

CYBERNETICS

Data Encryption:

The Role Of Key Management

January 2008

The Data Encryption Standard

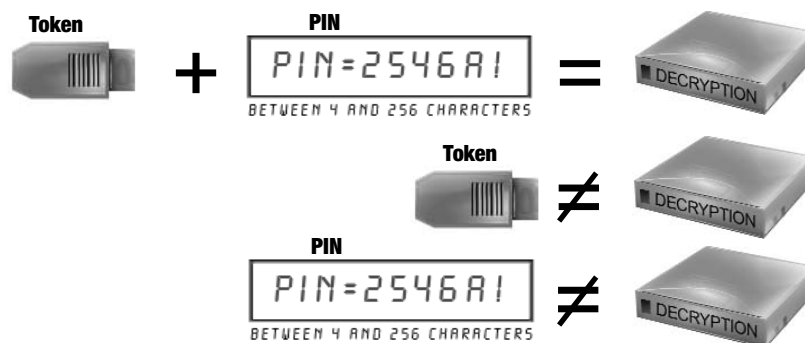
Advanced Encryption Standard, AES, is a national standard for securely encrypting data with powerful cryptographic keys of up to 256 bits in length. Today, many tape drives have embedded this standard to provide native encryption capability. Failure to adequately protect personal or confidential employee, customer, and client data makes organizations vulnerable to serious legal and financial consequences. Given the fact that encryption is a readily available standard, one might wonder why there are still so many new stories published about the exposure of this data – often resulting from lost or stolen backup media. Virtually anyone can encrypt data; yet complexity, performance drain, and high cost have prevented many organizations from implementing a comprehensive plan for full protection. Cybernetics released its first data encryption option in 1991. Now in its third generation, it combines high performance with a remarkably intuitive key management strategy - all at a very affordable price point.

Vulnerability

Data storage comes in many forms - DAS, NAS and SAN. Data accessible to servers within an enterprise is typically well protected by network security as well as physical security. However, in order to maintain everyday business continuity, as well as preserve important data archives, companies must distribute backup copies to local and remote devices and locations, putting data on a widening path of vulnerability. Data is first migrated to near-line storage in the form of virtual tape libraries for the ability to restore lost data in an instant; next, data is written to removable tape for vault storage; and finally, data is transported offsite for disaster recovery. Each step increases the data's risk of exposure.

Simplicity

Data that is encrypted before it is stored as a virtual tape or removable tape is completely useless to anyone without the key to unlock it. This includes those with legitimate intentions. Cybernetics state of the art encryption feature uses 256bit AES cryptography and truly random key generation with a very simple and intuitive key management scheme. A physical smart key USB token and a secret PIN are required to decrypt any data. No one can see your data without the token generated at your location, and the unique PIN you have created to activate that token. The security of the data is managed through the physical security of the token as well as through the secrecy of an intangible PIN. Since a unique key is created for each and every encrypted tape, even if a tape falls off a truck in Times Square, no one will be able to read any portion of its data, unless you've given them both your token and your PIN.



Performance

Hardware data compression is the workhorse that drives backup at two times speed and two times capacity. Without the power of compression, backup windows and media requirements can double. Data compression relies on patterns of data, and because cryptographic encryption randomizes data, encrypted data simply will not compress. This is never a problem in Cybernetics miSAN and iSAN VTLs because the encryption option utilizes hardware to compress data before it is encrypted. Cybernetics encryption customers enjoy all the speed and capacity benefits of high performance hardware data compression, as well as the highest levels of encryption security.

There are a variety of encryption solutions based on software, but because software cryptography taxes the system processors with both encryption and key management, resulting overhead can be as high as 40%. Since this data is encrypted before it is sent to a tape device with on-board hardware compression, there is no possibility of gaining offloaded data compression benefits. If the software compresses the data before encrypting it, the performance hit doubles. The fact is that most companies operating in a dynamic 24x7 world cannot afford to employ software to secure data through encryption.

Affordability

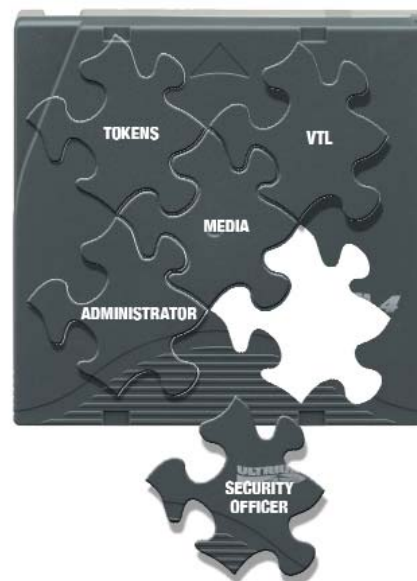
Historically, encryption solutions have been astronomically expensive - well beyond the budgets of even medium to large customers. Cybernetics miSAN VTLs featuring virtual tape array hardware, management software, plus hardware compression and encryption, start at less than \$11,000, considerably less than competitive solutions.

