



White Paper

Enterprise Tape Encryption

By:

Jon Oltsik
Enterprise Strategy Group

August 2006

Table of Contents

Table of Contents	i
Executive Summary	2
The Growing Need for Tape Encryption.....	2
Tape Encryption Must Support the Business	3
Large Organizations Need Enterprise Tape Encryption	5
The ETE Architecture.....	6
IBM's Encryption Offerings: The ETE Model at Work Today	7
The Encryption Facility for z/OS - Business Partner Exchange.....	8
IBM TS1120 Tape Drive-based Encryption -- Data Archive	8
ETE at work	9
Moving Forward: The Implications of ETE	10
The Bottom Line	11

This paper was developed with assistance and funding by IBM.

Executive Summary

It seems like there is a new publicly-disclosed data breach in the headlines of the major business media outlet each day. Some of these incidents are related to lost laptops while others are linked to hacking incidents. But many of the most infamous of these breaches were the result of lost or stolen backup tapes. Little wonder then why tape encryption has become such a hot topic of late.

ESG believes that tape encryption is long overdue and will become commonplace in the future. Nevertheless, most enterprise still think of tape encryption with a myopic perspective around off-site tape storage and this tactical mindset doesn't go far enough. This paper concludes:

- **Tape encryption must deliver for the business and IT.** Encrypting tape must be more than a basic insurance policy. Rather, it should enable secure business processes like data sharing and records retention where tape is involved. It must also provide this functionality without adding any undue operational burden or security risk within IT.
- **What's needed is an Enterprise Tape Encryption (ETE) architecture.** Rather than deploying a tape encryption product, large organizations should strive for a tape encryption architecture made up of encryption services. A tape encryption architecture will help ensure that tape encryption can be flexible enough to address configuration changes and scalability requirements.
- **Users must address short-term vulnerabilities while planning for long-term needs.** Since tape encryption has become an enterprise requirement, CIOs can't wait around while vendors develop next-generation ETE architectures. In lieu of this, smart companies will acquire open tape encryption solutions today that allow for integration and configuration changes in the future.

The Growing Need for Tape Encryption

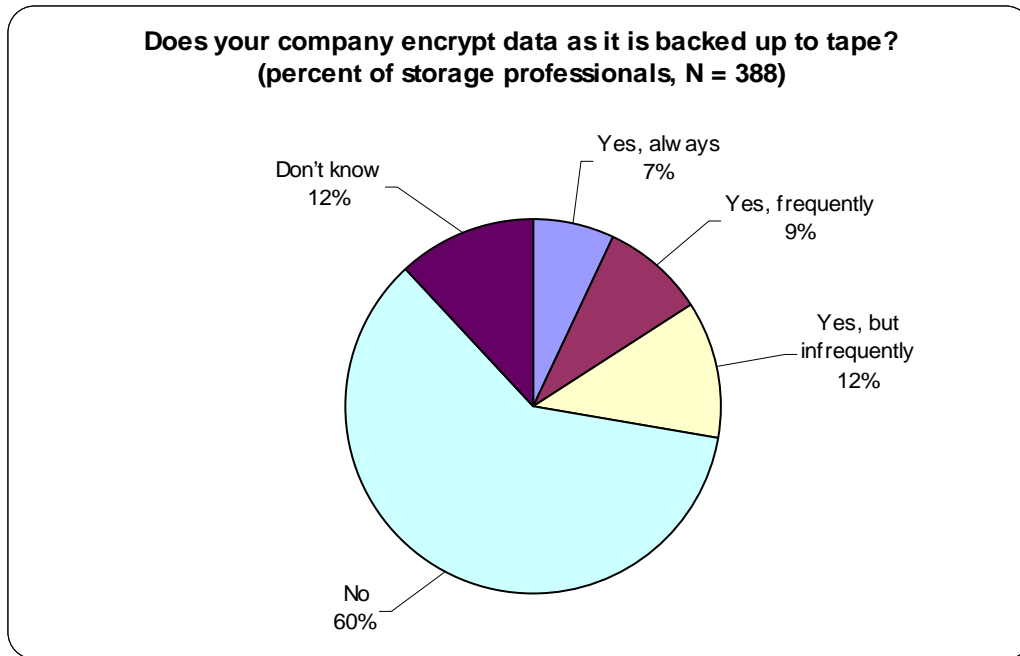
Backup vendors have supported encryption in their products for years but few customers ever bothered with this type of protection in the past. Why? IT managers always assumed that tape-based data was relatively safe. After all, tapes were used by IT professionals and tape devices sat well behind vulnerable IP networks. Encryption was also eschewed because it could lead to slower performance, additional IT operational chores, and higher capital costs. Given the perceived low risk, most CIOs tended to eschew tape encryption outright. According to ESG Research, most storage professionals claimed that their organizations "never" encrypted their tapes (see Figure 1).

