IBM Power Systems Platform
IBM System i and i5/OS
Data Encryption Options

Sue Baker
IBM Advanced Technical Support
Rochester, MN

i5OS

Agenda

- **Why is Encryption Hot in the Marketplace Today?**
- **Alternatives for Encryption on IBM System i and i5/OS**

  – Encrypt Data in your Database/Application

  – Encrypt Data using Middleware

  – Encrypting Data via an Encrypted ASP – V6R1

  – Encrypt Data via Tape Appliances

  – Encrypting Data via Tape Drives with Built-in Encryption

  – Overview of Encryption Solution on IBM Tape Drives

  – The Encryption Key Manager (EKM)

  – BRMS and Tape Encryption

  – Encryption - How to get Started
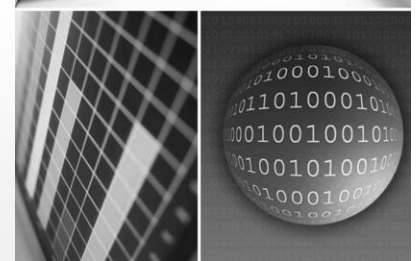
Why is Encryption Hot in the Marketplace Today?

Tape and Data Encryption

Customer Data EXPOSED!!

- **Many government agencies are requiring disclosure of security breaches**
  - 38 states have enacted legislation requiring notification in cases of security breaches
    - Source: www.Privacyrights.org
  - Similar federal 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 90 million consumers have been notified of potential security breaches regarding personal information since 2/2005**
  - Source: www.Privacyrights.org

In the News

TAPES LOST!

Privacy Commission Contacted

In a move that could fuel efforts to change data storage practices, records management provider ABC Co has admitted losing a customer's backup tapes and is recommending that customers begin encrypting tapes.

Although data encryption is not a new issue, it is a growing business security focus. Increased awareness of customer privacy, an increase in identity theft crimes, and more technical savvy criminals are all contributing.

New state, federal and industry regulations to protect personal data, credit card numbers, etc, are making this an issue of interest to many businesses

Tape and Data Encryption

- **Many government agencies are requiring disclosure of security breaches**
  - 38 states have enacted legislation requiring notification in cases of security breaches
    - Source: www.Privacyrights.org
  - Similar federal 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 90 million consumers have been notified of potential security breaches regarding personal information since 2/2005**
    - Source: www.Privacyrights.org

Customer Data EXPOSED!!

Costs from Security Breach

Direct Costs
- Fines and penalties
- Customer notification
  - letters
  - postage
  - hotline
  - credit checks
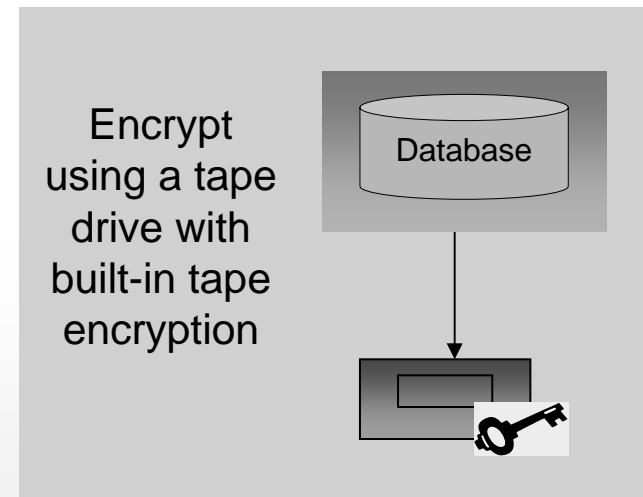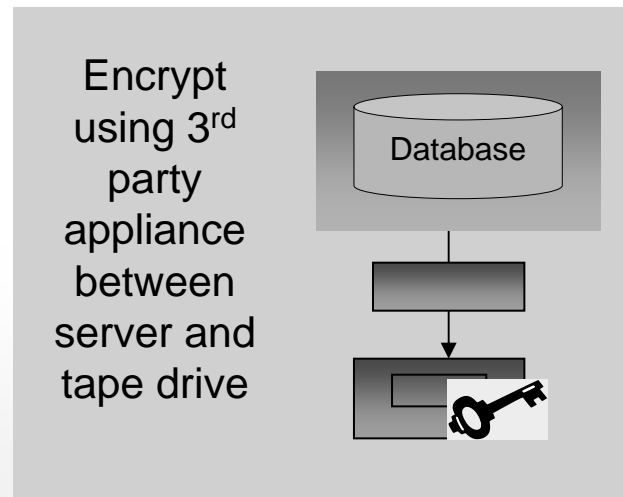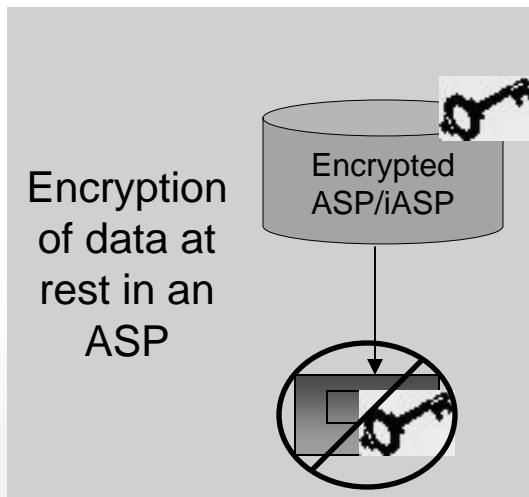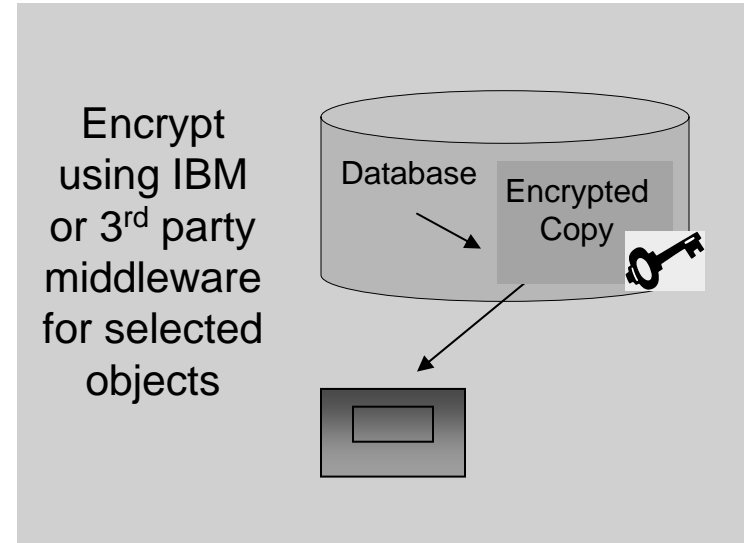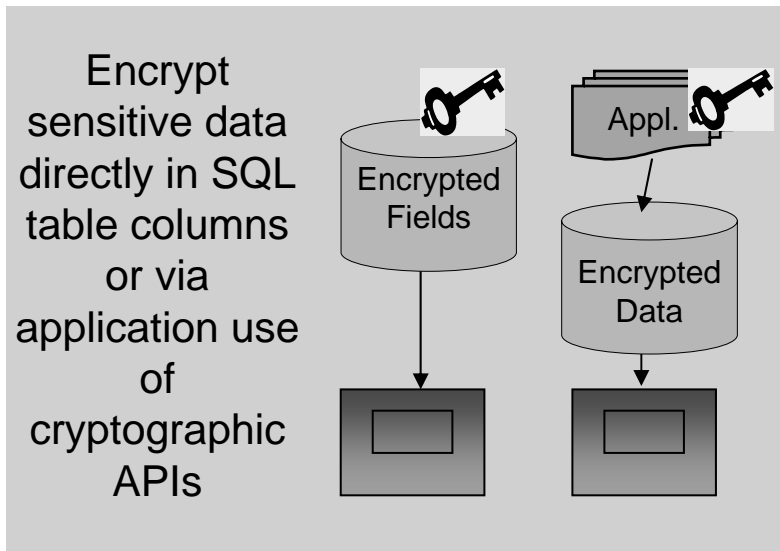- Public Relations costs
- Legal Actions

$$\$\$$$

Indirect Costs
- Loss of reputation
- Loss of customer goodwill
- Government investigations

Alternatives for Encryption on IBM System i

Techniques for Encrypting Data on System i

Encrypt sensitive data directly in SQL table columns or via application use of cryptographic APIs

Encrypted Fields

Appl.

