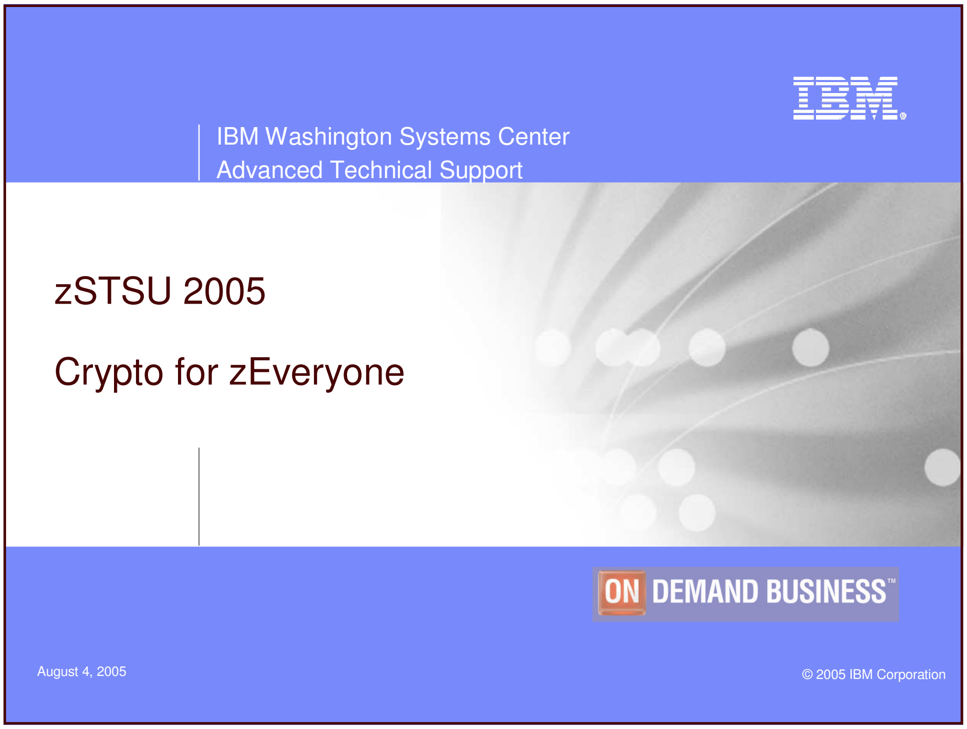


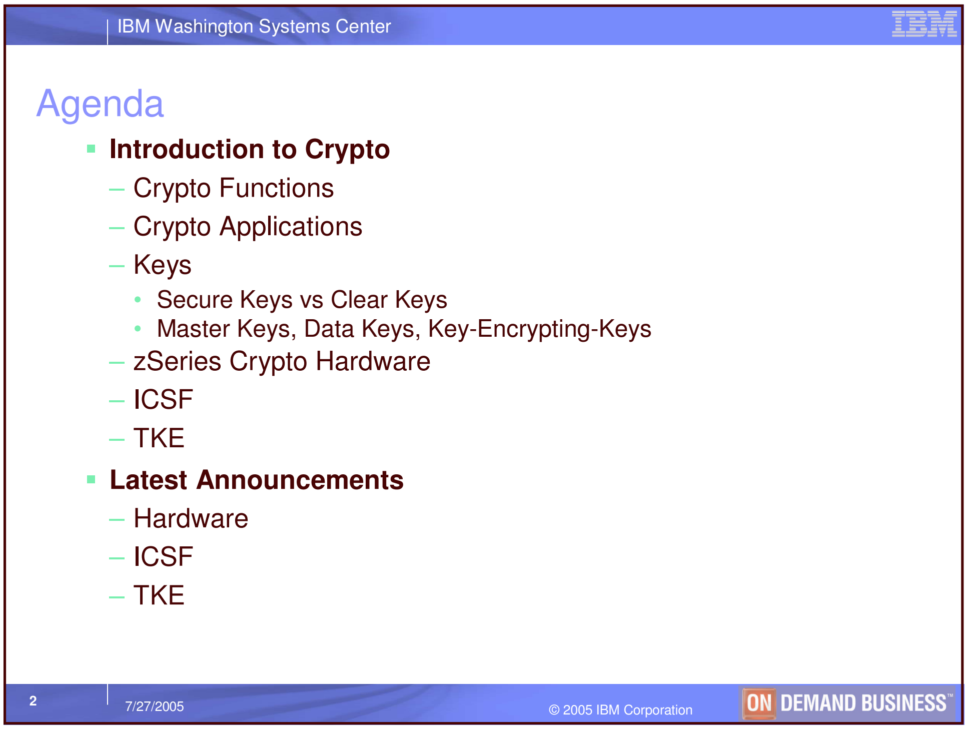
IBM Washington Systems Center
Advanced Technical Support

