nCIPHER™

Time Stamp Solution

玉山科技股份有限公司

http://www.asiapeak.com
fred@asiapeak.com
+886-2-77128295#11

APTECH

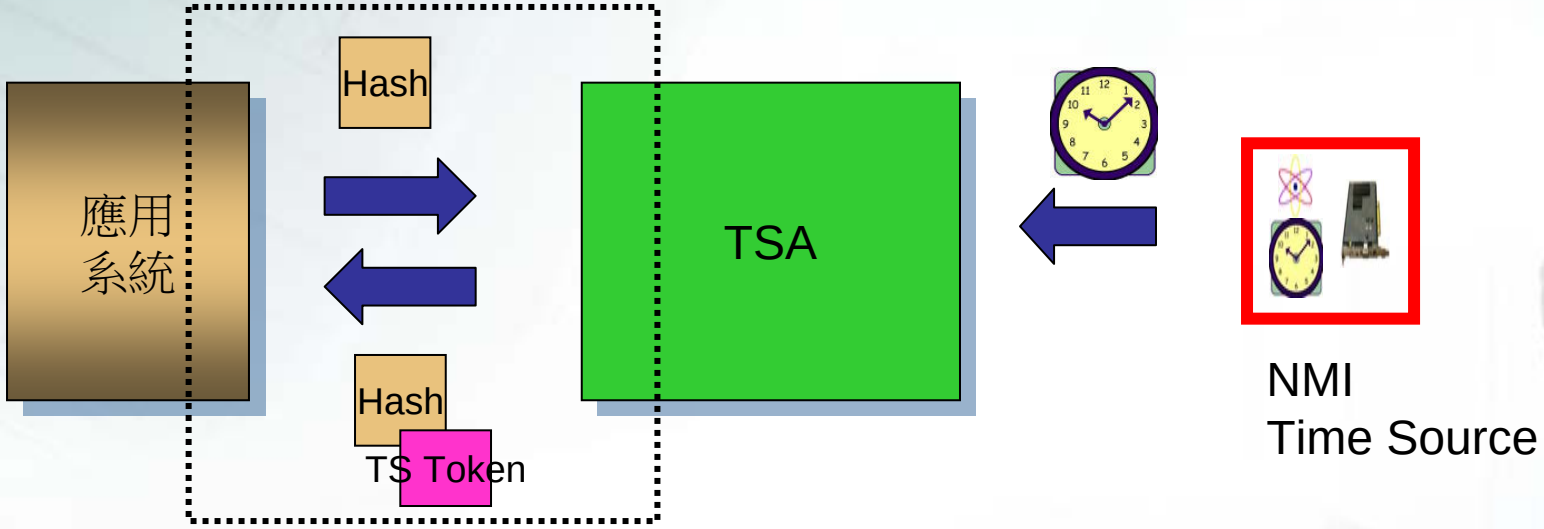
Agenda

- 時戳服務架構與安全考量
- nCipher 的解決方案
- 時戳服務時間源(TimeSource Master Clock)
- 時戳伺服器 (TSS, DSE200)
- nCipher TSS SDK

Requirements of the TSA

- to use a trustworthy source of time.
- to include a trustworthy time value for each time-stamp token.
- to include a unique integer for each newly generated time-stamp token.
- to produce a time-stamp token upon receiving a valid request from the requester, when it is possible.
- to include within each time-stamp token an identifier to uniquely indicate the security policy under which the token was created.
- to only time-stamp a hash representation of the datum
- to examine the OID of the one-way collision resistant hash-function and to verify that the hash value length is consistent with the hash algorithm.
- not to examine the imprint being time-stamped in any way
- not to include any identification of the requesting entity in the time-stamp tokens.
- to sign each time-stamp token using a key generated exclusively for this purpose and have this property of the key indicated on the corresponding certificate.
- to include additional information in the time-stamp token, if asked by the requester using the extensions field, only for the extensions that are supported by the TSA. If this is not possible, the TSA SHALL respond with an error message.

