

# SUN STORAGE TEK™ CRYPTO KEY MANAGEMENT SYSTEM

Selecting an Appropriate Encryption Method for the  
Enterprise Environment

White Paper

January 2008

## **Abstract**

The legal and financial consequences of foregoing data encryption in the enterprise are considerable. Businesses must identify and evaluate their data encryption needs to balance the security, performance, interoperability, scalability, and ease of management of the solutions available. While in-band and appliance-based encryption have their place, most organizations will conclude that storage device-based encryption solutions, such as the Sun StorageTek™ Crypto Key Management System, offer the greatest simplicity, security, and scalability.

## Table of Contents

Executive Summary.....	3
1 Catalysts for Implementing Encryption in the Enterprise .....	4
Business Risks: Why Your Organization Cannot Afford Not to Encrypt.....	4
Direct Losses.....	4
Indirect Losses .....	4
Legal Exposure.....	5
2 Safeguarding Data in the Enterprise: An Encryption Architecture Overview.....	6
Host-Based Encryption.....	6
In-Band Appliance-Based Encryption.....	7
Device-Based Encryption .....	8
3 Key Issues to Consider When Selecting an Encryption Solution .....	9
Identify and Evaluate Risks to the Organization .....	9
Identify Encryption Requirements .....	9
Determine Acquisition Costs .....	10
Confirm Interoperability with Existing Hardware and Software .....	10
Research Vendors' Implementation Process and Requirements .....	11
Identify Effects on Current Data Management Policies.....	12
Compare Vendors' Key Management Features and Flexibility .....	12
4 How the Sun Encryption Solution Helps Your Organization Meet the Challenges of Implementing Encryption in the Enterprise .....	13
Compliance .....	13
Interoperability.....	13
Implementation.....	14
Data Management Policy .....	15
Key Management.....	15
5 Summary.....	16
Encryption Terms .....	16

## Executive Summary

From January 2005 to December 2007, an estimated 216 million unencrypted records containing sensitive personal information have been lost in the United States due to data breaches<sup>1</sup>. The consequences of losing sensitive unencrypted data, either by error or through a malicious act, can be devastating to your business. The financial exposure for an organization can run into the tens of millions of dollars, and the legal repercussions — including lawsuits and criminal prosecution — can jeopardize the very future of a business.

Depending upon the size and nature of your business, your organization must determine the most cost-effective and least disruptive method of data protection. While host-based and in-band appliance-based encryption have their place, most businesses require a level of scalability and interoperability that may go beyond the capabilities of these solutions.

Sun offers a simple, secure, and scalable encryption solution that addresses the needs of entry- to enterprise-level data environments, while providing excellent value and the highest levels of security. And, Sun Encryption Consulting Services are ready to help your organization assess its encryption readiness, needs, and risks to help quickly tailor a custom solution that is easy to implement, manage, and grow. In fact, Sun can help your organization evaluate your current infrastructure and implement a fully operational, highly secure encryption solution in fewer than 21 days.

The time to encrypt is now. With Sun as part of your team, you can bring the protection and peace of mind of data encryption to your organization and customers in less than a month.

<sup>1</sup> Privacy Rights Clearinghouse. (2008). "A chronology of data breaches." Retrieved from <http://www.privacyrights.org/ar/ChronDataBreaches.htm#Total>.

## 1 Catalysts for Implementing Encryption in the Enterprise

Over the past several years, it's been nearly impossible to miss the steady drumbeat of news stories reporting very large, very public losses of sensitive data. Since it began keeping track in 2005, the San Diego-based Privacy Rights Clearinghouse estimates that in the United States alone, over 216 million electronic records containing sensitive, personal information have been lost due to data breaches<sup>2</sup>. Regardless of whether the electronic data was lost through error or malice, these breaches share one alarming characteristic: not a single byte of the lost information was encrypted.

By encrypting at-rest data, your organization can greatly reduce the risk of financial devastation, loss to reputation, and civil or criminal penalties associated with data breaches.

