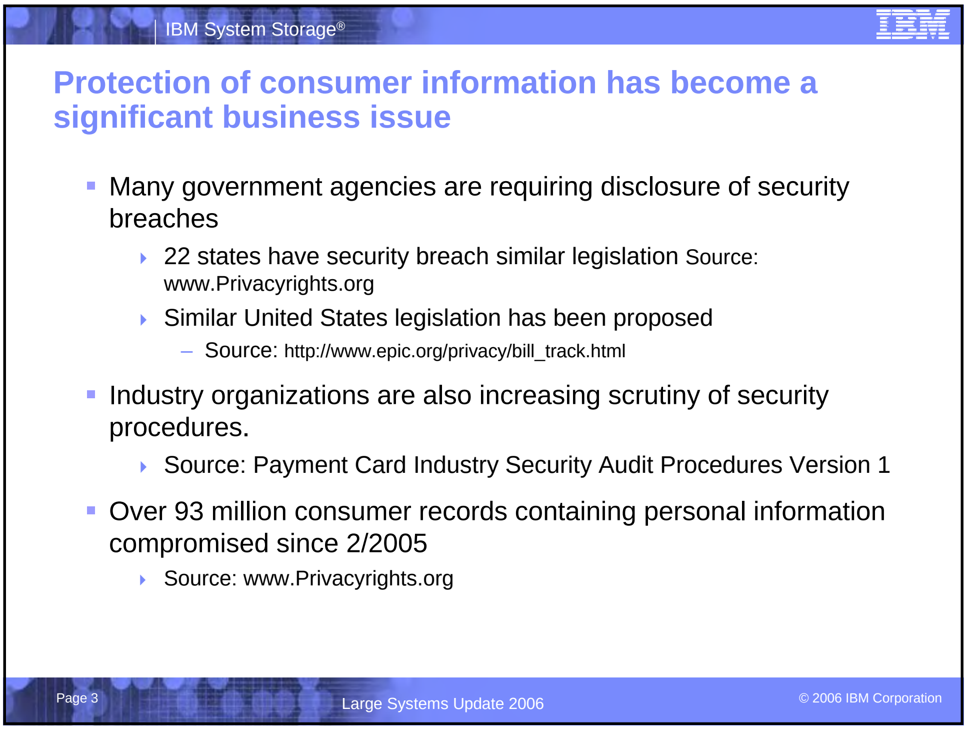
IBM Tape Encryption Overview

Keijo Ekman
Consultant IT Specialist
kekman@fi.ibm.com

Large Systems Update 2006

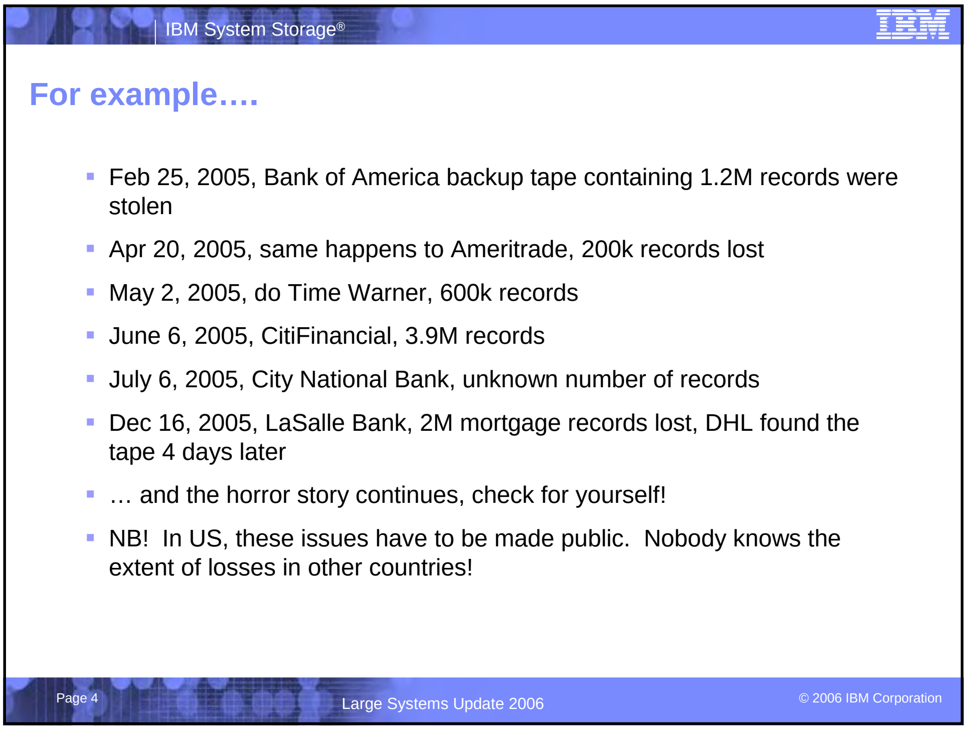
Agenda

- The need for improved data protection
- What is encryption?
- Today’s encryption solutions
- TS1120 Tape Drive encryption overview
- Encryption Key Manager Highlights
- Tape Encryption Solution Alternatives
- Summary



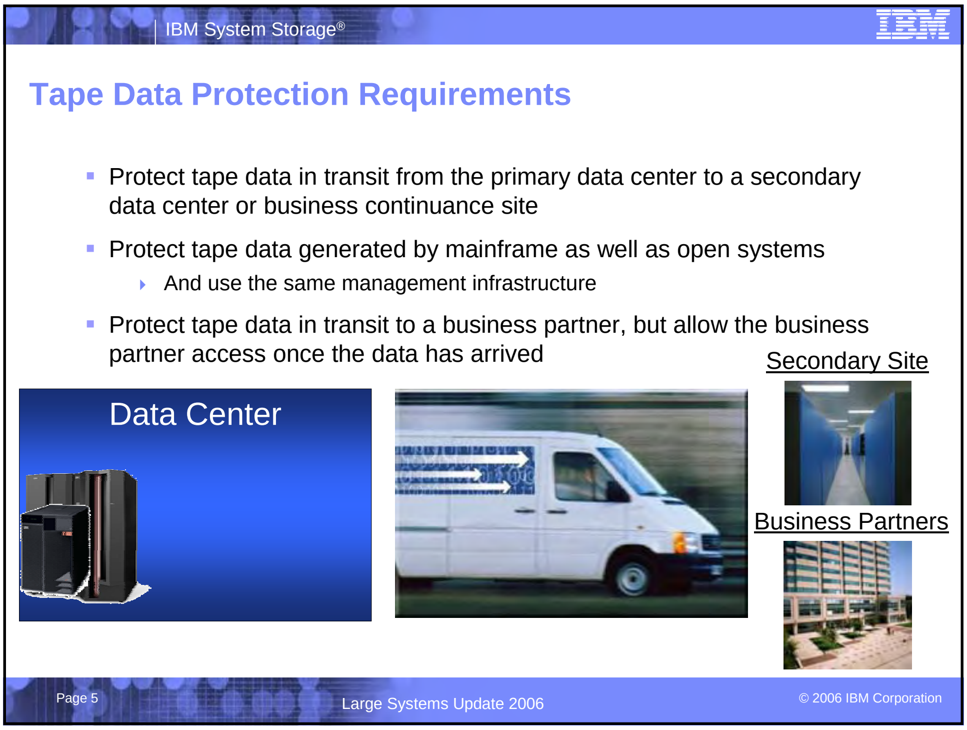
Protection of consumer information has become a significant business issue

