IBM System Storage™ TS1120 Tape Drive & Tape Data Encryption Overview

Helping customers protect vital information &

Supporting Business Continuity and Information Lifecycle Management

50 YEARS OF TAPE INNOVATION

Agenda

- Introduction
- IBM TS1120 Tape Drive Overview
- IBM TS1120 Tape Controller Overview
- IBM Tape Data Encryption Overview

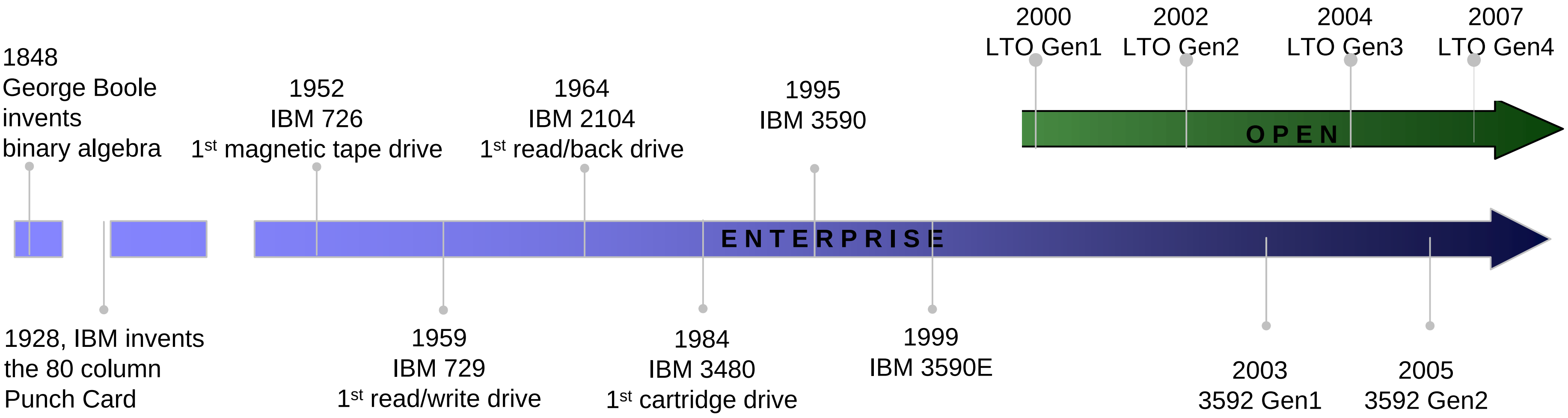
IBM System Storage

Introduction

50 YEARS OF TAPE INNOVATION

Over 50 Years of Tape Innovation

- Starting in 1952
  - IBM 726 Tape Unit
    - 7,500 characters per second
    - 100 bits per inch
- and continuing in 2007
  - IBM TS1040 Tape Drive
    - up to 120 MB/sec[1]
    - up to 800 GB[1]



1848
George Boole
invents
binary algebra

1928, IBM invents
the 80 column
Punch Card

1952
IBM 726
1st magnetic tape drive

1959
IBM 729
1st read/write drive

1964
IBM 2104
1st read/back drive

1984
IBM 3480
1st cartridge drive

1995
IBM 3590

1999
IBM 3590E

ENTERPRISE

2000
LTO Gen1

2002
LTO Gen2

2003
3592 Gen1

2004
LTO Gen3

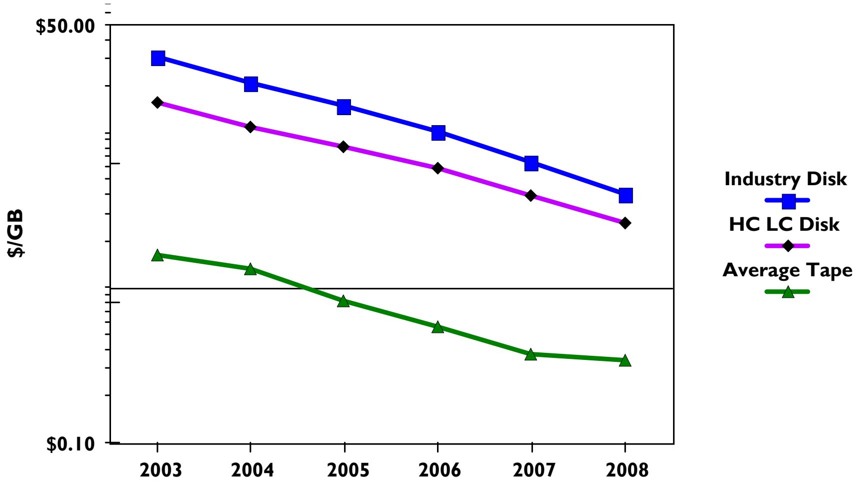
2005
3592 Gen2

2007
LTO Gen4

OPEN

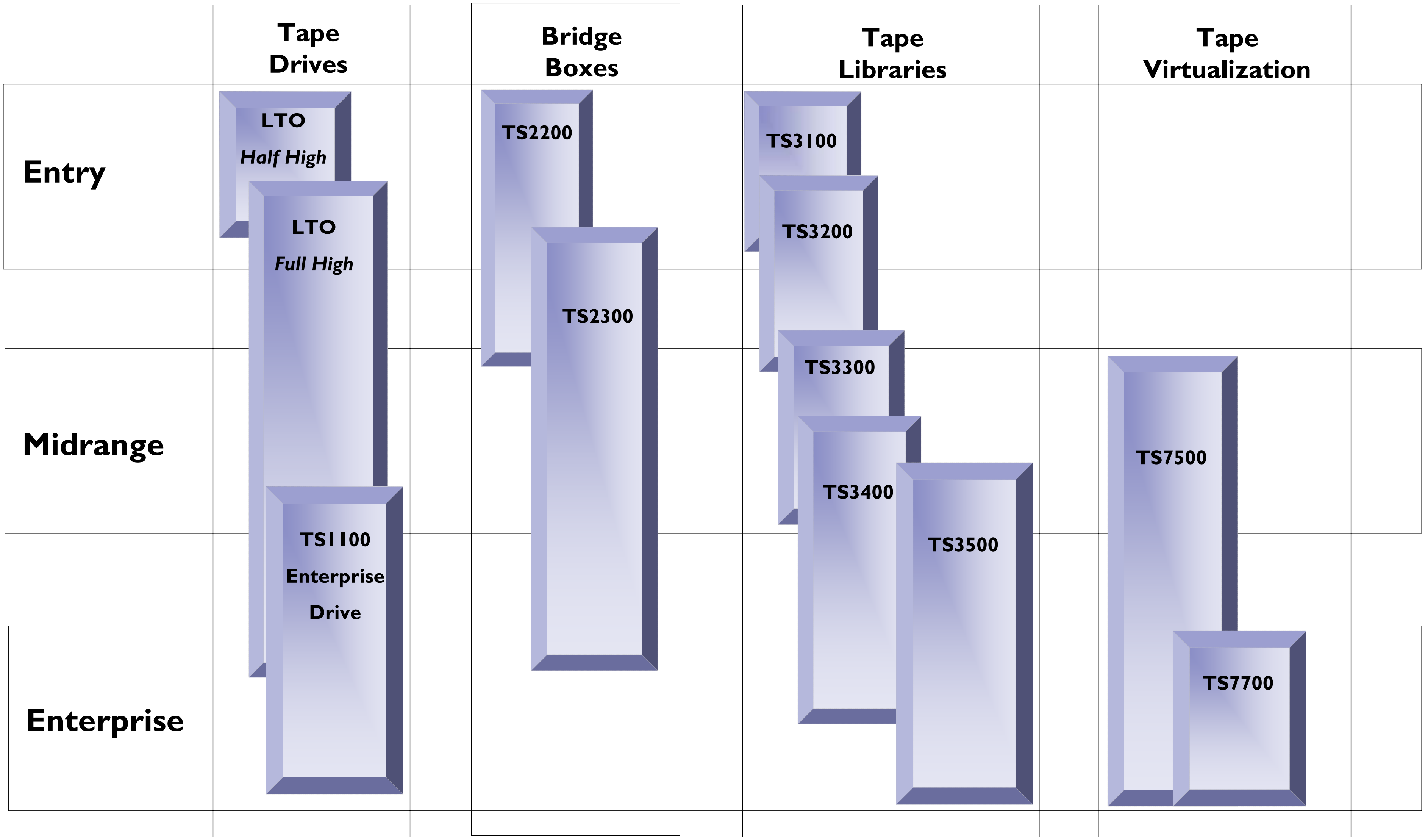
Tape's Continuing Role

- Tape is an integral part of the storage hierarchy
  - Customers store 4-15X more data on tape than disk
- Tape is low cost
- Tape is intrinsically "On-Demand"
- Tape is removable and portable
- Tape provides high volumetric efficiency
- Tape media has a long life
- Tape is ideally suited for:
  - Information Lifecycle Management
  - Business Continuance



