IBM Technically Speaking Storage

Unlocking the Mysteries of Tape Encryption

Christina Coutts
FTSS Removable Media
christina_coutts@uk.ibm.com

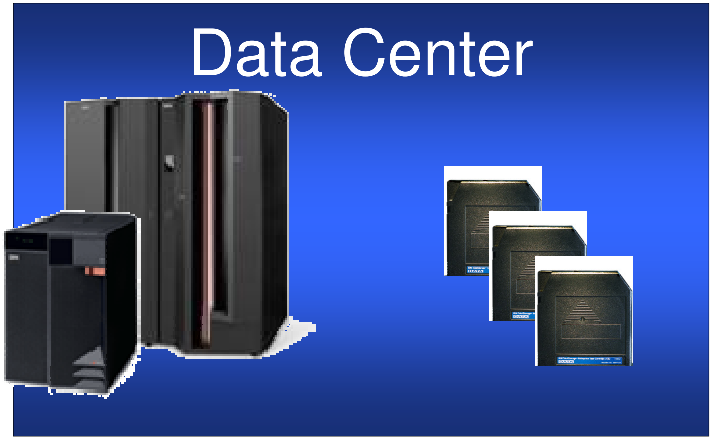
IBM System Storage

Security of Data: a Business Imperative

- **Many government agencies are requiring disclosure of security breaches**
  - 32 states in USA have security breach similar legislation, *Source: www.Privacyrights.org*
- **Industry organizations are also increasing scrutiny of security procedures.**
  - Source: Payment Card Industry Security Audit Procedures Version 1
- **Over 90 million consumers have been notified of potential security breaches regarding personal information since 2005**
  - Source: www.Privacyrights.org
- **Information is the most valuable property of a company**
  - Computer crime grows steadily

Tape Data Protection Requirements

- **Protect tape data in transit from the *primary data center* to a *secondary data center* or *business continuance site***
- **Protect tape data generated by *mainframe* as well as *open systems***
  - and use the same management infrastructure
- **Protect tape data in transit to a *business partner*, but allow the business partner access once the data has arrived**



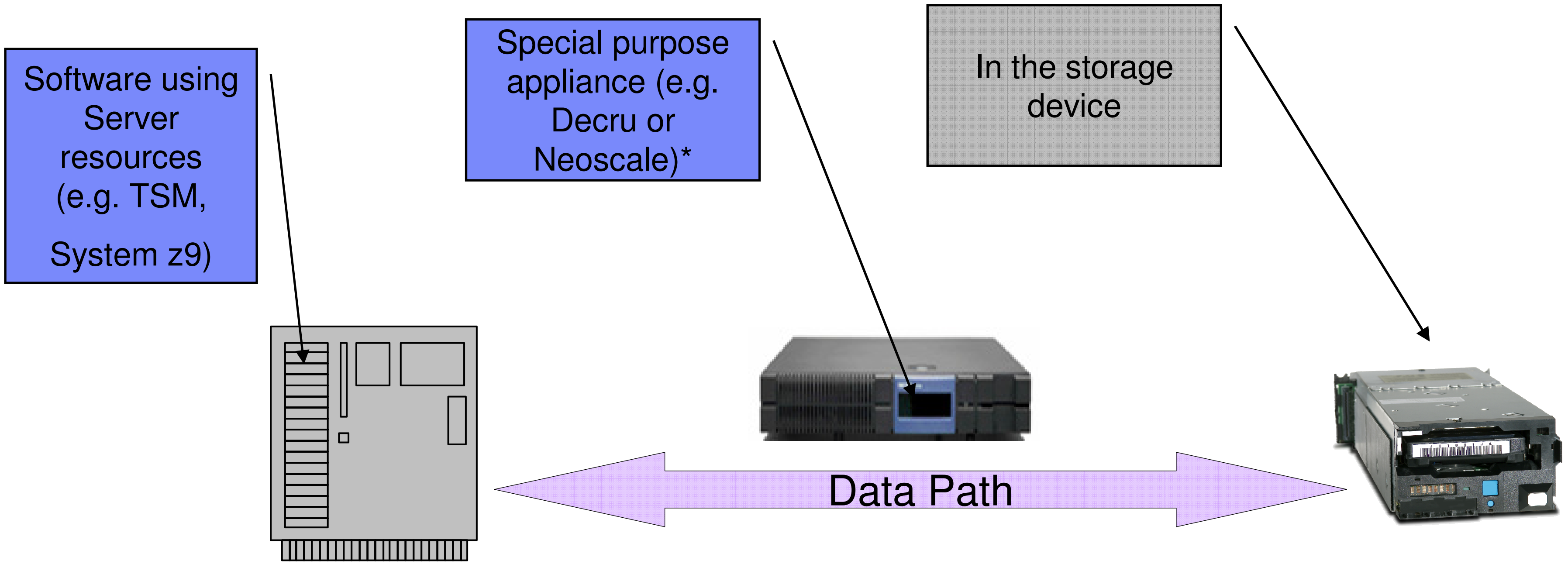
Second Site

Business Partners

Agenda

- Topic Overview
- Encryption algorithms
- How does it work with the IBM solution?
- How do I trigger IBM tape encryption?
- How do I manage the keys?
- Do I already have it?
- How do I implement it?
- What environments are supported?
- Where can I go for more detailed information?
- Breaking News....

Today’s typical encryption solutions



Software using Server resources (e.g. TSM, System z9)

Special purpose appliance (e.g. Decru or Neoscale)*

In the storage device

Data Path

Considerations:

- Key Management – where is it done?
- Performance (encrypted data does not compress)
- Integration with existing infrastructure
- Cost – server *versus* appliance *versus* storage device

* TotalStorage Proven

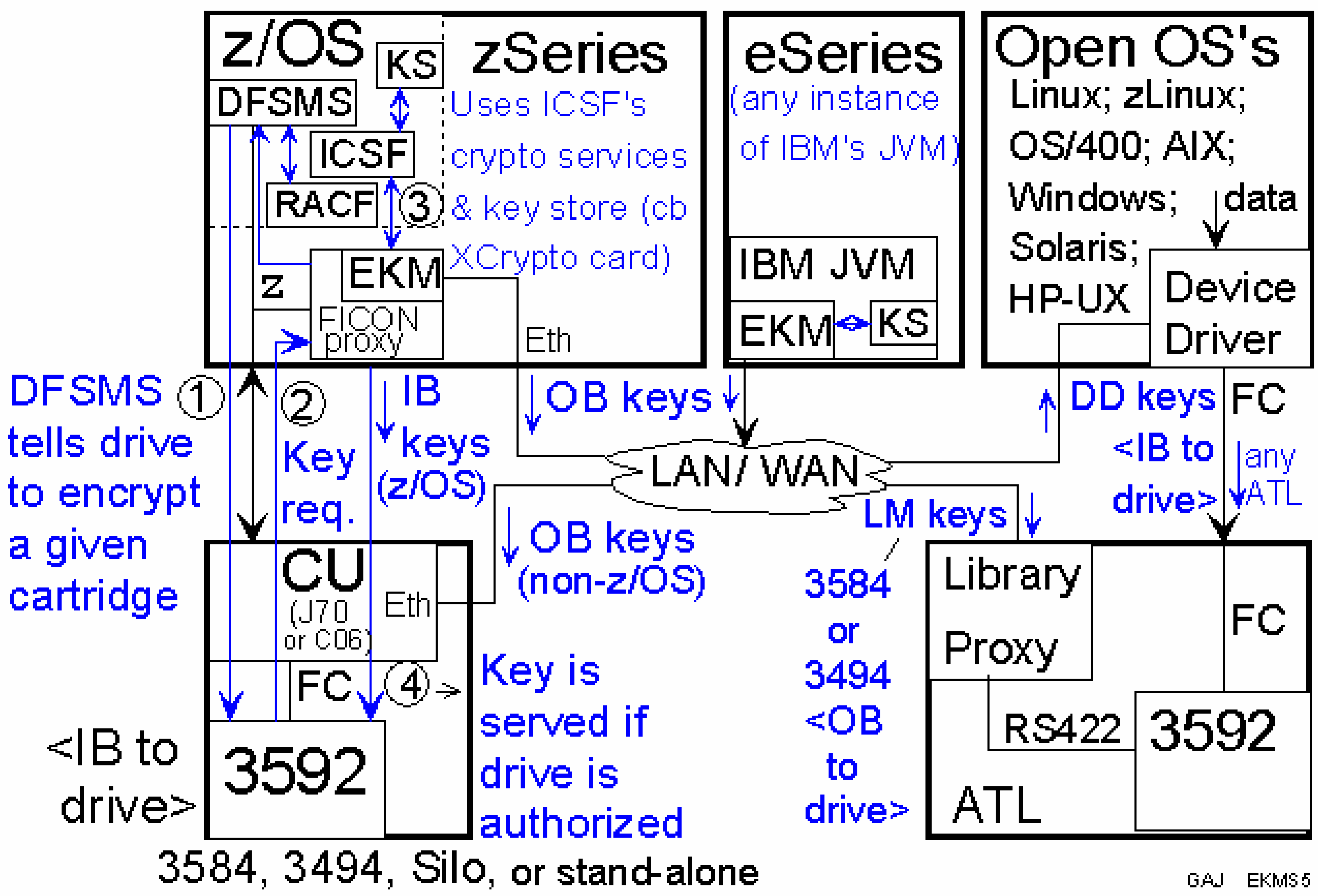
IBM's Tape Data Encryption Solution: the industry's first comprehensive tape security solution

- **The industry's first encrypting tape drive – IBM System Storage TS1100 tape drive family**
  - Standard feature on all TS1120 Model E05 drives
  - Chargeable upgrade feature for existing E05 drives

- **A new, innovative Encryption Key Manager (EKM) component for the Java™ platform supported on a wide range of systems including:** z/OS, i5/OS, AIX, HP, Sun, Linux and Windows

Encryption Key Manager

- **Integration with existing IBM tape systems and libraries**
- **New capabilities for Tivoli Storage Manager to exploit outboard encryption**
- **Integration with System z encryption key, policy management, security and cryptographic capabilities:** complements existing System z Encryption Facility for z/OS program product
- **New services and consulting for tape data encryption and management**

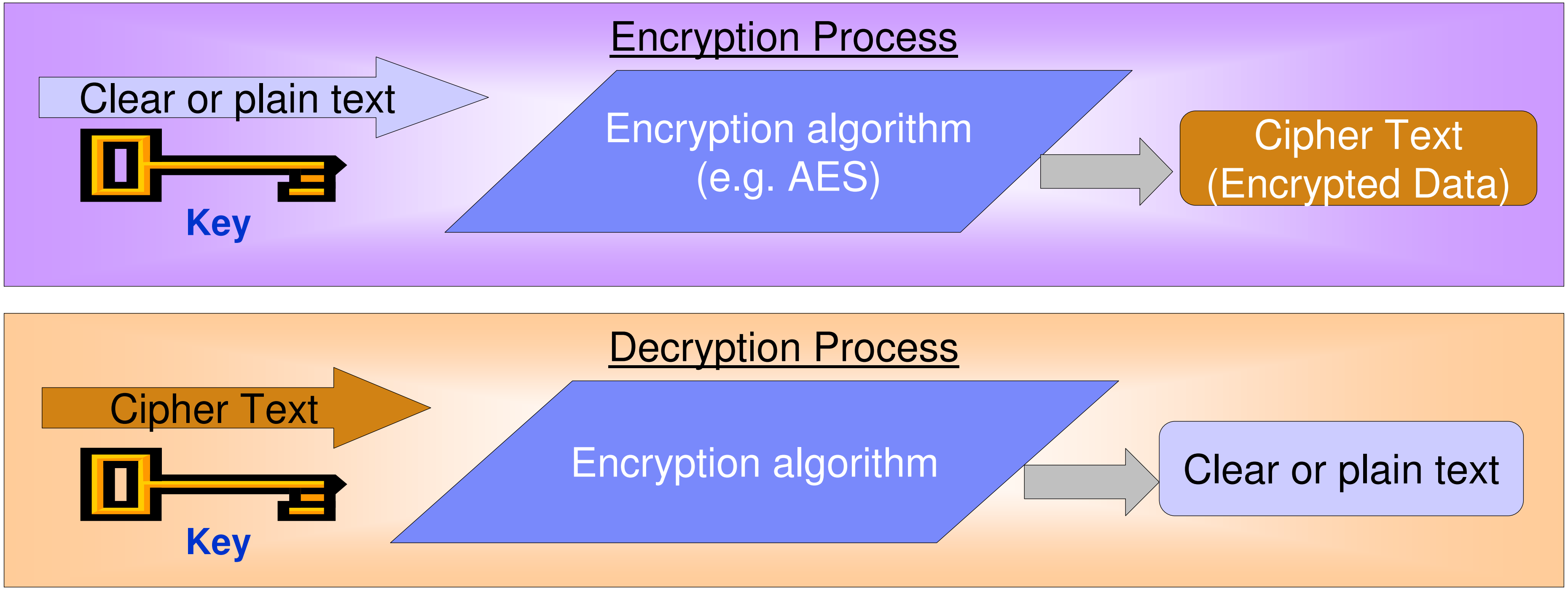


Transparent Key Serving, made simple ;->

Agenda

- Topic Overview
- **Encryption algorithms**
- How does it work with the IBM solution?
- How do I trigger IBM tape encryption?
- How do I manage the keys?
- Do I already have it?
- How do I implement it?
- What environments are supported?
- Where can I go for more detailed information?

