IBM System z9 Business Resiliency and Security
Frequently Asked Questions

Worldwide
# Table of Contents

- IBM System z9 109 Overview .................................................. 3
- Availability Enhancements ...................................................... 5
- Cryptographic Enhancements ................................................... 6
- Data Encryption ................................................................. 14
- GDPS Enhancements ............................................................. 24
- Business Resiliency and Security-Related Statements of Direction ............ 25
- z/OS V1R7 Security and Resiliency Enhancements ................................ 27
- z/VM V5R2 Security Enhancements .......................................... 29
IBM System z9 109 Overview

Question:
What is the new IBM System z9 product that was announced on July 26, 2005?

Answer:
The announcement on July 26, 2005, of the IBM System z9™ 109 (z9-109) brings significant technology advances that deliver on the strategy announced in October 2004, while also strengthening the mainframe’s leadership in enterprise computing. These leadership capabilities in areas such as security and resiliency, intelligent workload management, integration and virtualization make the z9-109 an ideal platform for supporting central corporate databases and mission-critical enterprise-wide applications.

The z9-109 is built using the modular, multi-book design introduced with the IBM zSeries® 990 (z990) and delivers enhancements in the area of performance, scalability, availability, security and virtualization. The z9-109 is focused on providing higher availability and reducing planned and unplanned outages—which may be accomplished with improved nondisruptive replace, repair and upgrade functions for memory, books and I/O as well as extending nondisruptive capability to download Licensed Internal Code upgrades. New integrated clear key encryption security-rich features on the z9-109 include support for Advanced Encryption Standard, Secure Hash Algorithm-256 and an integrated Pseudo Random Number Generator. Performing these functions in hardware is designed to contribute to improved performance.

* This is a comparison of the z9-109 54-way and the z990 D32 and is based on the LSPR mixed workload average.

The new z9-109 is designed to support the following security related enhancements:

- CPACF enhancements
  - Advanced Encryption Standard (AES)
  - Pseudo Random Number Generator (PRNG)
  - Secure Hashing Algorithm (SHA-256)
- Configurable Crypto Express2

Question:
Who would be interested in the z9-109?

Answer:
The z9-109 is intended to provide customers with the latest mainframe technology to manage their businesses. Enterprises that need the most advanced mainframe availability enhancements, as well as those that require high levels of security for their business, will find the enhancements offered on the z9-109 to be exciting. While zSeries, working in close symmetry with our operating system software, has long excelled at reducing unplanned outages that may disrupt applications, the z9-109 offers new availability technology that can help provide a reduction in planned outages. With proper planning, a multi-book system may be able to avoid outages to applications when features such as memory or a book are upgraded, repaired or replaced. New on IBM System z9 is the ability to configure Crypto Express2 PCI-X adapters as accelerators.
When both PCI-X adapters are configured as accelerators, the Crypto Express2 feature can perform up to 6000 SSL handshakes per second. This represents, approximately, a 3X performance improvement compared to the PCICA feature or the current Crypto Express2 feature on z990, on a per card basis. The SSL rate was achieved with a System z9 with four processors and two Crypto Express2 cards (one feature, both configured as accelerators), 1 z/OS® V1R7 (1.7) with Cryptographic Support for z/OS 1.6/1.7 Web deliverable, and ICSF FMID HCR7730. Since the performance enhancements are implemented in Licensed Internal Code, current Crypto Express2 features carried forward from z990 to System z9 platform can take advantage of increased SSL performance and the new configuration capability. These measurements are examples of the maximum transactions per second achieved in a laboratory environment with no other processing occurring and do not represent actual field measurements. Details are available upon request.

1 Note, the previously reported SSL performance of 4995 handshakes per second was obtained on a 4-way z990 with four Crypto Express2 Coprocessors (CEX2C) features, whereas in this case the performance was measured on a 4-way z9-109 with one Crypto Express2 feature with both configured as accelerators. It would be expected that the SSL performance on a 16-way z9-109 with six Crypto Express2 features would be greater than that obtained on a z990, however, actual measurements have not been taken. Also the integration of new functions in the hardware (such as AES, SHA-256 and PRNG) may also contribute to improved TCO.

Customers needing maximum capacity and I/O constraint relief will find the new capacity and innovative technology of the z9-109 may fit their business needs. The performance of the z9-109 is expected to be 1.35 times the z990 unit (LSPR workload average). Similar capacity improvement may be seen on all PUs; general purpose as well as all specialty engines. Multiple subchannel sets and an increase in subchannel volumes can allow for more logical volumes allowing for access to more data.

Enterprises that are running early zSeries technology (the z900) or S/390® technology (G5/G6) should consider the z9-109 for replacing or consolidating their infrastructures. Improved capacity Integrated Facility for Linux® (IFL) can allow expansion of current new workload applications in a cost effective manner. With the z9-109, customers may see price/performance improvements in hardware maintenance, memory prices and software pricing. Also, as enterprises look for disaster recovery solutions, the z9-109 can provide reserved emergency backup capacity using the Capacity Backup (CBU) feature. This feature gives extra capacity to your data center in emergency situations where you have lost capacity in another part of the establishment and need to recover capacity on a designated z9-109. Enhancements on the z9-109 allow CBU on Central Processors (CPs) as well as IFLs, Internal Coupling Facility (ICFs), and System z9 or zSeries Application Assist Processors (zAAPs).

**Question:**
Where can I review more comprehensive FAQs for System z9?

**Answer:**
You will find a complete set of System z9 product FAQs at: [ibm.com/servers/eserver/zseries/faq/](http://ibm.com/servers/eserver/zseries/faq/)
Enhanced driver maintenance, exclusive to the z9-109, is another step IBM is taking to help reduce the duration of a planned outage.

**Question:**
What is the advantage of enhanced driver maintenance on the z9-109?

**Answer:**
Some of the greatest contributors to downtime during planned outages are Licensed Internal Code (LIC) updates performed in support of new features and functions. When properly configured, the z9-109 is designed to support activating select new LIC levels concurrently. Concurrent activation of the select new LIC level is only supported at specific sync points. Sync points may exist throughout the life of the current LIC level. Once a sync point has passed, you will be required to wait until the next sync point supporting concurrent activation of a new LIC level. Certain LIC updates will not be supported by this function.