Source: Disk - Industry Analysts, Tape - IBM

IBM System Storage Tape Portfolio



Tape Drives

Bridge Boxes

Tape Libraries

Tape Virtualization

Entry

Midrange

Enterprise

LTO *Half High*

LTO *Full High*

TS1100 Enterprise Drive

TS2200

TS2300

TS3100

TS3200

TS3300

TS3400

TS3500

TS7500

TS7700

IBM

IBM System Storage

TS1120 Tape Drive Overview

50 YEARS OF TAPE INNOVATION

TS1120 Tape Drive Overview

- 2nd Generation of 3592 enterprise tape drive roadmap
  - 100 MB/sec performance (up to 260 MB/s at 3:1 compression)
  - 100 / 500 / 700 GB native capacity (up to 300 GB / 1.5 TB / 2.1 TB at 3:1 compression)
    - Re-Writable and Write Once Read Many (WORM) cartridges
  - Dual 4Gb fiber interface
  - Supports data encryption and key management
- Supported in
  - IBM 3494 and TS3500 tape libraries
  - IBM 3592 C20 silo compatible frame
  - IBM 7014 Rack

Includes Advanced IBM Tape Technology

- Includes common* IBM tape drive technology
  - Flat Lapped Heads are designed to lower friction to improve head and tape cartridge longevity by enables low wrap
  - Surface Control Guiding is designed to prevent edge damage and debris accumulation by eliminating edge guiding
  - Dual Stage Actuators are designed to support higher capacities by reducing vibration and enabling precise 'head-to-track' alignment
  - Improved SARS interface supports predictive drive and cartridge maintenance and supports customer access to performance and reliability metrics
  - Speed Matching reduces the speed of the drive to better match the attached servers ability to stream data
  - 'Read after Write' verification is performed during write operations to help guard against any non-reversible data compression failure

* shared with IBM LTO tape drives

Includes Advanced IBM Tape Technology (continued)

- Includes unique* IBM enterprise tape drive technology
  - A High Resolution Directory that indexes all host records and file mark positions supports fast, consistent locate times
  - A large data buffer (512 MB) and enhanced read-ahead buffer management that reduces random and skip forward sequential (short hop) locate times
  - Capacity Scaling supports of 3592 JA cartridge to be formatted to a short length to support fast access to data
  - Non volatile caching that reduces the impact of back-hitching caused by checkpoint and small block transfers
- Includes new IBM enterprise tape drive technology
  - A new String Search function allows a host application to offload search arguments to the TS1120 tape drive

* Unique to IBM TS1120 and 3592 J1A tape drives

Second Generation Technology Enhancements

- Larger Data Buffer
  - Increased from 128 MB to 512 MB and improved read-ahead algorithm
  - Improves random and 'skip-search' operations
- Faster high speed space/locate
  - Increased from 8 meters/sec to 10 meters/sec
  - Improves time-to-data and rewind operations
- Faster load to ready time
  - Load to ready time reduced by up to 33%
  - Improves time-to-data by up to five seconds
- Enhanced Virtual Backhitch
  - Up to 100% improvement in Virtual Backhitch Performance
  - Improves performance of small block and slow host data transfers

Supports Lightning Fast Performance

- Includes two 4 Gbit FC / FC-AL interfaces
- Uses existing 3592 cartridge media
  - JJ/JR cartridge media supports fast access
  - JA/JW cartridge media supports high capacity
  - JB/JX extended capacity cartridge media
  - Capacity scaling function can also be used to support fast access on JA and JB media

Average Tape Drive Performance Metrics

	Machine Model	TS1120			3592 J1A		3590 H1A	LTO Gen 3
	Cartridge Type	**JB**	**JJ**	**JA**	**JJ**	**JA**	**K**	**Gen3**
A	**Load**	13	13	13	19	19	42	12
B	**Initial Search**	45	11	33	12	40	62	47
C	**Average Access (A+B)**	58	24	46	31	59	104	59
D	**Rewind**	47	11	35	12	40	56	45
E	**Unload**	23	23	23	20	20	18	15
F	**Mount/Demount (A+B+C+D)**	128	58	104	63	119	178	119

3592 Cartridge Media

- Cartridges are in rewritable and WORM
- Cartridges are available in three lengths
  - JJ and JR cartridges provide rapid access to data
  - JA and JW cartridges provide fast access to data or high capacity
  - JB and JX extended data cartridges provide higher capacity
- Cartridges can be formatted to either Gen 1 or Gen 2 formats[1]
  - TS1120 tape drives can read or write Gen 1 or Gen 2 formats
  - 3592 J1A tape drives can read or write the Gen 1 format

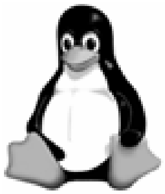
3592 Cartridge Media		TS1120 Tape Drive		3592 J1A Tape Drive	
Type	**Format**	**Capacity**	**Performance**	**Capacity**	**Performance**
JJ / JR	Gen 1	60 GB	50 MB/sec	60	40 MB/sec
	Gen 2	100 GB	100 MB/sec		
JA / JW	Gen 1	300 GB	50 MB/sec	300	40 MB/sec
	Gen 2	500 GB	100 MB/sec		
JB / JX	Gen 2	700 GB	100 MB/sec		

[1] iSeries only supports writing cartridges native 3592 Gen 2 format

Platform Support

- eServer Platforms
  - System z™
    - zOS™ / OS/390®
    - zVM™
    - VSE / VSE/ESA with VGS
    - SuSE Linux Enterprise Server
  - System p™
    - AIX®
    - SuSE Enterprise Server
  - System i™
    - OS/400®
    - i5
  - System x™
    - Supported Microsoft and Linux platforms

- Other Vendor Platforms
  - Sun Microsystems
    - Selected SUN Servers/ FC HBAs
    - Solaris 7, Solaris 8, Solaris 9
  - Hewlett Packard
    - Selected HP Servers/ FC HBAs
    - HP-UX 11.0, HP-UX 11.i
  - Microsoft Corporation
    - Windows NT™ Server Version 4
    - Windows 2000™ /
    - Windows Server™ 2003
  - Linux
    - RedHat Enterprise Linux
    - SuSE Linux Enterprise Server 8
    - Turbolinux Enterprise Server 8
    - Conectiva Linux Enterprise Edition



* See http://www-03.ibm.com/servers/storage/tape/resource-library.html#interoperability for current platform support

Enterprise Tape Drive Roadmap

	3590 Tape Drive Generations			TS1100 Tape Drive Generations		
	Model B	**Model E**	**Model H**	**Gen 1**	**Gen 2**	**Gen 3**
Servo Bands				5	5	TBD
Servo Type	Analogue			Digital		
Tracks	128	256	384	512	896	TBD
Upgrade available	y					
Read Previous Generations		y	y		y	y*
Write Previous Generation		n	n		Gen 1	Gen 2[1]
Write Once Read Many	n			y		
Virtual Backhitch	n			y		
	J Cartridge			JA / JW Cartridge		
Native Capacity (GB)	10	20	30	60	100	TBD[1]
	K Cartridge			JJ / JW Cartridge		
	20	40	60	300	500	TBD[1]
				JB/JX High Capacity Cartridge		
					700	TBD[1]
Transfer Rate (MB/sec)[2]	9	14		40	100	100 - 160[1]
FC-AL	1 Gbit			2 Gbit	4 Gbit	TBD
FC Fabric	N/A					

[1] Statements of future IBM plans and directions are provided for information purposes only and are subject to change without notice

[2]Uncompressed data.