Encrypted Data

Encrypt using IBM or 3rd party middleware for selected objects

Database

Encrypted Copy

Encryption of data at rest in an ASP

Encrypted ASP/iASP

Encrypt using 3rd party appliance between server and tape drive

Database

Encrypt using a tape drive with built-in tape encryption

Database

i5/OS V6R1 Enhancements

- **i5/OS V6R1 cryptographic key management enhancements**
- **Encrypted BRMS backups of user data to tape or virtual tape**
- **Encryption of data residing in an ASP (user and independent)**

Announce	1/29/08
GA	3/21/08

Encrypting Data in your Database/Application

Encrypting Data in your Database/Application

Four methods to choose from:

- DB2 column encryption (V5R3 onwards)

- i5/OS cryptographic API's (V5R3 onwards)

- Java cryptographic extensions (API's)

- 4764 cryptographic co-processor and API's

Let's look at these in more detail!

DB2 Column Encryption	i5/OS Crypto API's	Java Crypto Extensions (API's)	4764 Crypto Co-Processor and API's

Encrypting Data in your Database/Application

DB2 column encryption

- Built-in to i5/OS from V5R3 onwards

- Native DB2: use "Before Insert" and "Update" triggers

- SQL: use SQL functions and "Instead of" triggers

- Details available in the i5/OS Information Center

DB2 Column
Encryption

Encrypting Data in your Database/Application

i5/OS cryptographic API's

- Built-in to i5/OS from V5R3 onwards

- Called by an application program

- Use industry standard encryption algorithms

- V5R3: Application must handle keys

- V5R4: Key Mgmt APIs store master keys below the Machine Interface (MI) – i.e., never in the clear in the application

Encryption
Services Provided

Encryption

Data
Integrity

Authentication

Digital
Signature

Random #'s

DB2 Column
Encryption

i5/OS
Crypto API's

Encrypting Data in your Database/Application – V6R1

- **i5/OS V6R1 cryptographic key management enhancements**
  - GUI and CL interface to manage master keys
    - New master key for ASP encryption (256 bit)
    - New master key for save/restore (256 bit)
  - GUI and CL interface to manage i5/OS keystore and keys

Announce	1/29/08
GA	3/21/08

Master Key Management – V6R1

i5OS™
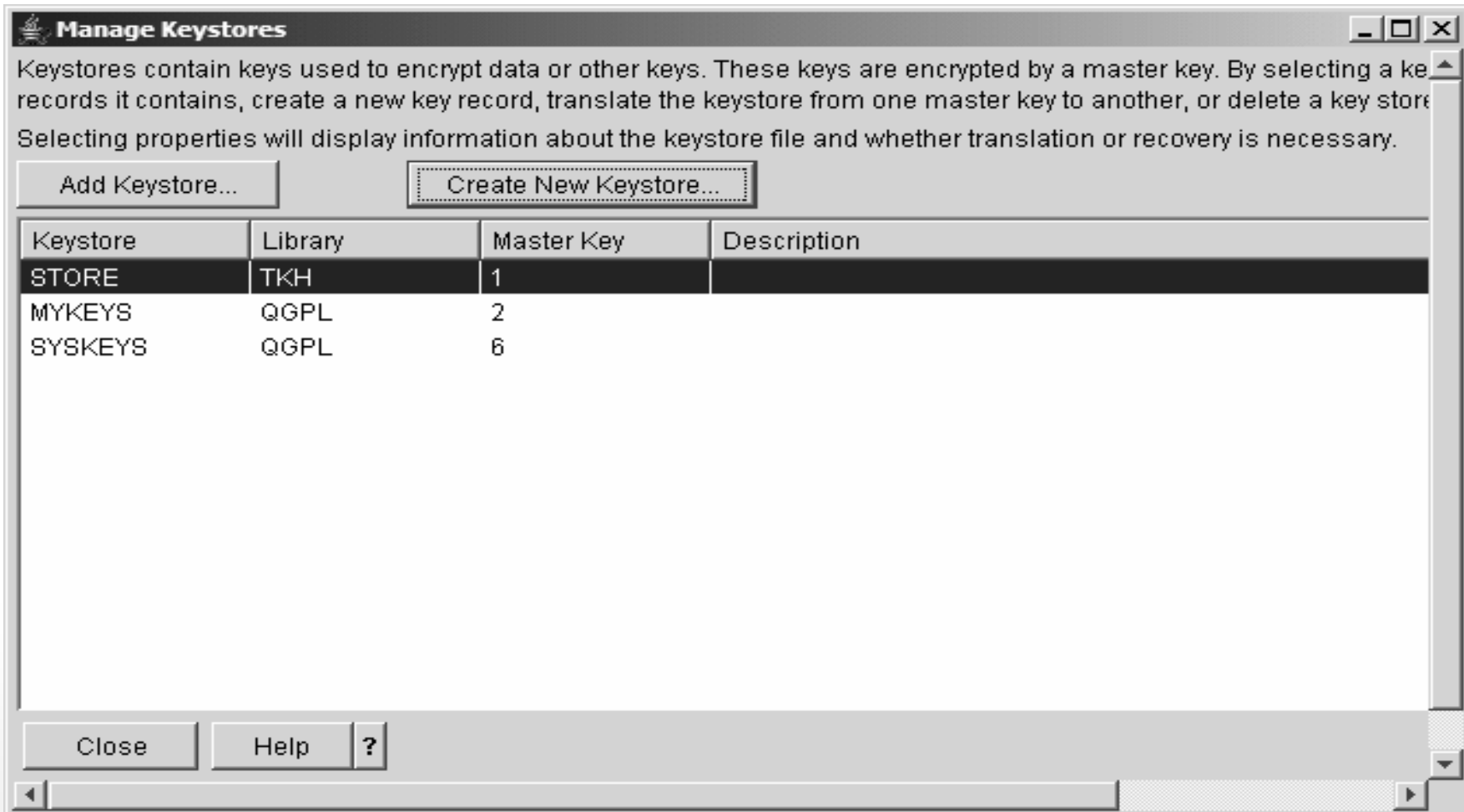Version 6 Release 1

Manage Master Keys ▬ ☐ ✕

Master keys are used to encrypt other keys. You can load, set, clear or display the properties of the selected master key.

Master Key	Status	Current Key Verification Value
1	Set	ED0CF6D746C7B560CAFF22FF7F82EFCC1D1CEE19
2	Set	D1922FE0A0F03FFCBA16631C8D490644E4ADC0E7
3	Set	1B2B8913098DEB8EC4DDBDAEDB8B9E38CCF70737
4	Not set	
5	Not set	
6	Set	1B2B8913098DEB8EC4DDBDAEDB8B9E38CCF70737
7	Not set	
8	Not set	
SAVRST	Default	16C1D3E3C073E77DB28F33E81EC165313318CE54
ASP	Not set	

Close   Help   ?

Set of master key 2 was successful.

Keystore Management – V6R1

Keystore Management – V6R1

Keystore Contents ✕

Keystore file:	MYKEYS
Keystore library:	QGPL
Master Key:	2

[New Key Record]

Key Record Label		Type	Key Size	Translation Status	Date Translated
AES KEY 1	...	AES	16	Current	January 11, 2008 1:35:07 PM CST
Triple DES key	...	Triple DES	16	Current	January 11, 2008 1:35:33 PM CST
My Private key	...	RSA private	1024	Current	January 11, 2008 1:36:05 PM CST
Another AES key	...	AES	16	Current	January 11, 2008 1:36:44 PM CST

[Close] [Help] [?]

Encrypting Data in your Database/Application – V6R1

- **i5/OS V6R1 cryptographic key management enhancements**
  - Save/restore of software master keys
  - Improved SSL acceleration using the 4764 Cryptographic coprocessor
  - New algorithm modes
  - New hardware based JCE provider

Announce	1/29/08
GA	3/21/08

Encrypting Data in your Database/Application

Java cryptographic extensions (API's)

- JCE for short

- Part of i5/OS Developer Toolkit for Java (5722-JV1)

- Similar services to i5/OS crypto APIs

  - Adds Digital Signature Algorithm (seldom used)

- Application must manage/store encryption keys

Encryption
Services Provided

Encryption
Data
Integrity
Authentication
Digital
Signature
Random #'s

Digital Signature
Algorithm

DB2 Column
Encryption

i5/OS
Crypto API's

Java Crypto
Extensions
(API's)

Encrypting Data in your Database/Application

Encryption Services Provided

4764 cryptographic co-processor and API's

- Orderable hardware feature

- Application program calls the APIs to access the encryption functions of the co-processor

- API's standard across platforms

- Main advantage: key is stored in hardware
  - FIPS 140 security standard

DB2 Column Encryption	i5/OS Crypto API's	Java Crypto Extensions (API's)	4764 Crypto Co-Processor and API's

