SPYRUS

Rosetta™ Micro Series II e Series III

Circuito Crittografico Integrato

Se i tuoi dispositivi necessitano di funzionalità di cifratura, puoi cercare di progettarli e costruirli da solo, comprarli da un fornitore ignoto, o affidarti a SPYRUS, la compagnia statunitense che ha implementato la crittografia della Suite B in tutte le sue linee di prodotto.

Moduli di Sicurezza ad Alta Affidabilità

Le Rosetta Micro Series II e Series III sono i più piccolo e più sicuri hardware security module (HSM). Progettati per integrare applicazioni crittografiche, i circuiti integrati Rosetta Micro (6 mm x 5 mm) supportano i più robusti algoritmi di crittografia e lunghezza chiavi attualmente disponibili sul mercato, the strongest cryptographic algorithms and key lengths commercially available, superando gli algoritmi della Suite B algorithms e le raccomandazioni sulla lunghezza delle chiavi approvate dal Governo degli Stati Uniti per proteggere le informazioni non classificate e quelle classificate fino al livello top secret.

Le Rosetta Micro Series II e Series III si adattano perfettamente sia a prodotti personalizzati che di consume come computer, telefoni cellulari, PDA, router wired e wireless, point-of-sale e terminali di gaming, set-top box, e dispositivi di controllo industriale che richiedano piccole dimensioni, bassi consumi ed elevata sicurezza.

Sicurezza By Design

SPYRUS è specialista in processori sicuri ad alta affidabilità e convenienza da quasi vent'anni, e tutta la sua esperienza è racchiusa in un formato pronto all'uso per integratori e OEM.

Rosetta Micro si basa sui security controller Infineon 16-bit e 32-bit utilizzati da SPYRUS Cryptographic Operating System (SPYCOS®). Per assicurare il più elevato livello di sicurezza, le funzionalità crittografiche native del chip sono state disabilitate e re-implementate all'interno di SPYCOS.

SPYRUS può personalizzare Rosetta Micro per venire incontro a specifici requisiti dei client circa capacità ed implementazioni. Una caratteristica opzionale è la tecnica "K of N split-knowledge" che abilita il controllo accessi multipli per le chiavi crittografiche in decifratura, il recupero delle chiavi, ed altre applicazioni simili. Un'altra opzione supporta tecniche anti-clonazione per provare che il chip è unico ed autentico.
Implementata nei dispositive premiati Hydra PC USB 3.0 WorkSafe e WorkSafe Pro, K of N implementa una sicurezza provata matematicamente assicurando il contenimento dei dati su host e dispositive autorizzati, ed impedendo l'uso del dispositivo su postazioni non autorizzate.

Rosetta Micro è progettata e sviluppata nello stabilimento statunitense da personale accuratamente selezionato. Gli aggiornamenti del firmware sono installati e testati in casa prima della spedizione al cliente.

Aumentato Supporto Crittografico

Se gli algoritmi ad alta affidabilità inclusi nella Suite B assicurano la sicurezza dei dati per decenni, Rosetta Micro supporta anche algoritmi tradizionali come RSA, triple-DES, and SHA-1 per compatibilità retroattiva con le applicazioni esistenti.

Rosetta Micro abilita le funzionalità di certificazione digitale PKI tradizionali ed avanzate come il logon della smart card, la firma e la crittografia delle email, l'autenticazione VPN, e la navigazione web autenticata. Vedi la lista completa degli algoritmi crittografici supportati nelle specifiche tecniche che seguono.

Caratteristiche	SPYRUS Rosetta	Concorrenza
Crittografia di nuova generazione a Curva Ellittica per cifratura/decifratura/firma	✔	⊘
Algoritmo K of N Split Knowledge (versioni selezionate)	✔	⊘

Caratteristiche Avanzate

- Protezione hardware ad alta affidabilitàper chiavi, ID digitali e dati confidenziali.
- Supporto del più robusto algoritmo crittografico attualmente disponibile sul mercato..
- Alte prestazioni a basso consumo nel formato più piccolo per le applicazioni integrate.
- Utilizza l'insieme aumentato di istruzioni 8051 e supporta l'interfaccia standard ISO 7816 interface per un'ampia compatibilità applicativa.
- Circa 32K di EEPROM disponibile per l'archiviazione di certificate X.509 e dati.
- Include un'unità hardware di gestione e protezione della memoria.
- Una tecnologia avanzata ad alta entropia di generazione numeri randomi garantisce chiavi sicure.
- Supporta la biometria ed altri fattori di autenticazione avanzata.
- Supporta tecniche anti-clonazione come un numero seriale unico per Rosetta Micro module and un'unica coppia di chiavi per token per modulo.
- Resistente alle manomissioni: il suo design protegge dagli attacchi fisichi e di reverse engineering delle applicazioni e dei dati caricati, nel caso in cui gli attaccanti siano in possesso di un prodotto contetnente Rosetta Micro.
- Validata FIPS 140-2 Livello 3. Progettata per sostenere la validazione FIPS 140-2 a Livello 4 e superiori, a seconda dei requisiti di applicazione.
- API compatibili con Microsoft CryptoAPI e Cryptographic API: Next Generation, incluso il support per Windows Vista; e PKCS #11.
- Librerie e driver personalizzate sono disponibili per ambienti applicative e sistemi operativi particolari.
- Qualificazione industriael e/o MIL-SPEC disponibili per ordini speciali.
- Stabilimento di produzione certificato ISO 9000.

