SPYRUS

Rosetta® microSDHC™ Card

Secure PKI Smart Card and TrustedFlash™ storage in a Micro-Sized Device

Rosetta microSDHC card è un formato ad alta capacità a livello degli standard di sicurezza industriali disponibile in due configurazioni: 1) Rosetta microSDHC PKI è un dispositivo public key infrastructure (PKI) con memoria flash in chiaro. 2) La configurazione TrustedFlash™ abilita la crittografia hardware AES-256 encryption per fornire la protezione dati più robusta attualmente disponibile sul mercato e funzionalità PKI da utilizzare con applicazioni abilitate a chiave pubblica.

Rosetta microSDHC PKI HSM

Mentre le smart card PKI o analoghi dispositivi abilitati NFC possono accrescere la sicurezza delle applicazioni attraverso l'uso di autenticazione multifattore, cifratura, e firma dei messaggi, di solito il loro impiego richiede un lettore oppure una porta USB speciale. Rosetta microSDHC PKI invece è una smart card contenuta in un formato microSDHC.

SPYRUS Cryptographic Operating System (SPYCOS®), validato FIPS 140-2 Livello 3, usato in Rosetta microSDHC è lo stesso di Rosetta Smart Card, Rosetta USB, PocketVault P-3X USB 3.0 (dispositivo di archiviazione cifrata) e la famiglia di Live Drive Windows To Go certificati Microsoft. SPYCOS fa da security controller con una resistenza alle manomissioni di grado EAL5+ nel corpo della micro SDHC Rosetta.

Rosetta microSDHC è un hardware security module (HSM) progettato per l'uso con applicazioni abilitate a chiave pubblica come cifratura di email, firma digitale, autenticazione VPN e web.

SPYRUS TrustedFlash™microSDHC

La micro SDHC TrustedFlash aggiunge memoria flash criptata AES-256 a livello hardware alle capacità di Rosetta microSDHC PKI, progettate dalle basi per garantire protezione di alto livello a chiavi e identità personale nei dispositivi mobili grazie all'impiego di crittografia avanzata.

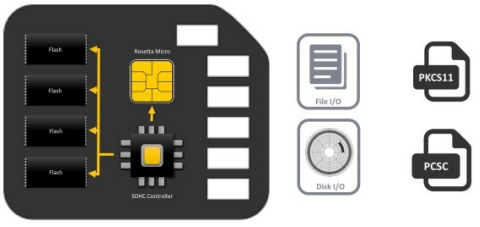
Il suo nucleo di cifratura SPYCOS protegge contro gli attacchi attivi e passivi, utilizzando uno scudo attivo e uno schema di memoria random per prevenire la manomissione fisica. Comprende anche contromisure contro gli attacchi laterali.

La crittografica hardware nel suo Trusted Flash rende Rosetta microSDHC invulnerabile a molti degli attacchi che hanno invece compromesso PC, tablet ed altri dispositivi mobili.

TrustedFlash assicura la cifratura al volo della memoria flash, progettata per proteggere informazioni personali sensibili o dati aziendali, nonchè Personally Identifiable Information (PII) all'interno di una cassaforte hardware. L'accesso a Trusted Flash avviene semplicemente inserendo Rosetta micro SDHC card nella porta microSD o SD disponibile nella maggior parte dei laptop e tablet. Il formato microSDHC è un modo estremamente conveniente di proteggere i dati a riposo senza utilizzare le limitate porte USB. L'accesso alla cassaforte ad hardware cifrato TrustedFlash è reso disponibile soltato dopo che un Utente ha effettuato con successo il login microSDHC. La chiave del dispositivo Rosetta è azzerata se si supera un massimo di tentativi errati di accesso, il cui numero può essere stabilito per policy.

L'azzeramento delle chiavi è molto più sicuro e rapido rispetto a quello dell'intero contenuto della memoria flash..

Le configurazioni Rosetta microSDHC PKI e TrustedFlash lavorano anche con le applicazioni NcryptNshare che forniscono protezione dati su una base file-per-file. La combinazione di NcryptNshare con TrustedFlash fornisce l'estrema difesa in profondità per gli ambienti Windows.



The PKI mode configures the file system as a standard non-encrypting flash file systems. The TrustedFlash™ mode configures the file system as a hardware-encrypting file system using Rosetta for all key management features

SPYRUS

Specifiche Tecniche

Funzionalità

Per chiavi e certificati digitali basati su PKI, come email cifrate/firmate, firme digitali, VPN e web browsing autenticati

La configurazione opzionale TrustedFlash™, a crittografia hardware AES 256-bit automatic fornisce protezione alla memoria flash nei servizi PKI

Azzeramento della chiave quando vengono superati i tentativi errati di accesso

Garanzia di protezione FIPS 140-2 Livello 3 per chiavi, ID digitali e dati sensibili

Numero seriale unico per ciascu dispositivo

Circa 32K di EEPROM disponibile all'interno del security controller per i certificati X.509

Compatibile con Windows 7, 8, 8.1, 10/Linux ed altri SO su richiesta

Lavora con le applicazioni opzionali NcryptNshare

Caratteristiche di SPYCOS®

Rafforzamento delle Policy di Sicurezza

Il Memory File Manager preserva l'integrità dei file se il dispositivo viene rimosso duranteRafforzamento delle Policy di Sicurezza

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

Data Firewall

Capacità di Memoria

4,8,16 GB

Capacità maggiori saranno disponibili a fine 2016

Consumo Elettrico

Voltaggio: Vcc = 3.3 to 5VDC

Consumo: ~30mA @ 3.3VDC

Ambiente

Temperatura operativa: -15° C - 55° C

Temperatura archiviazione: -20° C - 65° C

Formato

Micro SDHC

Standard & Sicurezza

SDIO Specification Version 1.10

SD Physical Layer Specification Version 2.0

FIPS PUB 46-3 Data Encryption Standard

FIPS PUB 180-2 Secure Hash Algorithm Standard

FIPS PUB 186-4 Digital Signature Standard

FIPS PUB 197 Advanced Encryption Standard

FIPS PUB 198-1 Keyed Hash Message Authentication Code (HMAC)

SP 800-38A Block Modes of Operation

SP 800-56A Key Establishment Schemes

SP800-90A. Rev.1 Deterministic Random Bit Generator

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

Crittografia a livello militare: 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)

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

ECDSA Digital Signature Algorithm

Key Agreement / Establishment: CVL (ECC CDH), KAS, KTS

RSA 2048 digital signature algorithm

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

SHA-1, SHA-224/256/384/512 Secure Hash Algorithms

Altri algoritmi approvati FIPS:

HMAC (min 112 bit key) keyed hash MAC

SP800-90A HASH_DRBG (RNG)

TDES-3, ECB, CBC

SUITE B ON BOARD

Microsoft Partner
Gold OEM Hardware
Silver Independent Software Vendor (ISV)

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