Fast forward to 2006 and times have certainly changed. Interest in tape encryption is growing rapidly due to:

- **Increasing privacy regulations.** Tape-based private data has long been subjected to well established global privacy laws like the EU Directive on Privacy and Electronic Communication (2002), and the Japanese Bill to Protect Personal Data (2001). The trend toward privacy regulations continues to gain momentum worldwide. As of the beginning of 2006, 23 states had privacy regulations in place while 13 disparate bills were introduced in the U.S. Congress in 2005. The flip side of these regulations is industry guidelines around business best practices. The Visa/Mastercard PCI requirements and the Japan Bank Association's Data Protection Support standard are visible examples that detail data privacy technologies and controls. Tape encryption is an obvious outgrowth of these regulatory and business initiatives.

- **Publicly-disclosed data breaches.** Some regulations like the California Database Breach Act (aka California SB1386, 2003) mandate that any data breach involving the private

Figure 1. Tape Encryption Usage



data of a California citizen must be publicly disclosed. Between February 2005 and August 2006 there were a total of 17 publicly-disclosed data breaches as a result of lost/stolen backup tapes leading to the exposure of private data of over 9 million Americans (source: Privacyrights.org). A data breach requires activities like alerting customers, providing credit monitoring, and damage control - activities that can lead to millions of dollars in unanticipated costs.

- **New technology options.** The increasing need for tape encryption has not been lost on the IT market. First, crypto processor technology has greatly improved offering both high performance and lower prices. This development led to a slew of new hardware-based crypto acceleration and encryption appliances. With demand continuing, IT professionals can expect to see a dizzying array of encryption technology choices.

Driven by regulatory compliance, ESG has seen growing interest in tape encryption since the publication of its original research. In a more recent survey, 42% of storage professionals say that their organizations are researching, evaluating, or implementing tape encryption as a direct result of the series of publicly-disclosed data breaches associated with lost/stolen tapes (see Figure 2).

Tape Encryption Must Support the Business

In order to avoid the public humiliation of a data breach it is not surprising that so many companies are jumping on the backup tape encryption bandwagon. In this example, tape encryption can be seen as an insurance policy -- simply encrypt your backup tapes and the threat of lost/stolen tapes, embarrassing data breaches, and unexpected costs disappears. While this behavior is certainly logical, it is also shortsighted. Yes, tape encryption must provide protection

against accidental tape loss or criminal activities but it should also be integrated into the security procedures of tape-based business processes such as (see Table 1):

- **Data sharing.** Tape is still used frequently as a means for data exchange between business partners but this process shares the same risk of tape loss or theft as off-site solutions.