Encryption
Data
Integrity
Authentication
Digital Signature
Random #s
Digital Signature Algorithm
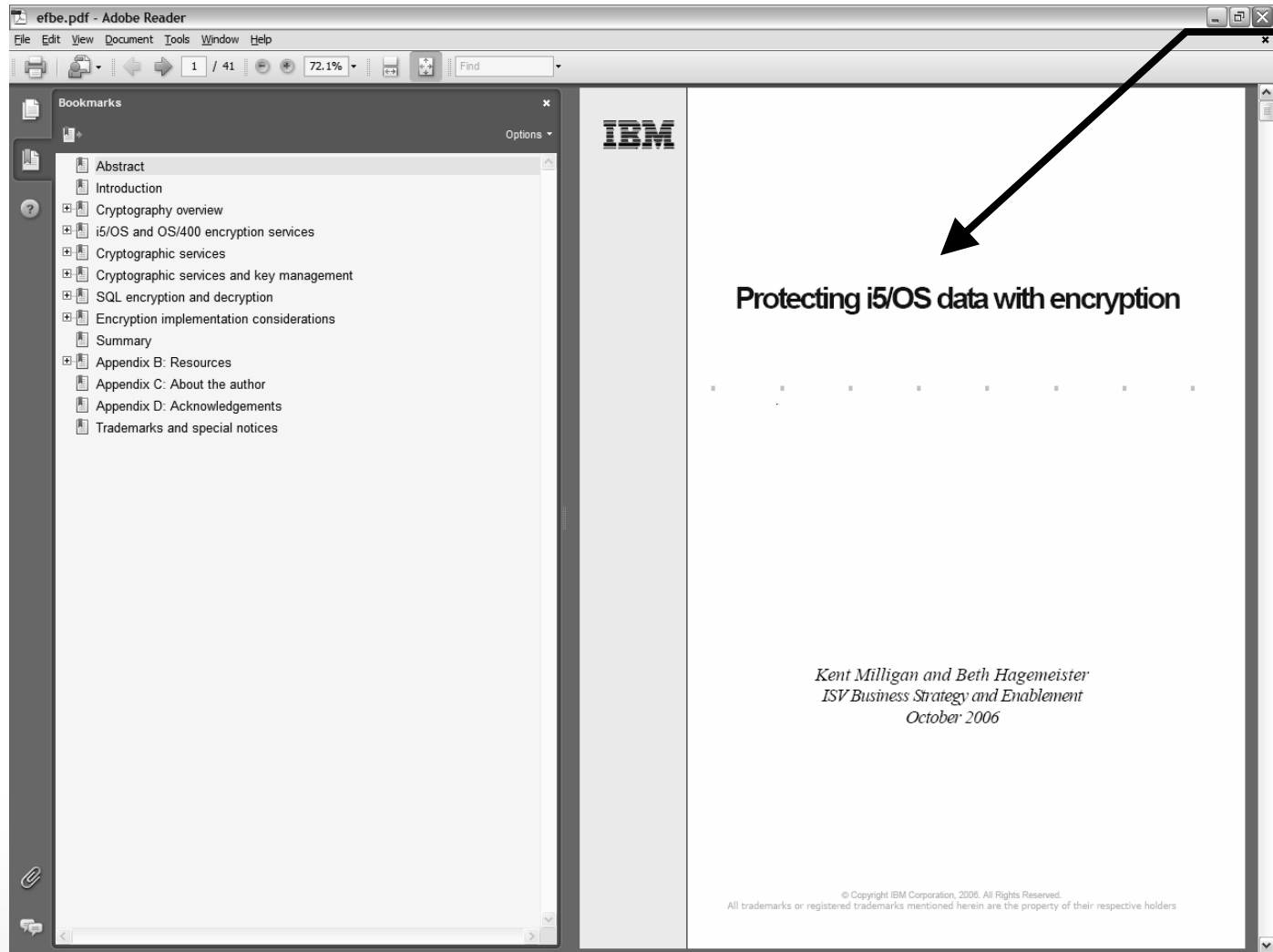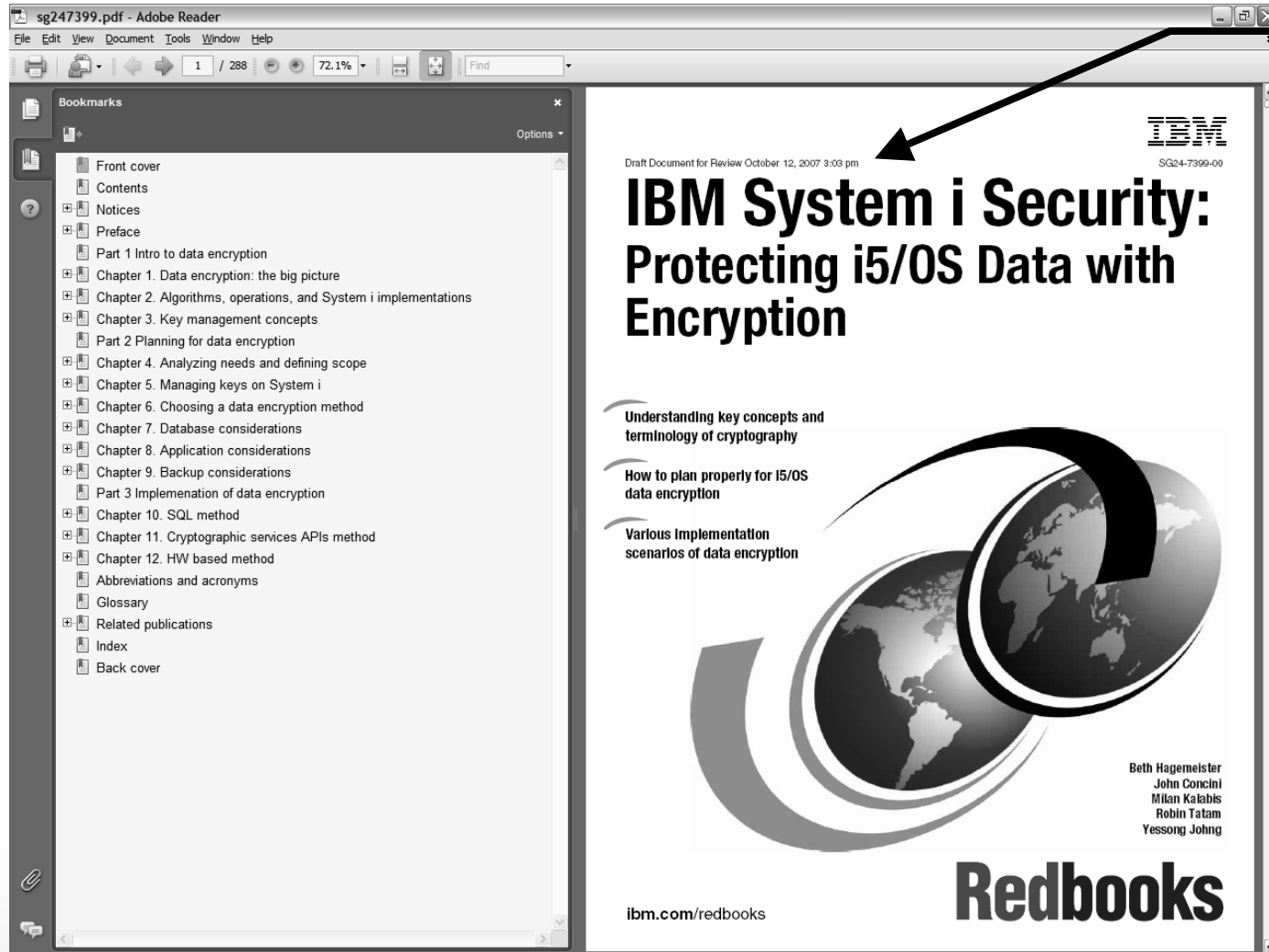Financial PIN
Europay
MC Visa

Protecting i5/OS Data with Encryption Whitepaper

Great whitepaper that came out last year

Protecting i5/OS data with encryption

Kent Milligan and Beth Hagemeister
ISV Business Strategy and Enablement
October 2006

Bookmarks
- Abstract
- Introduction
- Cryptography overview
- i5/OS and OS/400 encryption services
- Cryptographic services
- Cryptographic services and key management
- SQL encryption and decryption
- Encryption implementation considerations
- Summary
- Appendix B: Resources
- Appendix C: About the author
- Appendix D: Acknowledgements
- Trademarks and special notices