時戳服務的架構



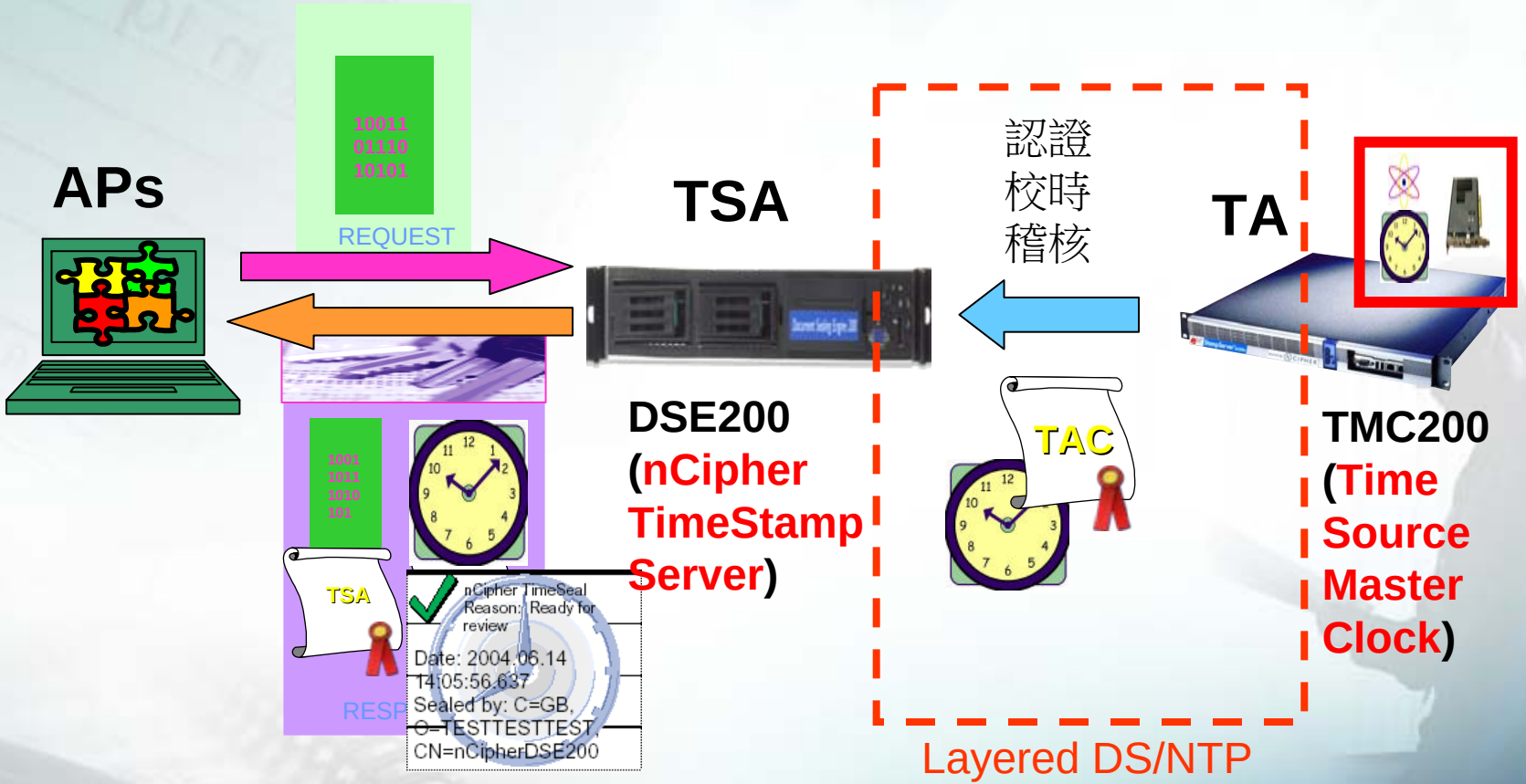
- Follow RFC3161?