Enhanced driver maintenance, exclusive to the z9-109, is another step IBM is taking to help reduce the duration of a planned outage.

**Question:**
What is the advantage of dynamic oscillator switchover?

**Answer:**
The z9-109 has two oscillator cards, a primary and a backup. In the event of a failure of the primary oscillator card, the backup is designed to detect the failure, switch over, and provide the clock signal to the server transparently. Previously, in the event of a failure of the active oscillator, a server outage would occur, the subsequent Power On Reset would select the backup, and the server would resume operation. Dynamic oscillator switchover is exclusive to the z9-109.
Cryptographic Enhancements

Question:
What cryptographic hardware is supported on the z9-109?

Answer:
CP Assist for Cryptographic Function (CPACF) on every CP and IFL and the Crypto Express2 feature.

Question:
What cryptographic hardware is not supported on the z9-109?

Answer:
PCI Cryptographic Coprocessor (PCICC), PCI X Cryptographic Coprocessor (PCIXCC), CMOS Cryptographic Coprocessor Facility (CCF) and the PCI Cryptographic Accelerator (PCICA) features are not supported on the z9-109.

Question:
Will the cryptographic hardware be offered as standard features on the z9-109?

Answer:
The CP Assist for Cryptographic Function (CPACF) is standard on every CP and IFL, however, a no-charge enablement feature #3863 is required. The Crypto Express2 feature is an optional feature. The first order increment is two features.

Question:
What is new about Crypto Express2?

Answer:
Crypto Express2 is now configurable: The Crypto Express2 feature has two PCI-X adapters, and each can be defined as a either Coprocessor or as an Accelerator

- The Crypto Express2 Coprocessor (default)
  - Supports:
    - Secure key encrypted transactions
    - Clear key RSA acceleration
    - Supports highly secure cryptographic functions, use of secure encrypted key values, and User Defined Extensions (UDX)
  - Designed for Federal Information Processing Standard (FIPS) 140-2 Level 4 certification.
- Crypto Express2 Accelerator – to enable significant improvement in SSL acceleration over z890 and z990 servers.
  - Supports clear key RSA acceleration
  - Offloads compute-intensive RSA public-key and private-key cryptographic operations employed in the SSL protocol.
• Since the configuration functions are implemented in Licensed Internal Code, current Crypto Express2 features can be carried forward from z990 to the z9-109 to take advantage of increased SSL performance and the new configuration capability.

• Up to eight Crypto Express2 features per server.

• All logical partitions (LPARs) in all Logical Channel Subsystems (LCSSs) have access to the Crypto Express2 feature, up to 32 LPARs per feature.

---

**Question:**
What is new about the P Assist for Cryptographic Function (CPACF) on the z9-109?

**Answer:**
CPACF has been enhanced to include support of the Advanced Encryption Standard (AES) for 128-bit keys, Secure Hash Algorithm-256 (SHA-256), and Pseudo Random Number Generation (PRNG). PRNG is a standard function supported on the Crypto Express2 feature.

CPACF, supporting clear key encryption, is activated using a no charge enablement feature #3863 and offers the following on every Processor Unit (PU) identified as a Central Processor (CP) or Integrated Facility for Linux (IFL).

• Data Encryption Standard (DES)
• Triple Data Encryption Standard (TDES)
• Advanced Encryption Standard (AES) (new)
• SHA-1
• SHA-256 (new)
• Pseudo Random Number Generation (PRNG) (new)

Performance is designed to scale with the addition of PUs. SHA-1 and SHA-256 are shipped enabled on all servers and do not require the enablement feature. DES, TDES and AES functions require enablement of the CPACF function (Feature Code 3863) for export control. CPACF cryptographic functions are aimed at encryption, decryption and hashing of data transferred over open networks and data sent to storage.

---

**Question:**
Will the Crypto Express2, feature code 0863, support Linux Secure Sockets Layer (SSL) and Transport Layer Security (TLS) cryptographic operations on the z9-109?

**Answer:**
Yes, it supports Public Key operations with Linux on System z9. IBM is working with its distribution partners to provide this function in future distribution releases, or service updates.

---

**Question:**
What are the functional differences between the Coprocessor and Accelerator configurations on Crypto Express2 features?

**Answer:**
New on System z9 is the ability to configure Crypto Express2 PCI-X adapters as accelerators. When both PCI-X adapters are configured as accelerators, the Crypto Express2 feature can perform up to 6000 SSL handshakes per second. This represents, approximately, a 3X performance improvement compared to the PCICA feature or the current Crypto Express2...
feature on z990, on a per card basis. The SSL rate was achieved with a System z9 with four processors and two Crypto Express2 cards (one feature, both configured as accelerators), 1 z/OS 1.7 with Cryptographic Support for z/OS 1.6/1.7 Web deliverable, and ICSF FMID HCR7730. Since the performance enhancements are implemented in Licensed Internal Code, current Crypto Express2 features carried forward from z990 to z9-109 can take advantage of increased SSL performance and the new configuration capability. These measurements are examples of the maximum transactions per second achieved in a laboratory environment with no other processing occurring and do not represent actual field measurements. Details are available upon request.

1 Note, the previously reported SSL performance of 4995 handshakes per second was obtained on a 4-way z990 with four Crypto Express2 Coprocessors (CEX2C) features, whereas in this case the performance was measured on a 4-way z9-109 with one Crypto Express2 feature with both configured as accelerators. It would be expected that the SSL performance on a 16-way z9-109 with six Crypto Express2 features would be greater than that obtained on a z990, however, actual measurements have not been taken.

Since the performance enhancements are implemented in Licensed Internal Code, current Crypto Express2 features carried forward from z990 to z9-109 may take advantage of increased SSL performance and the new configuration capability.

These measurements are examples of the maximum handshakes per second achieved in a laboratory environment with no other processing occurring and do not represent actual field measurements. Details are available upon request. Previously, the Crypto Express2 implementation was as a coprocessor. It was not optimized for SSL performance.

**Question:**
What Integrated Cryptographic Service Facility (ICSF) services are available with CP Assist for Cryptographic Function (CPACF)?

