SecureD™
Encryption Technologies




WHITEPAPER:

# SecureD Technical Overview

# WHITEPAPER: SecureD Technical Overview

## CONTENTS



Common Criteria
EAL 4+ Validated

FIPS 140-2
Level 3 Validated



US Office:
13000-F South Tryon Street, Suite #166, Charlotte, NC 28278, USA
Tel: +1-803-389-4799 | E-mail: mail@secured.no | www.securedhdd.com

Norway Office:
Vestre Strandgate 26, N-4611 Kristiansand, Norway
Tel: +47 38 10 44 80 | www.secured.no

## THE CHALLENGE TO PROTECT DATA AT REST 1

Safeguarding confidential data that resides on company-owned computers is a major security challenge facing public and private organizations alike. Today, confidential and sensitive data is in the custody and care of an increasingly mobile workforce, and no longer limited to desktop computers; employees bring their laptops back home and carry them on the road, thereby physically exposing confidential data to loss or theft. Data residing on office computers is also vulnerable to internal theft and unauthorized access to vital information such as unpublished research, source code and other intellectual property, customer personal information, employee records and financial reports.

All organizations have a financial and legal interest in preventing unauthorized access to sensitive information. The costs of stolen or lost confidential data increases as state and federal governments pass additional breach disclosure laws, and as many of these laws require notification and remediation when personal data is lost or stolen, data breaches can result in millions of dollars in customer notification costs, noncompliance fines, possible lawsuits, and company reputation damage.

How critical is this problem and what are the consequences of not doing anything about it? Numerous polls and studies all point to increased incidences of sensitive data lost or stolen from government organizations, academic institutions, and businesses. A recent Ponemon Institute survey of nearly 500 experienced information security practitioners revealed that 81 percent of the companies lost one or more laptop computers containing sensitive information during the previous 12 months.[1]

In a different survey, 95 percent of the businesses who experienced a data breach were, under state statutes or federal privacy acts such as HIPAA, GLBA and OCC, required to notify data subjects whose information was lost or stolen. Organizations that suffered a data breach incurred the following costs: 74% lost customers; 59% faced potential litigation, 33% faced fines, and 32% experienced a decline in share value.[2]

Data breaches are expensive. The survey found the average cost of a consumer data breach was $182 per record. An analysis of 31 different incidents revealed the total costs for each ranged from $226,000 to more than $22 million.[3]

## HARDWARE DATA ENCRYPTION PROVIDES MAXIMUM SECURITY 2

A logical solution to the problem of securing data at rest is to protect the data at its storage location. All data encryption products share the goal of encrypting plain text into a format that cannot be read by unauthorized people. Encrypting all the data on a disk, known as Full Disk Encryption (FDE), provides a barrier between unauthorized users and **all** data stored on the computer, including boot up system files and temporary files, which contain confidential data useful to attackers. No one can access any of the data on the drive until the encryption system has confirmed the user as authorized. The encrypted data must be decrypted to its original form in order to be read.

Encryption products fall into the categories of software- or hardware-based. It is beyond the scope of this document to weigh the benefits and disadvantages of each category. SecureD is hardware-based so the focus here is on its advantages.

Hardware-based encryption systems consist of a device that is physically installed in the computer, but operates independently of the computer's CPU, memory and storage. Physically separate "keys" are required to unlock the hard

[1] *U.S. Survey: Confidential Data at Risk.* Source: Ponemon Institute: August 2006

[2] *The Business Impact of Data Breach survey.* Source: Ponemon Institute and Scott & Scott LLP: May 2007

[3] *2006 Annual Study: Cost of a Data Breach.* Source: Ponemon Institute, PGP Corp. and Vontu, Inc.: October 2006

drive and enable decryption of the data. SecureD uses certified and secure Key Tokens (typically a Smart Card) to store and transport encryption keys.

The primary benefits of hardware-based encryption are summarized below, and the details of each feature will be described in subsequent sections of this document.