●TimeStamping
安全與效能？

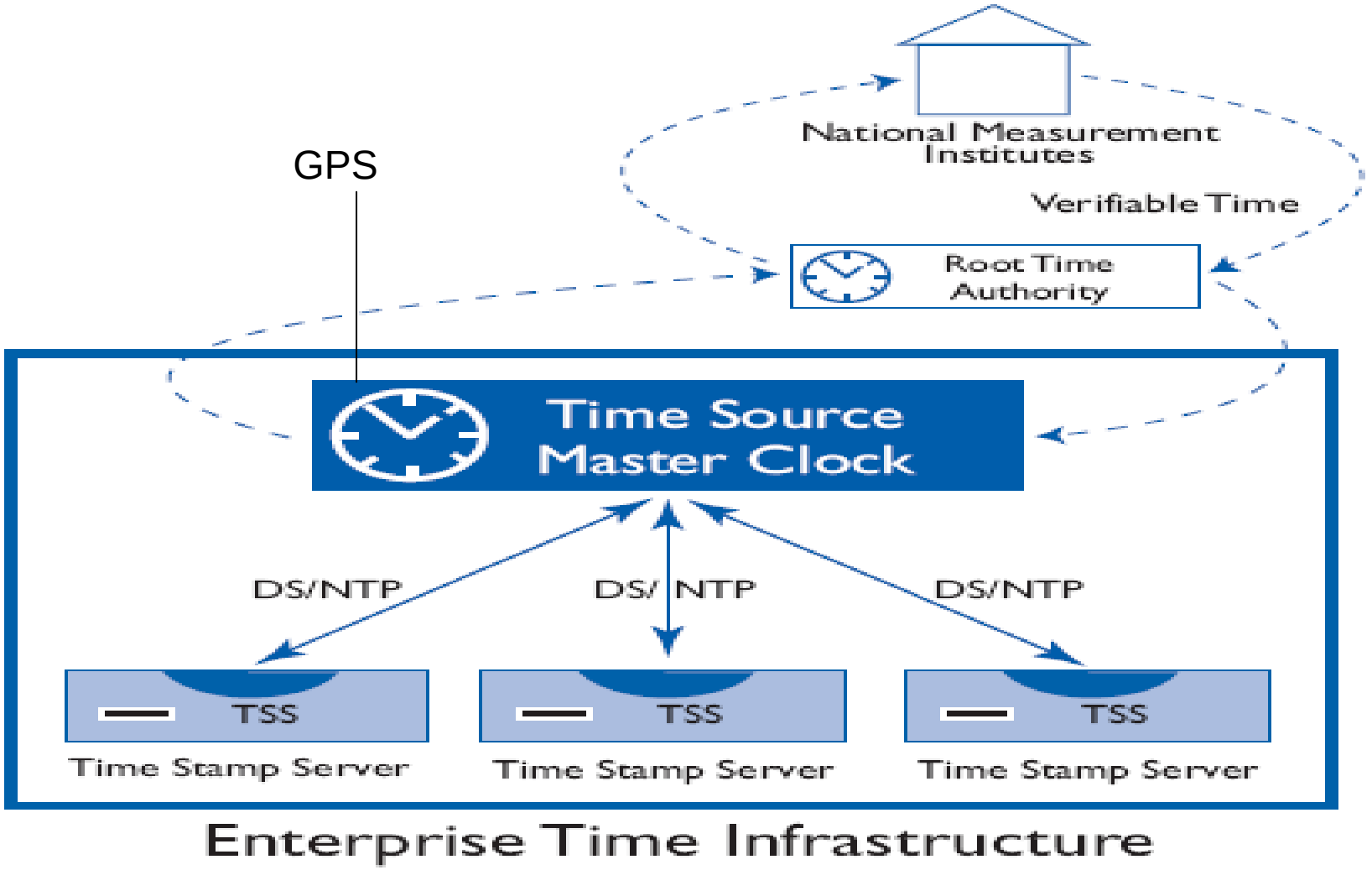
●標準時間源問題?
●安全的時間同步?

Auditable ?

nCipher Solution



Enterprise Time Infrastructure



Enterprise Time Infrastructure

nCipher TSMC

nCipher Time Source Master Clock

TimeSource Master Clock(TSMC)

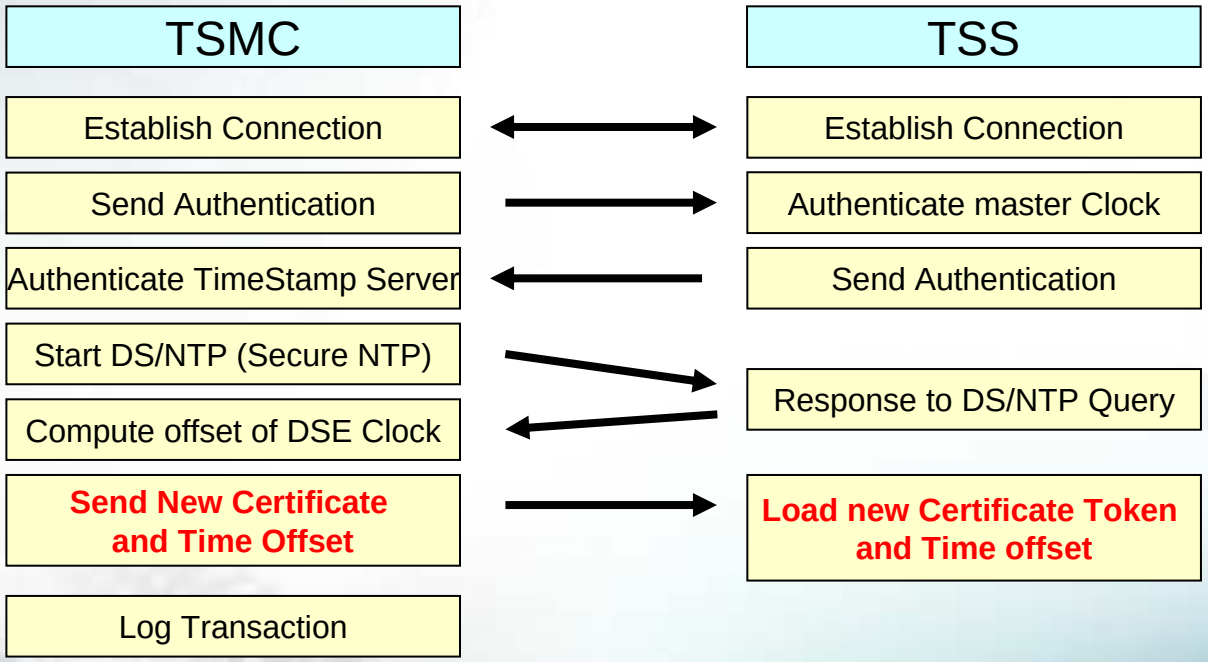
- 內部使用crystal oscillator clock (或銣原子鐘)維持精確時間
- 可接不同時間來源設備
  - ✓GPS; 1PPS; IRIG-B; NTP;DS/NTP
- 可做獨立時間源，提供NTP校時
- 內含HSM(保護金鑰及實行DS/NTP)
- 透過DS/NTP稽核下一層(TSMC或TSS的時間)
- 階層式連接多個TSMC及TSS
- Web-based 管理介面