### Business Risks: Why Your Organization Cannot Afford Not to Encrypt

If your organization is part of the estimated 60 percent<sup>3</sup> of US businesses that does not encrypt at-rest data, it is at serious risk. With the vast quantity and variety of storage devices in use within any modern organization, the potential for losing data due to human error or theft is very real. The consequences of such losses can be staggering and fall into three main categories: direct losses, indirect losses, and legal exposure.

#### Direct Losses

In May 2007, a large French telecommunications company announced that an unencrypted tape backup containing as many as 200,000 records of former and current employees and their dependents disappeared in transit from one vendor to another. The lost data included names, addresses, social security numbers, dates of birth, and salary data<sup>4</sup>.

When unencrypted data is involved, a misplaced tape archive or stolen hard disk can result in unauthorized access to intellectual property, customer data, or employee records, compromising your organization's competitiveness and exposing staff, their families, and customers to identity theft.

#### Indirect Losses

The consequences of losing unencrypted data often reach beyond the initial loss itself. Once made public, the data leak can create a public relations crisis leading to loss of customer confidence, negative brand perception, decreased competitive advantage, and ultimately, a drop in sales revenue that can cost an organization millions of dollars.

For instance, in 2006 a Connecticut-based bank lost a backup tape containing names, addresses, checking account and social security numbers for more than 90,000 customers. The tape was sent to a credit bureau using a commercial shipping company, but it disappeared in transit. While there is no evidence that the unencrypted data was stolen or used in an illegal manner,<sup>5</sup> the highly publicized breach forced the bank to offer credit monitoring and restoration services to its customers for one year and hire a large IT consulting firm to conduct an end-to-end security audit<sup>6</sup>.

<sup>2</sup> Ibid.

<sup>3</sup> Olsik, J. (2007). "Hot spots: the inevitability of tape encryption." Retrieved from [http://searchStorage.techtarget.com/magazineFeature/0,296894,sid5\\_gci1263665,00.html](http://searchStorage.techtarget.com/magazineFeature/0,296894,sid5_gci1263665,00.html).

<sup>4</sup> Joyce, E. (2007). "Alcatel-Lucent probing loss of employee data." Retrieved from <http://www.internetnews.com/security/article.php/3678736>.

<sup>5</sup> Lawson, S. (2006). "Bank tape lost with data on 90,000 customers." Retrieved from [http://www.infoworld.com/article/06/01/11/73831\\_HNbankdatalost\\_1.html](http://www.infoworld.com/article/06/01/11/73831_HNbankdatalost_1.html).

<sup>6</sup> Greenemeier, L., Malykhina, E., McDougall, P., Ricadela, A., & McGee, M. K. (2006). "The high cost of data loss." Retrieved from <http://www.informationweek.com/story/showArticle.jhtml?articleID=183700367&pgno=2>.

## Legal Exposure

Losing sensitive, unencrypted data also creates a very real potential for legal repercussions such as state or federally imposed fines, civil litigation, and even criminal prosecution. In the past several years, the number of laws and regulations governing on- or off-site data loss has expanded considerably and in many cases require that organizations report data breaches to state agencies and notify individuals affected by the loss.

For example, the United States and a number of other countries have passed laws that establish specific guidelines for handling sensitive data and levy stiff penalties against individuals and organizations that fail to do so. Some of these laws include:

- Sarbanes-Oxley (US)
- Heath Insurance Portability and Accountability Act (US)
- Gramm-Leach-Bliley Act (US)
- USA PATRIOT Act (US)
- Personal Information Protection and Electronic Documents Act (Canada)
- Data Protection Directive (European Union)
- Personal Information Protection Act (Japan)
- Personal Data Protection Code (Italy)

In addition, California Senate Bill (SB) 1386 requires notification of affected California residents any time an organization has reason to believe that unencrypted personal data has been lost or stolen. As of December 2007, 38 states have enacted notification laws modeled after SB 1386.<sup>7</sup>

When combined, these federal and state laws set the stage for very costly public disclosures and remedies any time an organization loses unencrypted personal data. In instances when the number of affected individuals is in the tens or hundreds of thousands, mail or email notification programs can be prohibitively expensive and time consuming. In some cases, organizations that have lost sensitive, unencrypted data may have to rely upon mass media advertising campaigns to reach affected individuals in a timely manner.