IBM

IBM System Storage

TS1120 Tape Controller Overview

50 YEARS OF TAPE INNOVATION

TS1120 Controller Overview

- 3rd Generation Tape Controller
  - Provides up to 626 MB/sec write performance
  - Supports single TS1120 tape drive datarate of up to 230 MB/sec
- Attaches to TS1120 (and/or 3592 J1A) tape drives
- Attaches to System z servers
- Supported on
  - z/OS®, z/VM®, TPF and OS/390®
  - VSE/ESA™ and VSE/ESA with VSE guest server (VGS)
- Supports tape drives installed in a
  - IBM TS3500 or 3494 tape library
  - IBM 3592 C20 frame attached to a StorageTek 9310 silo
  - IBM 7014 Model T00 or T42 frame

TS1120 Controller Description

- One to four FICON attachments
  - Single FICON TS1120 tape drive datarate of up to 230 MB/sec
- Two to eight ESCON attachments
- Supports attachment to ESCON® and/or FICON™ hosts
  - Ideal for mixed environments and facilitates migration
    - ESCON / FICON path group mixing supported
    - No need to statically determine ESCON / FICON mix
  - Reduces ESCON / FICON director port requirements
- Attaches up to sixteen TS1120 (and/or 3592 J1A) tape drives
  - Requires a supported ‘embedded’ switch[1] or
  - Attachment to a supported SAN Fabric switch[1]

[1] Switch support can be found at http://www.ibm.com/support/techdocs/atsmastr.nsf/webindex/FQ115356

IBM System Storage

Tape Data Encryption Overview

50 YEARS OF TAPE INNOVATION

Protection of consumer information has become a significant business issue

- Many government agencies are requiring disclosure of security breaches
  - 32 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 150 million consumers have been notified of potential security breaches regarding personal information since 2/2005
  - Source: www.Privacyrights.org

Customer Tape Data Protection Challenges

- Protect tape data when removed from the primary data center
- Protect tape data generated by a different applications on different systems
- Allow access to data after it has arrived at the business continuance site or business partner
- Employ a consistent management strategy across different applications ,systems and locations

Security Breaches Can Be Costly

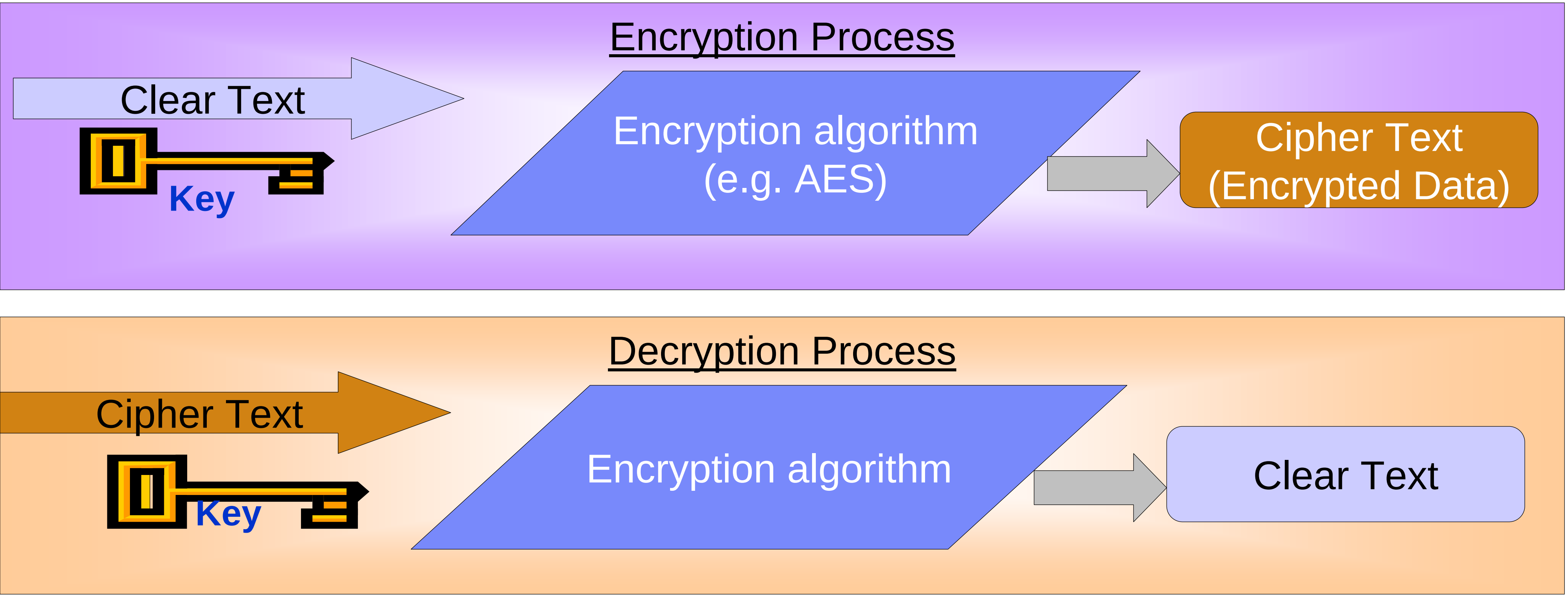
- Direct cost of mitigating security breach
  - ESG estimates the cost per lost record ranges from $25 to $150 *
- Fines and penalties
  - Security breach costs UK Financial institution nearly £1 million
- Lost consumer confidence
  - Publicly held companies also suffer a 5% stock drop in the wake of such a disclosure **

*Source: Enterprise Strategy Group Whitepaper, Enterprise Tape Backup Encryption Requirements for the Banking Industry
** Source: 2003 study “The Economic Cost of Publicly Announced Security Breaches”published in the Journal of Computer Security

Encryption
A powerful tool for protecting information

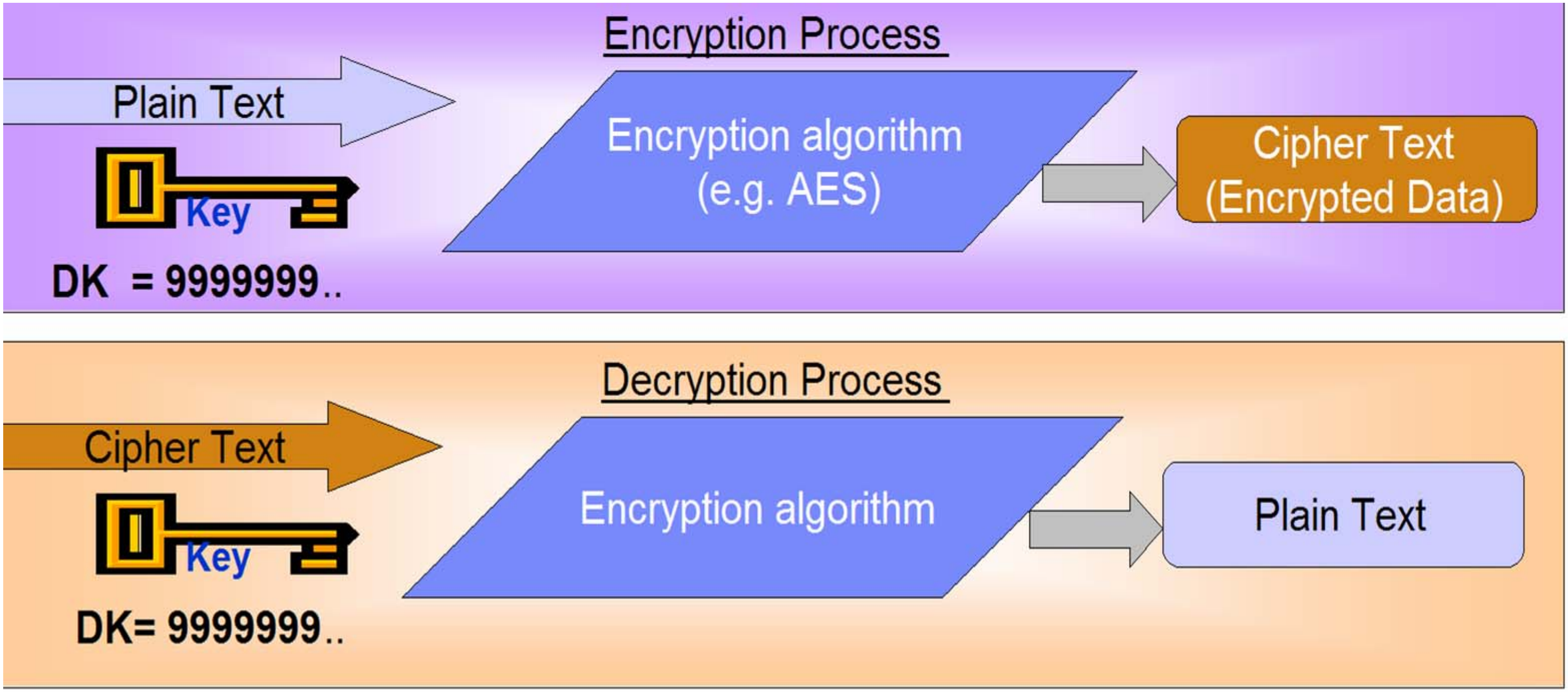
- Data is encrypted by applying an encryption method and a “key”
  - A common encryption technique is the Advanced Encryption Standard (AES)
  - Keys are random bit-streams of predetermined lengths
    - 128, 192 and 256 bits
- Encrypted data is unreadable without access to the “key”
- If encrypted data is exposed, it is generally not considered a security breach