TSMC

- **Time Accuracy**
  - ✓ Network: 1-10 milliseconds, typical
  - ✓ GPS and 1PPS: ± 100 nanoseconds
  - ✓ IRIG: ± 10 microseconds
  - ✓ OCXO-DHQ oscillator (TSMC-GPS units):
    - Short term stability (T = 1 sec): $2 \cdot 10^{-12}$
    - Accuracy of time free run, one year: ± 300 milliseconds
  - ✓ OCXO-HQ oscillator (TSMC-IRIG units):
    - ✓ Short term stability (T = 1 sec): $5 \cdot 10^{-12}$
    - ✓ Accuracy of time free run, one year: ± 1.6 seconds

DS/NTP Time Auditing and Tracking

DS/NTP is a mutually authenticated protocol based on TLS and NTP.



How the TSMC Works

- After being calibrated and audited by an NMI's upper clock, the TSMC can audit lower clocks further down the time distribution hierarchy.
- When this measurement and calibration process is complete, the TSMC can issue a Time Attribute Certificate (TAC), which attests to the calibration data and source of time, over DS/NTP to a lower clock.
- The TSMC is capable of maintaining time internally to a high degree of accuracy with a low degree of drift using an internal Rubidium oscillator. This allows the TSMC to free-run between audits.