By encrypting at-rest data, your organization can greatly reduce the risk of financial devastation, loss to reputation, and civil or criminal penalties associated with data breaches.

<sup>7</sup> National Conference of State Legislatures. (2007). "State security breach notification laws." Retrieved from <http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm>.

## 2 Safeguarding Data in the Enterprise: An Encryption Architecture Overview

There are three approaches to encryption in the enterprise:

- **Host-based** — Also called server-based encryption, data is encrypted as it is created
- **In-band appliance-based** — Providing network-level protection, data is encrypted en-route between the point of creation and its ultimate destination
- **Storage device-based** — An efficient, scalable method of encryption, data is encrypted at the tape drive or within a storage device

Together, these three methods allow your organization to choose how, when, and where it will encrypt data. But, depending on a range of factors, including the size of the organization, quantity of data that must be encrypted, and installed hardware base, you'll quickly find that one of these methods will address your business and data center needs more effectively than the others.

For example, while host- and in-band appliance-based solutions are appropriate for some data centers, most businesses ultimately conclude that the drawbacks outweigh the benefits.

The following sections will examine the advantages and disadvantages of each encryption method.

### Host-Based Encryption

Host-based encryption may be an appropriate solution for small, active data sets. But, intensive processor requirements, lack of compression capabilities, and interference with de-duping solutions limit its usefulness in the enterprise.

Host-based encryption provides organizations with the highest levels of security because the data is encrypted at the point of creation. Encrypting information in this manner eliminates the risks associated with an accidental or malicious interception of data along the data path, including the loss or theft of removable storage media. Even if an unauthorized user accessed the data during transport, encryption would render it unreadable and unusable.

Host-based encryption is a good choice for businesses that work with small, highly critical, and active data sets (such as databases that change constantly). Also, because encryption is accomplished at the host, this solution is independent of any storage devices used within the enterprise.

On the other hand, because encryption can increase processing overhead by as much as 40%, organizations encrypting large amounts of information must choose between slower processor performance — and the potential for longer backup windows — or investing in additional server hardware and space in the data center to maintain comparable computing power after implementing a host-based encryption solution. Therefore, this method is not a good fit for organizations encrypting large quantities of data, especially data at-rest.

Because encrypted data is random and cannot be compressed, host-based encryption typically requires two to four times more storage capacity than other encryption methods, driving up the cost to archive critical data. Unfortunately, compressing data at the host before encryption degrades processing performance even more than encryption alone.

In-band appliance-based encryption is useful with legacy storage devices that do not have built-in encryption support. But high acquisition and operation costs coupled with scalability and security shortfalls limit the utility of these appliances.

Another drawback is that in most cases host-based encryption will effectively neutralize any de-duplication solutions deployed in the enterprise. To work effectively, de-duplication must be able to access and compare unencrypted data to determine if it is redundant. If the data is encrypted upon creation, the de-duplication solution is unable to process the data, identify redundancies, and purge them from the system.

Finally, host-based encryption may be dependent on specific operating systems or applications. In some instances, upgrading the system environment or an application may introduce issues with backward compatibility that affect every server in the enterprise. To resolve these issues, IT administrators may need to engage in a time-consuming, hands-on process of applying patches and implementing workarounds.

## In-Band Appliance-Based Encryption

Like host-based encryption, in-band appliance-based solutions can work with virtually any storage device in the enterprise. This cross-compatibility allows an organization to write encrypted data to any storage device, specifically to those that do not have built-in encryption support (such as legacy tape drives, disks, and so on). Yet, unlike host-based methods, these dedicated appliances encrypt data after the point of creation but before it is written to a storage device.

In-band appliances allow an organization to encrypt to low-performance storage devices without experiencing any degradation to CPU performance or data throughput. Typically, these devices are simple to integrate into an existing network; if an organization requires one or two of these devices in the data center, the time and effort needed to install and configure the appliances is minimal.