Encryption is a technique used to help protect data from unauthorized access



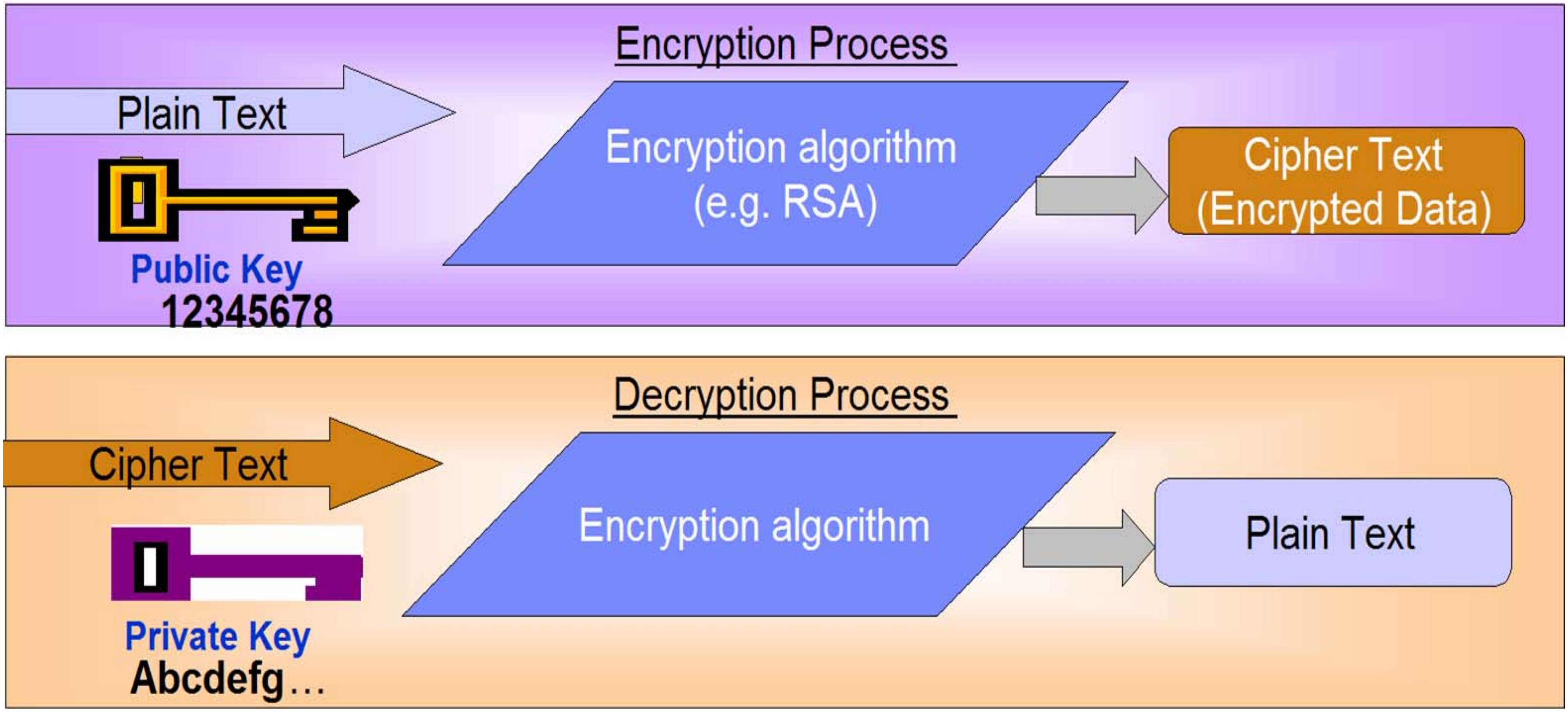
- Data that is not encrypted is referred to as “clear text”
- Clear text is encrypted by processing with a “key” and an encryption algorithm
  - Several standard algorithms exist, include DES, TDES and AES
- Keys are bit streams that vary in length
  - For example AES supports 128, 192 and 256 bit key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

Symmetric Encryption



- Data that is not encrypted – clear text
- Clear text is encrypted by processing with a “key” and an encryption algorithm
- Keys are bit streams, 256 bits for IBM drives
- Symmetric encryption – same key to encrypt and decrypt

Asymmetric Encryption



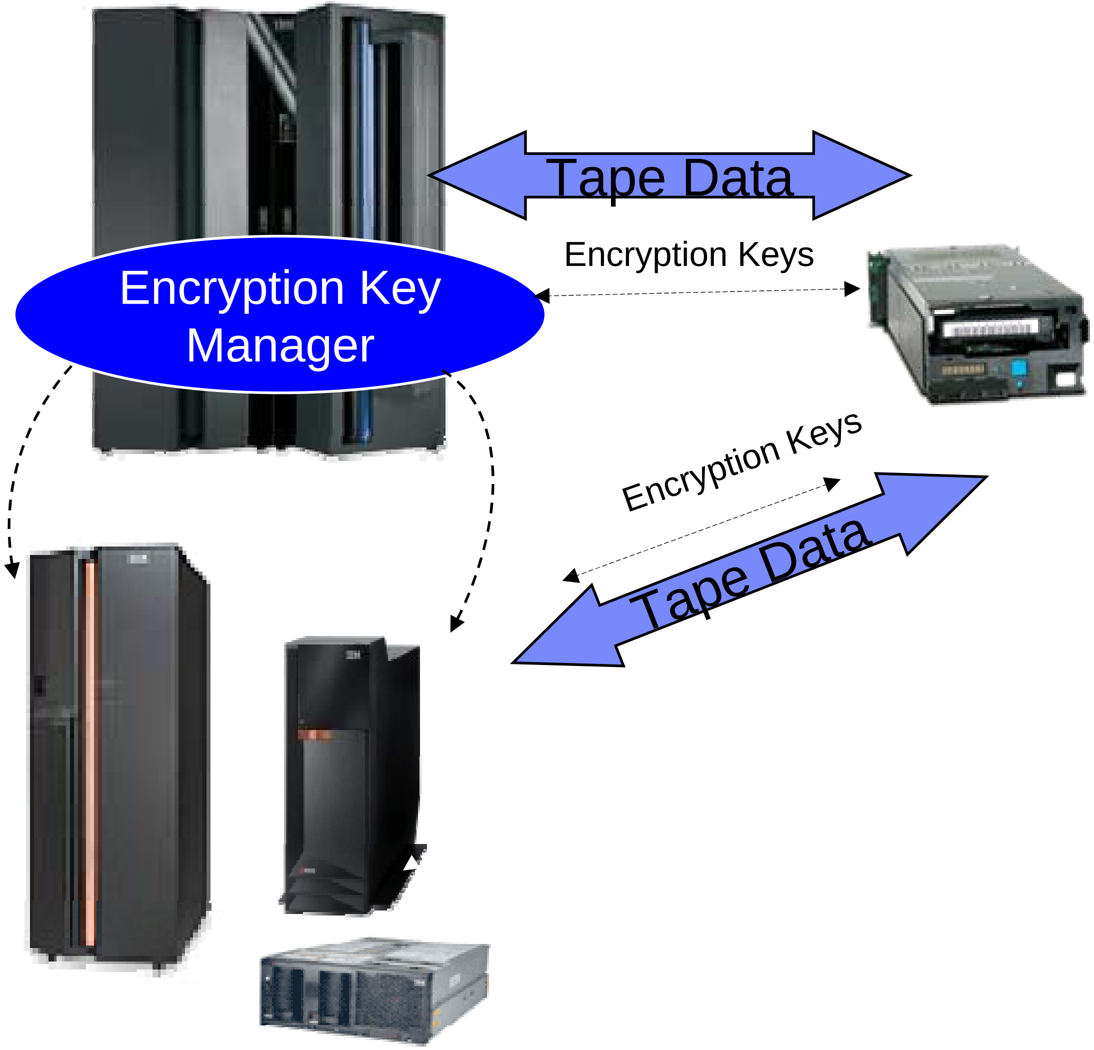
- The key used to encrypt is often referred to as the Public key, eg. the Key Encrypting Keys (KEKs) used to wrap the Data Key and create the External Encrypted Data Keys (EEDKs).
- The Public key may be made widely available without fear of compromise.
- The Key used to decrypt is referred to as the Private key.
- Private Keys must be secured against unauthorized access.
- Public / Private encryption is widely used for exchange of data between organizations.