SPYRUS

Technical Specifications

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

Security controller Infineon SLE66 e SLE88 16-bit e 32-bit

64K EEPROM, 206K ROM, 5052 RAM" con 32K disponibili per l'archiviazione dei certificati

Motore crittografico avanzato 1100-bit

Acceleratore 112-bit/192-bit DDES & ECC GF(2n)

Mantenimento dati minimo 10 anni

Cicli minimi scrittura/cancellazione 500,000 a 25°C

Layout ottimizzato per sicurezza e resistenza

Conforme normativa RoHS

Consumi Elettrici

Voltaggio: Vcc = 3.3 to 5VDC

Consumo: ~30mA @ 3.3VDC

Ambiente

Temperatura operativa: -15°C - 55°C

Temperatura archiviazione: -20° C to 65° C

Umidità: 90%, non condensante

Range di temperature estensibili a richiesta.

Standard MIL & JEDEC

High-temperature storage life: MIL-STD-883 Method 1008

Temperature cycle report: MIL-STD-883 Method 101 Condition C

Temperature humidity exposure: JEDEC JESD22-A101-B

HAST JEDEC JESD22-A110-B

Preconditioning: JEDEC JESD22 A113-E

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

Crypto-core validato FIPS 140-2 Livello 3/EAL 5+

Algoritmi di cifratura

Crittografia Suite B (un insieme di algoritmi crittografici pubblicati dal Governo USA come parte del suo programma per la modernizzazione della crittografia che serve come base crittografica interoperativa sia per le informazioni non classificate che per la maggior parte di quelle classificate) e altri algoritmi approvati FIPS, compresi:
Hash_DRBG RNG
Elliptic Curve Cryptography (P-256, P-384, P-521)

ECDH

ECDSA Digital Signature Algorithm

RSA 1024 and 2048 digital signature

TDES-2 and TDES-3, ECB, CBC

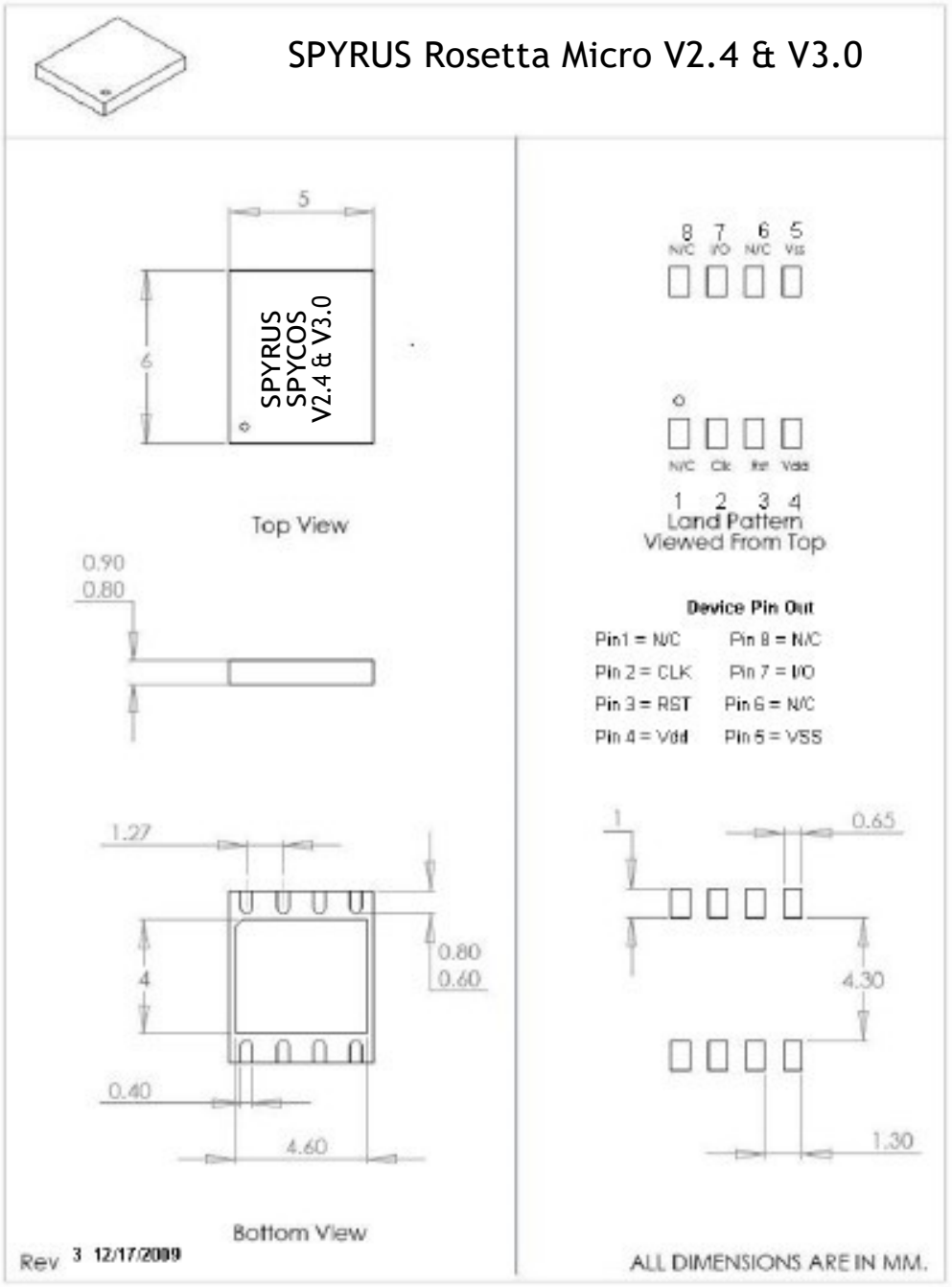
AES 128/192/256 with ECB, CBC, CTR

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

HMAC

SPYRUS

SPYRUS Rosetta Micro V2.4 & V3.0



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

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