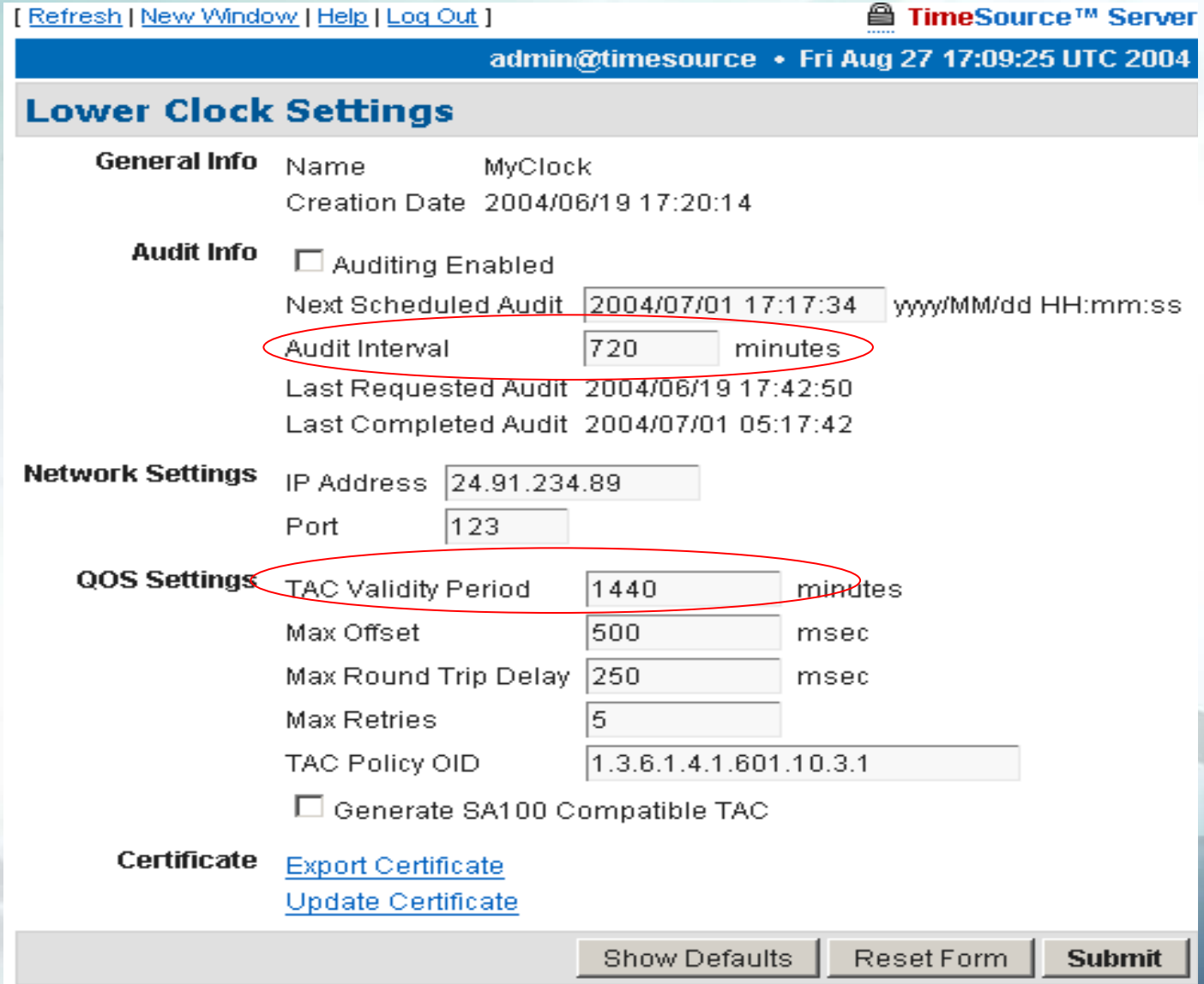
TSMC Signature

- The TimeSource Master Clock uses certificates, issued by public CA to authenticate between master clocks and subordinate devices and to authenticate audit records.

nCipher HSM inside

- All cryptographic functions, including processing, time stamping, and clock operations are performed within the secure confines of the nShield module. The nCipher nShield module meets internationally recognized FIPS 140-1 level 3 standards. The nShield's FIPS validation helps deliver confidence that the nShield protects the security of your private keys and software code.

Audit Lower Clocks



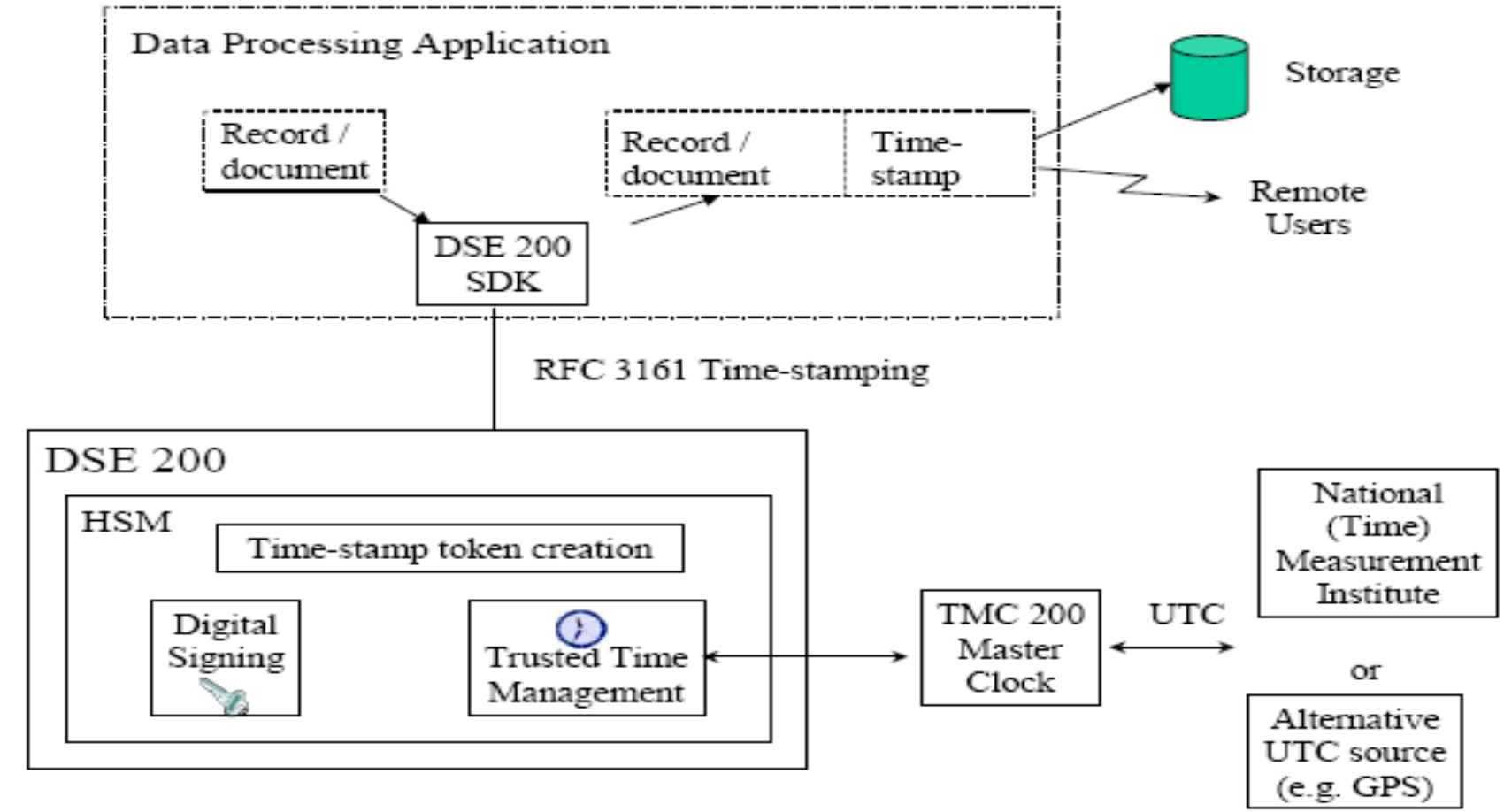
Time Stamp Serve(TSS)