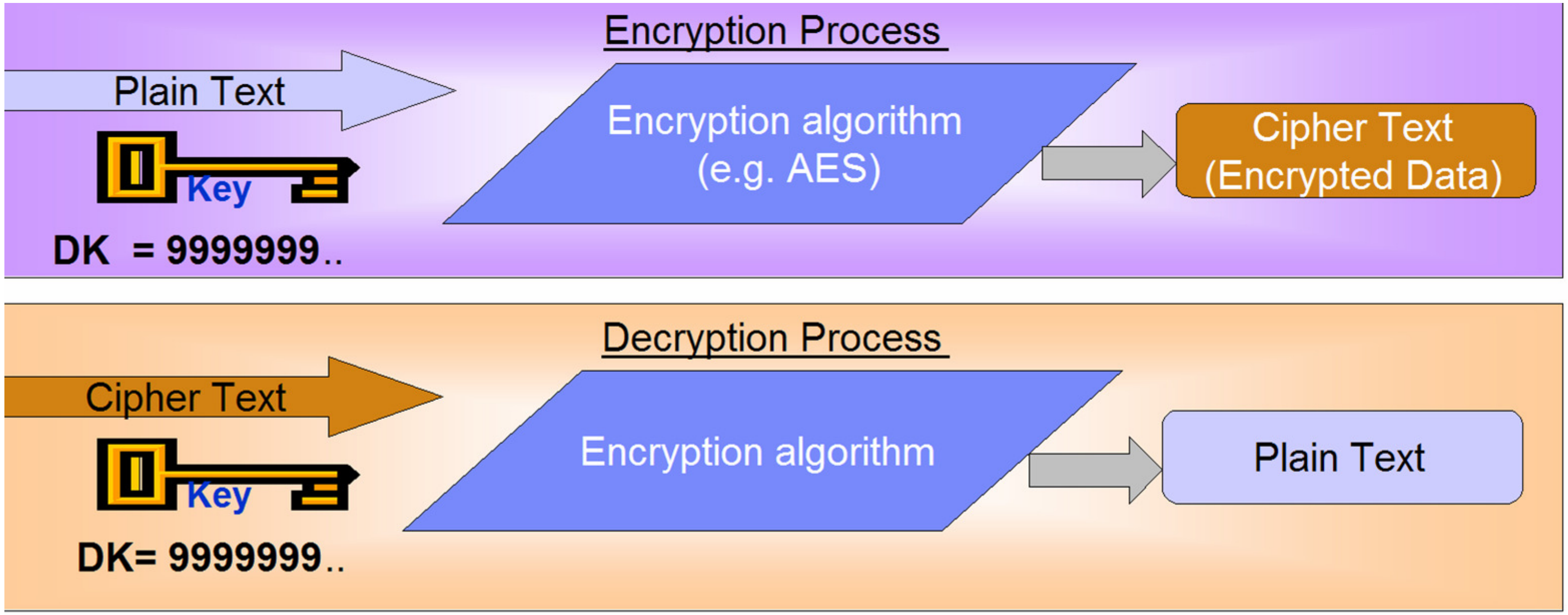
Encryption / Decryption Process



- **Data that is not encrypted is referred to as "clear text"**
- **"Clear text" is encrypted by processing with a "key" and an "encryption algorithm"**
  - Several standard algorithms exist, include DES*, TDES and AES
- **Keys are bit streams that vary in length**
  - For example AES supports 128, 192 and 256 bit key lengths

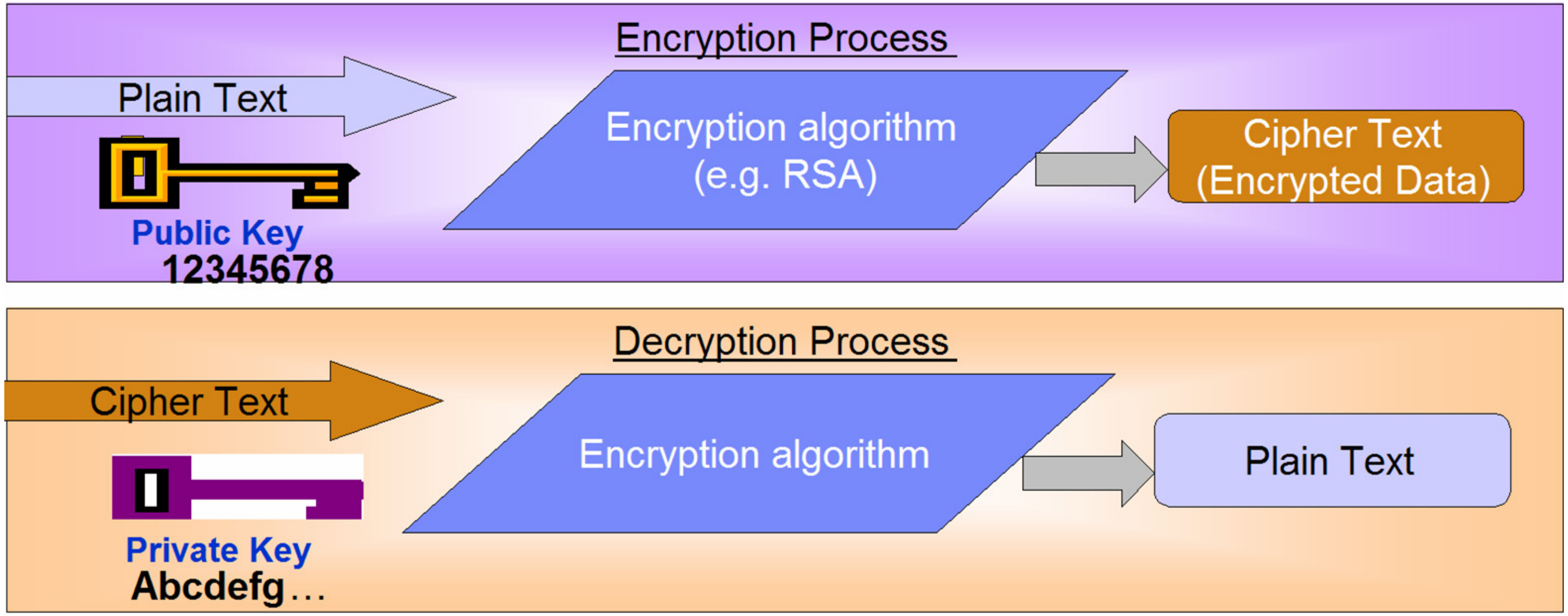
*DES, invented by IBM in 1974

Symmetric Encryption



- **Symmetric encryption – same key to encrypt and decrypt**
  - e.g. your hotel room

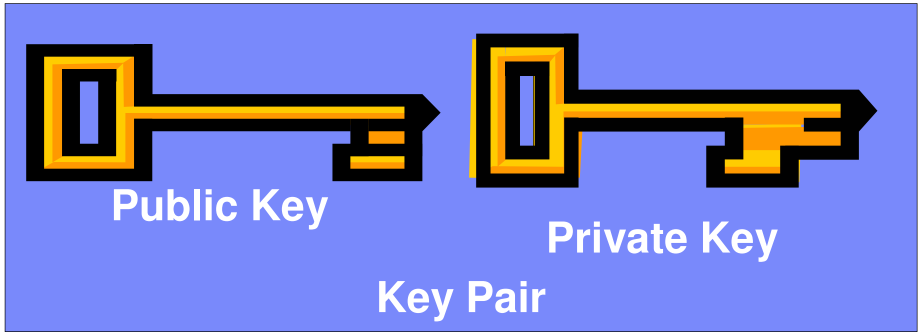
Asymmetric Encryption



- **The key used to encrypt is often referred to as the *Public key***
  - e.g. the KEKs used to wrap the DK and create the EEDKs *(we will see later on what those terms mean)*
- **The *Public key* may be made widely available without fear of compromise**
- **The Key used to decrypt is referred to as the *Private key***
- ***Private Keys* must be secured against unauthorized access !**
- ***Public / Private encryption* is widely used for exchange of data between organizations (eMail)**

IBM uses **both** methods in the implementation

Symmetric Key



- **One key to encrypt and decrypt**
- **e.g. DES, TDES, AES, AES256**
- **Why? Because it’s fast**
- **Used *within* an enterprise**
- **AES256 used by the TS1120 to encrypt data “on the fly”**
  - using the Data Key (DK)

- **Key pairs**
  - Public Key to Encrypt
  - Private Key to Decrypt
- **e.g. Diffie-Hillman, RSA***
- **Public key can be freely distributed**
- **Private key must be secured**
- **Used for the exchange of data *between* organizations**
- **RSA* used to by the Encryption Key Manager to protect the data key**

*Name of the three mathematics Rivest, Shamir and Adleman

Encryption Terms

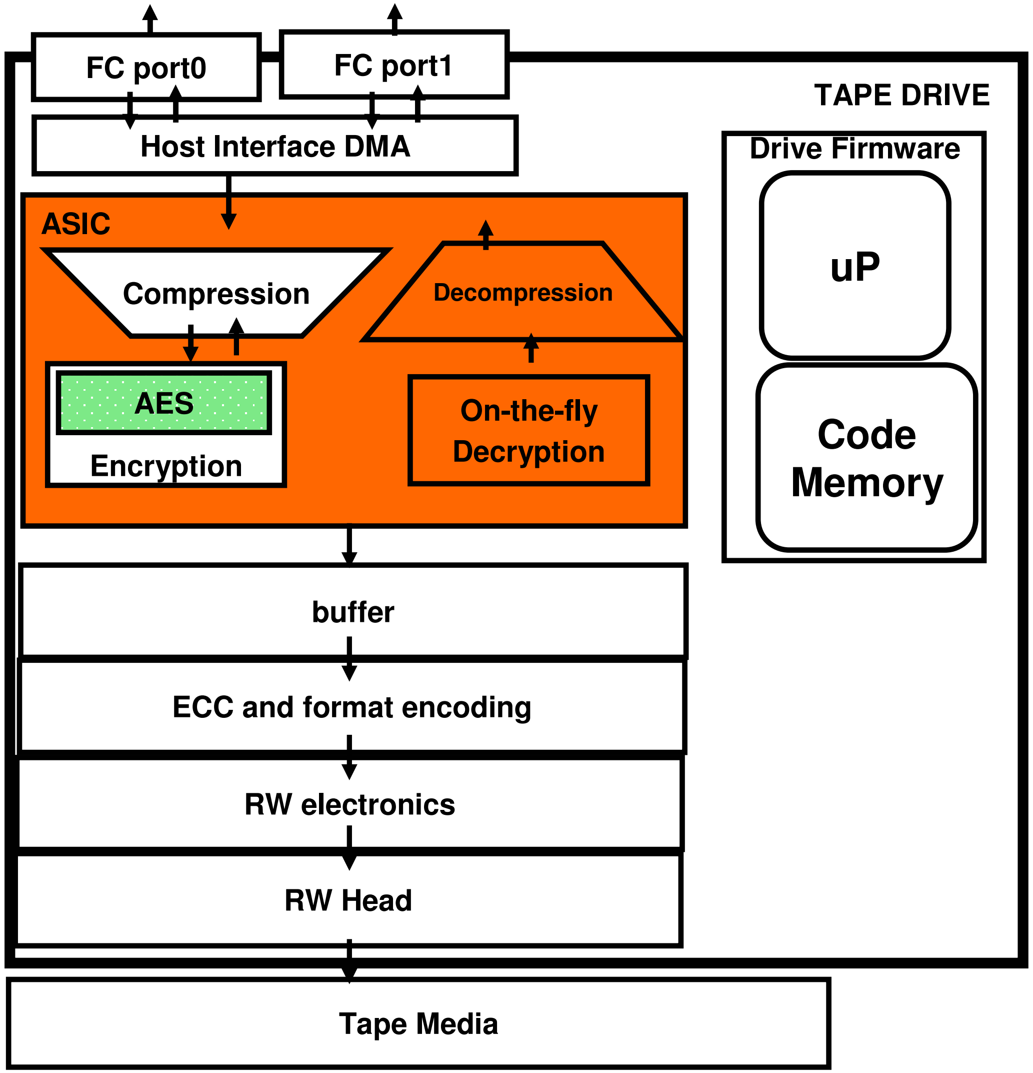
- **Symmetric / Private Key / Secret Key Encryption**
  - Single unique key
  - e.g. DES, TDES, AES, AES256
  - DK (Data Key)
- **Asymmetric / Public Key / Public-Private Key Pair**
  - Two different unique keys
  - e.g. RSA, Diffie-Hellman
  - KEK (Key Encrypting Key)
  - Certificate
- **Keystore**
- **Crypto Services**
- **Clear Text**
- **Wrapping a Key, EEDK (Externally Encrypted Data Key)**
- **Rekeying**

Agenda

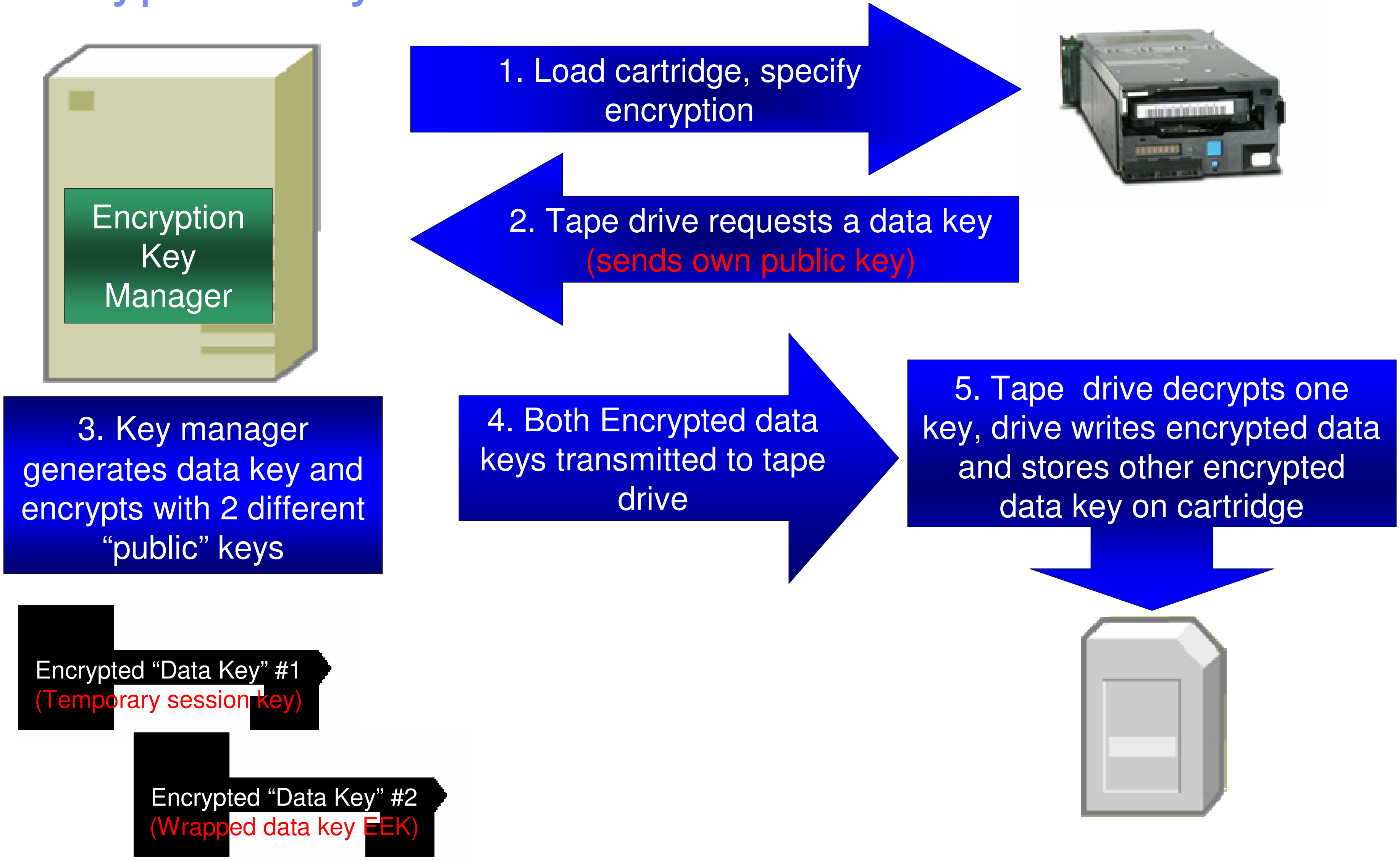
- Topic Overview
- Encryption algorithms
- **How does it work with IBM tape?**
- How do I trigger IBM tape encryption?
- How do I manage the keys?
- Do I already have it?
- How do I implement it?
- What environments are supported?
- Where can I go for more detailed information?

