THALES

- 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 2009 nCipher, che diventa una delle linee produttive di cui le soluzioni che seguono fanno parte.

Campi di impiego dei prodotti 1/2

SYMBOLIC

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

Campi di impiego dei prodotti 2/2

SYMBOLIC

Backup sicuri

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

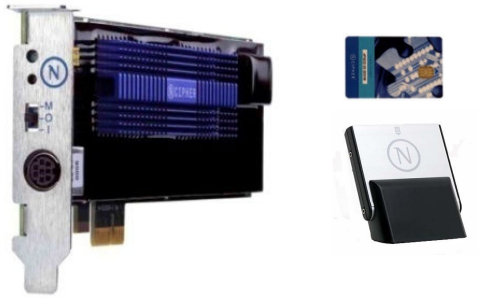
Protezione del codice eseguibile

- 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.

Dispositivi per uso generico 1/2



nShield Solo+
(scheda PCIe)

- 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.

Dispositivi per uso generico 2/2

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.

Perché acquistare un dispositivo nShield

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.

Ulteriori funzionalità dei dispositivi generici 1/2

SYMBOLIC

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.

Ulteriori funzionalità dei dispositivi generici 2/2

SYMBOLIC

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 Level 2 and Level 3, NIST SP 800-131A

nShield Connect+

- 2x1Gigabit Ethernet
- Modelli 500, 1500 e 6000
- Porta (a seconda del modello) fino a 10/20/100 client con autenticazione forte
- Client: Windows, Linux, Solaris, HP-UX, AIX
- Certificati FIPS 140-2 Level 2 and Level 3, NIST SP 800-131A

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

Dispositivi per applicazioni specifiche 1/3

SYMBOLIC

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).

SYMBOLIC

Payshield 9000

- Si tratta di un HSM progettato appositamente per sostenere le operazioni crittografiche legate al trasferimento elettronico di valuta (EFT).
- Viene tipicamente impiegato dalla banche e da chi gestisce le carte di credito per manipolare i PIN e abilitare le transazioni.

SYMBOLIC

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.

Info

Symbolic S.p.A.
Via Paradigna 38/A
43122 Parma
T. 0521 708811
F. 0521 708890

www.symbolic.it
sales@symbolic.it