Still, in-band appliance-based encryption has a variety of drawbacks. For instance, the plug-and-play design of the appliance allows it to be bypassed — either intentionally or unintentionally — simply by disconnecting the device from the network. If the appliance were detached from the network, an organization could unknowingly write unencrypted data to disk or tape, leaving your business exposed to a variety of serious risks should the non-encrypted information be lost or stolen.

In-band appliance-based encryption is not scalable. Most in-band appliances operate at 2Gb Fibre Channel speed with approximately 150 MB/second throughput, while high performance drives commonly found in the data center are capable of 120 MB/second throughput. So, while an in-band appliance is capable of supporting a faster drive operating at full speed, it requires one appliance per drive to do so. If your organization has many high throughput storage devices, the cost of implementing in-band appliance-based encryption adds up quickly. And the expense is not limited to acquiring the appliances. For each in-band device your organization adds to the enterprise storage infrastructure it can expect a range of additional costs, such as:

- Appliance installation
- Software Licensing
- Warranty plans
- Maintenance and service
- Controls and policies for physical and logical access
- Floor space in the data center
- Power requirements for processing and cooling
- Upgrades

In many cases, IT administrators in large data centers will need to increase their workforce to support these implementations, thereby increasing staffing overhead.

In-band appliance-based devices are essentially stopgap solutions that allow businesses to encrypt to older storage devices that do not have built-in encryption support. In the next few years, as most organizations complete the transition to encryption-enabled tape and disk controllers, in-band appliances may become obsolete. And, with decreased demand for these devices, it is possible that manufacturers may eventually stop selling in-band appliances.

## Device-Based Encryption

Device-based encryption is a scalable and secure approach to data protection. Because it uses the built-in encryption capabilities of newer tape or disk hardware, it has virtually no affect on processor performance.

Device-based encryption is an efficient and cost-effective approach that allows organizations to avoid the pitfalls associated with host-based or in-band appliance-based methods. Because device-based encryption takes advantage of encryption capabilities built directly into the tape drive or disk hardware, there's no need to add costly applications or appliances to protect your organization's data.

And, unlike host-based encryption, device-based methods support data compression and have virtually no affect on processor performance. That means your organization can encrypt all the data it requires without encountering the processor slowdowns or costly additional hardware acquisitions as with a host-based solution.

On the other hand, device-based encryption is an evolving technology, and there are currently a limited number of storage devices that support internal encryption. But as the number of supported devices increases, so too will the scalability of device-based encryption solutions.

## 3 Key Issues to Consider When Selecting an Encryption Solution

To select an appropriate encryption architecture for your organization, work with management and vendors to gather some critical information, such as:

- Risks to be mitigated by using encryption
- Encryption requirements in the enterprise
- Acquisition, implementation, administration, and operating costs
- Interoperability
- Implementation processes and requirements
- Effects on current data management policies
- Flexibility and scalability of the solution

When considered together, these factors will help drive the enterprise to select the best architecture for its specific requirements. The sections that follow provide your business with a checklist of key issues and criteria that you can use to compare host-based, in-band appliance-based, and device-based options.

### Identify and Evaluate Risks to the Organization

To determine which encryption method is best suited for your organization, you should first identify the most prevalent risks to your business. For example, an enterprise that requires employees to store sensitive data on laptops may have different encryption needs than one that routinely transports data between satellite offices or third parties using tape media.

List and rank the potential threats, based on the probability and cost of occurrence, to identify your highest priorities and vulnerabilities. Then select an encryption solution that addresses your greatest needs.

### Identify Encryption Requirements

Depending on the business type as well as internal policies set by management and legal counsel, your organization may need to encrypt either all of the data in the enterprise or merely a subset. In many cases, you can streamline this decision making process by selecting an encryption architecture that can encrypt all data, eliminating the risk that some sensitive data is overlooked and stored as clear text.

