

# WHAT YOU NEED TO KNOW

## > Why Encrypt Data Written to Tape Cartridges?

**For Security** — Tape encryption prevents business data from being compromised in the event that tapes are lost or stolen at your location, or while in transit.

**For Cost-effective and Secure Data Shipment** — Data encrypted on tape provides a secure and cost-effective means of transporting large amounts of data offsite — for backup, information distribution to satellite offices or branches, or for information exchange with a partner.

**For Compliance** — Data retention policies can be managed effectively to meet federal/business regulations and requirements. You can set expiration dates for encrypted data and ensure that data is irretrievable after the expiration dates by destroying the associated keys.

**To Reduce Complexity** — secure your data in a heterogeneous host environment. By implementing encryption in the tape drive with an environment agnostic key management appliance, data in a heterogeneous host environment is secured in a simplified manner.

## > The Data Security Landscape

Businesses are more vulnerable than ever to data exposure or loss, which is understandable when you consider the typical exchanges of data required to grow, to communicate with partners, to manage costs, and to comply with regulations. Newspaper headlines frequently lead to stories about security breaches and lost data. Consider these facts:

> January 2005 to July 2007 – 158 million individual Americans’ personal data exposed. Estimated cost per breached individual (Ponemon Institute) = \$182 total cost x 158M people = \$28.7 billion.<sup>1</sup>

What are the business consequences of lost or compromised data in your company? Lost customers? Damaged public image? Lost revenues?

Check your company’s financial exposure in the event of a breach:  
<http://informationshield.com/privacybreachcalc.html>

Law/Regulation	Penalty	Fine
Sarbanes-Oxley	20 years in prison	\$15 Million
Gramm-Leach-Bliley	10 years in prison	\$1 Million
USA Patriot	20 years in prison	\$1 Million
HIPPA	10 years in prison	\$100 per violation; \$25K cap per year
SEC rule 17a-14	Suspension/Expulsion	\$1 Million

<sup>1</sup> Sources: Privacy Rights Clearinghouse and Ponemon Institute

## > Key Encryption Terms

**Cryptography** — The practice and study of encryption and decryption — encoding data so that only specific individuals can decode it. A system for encrypting and decrypting data is a cryptosystem. This usually involves an algorithm for combining the original data “plaintext” with one or more “keys” — numbers or strings of characters known only to the sender and/or recipient.

**Encryption** — Any procedure used in cryptography to convert plaintext into ciphertext (encrypted message) in order to prevent anyone except the intended recipient from reading that data. Schematically, there are two classes of encryption primitives: public-key cryptography and private-key cryptography. They are generally used in complement.

**Federal Information Processing Standard (FIPS)** — U.S. government technical standard published by the National Institute of Standards and Technology (NIST). NIST develops a FIPS when there are compelling federal government requirements, such as for security and interoperability, but no acceptable industry standards or solutions. Computer-related products bought by the U.S. government must conform to FIPS.

**Key Management** — The system used to securely manage, administer, distribute, and store encryption keys.

**Private-Key Cryptography** — Also known as symmetric-key cryptography. This approach uses a class of cryptographic algorithms to encrypt data that requires a shared secret key. The same key is used to encrypt and decrypt the data, and it must be kept secret. Symmetric-key cryptography is typically used to encrypt bulk data because it is much less computationally intensive than asymmetric-key cryptography. Symmetric-key algorithms are not always used alone. In modern cryptosystem designs, both asymmetric (public-key) and symmetric algorithms may be used, taking advantage of the virtues of both. Asymmetric-key algorithms are one way to ensure secure key distribution for faster symmetric-key algorithms.

**Public-Key Cryptography** — Also known as asymmetric-key cryptography. This approach allows users to communicate securely without having prior access to a shared secret key. A pair of cryptographic keys, designated as public key and private key, are related mathematically. In public-key cryptography, the private key is kept secret while the public key may be widely distributed. One key “locks” a lock while the other is required to unlock it. Public-key cryptography is computationally very intensive and therefore not typically used to encrypt bulk data. Instead, it provides one way to operationally and securely transmit symmetric keys that have been used to encrypt bulk data. There are ways to securely transmit keys which do not require public-key cryptography.

**Token** — A hardware device that is used to authenticate its owner to computers and applications on a network. A token can be a one-time password generator, a physical device that plugs into a socket, a smart card that is run through a reader, or another similar device.

## Engage the Storage Experts

Sun StorageTek service professionals can help you pinpoint opportunities to reduce costs, mitigate business risk, and better leverage information assets. Covering over 125 countries, more than 2100 dedicated storage service professionals can help you gain and sustain measurable results with the reliability and flexibility that you require.



# KEEPING YOUR DATA SECURE

Trust Sun StorageTek™ Encryption Solutions  
[sun.com/encryption](http://sun.com/encryption)



© 2007 Sun Microsystems, Inc. All rights reserved. Sun, Sun Microsystems, the Sun logo, StorageTek, and the StorageTek logo are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. Information subject to change without notice.

09/07 SunWIN# 481185 Lit# STBR12060-0



## Sun Security — A Technical Foundation for Managing Data Security

Managing risk, cost, and complexity effectively requires achieving a careful balance across business, operational, and technical boundaries. Architectures must be sufficiently flexible to respond to ever-changing business opportunities, policies, regulatory pressures, and threat profiles.

Security should be built into your datacenter. Unfortunately, however, many of today's data storage IT infrastructures were put in place long before security and compliance requirements became the leading considerations in implementation decisions. As a result, organizations now need to retrofit their current environments to address deficiencies and support stronger security, privacy, and compliance practices.