## Key Benefits of SecureD Hardware-Based Encryption

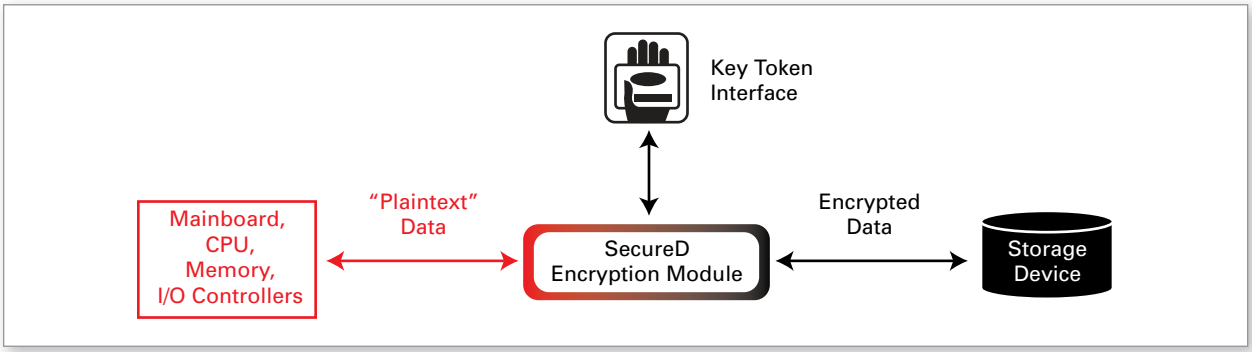
| | |
|---|---|
| **Maximum Data Security** | • Hardware encryption provides both a physical and logical barrier to intrusion, data theft<br>• Encrypted data can be unlocked only by using the correct "key" (Encryption keys stored in a key token)<br>• No software associated with SecureD is installed on the computer.<br>• Cryptographic keying materials are never stored in the computer's CPU, memory, or storage devices<br>• Cryptographic algorithms are inaccessible to processes running on the computer. |
| **Performance** | • The encryption hardware device is self-contained. It performs encryption independent of computer CPU and operating system so there is no performance degradation.<br>• Real-time encryption is performed on every bit of data before it is written to disk. There is no wait time when shutting down or starting up the computer. |
| **Efficient and Economical Implementation** | • Vendor independent – Install SecureD on any brand of computer, on any operating system, on any file system<br>• Install the SecureD device in the computer and start encrypting data. There are no software drivers to install.<br>• SecureD is transparent to users – Encryption is performed automatically and transparently. No user training beyond using the Key Token is required.<br>• Relative cost of protecting data on a laptop is low when compared to the costs of remediation. |
| **Auditable and Accountable Encryption Methods** | • Limits potential liability if the computer is lost or stolen. To prove lost data was encrypted, just provide the Key Token needed to decrypt the data. Data on an encrypted disk without the correct Key Token is inaccessible.<br>• SecureD always encrypts the entire disk; there is no option to perform partial encryptions.<br>• Human misuse or errors do not diminish the security of stored data. |

## SecureD ARCHITECTURE 3

SecureD is a hardware–based technology which encrypts all stored data on a computer. The SecureD device is connected in the data path between the hard drive controller and the hard disk drive, where data is stored. Encryption is performed on the entire disk, including boot-up information, swap space and temporary files. As users work, real-time encryption is performed on every bit of data as it is written to the hard disk.

User authorization is performed using Key Tokens. The key and disk pairing feature means that each SecureD encrypted disk can be unlocked by a specific key only. Users must use the correct Key Token in order to decrypt and access any data on the disk.

The following figure shows the SecureD product architecture. Inside the computer, the SecureD device, which contains a chip that performs data encryption, is placed directly in the data path between the motherboard and the storage device, to ensure every bit is encrypted as it is written to the storage disk.




## DESKTOP, LAPTOP AND EXTERNAL USB DRIVES 4

SecureD devices are available in three forms to facilitate deployment in a heterogeneous computing environment:

**SecureD Desktop:**
A PCI card that integrates with existing SATA hard drives

**SecureD Laptop:**
A completely integrated 2.5-inch, 60GB hard drive for laptop models


**SecureD USB:** An external 120GB drive that provides secure, portable data storage and backup

## 4.1 SecureD Desktop

Using the SecureD Desktop device with an existing SATA hard drive requires backing up the entire hard drive prior to installing SecureD, then re-imaging the hard drive after installing SecureD. This process is necessary because once the SecureD device is installed and activated using the Key Token, it attempts (unsuccessfully) to decrypt the existing unencrypted data on the hard drive. But, as re-imaging of the hard drive is performed, SecureD encrypts the data being written to disk. When the re-imaging is complete, all data on the drive is encrypted and work can proceed normally.

## 4.2 SecureD Laptop

The SecureD Laptop hard drive contains the integrated encryption chip and Key Token reader, and fits most laptops. The laptop drive offers full speed ATA 6-ATAPI performance with no degradation, and as the drive is unformatted, it is compatible with any operating system. After installing the hard drive in the laptop, format it and install the operating system and all application software. There is no SecureD software to install, so users can start working immediately.