Next, consider how each encryption solution will affect disaster recovery (DR), data sharing with third parties, or data sharing between your organization's satellite offices and primary data center. For example, the encryption architecture deployed in the data center must be duplicated and supported in any DR or satellite locations. A solution that uses a single key management platform — rather than a collection of disparate key management devices — greatly simplifies the task of supporting encryption across multiple sites. Likewise, if your organization shares data with third parties, it will need to be able to exchange and read encrypted data easily and inexpensively. The simplest way to enable sharing of encrypted data while keeping costs to a minimum is to choose a solution that is designed using an open architecture that will support interoperability standards as they emerge.

Choosing the most suitable encryption solution requires careful planning.

Your organization must identify the greatest areas of risk as well as the type and quantity of data that should be encrypted.

Once your organization has determined what data it will encrypt and how the encrypted information will be made available to DR sites or third parties, it will need to consider how each of the architectures will affect current processes and data management policies. Ultimately, the best solution for your organization will provide the most complete protection with the least amount of disruption to the enterprise or its ability to share and transfer encrypted data.

## Determine Acquisition Costs

Regardless of the architecture, any encryption solution will likely require a number of capital expenditures. Consider the additional technology that your business will need to purchase to deploy a solution successfully, such as:

Compare the acquisition costs for each prospective solution to determine which encryption method provides the best protection with the fewest requirements for additional hardware and software.

- Servers
- Appliances
- Tape libraries and drives
- Device controllers
- Software and related licenses
- Key management platforms

The best way to balance cost and security is to seek out vendors and encryption solutions that require a minimum of additional hardware and software to fulfill the encryption needs of your business. To control your operating costs, avoid encryption solutions that require your organization to purchase a large number of new servers, encryption appliances, software licenses, tape drives, or media and key managers.

Also, the design and implementation phases of the encryption deployment may represent another sizable cost to the enterprise. Be sure to ask if the vendor offers design and implementation services at a flat price or if it requires ongoing managed service agreements.

Control your costs by looking for vendors that measure their professional service engagements in days — not weeks or months. Identify vendors that offer a single, simple fee-based contract for the entire implementation, and steer away from those that require multiple statements of work or ongoing service contracts.

## Confirm Interoperability with Existing Hardware and Software

The encryption solution your organization selects should be designed to not only work with existing hardware and software in the data center, it should also allow your business to add new and varied storage devices as needed with minimal disruption and maximum interoperability.

Before choosing a solution, be certain that the key managers and encrypting devices you select are truly interoperable. For example:

- Key managers should be designed to operate seamlessly with multiple storage devices and device types, as well as support a wide range of vendors' products
- Encryption devices (such as disk controllers, in-band appliances, and so on) should work with multiple key manager vendors and products

If a solution your organization is evaluating is not built to support this level of cross-compatibility, be sure to ask the vendor about what safeguards, if any, are in place to prevent your organization from being locked into a proprietary architecture or multiple, standalone clusters of vendor-specific solutions. Whenever possible, avoid solutions that have the potential to create fiefdoms of encryption devices throughout the enterprise, each with its own management requirements, such as:

- Software or hardware licenses
- Compatibility issues
- Additional space in the data center
- Specially-trained IT resources to administer and maintain the solution

Check with potential vendors to understand their approach and commitment to interoperability. Confirm that the vendor has a track record of developing interoperable storage devices and is working with a variety of well-established storage and encryption partners toward developing open APIs rather than following a product roadmap that uses closed, proprietary systems designs.

Seek out encryption solution providers that have a history of developing interoperable storage devices and are committed to establishing formal standards across the storage industry.

Next, confirm with prospective vendors that they are devoted to establishing formal standards across the storage industry and are actively working with key standards committees, such as:

- IEEE 1619.1 — Tape Encryption Standard
- IEEE 1619.2 — Disk Encryption Standard
- IEEE 1619.3 — Common Standards for Key Management and Transmission
- T10 — SCSI Protocols Standards
- TCG — Trusted Computing Group
- OASIS — Common Standards for Key Management

## Research Vendors' Implementation Process and Requirements

Depending upon the vendor and solution, deploying encryption in the enterprise can be either:

- a lengthy, complex, and disruptive process or
- accomplished in a matter of days with negligible downtime or changes to your organization's data infrastructure.

