SPYRUS®

Rosetta® microSDHC™ Card

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

Rosetta microSDHC PKI HSM

Rosetta microSDHC card è un formato ad alta capacità a livello degli standard di sicurezza industriali. La configurazione Rosetta microSDHC PKI è un dispositivo PKI con capacità di memoria flash e PKI da utilizzare con applicazioni abilitate per chiave pubblica.

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.

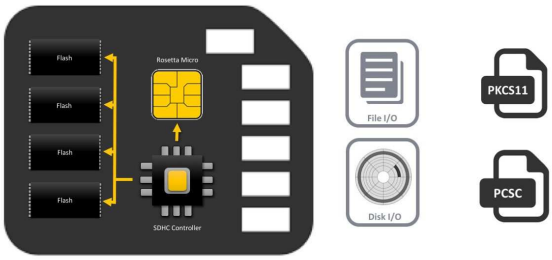
Le funzionalità di Rosetta microSDHC PKI sono progettate dalle basi per garantire protezione di alto livello a chiavi e identità personale nei dispositivi mobili grazie all'impiego di crittografia avanzata.

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 rende Rosetta microSDHC invulnerabile a molti degli attacchi che hanno invece compromesso PC, tablet e dispositivi mobili.

L'accesso ai servizi PKI 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 ai servizi PKI è reso possibile 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.

La configurazione Rosetta microSDHC PKI lavora anche congiuntamente con le applicazioni NcryptNshare che forniscono protezione dati su una base file-per-file. La combinazionoe di NcryptNshare con SPYRUS Rosetta microSDHC fornisce l'estrema difesa in profondità per gli ambienti Windows.



The PKI mode configures the file system as a standard non-encrypting flash file system.

SPYRUS®

Technical Specifications

Funzionalità

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

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 e 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

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

© Copyright 2013-2016 SPYRUS, Inc. All rights reserved. SPYRUS, the SPYRUS logos, Secured by SPYRUS, WorkSafe, Toughboot, SPYRUS Enterprise Management System, and Rosetta are either registered trademarks or trademarks of SPYRUS in the United States and/or other countries. All other trademarks are the property of their respective owners.
Patents: http://www.spyrus.com/patent-markings

Specifiche soggette a modifica senza preavviso.