Sun is the ideal technical adviser to help you deploy the infrastructure best suited to sustainable risk management and compliance:

- > We can help you plan and integrate better security into your existing IT infrastructure and engender trust from customers, employees, and business partners.
- > We can help you maximize the efficiency and value of your IT investments — bolstering security and accountability without paying for a lot of extras.
- > We can make it easier and faster to build secure systems and face new challenges. Our secure-by-design building blocks make security and compliance simpler to implement.

### Sun's Unique Encryption Approach, Revealed to You

Within the data security landscape, encryption not only solves the current problem of data getting into the wrong hands, but also forms the basis for an effective data access management system through rules-based key management.

Over time, key management can enable an effective, automated method to manage data in contrast to the manual effort required to track and eventually delete the data.

Encryption can be implemented across the system stack. Where you choose to encrypt your data depends on an assessment of both the areas of risk to your data security and the business compliance requirements. The critical challenges customers face are how to avoid ending up with islands of encryption solutions and how to manage what can be millions of keys across encryption points during the years that data is retained. Some questions to consider:

- > What are the security threats and compliance-related requirements?
- > Where should you encrypt the data to best satisfy security and compliance requirements within your existing environment?
- > How do you want to manage the keys associated with your encrypted data?

Contact your Sun account manager for more information or see [sun.com/encryption](http://sun.com/encryption) for more information.

## The Most Secure Data Encryption Solution

Sun offers you the ability to encrypt the data at creation, in-band, or where the data is stored. The decision really depends on your security requirements.

### Encryption at the point of data creation: host/application/software-based encryption

When data is encrypted at creation, it has almost no chance of being deciphered — even if data is intercepted. While host-based encryption is a highly secure approach, you do need to keep these considerations in mind:



Sun Cryptographic Accelerator 6000

- > Software-based encryption typically comes with a significant performance trade-off.
- > Hardware-based encryption, for example, with a cryptographic accelerator card, can alleviate much of the performance impact of host-based encryption but requires that the system accommodate the hardware with adequate slots. There's also cost and complexity associated with managing the cards.
- > Hardware-based encryption at the host may not easily accommodate encryption requirements in a heterogeneous host environment.

> Encrypting on the host may add significant storage cost. Once encrypted, data cannot be compressed, so storage needs could more than double.

**Bottom Line** — Host-based encryption is the most secure option if your primary concern is internal loss or theft of data. However, it may compromise performance and introduce unnecessary complexity, and it may not be the right solution for a heterogeneous host environment.

### In-band encryption

In-band encryption is when data is encrypted as it is transported from the point of its creation to its destination. Data leaves the host unencrypted and moves to a dedicated appliance where it is encrypted before it is transmitted onto a storage device such as disk or tape. The advantage of the encryption appliance approach is that it can typically be placed into an existing environment with little disruption. However, trade-offs for ease of deployment may include:

> Scalability and cost — Typically, the appliance approach is not as scalable as in-device encryption, and there is greater cost to add encryption appliances.



> Security — Encryption at the appliance is not as secure as encryption at the host since data has to move across the wire between the host and the appliance in clear text.

**Bottom Line** — In-band encryption can be easy to implement, and it is well suited for quick localized encryption. However, it may not meet long-term scalability requirements for secure data retention, especially given budget constraints.

### In-device encryption

Device-based encryption, such as encryption in a tape drive, is the right choice when the primary security threat is to data being stored on removable, portable media. Device-based encryption is advantageous in heterogeneous host environments and in the tape drive because data can be compressed prior to being encrypted, maximizing tape utilization.

If you are concerned with data being compromised internally (during transmission) prior to reaching the storage device, you may want to employ more than one method or point of encryption.

**Bottom Line** — Device-based encryption is the right solution when the primary security threat occurs with the utilization of removable media. This method of encrypting data in the tape drive is a straightforward and cost-effective way to secure data.

## Tape Device Encryption

Implementing Sun's tape-based encryption solution requires three elements:

- > Sun StorageTek Crypto-active T10000 tape drives
- > A Sun StorageTek Crypto Key Management Station, which includes a token bay and token for safe key storage and transportation of keys.
- > Appropriate accessory kit for the library platform
- > KMS Integration Services



## Encryption and Key Management

Regardless of where data is encrypted, access to data is controlled with a cryptographic key. Lose a key and you lose your data. Therefore, the choice of the right key management solution is one of the most important aspects of data security. A successful key management strategy



enables continuous authorized access to data with the highest level of security required with minimum complexity. A key management solution today should include the ability to:

- > Create and edit operator roles
- > Generate keys and create key sets
- > Distribute keys
- > Manage key rotation and retirement
- > Backup and restore secure key database

> Provide a tamper-resistant log capability for auditing purposes

> Be able to grow into a centralized key management station to manage keys across encryption points in the enterprise

## Engage Now with Sun

Sun's storage encryption professionals can help you replace guesswork with facts. They can provide you with the tools, roadmaps, and recommendations necessary to address risks, establish management policies, and create an ongoing approach to securing one of your corporation's most valuable assets — data. Sun Professional Services can help you with the following practices:

**Information Security Readiness** — A readiness plan for use in preparation for implementation of an encryption solution.

**Key Management** — Identification of best practices of encryption key management systems to meet security and business requirements.

**Operational Policy** — Recommendations on process and policy enhancements needed to handle backup and recovery of encrypted data.

**Role Management** — Role-based guidelines for managing an encryption-based security plan.

**Resilience to Risk** — Encryption-based data recovery practices and course of action for data recovery.