- DSE200 (Document Sealing Engine)
- 內含HSM
  - ✓ RFC 3161 implementation + Clock
  - ✓ DS/NTP implementation
  - ✓ Key Protection
- 時戳使用HSM內部Clock時間, 無法人為竄改
- 時間來源: DS/NTP, NTP → HSM Clock
- 每秒可處理150筆時戳簽章
- Web-based 管理介面

TSS Architecture

DSE 200 Architecture

The architecture of the DSE 200 is illustrated in the following diagram:



DSE200 功能

- 每秒可處理150個時戳需求
- 標準 1-U 大小的IP network Appliance
- 內含FIPS 140-2 Level 3的HSM, 時間(時鐘)被保護在HSM裡, 無法人為任意修改時間
- 實現IETF PKIX電子時戳標準規範(RFC-3161), 押時戳過程都在HSM裡進行
- 支援 NTP(Network Time Protocol, RFC-958)及加強安全的DS/NTP (無中間人破壞及偽造問題)
- 連接安全與可稽核的時間源(獨立In-house時間源或國家標準時間源)
- 自動對時機制,自動錯誤通知
- 安全的Web 管理介面
- 完整的Audit & Tracking 機制

Auditable Time Source

- Time is delivered from a Trusted Master Clock (TMC) at a Trust Authority (TA). A TA provides an evidentiary trail showing the origin of the time.
- The TA certifies the time on a locally-installed DSE200 that services time signing requests from an application or transaction server. The certifications occur at regularly scheduled intervals depending on the accuracy required.
- All exchanges between the TA and the DSE200 are digitally signed and logged, and all communications are via an authenticated, secure network connection.
- Once the TA completes the calibration and audit of the DSE200, it issues a signed Time Attribute Certificate (TAC) certificate to the DSE200 authorizing its operation.
- The TAC certifies the calibration and traceability of the DSE200 clock. The DSE200 is then ready to provide time via signed time signings.

Time-stamp protocol support

- RFC3161 Socket Base Protocol on TCP/318
- RFC3161 Time-stamp Protocol by HTTP at the following URL: http://*dse200-id*/TSS/HttpTspServer
- A WebService interface at the following URL: http://*dse200-id*/TSS/services/TimeStampService?wsdl

Signature

- The DSE200 uses certificates, issued by public certification authorities (CAs) to sign time stamps
- The time sign includes the time and document hash signed by the DSE200.
- The user gets this and the TAC. The time sign and the TAC gives all the necessary information to confirm that the time sign is accurate, valid, and traceable back to the Trusted Master Clock (e.g NIST)

nCipher HSM inside

- At the heart of the DSE200 is the nCipher HSM with SEE (Secure Execution Engine). All cryptographic functions, including processing, time stamping, and clock operations are performed within the secure confines of the nCipher HSM
- The DSE200 comes with nCipher code running in it, and it implements DS/NTP.

Multiple TSAs

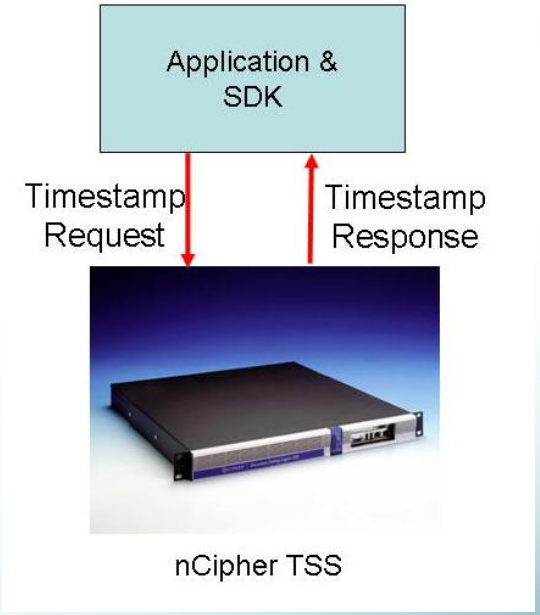
- DSE200 now supports the creation of multiple TSAs. You can create multiple TSAs for:
  - ✓ departments: each department in your organization might need a different TSA.
  - ✓ customers: if you are a service provider, you might want to operate a DSE200 for several customers. In such cases, you can create a separate TSA for each customer so that the TSA certificate name is related to the customer.
  - ✓ policies: you might need different TSAs for different policies within your organization. For example, you might have policies that require different types of signatures (DSA or RSA) or different key sizes (1024-bit or 2048-bit).