Encrypting tape drive elements

- Built-in AES 256-bit data encryption engine
- Located “below” compression engine
  - Virtually no performance or capacity impact (<1%)
  - data can be compressed and be encrypted simultaneous



Encryption Key Generation and Communication



Encryption Key Manager

1. Load cartridge, specify encryption

2. Tape drive requests a data key (sends own public key)

3. Key manager generates data key and encrypts with 2 different “public” keys

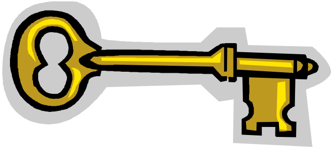
4. Both Encrypted data keys transmitted to tape drive

5. Tape drive decrypts one key, drive writes encrypted data and stores other encrypted data key on cartridge

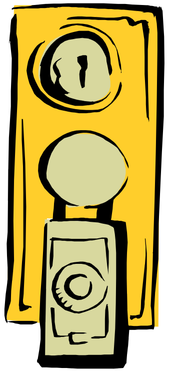
Encrypted “Data Key” #1
(Temporary session key)

Encrypted “Data Key” #2
(Wrapped data key EEK)

Wrapping of Data Keys

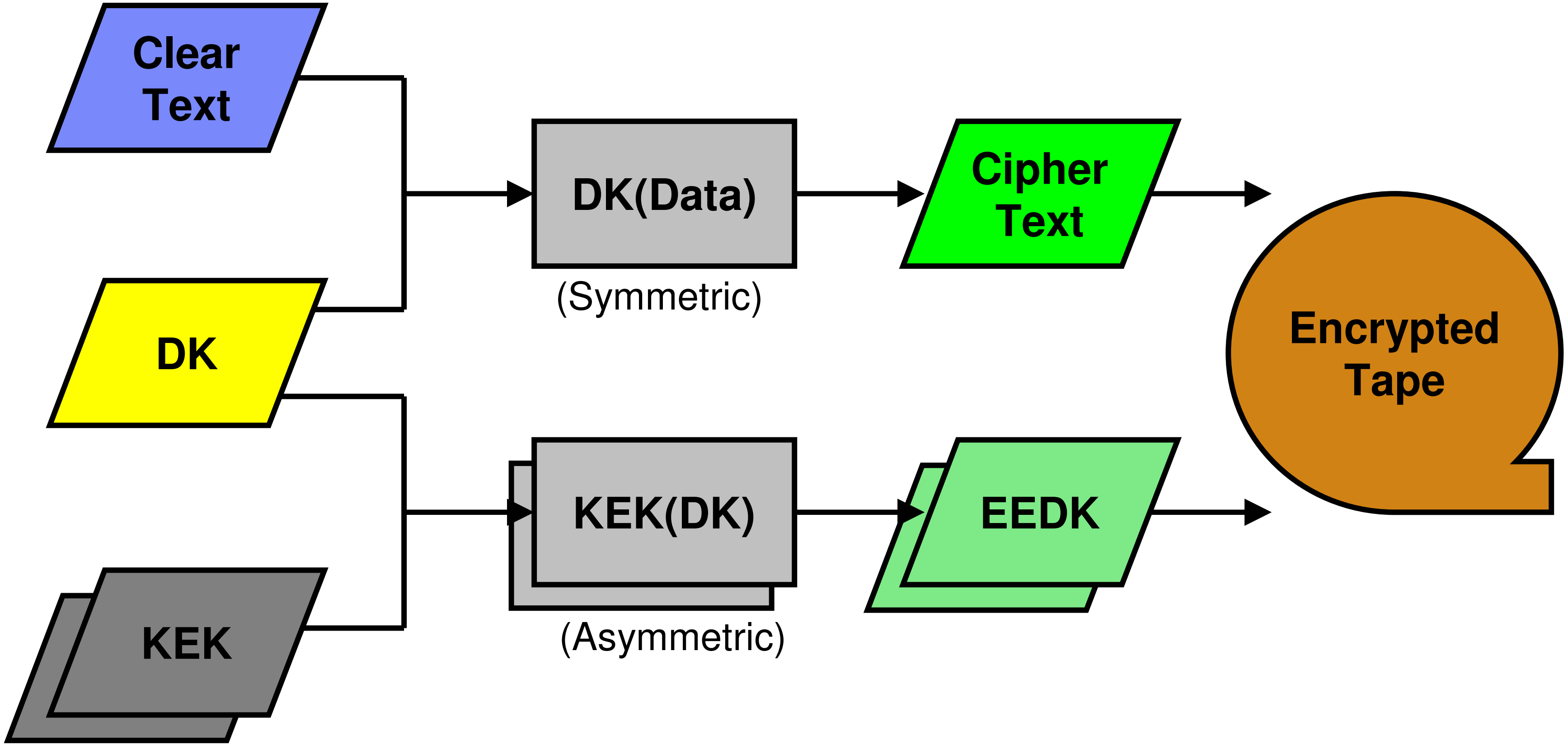


- **Data Key (DK) – 00100111001000…**
  - Symmetric Encryption AES-256
  - Random number generated by Crypto Provider Services
  - Used to encrypt/decrypt data
  - Very fast



- **Key Encrypting Key (KEK) Pair**
  - Asymmetric Encryption RSA-2048
  - Created by the Customer/Business Partner/Third Party Provider
  - Public half used to encrypt DK
  - Private half used to decrypt DK
  - Slower than Symmetric
  - Referenced by KEK Labels or Key Labels
  - Metaphor 1 – Real Estate Lock Box (Ultra Paranoid version)
    - Key to the house stored inside (DK)
    - One key can only close the box (public half of KEK)
    - Another key can only open it (private half of KEK)
  - Metaphor 2 – Blue mailbox – Public key is placing a “key” in the public access door,
    private key required to open rear of mailbox to access “key”.

TS1120 Encryption Process



DK – Data Key (Symmetric)
KEK – Key Encrypted Key (Asymmetric)
EEDK – Externally Encrypted Data Key

Encryption Terms

- *EKM* **Encryption Key Manager**
- *DK* **Data Key – used within the drive to do the AES Encryption and Decryption of the Data**
- *EEDK* **Externally Encrypted Data Key is an add. encrypted version of the DK, which is saved on the cartridge**
- *KEK* **Key Encrypting Key is the real key and the method to encrypt and decrypt the DK's (EEDK <-> DK)**
- *SEDK* **Session Encrypted Data Key - with the SK encrypted DK as a safety for the DK at that time it is transmitted from the EKM to the drive**
- *SK* **Session Key – Encryption and Decryption of the DK for SEDK and vice versa (SEDK <-> DK)**

KEK(DK)= EEDK SK(DK)= SEDK

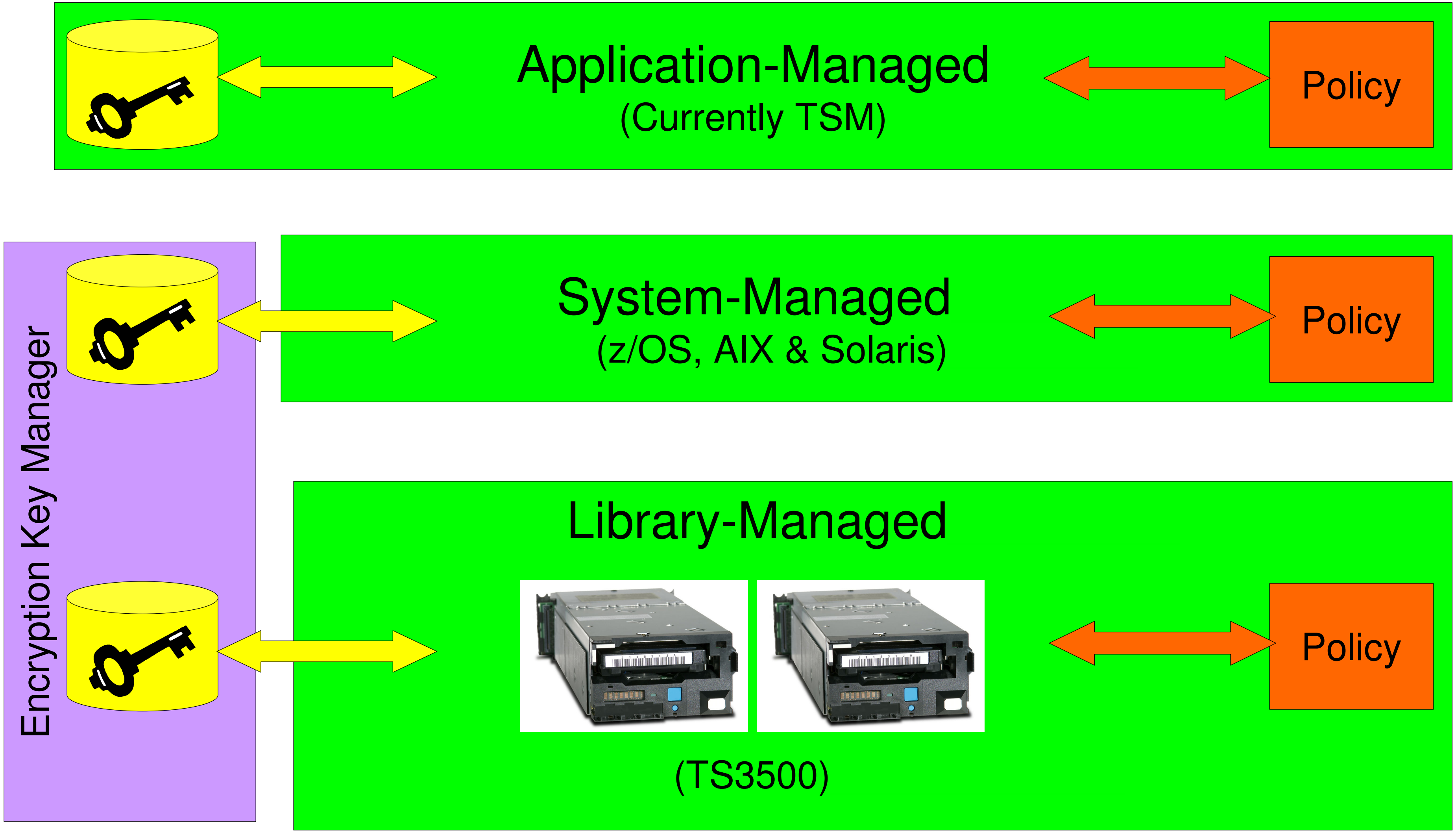
Some basic rules about TS1120 Encryption

- **Whether a volume is encrypted is determined when the first file sequence is written**
- **If the first file written to a volume is encrypted, all additional files written to that same volume will also be encrypted.**
  - There will NOT be a mix of encrypted and non-encrypted data on the same volume
  - All data written to the same volume will be encrypted under the same data key
- **Each volume will have its own data key**
  - An encrypted form of the data key is stored on the cartridge
- **For multi-volume data sets, each volume will have its own data key but will use the same key label**

Agenda

- Topic Overview
- Encryption algorithms
- How does it work with IBM tape?
- **How do I trigger IBM tape encryption?**
- How do I manage the keys?
- Do I already have it?
- How do I implement it?
- What environments are supported?
- Where can I go for more detailed information?