zSTSU 2005

Crypto for zEveryone

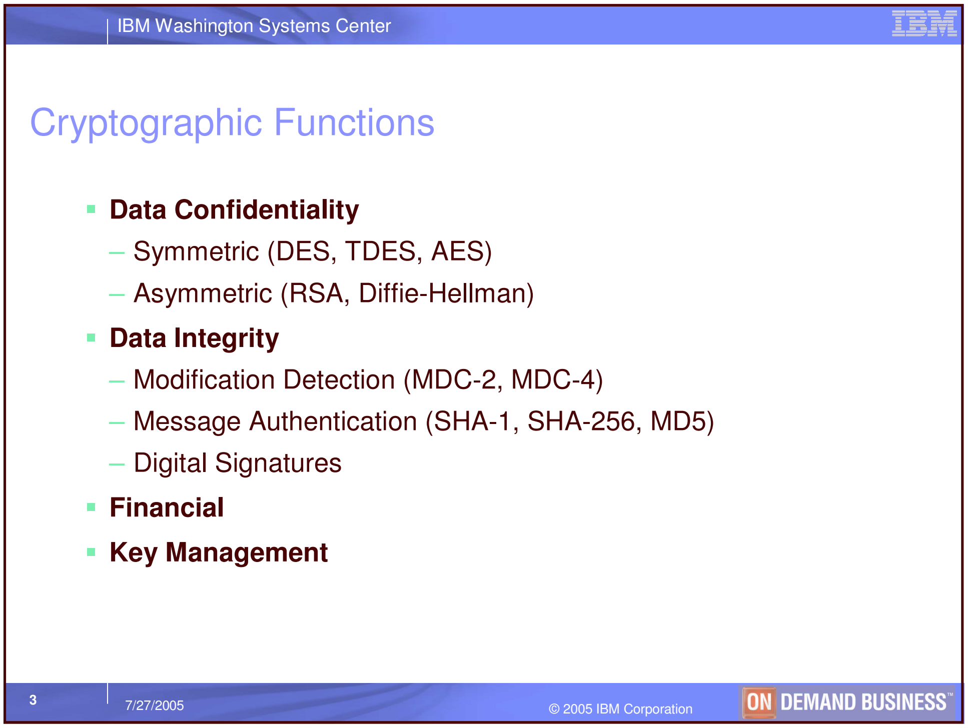
ON DEMAND BUSINESS™

August 4, 2005



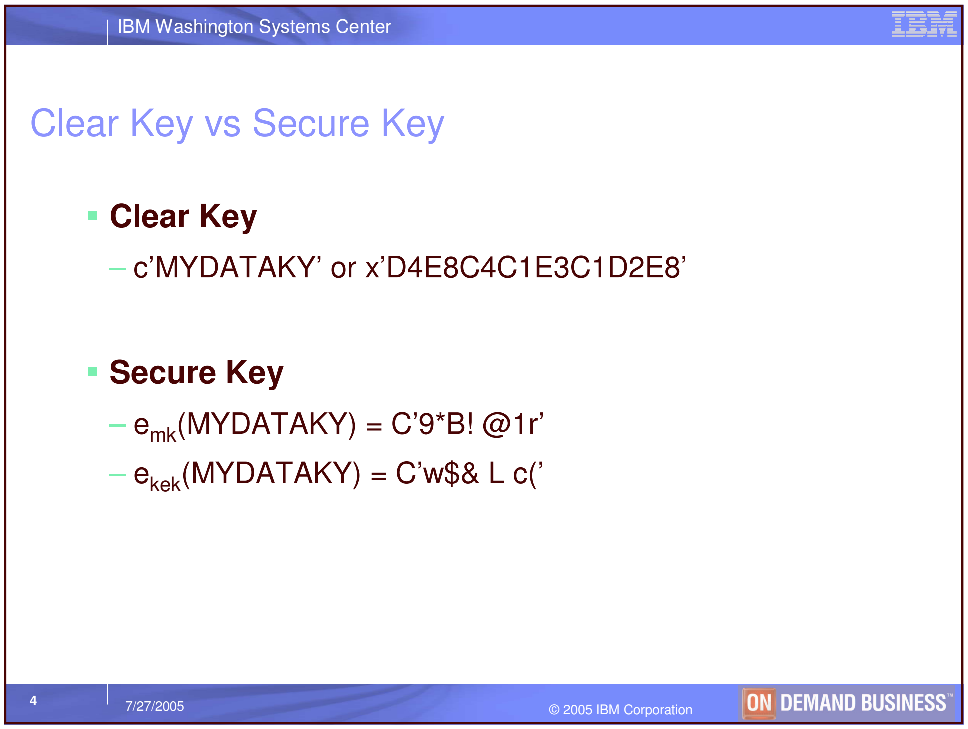
Agenda

- **Introduction to Crypto**
  - Crypto Functions
  - Crypto Applications
  - Keys
    - Secure Keys vs Clear Keys
    - Master Keys, Data Keys, Key-Encrypting-Keys
  - zSeries Crypto Hardware
  - ICSF
  - TKE
- **Latest Announcements**
  - Hardware
  - ICSF
  - TKE



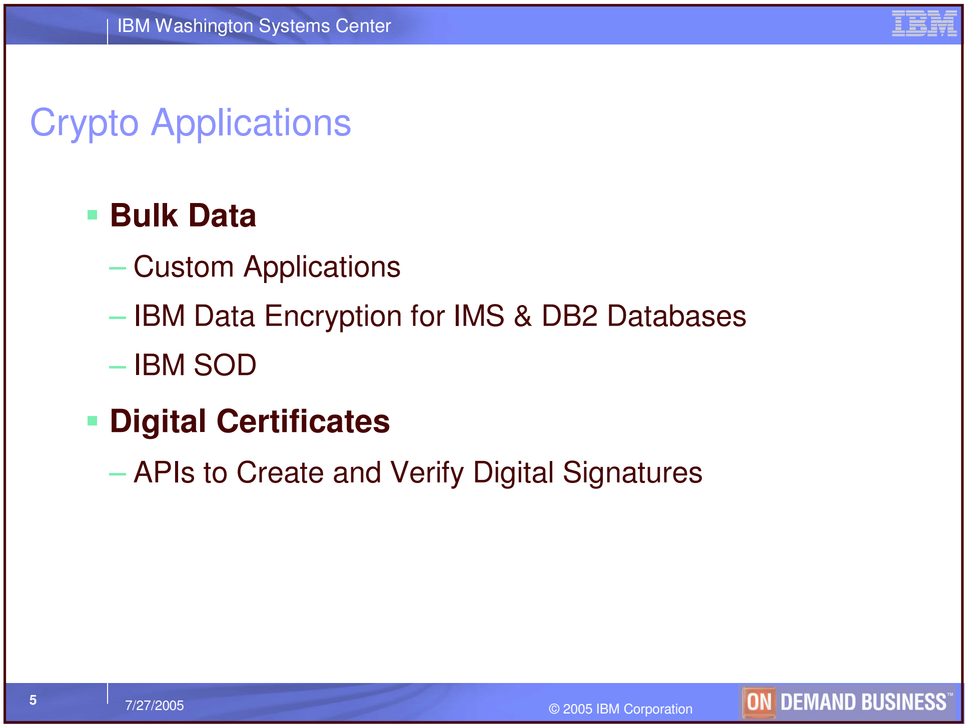
Cryptographic Functions

- **Data Confidentiality**
  - Symmetric (DES, TDES, AES)
  - Asymmetric (RSA, Diffie-Hellman)
- **Data Integrity**
  - Modification Detection (MDC-2, MDC-4)
  - Message Authentication (SHA-1, SHA-256, MD5)
  - Digital Signatures
- **Financial**
- **Key Management**