Figure 2. Data Breaches have led to Increasing Interest in Tape Encryption

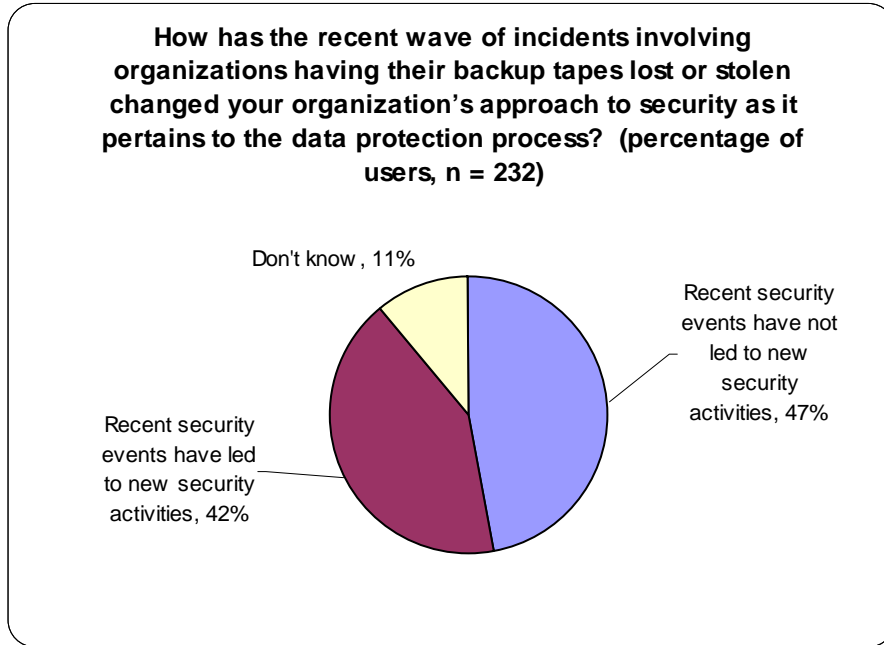


Table 1. Tape Encryption Needs for Business Processes

Activity	Business Requirement	Technical Requirement
Sharing data with business partners via tape cartridge distribution	Add security to data sharing process without interrupting existing processes	Encryption, key management, authentication and key sharing amongst partners
Data archiving	Secure records retention for multiple decades for regulatory compliance and intellectual property management	Long-term key management. Ability to accommodate technical changes while maintaining management and security

Tape encryption solutions must also provide for the sharing on encryption keys amongst business partners.

- **Data archiving.** Government regulations like HIPAA and SEC 17a-4 demand long-term records retention for periods of more than 20 years. Since tape media is often used for data archiving, tape encryption can be utilized to keep the data confidential and tamperproof. In an archiving application, tape encryption must be supported with key lifecycle management features built for long-term encrypted data storage.

These functions will certainly add to the business value of a tape encryption solution but it is also important that they don't create an inordinate amount of IT operations overhead in the process. To accommodate the business and IT, tape encryption solutions must:

- **Work with existing technologies and processes.** Tape encryption should be an easily integrated set of services that can be called by backup software, storage management systems, device drivers, libraries, and tape drives. Other than the security team's new responsibilities in the tape management process (i.e. key management, administration, auditing, etc.) tape encryption should not add any undue burden or performance degradation to day-to-day backup, restore, and archival operations.
- **Integrate into disaster recovery planning.** Since encrypted data must be decrypted to be useful, tape encryption operations must become part of the disaster planning/business continuity process. This requires tight controls for key management, key backup, and redundant key restoration equipment. All of these additional steps must be added without impacting business critical RTOs and RPOs. (Spell these out, please)
- **Allow flexible options for future growth.** Tape encryption solutions must maintain their integrity in an environment of constant change. For example, when a file is archived for 10 years, it is certain that tape drive, server, and application technologies will radically change during that timeframe. Tape encryption must be flexible enough to accommodate inevitable technology churn while maintaining the integrity of encryption keys and administrative policies over the long haul.

Providing the right level of business and IT functionality is a tall order. When weighed against this set of enterprise requirements most of today's tape encryption solutions fall woefully short.

Large Organizations Need Enterprise Tape Encryption

Tape encryption solutions that provide little more than "anti-disclosure" insurance may be in vogue today, but the encryption needs of large organizations will soon move beyond this limited scope. Rather than implement multiple tape encryption solutions, ESG believes that savvy CIOs will look at a new class of security solution that ESG calls Enterprise Tape Encryption (ETE). Unlike most self-contained point solutions, ETE is built as a set of encryption services. As such, ETE:

- **Separates encryption and administrative functions.** ETE services like cryptographic processing, key management, and administration are discrete objects. By separating these services, the actual cryptographic processing can be performed on high-speed security processors while key management and administration can be centralized for operational efficiency and high security. This object-based model is especially important over time as it offers scale and performance benefits as more and more data is encrypted. To avoid future scalability problems, today's all-in-one server-based solution can migrate gracefully to a distributed model over time (i.e. encryption across multiple devices and management across multiple servers).
- **Provides for ease-of-integration.** ETE services are easily accessible to those systems that need to encrypt data (i.e. applications, operating systems, security management, etc.) and those devices that perform the actual encryption operations (i.e. crypto processors, encryption software, appliances, etc.). In other words, ETE acts as encryption middleware with open APIs used for requesting or performing encryption services.