**Answer:**
All critical Integrated Cryptographic Service Facility (ICSF) services that currently execute on z890 and z990 PCIX Cryptographic Coprocessor (PCIXCC) feature are planned to be supported by the Crypto Express2 feature.

The following ICSF callable services will be available with CPACF.

CSNBSYE, CSNBSYE1, CSNBSYD, and CSNBSYD1 will provide support for clear-key AES encryption and decryption with 128-bit keys using the CPACF.

CSFNBOWH and CSNBOWH1 will provide support for SHA-1 and SHA-256 using the CPACF.

These services continue to support DES and TDES.
Question: What other means are available for customers to utilize CP Assist for Cryptographic Function (CPACF)?

Answer: For IBM and customer written programs, CPACF function for DES, TDES, AES, SHA-1 and SHA-256 functions can be invoked by five (5) instructions as described in the z/Architecture™ Principles of Operation, SA22-7832-02. As a group, these instructions are known as the Message Security Assist (MSA). These are all problem state instructions and are all in RRE format.

Question: What are the prerequisites for the installation of Cryptographic features on the z9-109?

Answer: DES, TDES, AES and PRNG functions require enablement of the CP Assist for Cryptographic Function, feature code 3863. This is also a prerequisite for the Crypto Express2 feature.

Question: What cryptographic functions are enabled when the z9-109 is shipped?

Answer: The z9-109 is shipped enabled with hash function SHA-1 and SHA-256 resident in each PU defined as a CP or IFL.

Question: Is a Trusted Key Entry (TKE) workstation required for the use of the CPACF?

Answer: No, the CP Assist for Cryptographic Function (CPACF) supports clear key functions and does not require entering of master keys.

Question: Will there be an update to the ATS TechDocs Web site to provide additional technical information about System z9 cryptographic hardware features?

Answer: ATS TechDocs Web site and several System z9 cryptographic technical papers will be updated as appropriate. The ATS TechDocs Web site URL is ibm.com/support/techdocs/atsmastr.nsf.
**Question:**
What are the functions and attributes of the CP Assist for Cryptographic Function (CPACF) and Crypto Express2 features?

**Answer:**
The following table highlights the features or attributes:

<table>
<thead>
<tr>
<th>Functions or attributes</th>
<th>CPACF</th>
<th>Crypto Express 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supports z/OS applications using ICSF</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Provides highest SSL handshake performance (in accelerator mode)</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Provides highest symmetric encryption performance (clear key)</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Provides highest symmetric encryption performance (secure key)</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Provides highest asymmetric (clear key) encryption performance (in accelerator mode)</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Provides highest asymmetric (encrypted key) encryption performance (in coprocessor mode)</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Uses CHPID numbers</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Physically imbedded on each Central Processor (CP)</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Requires CP Assist for Cryptographic Function (CPACF) enablement</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Requires ICSF to be active, for z/OS users</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Requires system master keys to be loaded (in coprocessor mode)</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Offers user programming function support (UDX) (in coprocessor mode)</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Usable for data privacy - encryption and decryption processing</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Usable for data integrity - hashing and message authentication</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Usable for financial processes and key management operations (in coprocessor mode)</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Crypto performance RMF monitoring</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>System (master) key storage (in coprocessor mode)</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Retained key storage (in coprocessor mode)</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Designed for tamper-resistant hardware packaging (in coprocessor mode)</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Designed for FIPS 140-2 level 4 certification (in coprocessor mode)</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Supports SSL functions</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Supports Linux applications performing SSL handshakes</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>RSA functions</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>High Performance SHA-1, SHA-256 Hash function</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Clear key DES/T-DES</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Clear key RSA</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
Question:
What releases of operating systems are required to support the Crypto Express2 hardware feature on the z9-109?

Answer:
The software support requirements for Crypto Express2 and CP Assist for Cryptographic Function (CPACF) features are as follows:

- **Crypto Express2:**
  - z/OS 1.6 and later with Cryptographic Support for z/OS 1.6 and 1.7 Web deliverable. Compatibility support is provided on z/OS 1.4 and 1.5. z990 and z890 enhancements to cryptographic support are Web deliverable.
  - z/VM® V5.1 for z/OS and Linux guests, with applicable PTFs.
  - Linux on System z9 – IBM is working with its distribution partners to provide this function in future distribution releases, or service updates.

- **CPACF (SHA-1, SHA-256, AES and PRNG):**
  - z/OS 1.6 and later with Cryptographic Support for z/OS 1.6 and 1.7 Web deliverable. Compatibility support is provided on z/OS 1.4 and 1.5. z990 and z890 enhancements to cryptographic support are Web deliverable.
  - z/VM 4.4 and later for guests.
  - z/VSE™ 2.7, and later, with applicable PTFs.
  - Linux on System z9 – IBM is working with its distribution partners to provide this function in future distribution releases, or service updates.

Question:
Will UDX's written for zSeries servers function on the z9-109?

Answer:
Pre-existing UDXs on current systems may need to be ported to the z9-109. Customers need to contact IBM to port existing UDXs to the new Crypto Express2 environment on the z9-109. For further information, see the answer to the next question.

Question:
Will new UDXs be supported on the z9-109?

Answer:
Yes. If you wish to inquire further about UDX support for Crypto Express2 feature, Please contact one of the following IBM representatives: Leo Moesgaard (Leo.Moesgaard@dk.IBM.com) or David Evans (Davee@us.IBM.com)
Question: Does the use of RSA Retained private keys limit availability?

Answer: Yes. The use of retained private keys creates an application single point of failure. Since RSA Retained private keys cannot be copied, backed up or scaled from a performance perspective, these keys should only be used if mandated by the customers' security policy. For those customers that require a private key that is intended to be shared across logical partitions, they should use RSA keys encrypted under a host master key instead of a retained key. The use of the RSA keys encrypted under a host master key will prevent the loss of the key associated with the RSA Retained private key specific to the Crypto Express2 feature.

Question: Will there be an upgrade to the Trusted Key Entry (TKE) workstation?

Answer: No upgrade will be available. However, with the introduction of the configurable Crypto Express2 feature and a new Graphical User Interface (GUI), there is a new TKE 5.0 workstation, feature code 0859. Customers must use the TKE 5.0 workstation to control the z9-109. Customers may continue to use TKE 3.x and 4.x workstations to control prior servers, but an existing workstation cannot be upgraded to TKE 5.0.