## 4.3 SecureD USB

The SecureD USB drive is a USB 2.0 compatible external hard drive that contains the encryption chip and Key Token reader. Plug it into any USB 2.0 port, on any computer and operating system, and begin to store or transfer encrypted data in a portable format.

| ***SecureD System Specifications:*** | |
|---|---|
| **Authentication:** | Key Token (Smart Card) and dedicated reader |
| **Computer Requirements:** | Independent of computer make/model |
| **Operating System:** | Independent of operating system |
| **Device Driver:** | None required |
| **Software:** | None required |
| **Data Bus I/O Standard:** | ATA/ATAPI-6, SATA, USB |
| ***Encryption:*** | |
| **Encryption Engine Algorithm:** | AES (Advanced Encryption System) |
| **Encryption Strength:** | 256-bit cryptographic key length |
| **Encryption Speed:** | Real-time encryption |
| **Encryption Execution:** | Transparent to user |
| **Encryption Key Transport Algorithm:** | TDEA (Triple Data Encryption Algorithm) |
| ***Performance:*** | |
| **Data Speed Rate:** | Equivalent to data bus standards |
| **Operational Delay:** | None |

## USER AUTHORIZATION 5

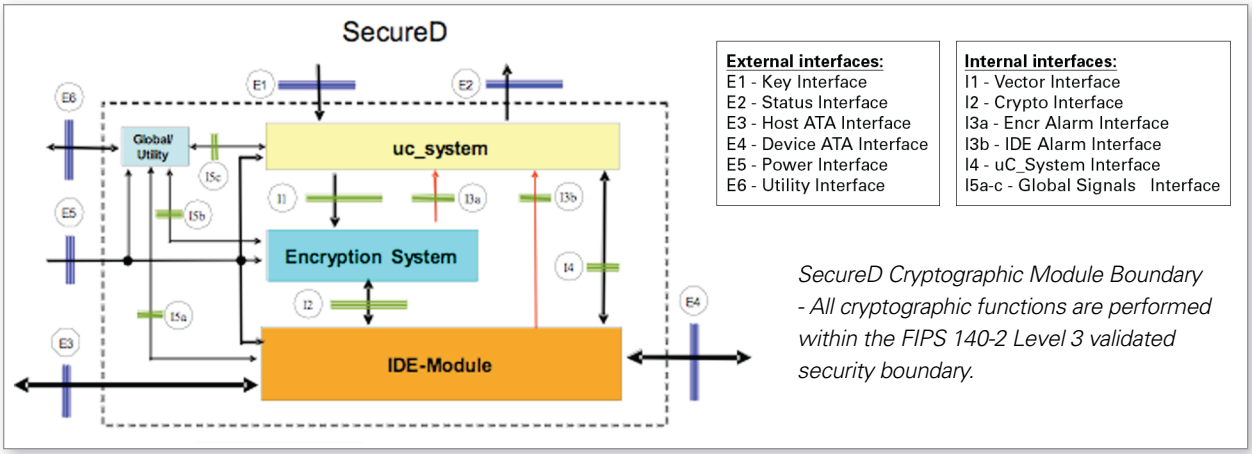
Each SecureD device ships with two Key Tokens (Smart Cards). Only these Tokens can unlock the data encrypted using this specific SecureD device, and users must insert the "User Key Token" in the reader in order to access the storage drive. The drive cannot start without the token, thus ensuring a stolen or lost hard drive remains physically secure and all the data on it remains encrypted. Depending on the operating system, unauthorized users who start the computer will see a blank screen and perhaps a message such as "Hard drive is inaccessible."

The Key Token transfers the encryption key at every startup. No keying material is stored in the computer CPU, memory, or storage devices or on the SecureD device, thus eliminating concerns about attackers obtaining encryption key information from the computer. Furthermore, the SecureD device halts immediately (optional through key parameter setting by key manager) if the key is removed from the reader. Real-time encryption ensures all data is protected and inaccessible.

## MEASURABLE, IMPENETRABLE SECURITY 6

SecureD provides Full Disk Encryption using strong encryption methods that meet globally-recognized encryption standards:

- **Encryption Algorithm:** Advanced Encryption Standards (AES) Implemented (NIST Certificate #383). SecureD uses this 256-bit data encryption method which is the U.S. federal government standard. The certificate of compliance is issued by the National Institute of Standards and Technology (NIST).
- **Encryption Strength:** 256-bit key length. Key length, the digit size used to create encrypted text, is a primary indicator of security strength. The longer the key, the harder it is to decipher. The current maximum AES 256-bit key length meets the U.S. government requirement for encrypting military graded data.
- **Physical Security:** FIPS 140-2 certified to Level 3, tamper evident (NIST Certificate #717). The U.S. federal government issues FIPS (Federal Information Processing Standards) 140-2 security requirements for cryptography products. SecureD is certified to Level 3, meaning it is physically tamper-resistant, provides identity-based authentication and has a physical separation between the interfaces by which critical security parameters enter and leave the encryption module and other interfaces. The following figure shows the SecureD encryption module with its cryptographic boundary clearly outlined.




