



IBM Washington Systems Center
Advanced Technical Support

RDS Training Hardware Overview

zSeries Security
Advanced Technical Support
Gaithersburg, MD

ON DEMAND BUSINESS™

August 5, 2005

© 2005 IBM Corporation

IBM Washington Systems Center



IBM Cryptographic Hardware – z800/z900 and earlier

Crypto Coprocessor Facility (CCF) $e_{mk}(k)$

PCI Crypto Coprocessor (PCICC) $e_{mk}(k)$

PCI Crypto Accelerator (PCICA)

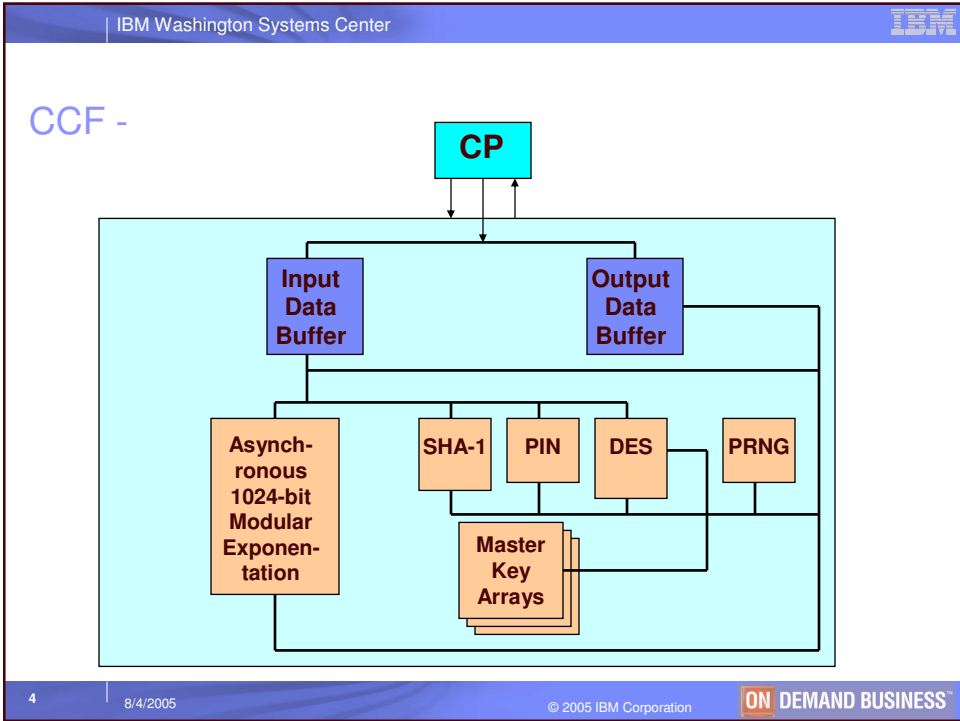
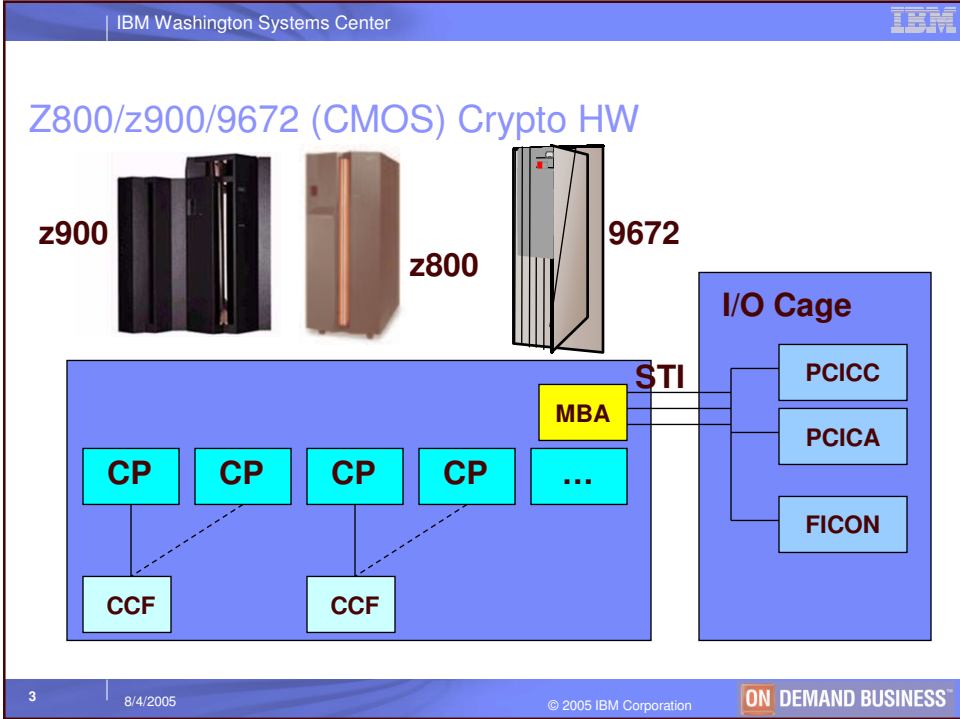