Question: Will customers have the option to order Trusted Key Entry (TKE) workstation with Token-Ring or Ethernet?

Answer: No, a TKE workstation with Token-Ring is not offered. Ethernet is the only option offered. This satisfies the Statement of General Direction in Hardware Announcement 104-115, dated April 7, 2004, Hardware Announcement 104-117, dated April 7, 2004, and Hardware Announcement 104-118, dated April 7, 2004.

Question: Will Smart card reader support be available with z9-109 TKE workstations?

Answer: Yes. Support is available for an optional Smart Card Reader to be attached to the new TKE 5.0 workstation. Customers may also carry forward optional Smart Card Reader features.

Question: Will the number of TKE workstations be limited to one per system?

Answer: Up to three (3) TKE 5.0 workstations per system will be supported on the z9-109. This means that up to three (3) smart card reader features, each feature consisting of two smart card readers, can be attached to the z9-109.
**Question:**
What are the migration requirements for customers with Crypto Express2 feature on z890 and z990 servers?

**Answer:**
The Crypto Express2 feature is supported on z890 and z990 servers and can be carried forward on an upgrade to the z9-109.

---

**Question:**
Can I perform an MES upgrade involving Crypto Express2 features on the z9-109 without an outage?

**Answer:**
The design of the Crypto Express2 feature allows for non-disruptive upgrades. Unfortunately, there are some environments where a disruptive upgrade will occur: for example; a z9-109 with insufficient I/O slots where an additional I/O cage is required.
Data Encryption

Question:
Why is IBM announcing the Encryption Facility for z/OS®?

Answer:
Businesses today are focused on the importance of securing customer and business data. Increasing regulatory requirements are driving the need for the security of data. Encryption is a powerful and widely used technology that helps protect data from loss and inadvertent or deliberate compromise. The IBM Encryption Facility for z/OS can help address these requirements.

Question:
What new functionality does the IBM Encryption Facility for z/OS, 1.1 (5655-P97) provide?

Answer:
The Encryption Facility for z/OS is designed to address the requirements of z/OS customers to encrypt files for archive or for transfer purposes. Encryption Facility for z/OS consists of two priced optional features:

- The Encryption Services feature supports encrypting and decrypting certain file formats on z/OS. This can allow you to transfer them to remote sites within your enterprise, transfer them to partners and vendors, and archive them. This feature supports hardware-accelerated compression before encryption.
- The DFSMSdss™ Encryption feature enables the encryption of DFSMSdss dump data sets. This feature supports hardware-accelerated compression before encryption to tape.

Question:
What benefits can the Encryption Services feature provide?

Answer:
The Encryption Services feature can allow you to encrypt data written to tape and other removable media. This can help you share sensitive information across platforms with partners, vendors, and customers. You can also use the Encryption Services feature to encrypt certain files for archival. This feature can use the z/OS key management and access authentication capabilities provided within the Integrated Cryptographic Services Facility (ICSF) and the hardware compression and the hardware cryptographic capabilities of IBM System z9™ and eServer™ zSeries® servers. The hardware cryptographic functions may require the configuration of one or more optional priced features on most IBM System z9 and zSeries processors.

Question:
What benefits can the DFSMSdss Encryption feature provide?

Answer:
The DFSMSdss Encryption feature can allow you to encrypt DFSMSdss dump data sets written to tape and DASD. This feature is designed to use the z/OS key management and access authentication capabilities provided within the Integrated Cryptographic Services Facility (ICSF)
and the hardware cryptographic and compression capabilities of System z9 and zSeries servers. The hardware cryptographic functions require the configuration of one or more optional priced features on most IBM System z9 and zSeries processors.

**Question:**
What do the Encryption Services and the DFSMSdss Encryption features have in common?

**Answer:**
Both features are designed to support hardware-accelerated compression before encryption. Both features are intended to use state-of-the-art encryption and centralized key management capabilities provided by functions of z/OS and features of IBM System z9 and zSeries servers to help secure data stored to tape and other removable media. And both features can leverage the centralized z/OS key management and access authentication capabilities provided within the Integrated Cryptographic Services Facility (ICSF) and the hardware cryptographic and hardware compression capabilities of System z9 and zSeries servers.

**Question:**
Can the Encryption Facility for z/OS be used to enhance the security of data shared with trusted business partners that don’t have z/OS or a mainframe?

**Answer:**
Yes. Non z/OS platform users can decrypt data by downloading a Java™ technology-based program, the IBM Encryption Facility for z/OS Client. This separately-licensed program can be used to decrypt the data encrypted by the Encryption Services feature running on z/OS. The Java technology-based client program can also be used to re-encrypt the sensitive data after it is used or referenced by the business partner. This can allow you to exchange encrypted data between z/OS systems and other operating systems.

**Question:**
When will the features of the Encryption Facility for z/OS be generally available?

**Answer:**
The IBM Encryption Services feature is planned to be available October 28, 2005. The IBM DFSMSdss Encryption feature is planned to be made available December 2, 2005.

**Question:**
What other Statements of Direction has IBM made recently in the area of encryption technology?

**Answer:**
IBM has announced the following Statements of Direction (SOD):

- IBM plans to provide an enhancement to the IBM System z9 109 Crypto Express2 feature in 2006 that will be designed to enable remote loading of initial keys for Automatic Teller Machines (ATMs), Point of Sale terminals, and other similar devices in which the distributed keys are protected using public-key cryptographic techniques. Remote loading of these keys may help provide a more secure and cost effective alternative to local loading of keys by couriers. This enhancement is planned to support public-key based distribution of initial cryptographic keys, which is intended to be similar to that which is expected to be defined in
the new ANSI X9.24-2 standard currently under development. In addition, the enhancement is planned to provide improved methods for exchanging Data Encryption Standard (DES) and Triple-DES keys with non-IBM cryptographic systems.

