SPYRUS

Rosetta™ Smart Card e USB Series II e Series III

Smart Card USB Normali e Readerless

Le smart card aumentano la sicurezza cifrando ed archiviando le tue chiavi private su un dispositivo sicuro anziché sul computer. Rosetta USB 3.0 di SPYRUS è compatta e non richiede un lettore separato, mentre le serie Rosetta II e Rosetta III offrono la sicurezza smart cardi nel tradizionale formato ISO 7816 card format. Le smart card sono perfette per l'autenticazione a più fattori, la cifratura e la firma dei messaggi aziendali.

Rosetta Smart Card e Rosetta USB si presentano diversamente, ma le loro funzionalità sono identiche – capacità PKI utilizzando i più robusti algoritmi crittografici presenti sul mercato.

La password di sblocco della smart card non viene mai archiviata da nessuna parte e viene usata per ricostrure una "key encryption key" master, che viene poi impiegata per aprire un'applicazione di protezione della chiave privata unica.

Se la password viene smarrita, una speciale utility dell'amministratore deve venire utilizzata per sbloccare il dispositivo e resettare la password.

I dispositive Rosetta Smart Card e Rosetta USB sono progettati utilizzando una forma di crittografia avanzata per garantire la massimo protezione delle informazioni su tutte le postazioni.

Il security controller Rosetta, validato FIPS 140-2 Livello 3, e SPYRUS Cryptographic Operating System (SPYCOS®) dei dispositivi Rosetta Smart Card e Rosetta USB sono gli stessi impiegati anche nei premiati Windows to Go WorkSafe Pro e nella famiglia di dispositivi USB cifrati P-3X.

La gamma Rosetta è multipiattaforma e si integra senza soluzione di continuità con un ampio spettro di sistemi operativi desktop e mobili. E' progettata per l'uso assieme a applicazioni classificate come dispositivo non-CCI (Controlled Cryptographic Item).

Il nucleo crittografico protegge contro gli attacchi attivi e passive, utilizzando uno scudo attivo e uno schema di memoria random per prevenire la manomissione fisica. Comprende anche contromisure contro gli attacchi laterali, come analisi del timing, analisi semplice e differenziale della Potenza, e analisi differenziale degli errori.

Il supporto crittografico hardware rende i dispositivi Roretta invulnerabili ai molti attacchi che hanno compromesso la crittografia software sui personal computer.

I dispositivi Rosetta supportano le funzionalità di certificazione digitale PKI, come il logon della smart card, la firma digitale e la cifratura delle email, l'autenticazione VPN e la navigazione web autenticata.

Specifiche Tecniche

Funzionalità

Massima protezione garantita per chiavi, ID digitali, e dati confidenziali

Forme/Interfacce disponibili

- Interfacci ISO 7816 (smart card)
- USB 3.0

Numero di serie unico per ciascun dispositivo.

Circa 32K di EEPROM disponibile per i certificati X.509 e l'archiviazione di dati

Tecnologia di generazione numeri random avanzata

Anti-clonazione

Driver certificate WHQL per Windows XP, Vista, Windows 7, Windows 8, Server 2008 e Server 2012.

Driver CCID e PKCS-11

Compatibile con Microsoft CryptoAPI e Cryptographic API: Next Generation, include il support per Windows Vista, Windows 7, Windows 8 e PKCS #11

Supporto minidriver per System Center.

Caratteristiche di SPYCOS®

Rafforzamento delle Policy di Sicurezza

Il Memory File Manager preserva l'integrità dei file se il dispositivo viene rimosso durante il loro trasferimento.

Memory Manager EEPROM, basato su kernetl, per allocazione dinamica della memoria non volatile

Data Firewall

Modulo di Circuito Integrato

EEPROM 64K con 32k di archiviazione

Conserva i dati per almeno 10 anni

Minimo 500,000 cicli scrittura/cancellazione a 25°C

Consumi

Voltaggio: Vcc = da 3.3 a 5VDC

Consumo elettrico: ~30mA @ 3.3VDC

Ambiente

Temperatura operativa: -15° C - 55° C

Temperatura di archiviazione: -20° C - 65° C

Standard e Sicurezza

ANSI X9.31 RSA Key Generation

FIPS PUB 46 Data Encryption Standard

FIPS PUB 180-2 Secure Hash Algorithm Standard

FIPS PUB 186-2 Random Number Generator FIPS

PUB 186-2 Digital Signature Standard

FIPS PUB 197 Advanced Encryption Standard

SP 800-38A Block Modes of Operation

SP 800-56A Key Establishment Guidelines

SP800-90A Hash_DRBG

FIPS 140-2 Level 3 / EAL 5+ validated crypto core

Cryptographic Algorithms

Crittografia Suite B (insieme di algoritmi crittografici pubblicati dal Governo USA come parte del programma di modernizzazione della crittografia per fornire una base crittografica interoperativa sia per le informazioni non classificate che per la maggior parte delle informazioni classificate) ed altri algoritmi approvati FIPS, comprendenti:

Hash_DRBG RNG

Elliptic Curve Cryptography (P-256, P-384, P-521)

ECDH

ECDSA Digital Signature Algorithm

RSA 1024 and 2048 digital signature algorithm

TDES-2 and TDES-3, ECB, CBC

AES 128/192/256 with ECB, CBC, CTR

SHA-1 and SHA-224/256/384/512 secure hash algorithms

HMAC

(Nota: le funzionalità di sicurezza possono variare a seconda della versione di Rosetta SPYCOS utilizzata nel prodotto.)

Per maggiori informazioni sui prodotti SPYRUS, visita il sito **www.digitree.it**, oppure contattaci via email o telefono.

Corporate Headquarters
1860 Hartog Drive
San Jose, CA 95131-2203
+1 (408) 392-9131 phone
+1 (408) 392-0319 fax
info@SPYRUS.com

East Coast Office
+1 (732) 329-6006 phone
+1 (732) 832-0123 fax

UK Office
+44 (0) 113 8800494

Venduto in Italia da:
DigiTree
Via di Romagna 9/134134
Trieste (Italy)
+39 366 8948545
sales@digitree.it
www.digitree.it