Providing the industry’s first comprehensive end-to-end tape encryption solution

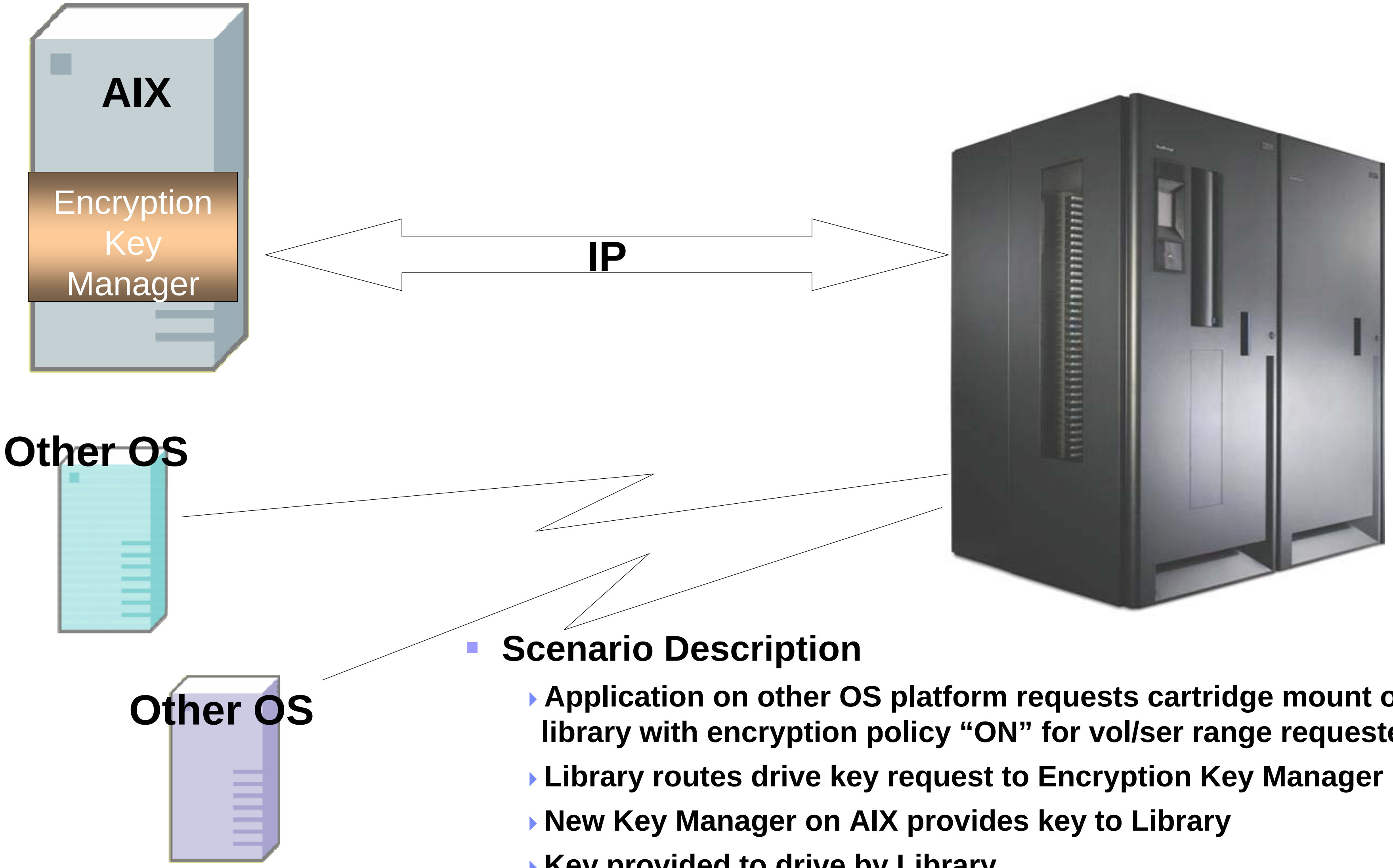
- IBM System Storage TS1120 Tape Drive
- IBM System Storage Ultrium LTO Generation 4 Tape Drive
- Encryption Key Manager program
- Integration with IBM tape systems, libraries
- Enhancements to Tivoli Storage Manager
- Integration with System z security and encryption capabilities
- New Services and consulting

Encryption Key Manager (EKM)

- Part of IBM Java
- z/OS, AIX, i5/OS, Linux, Linux for System z, HP, Sun, Windows
- Serves data keys to tape drive
- Supports System Managed Encryption (SME) and Library Managed Encryption (LME)
- Run on the same or different server than the tape application

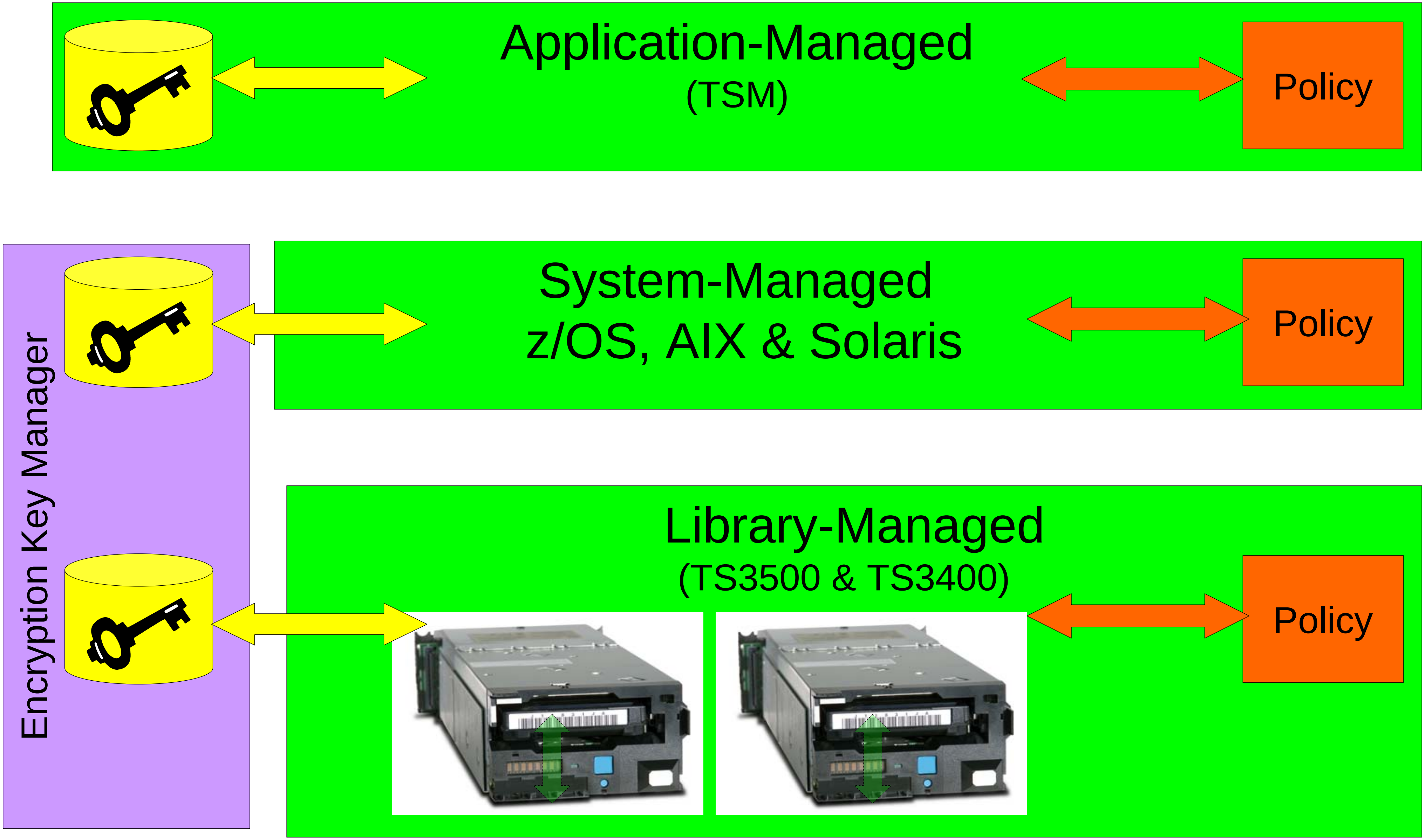


Centralized Encryption Key Manager



- **Scenario Description**
  - **Application on other OS platform requests cartridge mount on library with encryption policy “ON” for vol/ser range requested**
  - **Library routes drive key request to Encryption Key Manager**
  - **New Key Manager on AIX provides key to Library**
  - **Key provided to drive by Library**
  - **Application on other O/S begins write**

Encryption Methods



Application-Managed
(TSM)

Policy

System-Managed
z/OS, AIX & Solaris

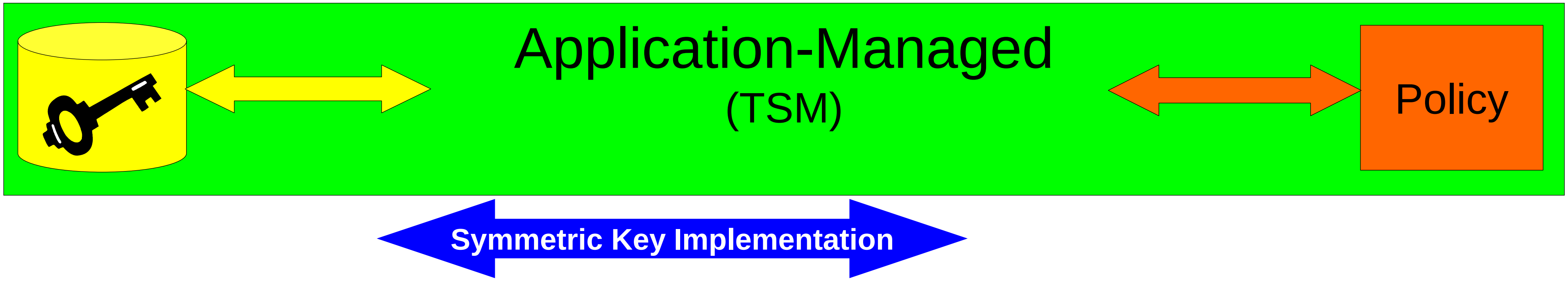
Policy

Library-Managed
(TS3500 & TS3400)