© Copyright IBM Corporation, 2006. All Rights Reserved.
All trademarks or registered trademarks mentioned herein are the property of their respective holders

http://www-03.ibm.com/servers/enable/site/education/wp/efbe/efbe.pdf

Protecting i5/OS Data with Encryption Redbook

New Redbook currently in a draft version

http://www.redbooks.ibm.com/redpieces/pdfs/sg247399.pdf

Encrypting Data using Middleware

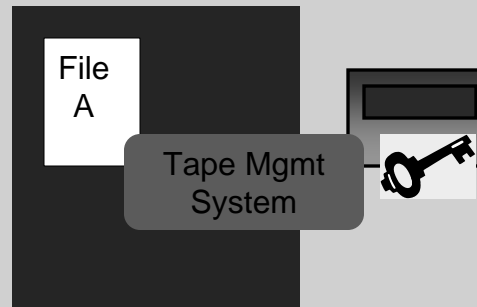# Non-IBM Middleware for Encryption

Encrypt then save/transmit

File A

File A'
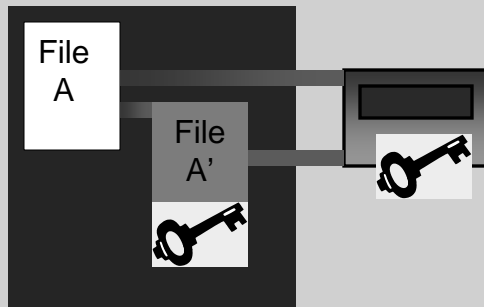
Benefits:

- Typically low cost
- Good for small amount of data to encrypt and/or long backup window

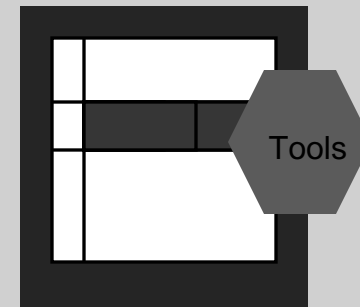## Tape Management Systems

File A

Tape Mgmt System

Watch for:

- Performance
- Extra disk required
- Key management functions
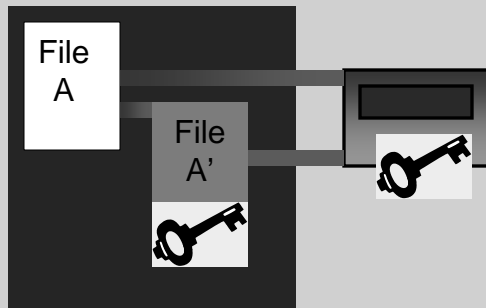- Added complexity

Encryption Tools

Tools

Example:

Records can grow when they are encrypted. Tools/techniques are available to help .

** Note: These products are supported by the vendor, not by IBM, and are included here only as examples

Non-IBM Middleware for Encryption
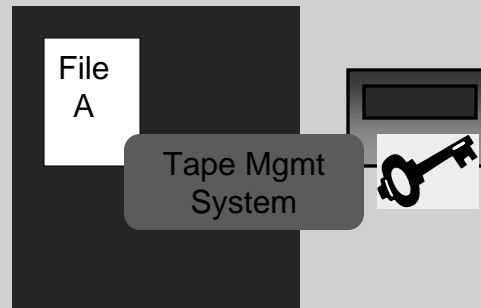
Encrypt then save/transmit

File A

File A'

PKWARE

PATRICK TOWNSEND & ASSOCIATES
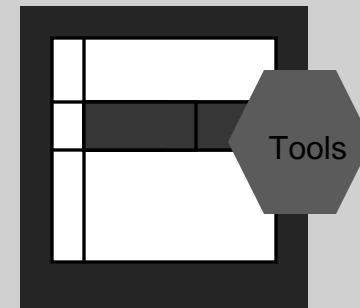
LINOMA SOFTWARE

Tape Management Systems

File A

Tape Mgmt System

help/systems INC.

Encryption Tools

Tools

nuBRIDGES

** Note: These products are supported by the vendor, not by IBM, and are included here only as examples

Third-party Host Software-based Encryption

- **Multiple vendors offer System i software-based encryption products, and many offer trial downloads of their product so that application functionality can be explored. Examples include:**

- **Help/Systems**
    - http://www.helpsystems.com/ops/save.html

- **Linoma Software**
    - http://www.linomasoftware.com/products/transferanywhere

- **Patrick Townsend & Associates, Inc**
    - http://www.patownsend.com/AES.htm

- **PKWARE, Inc**
    - http://www.pkware.com/index.php?option=com_content&task=view&id=37&Itemid=84

- **NuBridges**
    - http://www.nubridges.com/

** Note: These products are supported by the vendor, not by IBM, and are included here only as examples

IBM Middleware for Encryption – V6R1

- **Encrypted BRMS backups of user data to tape or virtual tape**
  - Encrypted Backup Enablement – i5/OS Option 44
  - This is a priced option

- **BRMS enabled encryption will be supported for:**
  - Any tape library
  - Standalone tape drive
  - Virtual tape
  - Media duplication

- **What can be encrypted?**
  - All user data
  - The operating system cannot be encrypted
  - Tape labels will not be encrypted

- **Performance considerations**
  - Software encryption will require additional processor capacity

Announce 1/29/08
GA   3/21/08

Encrypting Data via an Encrypted ASP – V6R1

Encryption of Data at Rest on Disk – V6R1

- **New in i5/OS V6R1, encryption of data residing in an ASP (user and independent)**
  - Encrypted ASP Enablement – i5/OS Option 45
  - This is a priced option

Announce	1/29/08
GA	3/21/08

Encryption of Data at Rest on Disk – V6R1

- **Meet regulatory requirements being imposed on our customers**
- **Reduce or eliminate the need for application providers to encrypt data**
- **Provide a more secure solution to help protect data**
  - Key management done by the system
- **Encryption of data at rest**
  - Software solution
  - Minimal key management requirements
- **Threats**
  - Protection of 'data in flight' to SAN
  - Protection of 'data in flight' in cross-site mirroring environment
  - Data loss
    - Physical loss of a disk drive (switched ASP)
    - Return a drive to a vendor (drive replacement or upgrade)

Implementation Approach – V6R1

- **Provide the capability to encrypt all data residing on an ASP**
- **Cryptographic keys will be stored in software but protected by "isolated" storage and master keys**
- **Minimal change required to an application**
  - ASP level changes may be required
- **Encryption/Decryption done at low level in SW**
  - Storage Management in LIC (Write and Read to/from disk)
- **Encryption keys, for switched ASPs, stored in the Independent ASP, protected by the master key in the system ASP**
- **Encryption keys for encrypted User ASP stored in the system ASP**
- **AES (Advanced Encryption Standard) algorithm**
- **Randomly generated 256 bit encryption keys (for both independent and user ASP)**

Restrictions in V6R1

- **Encryption decision must be specified during ASP configuration. No option to turn on/off encryption after configuration**
- **Master keys can be changed by the system administrator**
- **No option to change data encryption keys after configuration**

ASP Key Management – Independent ASP – V6R1

- **Master Key, in system ASP, protects data encryption key stored on the IASP**
- **Data encryption key is unique for each IASP**

