SPYRUS®

PocketVault™ Smart USB 3.0

Dual Storage and Integrated Rosetta® PKI Smart Card Capability

Protect the Key In Your Pocket

PocketVault Smart USB 3.0 combines SSD storage with a Rosetta Hardware Security Module (HSM) to create an integrated, FIPS 140-2 Level 3 smart card and storage device in the high performance USB 3.0 portable form factor.

PocketVault Smart USB works perfectly with Windows, Linux® or Macintosh computers to store your personal pictures, movies, Office files, or other next generation content such as in-memory data analytics.

SPYRUS PocketVault Smart USB is unlike any other USB 3.0 storage solution, containing a hardware security module and smart card services plus the device itself is tested to exhaustive MIL-STD-810 environmental specifications.

The Rosetta HSM validated security controller is designed, engineered, and manufactured in the United States.

PocketVault Smart USB 3.0

with Integrated Rosetta PKI Smart Card Capabiltiy

The Rosetta HSM delivers smart card functionality for storing certificates and signing credentials for PKI applications and BitLocker keys.

Features and Benefits

- Storage – The PocketVault Smart USB 3.0 SSD is available in 32 GB, 64 GB, 128 GB, 256 GB, and 512 GB memory capacities.
- Size – The PocketVault Smart USB is small and compact to easily fit in your pocket.
- BitLocker and TureCrypt Key Protection – Safely use it to protect BitLocker or TrueCrypt software-based disk encryption keys with optional SPYRUS software.
- Cryptography – The Rosetta HSM is designed with Cryptographic Algorithm Agility to support the RSA digital signature and SHA-1 hash algorithm in addition to the next generation Suite B cryptography suite, an interoperable cryptographic base promulgated by the US government for both unclassified information and most classified information.
- Key Generation - Keys are generated in the Rosetta HSM device using a random number generator compliant with NIST SP 800-90A.
- No passwords to hack – The Rosetta HSM does not store passwords nor does it use password hashes as simple logical control to gain access to Rosetta protected data. The correct password is entered into Rosetta from an external source in order to authenticate access to the decryption keys stored in FIPS 140-2 Level 3 tamper proof hardware module for use in decrypting Rosetta protected data.
- PKI Applications – Enable PKI applications such as smartcard logon for two factor authentication, encrypted email, VPN and web authentication, and digital signature applications when using the optional MiniDriver that is downloaded from the Windows Update site.

SPYRUS®

Technical Specifications

Capacities & Dimensions (LxWxH)

32 GB, 64 GB, 128 GB, 256 GB
86.1 mm x 24.2 mm x 10.8 mm (+/- 0.20)

512 GB
101.6 mm x 24.2 mm x 10.8 mm (+/- 0.20)

Performance (based on 512 GB drive*)

USB 3.0 Super Speed; USB 2.0 Compatible

Sequential Read: up to 249 MB/sec

Sequential Write: up to 238 MB/sec

* Not all drives have this performance.

Reliability

Data Retention: up to 10 years and is application dependent

Rosetta SPYCOS Certifications

FIPS 140-2 Algorithm Certificates

FIPS 140-2 Level 3

Electrical

Operating Voltage Vcc = 3.3 to 5 VDC

Power Consumption* 275mA @ 3.3 VDC

* Power Consumption may vary based on memory capacity.

Other

At SPYRUS, we understand that people rely on their WTG device for mission critical functions. In essence, it is their computer SSD drive. So unlike a traditional USB that is used less regularly and is much easier to replace, we realized early-on in our customer deployments that the device must withstand punishment from a physical design perspective. To that end we designed our Windows To Go devices meet the highest physical standards in design and component materials. The combination of stringent environmental testing and additional testing for magnetic fields, X-Ray and long term immersion demonstrate the usability of this high security configuration of the SPYRUS WTG devices in the challenging healthcare environments as well.

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

Environmental

Operating Temperature (MIL-STD-202, METH 503) 0°C - 70°C

Non-Operating Temperature Cycling (MIL-STD-810, METH 503) -40°C - 85°C

High Temperature Storage (MIL-STD-810, METH 501) 85°C; 96 hours

EMI (FCC/CE) FCC Part 15, Class B/EN55022 - EN55024/etc

ESD (EN61000-4-2) Enclosure Discharge - Contact & Air

Dust Test (IEC 60529, IP6) As per defined

Waterproof Test (IEC 60529, IPX7) As per defined

Operating Shock, MIL-STD 883J, Method 2002.5, Cond. B, 1500g, 0.5ms, 1/2 sine wave

High Temperature Storage/Data Retention, MIL-STD-810, METH 501, 100°C; 96 hours

Waterproof test,MIL-STD-810, METH 512.6,1 meter depth, 30 minutes

Rosetta HSM Security & Cryptographic Standards

ANSI X9.31 RSA Key Generation
FIPS PUB 46 Data Encryption Standard
FIPS PUB 180-2 Secure Hash Algorithm Standard
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

Suite B cryptography (a set of cryptographic algorithms published by the U.S. Government as part of its cryptographic modernization program to serve as a interoperable cryptographic based for both unclassified information and most classified information) and other FIPS-approved algorithms, including:

RNG
Elliptic Curve Cryptography (P-256, P-384, P-521)
ECDH
ECDSA Digital Signature Algorithm
RSA 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

Support for the cryptography can vary depending on version.

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

Australia Office
Level 7, 333 Adelaide Street
Brisbane QLD 4000, Australia
+61 7 3220-1133 phone
+61 7 3220-2233 fax
www.spyrus.com.au

Document number 400-500001-01