2

8/4/2005

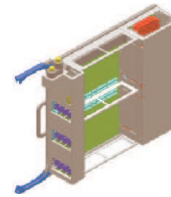
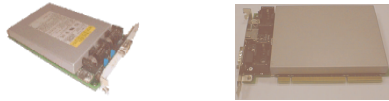
© 2005 IBM Corporation

ON DEMAND BUSINESS™



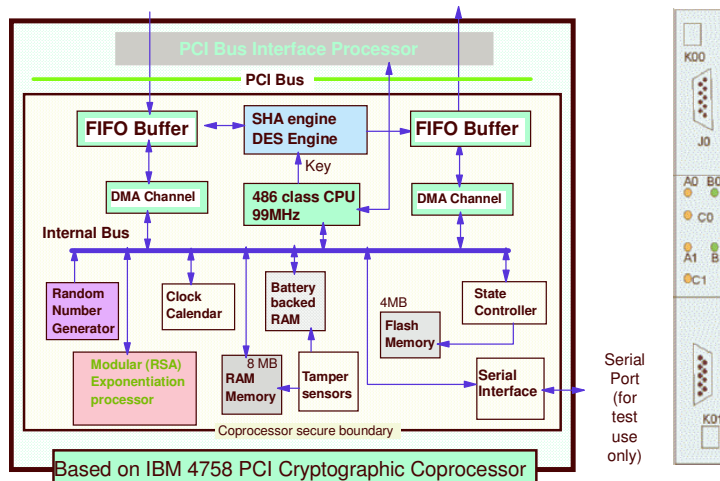
PCI Cards (General)

- Feature – Packaged as a book
- May consist of a single- or dual-card



- Card may also be referred to as a port
- On 9672, z900/z800 a book is associated with a CHPID
- On a z890/z990 a book is associated with a PCHPID

PCICC



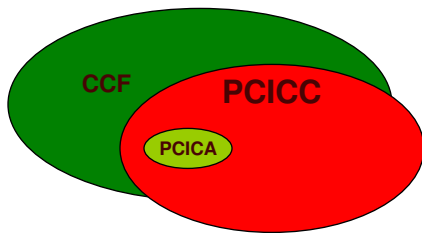
Based on IBM 4758 PCI Cryptographic Coprocessor

Original Chart provided courtesy of ITSO.

PCICA

- **It does one thing, and one thing only, but it does it very fast**
 - CSNDPKD – Public Key Decrypt API
 - Decrypt of the Pre-Master Secret

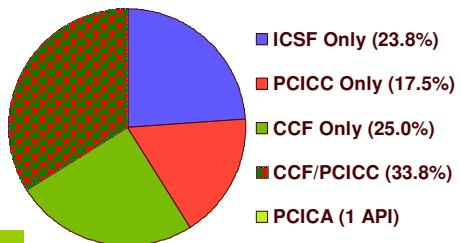
APIs on CCF/PCICC/PCICA



On a CCF Only system, 66 APIs are available

With a CCF & PCICC, 80 APIs are available

PCICA supports only 1 API



zSeries Cryptographic Hardware – z890/z990

CP Assist for Crypto Functions (CPACF)