*SecureD Cryptographic Module Boundary - All cryptographic functions are performed within the FIPS 140-2 Level 3 validated security boundary.*

### 6.1 SecureD Certifications

- FIPS 140-2 Level 3 Validated (NIST Certificate no. 717)
- Common Criteria EAL4 / ISO 15408-3 (Certificate no. CCEVS-VR-05-0141)
- Common Criteria EAL4+, augmented with AVA_VLA.3 (Certificate no. CCEVS-VR-06-0047)
- CMMI Maturity Level 2

## ENCRYPTION WITH NO PERFORMANCE COSTS 7

All key-reading and data encryption processes occur within the SecureD device, independent of the computer CPU. Unlike software encryption, which depends on CPU cycles, SecureD performs real-time data encryption on both ATA-6/ ATAPI and serial ATA without affecting the computer's performance.

## STREAMLINED, COST-EFFECTIVE IMPLEMENTATION 8

SecureD can be installed on any brand computer and on any operating system, making it easy for an organization to standardize its data encryption method. SecureD can be installed on existing systems in the field. Also, there is no annual licensing fee for SecureD.

No end user training is required, apart from how to use the Key Token. SecureD operates transparently to users; it generates no logs, errors or messages.

SecureD's transparent, independent operation enables IT professionals to upgrade operating systems and application software without stopping SecureD. Furthermore, fully-encrypted disks make computer repairs and recycling safer and less expensive.

## LIMITING POTENTIAL LIABILITY 9

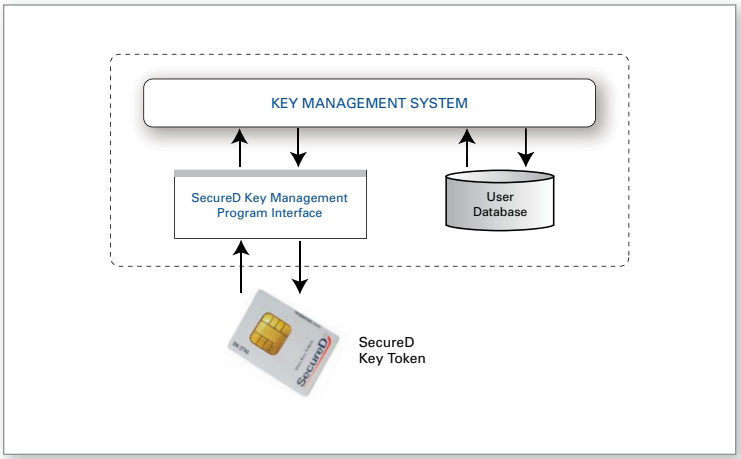
Federal and state legislation aimed at protecting personal identity data on computers is gaining widespread attention from government agencies, corporations and the general public. There is increasing pressure on the data custodians to notify individuals affected by a data breach, as well as to perform remediation for personal data exposure. Data breaches can cost a company millions of dollars in customer notification programs, noncompliance fines, lawsuit resolutions and restoring its public image.

When a computer with confidential data is lost or stolen, the organization that owns the computer can usually limit its liability by proving the data was encrypted at the time of loss. SecureD provides Full Disk Encryption at all times, and cannot be disabled, thus eliminating any potential claims of partial disk encryption. Moreover, to prove the data is encrypted, the owner need only provide the Key Token required to unlock the missing hard drive. Physical separation of the locked drive and its required key should be sufficient evidence to prove the missing drive is secure and tamper-resistant.

## ONSITE KEY MANAGEMENT SYSTEM 10

Each standalone SecureD device comes with two Key Tokens, one for use and one for backup. However, larger organizations find it efficient and secure to create and manage their own Key Tokens on-site using the SecureD Key Management System (KMS). Use the KMS to replace lost or damaged tokens and create tokens for new employees.

KMS is a software application that is installed on a dedicated computer along with a Smart Card reader/writer. For security reasons, it is always recommended to install SecureD on the KMS and store it in a physically-secured room. A designated Crypto Officer is the only person authorized to use the KMS.




## SecureD ADVANCED FEATURES 11

- The SecureD Key Management API is available to integrate SecureD management operations with other security management applications
- A wireless key technology will be released soon. Instead of inserting the Key Token into the Smart Card reader, users can push a button on a small device that resembles a remote car key, to perform remote authorization and start the hard drive.