- Many government agencies are requiring disclosure of security breaches
  - 22 states have security breach similar legislation Source: www.Privacyrights.org
  - Similar United States legislation has been proposed
    - Source: http://www.epic.org/privacy/bill_track.html
- Industry organizations are also increasing scrutiny of security procedures.
  - Source: Payment Card Industry Security Audit Procedures Version 1
- Over 93 million consumer records containing personal information compromised since 2/2005
  - Source: www.Privacyrights.org



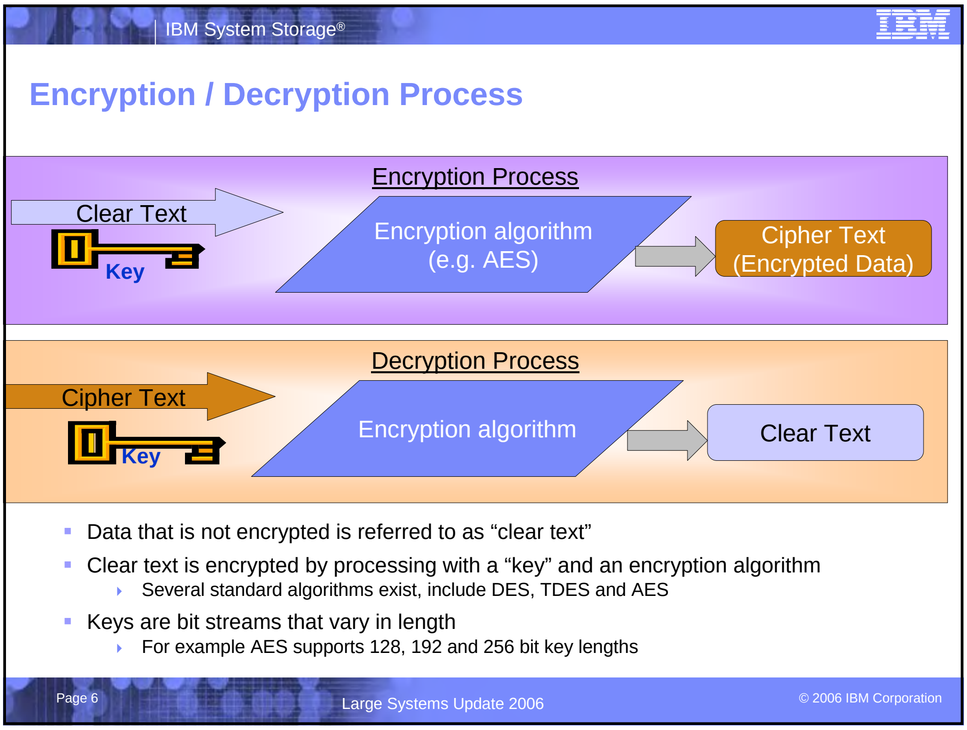
For example….

- Feb 25, 2005, Bank of America backup tape containing 1.2M records were stolen
- Apr 20, 2005, same happens to Ameritrade, 200k records lost
- May 2, 2005, do Time Warner, 600k records
- June 6, 2005, CitiFinancial, 3.9M records
- July 6, 2005, City National Bank, unknown number of records
- Dec 16, 2005, LaSalle Bank, 2M mortgage records lost, DHL found the tape 4 days later
- … and the horror story continues, check for yourself!
- NB! In US, these issues have to be made public. Nobody knows the extent of losses in other countries!



Tape Data Protection Requirements

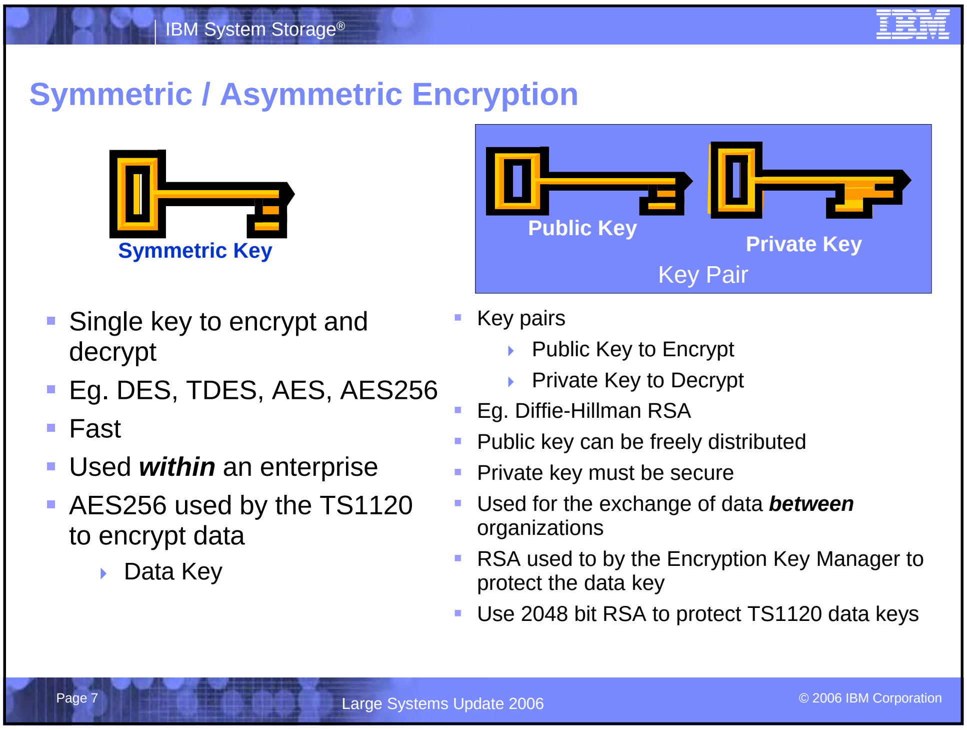
- Protect tape data in transit from the primary data center to a secondary data center or business continuance site
- Protect tape data generated by mainframe as well as open systems
  - And use the same management infrastructure
- Protect tape data in transit to a business partner, but allow the business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