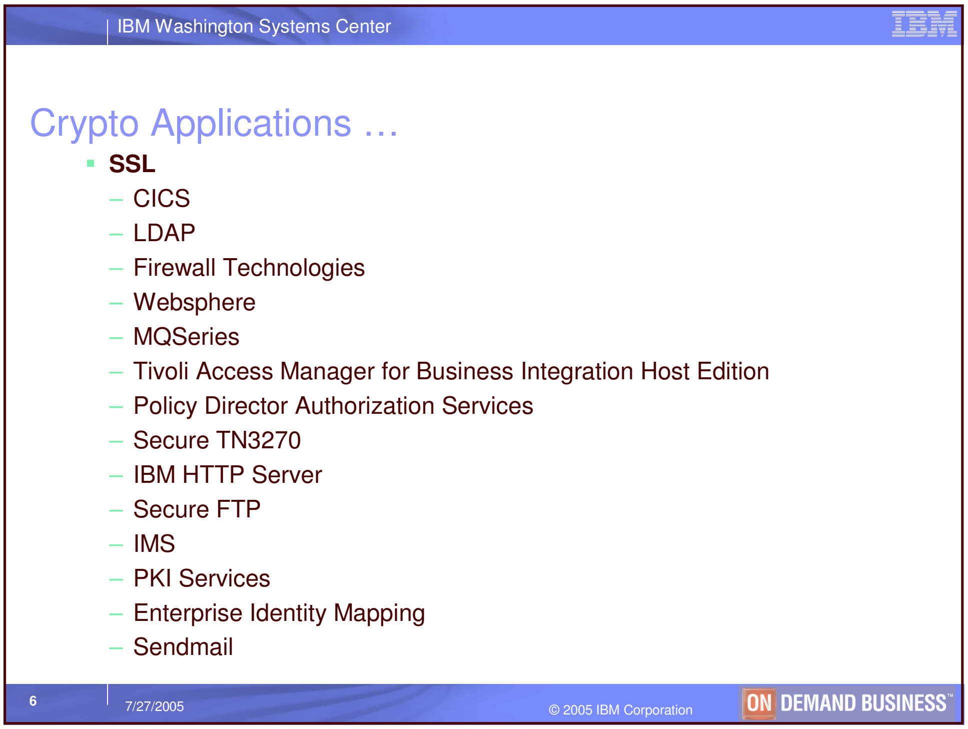
Clear Key vs Secure Key

- **Clear Key**
  - c'MYDATAKY' or x'D4E8C4C1E3C1D2E8'
- **Secure Key**
  - e_{mk}(MYDATAKY) = C'9*B! @1r'
  - e_{kek}(MYDATAKY) = C'w$& L c('



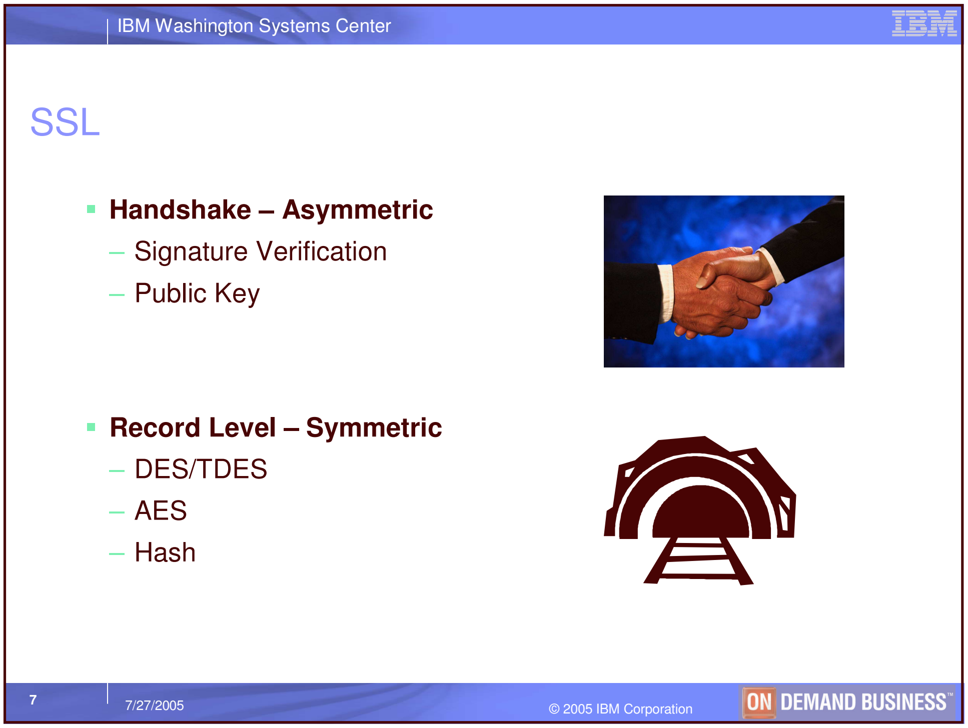
Crypto Applications

- **Bulk Data**
  - Custom Applications
  - IBM Data Encryption for IMS & DB2 Databases
  - IBM SOD
- **Digital Certificates**
  - APIs to Create and Verify Digital Signatures



