An Integrated Cryptographic Service Facility (ICSF HCR77A1) for z/OS Update for zEC12/zBC12 (GA2) and zBC12

Share 13724

Boston, MA August, 2013

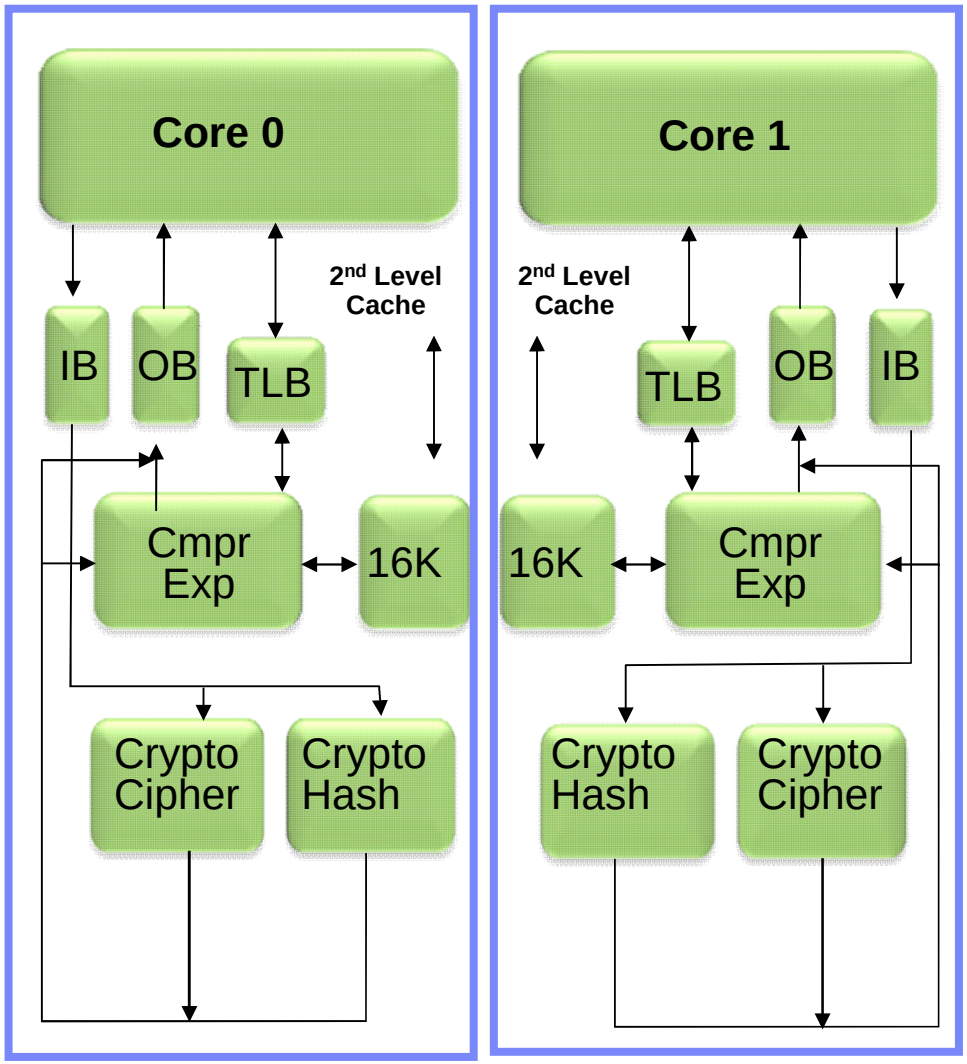
Greg Boyd (boydg@us.ibm.com)

Agenda

- **zEC12/zBC12/zBC 12 Hardware Changes**
  - CPACF
  - Crypto Express4S
- **ICSF HCR77A0**
- **ICSF HCR77A1**
- **TKE V7.2**
- **TKE V7.3**
- **A couple of other things**