IBM Encryption Methods



Application-Managed

(Currently TSM)

Policy

Encryption Key Manager

System-Managed

(z/OS, AIX & Solaris)

Policy

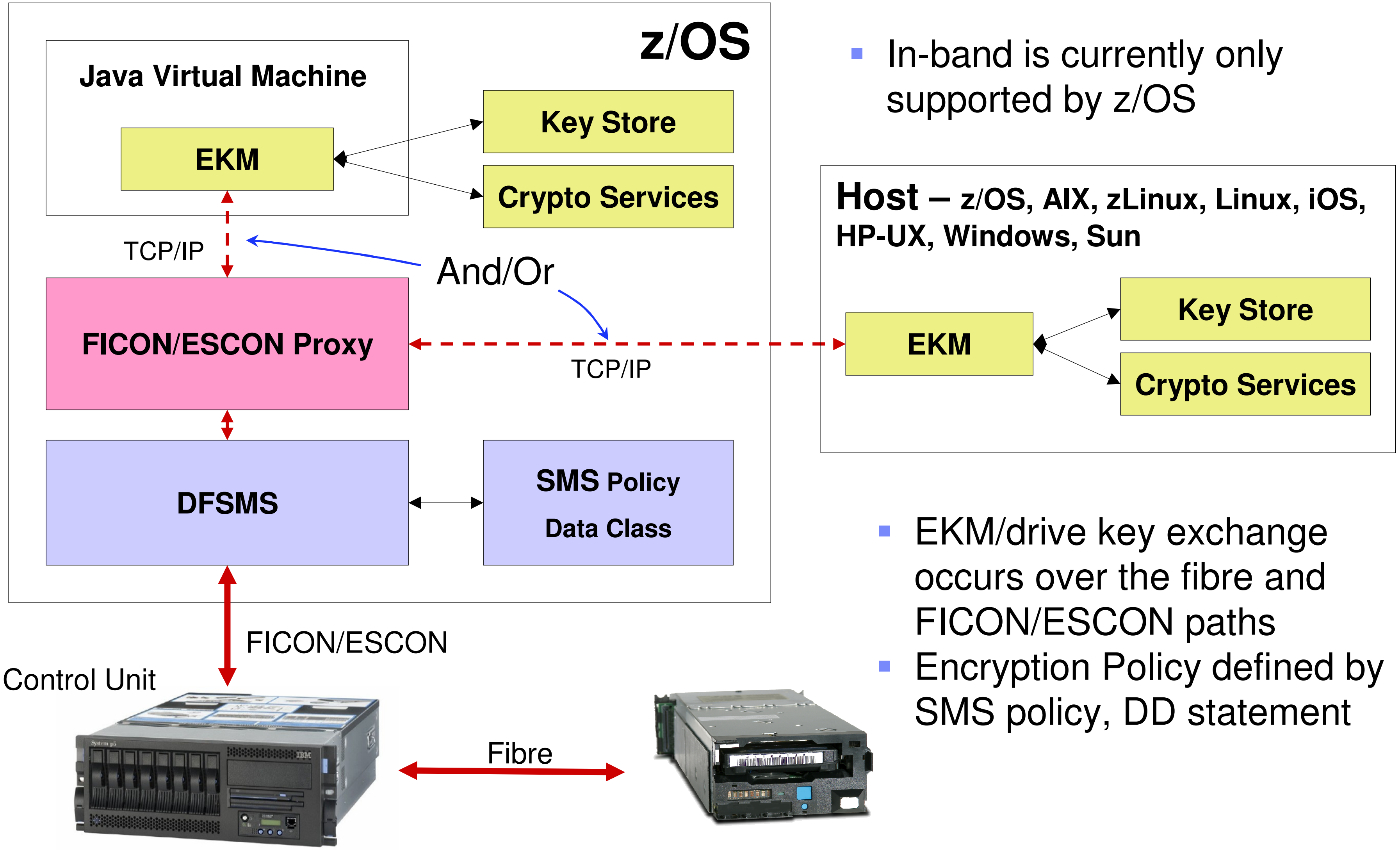
Library-Managed

(TS3500)

Policy

System Managed Encryption Components – z/OS In Band

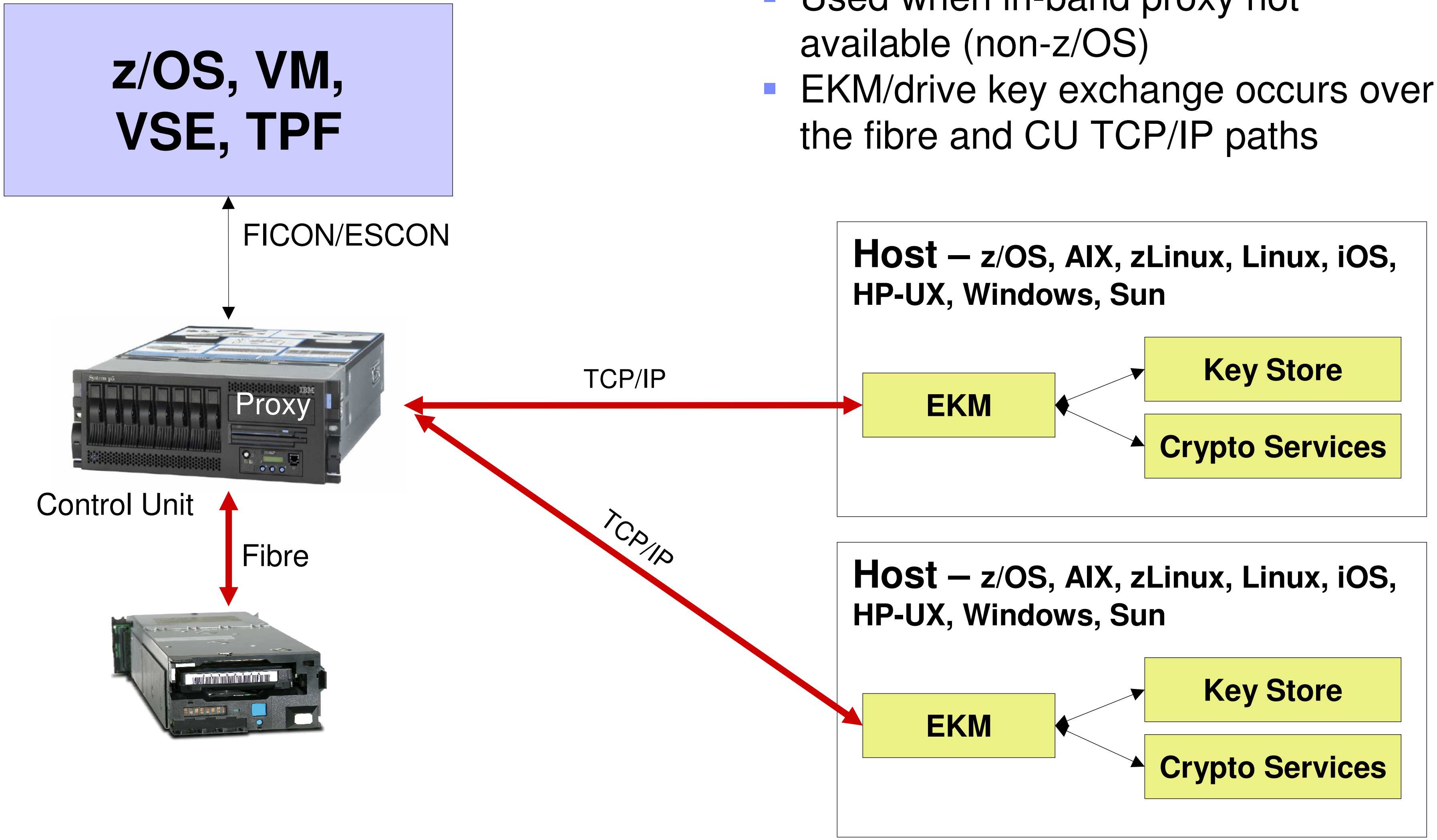
- In-band is currently only supported by z/OS



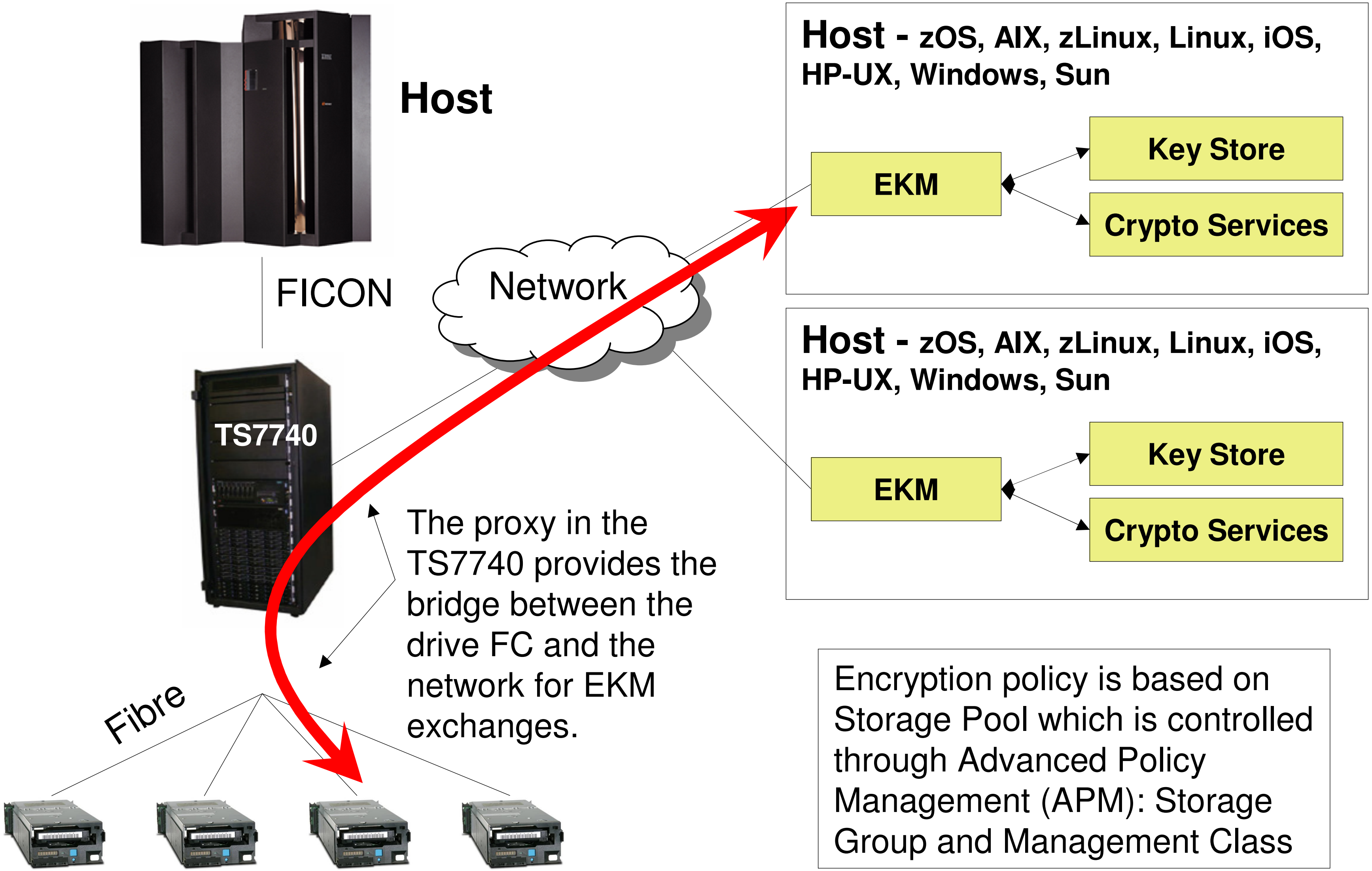
- EKM/drive key exchange occurs over the fibre and FICON/ESCON paths
- Encryption Policy defined by SMS policy, DD statement

System Managed Encryption Components – z/OS Out-of-Band

- Used when in-band proxy not available (non-z/OS)
- EKM/drive key exchange occurs over the fibre and CU TCP/IP paths



Encryption usingTS7740 as the EKM Proxy


Host
FICON
Network
TS7740
Fibre
Host - zOS, AIX, zLinux, Linux, iOS, HP-UX, Windows, Sun
EKM
Key Store
Crypto Services
Host - zOS, AIX, zLinux, Linux, iOS, HP-UX, Windows, Sun
EKM
Key Store
Crypto Services

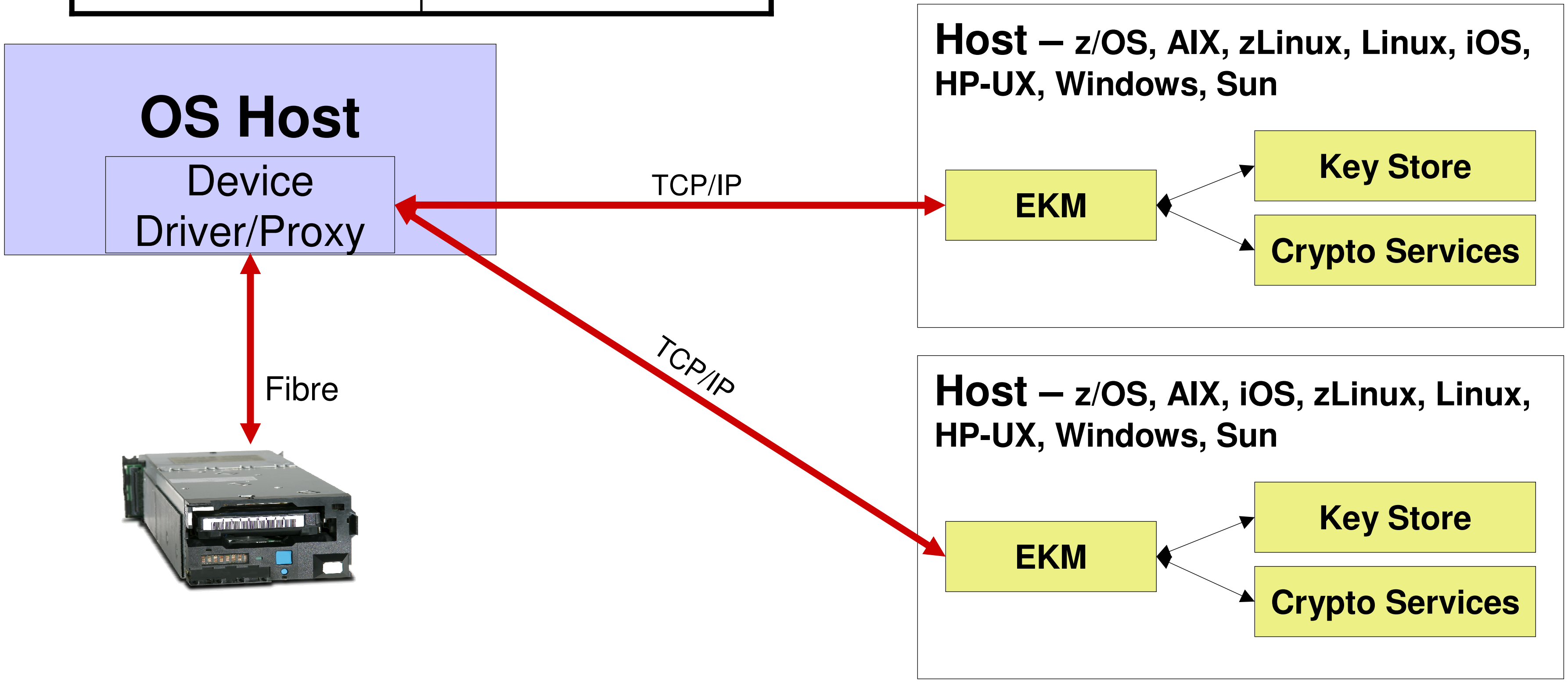
The proxy in the TS7740 provides the bridge between the drive FC and the network for EKM exchanges.