When researching prospective vendors, learn all you can about the implementation process.

For example, from a software application perspective, determine if or for how long your business will be required to take applications or software offline while the solution is installed. Be sure to assess the cost and effort associated with auditing the current configuration to ensure the appropriate versions of operating systems, applications, and microcode are installed on all affected backup and media servers. Determine if updating software or microcode within the solution will cause interoperability problems that require additional upgrades (or downgrades) to operating systems, applications, device drivers, or device controller hardware to maintain compatibility throughout the data center.

You'll also need to find out if any solutions require physical connections or reconfigurations to the existing environment. If so, determine if the physical changes to the network might cause your organization to dismantle all or part of the Fibre Channel network and force your staff to rebuild the fabric before your business is fully functional again.

In short, after analyzing various vendor solutions, your organization should have a clear idea of which implementation will cost the least in terms of downtime and disruption to the business.

### Identify Effects on Current Data Management Policies

Before selecting an encryption solution, determine if a particular deployment will require special training or skills to administer the new hardware or software that make up the solution. Also, you will want to evaluate the complexity and scope of asset management, warranties, and maintenance contracts for each prospective vendor and solution.

If the implementation is overly complex or has many touch points, your business may need to hire additional staff to manage it, adding to the overall cost of the solution.

### Compare Vendors' Key Management Features and Flexibility

Key management should be highly flexible and support role-based access and management. An optimal solution should always encrypt keys to protect them at-rest or while in transit.

Key management approaches can vary widely from vendor to vendor. As your organization evaluates its options, it should seek out those solutions that provide maximum flexibility and allow your business to use keys in a manner best suited for your environment. The key manager should create keys automatically based on user-defined policies and provide your organization with full control over how often, or infrequently, it changes keys.

Carefully examine the access and management capabilities of each vendor's key manager. Look for key managers that allow role-based configurations so that critical security functions are controlled using "quorum" functions that require action on the part of a predefined set of decision makers within the organization (such as a security officer, compliance officer, or auditor) to make any changes to encryption policies. Provided that your organization defines roles clearly and in accordance with National Institute of Standards and Technology (NIST) best practices, role-based access and management helps ensure a complete audit trail and maximum accountability any time data is accessed or keys are created, distributed, copied, exported, or deleted.

Evaluate each vendor's process for distributing and updating keys. Confirm that a given solution protects keys when they are stored or in transit with the same rigor your organization applies to its most critical data. Steer clear of any key management scheme that stores encrypted data — along with the keys used to encrypt it — on the same tape or disk. Also, avoid key managers that transmit unencrypted keys.

Some additional capabilities to look for in a solution include:

- The ability to organize data so that encryption keys can be assigned to a particular type or source of data.
- Policy-controlled (automatic) key life-cycle management.

Sun can assist your organization in assessing its encryption needs and offers a simple, secure, and scalable encryption solution suited for small-scale to enterprise-level data centers.

## 4 How the Sun Encryption Solution Helps Your Organization Meet the Challenges of Implementing Encryption in the Enterprise

By now, it should be clear that evaluating and selecting an encryption solution can be a daunting task. The costs and complexities are as varied as the number of solutions available. But here is some good news: Sun can assist your organization during every step of this critical decision-making process. From analyzing the type and quantity of data that requires encryption to inventorying and evaluating your current infrastructure, Sun can provide your organization with a risk analysis and unbiased recommendations to help you choose the best encryption architecture for your business needs.

And of course, Sun offers a simple, secure, and scalable encryption solution that is flexible enough to meet the operational needs of small-scale and enterprise-level data centers alike. This solution integrates easily into existing workflows and offers you a choice of when and where to encrypt and how to manage keys. Take a moment to learn how the Sun StorageTek™ Crypto Key Management System addresses the challenges described earlier in this paper.