The following statement of direction was published in Hardware Announcement 105-241 (RFA41038), dated July 27, 2005:

- IBM TotalStorage® encryption: To address customers’ growing concern with data security, IBM is planning for the development, enhancement, and support of encryption capabilities within storage environments such that the capability does not require the use of host server resources (so called "outboard" encryption capabilities). This includes the intent to offer, among other things, capabilities for products within the IBM TotalStorage portfolio to support outboard encryption and to leverage the key management functions provided by the Integrated Cryptographic Services Facility (ICSF).

All statements regarding IBM's plans, directions, and intent are subject to change or withdrawal without notice.

**Question:**
What benefits do you expect mainframe customers and their business partners to achieve by installing and deploying the features of the Encryption Facility for z/OS?

**Answer:**
Helping to protect data from loss and inadvertent or deliberate compromise is a critical concern for businesses. To help address this issue, IBM Encryption Facility for z/OS extends the scope of IBM's mainframe encryption capabilities to removable media. Customers can leverage the robust centralized capabilities of z/OS Integrated Cryptographic Services Facility (ICSF) and, when installed, mainframe cryptographic hardware to generate, maintain, and store key data. In addition, z/OS Security Server (RACF®), or a comparable product, can provide highly secure access management and auditability for key management tasks. Together these elements create a powerful centralized encryption solution.

**Question:**
What books and materials will be available for the Encryption Facility for z/OS?

**Answer:**
A program directory and one copy of the following publications are supplied automatically with the basic machine-readable material:

<table>
<thead>
<tr>
<th>Title</th>
<th>Publication number</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM Encryption Facility for z/OS Program Directory</td>
<td>GI10-0771</td>
</tr>
<tr>
<td>IBM Encryption Facility for z/OS Licensed Program Specification</td>
<td>GA76-0405</td>
</tr>
</tbody>
</table>

The following publications are available in softcopy at

Refer to the IBM Publications Center Web site for more information about publication ordering.

http://www.ibm.com/shop/publications/order

**Question:**
Who will provide installation and technical support for the Encryption Facility for z/OS?

**Answer:**
Installation and technical support is provided by local Field Technical Support Specialists and zSeries Advanced Technical Support in Gaithersburg, MD. Additional support is available through the Worldwide Question and Answer (WWQA) QAA 'SEARCH' and 'Submit a Product Usage Question (PMR)' found on the WWQA Web site at w3.ibm.com/support/wwqa

**Question:**
What pricing options are available for the Encryption Facility for z/OS?

**Answer:**
IBM Encryption Facility for z/OS 1.1 is eligible for sub-capacity WLC, EWLC, and PSLC pricing according to the terms in the Attachment for IBM System z9 and eServer zSeries Workload License Charges (Z125-6516) and the Attachment for IBM eServer zSeries 890 and 800 Software License Charges (Z125-6587).

**Question:**
What versions and releases of z/OS will support the Encryption Facility for z/OS?

**Answer:**
The Encryption Facility for z/OS is supported on z/OS and z/OS.e releases 1.4, 1.5, 1.6, and 1.7 running on System z9 and zSeries servers. Both features can use the state-of-the-art encryption and centralized key management capabilities provided by functions of z/OS and features of System z9 and zSeries servers to help secure data stored to tape and other removable media.

**Question:**
What major functions are supported by Encryption Services feature?

**Answer:**
The Encryption Services feature consists of two major functions, one to encrypt files, and the other to decrypt files. Both functions can leverage the centralized z/OS key management and access authentication capabilities provided within the Integrated Cryptographic Services Facility (ICSF) and the hardware cryptographic and hardware compression capabilities of System z9 and zSeries servers. Some hardware cryptographic functions require the configuration of one or more optional priced features on most IBM System z9 and zSeries servers. Samples of JCL required to invoke each program will be provided.
Question:
What major functions are supported by the DFSMSdss Encryption feature?

Answer:
The DFSMSdss Encryption feature includes two functions, one to encrypt data while processing DUMP commands, and the other to decrypt it while processing RESTORE commands.

Question:
What types of encryption does the Encryption Services feature support?

Answer:
The Encryption Services feature supports data encryption using TDES triple-length keys or 128-bit AES keys. RSA public/private keys can be specified to wrap and unwrap the AES and TDES data keys used to encrypt the file. The wrapped keys will be stored in a file header. With this technique, many files can be generated using different encryption keys, and each is expected to be able to be read even after years of archived storage. The Encryption Services feature also supports using a password key derivation scheme in place of RSA key wrapping.

Question:
What types of encryption does the DFSMSdss Encryption support?

Answer:
DFSMSdss Encryption supports encryption of data using TDES triple-length keys or 128-bit AES keys. Like the Encryption Services feature, this feature supports the use of RSA public/private keys to wrap and unwrap the AES and TDES data keys used to encrypt files as well as AES and TDES key generation using a specified password. You can also specify that DFSMSdss is to compress data before encrypting it.

Question:
What types of input does the Encryption Services feature support?

Answer:
The Encryption Services feature supports inputs from physical sequential input files, from members of partitioned data sets (PDS) and partitioned data set extended (PDSE) data sets, and from files stored in z/OS UNIX® System Services file systems. It can optionally compress input files before encrypting them and writing the output files. Also, it can use the large block interface for output files written to tape, to help optimize performance and media space.
**Question:**
What options can you specify when using the Encryption Services feature?

**Answer:**
You can specify several options when using the Encryption Facility. The availability of some options depends on the hardware, hardware cryptographic features, and ICSF features installed. These options include:

- Description of input file – Written to output file directly, bypassing encryption, to be used later, if needed, to help identify the source of encrypted data contained in the output file.
- Encryption type – Information about the encrypting key to be generated, including 3-key TDES, clear 128-bit AES, and secure 3-key TDES.
- Key protection – Information about the method to be used to generate and protect the data encrypting key, including RSA or password.
- Iteration count – Specifies the number of iterations of SHA-1 hash performed in the generation of the data key and the initial chaining vector (ICV) for encryption when using a password.
- Compression – Specifies whether or not to perform compression prior to encryption. (Note: The Encryption Facility for z/OS Client will not process compressed tapes.)