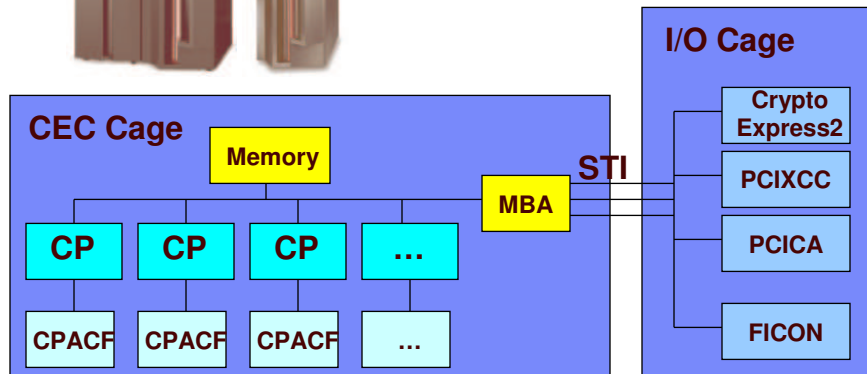
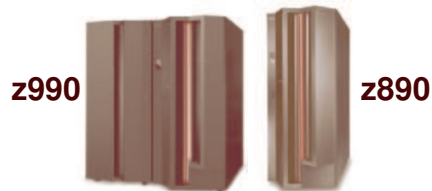
Crypto Express2
 $e_{mk}(k)$



PCI Crypto Accelerator (PCICA)

PCI X Crypto Coprocessor (PCIXCC)
 $e_{mk}(k)$

Z890/z990 Crypto HW

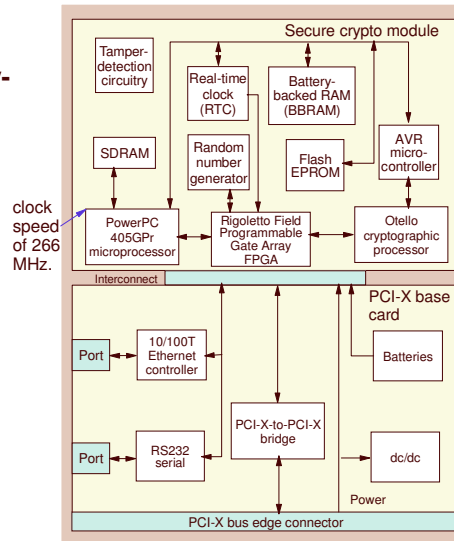


PCICA

- **It does three things, and only three things, but it does them very fast**
 - CSNDPKD – Public Key Decrypt API
 - Decrypt of the Pre-Master Secret
 - CSNDPKE – Public Key Encrypt API
 - Encrypt of the Pre-Master Secret
 - CSNDDSV – Digital Signature Verify API
 - Verifies a Digital Signature

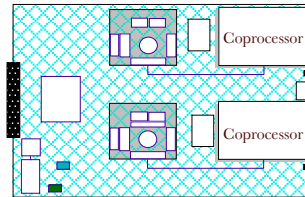
PCIXCC

Adapter card with all security-related components encased in a tamper responding security module

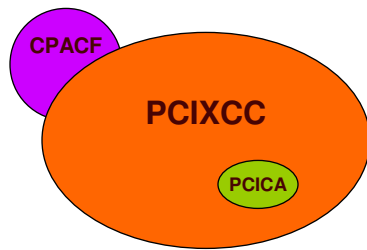


Crypto Express2

- **Combines functionality of PCIXCC and PCICA into a single feature**



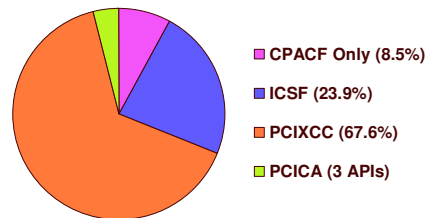
APIs on CPACF, PCIXCC, PCICA



In a CPACF only system, there are 14 APIs available (6 are routed to the CPACF, and 8 to ICSF)