Encryption / Decryption Process

Encryption Process
Clear Text
Key
Encryption algorithm
(e.g. AES)
Cipher Text
(Encrypted Data)
Decryption Process
Cipher Text
Key
Encryption algorithm
Clear Text

- 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

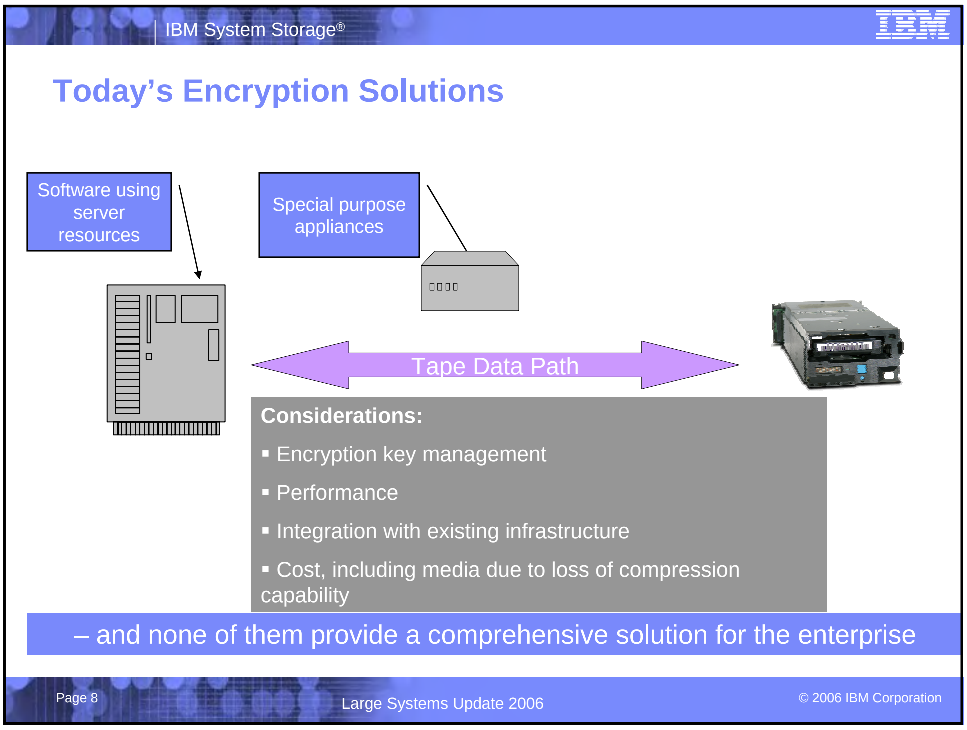


Symmetric / Asymmetric Encryption

Symmetric Key
Public Key
Private Key
Key Pair

- Single key to encrypt and decrypt
- Eg. DES, TDES, AES, AES256
- Fast
- Used ***within*** an enterprise
- AES256 used by the TS1120 to encrypt data
  - Data Key

- Key pairs
  - Public Key to Encrypt
  - Private Key to Decrypt
- Eg. Diffie-Hillman RSA
- Public key can be freely distributed
- Private key must be secure
- Used for the exchange of data ***between*** organizations
- RSA used to by the Encryption Key Manager to protect the data key
- Use 2048 bit RSA to protect TS1120 data keys



Today’s Encryption Solutions

Considerations:

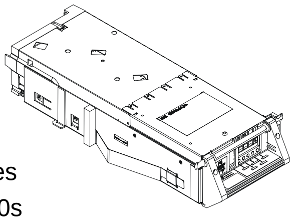
- Encryption key management
- Performance
- Integration with existing infrastructure
- Cost, including media due to loss of compression capability

– and none of them provide a comprehensive solution for the enterprise

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
  - 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 auditability

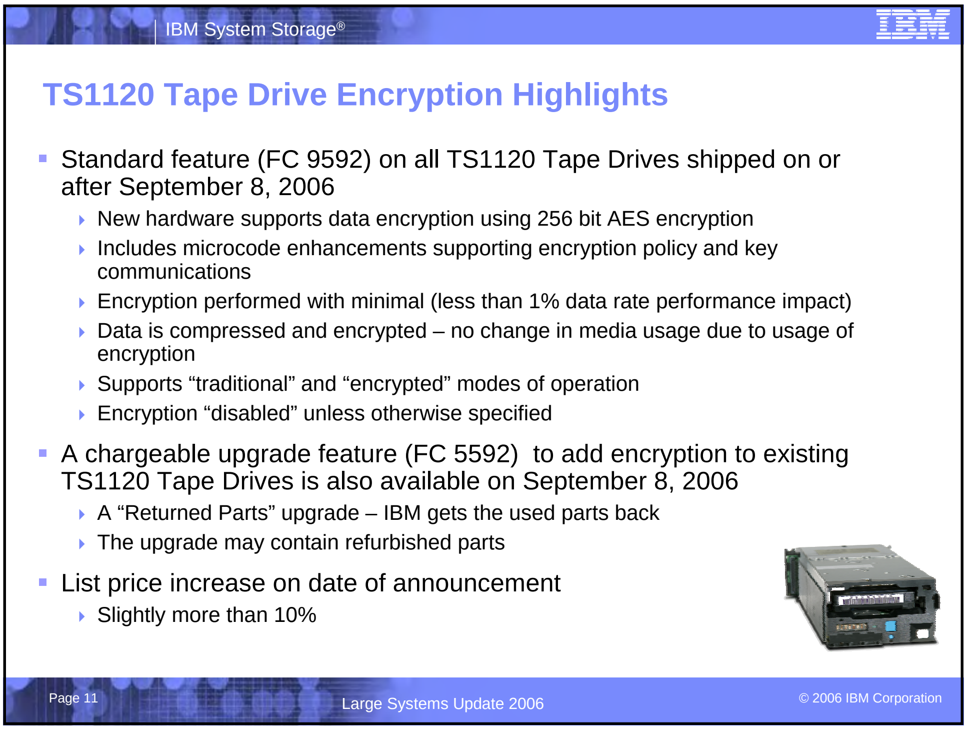
IBM Tape Data Encryption



- TS1120 Tape Drive
  - Addresses tape data security concerns
  - Standard feature on all new TS1120 Tape Drives
  - Chargeable upgrade feature for existing TS1120s