Policy

Encryption Key Manager

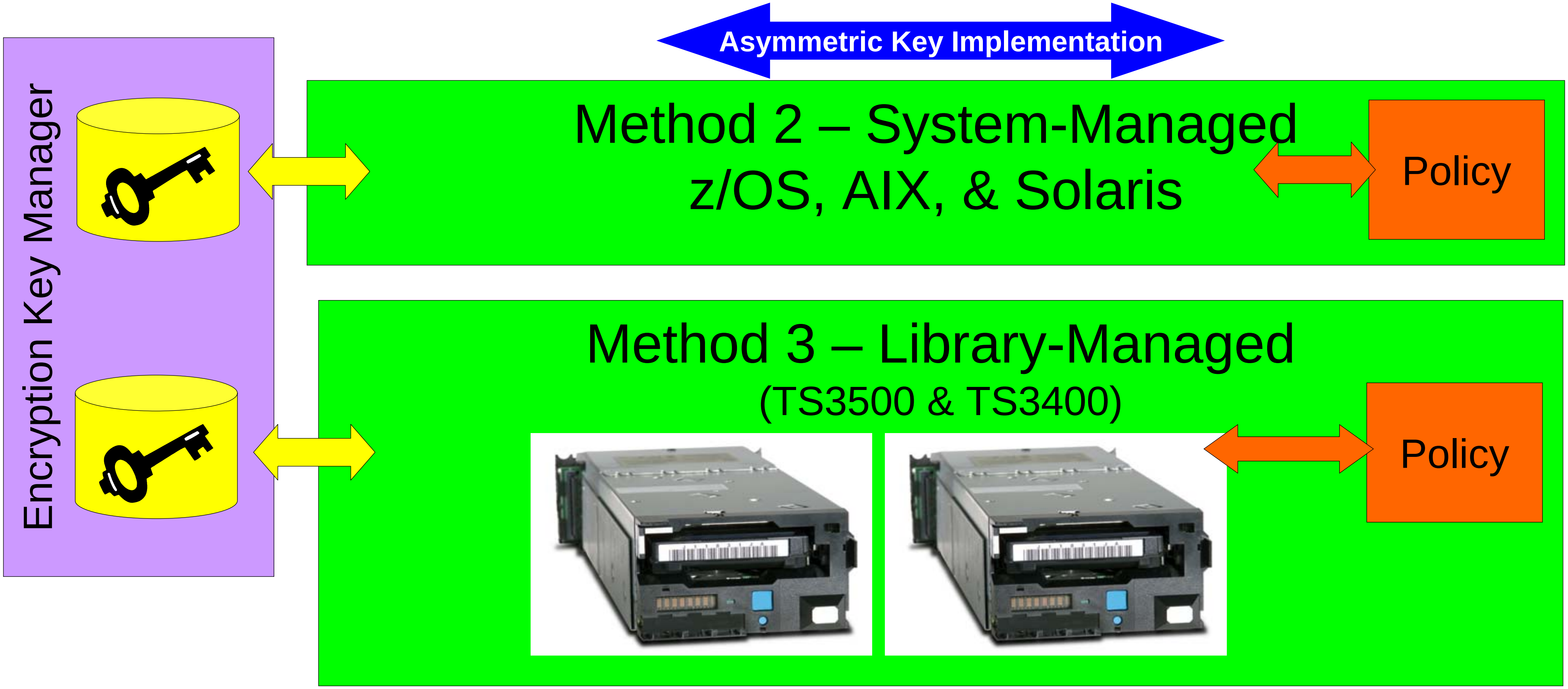
Applications which use the Application Managed reference architecture must be encryption aware.



- Application provides Policy Engine to determine if data is encrypted
- Application responsible for all Key Services
  - Generate keys
  - Associate correct key with file
  - Store/retrieve keys
  - Key flows to tape drive in the clear
- TSM supports Application Managed for the TS1120

The other reference architectures use the Encryption Key Manager to access Key Services.

- Encryption Policy provision varies by implementation
- Enterprise Key Manager (EKM) serves Keys to the TS1120 Tape Drive
  - Encrypted Data Key flows to tape drive
  - Encrypted Data Key stores on the tape media



Asymmetric Key Implementation

Encryption Key Manager

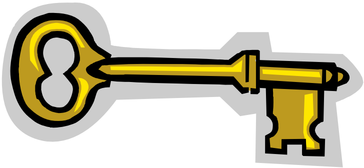
Method 2 – System-Managed
z/OS, AIX, & Solaris

Policy

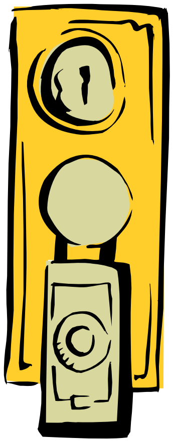
Method 3 – Library-Managed
(TS3500 & TS3400)

Policy

External Encrypted Data Key Overview



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

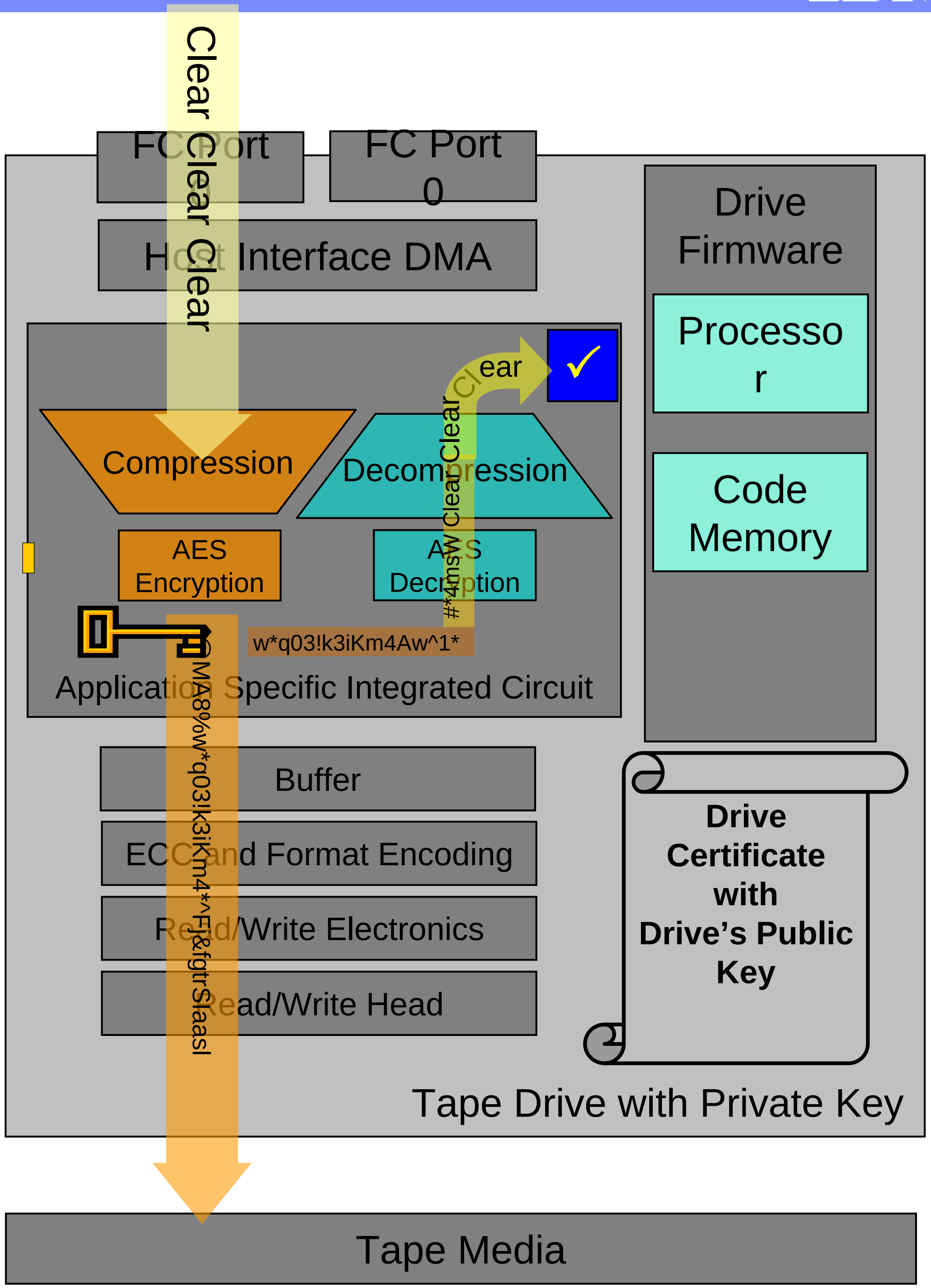


- Key Encrypting Key (KEK) Pair
  - Asymmetric Encryption RSA-2048
  - Created by the Customer/Business Partner/Third Party Provider
  - Public half used to encrypt DK
  - Private half used to decrypt DK
  - Slower than Symmetric
  - Referenced by KEK Labels or Key Labels
  - Metaphor – Real Estate Lock 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)