With a PCIXCC, 71 APIs are available

PCICA supports 3 APIs



zSeries Cryptographic Hardware – z9 109

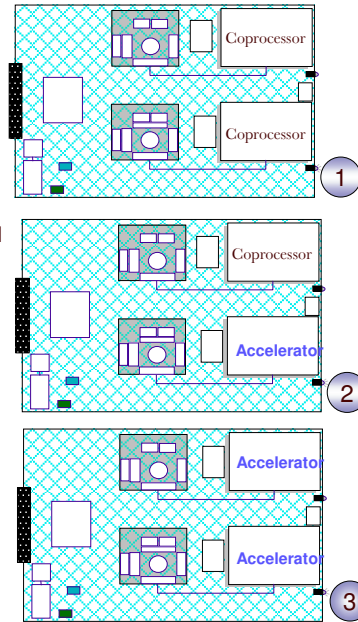
CP Assist for Crypto Functions (CPACF)

Crypto Express2 $e_{mk}(k)$



Z9 109 Crypto Express2 Configuration

- **Secure Coprocessor (default)**
 - Provides both “Secure key” and “Public key” functionality and performance equivalent to Crypto Express2 features on z990
 - “Secure key” improved performance compared to PCIXCC on z990 (requires multitasking)
 - “Public key” equivalent performance to PCICA on z990
 - No action required
- **Accelerator**
 - Provides only “Public key” functionality with enhanced performance
 - Must be configured using the HMC



Enablement Diskettes

- **CCF**
 - Shipped Inactive, must be enabled
 - Config file unique to each CCF
 - Config files are loaded into the CCF
- **PCICC**
 - Single config file loaded into HSA and shared among PCICCs
- **CPACF**
 - Secure Hash Algorithms available without Microcode load
 - DES/TDES/AES requires Microcode load

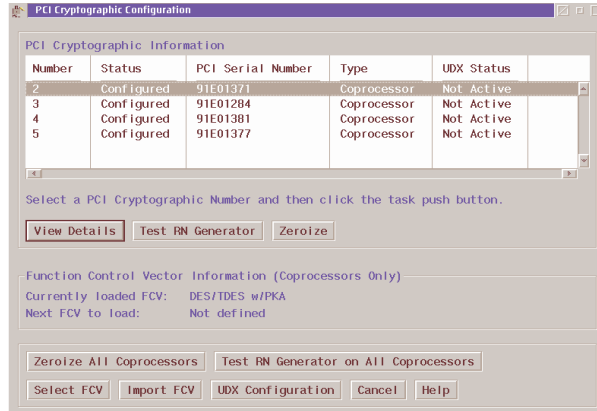
Z900 SE CCF Config

The screenshot shows a window titled "Cryptographic Coprocessor Configuration". Inside, there is a table with the following data:

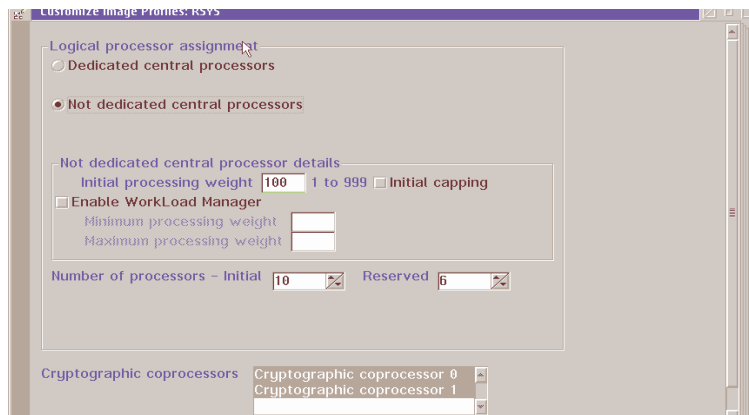
Coprocessor	Status	Current Configuration Description	Next Configuration Description	Cryptograph Module Iden
0	Initialized	DES/TDES w/PKA & TKE	DES/TDES w/PKA & TKE	041000000
1	Initialized	DES/TDES w/PKA & TKE	DES/TDES w/PKA & TKE	041000000

Below the table, there is a text instruction: "Select one of the cryptographic coprocessors and then click the task push button." Below this are four buttons: "Import", "View status", "Select for next activation", and "Test Pseudo-Random Number Generator". At the bottom of the window are five buttons: "PKSC Initialization", "Zeroize", "Cancel", and "Help".

