



Hydra Privacy Card® Personal Encryption Device

Encryption, Storage, and Transport of Classified Information

Every day, personally identifiable information and other sensitive and even classified information are at risk of falling into the wrong hands. It is just a fact of life. Look at a few examples from recent headlines:

- ▲ A laptop containing the Social Security numbers and other sensitive personal data of millions of veterans is stolen.
- ▲ Portable drives, some with classified military information, are stolen in Afghanistan and sold on the black market.
- ▲ Portable drives containing classified data are taken home without permission by a U.S. nuclear weapons lab employee.
- ▲ WikiLeaks—250,000 pages of classified US Government information including sensitive cables from overseas consulates is posted on the Internet.
- ▲ A laptop with personal data of nearly 200,000 retirement account holders is stolen.
- ▲ A drive with financial data and medical record numbers of 120,000 hospital patients is lost.

The Privacy Rights Clearinghouse estimates that over 500 million records of U.S. residents were compromised in 2010 alone. This number represents only reported data security breaches.

The consequences of lost or stolen sensitive data can be devastating. Even if the information is never actually misused, the fact that it might have been compromised can still result in huge expenses.

The Hydra PC Personal Encryption Device allows encrypted files to be stored on the device, on the host computer's hard drive, or anywhere else in the world, with complete security. You can encrypt a file in New York and pick it up in London.

Credit monitoring services typically cost from \$120 to \$180 per year for each person affected, and organizations responsible for data security breaches might be forced to pick up the tab for a number of years.

The cost of a data breach increased in 2009 to \$204 per compromised customer record, according to the Ponemon Institute's annual study. The average total cost of a data breach rose from \$6.65 million in 2008 to \$6.75 million in 2009.

When compromised data is classified, such as the information that showed up on WikiLeaks, potential costs can include human life and threats to national security.

Only strong hardware-based encryption can securely protect data from compromise.

Hydra PC™ Personal Encryption Device Overview

The Hydra Privacy Card® (Hydra PC™) Series II Personal Encryption Device (PED) from SPYRUS provides strong encryption in a small, portable, cost-effective, high-speed USB device. It implements Suite B cryptography, an interoperable cryptographic base for both unclassified information and most classified information. This is the most secure encryption technology commercially available.



Like all devices in the Hydra PC family, encryption keys are generated and stored in encrypted form on the Hydra PC PED. A password is required to unlock and access the Hydra PC, and other access authentication can be required.

For added security against “brute-force” access attempts, Hydra PC permanently deletes the encryption keys after 10 incorrect password attempts. After that, even the correct password will not work. A time delay that doubles after each incorrect entry further counters password attacks.

Encrypted files and folders can be stored within the Hydra PC on removable microSD storage cards, available at many retail stores. You can use any number of microSD cards with a single Hydra PC for unlimited capacity.

You can choose to store encrypted files and folders on the memory card, on the computer’s hard drive, on an external storage device, or even on an Internet-accessible storage drive, all with the same secure hardware-based encryption. Now every laptop and every desktop computer can receive complete protection against unauthorized access to sensitive data.

Mandatory file encryption makes Hydra PC PED ideal for organizations with regulatory requirements to protect personally identifiable or mission-critical information, such as financial, healthcare, and government. Every file stored on its microSD memory card is automatically encrypted, so there is no chance of transporting insecure data and no risk of compromise if the device is lost or stolen.

Files and folders can be encrypted and decrypted individually or as a group, and no matter where they are stored, they can be decrypted only by the device that encrypted them.