Summary

256bit encryption is a very solid, secure means of protecting data from unauthorized access. However, an encryption solution requires two components – encryption and key management for decryption. An AES encryption product is only as good as its key management. Cybernetics combines the use of tokens, which can be subjected to physical security, with PINs, which are known only by the authorized administrator, for an elegant, intuitive, flexible, and easily managed encryption security solution.

Key Management Elements

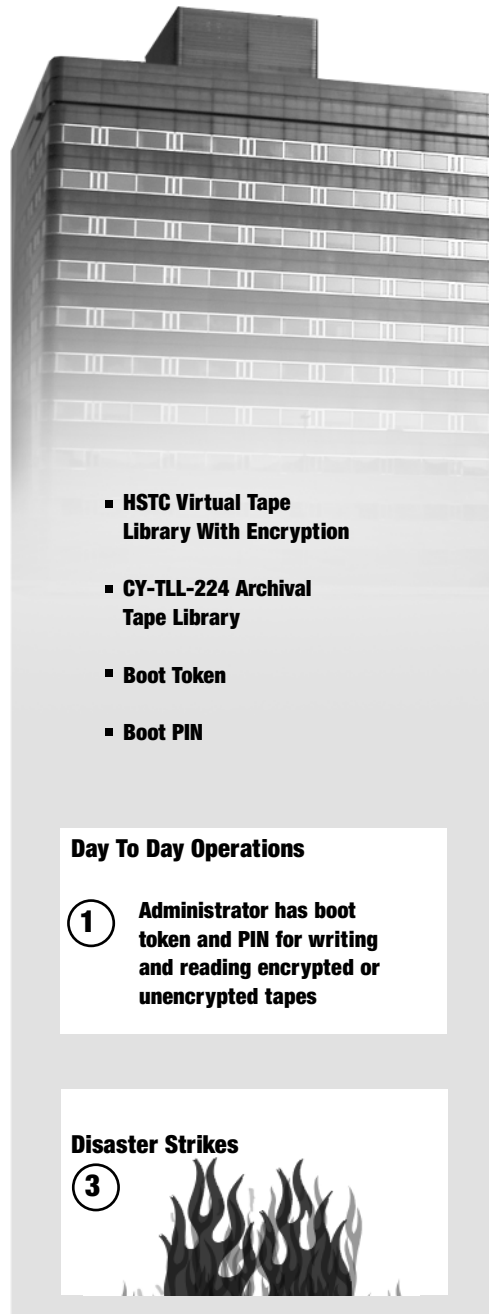
| | |
|---------------|---|
| People | Administrators and Security Officers have passwords and tokens |
| VTL | The hardware stores a distribution list and public keys |
| Tokens | USB smart tokens store private keys which cannot be extracted |
| Media | Encrypted tapes contain the distribution list and public session keys |



Practical Applications for Cybernetics Encryption

Best Company uses a commercial off-site disaster recovery facility and wants data access restricted to a recovery event. Best Company creates a “Boot” token and PIN for the administrator’s use upon a reboot of the VTL, as well as a Disaster Recovery token and PIN for encrypting full backup tapes sent to the DR facility. Best Company can provide the DR facility with the PIN matching their token only upon a recovery event, preventing any other access to the information.

Primary Site




- HSTC Virtual Tape Library With Encryption
- CY-TLL-224 Archival Tape Library
- Boot Token
- Boot PIN

Day To Day Operations

1 Administrator has boot token and PIN for writing and reading encrypted or unencrypted tapes

3 Disaster Strikes




Bank Safe Deposit Box



- Master Token
- Master PIN
- Disaster Recovery PIN

4 Disaster recovery PIN is sent to Disaster Recovery site

Disaster Recovery Site



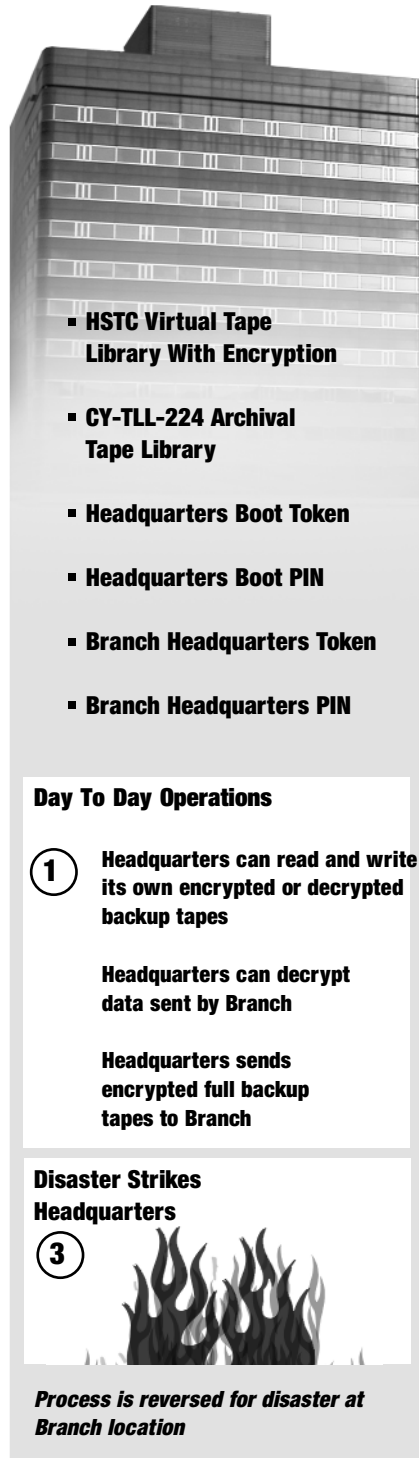
- miSAN With Encryption And Integral Tape Drive
- Disaster Recovery Token