- **Virtualizes key management.** To maintain availability of critical key management services, many of today's encryption appliance solutions must be configured in pairs for failover. Rather than clustered boxes, ETE uses a distributed database built upon multiple distributed systems similar to the global DNS infrastructure. This type of architecture increases performance by localizing ETE service requests thus minimizing latency. It also eliminates any single point of failure. If a local ETE system is off-line, the ETE service will simply call another.
- **Accommodates the need for key sharing.** ETE recognizes the need for key sharing amongst enterprise data centers and business partners. To accomplish this, ETE offers multiple technical solutions including PKI, Kerberos, shared secret keys, and secure decryption utilities.
- **Leverages tape compression.** Enterprise-class tape encryption can provide a 300% improvement in throughput, reduce media cost, and decrease the number of physical tapes handled by IT operations. To take advantage of the operational benefits of compression AND the security advantages of encryption, tapes must be compressed before being encrypted. To achieve operational and security goals, ETE can distribute encryption services where cryptographic processing can reside behind tape compression.

Like other central services (i.e. network directories, DNS, etc.) ETE changes the way tape encryption is performed. ETE services are available for disparate systems, applications, and devices as needed. In this way, users can achieve operations and security benefits from centralized encryption management while realizing performance advantages from distributed cryptographic processing.

The ETE Architecture

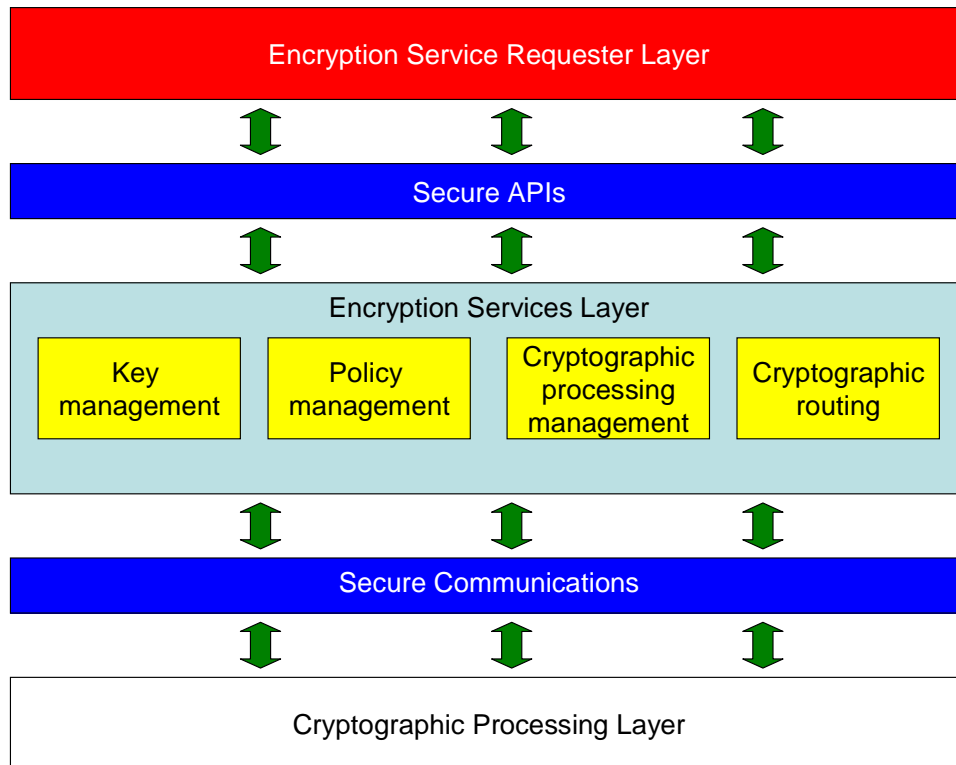
As described above, ETE is built on a series of distributed services that can be called through published (and secure) APIs. In its simplest form, the ETE architecture is composed on three discrete layers (see Figure 3):

- **Encryption service requester layer.** Various systems (i.e. file systems) and applications (backup applications) that need to encrypt data can call the encryption services layer and relay which data needs to be scrambled. Aside from this call, the tape encryption process is completely transparent to requester layer systems and applications. When a backup application wants to restore encrypted data, the encryption services layer will intercept this request, perform the necessary operations to decrypt the data, and then pass it along. The request layer can also handle the necessary integration with existing data management and system management products to minimize changes to customer's business processes.
- **Encryption services layer.** The ETE services layer acts as the workhorse of the architecture and masks the complexity of enterprise tape encryption from applications and devices. To accomplish this goal, the ETE encryption services layer serves as a middleware bridge between encryption requesters and cryptographic processors by providing services for key lifecycle management (i.e. key generation, key protection, administration, etc.), policy management, logging/reporting, and actual cryptographic processing. The services layer can also integrate with existing security software for access control, compliance assurance, auditing, etc.
- **Cryptographic processing layer.** Actual encryption operations can live anywhere in the infrastructure. When any cryptographic processor receives a request to encrypt data, it subsequently calls the key management server and asks it to generate an encryption key.