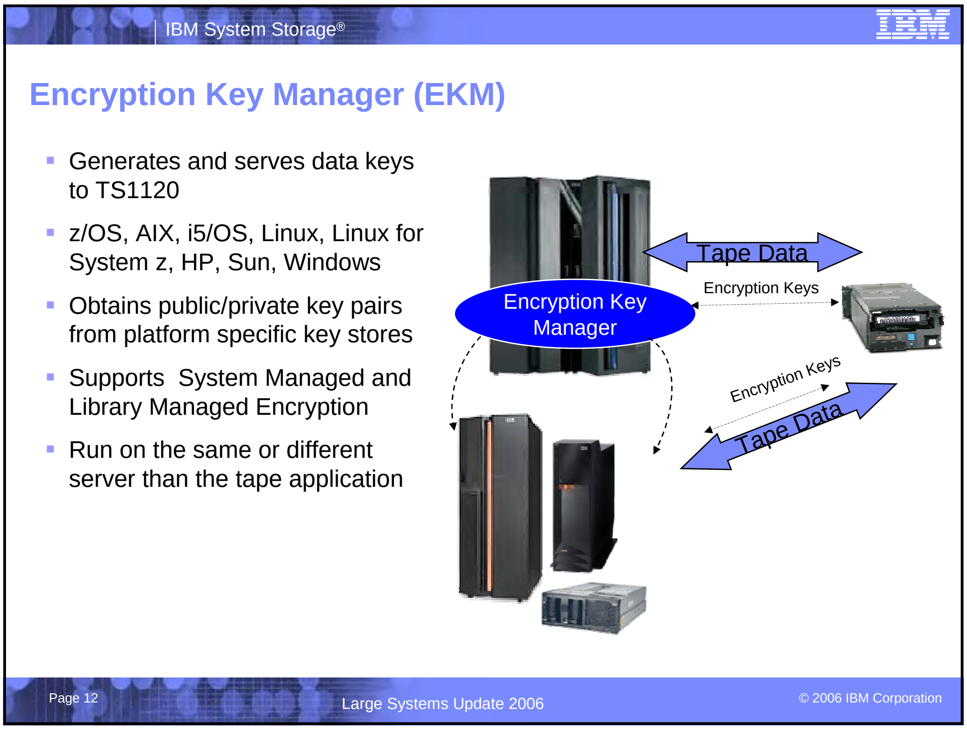
- IBM Encryption Key Manager (EKM)
  - IBM Java component
  - z/OS, i5/OS, AIX, HP, Sun, Linux and Windows
  - Generates and serves keys to TS1120 tape drive
  - Stores encryption keys in keystore

Encryption Key Manager



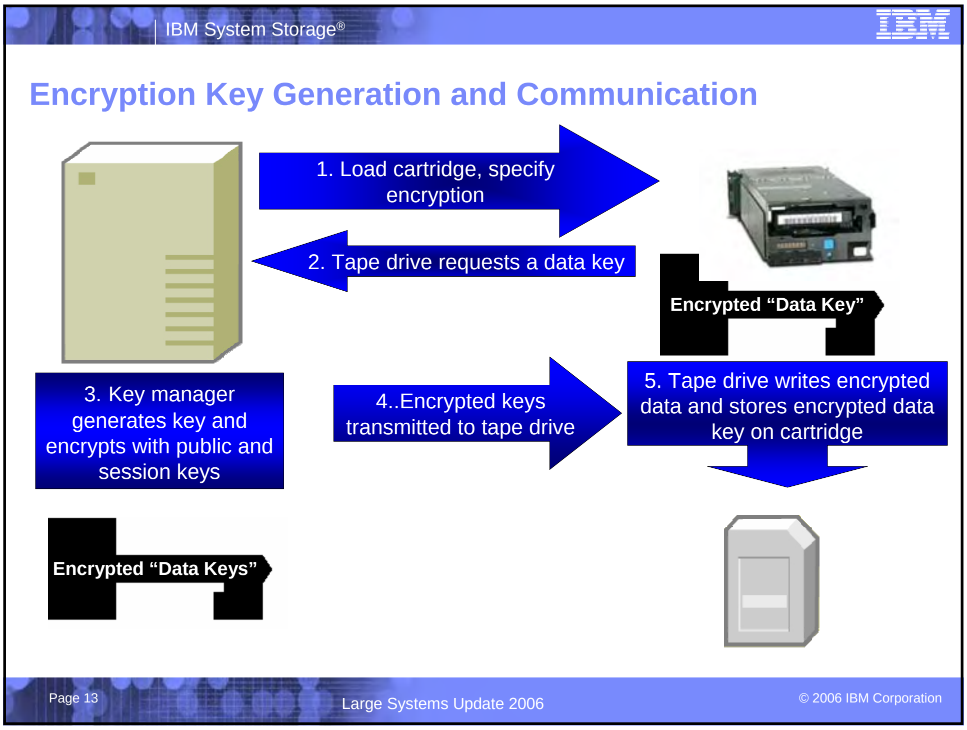
TS1120 Tape Drive Encryption Highlights

- Standard feature (FC 9592) on all TS1120 Tape Drives shipped on or after September 8, 2006
  - New hardware supports data encryption using 256 bit AES encryption
  - Includes microcode enhancements supporting encryption policy and key communications
  - Encryption performed with minimal (less than 1% data rate performance impact)
  - Data is compressed and encrypted – no change in media usage due to usage of encryption
  - Supports “traditional” and “encrypted” modes of operation
  - Encryption “disabled” unless otherwise specified
- A chargeable upgrade feature (FC 5592) to add encryption to existing TS1120 Tape Drives is also available on September 8, 2006
  - A “Returned Parts” upgrade – IBM gets the used parts back
  - The upgrade may contain refurbished parts
- List price increase on date of announcement
  - Slightly more than 10%



Encryption Key Manager (EKM)

- Generates and serves data keys to TS1120
- z/OS, AIX, i5/OS, Linux, Linux for System z, HP, Sun, Windows
- Obtains public/private key pairs from platform specific key stores
- Supports System Managed and Library Managed Encryption
- Run on the same or different server than the tape application



