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

Sue Baker
IBM Advanced Technical Support
Rochester, MN
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

- 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

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

Customer Data EXPOSED!!

Direct Costs

<table>
<thead>
<tr>
<th>Cost Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fines and penalties</td>
<td></td>
</tr>
<tr>
<td>Customer notification</td>
<td>letters, postage, hotline, credit checks</td>
</tr>
<tr>
<td>Public Relations costs</td>
<td></td>
</tr>
<tr>
<td>Legal Actions</td>
<td></td>
</tr>
</tbody>
</table>

Indirect Costs

<table>
<thead>
<tr>
<th>Cost Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss of reputation</td>
<td></td>
</tr>
<tr>
<td>Loss of customer goodwill</td>
<td></td>
</tr>
<tr>
<td>Government investigations</td>
<td></td>
</tr>
</tbody>
</table>
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

Encrypt using IBM or 3rd party middleware for selected objects

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

Encrypt using 3rd party appliance between server and tape drive

Encrypt using a tape drive with built-in tape encryption
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!
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
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
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

A screen shows a table titled "Manage Master Keys". The table lists various master keys with their statuses and current key verification values.

<table>
<thead>
<tr>
<th>Master Key</th>
<th>Status</th>
<th>Current Key Verification Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Set</td>
<td>ED0CF6D746C7B560CAFF22FF7F82EFC1D1CEE19</td>
</tr>
<tr>
<td>2</td>
<td>Set</td>
<td>D1922FE0A0F03FFCBA16631C8D490644E4ADC0E7</td>
</tr>
<tr>
<td>3</td>
<td>Set</td>
<td>1B2B8913098DEB8EC4DDBDAEDB8B9E38CCF70737</td>
</tr>
<tr>
<td>4</td>
<td>Not set</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Not set</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Set</td>
<td>1B2B8913098DEB8EC4DDBDAEDB8B9E38CCF70737</td>
</tr>
<tr>
<td>7</td>
<td>Not set</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Not set</td>
<td></td>
</tr>
<tr>
<td>SAVRST</td>
<td>Default</td>
<td></td>
</tr>
<tr>
<td>ASP</td>
<td>Not set</td>
<td></td>
</tr>
</tbody>
</table>

Set of master key 2 was successful.
Keystore Management – V6R1

Keystores contain keys used to encrypt data or other keys. These keys are encrypted by a master key. By selecting a key store record it contains, create a new key record, translate the keystore from one master key to another, or delete a key store. Selecting properties will display information about the keystore file and whether translation or recovery is necessary.
Keystore Management – V6R1

<table>
<thead>
<tr>
<th>Key Record Label</th>
<th>Type</th>
<th>Key Size</th>
<th>Translation Status</th>
<th>Date Translated</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES KEY 1</td>
<td>AES</td>
<td>16</td>
<td>Current</td>
<td>January 11, 2008 1:35:07 PM CST</td>
</tr>
<tr>
<td>Triple DES key</td>
<td>Triple DES</td>
<td>16</td>
<td>Current</td>
<td>January 11, 2008 1:35:33 PM CST</td>
</tr>
<tr>
<td>My Private key</td>
<td>RSA private</td>
<td>1024</td>
<td>Current</td>
<td>January 11, 2008 1:36:05 PM CST</td>
</tr>
<tr>
<td>Another AES key</td>
<td>AES</td>
<td>16</td>
<td>Current</td>
<td>January 11, 2008 1:36:44 PM CST</td>
</tr>
</tbody>
</table>
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
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
Encrypting Data in your Database/Application

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
Protecting i5/OS Data with Encryption Whitepaper

Great whitepaper that came out last year

Protecting i5/OS Data with Encryption Redbook

New Redbook currently in a draft version

Encrypting Data using Middleware
Non-IBM Middleware for Encryption

**Encrypt then save/transmit**

- File A
- File A'
- Keys

**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
- Key

**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

Tape Management Systems

Encryption Tools

** 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**

  - **Linoma Software**

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

  - **PKWARE, Inc**

  - **NuBridges**

** 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
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

**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

ASP2

ASP3

Data

Data

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, Inc

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

**LTO Family**
- New in 2007
- Low cost
- High capacity
- Fast streaming operations

**Enterprise Family**
- High performance
- High capacity
- Industrial strength
- Fast streaming and start/stop operations

NEW in 2007

- TS3310
- TS3200
- TS2340
- TS3100
- TS1120
- TS3400

NEW in 2007
The LTO4 Drives can be placed in the current LTO tape family devices:

- TS2340
- TS3100
- TS3200
- TS3310
- TS3500
- TS3500 / 3584

LTO4 new in 2007

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

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

- TS2340
- TS3100
- TS3200
- TS3310
- TS3500

TS2340 does NOT support encryption on System i.