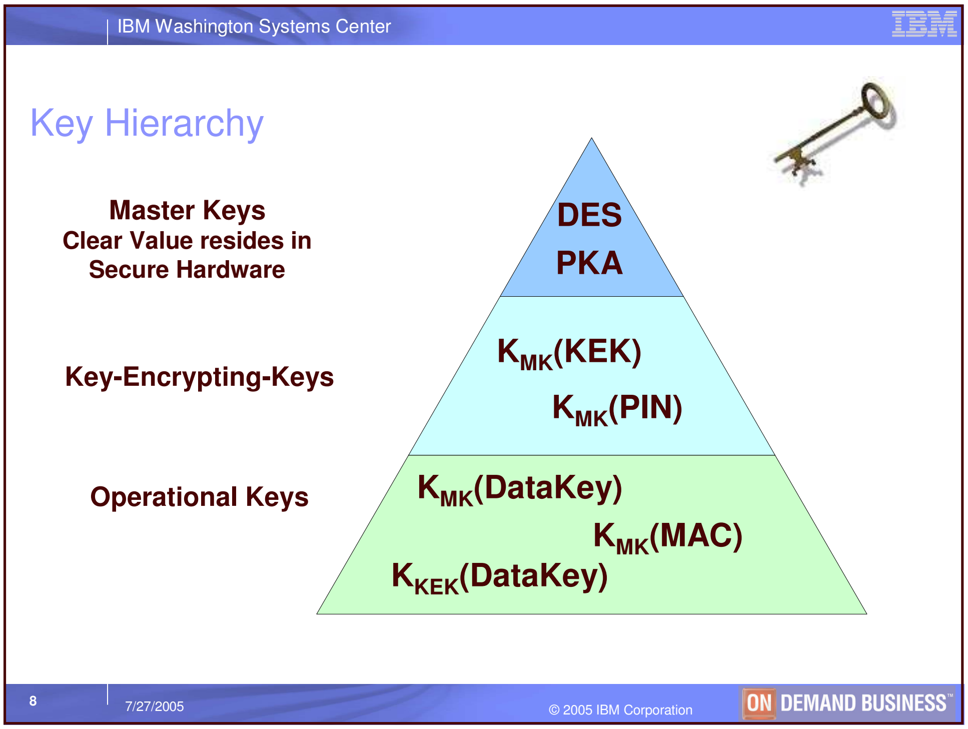
Crypto Applications …

- **SSL**
  - CICS
  - LDAP
  - Firewall Technologies
  - Websphere
  - MQSeries
  - Tivoli Access Manager for Business Integration Host Edition
  - Policy Director Authorization Services
  - Secure TN3270
  - IBM HTTP Server
  - Secure FTP
  - IMS
  - PKI Services
  - Enterprise Identity Mapping
  - Sendmail



SSL

- **Handshake – Asymmetric**
  - Signature Verification
  - Public Key
- **Record Level – Symmetric**
  - DES/TDES
  - AES
  - Hash



Key Hierarchy

Master Keys
Clear Value resides in
Secure Hardware

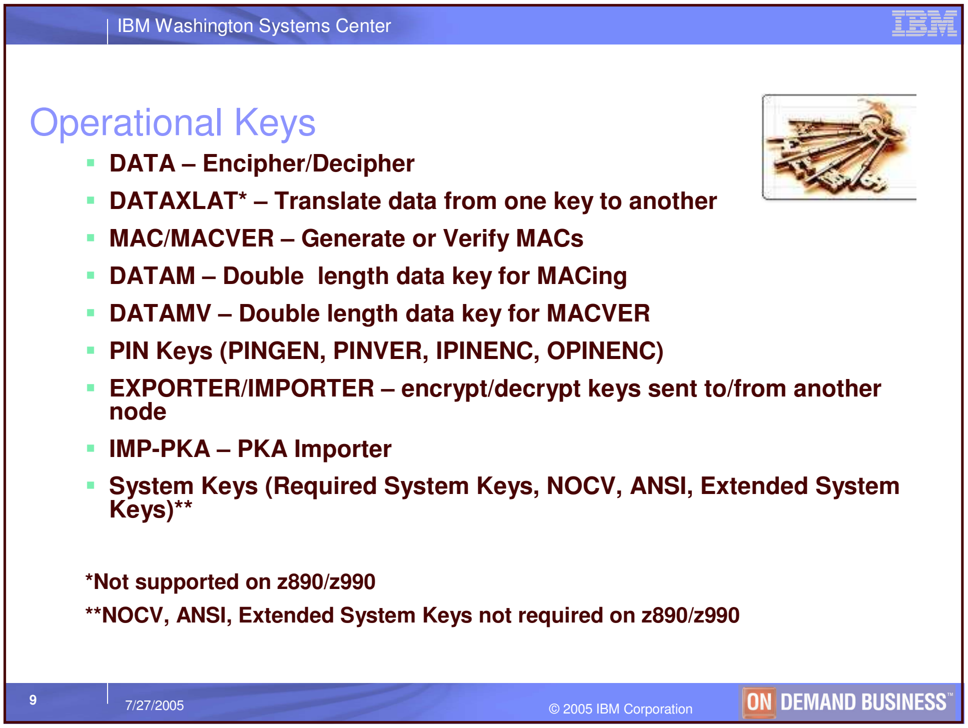
Key-Encrypting-Keys

Operational Keys

DES
PKA

K_{MK}(KEK)
K_{MK}(PIN)

K_{MK}(DataKey)
K_{MK}(MAC)
K_{KEK}(DataKey)

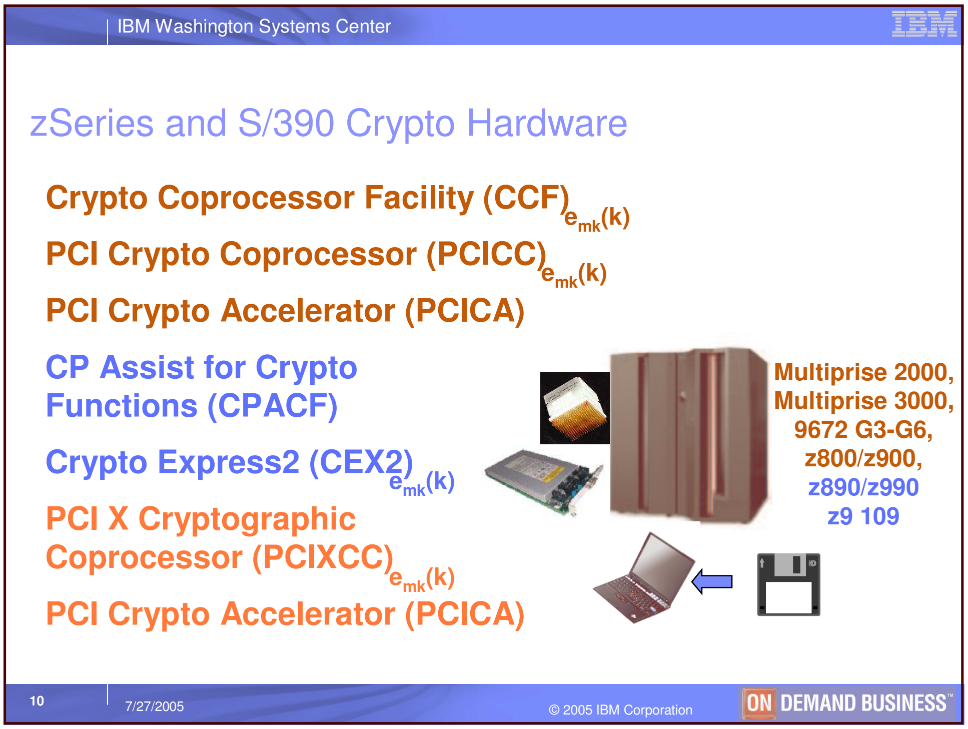


Operational Keys

- DATA – Encipher/Decipher
- DATAXLAT* – Translate data from one key to another
- MAC/MACVER – Generate or Verify MACs
- DATAM – Double length data key for MACing
- DATAMV – Double length data key for MACVER
- PIN Keys (PINGEN, PINVER, IPINENC, OPINENC)
- EXPORTER/IMPORTER – encrypt/decrypt keys sent to/from another node
- IMP-PKA – PKA Importer
- System Keys (Required System Keys, NOCV, ANSI, Extended System Keys)**

