

DIGITAL SIGNING & TIME STAMPING APPLIANCE

nCipher 的 Document Sealing Engine (DSE 200) 是一個專為數位簽章與電子時戳而設計的設備, DSE200 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

為文件封印 (Cryptographically Sealing a Document)

手寫的實體文件很容易判別是否更改過, 但是電子文件卻很難判斷是否篡改過, 所以電子文件易於受人操縱, 從法律觀點來看, 這就是「可疑的有效性」。在現今電子商業環境裡, 如何保護智慧財產、如何保存商業往來紀錄、如何採用業界標準與最佳實務、更多時候還要符合各種法律規範要求, 企業或組織必須在有限的資訊預算裡, 尋求同時能滿足安全與法規要求的電子文件與數位內容保存的解決方案。

解決方案

nCipher 的 Document Sealing Engine (DSE 200) 是一個能夠為文件簽證與押時戳的網路設備, DSE 200 能夠為代表某人、部門、組織、甚至代表整個公司的文件做電子簽證與稽核。大部份法規機構並不要求交付個人的數位簽章, 而是接受代表組織的數位簽章, DSE 200 最能表現這種容易實現的解決方案。

透過 DSE 200 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。



數位簽章

DSE 200 數位簽章是使用數位憑證與公開金鑰方法連結文件產生的, 這些數位憑證不只能夠鑑定簽名該文件的組織, 而且能夠為該簽名蓋上時戳, 這種結合數位簽章與時戳的用法就能確保信任的數位資料來源, 也能永久維持其證據的價值, 即使其原始數位憑證已過時失效。

碰觸過的一看即知 (Temper Evident)

即使只修改實體文件的一個字也會留下劃線或塗改的證據, 但電子文件整段文字被重新改寫過則很難知道, 所以若要使文件及其簽署具有可被信任性, 凍結該文件內容是基本要求。

DSE 200 產生亂碼過的湊雜值(hash) – 或謂數位指紋, 來代表該文件內容的唯一性, 該文件任何內容的變更, 都會造成驗證該簽章時的失敗, 換言之, 內容的任何微小改變都可判斷出來。

安全的時戳

DSE 能與提供校時及稽核服務的設備共同運作，這些服務提供者以安全的連線方式取得官方UTC(Coordinated Universal Time)的時間源，經由確認過的安全網路連線校時後，DSE就可提供時戳服務給任何需要PKIX相容時戳需求者。

FIPS 140-2 認證

金鑰是任何加解密與密碼運算的根本，但如果是在軟體環境下運作，則會變得脆弱與易招致攻擊，為了抵抗任何可能的攻擊，包括物理上的破壞，DSE 內部使用硬體加密模組(HSM)，HSM保護內部時間源以及儲存與管理簽章與封印用途的金鑰，簽章過程及加解密運算都在此HSM內部執行，這樣的保護等級讓人深具信心。

DSE的HSM已取得FIPS 140-2 Level 3 的認證

技術規格

前面板

連接界面:

- 2 * ethernet port
- Serial Port for communications
- VGA connector for VDU
- 2* USB ports

LED 燈號:

- 電源
- 硬碟
- Ethernet

後面板

- 電源開關

整合工具

DSE SDK/API 開發工具包括一群程序呼叫與範例程式碼，可以協助既有或新開發的應用系統快速整合與應用這個文件簽章與時戳功能，開發工具支援Unix 與Windows 平台，提供C語言程式庫與Java 語言類別 (Class)。

系統特色

- 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125個時戳需求 (1024 RSA key)
- 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

- 尺寸: 1U (1.75") x 17"寬x 18" 深
- 網路: 兩個 10/100 Base-Tx Ethernet
- Serial Port: DB-9
- Video Port: 15 pin VGA
- 兩的 USB 1.1 ports
- 輸入電壓: 100-240 伏 AC 自動切換, 50-60Hz (nominal) 最大電源消耗: 240 瓦 (2.1 amps at 110 volts AC)
- Mounting Systems: 19" rack mount
- 溫度/溼度: +10 to +35 °C, 10 to 85%
- 噪音: <50dB
- 標準認證:
FCC: CFR47, Part 15, Subpart B, Class A
CE: EN55022, Class A; EN55024-1; EN60950
FIPS 140-2 Level 3 certification