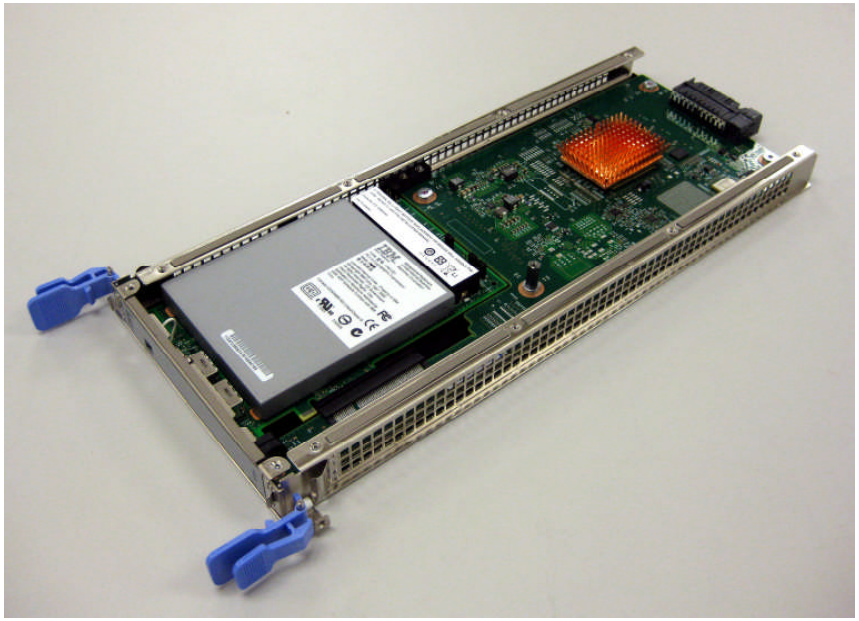
zEC12/zBC12/zBC12 Compression and Cryptographic Engine

- **Coprocessor dedicated to each core (Was shared by two cores on z196)**
  - Independent compression engine
  - Independent cryptographic engine
  - Available to any processor type
  - Owning processor is busy when it's coprocessor is busy
- **Data compression/expansion engine**
  - Static dictionary compression and expansion
- **CP Assist for Cryptographic Function**
  - 290-960 MB/sec bulk encryption rate
  - DEA (DES, TDES2, TDES3)
  - SHA-1 (160 bit)
  - SHA-2 (244, 256, 384, 512 bit)
  - AES (128, 192, 256 bit)
  - CPACF FC #3863 (No charge) is required to enable some functions and is also required to support Crypto Express4S or Crypto Express3 feature



Crypto Express4S

- **One PCIe Adapter per feature**
  - **Initial order – 2 features**
- **Up to 16 features per server**
- **FIPS 140-2 Level 4**
- **Installed in the PCIe I/O Drawer**
- **Prerequisite: CPACF (#3863)**



- Only one configuration option can be chosen at any given time
- Switching between configuration modes will erase all card secrets
  - ✓ Exception: Switching from CCA to accelerator or vice versa
- Accelerator
  - ✓ For SSL acceleration
  - ✓ Clear key RSA operations
- Enhanced: Secure IBM CCA coprocessor (default)
  - ✓ Optional: TKE workstation (#0841) for security-rich flexible key entry or remote key management
- New: IBM Enterprise PKCS #11 (EP11) coprocessor
  - ✓ Designed to meet public sector requirements
    - Both FIPS and Common Criteria certifications
  - ✓ Required: TKE workstation (FC #0841) for management of the Crypto Express4S when defined as an EP11 coprocessor