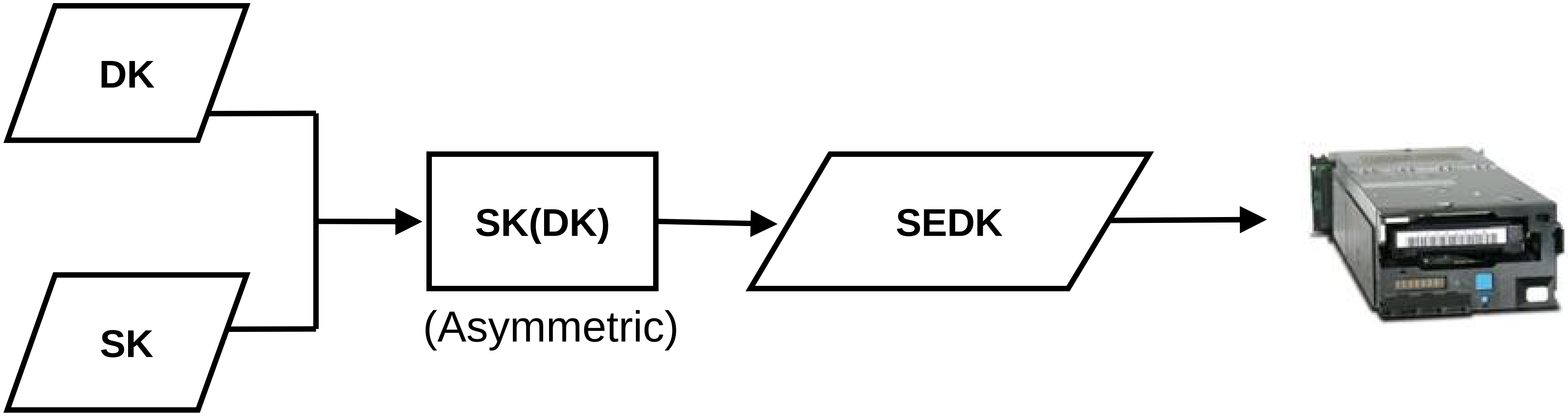
Asymmetric Key Implementation

TS1120 Encryption

- **Built-in AES 256-bit data encryption engine**
- **Look-aside decryption & decompression help assure data integrity.**
- **<1% performance and capacity impact**
- **Authentication: EKM queries drive certificate and uses public key to authenticate exchanges**



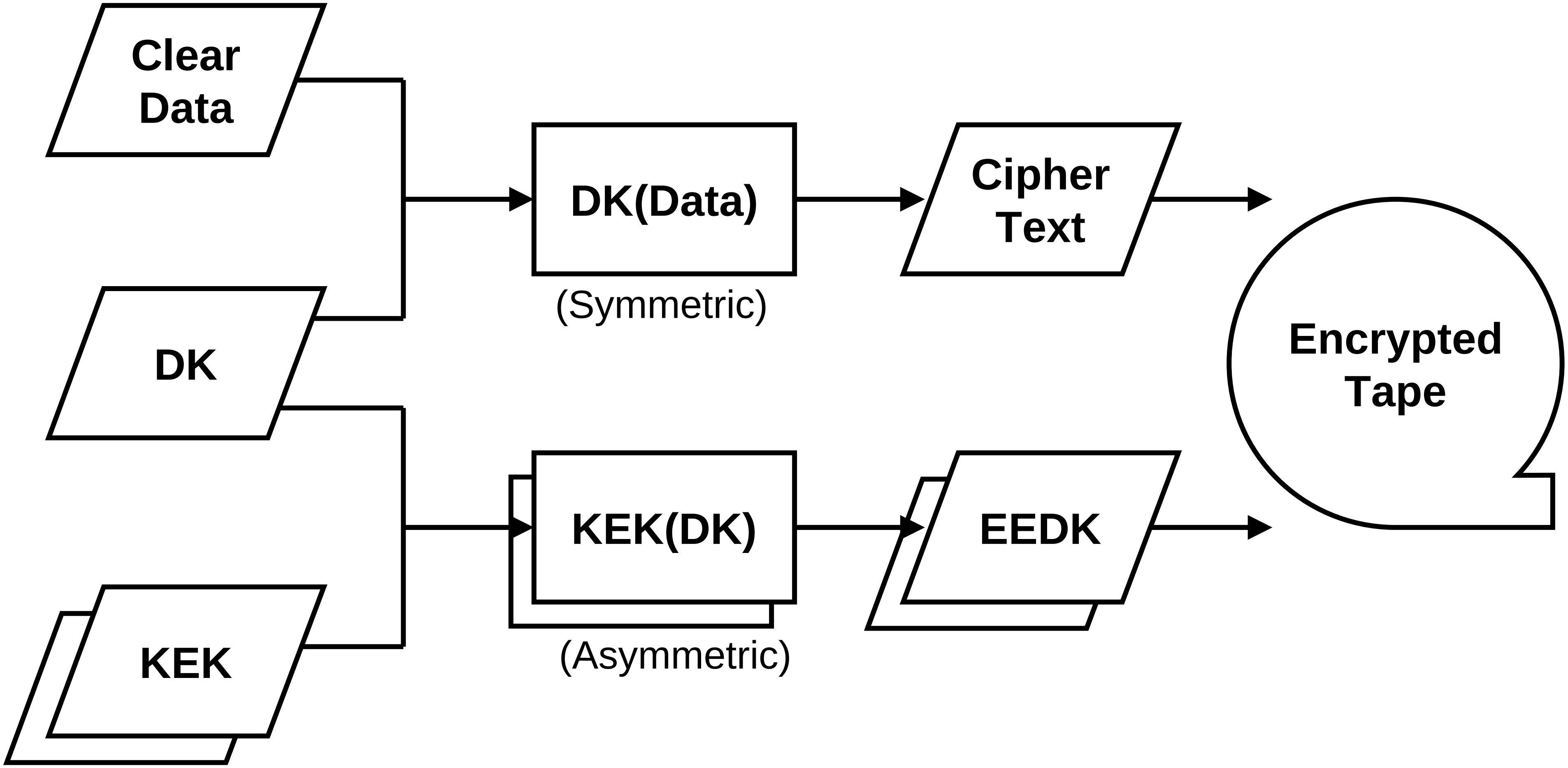
Session Key – (LME or SME)



The Session Key is an ephemeral key which is signed by the drive. The EKM authenticates the session key before using to encrypt the DK.

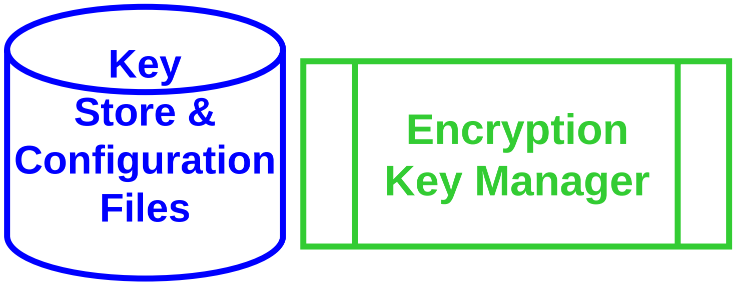
DK – Data Key (Symmetric)
SK – Session Key (Asymmetric) is randomly generated and signed by the drive (unique)
SK[DK] = SEDK = Session Encrypted Data Key

Encryption Process – TS1120 (LME or SME)



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

TS1120 Encryption Process



Write Request

1) TS1120 Receives Mount Request for write from BOT w/ Encryption

2) TS1120 Initiates Session w/ EKM, requests data key, passes optional key label

3) EKM Authenticates Drive in Drive Table

4) EKM generates a AES-256 random Data Key (DK)
EKM retrieves public key & certificate from keystore
EKM wraps Data Key w public key of KEK pair to create EEDK

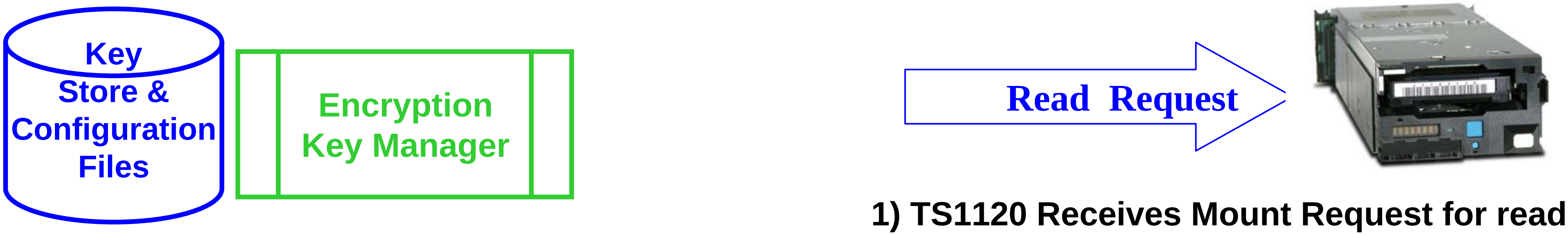
5) EKM Encrypts Data Key and Key Identifier with drive session key to create the Session Encrypted Data Key (SEDK)

6) EKM passes the EEDK & SEDK to the TS1120 Tape drive

7) TS1120 decrypts Date Key & Key Identifier

8) TS1120 writes EEDK on tape leader and CM
TS1120 encrypts & writes data to cartridge

TS1120 Decryption Process



1) TS1120 Receives Mount Request for read or append operation.

