

THALES  CIPHER™

- Offre da più di 40 anni soluzioni in settori critici come quello governativo, finanziario e della difesa.
- Specializzata in molti ambiti tra cui quelli dei servizi di sicurezza informatica e della crittografia.
- Acquista nel 2008 nCipher, che diventa una delle linee produttive di cui le soluzioni che seguono fanno parte.

Accelerazione crittografica

- Accelerazione SSL per i server Web
- Alleggerisce il carico della CPU nelle operazioni crittografiche

Protezione delle chiavi

- Dispositivi HSM *tamper proof/tamper resistant*
- Gestione delle chiavi crittografiche

Marca temporale (timestamping)

- Dimostra che un documento è stato firmato ad una particolare data e ora.
- Tiene traccia del fattore tempo

Backup sicuri

- Permette di cifrare e quindi proteggere gli archivi di backup consentendo di definire elaborate policy d'accesso ai dati.

Protezione del codice eseguibile

- Le applicazioni esterne possono comunque essere attaccate
- Vi sono porzioni critiche del codice che devono essere protette

Professional services

- Consulenze specialistiche per la programmazione e il deployment dei dispositivi in contesti complessi che richiedono la personalizzazione degli applicativi.



nShield Solo (scheda PCI)

- Protegge le chiavi
- Accelera le operazioni crittografiche
- Attraverso l'uso di smart-card consente l'accesso selettivo alle chiavi da parte dei vari utenti o applicazioni a seconda delle autorizzazioni assegnate loro.
- Offre servizi crittografici a tutte le applicazioni installate sull'host locale.



nShield Connect (appliance di rete)

Offre le stesse funzionalità delle schede nShield Solo, ma essendo un dispositivo di rete, può servire fino ad un massimo di 100 client contemporaneamente.

Permette quindi di risparmiare sui costi quando le macchine che necessitano di questi servizi sono più di una.

E' inoltre possibile installare hardware aggiuntivo (nToken) sui client per aumentare la sicurezza della rete locale.

Il concetto fondamentale è che:

le chiavi crittografiche non lasciano mai l'HSM

Tutta l'elettronica necessaria per eseguire i calcoli è integrata nel dispositivo.

Solo i risultati delle operazioni crittografiche vengono forniti all'esterno alle applicazioni.

Questo trasforma la sicurezza logica (proteggere un file) in sicurezza fisica (proteggere un oggetto) che è molto più semplice ad mettere in pratica, soprattutto perché l'oggetto non può essere duplicato abusivamente.

E' possibile utilizzare più dispositivi nShield per realizzare schemi di *loadbalancing* e *failover*.

- **Loadbalancing**: il carico di lavoro può essere distribuito su più dispositivi in modo da ottenere una quantità di operazioni nell'unità di tempo maggiore di quella che potrebbe gestire il singolo.
- **Failover**: più dispositivi permettono l'alta affidabilità poiché se uno di questi si rompe, gli altri continuano comunque ad operare e questo evita di interrompere l'erogazione di un servizio.

Possibilità di eseguire codice personalizzato all'interno del dispositivo (**Secure Execution Engine**).

- Normalmente i dispositivi sono pilotati da programmi esterni che chiedono all'HSM di apporre firme o cifrare dati.
- Tali programmi sono tuttavia vulnerabili ad attacchi dall'esterno perché girano su host convenzionali (es. comuni PC).
- Il SEE permette di compilare e lanciare codice all'interno del dispositivo, in modo da impedire il reverse engineering dell'applicazione.

nShield Solo

- PCI standard, PCI-X, PCIe
- Modelli 500, 2000, 4000, 500e, 6000e
- Certificati Win2008 e Vista (dalla versione v11.10)
- Host: Windows, Linux, Solaris, HP-UX, AIX
- Certificati FIPS 140-2 Lev2 and Lev3. EAL 4+

nShield Connect

- 2x1Gigabit Ethernet
- Modelli 500, 1500 e 6000
- Porta (a seconda del modello) fino a 10/20/100 client con autenticazione forte
- Certificati Win2008 e Vista (dalla versione v11.10)
- Client: Windows, Linux, Solaris, HP-UX, AIX
- Certificati FIPS 140-2 Lev2 and Lev3. EAL 4+

Nota: il numero associato al modello identifica il numero massimo di firme RSA a 1024 bit che possono applicare al secondo.



nFast accelerator



SSL off-loader

- Vengono utilizzati per ridurre il carico della CPU (tipicamente sui server Web)
- nFast accelera le operazioni crittografiche come l'nShield ma non è progettato per proteggere le chiavi
- SSL off-loader opera a livello di stack TCP/IP ed è quindi trasparente all'applicativo (proxy SSL).
- Vengono impiegati in quegli scenari in cui le chiavi sull'host locale non sono in pericolo.

Timestamp master clock



Timestamp server



- Utilizzati per applicare una marca temporale ad un documento
- Non solo il documento viene firmato, ma viene anche certificata la data e l'ora di quando questa firma è stata applicata
- Sono importanti in tutte quelle situazioni in cui il prima o il dopo fanno la differenza (es. giochi a scommesse come il Lotto o il Totocalcio).



Payshield 9000

- Si tratta di un HSM che oltre a proteggere le chiavi carica a bordo un apposito programma, protetto dal Secure Execution Engine (SEE), per gestire le transazioni finanziarie.
- Viene tipicamente impiegato dalla banche e da chi gestisce le carte di credito per manipolare i PIN e abilitare le transazioni.

CryptoStor Tape



- E' un dispositivo che si inserisce nella catena SCSI o Fiber Channel su cui sta l'unità di backup.
- Funziona come proxy. L'applicativo sul client parla col CryptoStor e il CryptoStor con il dispositivo fisico di backup.
- Permette di fare backup cifrati in modo trasparente, così che l'eventuale compromissione dei nastri non pregiudichi la sicurezza dei dati.

Symbolic S.p.A.
Viale Mentana, 29
43121 Parma
T. 0521 708811
F. 0521 776190

www.symbolic.it
sales@symbolic.it