How multiple TSAs work

- The DSE200 uses Policy Object Identifiers (OIDs) and hash algorithms to determine which TSA should be used to issue the time-stamp.
- When you create multiple TSAs, you can assign one of them as the default TSA. You can configure each TSA to support a specific policy OID and a list of hash algorithms. When a client requests a time-stamp, the DSE200 checks the policy OID and the hash algorithm on the request and:
  - If the request does not include an OID, it is sent to the default TSA or the first TSA that supports the hash algorithm.
  - If the request includes an OID, it is sent to the first TSA that supports the OID and the hash algorithm.
  - If the request includes an OID and none of the TSAs support the OID and the hashalgorithm, the DSE200 returns an error.
- A TSA on DSE200 must receive a DS/NTP audit before it can issue time-stamps.

TSS SDK

- 提供的一系列的functions (API)及範例程式協助程式開發人員快速的開發時戳應用系統或將時戳功能整合到既有應用系統裡



SDK API 功能

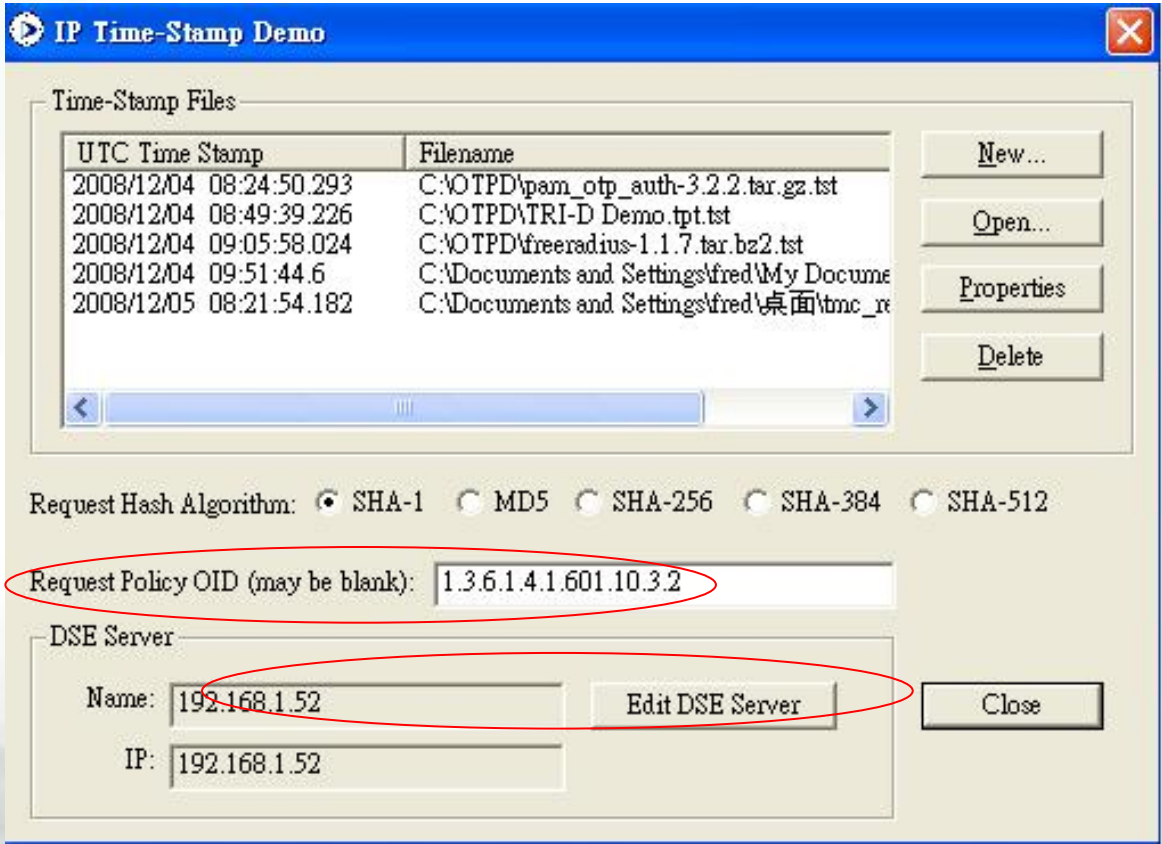
- Encoding and decoding time-stamp requests (時戳需求之編碼與解碼)
- Decoding time-stamp responses (時戳回應之解碼)
- Decoding time-stamp tokens (時戳解碼)
- Generating SHA-1/SHA-2 digests (雜湊值之產生)
- Verifying digital signatures of time-stamp tokens (時戳簽章之驗證)