*Not supported on z890/z990

**NOCV, ANSI, Extended System Keys not required on z890/z990



zSeries and S/390 Crypto Hardware

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

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

PCI Crypto Accelerator (PCICA)

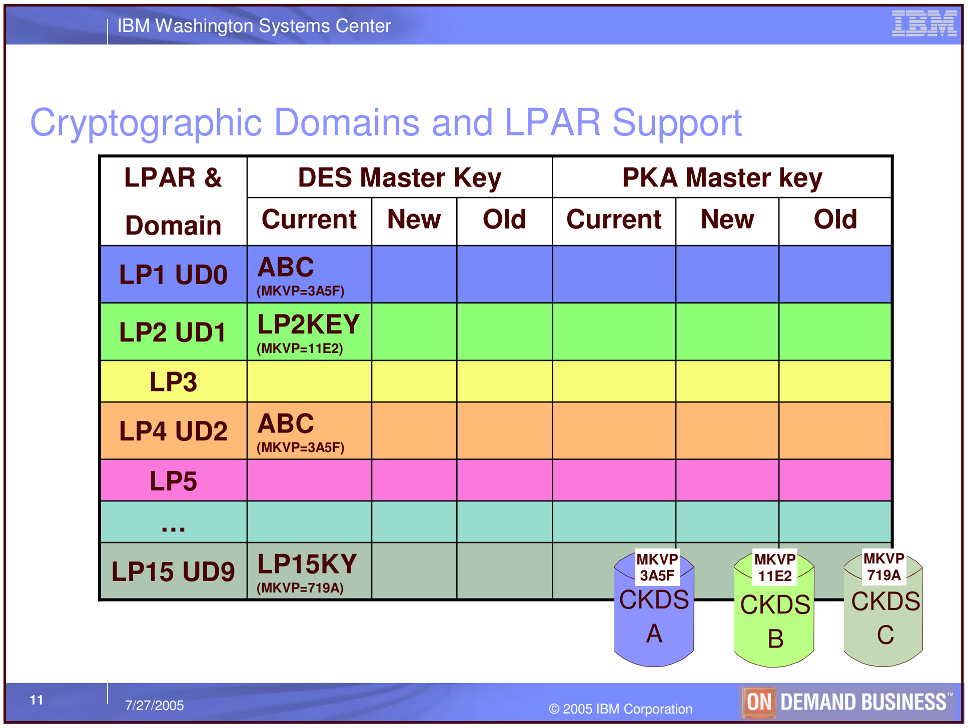
CP Assist for Crypto Functions (CPACF)

Crypto Express2 (CEX2)$e_{mk}(k)$

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

PCI Crypto Accelerator (PCICA)

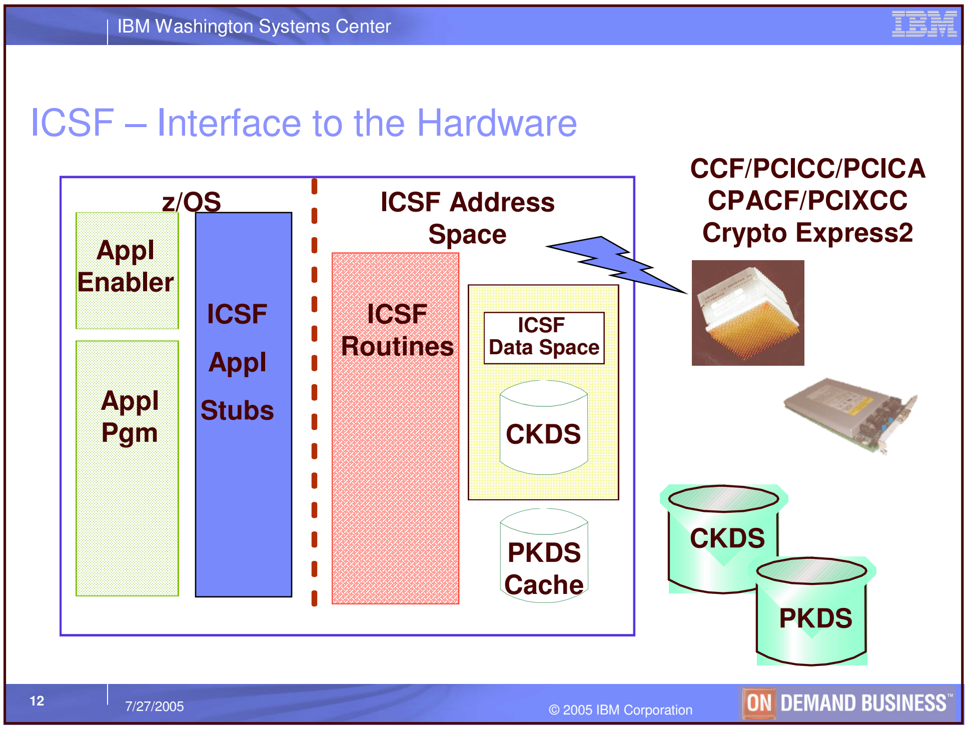
Multiprise 2000,
Multiprise 3000,
9672 G3-G6,
z800/z900,
z890/z990
z9 109