SE z/900 PCI Cards



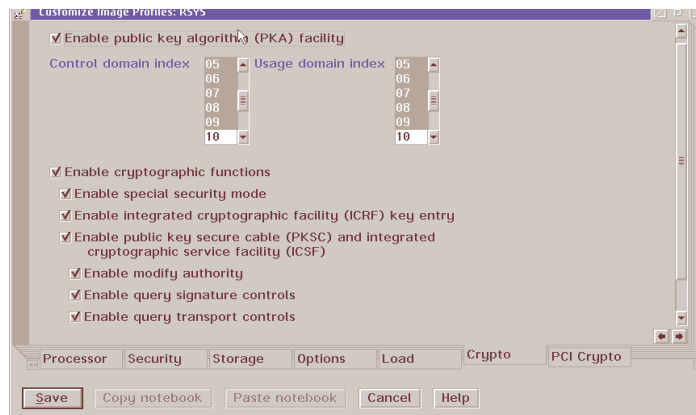
Processor Tab for ROASP6 (Top)



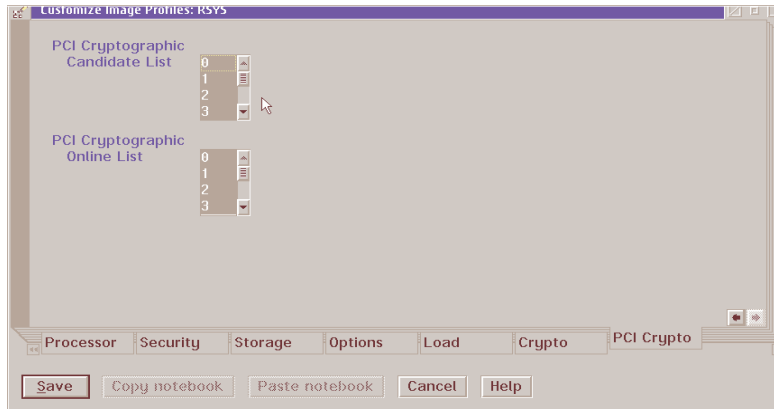
Processor Tab for ROSP6 (Bottom)



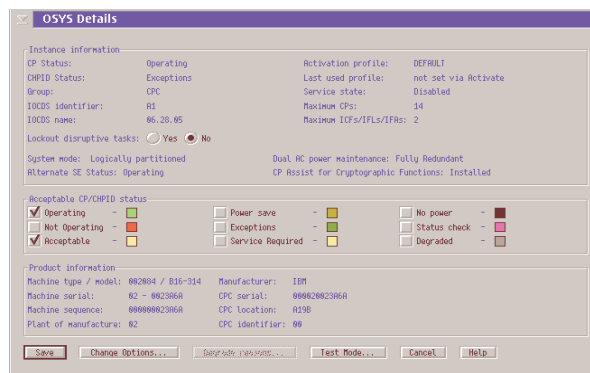
Crypto Tab for ROSP6



PCI Crypto Tab for ROSP6



SE z990 OSYS Details



SE z990 PCI Cards

PCI Cryptographic Configuration

Number	Status	PCI Serial Number	Type	UDX Status	TKE Commands
0	Configured	N32001V3	Accelerator	Not Supported	Not Supported
1	Configured	N32001V9	Accelerator	Not Supported	Not Supported
2	Configured	N42001V8	Accelerator	Not Supported	Not Supported
3	Configured	N52001V2	Accelerator	Not Supported	Not Supported
4	Configured	93001166	X Coprocessor	IBM Default	Not Supported
5	Configured	93001449	X Coprocessor	UDX	Permitted

Select a PCI Cryptographic Number and then press the task push button.

