



Hydra Privacy Card® Series II Enterprise Edition

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.
- ▲ Hundreds of laptops containing personal information from census responders are never returned by former employees.
- ▲ 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.

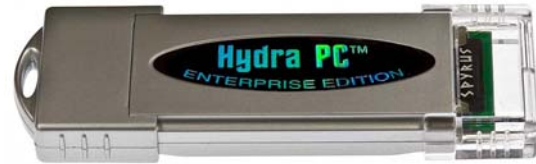
The Privacy Rights Clearinghouse estimates that over 100 million records of U.S. residents have been compromised. This number represents only reported data security breaches.

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.

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 Federal Trade Commission estimates that the average total cost of a single identity theft is

approximately \$18,000, including losses to the individual and the banking system, plus the hidden costs of trying to identify, apprehend, prosecute, and incarcerate the perpetrator. Add to that the cost of lost or stolen computers and portable drives. When compromised data is classified, potential costs can include human life and threats to national security.



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

Summary

The Hydra Privacy Card® (Hydra PC™) Series II Enterprise Edition is the strongest encryption solution commercially available. Key features:

- Hardware-based encryption technology exceeds algorithm standards approved by the U.S. government for classified data.
- Securely share encrypted files and folders anywhere among multiple users.
- Encrypted file storage on removable miniSD cards, PC hard drive, or external drive for unlimited capacity.
- Encryption keys can be recovered if Hydra PC is lost or destroyed or the PIN is forgotten.
- Strong protection against intruder attack.
- Exclusive authentication feature restricts use to only specifically designated PCs. Even with the PIN, Hydra PC will not work on an unauthorized computer.
- Supports security device functions, including smart card logon, secure e-mail, and secure network logon.

Hydra PC™ Enterprise Edition Overview

The Hydra Privacy Card (Hydra PC) Series II Enterprise Edition provides encryption solutions in a small, portable, cost-effective, high-speed USB device. Its hardware-based encryption uses algorithms and key sizes that exceed the new Suite B standard approved by the U.S. government. This is the most secure encryption technology commercially available.

Encryption keys are generated and stored in encrypted form on the Hydra PC. A Personal Identification Number (PIN) is required to 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 PIN entries. After that, even the correct PIN will not work. A time delay that doubles after each incorrect entry further counters these attacks.

Encrypted files and folders can be stored on the Hydra PC on removable miniSD™ storage cards. Standard miniSD storage cards are inexpensive and available at retail stores. You can use any number of miniSD 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.

Files and folders can be encrypted and decrypted individually or as a group. Hydra PC automatically encrypts every file stored on its miniSD memory card, so there is no chance of transporting insecure data and no risk of compromise if the Hydra PC is lost or stolen.

Files and folders encrypted on the miniSD card, the computer hard drive, or an external storage drive can be decrypted only by specifically designated Hydra PCs and users.

An exclusive feature lets you restrict a Hydra PC to work only with certain host computers. Even if you enter the correct PIN, the Hydra PC will work only when connected to a specifically authorized host computer.

The Hydra PC Enterprise Edition features a Secure File Sharing system that allows a user to encrypt files and folders and share them with one or more designated Hydra PC users. Only designated Hydra PC users can decrypt the files or folders with their own Hydra PC Enterprise Edition device.

Hydra PC-encrypted files and folders can be distributed as e-mail attachments, over networks or FTP, and on removable drives or CD/DVD with absolute security and data integrity.

The Hydra PC Enterprise Edition can be used as part of an enterprise disaster recovery plan to store encrypted data in multiple offsite locations. The Hydra PC Enterprise Edition includes a Recovery Agent that can decrypt encrypted files and folders when the Hydra PC is lost or destroyed or the PIN is forgotten.

Hydra PC software installs and runs on an individual computer, making it perfect for large or small organizations. Installation is fast and requires no special computer experience. The user interface integrates with Windows file capabilities and is easy to use.

You can use Hydra PC as a hardware security device to safeguard your Windows logon password and digital certificates. It is compatible with industry-standard smart card logon protocols, S/MIME secure e-mail technology, and Web-based mutual authentication. No one can log on to your computer, decrypt your email, or sign e-mail with your digital signature unless the Hydra PC is connected and you enter the PIN.

Why Hardware-Based Encryption is Stronger

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

- ▲ Hydra PC uses Elliptic Curve Cryptography (ECC) and the Advanced Encryption Standard (AES), the strongest available key-generation and encryption algorithms. These algorithms and key sizes are much stronger than the National Institute of Standards and Technology (NIST) requires for the next 25 years—strong enough to be used for classified information. Hardware-based encryption provides this support even if the computer’s operating system does not yet support advanced algorithms.
- ▲ 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 at least have the Hydra PC and know the PIN. An optional authentication level restricts Hydra PC use to specifically authorized computers. One-factor solutions, which require only a password or PIN, are vulnerable to brute-force attacks.
- ▲ The hardware is programmed to destroy encryption keys and block access to encrypted files after 10 incorrect PIN entries. This prevents entry by brute-force attack.
- ▲ The tamper-resistant hardware design protects keys and encrypted files from reverse-engineering attacks.