Encryption policy is based on Storage Pool which is controlled through Advanced Policy Management (APM): Storage Group and Management Class

System Managed Encryption Components – Open Systems

Operating System	Device Driver
AIX	Atape
Sun Solaris	IBMTape

- EKM/drive key exchange occurs over the fibre and TCP/IP paths
- Encryption Policy defined in device driver



OS Host

Device Driver/Proxy

TCP/IP

TCP/IP

Fibre

Host – z/OS, AIX, zLinux, Linux, iOS, HP-UX, Windows, Sun

EKM

Key Store

Crypto Services

Host – z/OS, AIX, iOS, zLinux, Linux, HP-UX, Windows, Sun

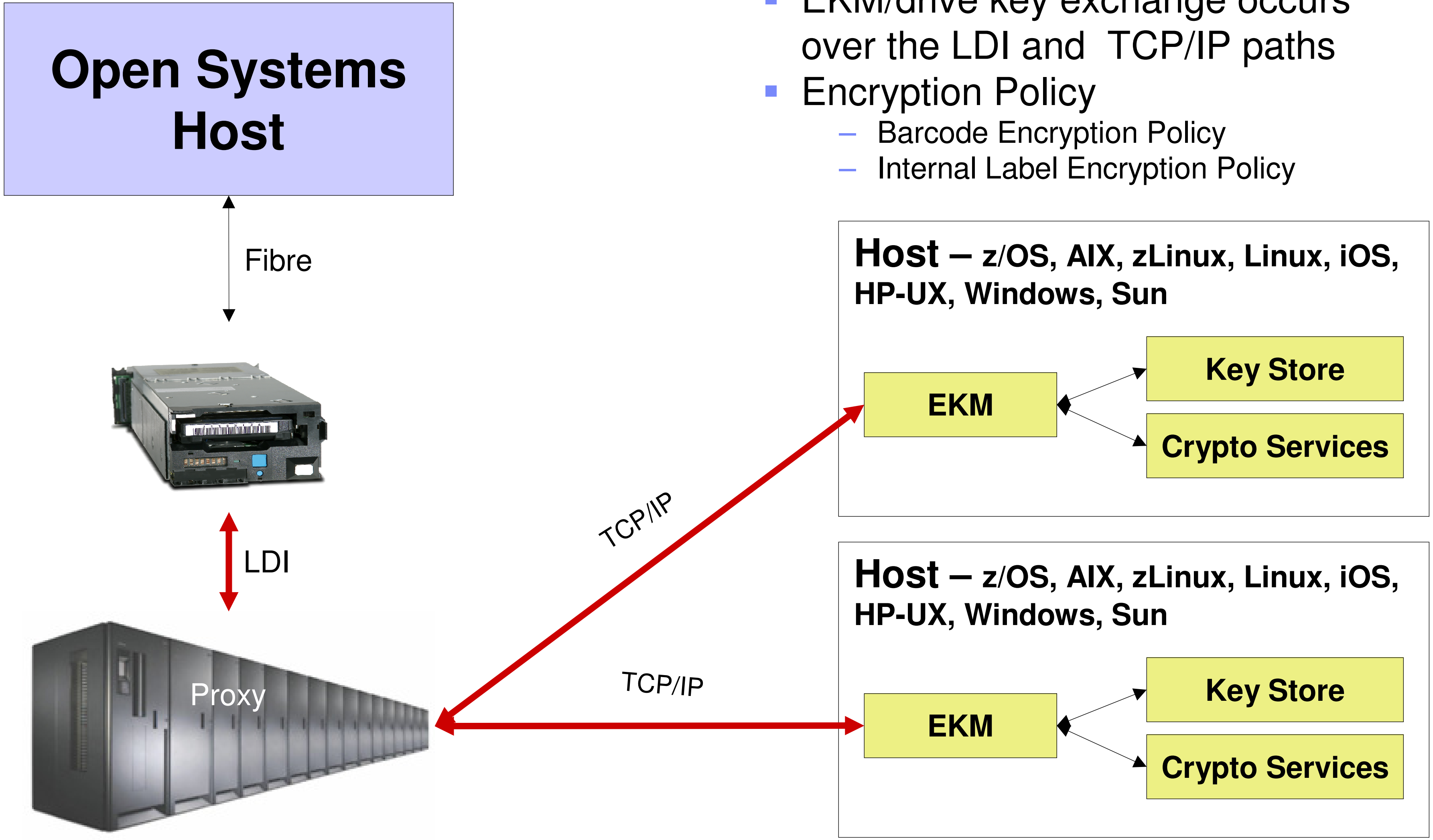
EKM

Key Store

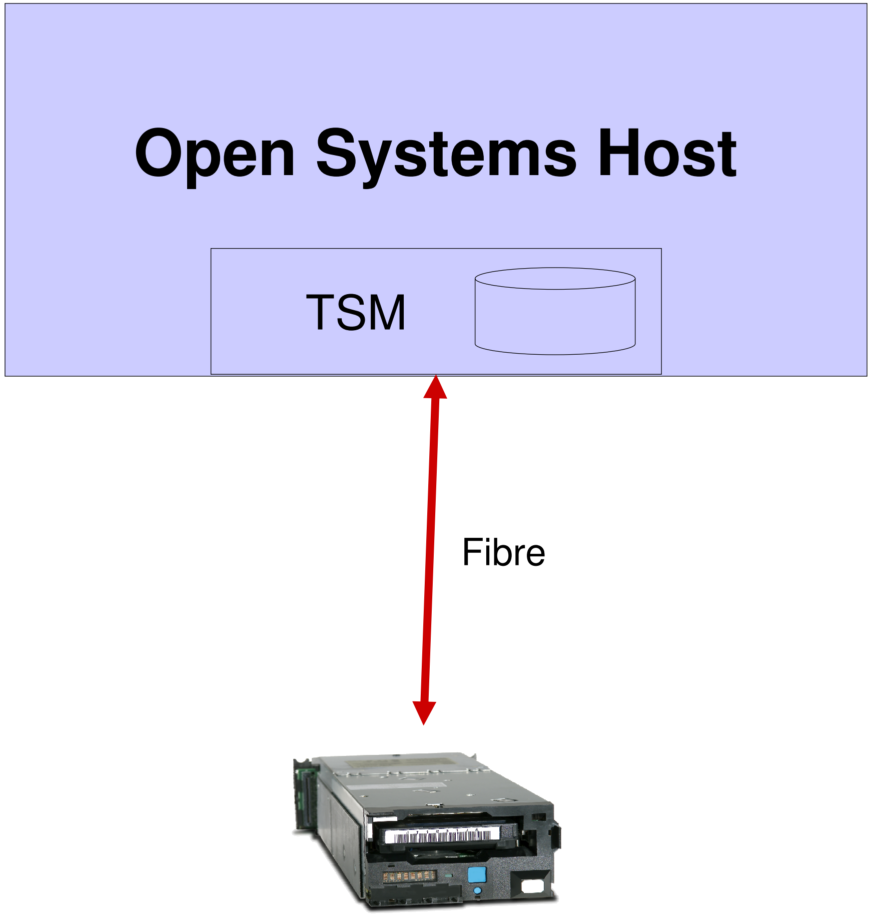
Crypto Services

Library Managed Encryption Components

- EKM/drive key exchange occurs over the LDI and TCP/IP paths
- Encryption Policy
  - Barcode Encryption Policy
  - Internal Label Encryption Policy


Open Systems Host
Fibre
LDI
Proxy
TCP/IP
TCP/IP
Host – z/OS, AIX, zLinux, Linux, iOS, HP-UX, Windows, Sun
EKM
Key Store
Crypto Services
Host – z/OS, AIX, zLinux, Linux, iOS, HP-UX, Windows, Sun
EKM
Key Store
Crypto Services

Application Managed Encryption Components



- TSM Handles Data Keys
  - Generates Data Keys
  - Key is passed across fibre to the drive
  - Stores DK in its database
  - DK is encrypted in TSM database
  - DK is not stored on tape
- Application Managed Encryption for TSM not supported on z/OS
- Encryption Policy determined by TSM DevClass

IBM Tape Encryption Methods

Encryption Method	Policy Encrypt?	Policy Key Label?	Data Key Generation
Application	TSM Devclass	NA	TSM
System Open	Atape/IBMtape Device Driver	Encryption Key Manager (EKM)	Encryption Key Manager (EKM)
System z/OS	DFSMS Data Class or JCL DD	DFSMS Data Class, JCL DD or EKM	Encryption Key Manager (EKM)
Library **(log. Lib or Volser range)**	TS3500 (3584) TS3400 (3577) Web Interface	TS3500 (3584) TS3400 (3577) Web Interface or EKM	Encryption Key Manager (EKM)

Agenda

- Topic Overview
- Encryption algorithms
- How does it work with IBM tape?
- How do I trigger IBM tape encryption?
- **How do I manage the keys?**
- Do I already have it?
- How do I implement it?
- What environments are supported?
- Where can I go for more detailed information?

Encryption key management is a particularly important and challenging part of an enterprise tape encryption solution

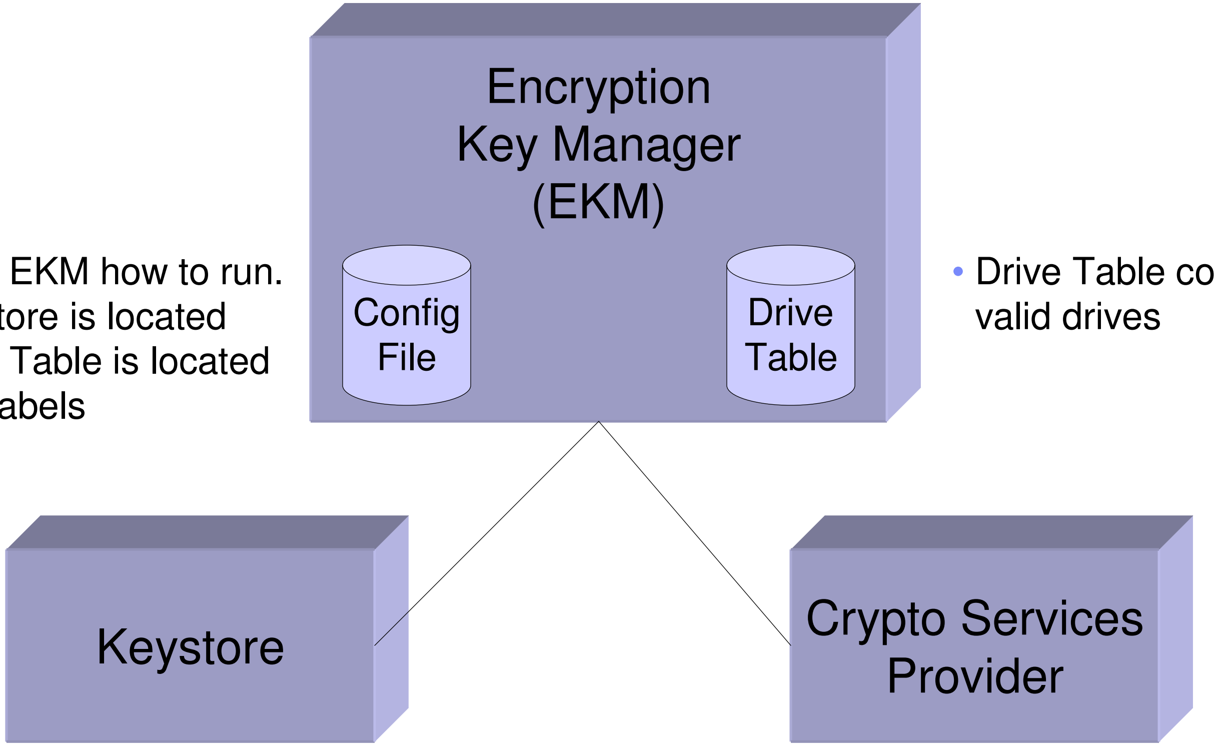
Encryption keys used to encrypt tape data cartridges must be rigorously managed because:

- there are many tape cartridges
- they are created in many systems environments
- they may be stored for a long time
- they require high levels of availability, security and audit ability

Encryption Key Manager Overview

- Runs in IBM Java Runtime Environment (JRE)
- Supplied free from IBM
- Does not perform any crypto operations itself

- Config File tells EKM how to run.
  - Where Keystore is located
  - Where Drive Table is located
  - Default key labels



- Drive Table contains list of valid drives

- Hardware or Software based
- Stores certificates and keys

- Hardware or Software based
- Generates Data Keys (DK)
- Wraps/Unwraps/Rewraps DKs