**Question:**
What options can you specify when using the DFSMSdss feature?

**Answer:**
You can specify several options when using this feature. The availability of some options depends on the hardware, hardware cryptographic features, and ICSF features installed. These options include:

- Encryption type – Information about the encrypting key to be generated, including 3-key TDES, clear 128-bit AES, and secure 3-key TDES
- Key protection – Information about the method to be used to generate and protect the data encrypting key, including RSA or password.
- Compression – Specifies whether or not to perform compression prior to encryption.

**Question:**
Will the DFSMSHsm™ exploit the encryption support provided by DFSMSdss in the DFSMSHsm?

**Answer:**
Yes. DFSMSHsm will exploit the encryption support provided by DFSMSdss in the DFSMSHsm full-volume dump function and the associated restore functions, including both full-volume and data set-level restore.
Question:
What function is the Encryption Facility for z/OS Client designed to provide?

Answer:
The Encryption Facility for z/OS Client, a separately licensed program (which is offered as is, with no warranty), is written in Java and can be used on multiple platforms. It is designed to enable the exchange of encrypted data between z/OS systems that have the Encryption Facility installed and systems running on other platforms that provide the needed supported functions. The Encryption Facility for z/OS Client is designed to:

- Decrypt data that was created on a z/OS system using the Encryption Facility
- Encrypt data to be sent to a z/OS system, where the file will be decrypted using the Encryption Facility

Question:
When and where can I obtain a copy of the Encryption Facility for z/OS Client?

Answer:
Starting on October 28, 2005, you can download the Encryption Facility for z/OS Client from


Note: Data that is to be processed using the Encryption Facility Client cannot be created using compression.

Question:
Does IBM provide hardware and software support services for this product?

Answer:
Yes. IBM offers a number of remote and on-site IBM SmoothStart (TM) Services, Operational Support Services, Migration Services, and Installation Services designed to accelerate productive use of the IBM solution. These services are provided by IBM or an IBM Business Partner at an additional charge. For additional information, contact an IBM representative and ask for IGS Services for Encryption Facility for z/OS.

Question:
When can I order the Encryption Facility for z/OS?

Answer:
Orders for new licenses of the IBM Encryption Facility for z/OS, 1.1 (5655-P97) can be placed now. Registered customers can access IBMLink® for ordering information and charges.

Shipment will not occur before the availability date.
**Question:**
What hardware is required to run the Encryption Services and the DFSMSdss Encryption features of the Encryption Facility for z/OS?

**Answer:**
The Encryption Services and the DFSMSdss Encryption features of the Encryption Facility for z/OS run on the following IBM servers:

- System z9 109 (z9-109), or equivalent
- zSeries z900 or z990, or equivalent
- zSeries z800 or z890, or equivalent

The cryptographic options have the following requirements:

- For the PASSWORD option, use one of the following:
  - CPACF only
  - CCF
- For the Clear-TDES and Clear-AES128 (no ENCTDES), use one of the following:
  - CPACF only, or CPACF with PCIXCC / CEX2C
  - CCF, or CCF with PCICC
- For 2048-bit keys, use one of the following:
  - CEX2C with Licensed Internal Code (LIC) at or above the January 2005 level
  - PCIXCC with Licensed Internal Code (LIC) at or above the January 2005 level
- For RSA keys generated through RACF using ICSF or directly through ICSF, use one of the following:
  - CEX2C
  - PCIXCC
  - PCICC
- For 1024-bit ME keys generated through RACF BSAFE and imported into ICSF, a CCF is required.

**Question:**
What software is required to run the Encryption Services and the DFSMSdss Encryption features of the Encryption Facility for z/OS?

**Answer:**
The Encryption Services and the DFSMSdss Encryption features of the Encryption Facility for z/OS require the following:

- z/OS (5694-A01) or z/OS.e (5655-G52) 1.4 or higher
- PTF for z/OS DFSMS APAR OA09868
- z/OS Cryptographic Services – Integrated Cryptographic Services Facility with z990 Cryptographic Support Web deliverable (FMID HCR770A) or later. Some hardware features require the z990 and z890 Enhancements to Cryptographic Support Web deliverable (FMID HCR770B).
The optional PTF for APAR OA13030 is required to:

- Use the RACF RACDCERT command to allow the storage of RSA public keys in the ICSF PKDS
- Specify the PKDS labels to be used when storing public or private keys in the PKDS
- List the PKDS labels of existing certificates

The DFSMSdss Encryption feature requires:

- Either the DFSMShsm/DFSMSdss combination priced feature or the DFSMSdss priced feature of z/OS 1.4 or z/OS.e 1.4 or higher.
- PTF for z/OS DFSMS APAR OA13300

The Encryption Facility Client requires the following:

- To run on z/OS, one of the following is required:
  - IBM SDK for z/OS, Java 2 Technology Edition, 5655-I56, at PTF UQ90449 or higher (SDK1.4.2)
  - IBM Developer Kit for OS/390, Java 2 Technology Edition, 5655-D35, at PTF UQ88094 or higher (SDK1.3.1)
- To run on other platforms, one of the following is required:
  - Sun SDK 5.0
  - An IBM JVM at SDK1.4.2
  - A JVM with a JCE cryptographic provider installed that supports all the required algorithms. See the Encryption Facility Client documentation for details on the algorithms, modes, and padding schemes needed.

For information about Java on z/OS, visit


**Question:**
When does IBM expect to have performance data available for the Encryption Services and the DFSMSdss Encryption features of the Encryption Facility for z/OS?

**Answer:**
IBM plans to have performance data available for customer review at general availability of both features.

**Question:**
What is unique about the capabilities IBM is delivering with the Encryption Facility for z/OS?

**Answer:**
The IBM Encryption Facility for z/OS is intended to provide a host-based solution that not only leverages existing centralized key management and access authentication capabilities found in ICSF, but also has the ability to take advantage of our existing hardware capabilities such as compression and high performance encryption.
**Question:**
What is ICSF?

**Answer:**
The Integrated Cryptographic Service Facility (ICSF) is currently delivered as part of z/OS. ICSF, leveraging the secure key cryptographic hardware available on zSeries processors, enables the encryption and decryption of data and the generation and management of cryptographic keys, and performs other cryptographic functions dealing with digital signatures.