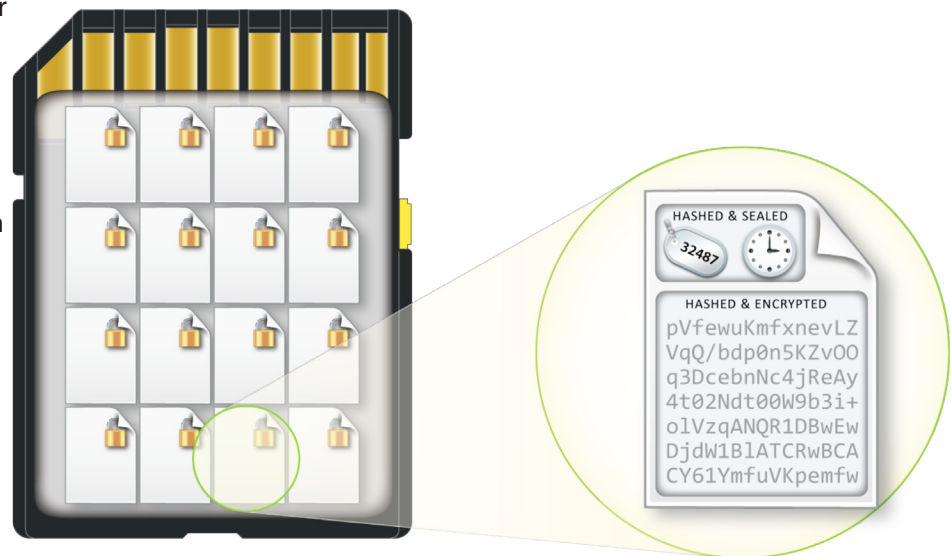
An exclusive feature lets you restrict a Hydra PC to work only with certain host computers. Even if you enter the correct password, the Hydra PC will

work only when connected to an authorized host computer.

Hydra PC software is easily installed and run, making it perfect for large or small organizations and even home users. Installation is fast and requires no special computer experience. The user interface integrates with the Windows file system and is easy to use.

Device management operations are simple and easy. Management can be restricted to designated administrators for better control in large organizations.

When you consider that Hydra PC provides the strongest encryption commercially available, the highest number of access authentication factors, and easy adaptability to home, enterprise, or government use, no other solution can compete in total cost-effectiveness.



Why Hardware-Based Encryption is More Secure

Hardware-based encryption sets Hydra PC apart from other encryption solutions that manage encryption operations within software. Why is hardware-based encryption on Hydra PC stronger? Take a look:

- ▲ The file encryption supported by PED provides superior confidentiality for sensitive information through the use of the strongest unclassified private key and symmetric algorithms approved by the US Government, including elliptic curve

cryptography (ECC) with key sizes up to P-521 for key wrapping, together with AES-256 symmetric encryption. These algorithms and key sizes are conservatively estimated to be sufficient to resist cryptanalysis for 170+ years, against all known attacks.

- ▲ Even if the computer’s operating system does not yet support advanced algorithms, Hydra PC does.
- ▲ Encryption keys are generated and stored in encrypted form on the Hydra PC and not on the computer. Even if your laptop is lost or stolen, files encrypted with Hydra PC are completely safe.
- ▲ Access to the Hydra PC requires up to three levels of authentication. Users must have the Hydra PC and know the password. An optional authentication level restricts Hydra PC use to authorized computers. Single-factor solutions, which require only a password (and use it as the encryption key) are vulnerable to brute-force attacks.

- ▲ The hardware is programmed to destroy the encryption keys and prevent access to protected files after 10 incorrect password entries. This prevents entry by brute-force attack.
- ▲ The tamper-resistant hardware design protects keys and encrypted files from reverse engineering attacks. A \$10,000 reward offered at the RSA Security Conference in early 2010 to anyone who could decode a file encrypted by a Hydra PC device is still unclaimed.

The table below compares important features of various encryption solutions.

Unprecedented Data Access Security

Data encrypted with Hydra PC cannot be decrypted until you have successfully authenticated yourself to the device. This makes authentication at least as important as encryption strength. Hydra PC provides the most secure authentication available.

	Hydra PC Personal Encryption Device	USB Flash Drive with SW-Based Encryption	Full Disk Encryption (FDE) on PC
Capacity	Unlimited with replaceable microSD	Limited to flash memory on drive	Available space on computer hard drive
Encrypted File Location	Hydra PC, computer hard drive, external drive, or Internet	Flash drive only	Computer hard drive only
Run-time Processing Integrity Checks?	Yes	No	No in most cases
Encryption Keys Vulnerable?	No—Encrypted on Hydra PC Provable security	Yes—Derived from password and easily broken	Yes—Stored on PC and either weakly encrypted or not encrypted at all
Restrict Use To Authorized PCs?	Yes	No	Product dependent by using TPM module present on some enterprise PCs
Compatible With Smart Card Logon & Digital Certificate Applications?	Yes	No	Product dependent

The National Security Agency’s USB Flash Drive Program has developed specifications for physically transferring SECRET data between secure enclaves. SPYRUS, Inc. asserts that the Hydra PC meets NSA’s USB Flash Drive specifications, documented in the Universal Serial Bus (USB) Flash Drive Personal Token for Tactical SECRET Minimum Essential Requirements 1.0, and as such, is acceptable for use in national security systems.