2 Encrypted tapes are sent to Disaster Recovery site

5 Disaster Recovery site restores encrypted tapes

Headquarters and Branch have a reciprocal disaster recovery arrangement, and they also need to share some information on a regular basis. Each facility can create tokens and PINs for these specific purposes. Each administrator for Headquarters and Branch will have “Boot” tokens and PINs for in-house day-to-day operations, as well as tokens and PINs for decrypting the other site’s shared data. Access to full backup tapes for disaster recovery purposes can be restricted through withholding the appropriate PIN until the time of a disaster event.

Headquarters



- HSTC Virtual Tape Library With Encryption
- CY-TLL-224 Archival Tape Library
- Headquarters Boot Token
- Headquarters Boot PIN
- Branch Headquarters Token
- Branch Headquarters PIN


Day To Day Operations

1 Headquarters can read and write its own encrypted or decrypted backup tapes

Headquarters can decrypt data sent by Branch

Headquarters sends encrypted full backup tapes to Branch

Disaster Strikes Headquarters

3 

Process is reversed for disaster at Branch location

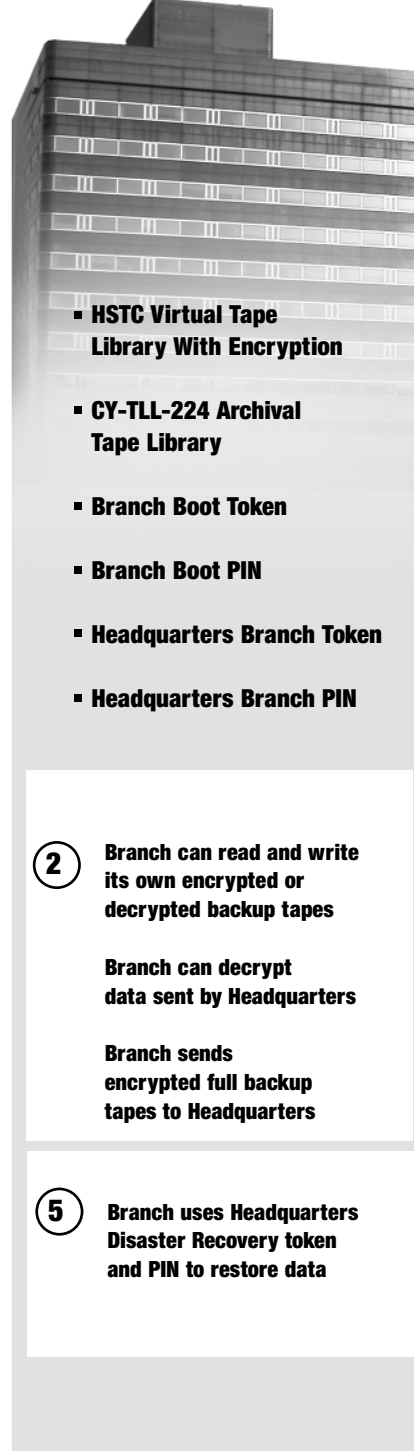
Headquarters Bank Safe Deposit Box



- Headquarters Master Token
- Headquarters Master PIN
- Headquarters Disaster Recovery PIN
- Branch Disaster Recovery Token

4 Headquarters Disaster recovery PIN is sent to Branch

Branch



- HSTC Virtual Tape Library With Encryption
- CY-TLL-224 Archival Tape Library
- Branch Boot Token
- Branch Boot PIN
- Headquarters Branch Token
- Headquarters Branch PIN

2 Branch can read and write its own encrypted or decrypted backup tapes

Branch can decrypt data sent by Headquarters

Branch sends encrypted full backup tapes to Headquarters

5 Branch uses Headquarters Disaster Recovery token and PIN to restore data

Branch Bank Safe Deposit Box



- Branch Master Token
- Branch Master PIN
- Branch Disaster Recovery PIN
- Headquarters Disaster Recovery Token