Enterprise Public Key (EP11) Mode

- **PKCS #11 (from Wikipedia)**

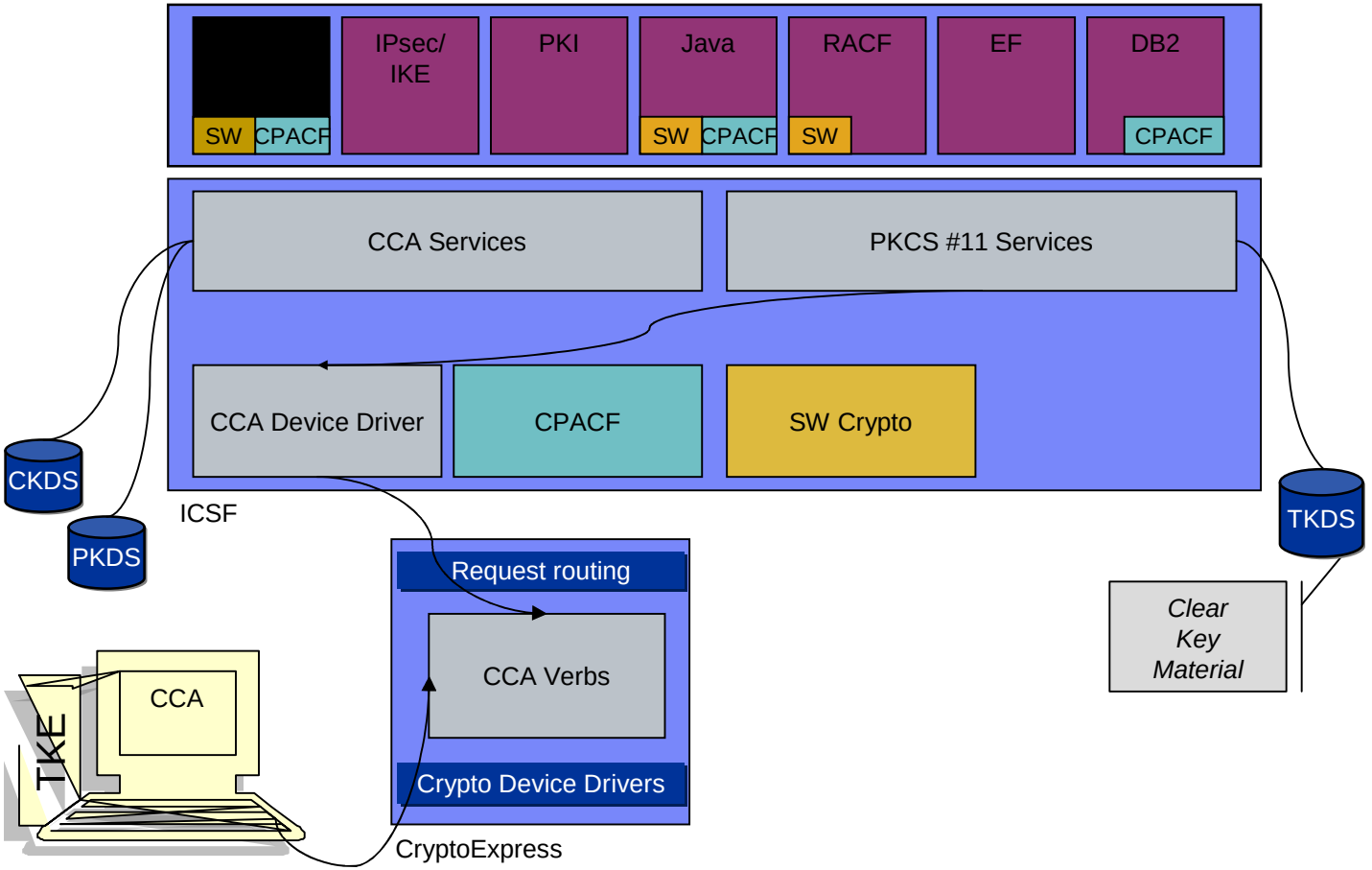
  Since there isn't a real standard for cryptographic tokens, this API has been developed to be an abstraction layer for the generic cryptographic token. **The PKCS #11 API defines most commonly used cryptographic object types (RSA keys, X.509 Certificates, DES/Triple DES keys, etc.) and all the functions needed to use, create/generate, modify and delete those objects.**

  PKCS #11 is largely adopted to access smart cards and HSMs. Most commercial Certification Authority software uses PKCS #11 to access the CA signing key or to enroll user certificates. Cross-platform software that needs to use smart cards uses PKCS #11, such as Mozilla Firefox and OpenSSL (using an extension).