Encryption Key Generation and Communication

1. Load cartridge, specify encryption

2. Tape drive requests a data key

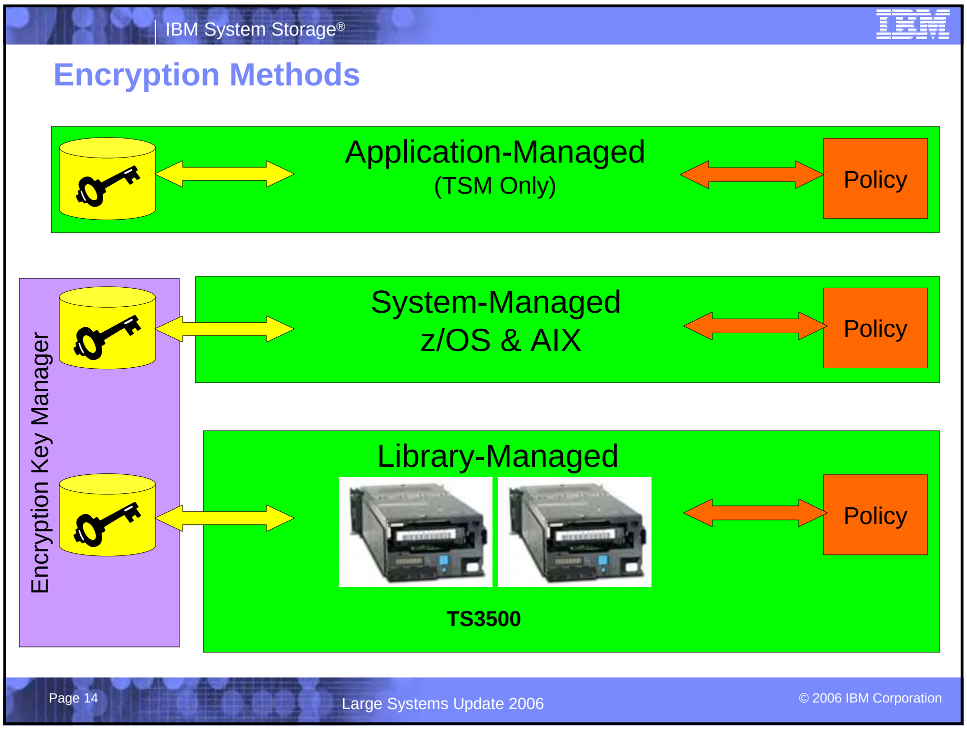
Encrypted “Data Key”

3. Key manager generates key and encrypts with public and session keys

4..Encrypted keys transmitted to tape drive

5. Tape drive writes encrypted data and stores encrypted data key on cartridge

Encrypted “Data Keys”



Encryption Methods

Application-Managed
(TSM Only)

Policy

System-Managed
z/OS & AIX

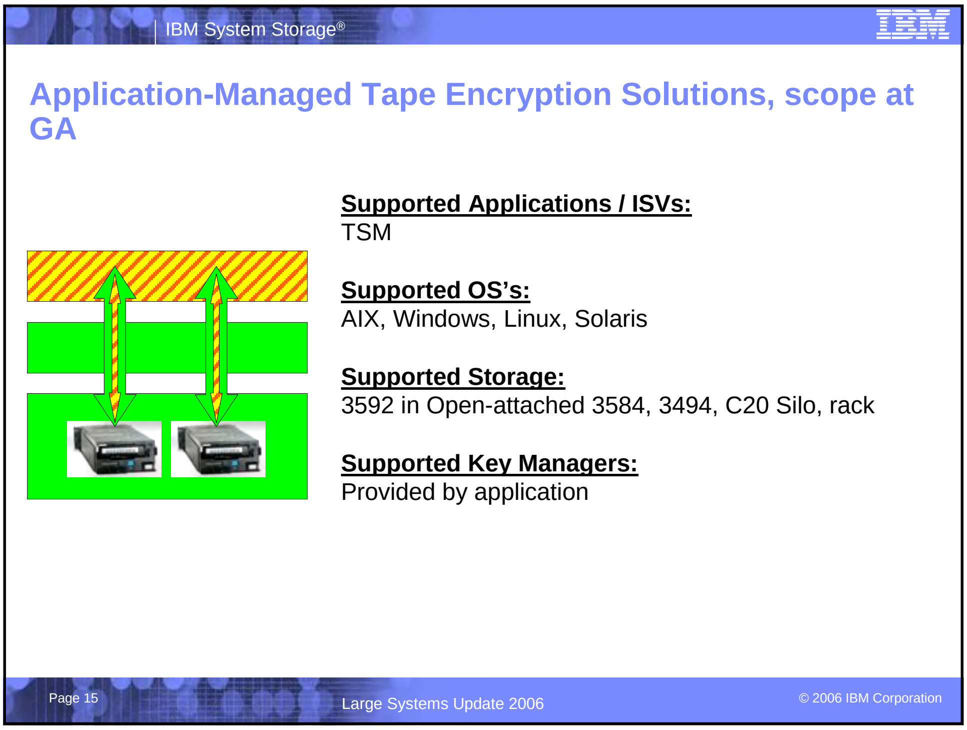
Policy

Library-Managed

TS3500

Policy

Encryption Key Manager



IBM System Storage®

Application-Managed Tape Encryption Solutions, scope at GA

Supported Applications / ISVs:
TSM

Supported OS's:
AIX, Windows, Linux, Solaris

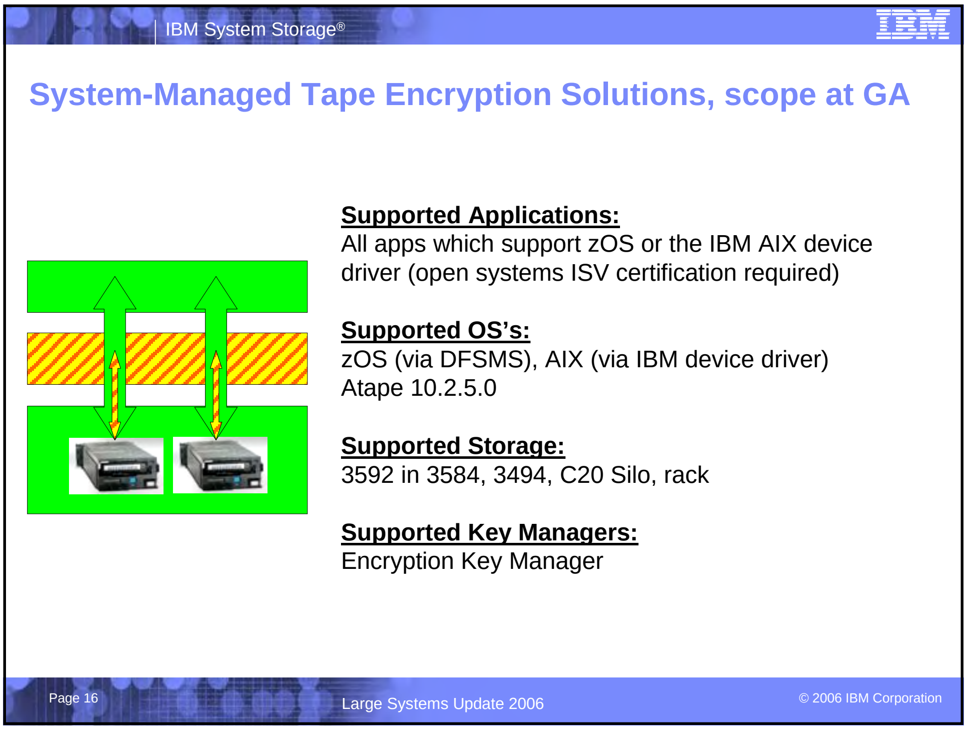
Supported Storage:
3592 in Open-attached 3584, 3494, C20 Silo, rack