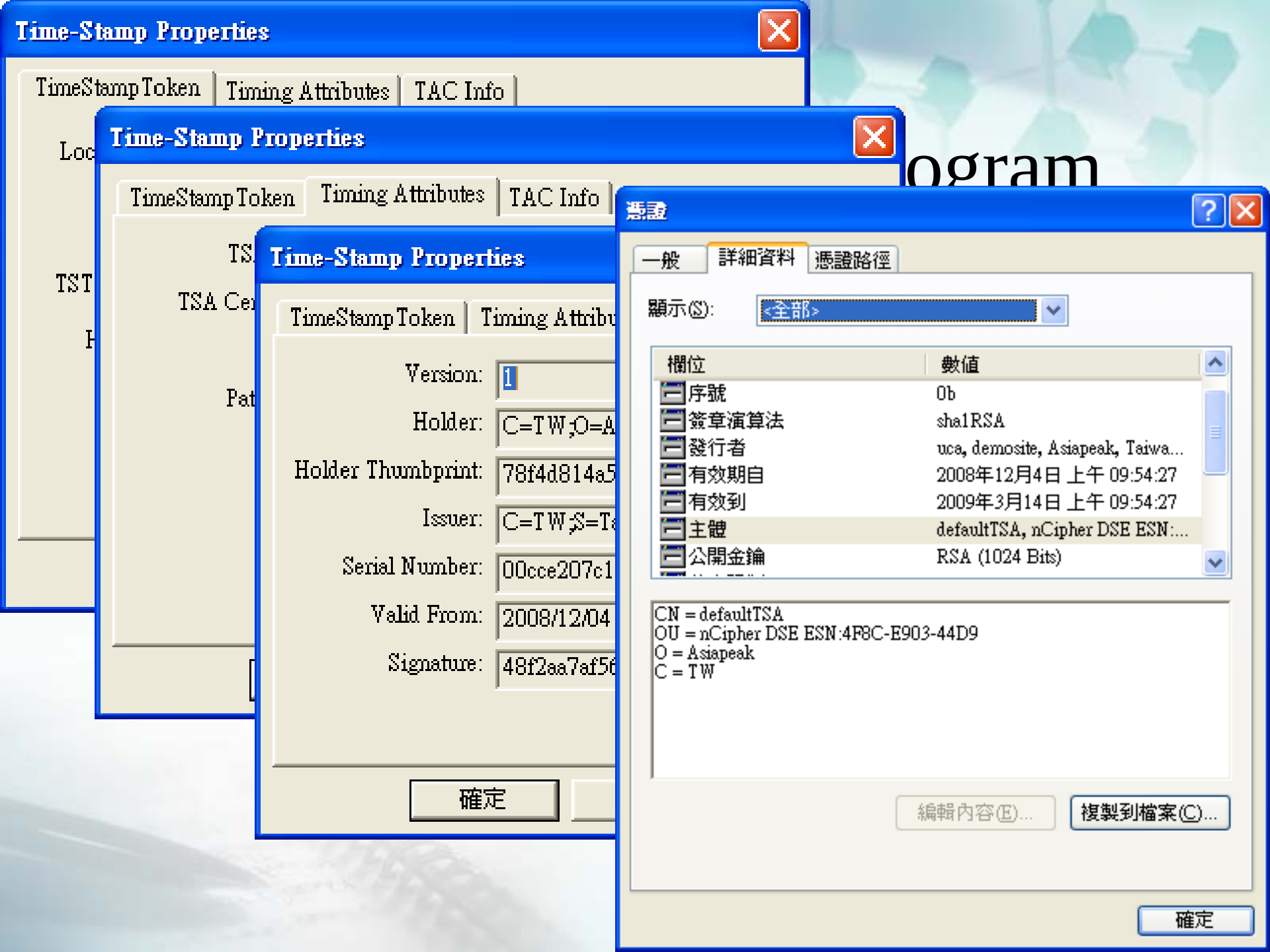
SDK API支援程式語言

- Java 類別(Class)
- C 語言程式庫 (Librairy)
  - ✓ Win32 DLL
  - ✓ Sun Solaris and Linux static libraries
  - ✓ 可再由程式人員加值支援ActiveX 與 COM 介面

Sample Code & Test Program

- C:\nfast\c\dsesdk
- Iptsdemo.exe




Time-Stamp Properties
TimeStamp Token
Timing Attributes
TAC Info
Time-Stamp Properties
TimeStamp Token
Timing Attributes
TAC Info
Time-Stamp Properties
TimeStamp Token
Version:
1
Holder:
Holder Thumbprint:
Issuer:
Serial Number:
Valid From:
2008/12/04
Signature:
確定
憑證
一般
詳細資料
憑證路徑
顯示(S):
<全部>
欄位
數值
序號
0b
簽章演算法
sha1RSA
發行者
uca, demosite, Asiapeak, Taiwa...
有效期自
2008年12月4日 上午 09:54:27
有效到
2009年3月14日 上午 09:54:27
主體
defaultTSA, nCipher DSE ESN:...
公開金鑰
RSA (1024 Bits)
CN = defaultTSA
OU = nCipher DSE ESN:4F8C-E903-44D9
O = Asiapeak
C = TW
編輯內容(E)...
複製到檔案(C)...
確定

問題討論