- **PKCS #11 (from RSA, http://www.rsa.com/rsalabs/node.asp?id=2133)**

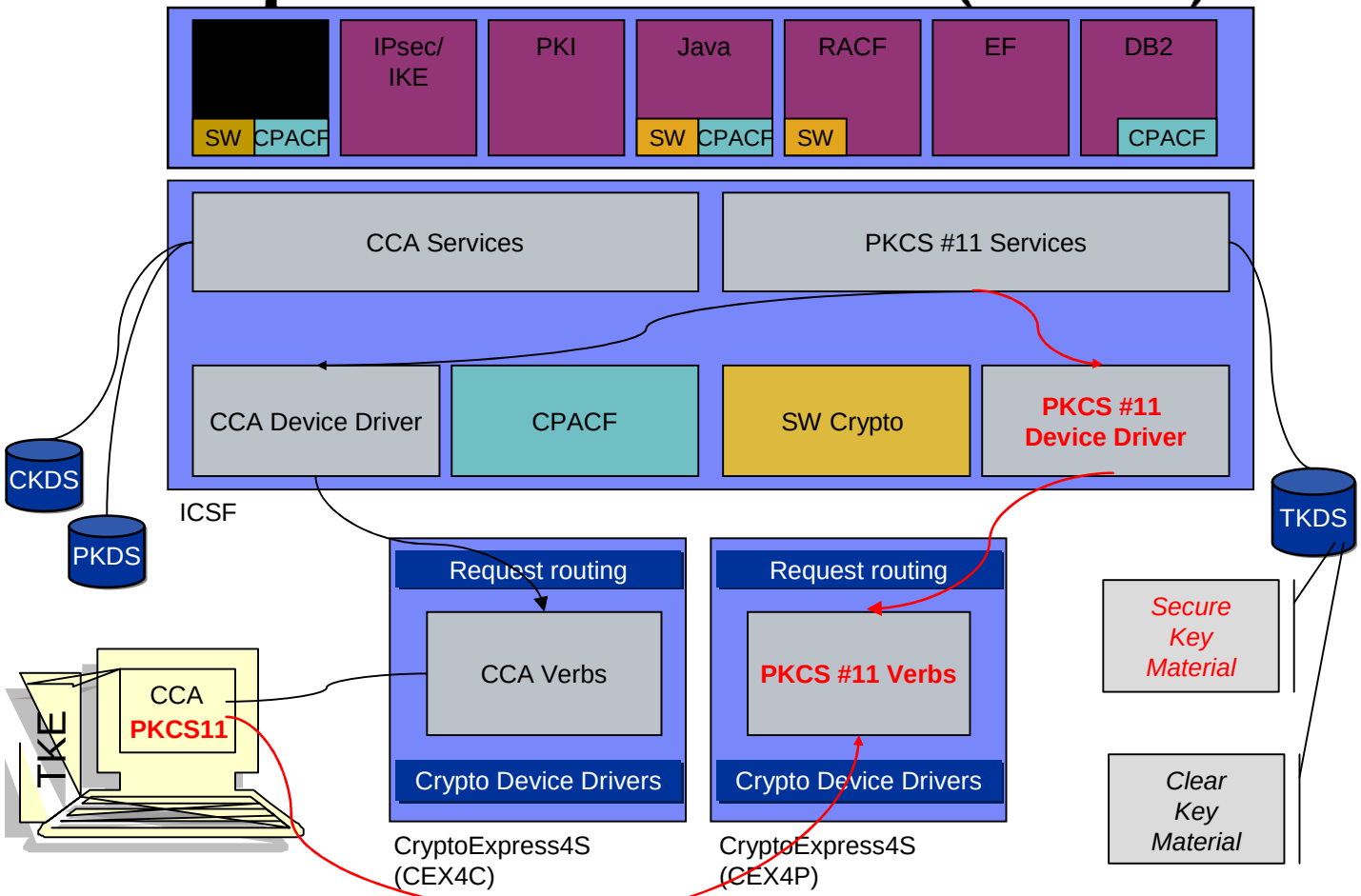
  This standard specifies an API, called Cryptoki, to devices which hold cryptographic information and perform cryptographic functions. **Cryptoki, pronounced crypto-key and short for cryptographic token interface, follows a simple object-based approach, addressing the goals of technology independence (any kind of device) and resource sharing (multiple applications accessing multiple devices), presenting to applications a common, logical view of the device called a cryptographic token.**

z/OS Security Stack (Current)



Problem: PKCS #11 support is clear key only

z/OS Security Stack – Enterprise PKCS #11 (EP11) Mode



EP11 enables Secure Key PKCS #11

IBM Common Cryptographic Architecture (CCA) Enhancements (Crypto Express4S on zEC12/zBC12)

- **Wrap weaker keys with stronger keys for security standards compliance**
  - 24-Byte DES-MK (TKE Required)
- **Secure Cipher Text Translate (CIPHERXI, CIHPERXL, CIPHERXO key types)**
- **Derived Unique Key per Transaction (DUKPT) for derivation of MAC and Encryption Keys**
- **Compliance with new Random Number Generator standards**
- **Europay, Mastercard and Visa (EMV) enhancements for applications supporting American Express cards**

IBM Common Cryptographic Architecture (CCA) Enhancements (Crypto Express4S on zBC12 and zEC12/zBC12 GA2) . . .