System ASP

ASP-Master-Key-Sys-1

ASP1

ASP2

ASP3

'DATA-KEY1

'DATA-KEY2

'DATA-KEY3
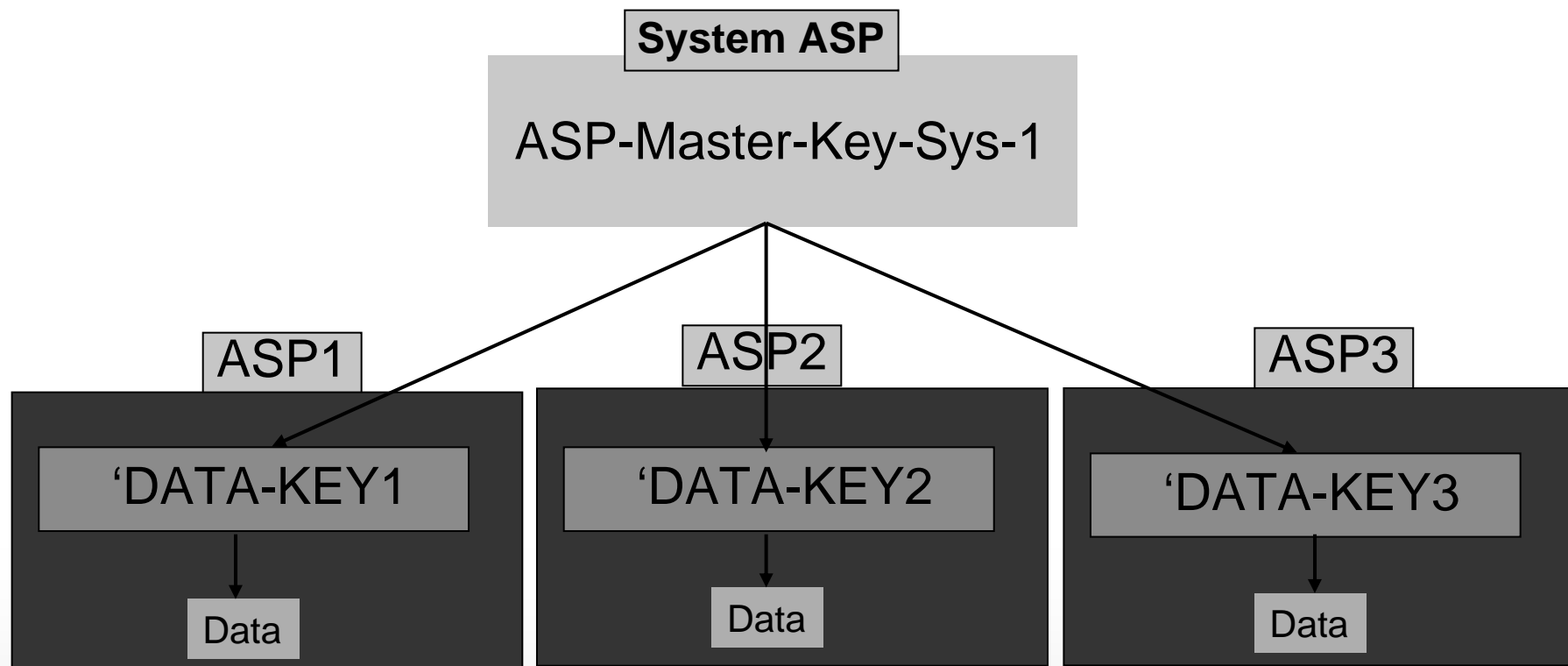
Data

Data

Data

REQUIREMENT: ASP Master Key equal on all systems in cluster

ASP Key Management – User ASP – V6R1

- **Data encryption key is stored in the system ASP**
- **One data encryption key is used to protect all User ASPs**

System ASP

ASP-Data-Key1

ASP1

Data

ASP2

Data

ASP3

Data
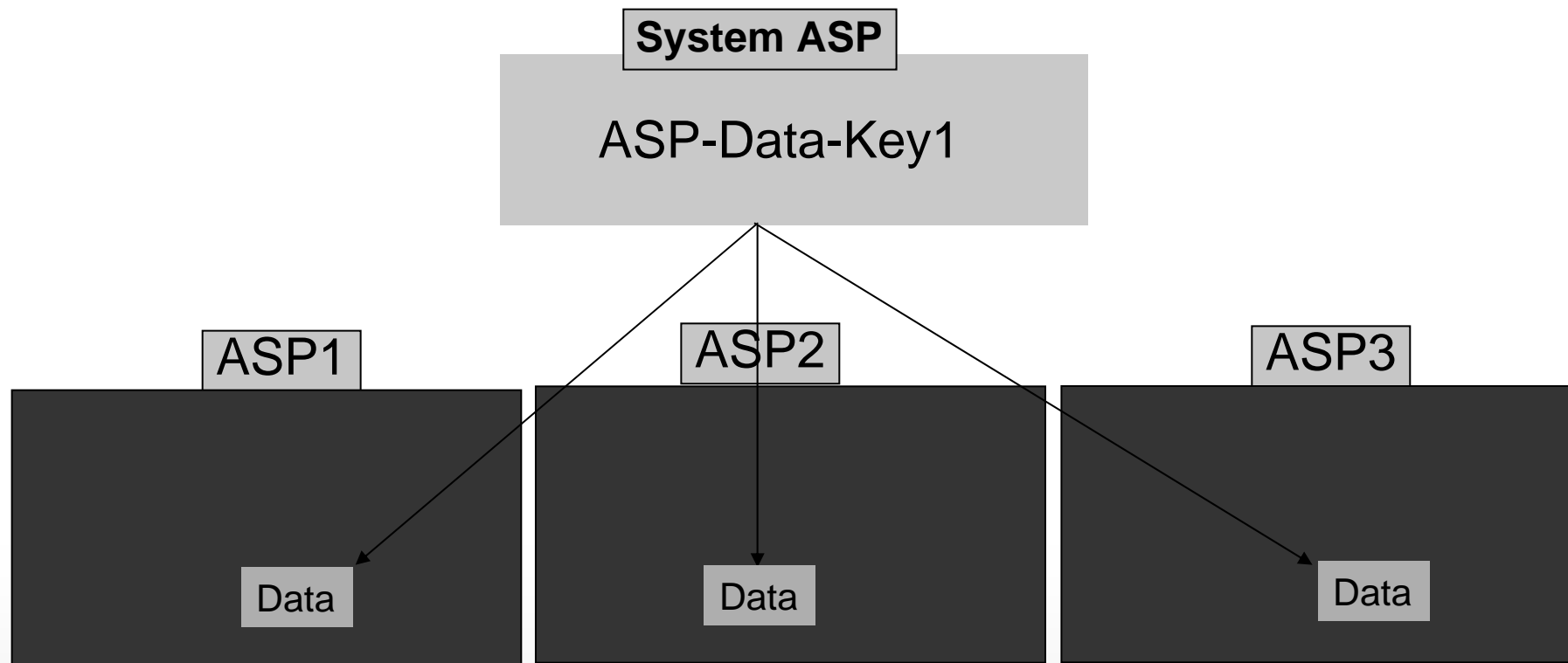
Encryption Performance – V6R1

- **Encryption is CPU intensive**
- **Certain types of applications can perform well, others may have problems**
  - Encrypting/decrypting many pages (objects) when CPU bound will be a problem
  - Encrypting/decrypting many pages (objects) when CPU capacity is available will NOT be a problem
  - Disk paging rate of the application will determine feasibility
- **AES Algorithm**
  - ~85MB per second on single dedicated POWER5 processor
    - ~22,000 4K pages per second

Encrypting Data via Tape Appliances

Non-IBM External Tape Encryption Appliances

System i

SAN Switch

Tape Drive

Encryption Appliance
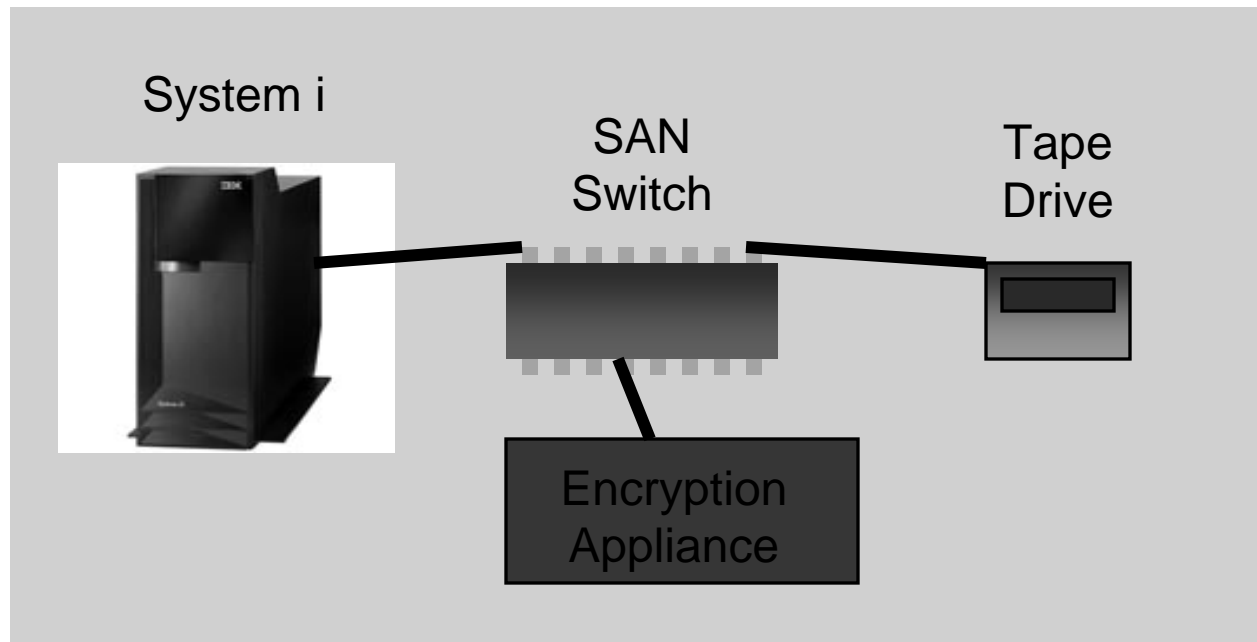
Benefits

- Don't need latest tape drives

Watch For

- Performance, especially if appliance encrypts prior to compaction

- Recovery/alternate IPL testing

- Key management

Examples:

DECRU®
A NetApp Company

Decru, Inc
    http://www.decru.com/products/dsSseries.htm
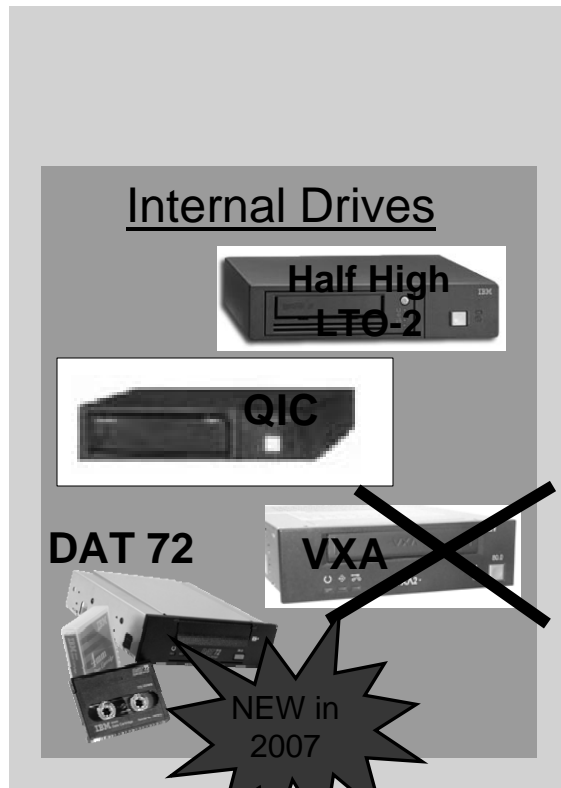
NeoScale™

NeoScale Systems, Inc
    http://www.neoscale.com/English/Products/CryptoStor_Tape.html

** Note: These products are supported by the vendor, not by IBM, and are included here only as examples

Encrypting Data via Tape Drives with Built-in Encryption

Current IBM Tape Product Line for System i

Internal Drives

Half High LTO-2

QIC

DAT 72   **VXA**

NEW in 2007

LTO Family

LTO4 new in 2007

TS3200

TS3310

TS2340   **TS3100**

TS3500

Enterprise Family
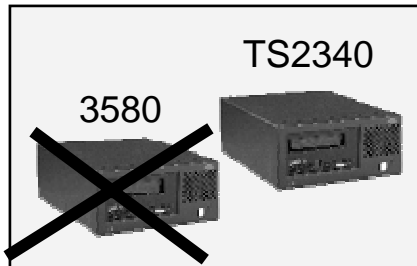
TS3400

NEW in 2007

TS1120

- Low cost
- Good capacity
- Good speed
- SCSI only

- Low cost
- High capacity
- Fast streaming operations

- High performance
- High capacity
- Industrial strength
- Fast streaming and start/stop operations
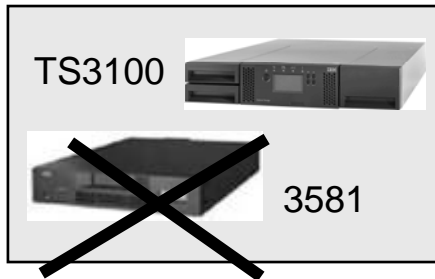
LTO Ultrium Tape Family

The LTO4 Drives can be placed in the current LTO tape family devices

- TS2340
- TS3100
- TS3200
- TS3310
- TS3500

LTO4 new in 2007

TS2340

3580

TS3200

3582

TS3500 / 3584

TS2340 does NOT support encryption on System i

TS3100

3581

TS3310

3583

Encryption is supported for FIBRE LTO4 drives in the TS3100 and up

	3580	TS2340	3581	TS3100	3582	TS3200	3583	TS3310	3584	TS3500
Machine Name	3580		3573-L2U		3573-L4U		3576		3584	
Max # drives	1	1	1	1	2	2	6	18	192	
Max # Cartridges	1	1	7 or 8 (*)	22+1	24	44+3	72	396	>6200	
Partition Capable	No	No	No	No	Yes	Yes	Yes	Yes	Yes	
LVD Drives	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
SAS Drives (not i)	No	Yes	No	Yes	No	Yes	No	Yes	No	No
Fibre Drives	No	No	2 Gbit	4 Gbit	2 Gbit	4 Gbit	2 Gbit	4 Gbit	2 Gbit	4Gbit

Enterprise Tape Family

Encryption is supported for TS1120 drives in the TS3400 and TS3500 (and 3494), but not standalone drives
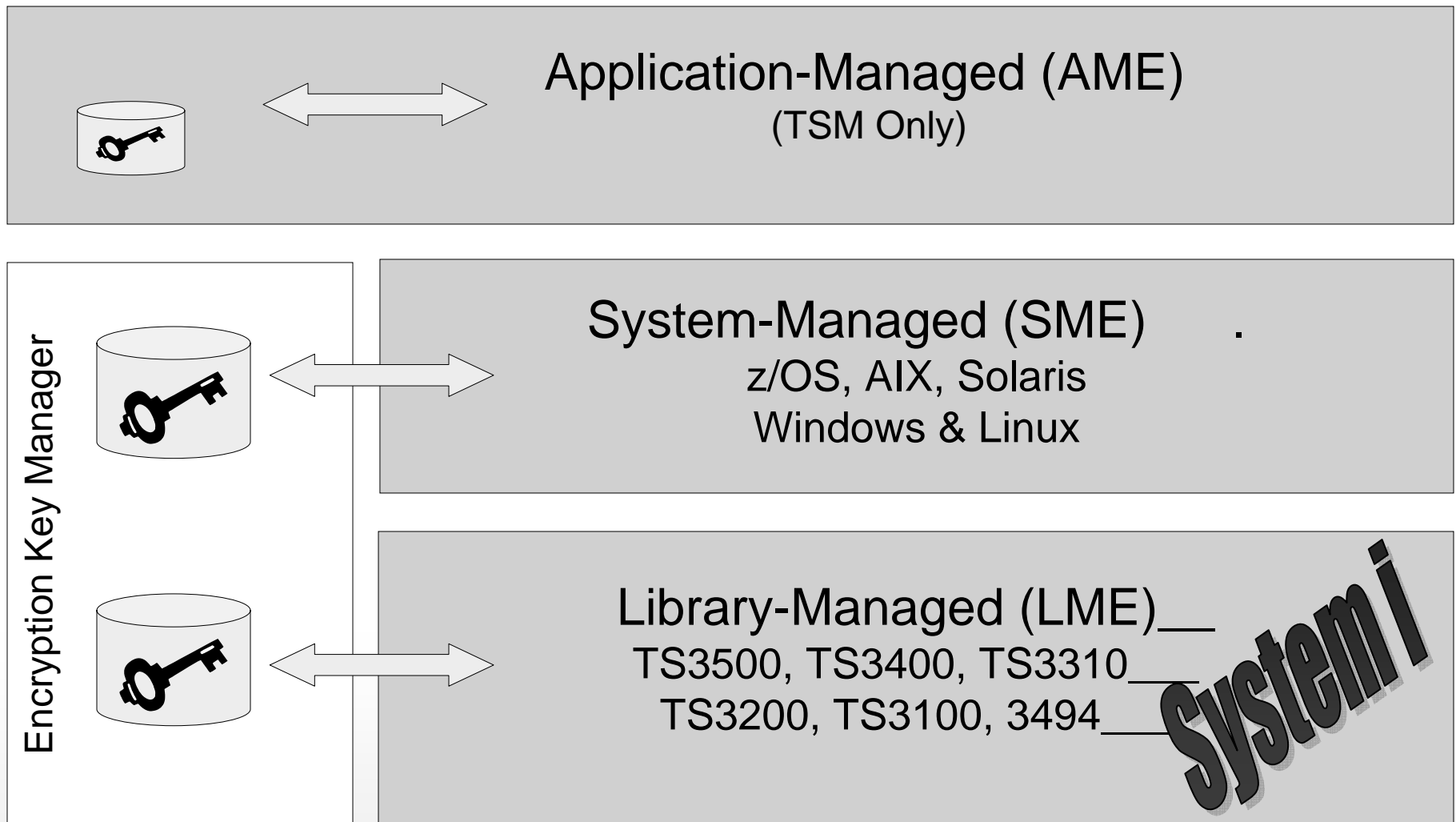
NEW in 2007

TS3500

TS1120 Standalone Drive

TS3400

	TS1120 Standalone	TS3400	TS3500
Machine Name	**3592-E05**	**3577-L5U**	**3584**
Max # drives	1	2	192
Max # Cartridges	1	18	>6200
Partition Capable	No	Yes	Yes
LVD Drives	No	No	No (for TS1120)
Fibre Drives	4 Gbit	4 Gbit	4 Gbit (for TS1120)
Library Managed Encryption Capable	No	Yes	Yes