2) TS1120 retrieves EEDK & Key Identifier

3) TS1120 Initiates Session w EKM, passes EEDK & Key Identifier to EKM

4) EKM Authenticates Drive in Drive Table

5) EKM fetches private key and certificate from keystore

6) EKM unwraps EEDK using private key of KEK pair
to recover Data Key

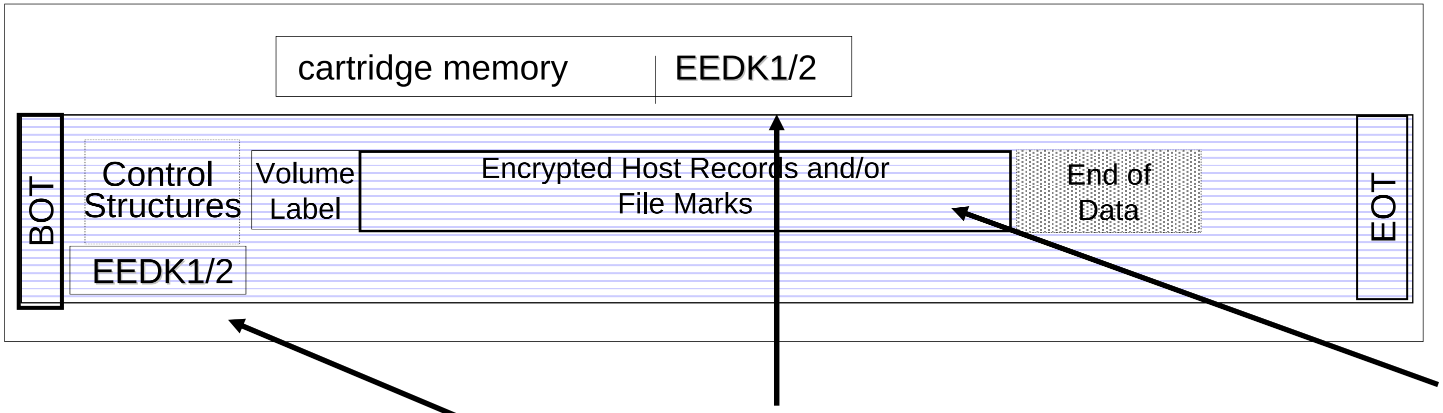
7) EKM Encrypts Data Key w drive session key
EKM passes SEDK to the drive

8) TS1120 receives & decrypts Date Key

9) TS1120 reads data from or write appends data to the cartridge.

TS1120 Media Format Elements

- Encrypted Tape Volume
  - Standard 3592 media
  - Entire volume is encrypted or non-encrypted
  - Common scratch pool with full re-format between encrypted and non-encrypted
  - Full support for wrapping keys
    - Simplifies key management and DR/ BP scenarios
  - Two Wrapped Key Structures (EEDKs) may be active on a cartridge

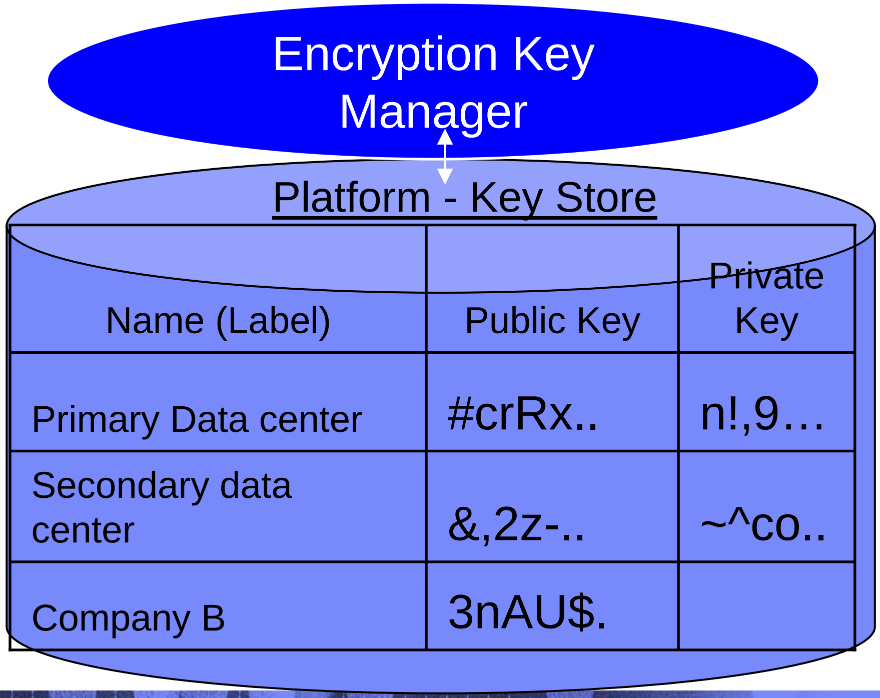


Data area symmetric encryption AES-256 with DK

"wrapped keys" KEK[DK]
Asymmetric encryption
RSA-2048 with KEK

Use of Public Key Cryptography greatly simplifies encryption key management while supporting high levels of security

- A public key can be used to encryption many tape cartridge keys
  - For example, all cartridge keys at a given location may be encrypted with the same public key, substantially reducing the number of keys the customer manages
- Encrypted data keys are stored on the tape cartridge
  - If the cartridge is available, the encrypted cartridge keys are protected
- Business partner exchange uses partner’s public key
  - Eliminates need to share secret cartridge keys

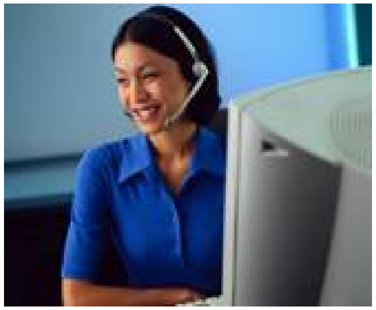


Name (Label)	Public Key	Private Key
Primary Data center	#crRx..	n!,9…
Secondary data center	&,2z-..	~^co..
Company B	3nAU$.	

Example of Tape Data Exchange

Company A

Company B



Please send us the data, here is our public key

Company A Key Store

Name (Label)	Public Key	Private Key
Primary Data center	#crRx..	n!,9…
Secondary data center	&,2z-..	~^co..

Company B Key Store

Name (Label)	Public Key	Private Key
…..	….	…..
……	…..	…..
External Key	3nAU$.	oi!~>

Transport encrypted tape cartridge to Company B

IBM Tape Encryption Solution – *Customer Value*

- **High performance** data encryption provides solution for large volume data encryption
  - Encryption performed at tape drive hardware speeds of up to 100 MB/second (uncompressed)
- **Simplified tape encryption management**
  - Application transparent implementations available for systems and library managed environments
  - Cartridge data keys stored in encrypted form on the tape cartridge
  - Supports a single encryption key mgt approach which may help reduce audit and compliance costs
- Provides an **enterprise** encryption key management solution
  - Common software for open systems and mainframe environments-May share a common key store
  - Integration with z/OS policy, key management, and security capabilities provides a proven, highly secure infrastructure for encryption key management
  - Uses Public Key encryption to support business partner tape cartridge exchanges
- **Comprehensive solution** for z/OS customers
  - Encryption Facility for z/OS software provides a method using the same secure infrastructure as the TS1120 encryption for share tape data with business partners who utilize different tape formats
- A **cost effective** solution for tape data encryption
  - Encryption in tape drive off-loads encryption task from servers
  - Leverages existing tape infrastructure – incorporated into standard IBM tape libraries
  - Eliminates need for unique appliance hardware

Thank You!