- **UDX Integration**
  - Recover PIN from Offset
  - Symmetric Key Export with Data
  - Authentication Parameter Generate
- **Export TDES keys using AES keys**
- **Diversified Key Generation using CBC**

. . . IBM Common Cryptographic Architecture (CCA) Enhancements (Crypto Express4S on zBC12 and zEC12/zBC12 GA2)

- **Initial PIN Encrypting Key (IPEK) Support**
- **Remote Key Export (RKX) Key Wrapping**
- **EMV Enhancements**
- **AES MAC Enhancements**

PKCS #11 Enhancements (Crypto Express4S on zBC12 and zEC12/zBC12 GA2)

- **New algorithms:**
  - PKCS-DH
  - ECDH
  - RSA-PSS - sign and verify
- **DSA/DH Domain Parm generate in card**
- **Brainpool EC Curves in FIPS mode**
- **Changing compliance mode (FIPS 2009, BSI 2009, FIPS 2011, BSI 2011)**

HCR77A0 Enhancements

- **Coordinated Key Administration Extended to RSA-MK, ECC-MK and PKDS**
- **Random Number Cache**
- **Key Generation Utility Program (KGUP) Enhancements**
- **FIPS on Demand (to verify FIPS 140-2 Level 1 compliance)**

Coordinated KDS Administration:
Coordinated CKDS Master Key Change and Coordinated CKDS Refresh

- Simplified process for performing ICSF CKDS administration in both a single system environment and more importantly in a sysplex environment.
- In a sysplex environment coordinated CKDS refreshes and coordinated CKDS change-mk operations are driven from a single ICSF instance across the sysplex.
- CKDS sysplex communication protocol level 2 provides better sysplex communication performance, uses less overhead, and is more serviceable then the prior release sysplex communication protocol.

HCR77A1 Enhancements

- **OWH/RNG SAF Check**
  - CSF.CSFSERV.AUTH.CSFOWH.DISABLE
  - CSF.CSFSERV.AUTH.CSFRNG.DISABLE
- **SAF/ACEE Enhancements - Under certain circumstances, authorization calls made by ICSF do not reflect the desired security context.**
- **Dynamic SSM**
- **AP Configuration Simplification**
- **Improved CTRACE**
  - New tracing options
  - Dynamic changes
- **KDS Utilization Statistics, Common Record Format**
- **SSL Non-SAF Protected IQF**
- **CCF Removal**

CEX4S Support …

- **z/OS Support**
  - HCR77A1 – Cryptographic Support for z/OS V1R13 – z/OS V2R1 (web download)
  - HCR77A0 – Cryptographic Support for z/OS V1R12 – z/OS V1R13 (web download and with z/OS V2R1
    - OA40267/UA66810 – Timing issue when running as a VM Guest
  - HCR7790 – Cryptographic Support for z/OS V1R11 – z/OS V1R13 (web download) plus OA39075
  - HCR7780 – Cryptographic Support for z/OS V1R10 – z/OS V1R12 (ships with z/OS V1R13) plus OA39075
  - HCR7770 – Cryptographic Support for z/OS V1R9 – z/OS V1R11 (ships with z/OS 1.12) plus OA39075
- **z/VM Support**
  - VM65007 – Compatibility support for CEX4S

… CEX4S

- **z/VSE Support**
  - z/VSE 5.1 with DY47414 – Provides support for zEC12 and CEX4S (in accelerator or coprocessor mode)
  - z/VSE 5.1 with DY47397 & UD53864 provides OpenSSL support
  - z/VSE 4.3 will run on zEC12, but it will not recognize a CEX4S (but it will use a CEX3 on the zEC12)
- **z/TPF Support**
  - PJ40362 – Support for CEX4S (accelerator mode only)
- **Linux on System z Support**
  - Exploitation on RHEL 6.4 and SUSE SLES 11 SP3
  - Toleration on RHEL 5 and RHEL 6 and SUSE SLES10 and SLES11

New Healthcheck – OA42011

- **ICSFMIG77A1_CCA_COPROCESSOR_ACTIVE**
- **ICSFMIG77A1_UNSUPPORTED_HW**
- **ICSFMIG77A1_TKDS_OBJECT**

Applies to HCR7770, HCR7780, HCR7790, HCR77A0

Coexistence – KDS Sharing

- **HCR7780, HCR7790, HCR77A0**
  - OA42014 (UA?????, UA?????, UA?????) – HCR77A1 introduces a common keystore record format and new key type DESUSECV
- **HCR7770, HCR7780, HCR7790**
  - OA39484 (UA90038, UA90639, UA90640) - HCR77A0 introduced new key wrapping support for ECC private key tokens wrapped with ECC-MK and PKCS #11 secure keys
- **HCR7780**
  - OA36718 (UA62059) – HCR7790 introduced variable length CKDS keys support

