密金鑰是被安全地儲存在FIPS-2 Level 3 認證過的硬體加密器(HSM)裡,確保時間值傳遞過程安全無虞。
- 使用自動校時與稽核的機制。TSMC處理校時需求後會傳送一個簽署過的時間憑證到需求端, 以證明時間來源。此過程使用之金鑰也被保護在HSM裡。
- 階層式連接多個TMC及DSE,透過DS/NTP稽核下一層TMC或 DSE的時間



Enterprise Time Infrastructure

DSE (Document Sealing Engine)專為數位簽章與電子時戳而設計的設備

DSE是一個能夠為文件簽證與押時戳的網路設備,能夠為代表某一人、部門、組織、甚至代表整個公司的文件做電子簽證與稽核。

透過DSE 的整合工具,你的組織可以很容易的將DSE 與您的既有應用系統整合,完成整個組織層面的電子文件的簽證、封印與押時戳。

DSE 提供需要高安全性與不可否認性的文件追蹤、儲存、傳遞功能的企業一個快速導入的解決方案

DSE系統功能

- ✓ 電子簽章與時戳設備
- ✓ 自動校時
- ✓ 實行IETF所定之PKIX時戳標準規格
- ✓ 每秒可執行150個時戳需求
- ✓ 簽章與時戳執行在FIPS認證過的HSM裡
- ✓ 1U, Rack-mounted網路設備
- ✓ 相容 VeriSign 時戳憑證
- ✓ 安全的瀏覽器與Web伺服器連線管理介面
- ✓ 開發工具支援ANSI C, MS VC++, Java
- ✓ 自動錯誤通知

ASIAPEAK 玉山科技
tel:(02)77128295
http://www.asiapeak.com
e-mail:services@asiapeak.com