Once it receives an encryption key from the key manager it performs the requested cryptographic operations. In this way, the cryptographic processing layer also acts as a service but remains dormant much of the time. When called to encrypt data, it wakes up and works with the encryption services layer to execute cryptographic operations based upon specific policies.

Given the services-based architecture of ETE and the distributed nature of systems and devices in a typical enterprise, the goal of ETE is to provide flexibility for any-to-any tape encryption requirement. For example, a backup system could ask for encryption services

Figure 3. The ETE Architecture



from any available drive in a tape farm composed of multiple libraries. Likewise, an archiving system could encrypt large files to a set of remote tape drives in a secure location. This also allows for changes over time. As new servers, backup applications, and tape drives are added across the enterprise, they can join the ETE process because it is controlled by the ETE services layer rather than hard-wired into specific systems.

IBM's Encryption Offerings: The ETE Model at Work Today

While pieces of the ETE architecture are available, an entire ETE solution remains a vision. That said, IBM has established itself as an early ETE leader by offering its customers two complementary encryption options: the Encryption Facility for z/OS and the recently released

T1120 tape drive with on-board encryption. Both products use the same key distribution and protection mechanism based on public key infrastructure. Both products can leverage cryptographic hardware features available on System z. In particular, System z offers tamper resistant cryptographic units so that no key information ever resides in the clear in system memory. This type of cryptographic support is called secure-key cryptography, and it is an important key management requirement for many enterprises.

The Encryption Facility for z/OS - Business Partner Exchange.

The Encryption Facility for z/OS is a mainframe based program that encrypts data using host cryptographic hardware acceleration. This encryption can be invoked with the addition of a jobstep. The encrypted data can be written directly to any currently supported tape storage device. The Encryption Facility will also optionally compress the data before encryption. The Encryption Facility also provides a free-of-charge client so that receiver of data can easily decrypt or re-encrypt the data without necessarily purchasing new encryption product. Because of its client support and its ability to use legacy storage devices, the Encryption Facility is ideal for most business partner data exchanges.

IBM TS1120 Tape Drive-based Encryption -- Data Archive

In August 2006, IBM announced enhancements to its encryption offerings with the new version of its TS1120 tape drive (note: existing TS1120s are field upgradeable). Rather than encrypting at the host, TS1120 drives encrypts the data at near native tape drive speeds on the tape device itself after compressing the data. The TS1120 tape drive is supported for both mainframe and open systems. This placement of the encryption function in the tape drive provides:

- **High performance and media utilization.** IBM testing demonstrates that TS1120 write performance can be maintained at up to 100MB per second even with crypto processing turned on. TS1120 encryption does not interfere with existing compression functions so users can still compress data for up to a 3x improvement in media utilization.
- **Key management integration.** Key management for TS1120 can be centralized on any connected and Java enabled server, and has the ability to take advantage of the platform unique security features available on the key management server. On z/OS, centralized key management will take advantage of ICSF, RACF, and the secure-key cryptographic hardware. In this way, TS1120 encryption remains focused on high performance crypto processing and takes advantage of existing security, high availability, and operational efficiency in the existing mainframe key management system..
- **Policy flexibility.** TS1120 encryption can also be integrated into various policy management applications. For example, mainframe tape encryption policy may be managed by utilities like DFDSM while UNIX, Linux, System i 5/OS, and Windows may need encryption policies based upon tape drive, cartridge serial numbers or tape libraries. This maps closely with the ETE model allowing device sharing options for large users.

Because of its high performance the TS1120 tape drive is well suited for data archival where large amounts of data needs to be encrypted onto tape. Also because the centralized key management can leverage secure key-stores such as ICSF on z/OS, archived data can be safely retained for years.