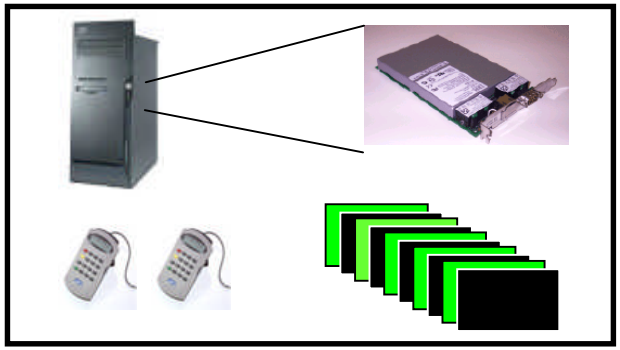
Coexistence – KDS Sharing

- **HCR7740, HCR7750, HCR7751**
  - OA29997 (UA51253, UA51254, UA51255) – HCR7770 introduced new TKDS record types
- **HCR7740, HCR7750, HCR7751, HCR7770**
  - OA33320 (UA90554, UA90555, UA90556, UA90557) - HCR7780 introduced new support for X9.24 CBC key wrapping

Trusted Key Entry (TKE) Workstation

Components

- **Workstation with a 4765 Cryptographic Coprocessor**
- **TKE 7.2 LIC**
- **Smart card readers and smart cards**
  - Required if using Enterprise PKCS #11 LIC
  - Optional if using IBM CCA LIC

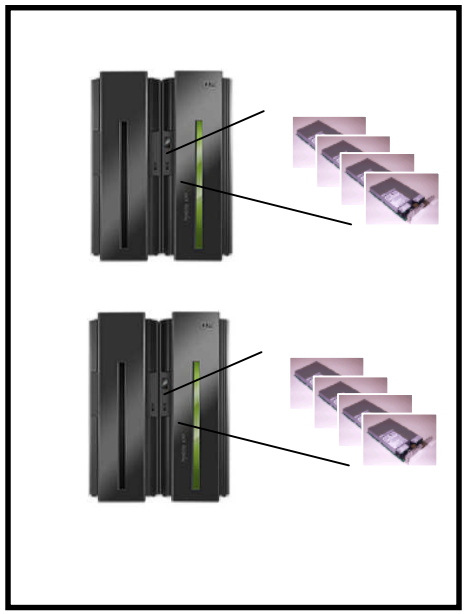


Purpose

- **Used to manage multiple Cryptographic Coprocessors and keys on various generations of System z (zEC12/zBC12, z196, z114 and z10 EC/BC) from a single point of control**
  - Support requirements for standards
  - Simplification of tasks

Trusted Key Entry (TKE) 7.2

- **Support of new hardware or firmware functions**
  - Support for Crypto Express4S defined as a CCA processor
  - Required for Crypto Express4S defined as an Enterprise PKCS #11 coprocessor
  - New DES operational keys
  - New AES Cipher key attribute
  - Allow creation of corresponding keys
  - Support 4 smart card readers
- **Support requirements for standards**
  - Stronger key wrapping
- **Support for up to Four Smart Card Readers**
  - PKCS #11 mode may require more signatures, and thus more smart cards