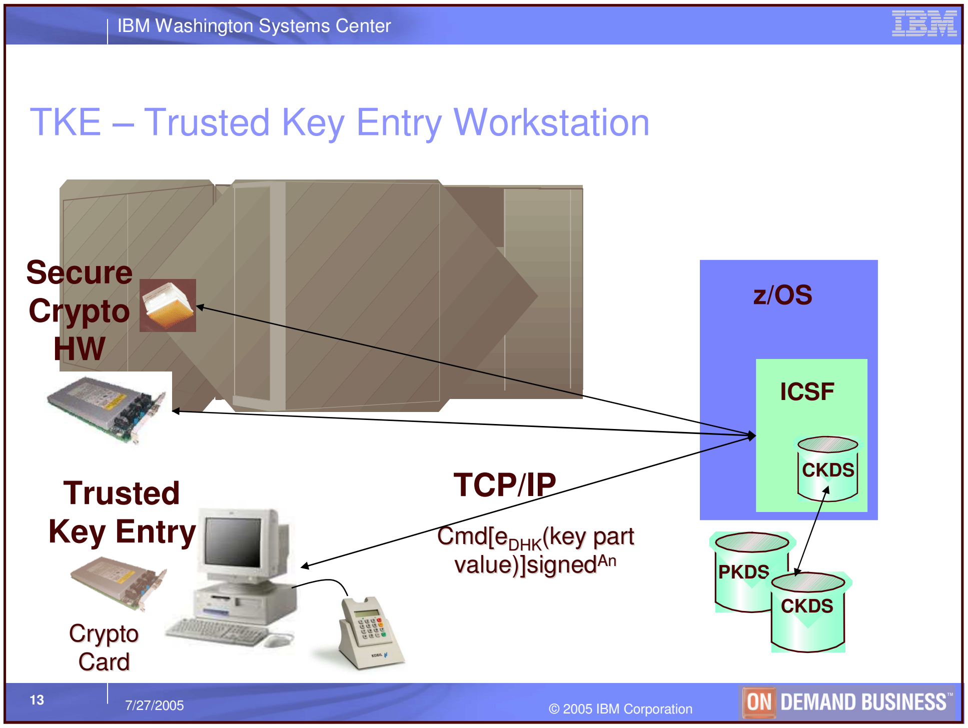
Cryptographic Domains and LPAR Support

LPAR &	DES Master Key			PKA Master key		
Domain	Current	New	Old	Current	New	Old
LP1 UD0	ABC (MKVP=3A5F)					
LP2 UD1	LP2KEY (MKVP=11E2)					
LP3						
LP4 UD2	ABC (MKVP=3A5F)					
LP5						
…						
LP15 UD9	LP15KY (MKVP=719A)					