ETE at work

Both the Encryption Facility for z/OS and outbound encryption on the TS1120 map well with the ETE requirements defined above (See Table 2). IBM has also indicated that it intends to extend its encryption technologies, enabling encryption within disk subsystems while continuing to leverage centralized key management technologies of mainframe hardware and software.

Table 2. IBM's Offerings Map to ETE Requirements

ETE Requirement	Business Partner Exchange: Encryption Facility for z/OS	Data Archiving: TS1120 Outboard Encryption
Separates encryption and administrative functions	Encryption in the server with HW cryptographic acceleration. Key management and administration centralized in z/OS. Public keys of partners and enterprise private keys can be managed in highly secure data stores.	Compression and encryption in the tape drive at line speed. Tape key management for the enterprise can be centralized on z/OS. Public keys for partners and enterprise private keys can be managed in highly secure data stores.
Provides ease-of-integration	Easily integrates into existing processes by inserting an additional job step. Customers can use existing tape exchange devices and policies. Java-based client is available to business partners who do not have a mainframe or Encryption Facility for z/OS. Can use the existing authentication, authorization and auditing services in the mainframe (RACF)	Integrates with existing data management processes. Policy driven encryption can be defined in z/OS System Managed Storage. For non-z/OS systems, encryption requests can be made based on ranges of cartridge volume serial numbers. For z/OS centralized key management, can use the existing authentication, authorization and auditing services in the mainframe (RACF)
Virtualizes key management	Highly available key store on z/OS. Designed for no single point of failure with Parallel Sysplex configuration which can allow multiple instances of z/OS to access the key store.	Highly available key store on z/OS. No single point of failure with Parallel Sysplex configuration which can allow multiple instances of z/OS to access the key store. Each z/OS image can have a local key manager to maximize availability and performance. Remote access to these key managers can be routed automatically to the appropriate key manager using virtual IP addressing (VIPA) for high availability.
Accommodates the need for key sharing	Secure exchange between partners can be established using either passwords or public keys. Takes advantage of industry standard public key management processes and existing mainframe digital certificate services.	Secure exchange between partners or data center locations can be established using public keys. Can take advantage of industry standard public key management processes and existing mainframe digital certificate services.
Leverages tape compression	Can take advantage of host-based compression before encryption	Can take advantage of TS1120 drive-based compression before encryption

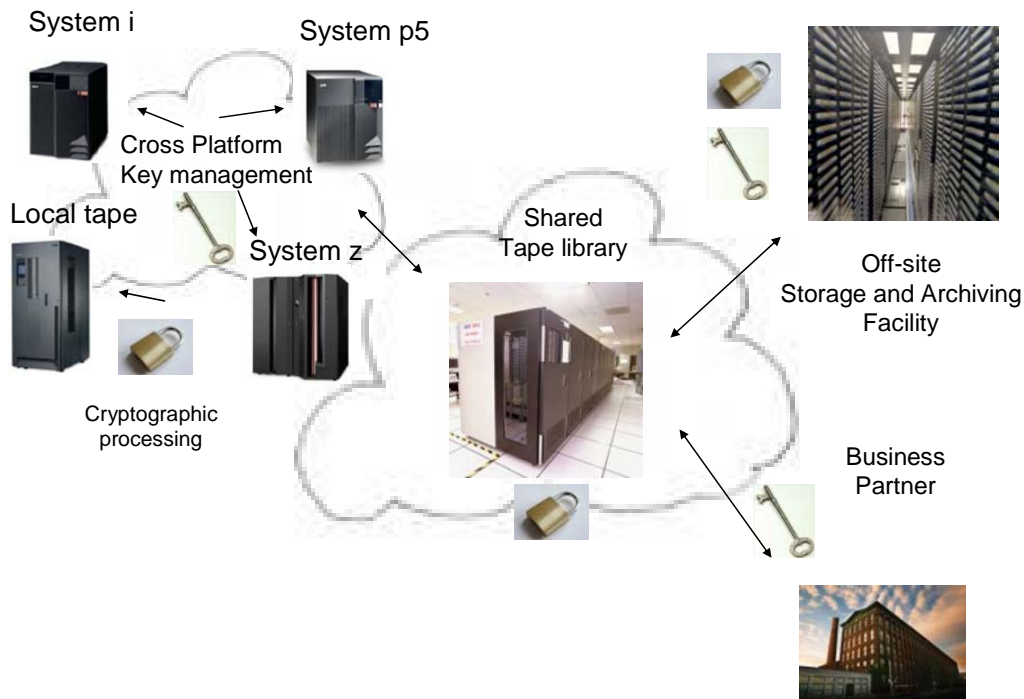
Moving Forward: The Implications of ETE

As far as encryption is concerned, two things are certain for the next few years. First, there will be more and more encryption used to keep private data confidential. Second, disparate encryption technology implementation could ultimately have a profound impact on IT operations and disaster recovery preparation.