**Question:**
Does encryption of data require key management?

**Answer:**
Yes. Key management is an essential part of any encryption solution. ICSF provides centralized key management and access authentication capability to securely generate, distribute and backup cryptographic keys. The use of keys may be distributed across your enterprise; using ICSF you may be able to simplify the complexity of managing the keys by centralizing the control in one place.

**Question:**
How do you expect the proposed technology contained in the TotalStorage SOD to work with the mainframe and z/OS?

**Answer:**
IBM intends to support encryption and decryption capabilities on our tape and disk subsystems to minimize server resources consumed for these functions. When a mainframe and z/OS is available in the configuration, we intend to use ICSF on z/OS to provide centralized key management capability.

**Question:**
What is unique about IBM’s approach to data encryption?

**Answer:**
The plans outlined in this announcement and the TotalStorage SOD are designed to provide a comprehensive approach for data encryption. Our approach is designed to leverage the existing hardware capabilities such as compression and high performance encryption, enable centralized key management and access authentication, and allow customers the ability to protect vital information used within your enterprise, storage in a long term archive, and shared across platforms with partners, suppliers and customers.
**GDPS Enhancements**

**Question:**
What new GDPS® functions are being announced?

**Answer:**
IBM is announcing extensions to the HyperSwap™ functionality. HyperSwap is the technology within GDPS that designed to allow z/OS and z/VM systems to “switch” to secondary disks in the event of a disk failure or disk maintenance with only a momentary pause in application availability. GDPS is adding a new HyperSwap trigger to allow tailoring for unplanned HyperSwap conditions when a disk subsystem is experiencing soft failures, such as a non-responsive disk subsystem. This is planned to be available to GDPS V3.2 customers in 3Q05.

**Question:**
Are there any GDPS functions being previewed?

**Answer:**
GDPS/HyperSwap Manager within a single Data Center allows GDPS/PPRC HyperSwap Manager configured within a single data center to invoke HyperSwap for individual disk subsystems that need to be switched, helping to simplify systems management and improve availability.

**GDPS Enhanced Recovery Support:** GDPS/PPRC enhancement helps to reduce potentially long or variable recovery times when there is a failover by helping to ensure that the secondary copy of the data at the recovery site and the data in the coupling facility are time consistent. This helps to enable consistent application restart times and reduce the need for special recovery procedures.

**z/OS R7 XRC+ Support:** System Logger is planned to provide new support for XRC+ by allowing asynchronous writes to staging data sets for logstreams improving the throughput for high-volume logging applications, such as WebSphere®, CICS®, and IMS™. The use of asynchronous writes can allow the use of XRC for some application for which it was not previously practical, which may significantly help to improve availability and recovery.

The previewed functions will be available with GDPS V3.3, planned for 4Q05.

**Question:**
When will GDPS/Global Mirror be available?

**Answer:**
GDPS is planning on making the IBM TotalStorage Global Mirror offering available in October 2005.

GDPS/Global Mirror Services, including the licensed GDPS Automation Code, may be delivered to customers prior to October 2005. Contact your IBM representative or send an e-mail to gdps@us.ibm.com for information regarding participation in an early implementation.
Business Resiliency and Security-Related Statements of Direction

All statements regarding IBM's plans, directions, and intent are subject to change or withdrawal without notice.

Question:
What statements of direction has IBM made for IBM TotalStorage?

Answer:
IBM intends to provide the following enhancements:

IBM TotalStorage DS8000 Series of disk products: These enhancements for use in the System z9 environment include:

- IBM TotalStorage z/OS Global Mirror (XRC) and IBM TotalStorage Global Mirror (asynchronous PPRC) capability on the IBM TotalStorage DS8000 Series to enable the use of consistency groups that can span both remote mirroring products for enhanced business continuity. This capability is intended to help customers maintain and leverage their investment in z/OS Global Mirror (XRC) while implementing Global Mirror (asynchronous PPRC) for heterogeneous server environments.
- A continuous data protection function on the IBM TotalStorage DS8000 Series for System z9 environments. This capability is intended to provide support for enhanced data resiliency and business continuity.

IBM TotalStorage SAN Volume Controller (SVC): To enhance the interoperability of the IBM TotalStorage SAN Volume Controller, IBM is planning to provide SVC support for Linux on System z9 environments. This is designed to allow System z9 hosts and supported open system hosts to share storage pools created by the SAN Volume Controller.

IBM TotalStorage Virtual Tape Server (VTS) – business continuity enhancements:

- Provision of an enhanced Import/Export function designed to allow sets of cartridges to be interchanged between VTSs and/or Peer-to-Peer (PtP) VTSs or exported for storage in a remote vault. This enhancement is designed to allow virtual volumes to be directed to a VTS volume pool, subsequently exported on physical cartridges under host control, and imported into another VTS under host control.
- Extension of the PtP VTS – support for full-duplex virtual volume replication between three sites. DFSMS parameters are designed to provide policy-based copy management to control the source and target VTSs, the preferred routing, and the mode of operation.
- **IBM TotalStorage SAN File System (SFS):** SFS was designed to help you manage the growing complexities and rising costs associated with dramatic growth in disk storage requirements. IBM continues to expand on the concept of system-managed storage by working to extend some of the storage management capabilities of DFSMS to open system environments to support improvements in storage asset utilization and administrator productivity.
IBM plans to increase the range of IBM TotalStorage SAN File System supported hosts to include the 31-bit SUSE Linux Enterprise Server 8 (SLES 8) client distribution running under z/VM on System z9 and zSeries platforms. This support is designed to apply exclusively to hosts acting as the SFS client in a System z9 or zSeries server running SUSE SLES 8. This extension of host support for SFS is intended to support increased data sharing between UNIX®, Linux, Microsoft® Windows®, and mainframe platforms.

- **IBM TotalStorage encryption**: To address customers’ growing concern with data security, IBM is also announcing a statement of direction for the development, enhancement and support of encryption capabilities within storage environments such that the capability does not require the use of host server resources (so called "outboard" encryption capabilities). This includes the intent to offer, among other things, capabilities for products within the IBM TotalStorage portfolio to support outboard encryption and to integrate with the key management functions planned for ICSF.
z/OS V1R7 Security and Resiliency Enhancements

**Question:**
What are the key business resiliency and security related enhancements in z/OS Version 1 Release 7 (1.7)?

**Answer:**
z/OS 1.7 has two important enhancements to extend the business resiliency provided with GDPS. We enhanced the scope of GDPS with support for HyperSwap for JES3. We have also enhanced GDPS for customers with very high volume applications – recovery for these large systems is improved with better log management synchronization between sites.