View Details Test RN Generator Zeroize TKE Commands

Zeroize All X Coprocessors Test RN Generator on All X Coprocessors UDX Configuration

Refresh Cancel Help

OOSP3 Image – PCICrypto Tab

Customize Image Profiles: OOSP3

Control domain index: 00, 01, 02, 03, 04, 05

Usage domain index: 00, 01, 02, 03, 04, 05

PCI Cryptographic Candidate List: 00, 01, 02, 03, 04, 05

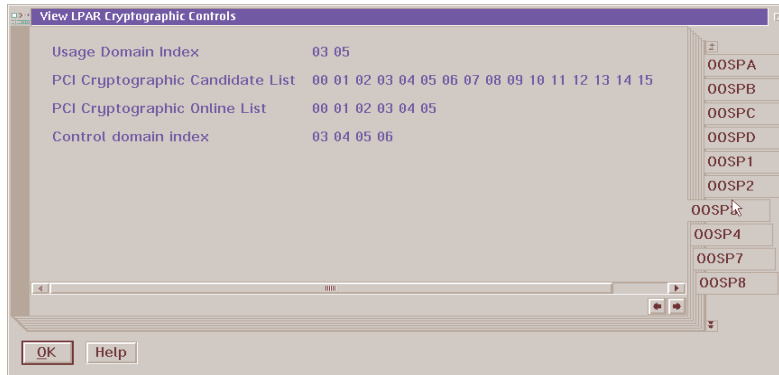
PCI Cryptographic Online List: 00, 01, 02, 03, 04, 05

Attention: You must install the 'IBM CP Assist for Cryptographic Functions' (CPACF) feature if a PCI Cryptographic Candidate is selected from the list box; otherwise, some functions of Integrated Cryptographic Service Facility (ICSF) may fail.

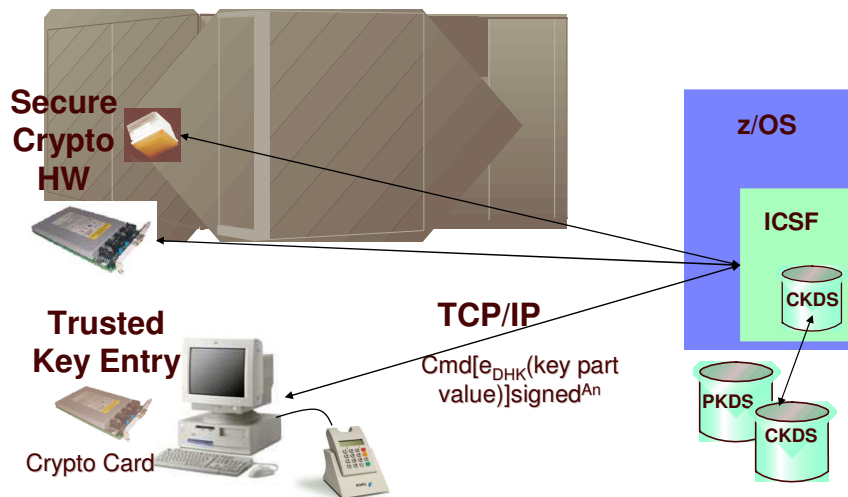
General Processor Security Storage Options Load **PCICrypto**

Save Copy notebook Paste notebook Assign profile Cancel Help

Crypto Defined to LPAR OOSP3 on z990



TKE – Trusted Key Entry Workstation



Questions?

Trademarks

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries. For a complete list of IBM Trademarks, see www.ibm.com/legal/copytrade.shtml: AS/400, DBE, e-business logo, ESCON, eServer, FICON, IBM, IBM Logo, iSeries, MVS, OS/390, pSeries, RS/6000, S/390, VM/ESA, VSE/ESA, Websphere, xSeries, zOS, zSeries, zVM

The following are trademarks or registered trademarks of other companies

Lotus, Notes, and Domino are trademarks or registered trademarks of Lotus Development Corporation
 Java and all Java-related trademarks and logos are trademarks of Sun Microsystems, Inc., in the United States and other countries
 LINUX is a registered trademark of Linux Torvalds
 UNIX is a registered trademark of The Open Group in the United States and other countries.
 Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation.
 SET and Secure Electronic Transaction are trademarks owned by SET Secure Electronic Transaction LLC.
 Intel is a registered trademark of Intel Corporation
 * All other products may be trademarks or registered trademarks of their respective companies.

NOTES:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

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

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

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 product or services available in your area.

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

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

References in this document to IBM products or services do not imply that IBM intends to make them available in every country.

Any proposed use of claims in this presentation outside of the United States must be reviewed by local IBM country counsel prior to such use.

The information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.