Overview of Encryption Solution on IBM Tape Drives

Encryption Methods

Application-Managed (AME)
(TSM Only)

Encryption Key Manager

System-Managed (SME)   .
z/OS, AIX, Solaris
Windows & Linux

Library-Managed (LME)__
TS3500, TS3400, TS3310___
TS3200, TS3100, 3494___

System i

System i Tape Encryption on IBM Tape Drives

Encryption Key Manager
(EKM) Server

System i

Encryption Key Manager
(EKM) Server

LTO4 or TS1120 Drives
in a Tape Library
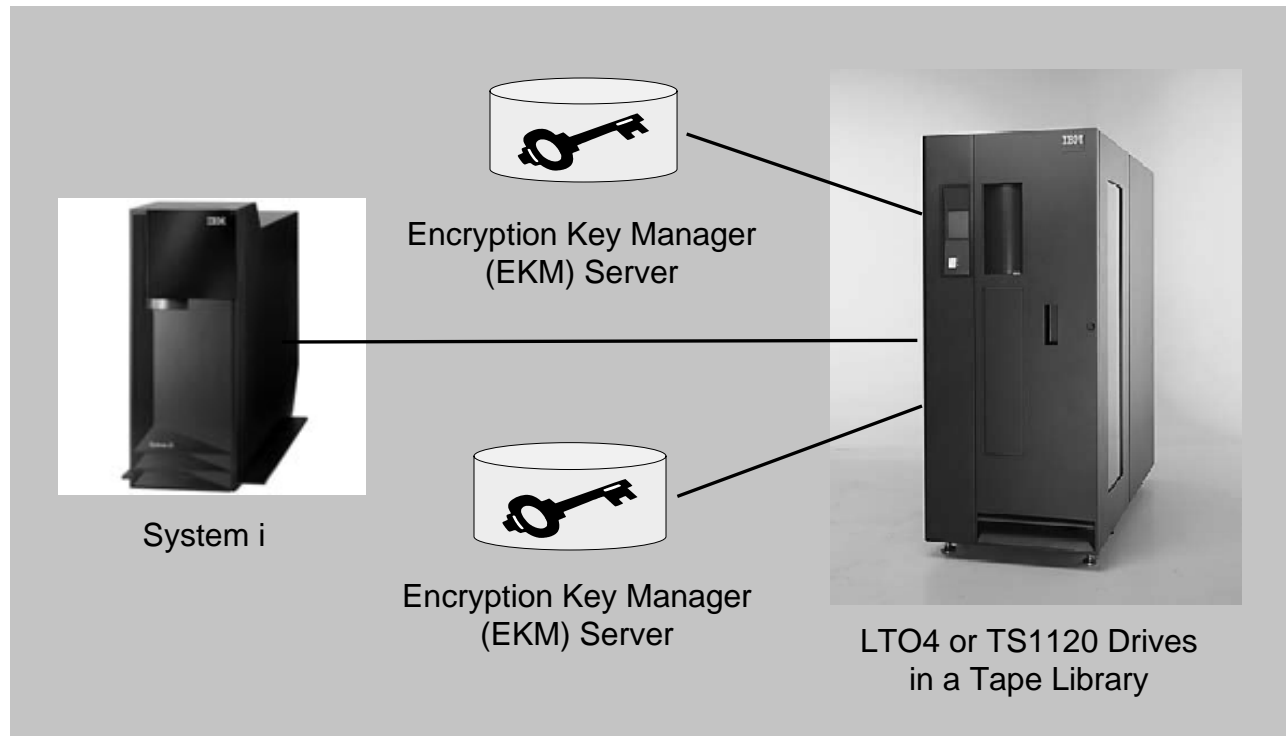
How does it work?

- System i sends the backup to the tape library

- If the drive has encryption turned on, then the library gets the keys from the EKM

- The drive/library writes the save

- BRMS is recommended to keep encrypted/non-encrypted tapes separate

Components
- Encryption capable tape drive(s) – fibre LTO4 or TS1120
- A tape library – TS3100/3200/3310, TS3400, TS3500, 3494
- Multiple Encryption Key Managers (EKMs)
- Suitable drive/library/EKM at recovery/DR/HA site to restore

The Encryption Key Manager (EKM)
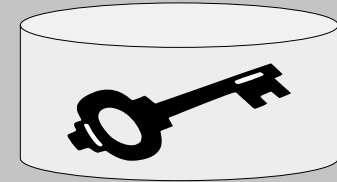
The Encryption Key Manager (EKM) – Details

EKM runs in Java on the following platforms:

IBM operating Systems
- i5/OS V5R3 and above
- AIX V5R2 and above
- System z operating systems

Non-IBM operating Systems
- Windows
- Linux
- HP
- Sun

How to get the latest copy of the EKM code:
- Download from http://www-1.ibm.com/support/docview.wss?&uid=ssg1S4000504

How to get the IBM Java Runtime Environment (IBM JRE)
- For i5/OS: get the no-charge "IBM Developer Kit for Java" (5722-JV1)
- For other platforms – follow the links by platform from the EKM web site above to get either a code download, or to order the no-charge "IBM TotalStorage Productivity Center – Limited Edition" CD
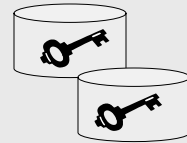
Installation Instructions
- Get the EKM "Introduction, Planning and User's Guide" (GA76-0418) from the EKM web site above

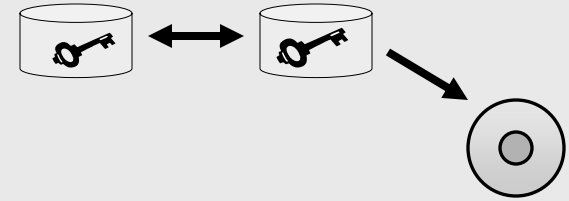# The Encryption Key Manager (EKM) – IMPORTANT

Primary Site

TEST YOUR RECOVERY CAREFULLY!

Run Multiple EKMs
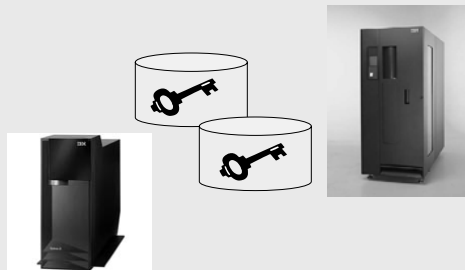
(so backups can still run when one is down)

Export-Synch / Save Keys

- Export-Synch keys on all EKMs each time keys change
- Keep offsite backup of EKM

Disaster Recovery Site

Comparable DR Site Gear

- Encryption Capable Drive / Library
- Access to EKMs

Don't Encrypt EKM

- Run EKM on a system/LPAR where none of the saves will be encrypted

BRMS and Tape Encryption

BRMS and Tape Encryption

BRMS is recommended for tape libraries and for tape encryption

Media Class for Regular Tapes
(for TS1120, use Density FMT3592A2)

| Vol 1 | Vol 2 | Vol 3 |

Media Class for Encrypted Tapes
(for TS1120 use density FMT3592A2E)

| Vol 4 | Vol 5 | Vol 6 |

Scratch Encryption Policy

Regular Volumes
Vol1 to Vol 3

Encrypted Volumes
Vol4 to Vol 6

BRMS and Tape Encryption

- In TS3500 and 3494, user needs to keep encrypted / non-encrypted media inventories in synch between BRMS and Tape Library records

- BRMS PTFs for "Encryption Awareness" on TS1120 drives will help

    SI24932 - V5R2M0
    SI24933 - V5R3M0
    SI24934 - V5R4M0

    These PTFs provide
    a new Media Density for TS1120
    "FMT3592A2E"
    (the final E stands for "Encrypted"!)

- LTO4 does not have a special density for encrypted tapes

Encryption - How to get Started

Encryption – Getting Started

Careful Planning is required

- **Encryption strategy**

  - What data will / won't be encrypted?

  - Which encryption techniques should be used?

  - Which vendor should be selected?

  - What other companies need to exchange data with us?

- **Key management strategy**

  - Which platform should run the EKM? Where should it be located?

  - What keys are required and how often will they change?

  - What is the HA and DR strategy for the keys?

  - Should you use enterprise-wide keys, or segment by platform or ??