ESG believes that the only way to gain the data privacy benefits of encryption without the associated operational setbacks is to approach encryption with a strategic and architectural plan. To prepare for the predictable insertion of encryption within IT and business processes, smart CIOs will:

- **Plan for centralized key management from the onset.** Even under tight processes and strong management, multiple key management servers will inexorably lead to redundant operations, security vulnerabilities, and complex disaster recovery scenarios. To avoid these pitfalls, IT executives should focus their planning effort on centralized key management services. In instances where multiple key management systems are unavoidable, CIOs should make sure that these servers can be easily integrated or consolidated in the future.
- **Build short- and long-term plans for cryptographic processing.** Given the direction of cryptographic processors and storage vendors it is a near certainty that future devices will contain on-board encryption but this functionality will roll in slowly as older devices are

Figure 4. ESG VIEW of the IBM ETE Architecture



- replaced. . To avoid any lock-in to a single model, use standard encryption algorithms, make sure that encryption keys are exportable and look for open key management functionality that can interoperate with a centralized key management server.
- **Drill vendors on their commitments to open standards, interoperability, and platform support.** Since encryption and key management solutions are relatively immature, many solutions will be built with proprietary hooks. Remember that enterprises will need flexibility over the long-term as they more applications encrypt their data and additional devices provide cryptographic functionality. CIOs should make sure that vendors adhere to open standards enabling future ETE integration. It is also important to consider platform support. Many enterprise applications cross Windows, UNIX, Linux, System I 5/OS and mainframe tiers. The best ETE solutions will support all of these standard enterprise platforms.
 - **Think in terms of records retention periods - not product cycles.** Technology products generally have a useful life of 3-5 years and can be replaced once their value is fully amortized. This mentality does not align with records retention where regulations may require the archival of certain data for dozens of years. When looking at tape encryption, it is important to ask a fundamental question, “Will the technology (or the vendor) be around in 20 years? If there are any doubts with regards to a particular solution, move on.

These important criteria once again align with the strengths of the IBM's tape encryption solutions. Given the long history and strong key management services of z/OS, customers with mainframes should be considering centralizing key management on their z/OS server.

The Bottom Line

What's driving tape encryption today? That's easy - regulatory compliance and data breach disclosure paranoia. While it is certainly worthwhile to avoid regulatory compliance violations, security protection should be thought of as more than a check-off box. Security technologies like encryption provide the most value when they enable secure business processes while meshing seamlessly with ongoing IT operations.

This is the exact design point of Enterprise Tape Encryption. ETE delivers tape encryption benefits in terms of:

1. **Business requirements.** ETE provides encryption services for business applications in order to protect data at rest on tape. Since this data is often shipped to business partners, ETE provides multiple ways for business partners to identify themselves, provide proof of authentication, decrypt confidential data, and then ultimately utilize the cleartext data with confidence.
2. **Tactical needs and strategic planning.** Because ETE provides for separate encryption services, large organizations can mix and match them based upon their technology infrastructure and business needs over time. This prevents against vendor lock-in while providing for flexibility over time.
3. **Integration into existing IT operations.** Tape encryption can't add a series of new IT operations tasks or disaster recovery exposure. ETE adds little overhead other than introducing the security team into standard tape management processes. The objective is to be as transparent as possible.

In its ultimate state, ETE calls for an architecture featuring typical enterprise qualities like high availability, scale, reliability, and tight security. In addition, ETE must stand the test of time. In spite of technology differences 20 years down the road, ETE must be able to locate keys and decrypt data from 2006.

All of these requirements align with the combination of the Encryption Facility for z/OS and the encryption solution based on the IBM System Storage TS1120. In this regard, IBM should be on every CIO's short list as they consider tape encryption solutions for today's tactical needs or future strategic initiatives.