Encryption Key Manager - EKM

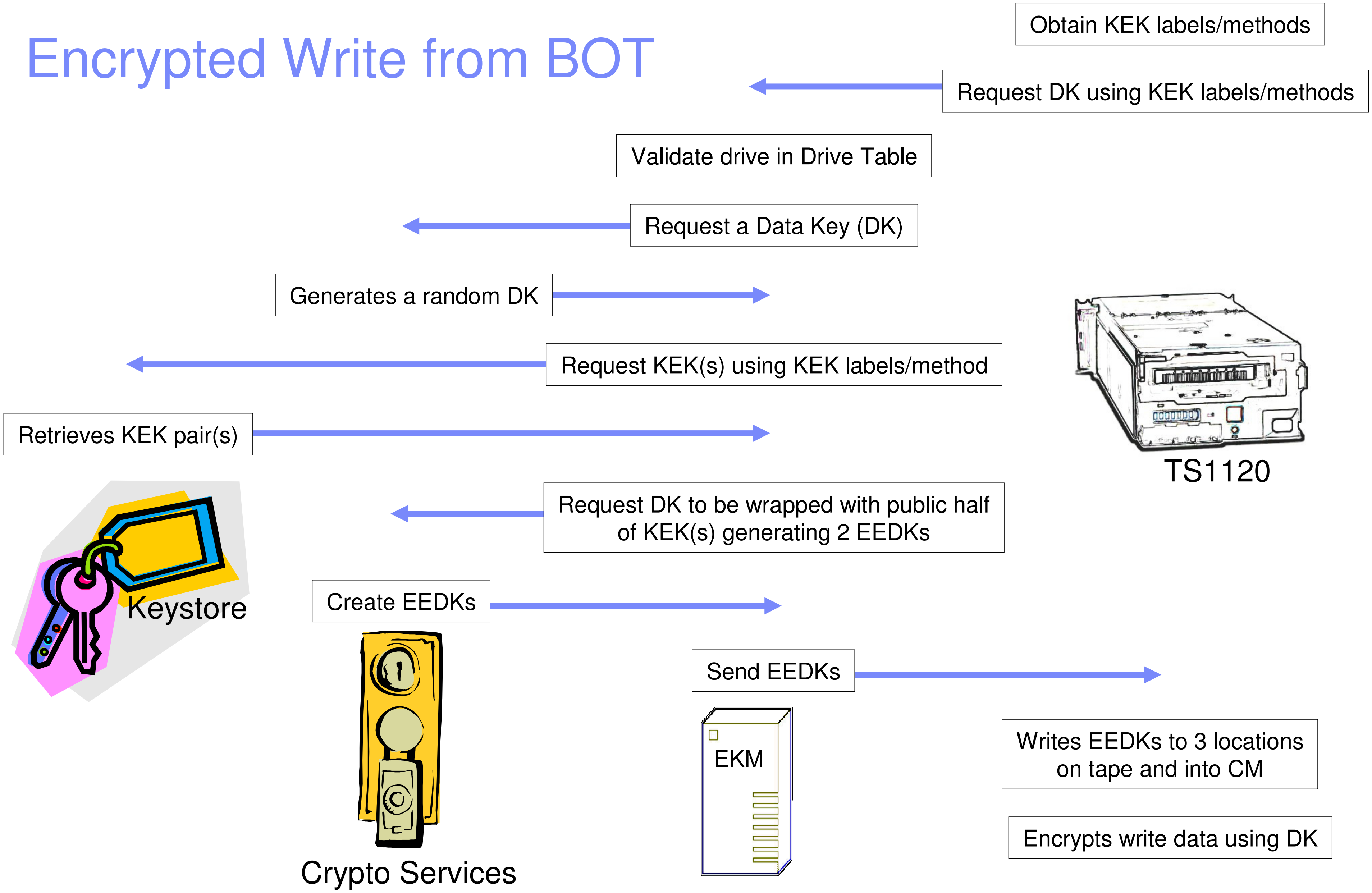
- **Part of IBM JRE**
- **Generates encryption keys**
- **On writes**
  - Generates encryption key to be used by the drive in encrypting data
- **On reads**
  - Determines the encryption key used to encrypt data
  - Supplies this key to the drive for use in decrypting data

Encryption Keystore

- **Maintained on server or in hardware crypto device**
- **Contains key label, public keys and private keys**
- **Populated by self generated or imported certificates**
- Example:

Key Label	Public Key	Private Key
Acme	12345…	abcde…
Offsite BP RR	98765…	Not Available

Encrypted Write from BOT



Obtain KEK labels/methods

Request DK using KEK labels/methods

Validate drive in Drive Table

Request a Data Key (DK)

Generates a random DK

Request KEK(s) using KEK labels/method

Retrieves KEK pair(s)

Request DK to be wrapped with public half of KEK(s) generating 2 EEDKs

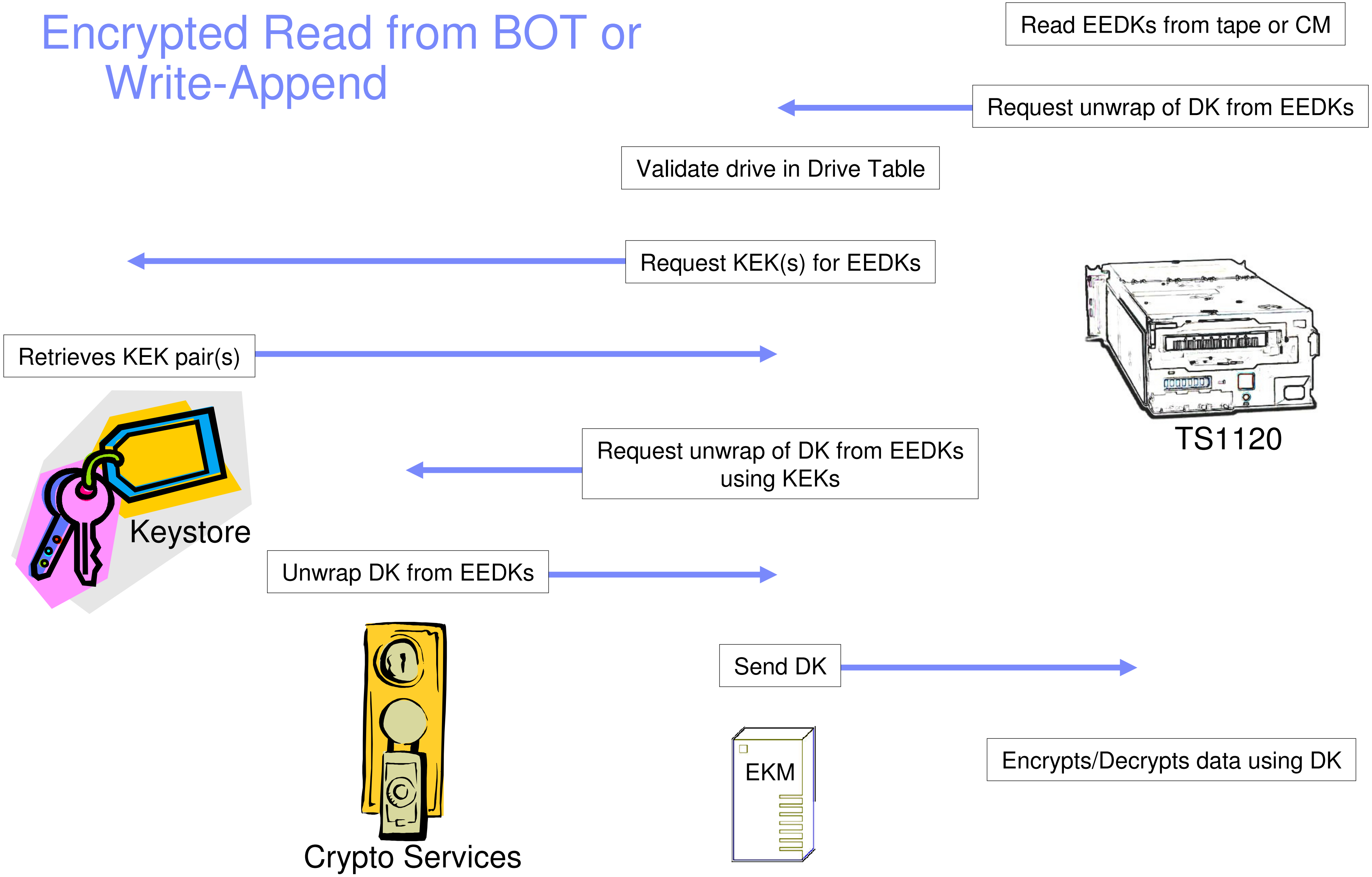
Create EEDKs

Send EEDKs

Writes EEDKs to 3 locations on tape and into CM

Encrypts write data using DK

Encrypted Read from BOT or Write-Append



Read EEDKs from tape or CM

Request unwrap of DK from EEDKs

Validate drive in Drive Table

Request KEK(s) for EEDKs

Retrieves KEK pair(s)

Request unwrap of DK from EEDKs using KEKs

Unwrap DK from EEDKs

Send DK

Encrypts/Decrypts data using DK

Agenda

- Topic Overview
- Encryption algorithms
- How does it work with IBM tape?
- How do I trigger IBM tape encryption?
- How do I manage the keys?
- **Do I already have it?**
- How do I implement it?
- What environments are supported?
- Where can I go for more detailed information?

TS1120 Tape Drive Encryption Capable

- **Automatically shipped on <u>all new drives</u> shipped 9.8.2006 or later**
  - Feature Code # 9592 – Encryption Capable – Plant
  - No charge (NC) feature
  - Identified by label on drive canister
- **Can be added to existing TS1120 3592E05s by MES Upgrade**
  - Feature Code # 5592 – Encryption Capable – Field
  - Chargeable feature (~£4K list)
  - CE Installed – new hardware and drive microcode
- **Limitations on use of encryption**
  - Not supported when E05 used in J1A Emulation Mode
  - VTS support TS7700 only

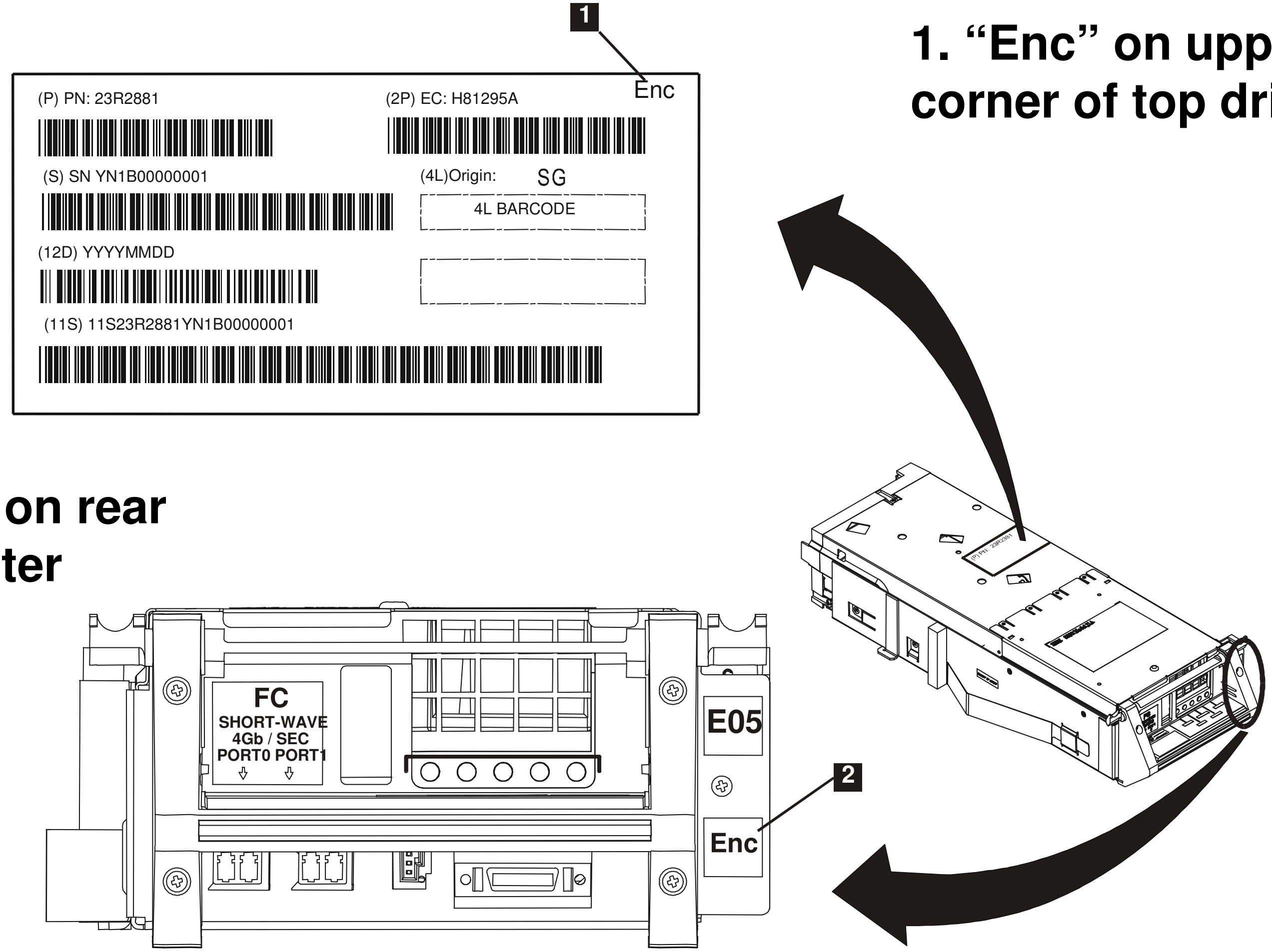
“Capable” but not “Enabled”

- **Default on shipment is encryption capable but not enabled**
  - Identified on drive by external label, and service panel
- **If not using encryption, no effect on drive or customer environment**
- **If using encryption, drive installation environment determines how it should be enabled:**
  - TS3500 installed – customer enables/configures at TS3500
  - Open Systems with 3494, rack or silo – CE enables/configures on each drive
  - z/OS with 3494, rack or silo – CE enables/configures on each drive