MKVP 3A5F
CKDS A
MKVP 11E2
CKDS B
MKVP 719A
CKDS C



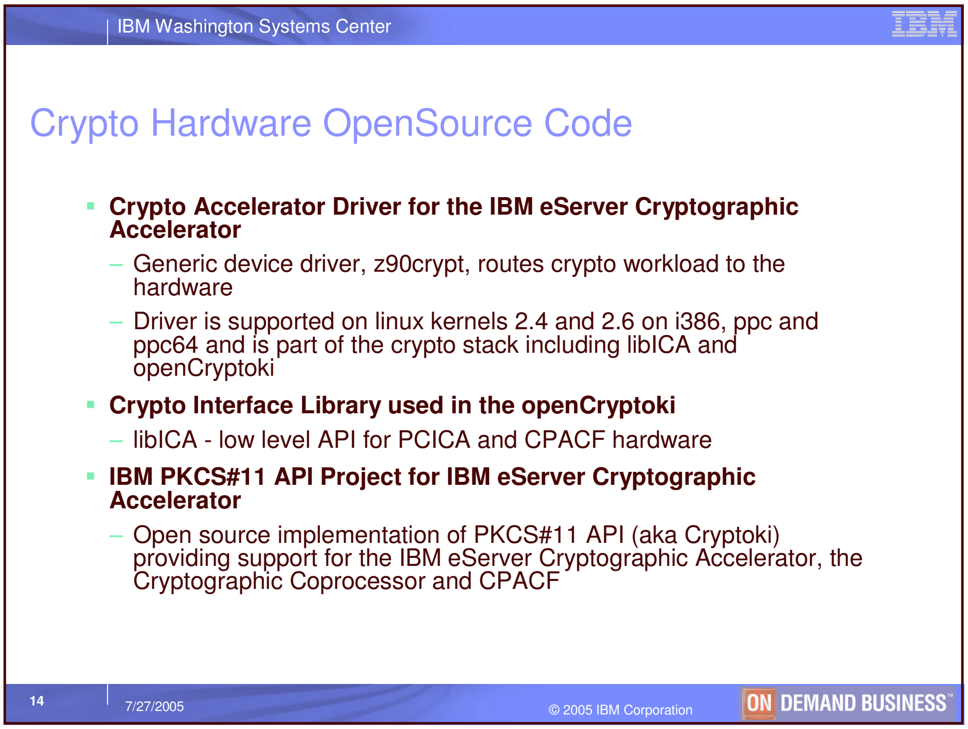
ICSF – Interface to the Hardware



IBM Washington Systems Center

TKE – Trusted Key Entry Workstation

13 7/27/2005 © 2005 IBM Corporation ON DEMAND BUSINESS™

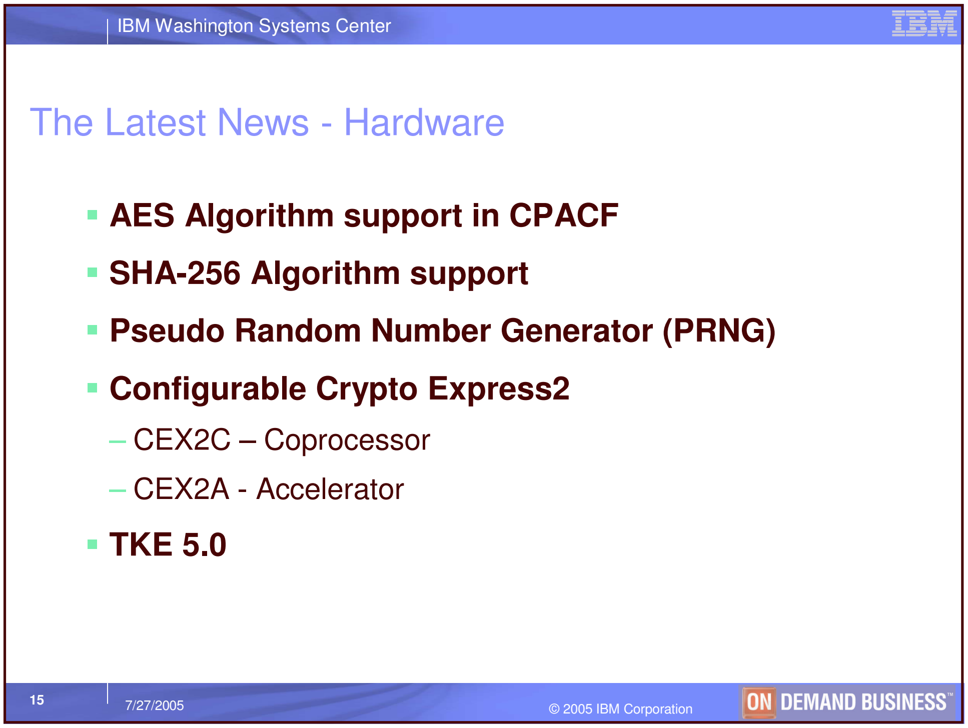


IBM Washington Systems Center

Crypto Hardware OpenSource Code

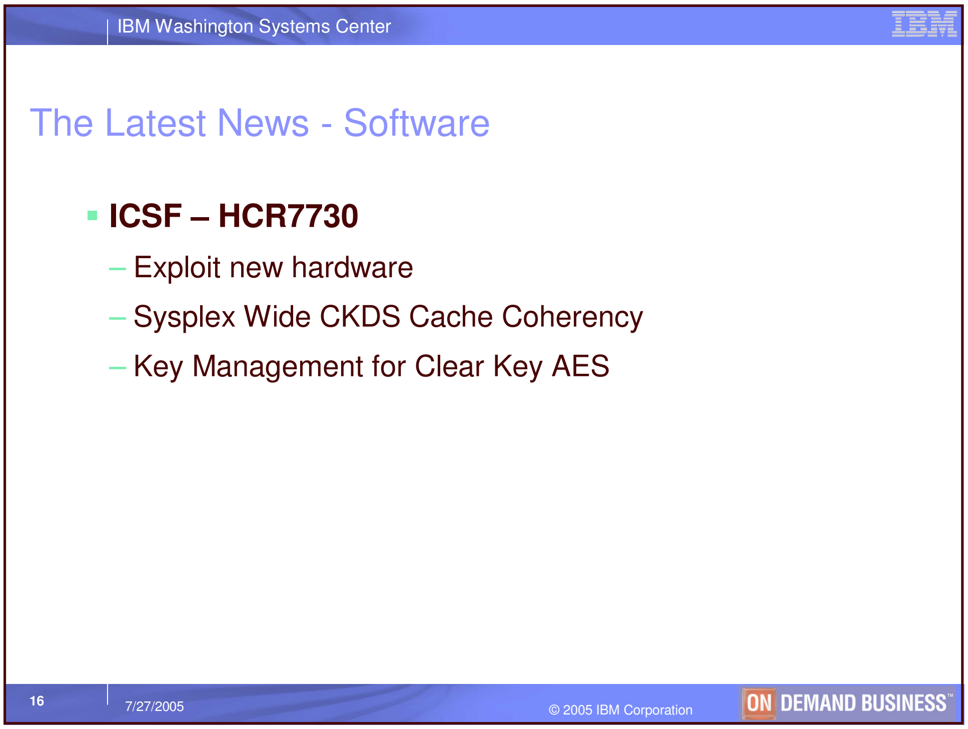
- **Crypto Accelerator Driver for the IBM eServer Cryptographic Accelerator**
  - Generic device driver, z90crypt, routes crypto workload to the hardware
  - Driver is supported on linux kernels 2.4 and 2.6 on i386, ppc and ppc64 and is part of the crypto stack including libICA and openCryptoki
- **Crypto Interface Library used in the openCryptoki**
  - libICA - low level API for PCICA and CPACF hardware
- **IBM PKCS#11 API Project for IBM eServer Cryptographic Accelerator**
  - Open source implementation of PKCS#11 API (aka Cryptoki) providing support for the IBM eServer Cryptographic Accelerator, the Cryptographic Coprocessor and CPACF

14 7/27/2005 © 2005 IBM Corporation ON DEMAND BUSINESS™



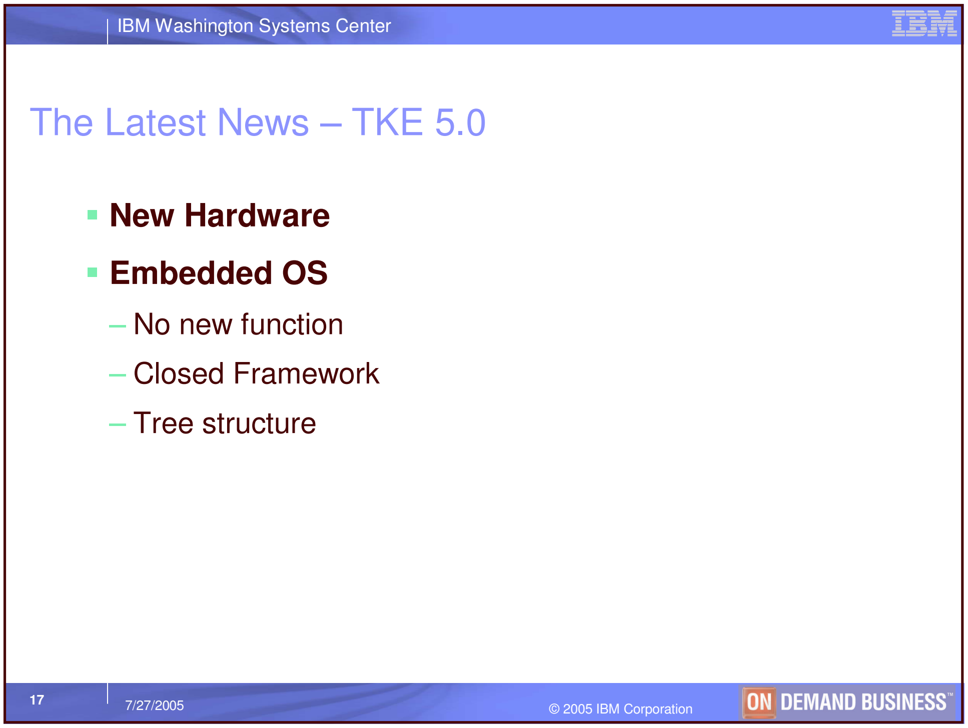
The Latest News - Hardware

- **AES Algorithm support in CPACF**
- **SHA-256 Algorithm support**
- **Pseudo Random Number Generator (PRNG)**
- **Configurable Crypto Express2**
  - CEX2C – Coprocessor
  - CEX2A - Accelerator
- **TKE 5.0**