For customers looking to provide highly secure IP connections for their core z/OS applications, we are introducing TLS designed to be application transparent. Customers can apply TLS or SSL to encrypt transactions over IP without necessarily having to modify the applications! Today TLS must be managed at the application level. This new support can help reduce application development and maintenance costs while helping to improve the security of applications on z/OS.

This is an overview of just some of the many improvements in z/OS 1.7. For more information, see the z/OS 1.7 Web page [ibm.com/zseries/zos/overview/zosnew_summary.html](http://ibm.com/zseries/zos/overview/zosnew_summary.html)

**Question:**
What are the network security enhancements to be delivered in z/OS 1.7?

**Answer:**
z/OS 1.7 can help make it easier to deploy Internet security for mainframe workloads. As financial services companies, government agencies and manufacturers move away from relying on more expensive private networks and increasingly tap the Internet to expand their ecosystem of partners, they are looking to secure their mission-critical z/OS applications like CICS on the Internet. z/OS 1.7 has a new function, Transport Layer Security, which allows businesses to apply Internet-standard TLS or SSL encryption with no anticipated changes to their core applications. This feature can make it easier to deploy the mainframe's leading encryption for z/OS managed data and transactions traveling on the Internet which can help prevent outsiders from snooping data on the network.

Also new in z/OS 1.7 is Communications Server IPSec (CS IPSec). This function provides an alternative to z/OS Firewall Technologies for host-based IPSec and IP filtering. The trend for IPSec deployment on z/OS is moving toward host-to-host security. Another prevalent scenario is host-to-branch office gateway protection.

This integrated security functionality provides a simple packet screening function with IP filtering and enables the creation of a network security infrastructure based on pure AT-TLS, IPSec, or a mix of AT-TLS and IPSec.
**Question:**
What are the z/OS encryption plans that were previewed in this announcement?

**Answer:**
IBM intends to deliver a software-based file encryption solution for z/OS that leverages the existing z/OS key management capabilities provided within the Integrated Cryptographic Services Facility (ICSF) in 2005. More information will be provided at a later date.
**z/VM V5R2 Security Enhancements**

**Question:**
Is there an overview available of the z/VM 5.2 Business Resiliency and Security related enhancements?

**Answer:**
Here is an overview of the z/VM 5.2 security and resiliency related announcements.

- Virtualization technology and Linux enablement:
  - SSL server support for additional Linux distributions
- Network virtualization and security:
  - Improved problem determination for Guest LANs and Virtual Switches
  - Enhanced dynamic routing capabilities with new MROUTE server
- Technology exploitation:
  - Support for the IBM System z9 platform:
    - Crypto Express2 Accelerator for Crypto sharing among Linux and z/OS guests

**Question:**
What features are optional for z/VM V5?

**Answer:**
The priced optional features of the z/VM V5 base product are the Performance Toolkit for VM™, DirMaint™, and RACF®.

**Question:**
Which servers are supported by z/VM V5?

**Answer:**
z/VM V5 is supported on the new IBM System z9 109 (z9-109), IBM zSeries 990, zSeries 890, zSeries 900, and the zSeries 800.

**Question:**
What new security features does z/VM V5.2 exploit on z9-109, z990, and z890?

**Answer:**
z/VM V3.1, V4.4, V5.1, and V5.2 provide exploitation support for the following z9-109, z990, and z890 as configured:

**z/VM V4.4, V5.1, V5.2**
- PCICA support for Linux and z/OS guests (z/OS guests supported on z/VM V5 only and not supported on z9-109)
- PCIXCC support for Linux and z/OS guests (z/VM V5 only and not supported on z9-109)
- Crypto Express2 support (coprocessor) for Linux and z/OS guests (z/VM V5 only)
- Crypto Express2 supported as an accelerator card for SSL acceleration for Linux and z/OS guests (V5.1 requires the PTF for APAR VM63646, V5.2)
**Question:**
What cryptography support is provided by z/VM for the z9-109, z990, and z890?

**Answer:**
z/VM software support for the PCIX Cryptographic Coprocessor (PCIXCC), the CP Assist for Cryptographic Function (CPACF), and the PCI Cryptographic Accelerator (PCICA) features are as the follows:

- **PCICA:** z/VM Versions 4.4 and later (for Linux guests only), z/VM V5.1 (for Linux and z/OS guests also)
- **CPACF:** z/VM Versions 3.1, 4.4 and later (for guests only)
- **PCIXCC:** z/VM Version 5.1 and 5.2 (for Linux and z/OS guests)
- **Crypto Express2:** z/VM Version 5.1 and 5.2 (for Linux and z/OS guests)

**Question:**
Where can I review more comprehensive FAQs for z/VM V5?

**Answer:**
You will find a complete set of FAQs on the VM Web site at: http://www.vm.ibm.com
IBM, the IBM logo, IBM @server, IBM eServer, e-business logo, CICS, DB2, DirMaint, ECKD, ESCON, FICON, GDPS, HyperSwap, IMS, On Demand Business logo, Performance Toolkit for VM, RACF, Resource Link, S/390, System z9, TotalStorage, VSE/ESA, WebSphere, z/Architecture, z/OS, z/VM, z/VSE, and zSeries are trademarks or registered trademarks of the International Business Machines Corporation.

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

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

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

UNIX is a registered trademark of The Open Group in the United States and other countries. All other registered trademarks and trademarks are the properties of their respective companies.

This publication was produced in the United States.

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

You can find additional information via IBM's World Wide Web server at ibm.com.

IBM Hardware products are manufactured from new parts or new and serviceable used parts. Regardless, our warranty terms apply. Actual performance and environmental costs will vary depending on individual customer configurations and conditions.

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

z/VSE can execute in 31-bit mode only. It does not implement z/Architecture, and specifically does not implement 64-bit mode capabilities. z/VSE is designed to exploit selected features of IBM z9 and zSeries hardware.