IBM has service offerings to help you get started as quickly and smoothly as possible

References – Encrypting Data in your Database/Application

- **i5/OS Information Center**
  - http://publib.boulder.ibm.com/infocenter/iseries/v5r4/index.jsp
- **i5/OS Cryptographic Services APIs**
  - http://publib.boulder.ibm.com/infocenter/iseries/v5r4/topic/apis/catcrypt.htm
- **Java Cryptography Extension (JCE)**
  - http://publib.boulder.ibm.com/infocenter/iseries/v5r4/topic/rzaha/rzahajce.htm
- **System i cryptographic hardware: 4764/4758 Cryptographic Coprocessors**
  - http://publib.boulder.ibm.com/infocenter/iseries/v5r4/topic/rzajc/rzajcco4758.htm
- **DB2 Column Encryption – Scalar Functions**
  - http://publib.boulder.ibm.com/infocenter/iseries/v5r4/topic/db2/rbafzmstscale.htm
- **i5/OS Secure Sockets Layer (SSL)**
  - http://publib.boulder.ibm.com/infocenter/iseries/v5r4/topic/rzain/rzainoverview.htm
- **i5/OS Digital Certificate Manager (DCM)**
  - http://publib.boulder.ibm.com/infocenter/iseries/v5r4/topic/rzahu/rzahurazhudigitalcertmngmnt.htm
- **i5/OS Virtual Private Networking (VPN)**
  - http://publib.boulder.ibm.com/infocenter/iseries/v5r4/topic/rzaja/rzajagetstart.htm
- **System i Performance Capabilities Reference contains crypto performance information**
  - http://publib.boulder.ibm.com/infocenter/iseries/v5r4/topic/books/sc410607.pdf

References – Tape Drive Encryption

- **TS1120/TS3500 Tape Encryption on System i** – Whitepaper
  - http://www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/TD103557

- **IBM Encryption Key Manager Code and User's Guide**
  - http://www-1.ibm.com/support/docview.wss?&uid=ssg1S4000504

- **IBM System Storage TS1120 Tape Encryption: Planning, Implementation and Usage Guide** - Redbook
  - http://www.redbooks.ibm.com/redbooks/pdfs/sg247320.pdf

** This Redbook is currently being updated to include LTO4 encryption. Once done, the new title will be "IBM System Storage Tape Encryption Solutions"

Special Notices

This document was developed for IBM offerings in the United States as of the date of publication. IBM may not make these offerings available in other countries, and the information is subject to change without notice. Consult your local IBM business contact for information on the IBM offerings available in your area.

Information in this document concerning non-IBM products was obtained from the suppliers of these products or other public sources. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. Send license inquires, in writing, to IBM Director of Licensing, IBM Corporation, New Castle Drive, Armonk, NY 10504-1785 USA.

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

The information contained in this document has not been submitted to any formal IBM test and is provided "AS IS" with no warranties or guarantees either expressed or implied.

All examples cited or described in this document are presented as illustrations of the manner in which some IBM products can be used and the results that may be achieved. Actual environmental costs and performance characteristics will vary depending on individual client configurations and conditions.

IBM Global Financing offerings are provided through IBM Credit Corporation in the United States and other IBM subsidiaries and divisions worldwide to qualified commercial and government clients. Rates are based on a client's credit rating, financing terms, offering type, equipment type and options, and may vary by country. Other restrictions may apply. Rates and offerings are subject to change, extension or withdrawal without notice.

IBM is not responsible for printing errors in this document that result in pricing or information inaccuracies.

All prices shown are IBM's United States suggested list prices and are subject to change without notice; reseller prices may vary.

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

Any performance data contained in this document was determined in a controlled environment. Actual results may vary significantly and are dependent on many factors including system hardware configuration and software design and configuration. Some measurements quoted in this document may have been made on development-level systems. There is no guarantee these measurements will be the same on generally-available systems. Some measurements quoted in this document may have been estimated through extrapolation. Users of this document should verify the applicable data for their specific environment.

Revised September 26, 2006

Special Notices (Cont.)

The following terms are registered trademarks of International Business Machines Corporation in the United States and/or other countries: AIX, AIX/L, AIX/L (logo), AIX 6 (logo), alphaWorks, AS/400, BladeCenter, Blue Gene, Blue Lightning, C Set++, CICS, CICS/6000, ClusterProven, CT/2, DataHub, DataJoiner, DB2, DEEP BLUE, developerWorks, DirectTalk, Domino, DYNIX, DYNIX/ptx, e business (logo), e(logo)business, e(logo)server, Enterprise Storage Server, ESCON, FlashCopy, GDDM, i5/OS, i5/OS (logo), IBM, IBM (logo), ibm.com, IBM Business Partner (logo), Informix, IntelliStation, IQ-Link, LANStreamer, LoadLeveler, Lotus, Lotus Notes, Lotusphere, Magstar, MediaStreamer, Micro Channel, MQSeries, Net.Data, Netfinity, NetView, Network Station, Notes, NUMA-Q, OpenPower, Operating System/2, Operating System/400, OS/2, OS/390, OS/400, Parallel Sysplex, PartnerLink, PartnerWorld, Passport Advantage, POWERparallel, Power PC 603, Power PC 604, PowerPC, PowerPC (logo), Predictive Failure Analysis, pSeries, PTX, ptx/ADMIN, Quick Place, Rational, RETAIN, RISC System/6000, RS/6000, RT Personal Computer, S/390, Sametime, Scalable POWERparallel Systems, SecureWay, Sequent, ServerProven, SpaceBall, System/390, The Engines of e-business, THINK, Tivoli, Tivoli (logo), Tivoli Management Environment, Tivoli Ready (logo), TME, TotalStorage, TURBOWAYS, VisualAge, WebSphere, xSeries, z/OS, zSeries.

The following terms are trademarks of International Business Machines Corporation in the United States and/or other countries: Advanced Micro-Partitioning, AIX 5L, AIX PVMe, AS/400e, Calibrated Vectored Cooling, Chiphopper, Chipkill, Cloudscape, DataPower, DB2 OLAP Server, DB2 Universal Database, DFDSM, DFSORT, DS4000, DS6000, DS8000, e-business (logo), e-business on demand, EnergyScale, Enterprise Workload Manager, eServer, Express Middleware, Express Portfolio, Express Servers, Express Servers and Storage, General Purpose File System, GigaProcessor, GPFS, HACMP, HACMP/6000, IBM Systems Director Active Energy Manager, IBM TotalStorage Proven, IBMLink, IMS, Intelligent Miner, iSeries, Micro-Partitioning, NUMACenter, On Demand Business logo, POWER, PowerExecutive, PowerVM, PowerVM (logo), Power Architecture, Power Everywhere, Power Family, POWER Hypervisor, Power PC, Power Systems, Power Systems (logo), Power Systems Software, Power Systems Software (logo), PowerPC Architecture, PowerPC 603, PowerPC 603e, PowerPC 604, PowerPC 750, POWER2, POWER2 Architecture, POWER3, POWER4, POWER4+, POWER5, POWER5+, POWER6, POWER6+, pure XML, Quickr, Redbooks, Sequent (logo), SequentLINK, Server Advantage, ServeRAID, Service Director, SmoothStart, SP, System i, System i5, System p, System p5, System Storage, System z, System z9, S/390 Parallel Enterprise Server, Tivoli Enterprise, TME 10, TotalStorage Proven, Ultramedia, VideoCharger, Virtualization Engine, Visualization Data Explorer, Workload Partitions Manager, X-Architecture, z/Architecture, z/9.

A full list of U.S. trademarks owned by IBM may be found at: http://www.ibm.com/legal/copytrade.shtml.

The Power Architecture and Power.org wordmarks and the Power and Power.org logos and related marks are trademarks and service marks licensed by Power.org.

UNIX is a registered trademark of The Open Group in the United States, other countries or both.

Linux is a trademark of Linus Torvalds in the United States, other countries or both.

Microsoft, Windows, Windows NT and the Windows logo are registered trademarks of Microsoft Corporation in the United States, other countries or both.

Intel, Itanium, Pentium are registered trademarks and Xeon is a trademark of Intel Corporation or its subsidiaries in the United States, other countries or both.

AMD Opteron is a trademark of Advanced Micro Devices, Inc.

Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries or both.

TPC-C and TPC-H are trademarks of the Transaction Performance Processing Council (TPPC).

SPECint, SPECfp, SPECjbb, SPECweb, SPECjAppServer, SPEC OMP, SPECviewperf, SPECapc, SPEChpc, SPECjvm, SPECmail, SPECimap and SPECsfs are trademarks of the Standard Performance Evaluation Corp (SPEC).

NetBench is a registered trademark of Ziff Davis Media in the United States, other countries or both.

AltiVec is a trademark of Freescale Semiconductor, Inc.

Cell Broadband Engine is a trademark of Sony Computer Entertainment Inc.

InfiniBand, InfiniBand Trade Association and the InfiniBand design marks are trademarks and/or service marks of the InfiniBand Trade Association.

Other company, product and service names may be trademarks or service marks of others. Revised January 15, 2008