Each authentication factor is like a test to prove that you are authorized to access encrypted data. The more authentication factors required, the more secure your encrypted data is. You can require up to three authentication factors with the Hydra PC—more than any other encryption solution currently available.

Think of an authentication factor in terms of the proof that you need to pass the test. Each proof describes the authentication factor and the situation where you use it. The three factors for Hydra PC are “what you have,” “what you know,” and “where you are.”

WHAT YOU HAVE

You must have possession of the Hydra PC before you can do anything else.

Even if the files that you want to decrypt are stored on the computer or an external drive, the keys are stored on the Hydra PC, and all encryption and decryption takes place within the Hydra PC.

WHAT YOU KNOW

You must know and enter the password to gain access to encrypted information.

The default Hydra PC password length is seven characters to make it difficult to guess the password within the 10 tries allowed—and up to 256 characters are allowed.

WHERE YOU ARE

You can designate which computers will allow each Hydra PC to be unlocked. You can limit use of a Hydra PC to one computer, a dozen computers, or hundreds of computers, depending on your requirements. Unless you use the Hydra PC with an authorized computer, you cannot unlock the Hydra PC, even with the correct password.

The *Where You Are* authentication factor requires a 256-bit Enclave Authentication Value from the computer before encryption or decryption can occur, even if the user knows the password.

You can restrict the ability to set or change the *Where You Are* authentication factor to specific authorized administrators.



As Secure As Possible

Hydra PC offers the most secure hardware-based encryption currently available in a commercial product.

Hydra PC cryptographic algorithms include the latest elliptic curve technology adopted by the U.S. government in its Suite B standard. Hydra PC cryptographic algorithms are designed to meet U.S. Department of Defense dual-use requirements for protecting classified or unclassified data.

Specific cryptographic algorithms supported by Hydra PC include the following:

- ▲ Approved high-entropy random number generator used for all key, initialization vector (IV), and nonce generation
- ▲ Elliptic Curve Cryptography (ECC) using the NIST curves in GF(p) (P-256, P-384, and P-521)
- ▲ Elliptic Curve Diffie-Hellman (ECDH) key establishment meeting NIST SP 800-56A Key Establishment Guidelines
- ▲ ECDSA Digital Signature algorithm
- ▲ AES 128/192/256 with ECB, CBC, and CTR encryption modes
- ▲ Secure Hash Algorithms (SHA)—SHA-224/256/384/512

The default Suite B key lengths— ECC P-384, AES-256, and SHA-384 — meet U.S. Department of Defense strength requirements for Top Secret data under the appropriate circumstances.

All encryption operations take place in the on board, hardware-based encryption engine. Each file is uniquely encrypted on a pair-wise basis using an ECDH key establishment protocol between an originator and a specific recipient.

Each file is encrypted with a different AES-256 key and initialization vector every time it is encrypted to prohibit an attacker from determining changes by comparing different instances of the same encrypted file.

By default, the plaintext source file is hashed, compressed, and digitally signed. This signature is verified when the file is decrypted to provide irrefutable assurance that the file is unmodified from the original (see the illustration on page 1).

The Hydra PC Sentry feature enables administrators to block normal read/write access to removable USB or FireWire storage drives that use a disk file system, including USB flash drives and music players. Users cannot write to, open, or modify files on a blocked drive.

Private keys are stored within a tamper-resistant, tamper-evident security processor chip that is EAL5+ Common Criteria certified. The Hydra PC PED is FIPS 140-2 Level 3 validated.

The password is never stored on the device. When a session ends, through user logoff or disconnection of the device, all unencrypted keys are zeroized.

Hydra PC is designed to be fail safe and fail secure. During the power-on self-test and before and after each file encryption, Hydra PC executes extensive self checks and compares redundant algorithm implementations. The device contains defenses against side-channel attacks, including timing and power analysis attacks.

Device Management

Every Hydra PC device order includes basic device management software that allows administration operations such as initialization and key management to be restricted to designated personnel.