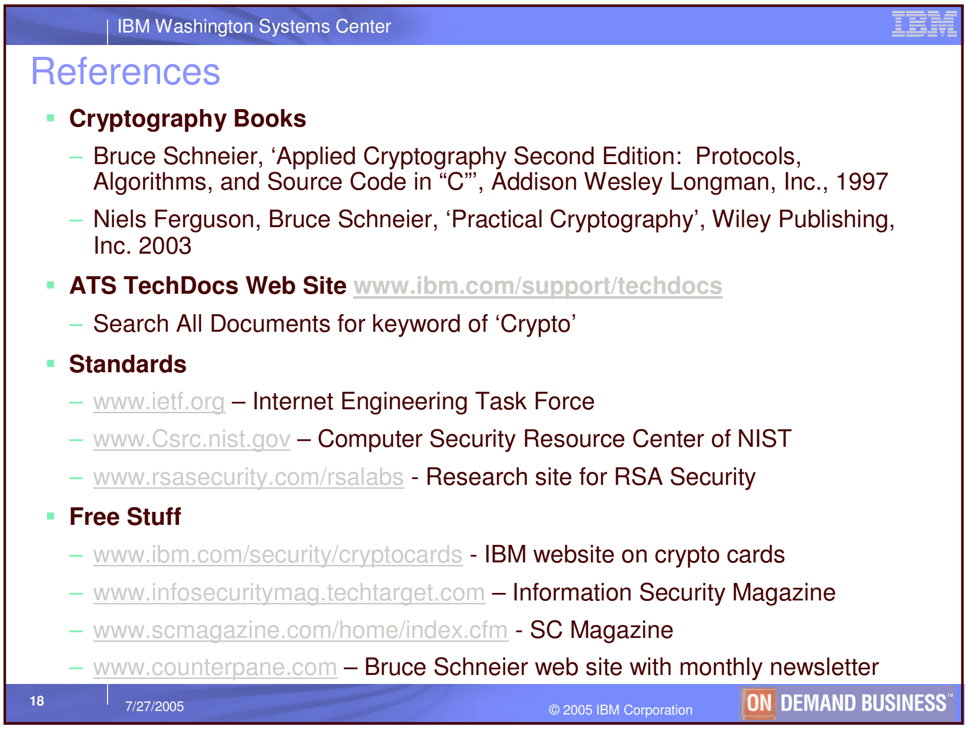
The Latest News - Software

- **ICSF – HCR7730**
  - Exploit new hardware
  - Sysplex Wide CKDS Cache Coherency
  - Key Management for Clear Key AES



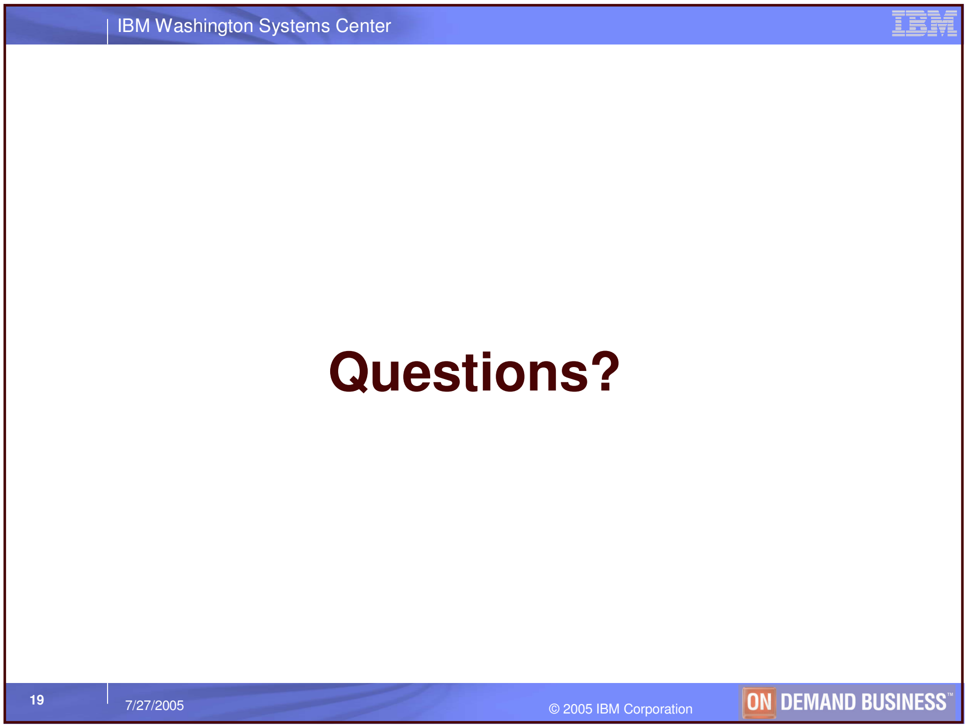
The Latest News – TKE 5.0

- **New Hardware**
- **Embedded OS**
  - No new function
  - Closed Framework
  - Tree structure



References

- **Cryptography Books**
  - Bruce Schneier, ‘Applied Cryptography Second Edition: Protocols, Algorithms, and Source Code in “C”’, Addison Wesley Longman, Inc., 1997
  - Niels Ferguson, Bruce Schneier, ‘Practical Cryptography’, Wiley Publishing, Inc. 2003
- **ATS TechDocs Web Site** www.ibm.com/support/techdocs
  - Search All Documents for keyword of ‘Crypto’
- **Standards**
  - www.ietf.org – Internet Engineering Task Force
  - www.Csrc.nist.gov – Computer Security Resource Center of NIST
  - www.rsasecurity.com/rsalabs - Research site for RSA Security
- **Free Stuff**
  - www.ibm.com/security/cryptocards - IBM website on crypto cards
  - www.infosecuritymag.techtarget.com – Information Security Magazine
  - www.scmagazine.com/home/index.cfm - SC Magazine
  - www.counterpane.com – Bruce Schneier web site with monthly newsletter



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, z/OS, zSeries, z/VM

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.