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

### Table: LTO Ultrium Tape Family Specifications

<table>
<thead>
<tr>
<th>Machine Name</th>
<th>3580</th>
<th>TS2340</th>
<th>3581</th>
<th>TS3100</th>
<th>3582</th>
<th>TS200</th>
<th>3583</th>
<th>TS3310</th>
<th>3584</th>
<th>TS3500</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max # drives</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>6</td>
<td>18</td>
<td>192</td>
<td></td>
</tr>
<tr>
<td>Max # Cartridges</td>
<td>1</td>
<td>1</td>
<td>7 or 8 (*)</td>
<td>22+1</td>
<td>24</td>
<td>44+3</td>
<td>72</td>
<td>396</td>
<td>&gt;6200</td>
<td></td>
</tr>
<tr>
<td>Partition Capable</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>LVD Drives</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>SAS Drives (not i)</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Fibre Drives</td>
<td>No</td>
<td>No</td>
<td>2 Gbit</td>
<td>4 Gbit</td>
<td>2 Gbit</td>
<td>4 Gbit</td>
<td>2 Gbit</td>
<td>4 Gbit</td>
<td>2 Gbit</td>
<td>4 Gbit</td>
</tr>
</tbody>
</table>

TS2340 does NOT support encryption on System i.

Encryption is supported for FIBRE LTO4 drives in the TS3100 and up.
Enterprise Tape Family

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

<table>
<thead>
<tr>
<th>Machine Name</th>
<th>TS1120 Standalone</th>
<th>TS3400</th>
<th>TS3500</th>
</tr>
</thead>
<tbody>
<tr>
<td>Machine Name</td>
<td>3592-E05</td>
<td>3577-L5U</td>
<td>3584</td>
</tr>
<tr>
<td>Max # drives</td>
<td>1</td>
<td>2</td>
<td>192</td>
</tr>
<tr>
<td>Max # Cartridges</td>
<td>1</td>
<td>18</td>
<td>&gt;6200</td>
</tr>
<tr>
<td>Partition Capable</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>LVD Drives</td>
<td>No</td>
<td>No</td>
<td>No (for TS1120)</td>
</tr>
<tr>
<td>Fibre Drives</td>
<td>4 Gbit</td>
<td>4 Gbit</td>
<td>4 Gbit (for TS1120)</td>
</tr>
<tr>
<td>Library Managed Encryption Capable</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Overview of Encryption Solution on IBM Tape Drives
Encryption Methods

Application-Managed (AME)
(TSM Only)

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

Library-Managed (LME)
TS3500, TS3400, TS3310
TS3200, TS3100, 3494

Encryption Key Manager
System i Tape Encryption on IBM Tape Drives

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

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

**EKM runs in Java on the following platforms:**

<table>
<thead>
<tr>
<th>IBM operating Systems</th>
<th>Non-IBM operating Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>• i5/OS V5R3 and above</td>
<td>• Windows</td>
</tr>
<tr>
<td>• AIX V5R2 and above</td>
<td>• Linux</td>
</tr>
<tr>
<td>• System z operating systems</td>
<td>• HP</td>
</tr>
<tr>
<td></td>
<td>• Sun</td>
</tr>
</tbody>
</table>

**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!

Disaster Recovery Site

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

Comparable DR Site Gear
• Encryption Capable Drive / Library
• Access to EKMs

Export-Synch / Save Keys
• Export-Synch keys on all EKMs each time keys change
• Keep offsite backup of 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

- 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

---

**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**
Vol 1 to Vol 3

**Encrypted Volumes**
Vol 4 to Vol 6
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**

- **i5/OS Cryptographic Services APIs**

- **Java Cryptography Extension (JCE)**

- **System i cryptographic hardware: 4764/4758 Cryptographic Coprocessors**

- **DB2 Column Encryption – Scalar Functions**

- **i5/OS Secure Sockets Layer (SSL)**

- **i5/OS Digital Certificate Manager (DCM)**

- **i5/OS Virtual Private Networking (VPN)**

- **System i Performance Capabilities Reference contains crypto performance information**
References – Tape Drive Encryption

- **TS1120/TS3500 Tape Encryption on System i** – Whitepaper

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


** 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 inquiries, 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/pxt, 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, 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.


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, SPECcpu, SPECjbb, SPECweb, SPECjAppServer, SPEC OMP, SPECviewperf, SPECapc, SPECjpc, SPECjvm, SPECmail, SPECmap 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