Supported Key Managers:
Provided by application

Page 15

Large Systems Update 2006

© 2006 IBM Corporation



IBM System Storage®

System-Managed Tape Encryption Solutions, scope at GA

Supported Applications:
All apps which support zOS or the IBM AIX device driver (open systems ISV certification required)

Supported OS's:
zOS (via DFSMS), AIX (via IBM device driver)
Atape 10.2.5.0

Supported Storage:
3592 in 3584, 3494, C20 Silo, rack

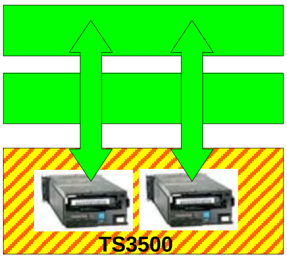
Supported Key Managers:
Encryption Key Manager

Page 16

Large Systems Update 2006

© 2006 IBM Corporation

Library-Managed Tape Encryption Solutions, scope at GA



Supported Applications:
All applications which support IBM storage listed below (open systems ISV certification required)

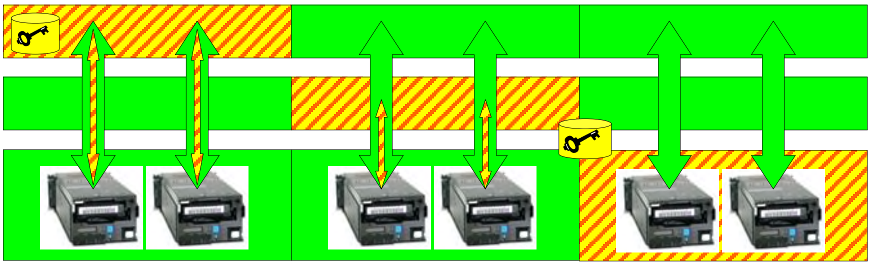
Supported OS's:
All open OS's supported by the apps above

Supported Storage:
3592 in open-attached TS3500 (3584)

Supported Key Managers:
Encryption Key Manager

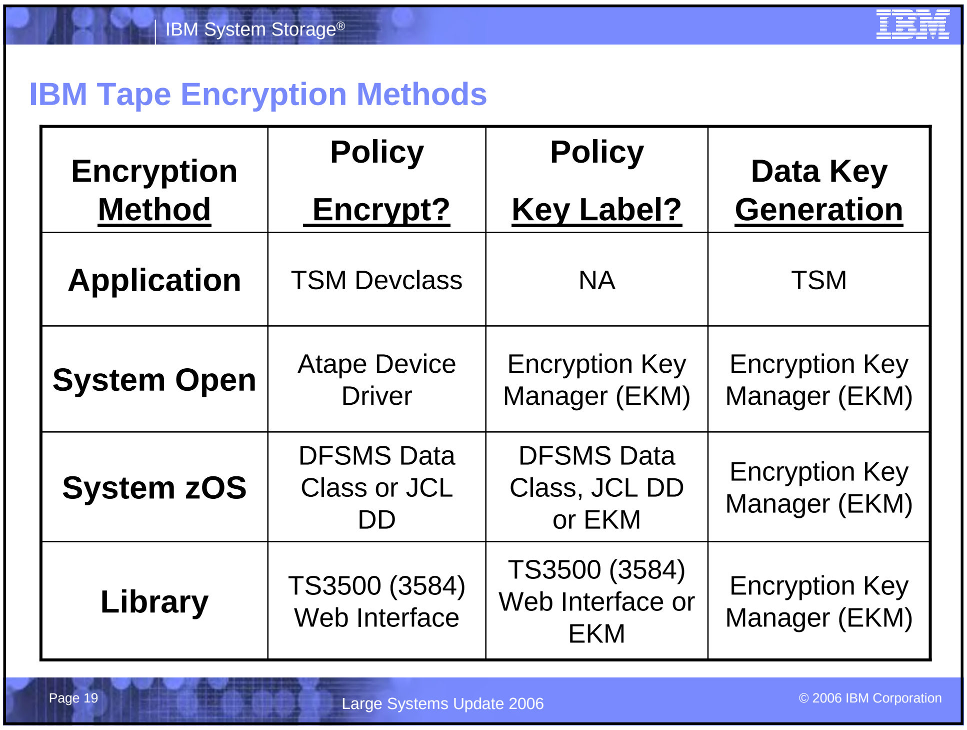
Support for Different Encryption Methods

Different methods can be used on separate servers, LPARs on a single server, or blades in the same BladeCenter.



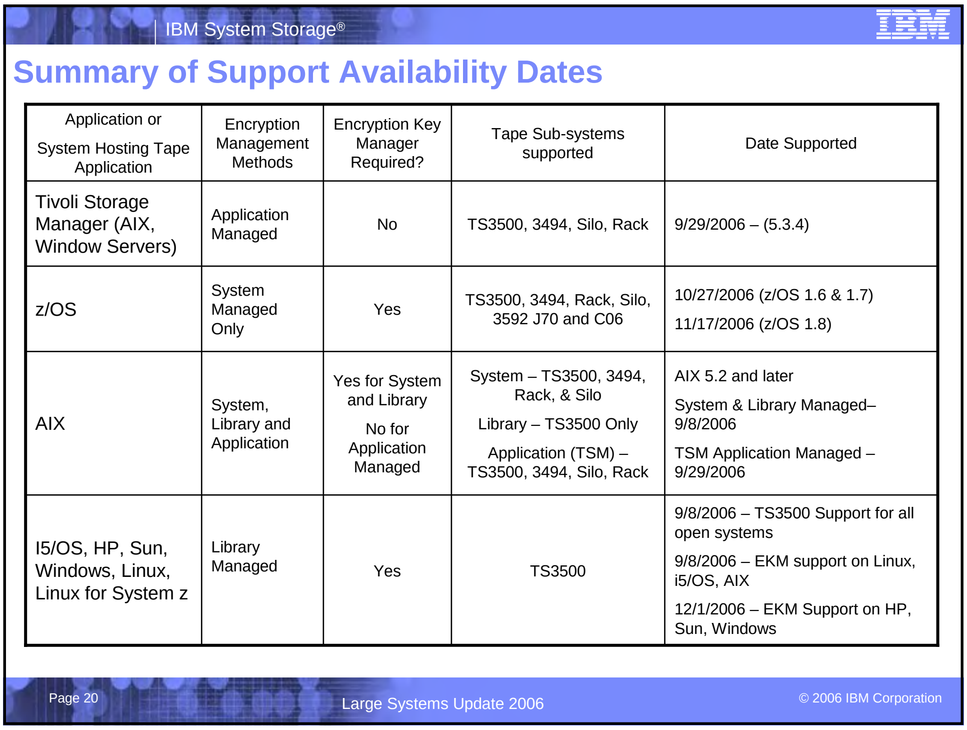
Different methods can be used on separate libraries or library partitions.