### Compliance

Sun's encryption solution will help your organization comply with current state and federal rules, regulatory statutes, and standards. Created to meet the most stringent US Government security requirements, the Sun StorageTek™ Crypto Key Management System (KMS) offers AES-256 CCM encryption. And, Sun's hardware appliances, key transmission protocols, and storage devices are designed to meet a wide range of government certification standards.

With our solution, encryption is implemented from end-to-end. For example, keys are:

- Never stored as clear text or on the same media as the data it encrypted
- Encrypted in the Sun StorageTek Crypto KMS
- Encrypted for transport from the Sun StorageTek Crypto KMS to another storage device
- Encrypted when copied to backup devices

The Sun solution provides the highest levels of protection against on- and off-site data loss arising from error or theft. Keys are protected with the same rigor as customer data. With a Sun solution, your organization can move data to and between DR locations or third parties with the piece of mind of knowing that your information is safe from unauthorized access.

With more than thirty years of experience in developing and supporting storage and automation solutions, you can trust Sun StorageTek to create encryption solutions that set the industry standard for security, ease of use, and scalability.

### Interoperability

Standards-based interoperability is the key to flexible, scalable encryption solutions. Interoperability significantly reduces the cost of encryption by leveraging the storage hardware currently in your organization's data center and supporting new devices seamlessly as your business grows.

The Sun StorageTek™ Crypto Key Management System provides businesses with a highly secure and interoperable encryption solution.

Working with the prominent standards committees, Sun is taking a lead role in defining the standards of interoperability to help ensure that new technologies are fully compatible with our encryption solutions and third-party devices. To that end, Sun shares the KMS API with our partners in the tape, disk, third-party key management, and software application markets to promote true interoperability in the future.

	2004	2005	2006	2007	2008	2009
Phase	Forming	Storming		Norming		Conforming
Characteristic	Uncertainty	Competition		Standards Development		Synergy
Activity	Concept Development	Point Solutions		Integration		Compatibility
Sun Products	SCA4000 Solaris 9	Niagara SCA6000 Solaris 10		T10000 LTO KMS		Interoperability
Non-Sun Products		IBM ICSF Decru Neoscale RSA nCipher etc.		IBM TS1120 LTO4		

Figure 1 — Sun is actively involved in developing and formalizing interoperability standards with each of the standards groups mentioned earlier.

Sun encryption experts can provide your organization with an Encryption Readiness Assessment to help evaluate the potential for interoperability within your current environment. Based on the assessment findings, Sun will recommend enhancements to the data center that help ensure ongoing interoperability once the enterprise has deployed an encryption solution.

### Implementation

Sun encryption solutions allow for a low-touch, straightforward integration into your organization’s current workflow. When you choose a Sun implementation, your business can use current operating systems, microcode, and backup applications and processes without worrying about conflicts or incompatibilities with the encryption solution.

The Sun Encryption Readiness Assessment team can help your organization design and implement an encryption solution and supporting policies quickly. In fewer than two weeks, Sun will work with your organization to assess its encryption needs and identify a range of optimal solutions based on criteria such as:

- Current environment and hardware
- Time required to implement the solution
- Overall cost

Once your business selects the best encryption solution for its needs and budget, Sun KMS Integration Services is available to work with your organization to implement and configure the system, define roles, and train your staff to manage and maintain the solution. Typically, the entire deployment and training effort requires no more than five days and is often completed in less time.

The Sun Encryption Readiness Assessment team can work with your organization to design and implement an encryption solution that provides maximum data protection and compatibility with your existing data infrastructure.

If your organization is ready to reduce its risk by implementing a comprehensive encryption solution, Sun can get you there — from assessment to implementation and training — in as few as 21 days. And in most cases, current Sun StorageTek customers with existing tape libraries can take advantage of an even more streamlined implementation process by simply enabling the powerful encryption features found in the storage systems already in their data centers.