Encryption Capable – label on drive canister

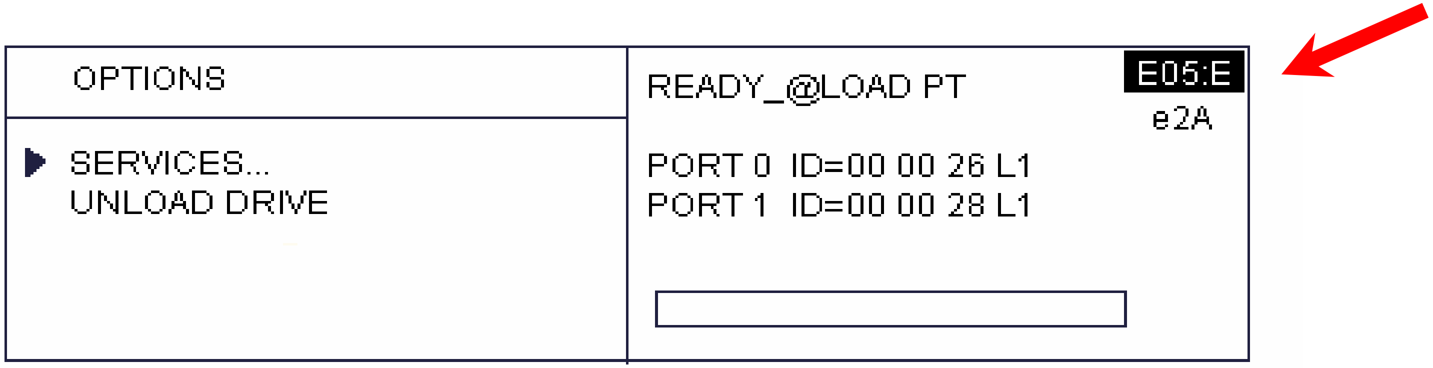
1. "Enc" on upper right corner of top drive label

2. "Enc" label on rear of drive canister



Encryption Capable – Service Panel Display

- Drive Model information
  - Upper right corner shows drive model informatior
  - Supported E05 drive configurations:
    - E05-FE (original, non-encryption capable)
    - **E05:e** (encryption capable but not enabled)
    - **E05:E** (encryption enabled)
    - **J1A*e** (encryption capable but not enabled, emulating a J1A drive)

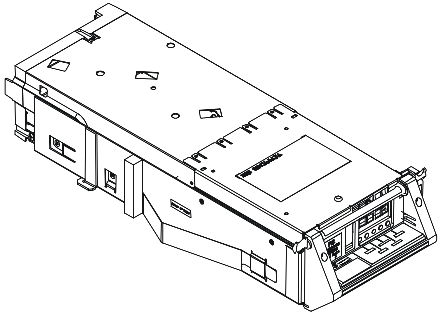


```
OPTIONS                         READY_@LOAD PT            E05:E
                                                           e2A
▶ SERVICES...                   PORT 0  ID=00 00 26 L1
  UNLOAD DRIVE                  PORT 1  ID=00 00 28 L1
```

Agenda

- Topic Overview
- Encryption algorithms
- How does it work with IBM tape?
- How do I trigger IBM tape encryption?
- How do I manage the keys?
- Do I already have it?
- **How do I implement it?**
- What environments are supported?
- Where can I go for more detailed information?

IBM Tape Data Encryption



- **TS1120 Enterprise Tape Drive**
  - Addresses tape data security concerns
  - NC standard feature on all new TS1120 Tape Drives
  - Chargeable upgrade feature for existing TS1120s

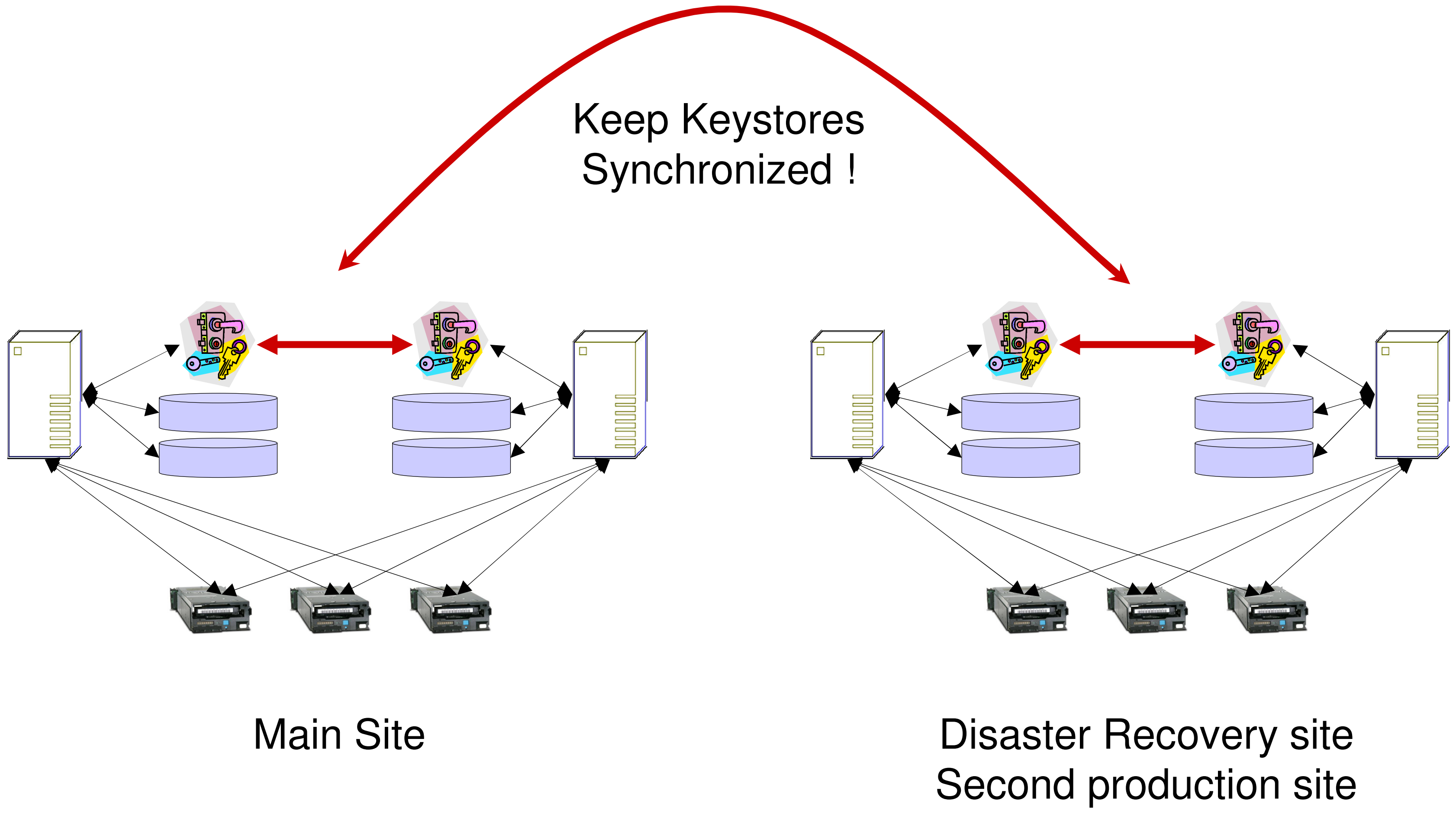
- **IBM Encryption Key Manager (EKM)**
  - IBM Java component
  - z/OS, i5/OS, AIX, HP, Sun, Linux and Windows
  - Generates and serves keys to TS1120 tape drive
  - Obtains encryption keys from the keystore

Encryption Key Manager

EKM Implementation

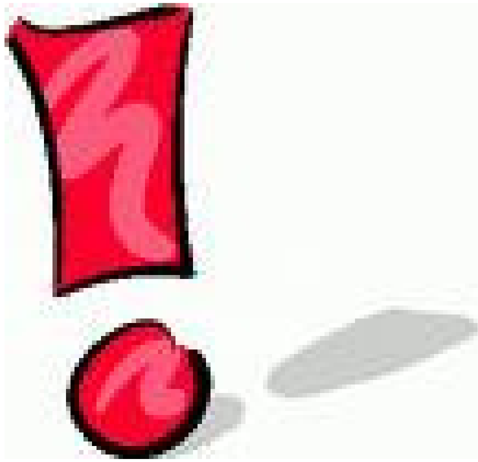
1. Decide on EKM Server Deployment
2. Choose KeyStore
3. Define KeyStore
4. Import / Create keys and certificates into KeyStore
5. Install EKM
6. Define EKM configuration file
7. Define tape drives to EKM
8. Start EKM

Multiple EKM Servers – Multiple Sites



Advice on working with keys/certificates

- **Don't lose your (public/private) keys and certificates**
- **Don't leave your (public/private) keys and certificates lying around**
- **Make sure you backup your (public/private) keys and certificates**



Agenda

- Topic Overview
- Encryption algorithms
- How does it work with IBM tape?
- How do I trigger IBM tape encryption?
- How do I manage the keys?
- Do I already have it?
- How do I implement it?
- **What environments are supported?**
- Where can I go for more detailed information?

Encryption Management supported options: based on operating system and tape drive attachment

Open-attach IBM Library	Open-attach Rack or Silo	Mainframe-attach IBM Library	Mainframe-attach Rack or Silo
Application Managed (TSM only) System Managed (AIX, Solaris only) Library Managed (TS3500 only)	Application Managed (TSM only) System Managed (AIX, Solaris only)	System Managed (z/OS only)	System Managed (z/OS only)

Encryption support:

- **Application Managed**
  - Tivoli Storage Manager (AIX, Window Servers) 5.4.3
- **System Managed**
  - z/OS 1.6, 1.7 & 1.8 (via DFSMS)
  - AIX 5.2 and later (via device driver: Atape 10.2.5.0)
  - Solaris (via IBM supplied driver: IBMtape 4.1.4.4)
- **Library Managed**
  - TS3400 TS3500 Support for all open systems (requires ISV certification)
  - EKM support on Linux, i5/OS, AIX
  - EKM Support on HP, Sun, Windows
- **TS7700 supported by pool - code R1.2 March 9th 2007.**

EKM support

- **z/OS 1.6, 1.7, 1.8**
- **AIX 5.2 or higher**
- **I5/OS 5.2 or higher**
- **HP-UX 11.0, 11i, and 11.23PI**
- **Sun Solaris 8, 9 and 10**
- **Linux – System z, System p and Intel**
- **Red Hat Enterprise Linux 4 (REHL 4)**
- **SUSE Linux Enterprise Server 9 (SLES 9)**
- **Windows 2000 and 2003**

Supported KeyStores

- **Distributed**
  - JCEKS (file based)
  - PKCS11IMPLKS (PKCS11 hardware crypto)
- **I5**
  - JCEKS (file based)
  - IBMi5OSKeyStore (I5 platform capabilities)
- **z/OS**
  - JCEKS (file based)
  - JCE4758KS/JCECAAKS (ICSF Secure hardware)
  - JCE4785RACFKS/JCECCARACFKS (RACF with secure hardware)
  - JCERACFKS (RACF/SAF)

IBM Statement of Direction: expanded support of TS1120 Tape Drive encryption to other environments

- **z/TPF V1.1 support of the TS1120 Tape Drive with encryption***
- **z/VSE™ 4.1 support of the TS1120 Tape Drive with encryption* (Not supported at GA date March 16th 2007)**
- **z/VM® V5.3 support, including z/VM guest support of the TS1120 Tape Drive with encryption* (GA June 29th 2007)**
- **Linux on System z source code for FICON and ESCON-connected TS1120 Tape Drives**

* Will require access to an Encryption Key Manager for Java component running on another operating system

All statements regarding IBM's plans, directions, and intent are subject to change or withdrawal without notice. Any reliance on these Statements of General Direction is at the relying party's sole risk and will not create liability or obligation for IBM.

Agenda

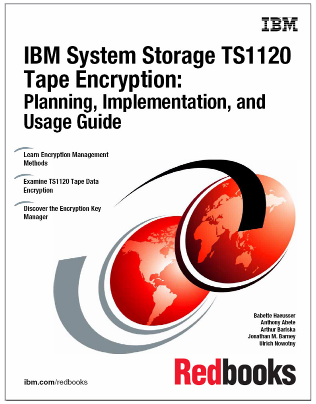
- Topic Overview
- Encryption algorithms
- How does it work with IBM tape?
- How do I trigger IBM tape encryption?
- How do I manage the keys?
- Do I already have it?
- How do I implement it?
- What environments are supported?
- **Where can I go for more information?**

IBM Tape Encryption Documentation

- **Library**
  - 3584 Intro and Planning Guide - GA32-0469
  - 3584 Operator's Guide - GA32-0468
  - EKM Intro, Planning, and Users Guide - GA76-0418
- **System**
  - 3584 Intro and Planning Guide - GA32-0469
  - 3584 Operator's Guide - GA32-0468
  - EKM Intro, Planning, and Users Guide - GA76-0418
  - IBM Tape Device Driver Install and Users Guide - GC35-0154
  - DFSMS Software Support for IBM TotalStorage Enterprise Tape Drive TS1120 (3592) - SC26-7514
- **Application**
  - 3584 Intro and Planning Guide - GA32-0469
  - 3584 Operator's Guide - GA32-0468
  - TSM 5.4 Admin Guide - GC32-0768
    - TSM 5.3.4 Readme interim

Other IBM Resources

- **Java Encryption Key Manager Support Page**
  - http://www-1.ibm.com/support/docview.wss?&uid=ssg1S4000504
- **White Papers**
  - TS1120 Performance with Encryption
  - TS1120 Encrypting Data
  - TS3500 Library Managed Encryption
- **Redbook**
  - IBM System Storage TS1120 Tape Encryption: Planning, Implementation, and Usage Guide (SG24-7320)
- **TSM Encryption Overview Presentation**
  - http://w3-103.ibm.com/software/xl/portal/viewcontent?type=doc&srcID=XW&docID=H800739N06088R56


IBM

IBM System Storage TS1120 Tape Encryption: Planning, Implementation, and Usage Guide

