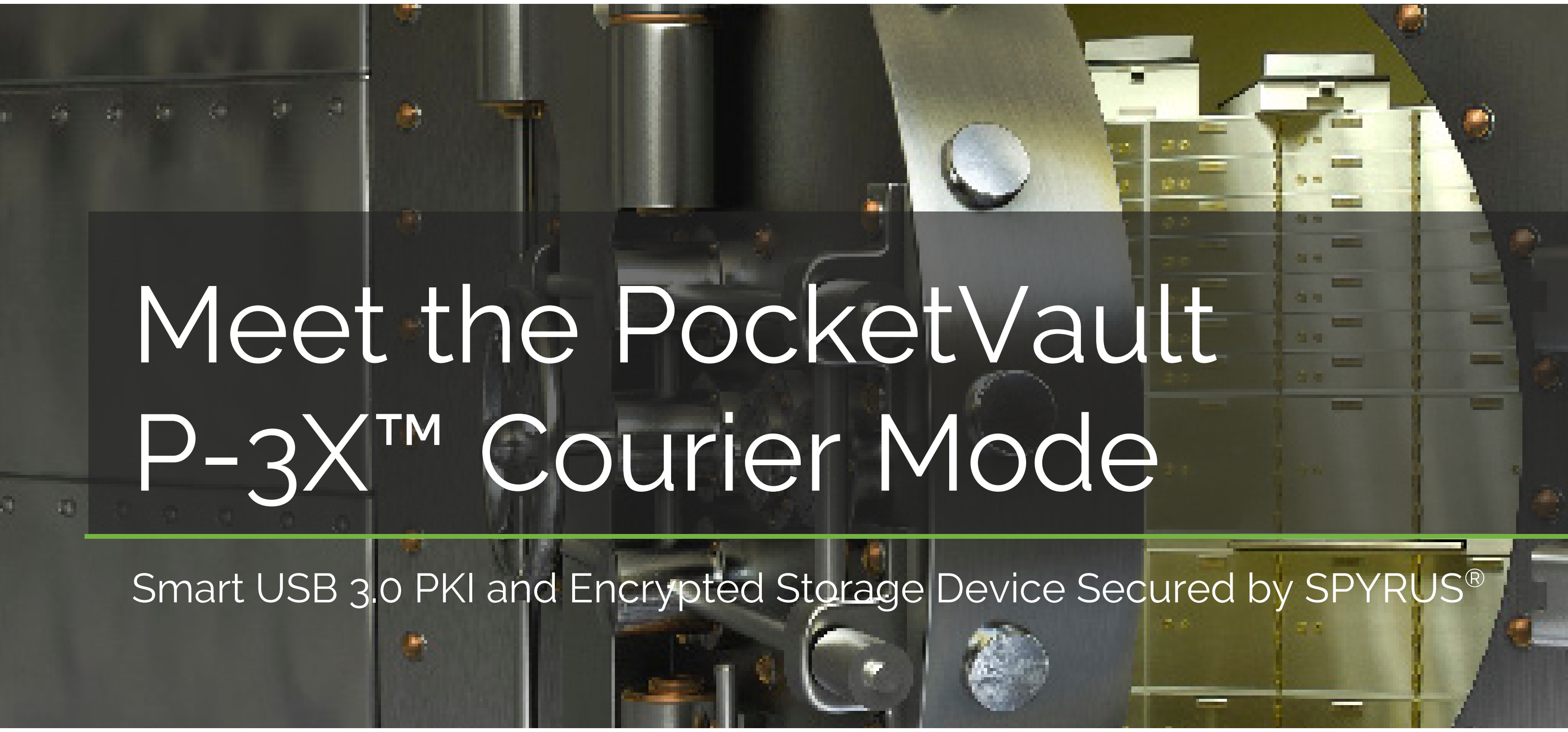
SPYRUS®



Meet the PocketVault P-3X™ Courier Mode

Smart USB 3.0 PKI and Encrypted Storage Device Secured by SPYRUS®

Like A Bank Vault In Your Pocket

The PocketVault P-3X USB 3.0 secure storage device is a high-security, use-anywhere encrypting solid-state disk (SSD) drive that protects data like a bank vault.