## Data Management Policy

When you select a Sun encryption solution, your organization can manage a nearly unlimited number of storage devices from multiple secure, remote terminals. The Sun StorageTek Crypto Key Management System (KMS) is comprised of two rack-mountable servers with an encryption user interface, known as Key Management Appliances (KMAs). KMAs operate in a cluster for redundancy and high availability. When installed on a client computer, the KMS Manager GUI application provides the means to manage the KMAs remotely. And, if required, the KMAs can be integrated into a larger, WAN-connected cluster to provide encryption to multiple sites in your organization.

With a Sun encryption solution, you can count on simple management and low overhead for your business.

## Key Management

Sun believes strongly that key management should be simple. That's why our encryption solution delivers automated key management and redundancy that instantly and transparently updates every KMA in the cluster with any changes made to the database.

With the Sun encryption solution, your organization is not bound to a typical master-slave management configuration when an IT administrator needs to make a change to the system. Instead, authenticated users can manage the system from almost any workstation attached to the cluster that is configured with the KMS Management GUI.

The Sun StorageTek KMA, a critical component of the StorageTek Crypto Key Management System (KMS), is a pre-configured, dedicated appliance that reduces installation complexity and provides a single access point that your organization can use to manage every key in the enterprise. Also, because the Sun StorageTek Crypto KMS is a separate, standalone solution, updates and changes to operating systems, applications, and hardware microcode have no effect on your organization's ability to manage existing keys.

When encrypting to tape, the Sun solution supports more than 1 million keys, which allows your organization to take advantage of the encryption period policy feature available in the Sun StorageTek Crypto KMS. This extra level of security allows your business to set a pre-defined schedule to change keys automatically.

To stay ahead of the curve, the Sun StorageTek Crypto KMS encryption solution includes next-generation key management features, such as time-based data and key expiration, which allows your business to deploy a secure, verifiable method of data disposal. When implemented, your organization can set policies to delete keys permanently and render the associated, encrypted data unreadable.

The Sun StorageTek Key Management Appliance is pre-configured to simplify the installation process and provides a single access point to manage every key in the enterprise.

## 5 Summary

The risks associated with archiving and transferring unencrypted data are too great for your organization to ignore. Stiff penalties, lawsuits, criminal prosecution, and loss of brand reputation are just a few of the consequences of losing sensitive data through human error or theft. Now is the time to encrypt your data.

To choose among three methods of encryption available to the enterprise, examine closely the quantity and type of data you need to encrypt. Consider the cost and complexity of each encryption architecture to determine which solution is the best fit — and least disruptive — to your enterprise.

The Sun StorageTek Crypto Key Management System encryption solution is simple, secure, and scalable. Key management is simple and allows for automated, policy-based changes. Data and keys are encrypted from end-to-end, and changes to policy or data requires authentication from multiple, authorized personnel in the organization. And critically, this Sun solution supports interoperability to help keep your investment costs low while ensuring a high level of compatibility in the data center and long-term investment protection.

## Encryption Terms

**AES-256 Counter with CBC-MAC (CCM) mode encryption** — A NIST-approved mode of operation for cryptographic block ciphers that is designed to provide authentication and privacy.

**Application programming interface (API)** — A set of standards and tools used to facilitate software application development for and operation with an operating system.

**Clear text** — Data that has not been encrypted.

**Device-based encryption** — An encryption method that encrypts data at the tape drive or within a storage device.

**Host-based encryption** — An encryption method that encrypts data at the moment it is created. (Also called server-based encryption.)

**In-band appliance based encryption** — An encryption method that uses an appliance to encrypt data as it is being transported from the point of creation to its destination.

**Key Management Appliance (KMA)** — A security-hardened Sun Fire x2100 M2 rack-mounted server that delivers policy-based key management, authentication, access control, and key provisioning services. As a trust authority for storage networks, the KMA ensures that all storage devices are registered and authenticated, and that all encryption key creation, provisioning, and deletion is in accordance with prescribed policies.

**Sun StorageTek™ Crypto Key Management System (KMS)** — A dedicated encryption key management system comprised of two or more KMAs clustered together to provide high availability and dynamic key management, while having no dependencies on operating system, controller hardware, or applications.