The following table compares important features of various encryption solutions:

Compare Hydra PC with Software-Encryption Solutions

	Hydra PC Enterprise Edition	USB Flash Drive with SW-Based Encryption	SW Encryption Application on PC
Capacity	Unlimited with replaceable miniSD	Limited to flash memory on drive	Available space on computer hard drive
Encrypted File Location	Hydra PC, computer hard drive, external or Internet drive	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 PIN and easily broken	Yes — Stored on PC Weakly encrypted or unencrypted
Restrict Use To Authorized PCs?	Yes	No	Not applicable
Compatible With Smart Card Logon & Digital Certificate Applications?	Yes	No	Product dependent

Unprecedented Data Access Security


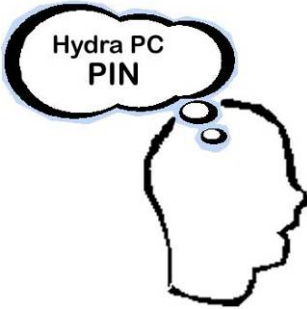

Data encrypted with Hydra PC cannot be decrypted until you gain access to the device. This makes access protection at least as important as encryption strength. Hydra PC provides the most secure access control available.

An 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. 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.”

Hydra PC Authentication Factors

What You Have	What You Know
 <p>You must have the Hydra PC before you can do anything else.</p> <p>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 on the Hydra PC.</p>	<p>You must know and enter the PIN to gain access to encrypted information.</p> <p>Hydra PC requires a PIN of at least seven characters to make it difficult to guess the PIN within the 10 tries allowed.</p> 
Where You Are	
 <p>You can designate exactly which computers will work with each Hydra PC. You can limit use of a Hydra PC to one computer, two computers, or many computers, depending on your requirements. Unless you use the Hydra PC with an authorized computer, you simply cannot access the Hydra PC, even with the PIN.</p> <p>You can restrict the ability to set or change the Where You Are authentication factor to specific authorized administrators.</p>	

A Closer Look at Hydra PC Technology

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) and ECMQV 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-1 (for legacy applications) and SHA-224/256/384/512
- ▲ RSA 1024 and 2048 digital signature and key exchange algorithms (for legacy applications)
- ▲ Two-key and three-key triple Digital Encryption Standard (DES) (for legacy applications)

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

All encryption operations take place in the onboard, 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.

Users can create a secure Hydra PC Identity based on valid digital certificates without requiring a new ECC-based public key infrastructure. This

means that DOD Common Access Card (CAC), PIV cards, and other hardware and software certificates and keys can be used to link the user's identity to the Hydra PC's keys.

When a file or folder is encrypted, users can designate multiple Hydra PC Identities to share decryption capability along with the encrypting Hydra PC. Individual key establishments are performed for each recipient.

Each file is encrypted with a different AES-256 key and IV every time 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.

The Where You Are authentication factor requires a 256-bit "Host Authorization Code" from the computer before encryption or decryption can occur, even if the user knows the PIN.

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 open or modify files on a blocked drive.

Private keys are stored on a tamper-resistant, tamper-evident security processor chip that is EAL5+ Common Criteria certified. The Hydra PC security processor is designed to meet FIPS 140-2 Level 4 physical protection standards when not in use and overall Level 3 standards when in use. The PIN is never stored on the device. When a session ends, through user logoff or disconnection of the device, all unencrypted keys (accessed only in RAM) 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 health tests and compares redundant algorithm implementations. The device contains defenses against side-channel attacks, including timing and power analysis attacks.

About SPYRUS

SPYRUS, Inc. has provided products and services for the information security market since its inception in 1992. Our focus is on customers in government and commercial enterprises, particularly those needing data protection and privacy in vertical markets regulated by legislation such as the Gramm-Leach-Bliley Act, Health Insurance Portability and Accountability Act (HIPAA), and Sarbanes-Oxley Act.

The Hydra Privacy Card Series II is part of the Talisman/DS Data Security Suite of encryption products. Other SPYRUS product lines include LYNKS Hardware Security Modules (HSMs), Rosetta Client Authentication (smart cards, USB security devices, and readers), and identity management products (Signal Identity Manager and SPYRUS PKI).

We implement the strongest commercial cryptographic algorithms available today. These algorithms, termed Suite B, have been designed to exceed the highest standards of security certification such as Common Criteria, FIPS 140-2 Levels 2 through Level 4, HSPD-12, and FIPS 201. Hundreds of government entities, corporations, systems integrators, and resellers worldwide have deployed our solutions.

SPYRUS is a privately held corporation headquartered in San Jose, California, with offices in Canada and Australia.

SPYRUS, Inc.



For additional details about SPYRUS products, visit www.spyrus.com or contact us at:

- ▲ USA +1 408 392-9131 info@spyrus.com
- ▲ Australia +61 7 3220-1133 info@spyrus.com.au



©2006–2008 SPYRUS, Inc. All rights reserved. SPYRUS, the SPYRUS logos, Security to the Edge, Hydra Privacy Card, Hydra PC, Signal Identity Manager, 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. Individual SPYRUS products may embody technology protected by one or more of the following patents or patent applications: U.S. Pat. Nos. 6,088,802; 6,003,135; 6,981,149; 5,761,305; 5,889,865; 5,896,455; 5,933,504; 5,999,626; 6,122,736; 6,141,420; 6,336,188; 6,487,661; 6,563,928; 6,618,483, U.S. Pat. Appl. Ser. Nos. 09/434,247; 09/558,256; 09/942,492; 10/185,735; Can. Pat. Appl. Ser. Nos. 2176972; 2176866; 2202566; 2174261; 2155038; 2174260; E.P. Pat. Appl. Ser. No. 96201322.3; 97106114.8; 96105920.1; 95926348.4; 96105921.9.

Document number 412-070101-02