Key managers can be shared by any or all System-Managed and Library-Managed solutions



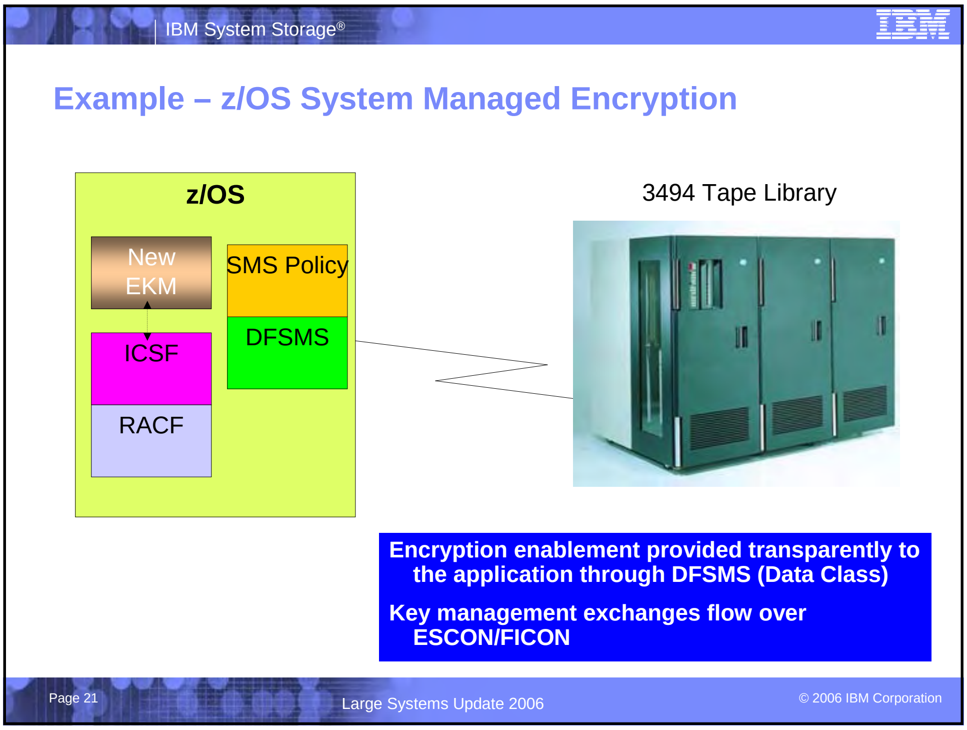
IBM Tape Encryption Methods

Encryption Method	Policy Encrypt?	Policy Key Label?	Data Key Generation
Application	TSM Devclass	NA	TSM
System Open	Atape Device Driver	Encryption Key Manager (EKM)	Encryption Key Manager (EKM)
System zOS	DFSMS Data Class or JCL DD	DFSMS Data Class, JCL DD or EKM	Encryption Key Manager (EKM)
Library	TS3500 (3584) Web Interface	TS3500 (3584) Web Interface or EKM	Encryption Key Manager (EKM)



Summary of Support Availability Dates

Application or System Hosting Tape Application	Encryption Management Methods	Encryption Key Manager Required?	Tape Sub-systems supported	Date Supported
Tivoli Storage Manager (AIX, Window Servers)	Application Managed	No	TS3500, 3494, Silo, Rack	9/29/2006 – (5.3.4)
z/OS	System Managed Only	Yes	TS3500, 3494, Rack, Silo, 3592 J70 and C06	10/27/2006 (z/OS 1.6 & 1.7) 11/17/2006 (z/OS 1.8)
AIX	System, Library and Application	Yes for System and Library No for Application Managed	System – TS3500, 3494, Rack, & Silo Library – TS3500 Only Application (TSM) – TS3500, 3494, Silo, Rack	AIX 5.2 and later System & Library Managed– 9/8/2006 TSM Application Managed – 9/29/2006
I5/OS, HP, Sun, Windows, Linux, Linux for System z	Library Managed	Yes	TS3500	9/8/2006 – TS3500 Support for all open systems 9/8/2006 – EKM support on Linux, i5/OS, AIX 12/1/2006 – EKM Support on HP, Sun, Windows