Features and Benefits Summary

- ▲ **Encrypt and store data anywhere**—on the device, on a server, or in the cloud.
- ▲ **Infinite storage capacity**—uses replaceable microSD cards for the **lowest cost per GB**.
- ▲ **Data Containment**—Even with the correct password, users can unlock or decrypt files encrypted by the Personal Encryption Device only when it is connected to an authorized computer.
- ▲ Prohibit rogue device connection to **prevent data leakage**.
- ▲ Keys are generated in the device and **never exported or escrowed**.
- ▲ Quorum technology reconstitutes keys as required—they are **never stored** anywhere.
- ▲ Implements **Suite B cryptography**, an interoperable cryptographic base for both unclassified information and most classified information.
- ▲ Optional Sentry A-V **active anti-malware** delivers real-time protection to stop malware and worms in their tracks.
- ▲ Security designed, engineered, and manufactured in the USA to prevent the introduction of untrusted components

About SPYRUS

SPYRUS provides the world's most secure, portable hardware-based encryption, authentication, and content security/storage products for government and enterprise. Using advanced Suite B cryptographic algorithms, SPYRUS encryption devices protect data against outside threats and limit access to legitimate users with a specific need. SPYRUS cryptographic elements are proudly designed, engineered, and manufactured in the USA to mitigate the risks of untrusted parts entering the supply chain.

Founded in 1992, SPYRUS is based in San Jose, California in the heart of the Silicon Valley.

Technical Specifications

- **Capacity***
 - Entombed 2GB, 4GB, 8GB, 16GB, 32GB
 - Replaceable standard or SDHC microSD cards for infinite capacity
- **Speed (dependent on microSD card)**
 - Up to 20MB per second read
 - Up to 10MB per second write
- **Dimensions**
 - 3.2 x 0.5 x 0.9 inches
 - Custom design and packaging available, including raw epoxied PC board
- **Weight**
 - .8 oz (22 grams)
- **Temperature**
 - Operating: -20°C, +65°C
 - Storage: -40 °C, +85 °C
- **Interface**
 - USB 2.0 high speed
- **Operating System Compatibility***
 - Windows 2000 SP4
 - Windows XP SP2+
 - Windows Vista
 - Windows 7
 - Windows Embedded Standard
- **Multiple individually validated FIPS 140-2 Level 3 security boundaries create a flexible and extensible architecture allowing continuous technology upgrades.**
 - Cryptographic operating system (SPYCOS®)
 - File encryption
- **Active anti-malware**
 - Sentry A-V using McAfee anti-virus engine with auto-update
- **Manageability**
 - Can be managed by the SPYRUS Enterprise Management System (SEMS)
- **Encryption—US Department of Defense-approved Suite B cryptography**
 - File: AES CBC 256 bit
 - Encryption Keys: 256-bit hardware
 - Secure Channel: ECDH P-384 and AES 256
 - PKI Signing: ECDSA P-521 and lower
 - Hashing: SHA-384

- **Standards Compliance**
 - Microsoft CryptoAPI, Microsoft Card Module, and PKCS #11 interoperability
 - 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 and 800-38E Modes of Operation
 - SP 800-56A Key Establishment Guidelines
 - SP 800-90 Random Number Generation

How To Buy

- On the USCYBERCOM approved list
- On the DoD IDIQ—call or email sales@spyrus.com
- Federal and civilian agencies can source via DAR ESI/BPA reseller Autonomic Resources (www.autonomicresources.com) #GS-35F-0587R
- Available in the USA from Amazon and from resellers worldwide.

Proudly designed, engineered,



and manufactured in the USA

For more information about SPYRUS products, visit www.spyrus.com or contact us by email or phone.

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) 329-6211 fax

Australia Office

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



© Copyright 2010 SPYRUS, Inc. All rights reserved. SPYRUS, the SPYRUS logos, Security to the Edge, Hydra Privacy Card, Hydra PC, Hydra PC Digital Attaché, Hydra PC Secure Pocket Drive, Rosetta, LYNKs, En-Sign, and SPYCOS 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. Individual SPYRUS products may embody technology protected by one or more of the following patents or patent applications:
U.S. Pat. Nos. 7,380,140; 6,088,802; 6,003,135; 6,981,149;
U.S. Pat. Appl. Ser. Nos. 12/018,094; 12/126,759.