Learn Encryption Management Methods

Examine TS1120 Tape Data Encryption

Discover the Encryption Key Manager

Babette Haeusser
Anthony Abete
Arthur Bariska
Jonathan M. Barney
Ulrich Nowotny

ibm.com/redbooks

Redbooks

Other Resources

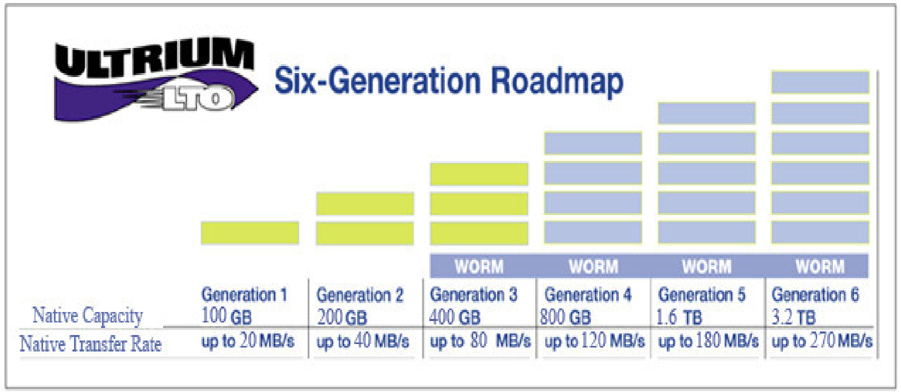
- **Cryptography Decrypted – Mel and Baker, 2001**
- **Privacy Rights Clearinghouse –** www.privacyrights.org
- **Consumer Union -** http://www.consumersunion.org/campaigns/Breach_laws_May05.pdf
- **California Department of Consumer Affairs – "Recommended Practices on Notification of Security Breach Involving Personal Information"** http://www.privacy.ca.gov/recommendations/secbreach.pdf
- **National Institute of Standards and Technology** http://csrc.nist.gov/publications/nistpubs

Agenda

- Topic Overview
- Encryption algorithms
- How does it work with IBM tape?
- How do I trigger IBM tape encryption?
- How do I manage the keys?
- Do I already have it?
- How do I implement it?
- What environments are supported?
- **Where can I go for more information?**
- **Breaking News.....**

IBM Ultrium 4

- **Announce 24th April – GA 27th April 2007**
- **800 GB Native Physical Capacity** (1.6 TB compressed) on LTO Ultrium 4 media
- Up to **120 MB/s** native data transfer rate
- 4Gbps Fibre Channel, Ultra160 LVD SCSI* and/c **New 3Gbps SAS**** attach
- **Encryption capable** for LTO4 SAS and Fibre Channel
- Digital Speed Matching (30, 48, 66, 84 103, 120 MB/s)
- 256 MB Internal Buffer (128 MB for IBM Ultrium 3)
- Several continued features/functions from IBM Ultrium 3
  - WORM technology
  - Dual stage 16-channel head actuator
  - Independent tape loader and threader motors
  - Graceful dynamic braking
  - SARS (Statistical Analysis and Reporting System) and ECC (Error Correction Code)
  - Same 5 ¼" form factor



Six-Generation Roadmap

	Generation 1	Generation 2	Generation 3	Generation 4	Generation 5	Generation 6
			WORM	WORM	WORM	WORM
Native Capacity	100 GB	200 GB	400 GB	800 GB	1.6 TB	3.2 TB
Native Transfer Rate	up to 20 MB/s	up to 40 MB/s	up to 80 MB/s	up to 120 MB/s	up to 180 MB/s	up to 270 MB/s

*Available only for TS2340, TS3100, and TS3200

**Not available with TS1040 (TS3500)

Announcing IBM's LTO Generation 4 Tape Data Encryption Solution - a comprehensive tape security solution

- **New IBM LTO Ultrium Generation 4 Tape Drives with Encryption**
  - Standard capability on all IBM Gen 4 Fibre Channel and SAS drives
  - Integrated into all IBM LTO Automation offerings
- **Enhanced Encryption Key Manager (EKM) component for the Java™ platform**
  - Supports LTO Gen 4 encryption key serving on a wide range of systems including:
  - z/OS, i5/OS, AIX, HP, Sun, Linux and Windows
- **New Tivoli Storage Manager support for LTO Gen 4 encryption**
- **Integration with System z encryption key, security and cryptographic capabilities**
- **New services and consulting for LTO tape data encryption and management**

Encryption Key Manager

The LTO Gen 4 standard differs from the TS1120 implementation of tape drive based encryption

- **Unlike the TS1120 tape drive, the LTO Gen 4 specification does not support encrypted (wrapped) key storage on the LTO cartridge**
  - Key identifier is stored on the cartridges
  - Associated Cartridge Data Keys stored in a Key store
- **LTO Gen 4 supports Application Managed Encryption via SCSI T10 commands**
  - This is the standards-based implementation that will provide for cartridge interchange between drive vendors
  - Requires Application ISVs to enable AME functions
    - TSM available at GA
    - Other ISV's considering
- **LTO Gen 4 does support external key management and out of band key delivery**
  - With appropriate modifications, encryption appliance suppliers or third party software may support LTO Gen 4 encryption
  - IBM's approach is to enhance the EKM to support transparent LTO Gen 4 encryption

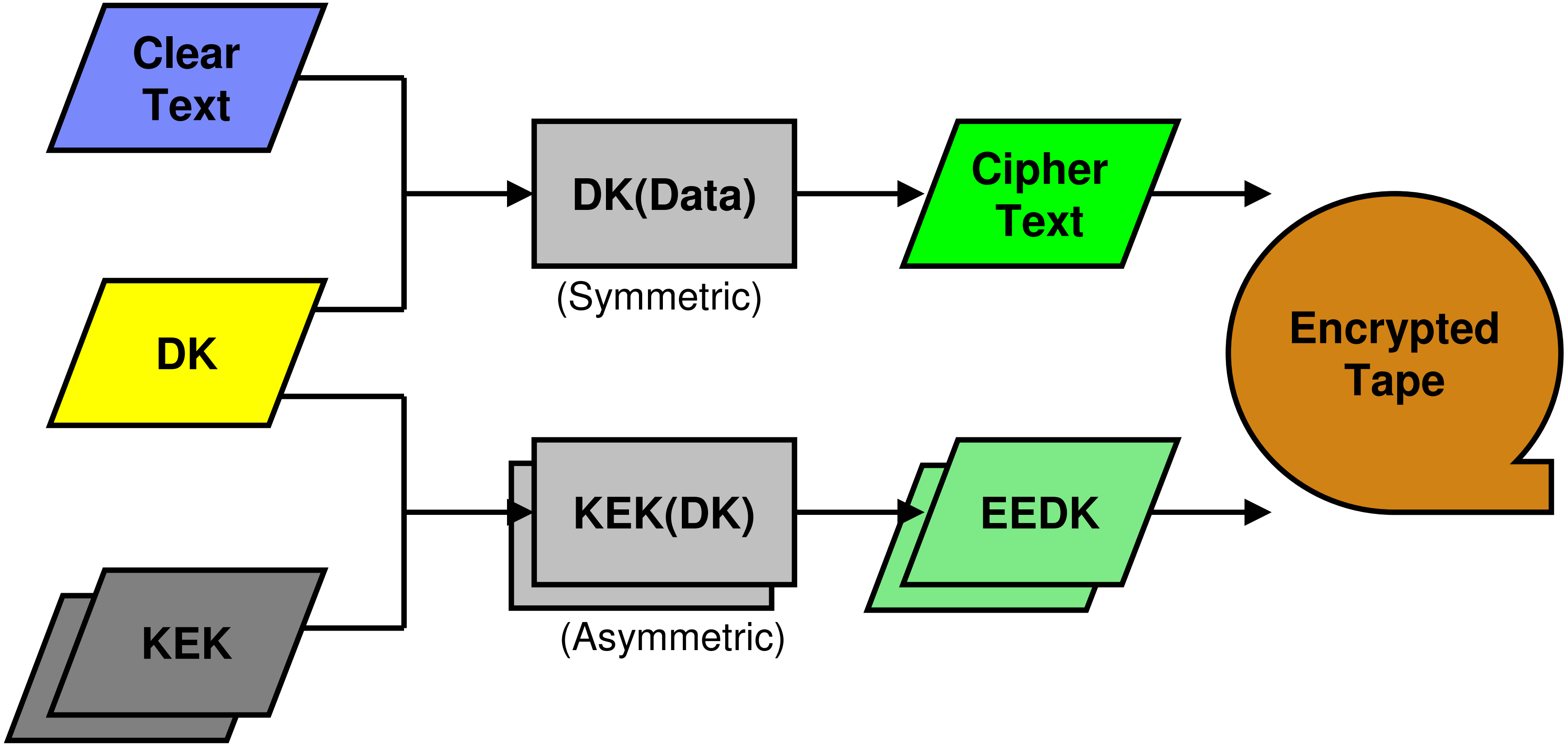
TS3500 Tape Library Announcement Overview

- **IBM Ultrium 4 Tape Drive support**
- **LTO Encryption**
  - Prerequisites for Encryption
- **4 I/O Station D-Frame**
- **Rack mounted TS3000 (TSSC)**
- **Single feed bifurcated AC line cord**
- **Customizable Web Access**

IBM Ultrium 4 Tape Drive Support in TS3500

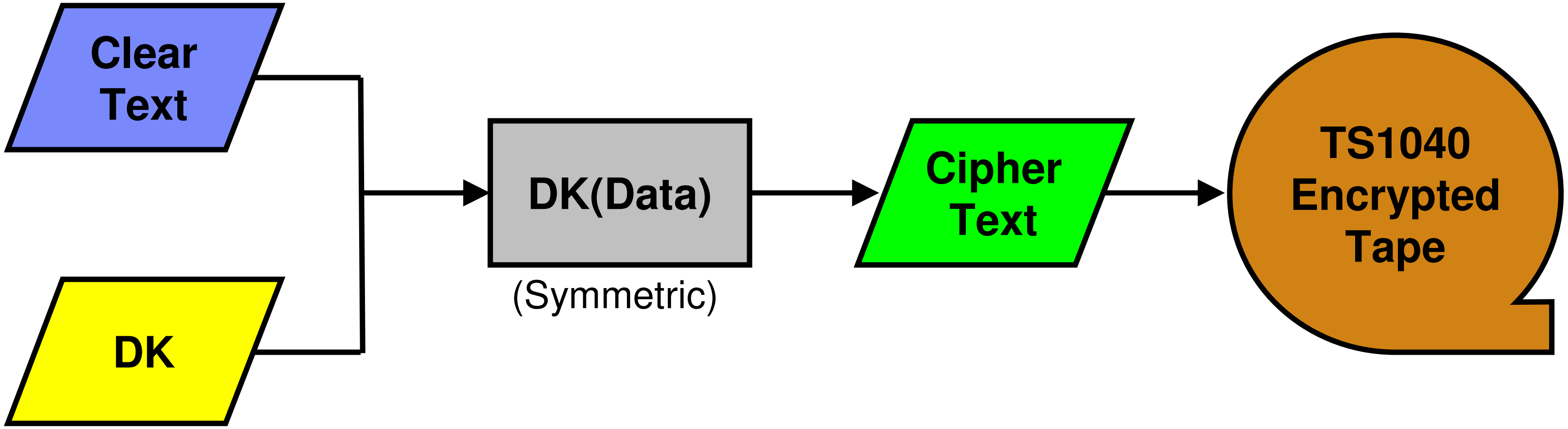
- **New encryption-capable IBM Ultrium 4 tape drive**
  - IBM System Storage TS1040 Tape Drive (3588-F4A)
    - Ordered separately, not a feature of the library
  - 4 Gbps Fibre Channel interface
- **Can be intermixed with existing LTO drives and media in the same frame**
  - Supported frames: L32/D32, L52/D52, L53/D53
- **Media compatibility:**
  - Read/Write Gen 4 or Gen 3 media
  - Read only Gen 2 media
  - Gen 1 media is not supported

TS1120 Encryption Process



DK – Data Key (Symmetric)
KEK – Key Encrypted Key (Asymmetric)
EEDK – Externally Encrypted Data Key

Encryption Process – TS1040



DK – Data Key (Symmetric)

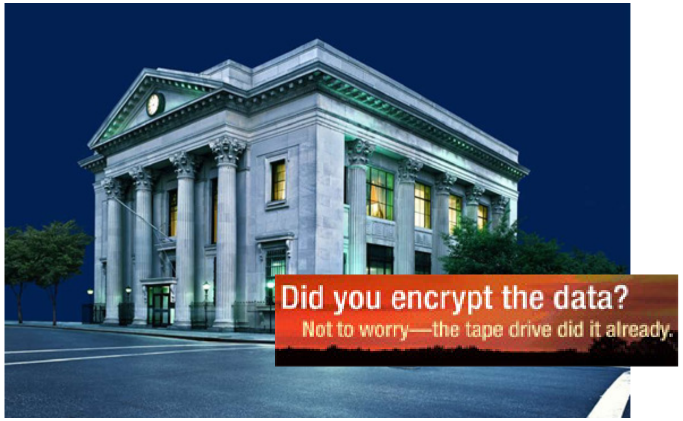
- Encryption Process Defined by T10 Standard

LTO Encryption Support in TS3500 Tape Library

- **Supports Application Managed Encryption**
  - –Tivoli Storage Manager
- **Supports LTO Transparent Encryption**
  - –System Managed and Library Managed Encryption (SME, LME)
  - –Available as a chargeable licensed key feature on the TS3500

TS3500 Prerequisites for LTO Encryption

- **Encryption-capable tape drive**
  - TS1040 / 3588-F4A
    - LTO 4 media
- **TS3500 frames that support TS1040**
  - 3584-L32/D32, 3584-L52/D52, 3584-L53/D53
- **FC1604 - Transparent LTO Encryption**
  - License keys to enable encryption for SME and LME
  - Not required for AME
- **Encryption Key Manager R2**
  - Available as web download
  - Supports both LTO and TS1120 encryption
- **Newest level of library and drive firmware**
- **FC9900 - Encryption Assurance and Readiness**


Did you encrypt the data?
Not to worry—the tape drive did it already.

Encryption Implementation

- **Encryption settings performed via the library web interface**
- **Encryption with ALMS (recommended)**
  - Offers flexibility
    - Encryption can be set per logical library
    - Allows intermix of encrypting and non-encrypting drives in the same logical library
- **Static mode (non-ALMS)**
  - Enforces homogeneity
    - All drives in TS3500 must support encryption
      - Must be LTO 4
      - No intermix
        - *Encryption cannot be enabled on LTO 4 drives added to a library with LTO 1, 2, or 3 drives*
    - All logical libraries must be set to same encryption mode
    - LTO 1, 2 or 3 drives added to a library with encryption enabled cannot be used

Trademarks

NOTES:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

References in this document to IBM products or services do not imply that IBM intends to make them available in every country.

Any proposed use of claims in this presentation outside of the United States must be reviewed by local IBM country counsel prior to such use.

The information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.