Example – z/OS System Managed Encryption

z/OS

New EKM

SMS Policy

ICSF

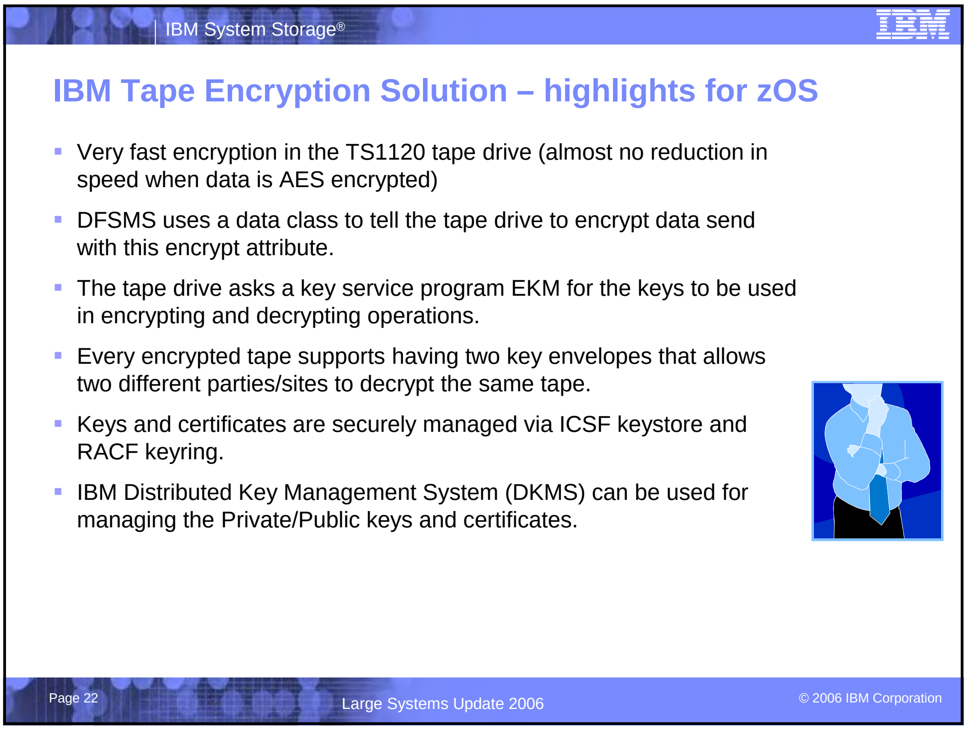
DFSMS

RACF

3494 Tape Library

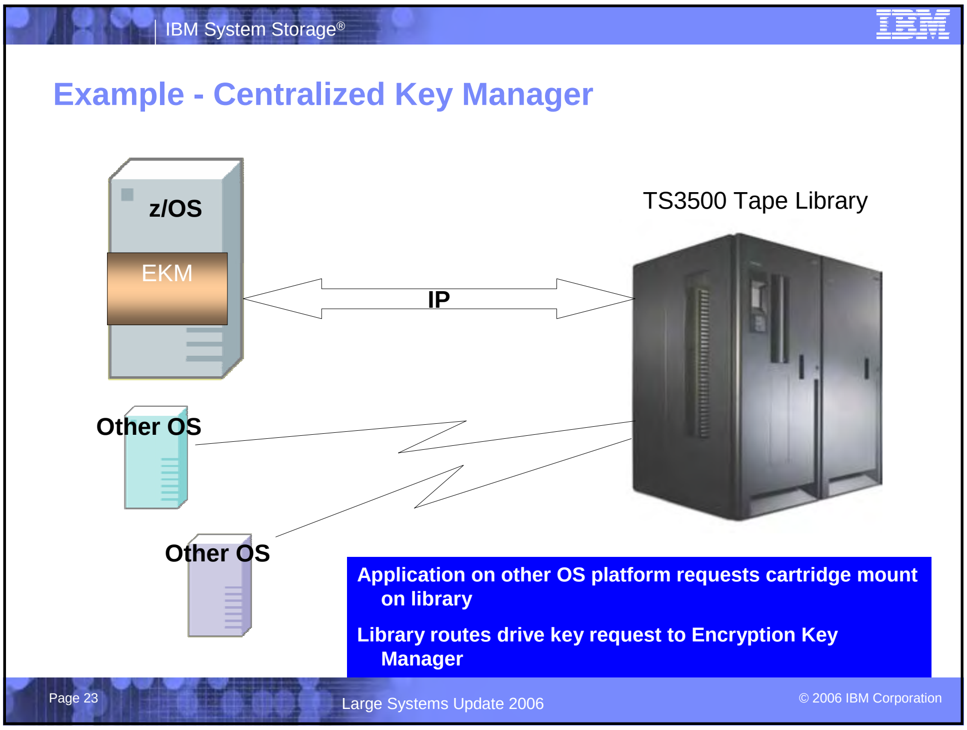
Encryption enablement provided transparently to the application through DFSMS (Data Class)

Key management exchanges flow over ESCON/FICON



IBM Tape Encryption Solution – highlights for zOS

- Very fast encryption in the TS1120 tape drive (almost no reduction in speed when data is AES encrypted)
- DFSMS uses a data class to tell the tape drive to encrypt data send with this encrypt attribute.
- The tape drive asks a key service program EKM for the keys to be used in encrypting and decrypting operations.
- Every encrypted tape supports having two key envelopes that allows two different parties/sites to decrypt the same tape.
- Keys and certificates are securely managed via ICSF keystore and RACF keyring.
- IBM Distributed Key Management System (DKMS) can be used for managing the Private/Public keys and certificates.



Example - Centralized Key Manager

z/OS

EKM

IP

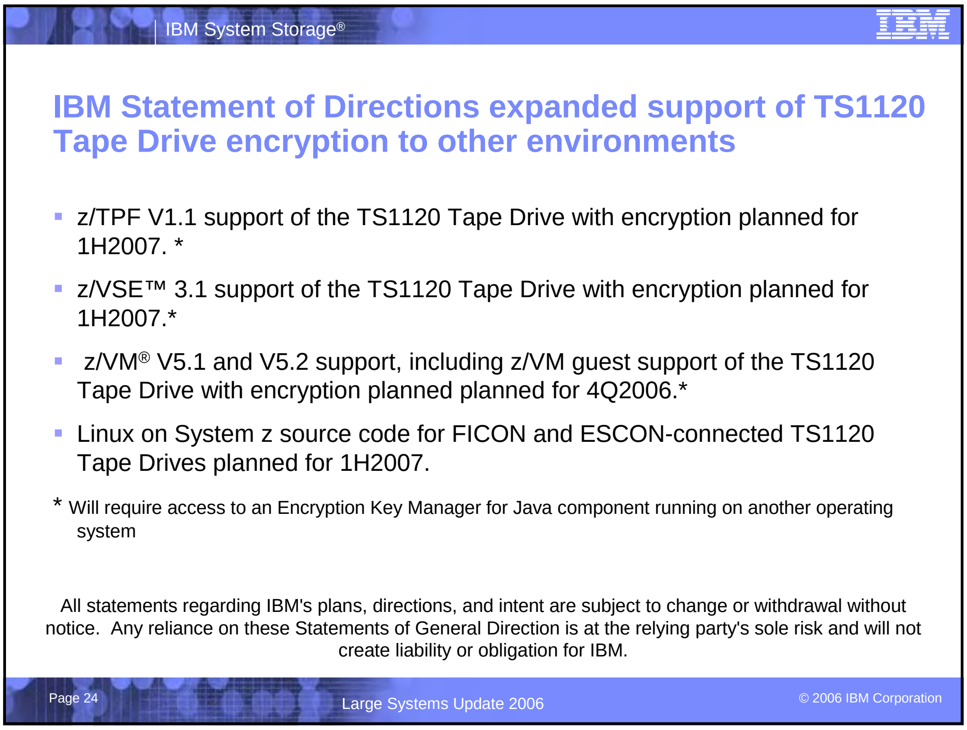
TS3500 Tape Library

Other OS

Other OS

Application on other OS platform requests cartridge mount on library

Library routes drive key request to Encryption Key Manager



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

- z/TPF V1.1 support of the TS1120 Tape Drive with encryption planned for 1H2007. *
- z/VSE™ 3.1 support of the TS1120 Tape Drive with encryption planned for 1H2007.*
- z/VM® V5.1 and V5.2 support, including z/VM guest support of the TS1120 Tape Drive with encryption planned planned for 4Q2006.*
- Linux on System z source code for FICON and ESCON-connected TS1120 Tape Drives planned for 1H2007.

* 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.