The combination of USB 3.0 and SSD storage adds up to the fastest performance available.

PocketVault P-3X is easy to use, too. Just log on and drag files to it as you would with any USB drive. Every file on the PocketVault P-3X is securely protected in its encrypted solid-state storage.

The cryptographic components in every SPYRUS secure storage device are designed, engineered, and manufactured in the United States by carefully vetted personnel.

The PocketVault P-3X PKI smartcard is used for two factor authentication to Windows PCs and cloud services!

PocketVault P-3X Features and Benefits

- Incredibly fast USB 3.0 and SSD performance. No waiting to access your data.
- Absolute security from XTS-AES 256 full disk encryption and next-generation P-384, SHA-2 384 cryptography promoted by the multiple governments for unclassified information and even classified information.
- Keys are generated in the FIPS 140-2 Level 3 device and are never exported or escrowed.
- Patent pending technology reconstitutes keys as required—they are not stored anywhere.
- Passwords are never stored on the device, even in hashed form.
- Optional SEMS device management on premise or cloud service.
- Can be set to hardware read only mode for protection against malware from untrusted computers.
- Simple user interface makes logon, encryption, and setup easy.

SPYRUS® PocketVault P-3X™

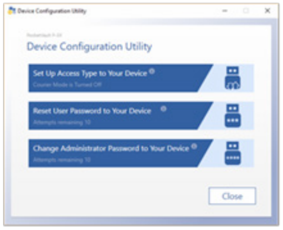
Courier Mode Operation Overview and Preliminary Product Specifications

4 CONFIGURATIONS: 1 DRIVE
1. XTS-AES 256-bit hardware encrypted storage
2. Windows accessible Hardware Security Module for multi-factor authentication and Smartcard services
3. USB 3.0 speeds/SSD quality memory
4. Read-only "courier mode" to permit privileged users to modify data, other authorized users to read only without tampering
SPYRUS
512GB

P-3X Courier Mode Features

- Files are controlled by the data owner, not the user
- Users are restricted to logon and can only read files from P-3X
- Users can change their password
- Data Administrators can add files to or delete them from P-3X in Courier Mode
- Data Administrators can reset P-3X in Courier Mode ensuring that all data will be destroyed
- Data Administrators can reset User passwords without loss of data
- Transition to management with SPYRUS Enterprise Management System

P-3X Courier Mode: Administrator Login

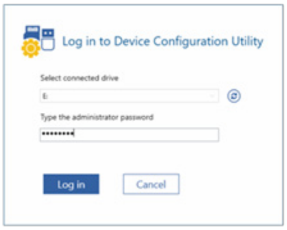


Device Configuration Utility

Set Up Access Type to Your Device
Courier Mode is Turned Off

Reset User Password to Your Device
Attempts remaining 10

Change Administrator Password to Your Device
Attempts remaining 10



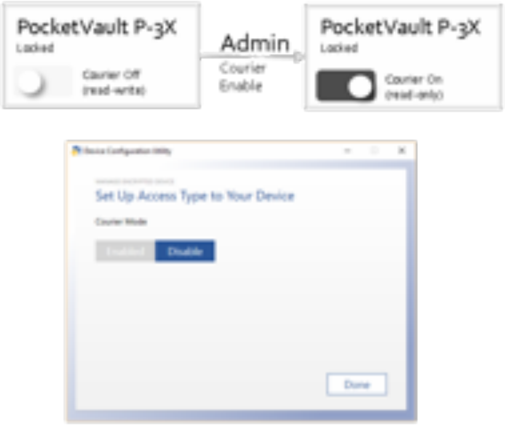
Log in to Device Configuration Utility

Select connected drive: E:

Type the administrator password: ••••••••

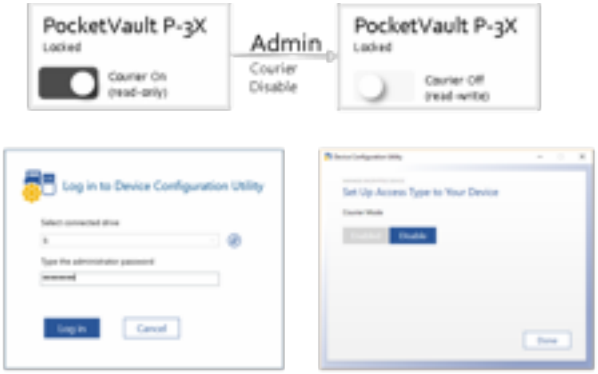
Using the newly created Administrator password, Courier Mode can only be enabled using that password. The User password will not work. When the user logs onto the drive to unlock it, hardware read-only mode is enforced. The user can not add, remove nor change any files.

P-3X Courier Mode: Enable



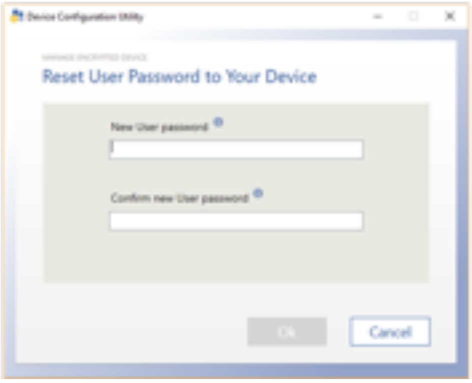
Using the newly created Administrator password, Courier Mode can only be enabled using that password. The User password will not work. When the user logs onto the drive to unlock it, hardware read-only mode is enforced. The user can not add, remove nor change any files.

P-3X Courier Mode: Disable



Using the newly created Administrator password, Courier Mode can only be disabled using that password. The User password will not work. AFTER THE admin disables Courier Mode, when the user logs onto the drive to unlock it, read-write mode is allowed. The user can now add, remove and change any files.

P-3X Courier Mode: Reset User Password


Device Configuration Utility
MANAGE ENCRYPTED DEVICE
Reset User Password to Your Device
New User password
Confirm new User password
OK
Cancel

Data Administrators can reset User passwords without loss of data

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 capacities
101.6 mm x 24.2 mm x 10.8 mm (+/- 0.20)

1 TB capacities - Contact Sales

Performance (based on 512 GB drive)

USB 3.0 Super Speed; USB 2.0 Compatible

Please note Random Read and Random Write Performance is the most important metrix for bootable live drives.

Sequential Read: up to 249 MB/sec

Sequential Write: up to 238 MB/sec

Reliability

Data Retention: 10 years

Other Certifications

FIPS 140-2 Algorithm Certificates

FIPS 140-2 Level 3

MIL-810 Tested to no failure (40 + approved testing scenarios)

Electrical

Operating Voltage	Vcc = 3.3 to 5 VDC
Power Consumption	275mA @ 3.3 VDC

Other

Humidity	90%, noncondensing

Physical Device Integrity:

At SPYRUS, we understand that people rely on their USB 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 USB 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

Hardware Security & Cryptographic Standards

SPYRUS Algoritm Agility includes Suite B (a set of cryptographic algorithms used for cryptographic modernization) and RSA based cryptography.

XTS - AES 256 Full Disk Encryption

AES 128, 196, and 256 ECB, CBC, CTR, and Key Wrap Modes

SP800 - 90 DRBG (Hash DRBG)

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

ECDSA Digital Signature Algorithm

CVL (ECC CDH) [ECDH per SP 800-56A]

Concantenation KDF (SP800-56A)

RSA 1024 and 2048 Signature Algorithm (Note RSA 1024 has been depricated by NIST.)

RSA 1024 and 2048 Key Exchange (Note RSA 1024 has been depricated by NIST.)

PBKDF - 2 (per PKCS#5 version 2)

DES, two-& three-key triple DES with ECB, CBC Mode (Note DES has been deprecated by NIST.)

SHA-1 and SHA-224/256/384/512 hash algorithms with HMAC Support

Support for the cryptography can vary depending on version.

FIPS 140-2 Level 3 opaque epoxy filled housing can be modified by special order.

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

Specifications subject to change without notice.