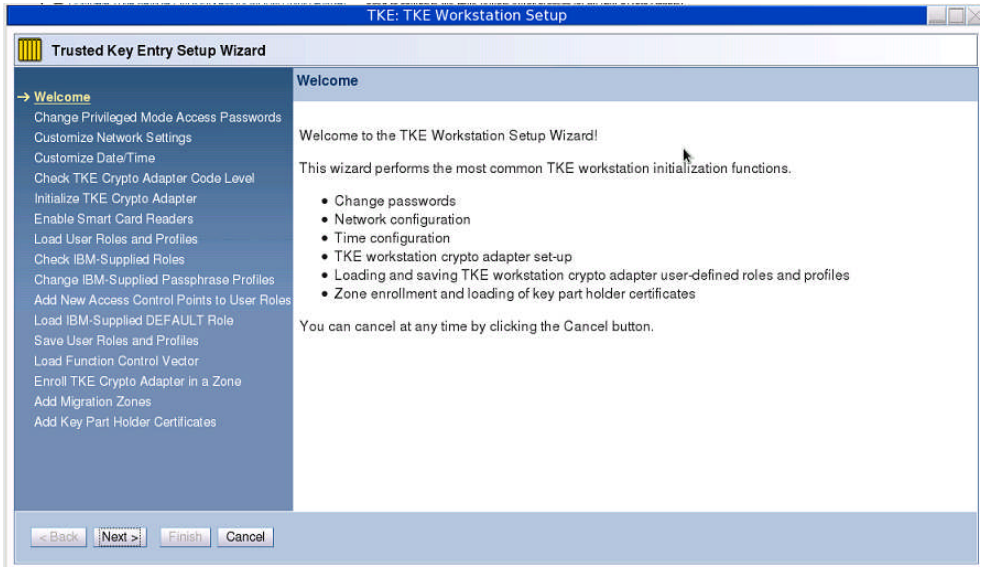


Smart Card part 74Y0551

- **Smart cards used to**
  - Hold credentials
  - Hold key material
  - Perform encryption functions.
- **TKE has 6 different uses for smart cards**
  - Certificate Authority – used to define TKE Zones
  - TKE – for managing CCA adapters
  - EP11 – for managing EP11 adapters
  - MCA (Migration Certificate Authority) - for defining zones associated with the migration wizard
  - Key Part Holder – for holding parts of a master key being transported
  - Injection Authority – for injecting master keys into new adapters

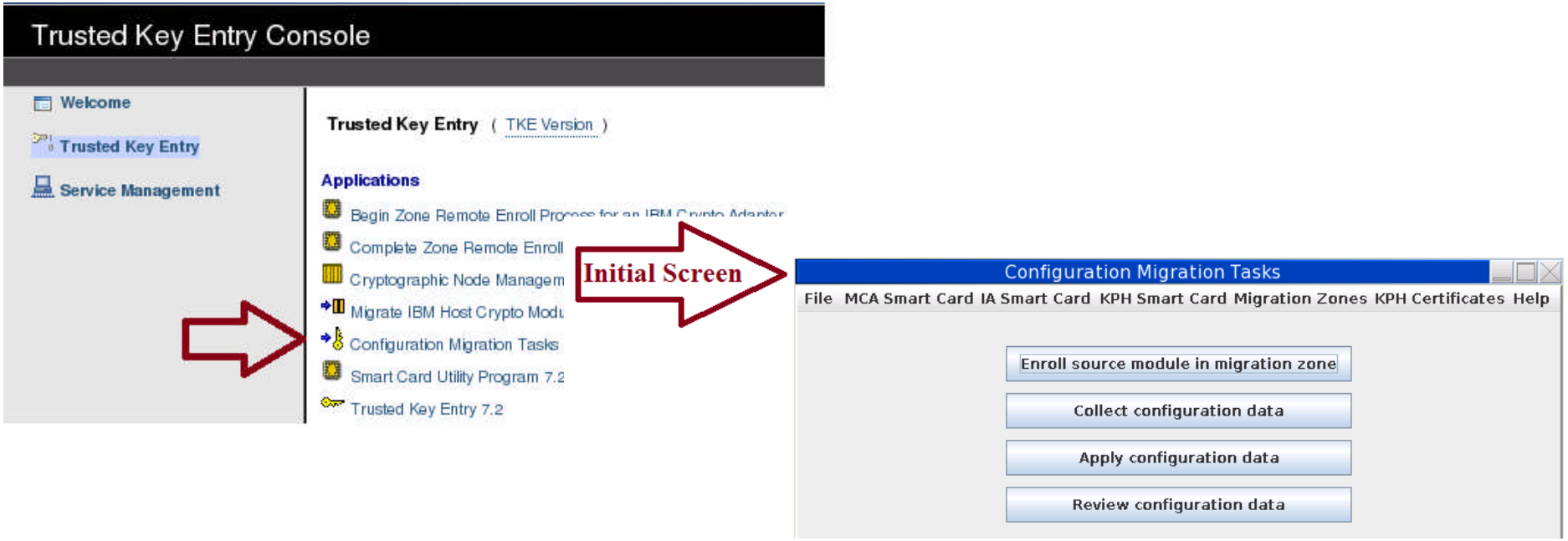
TKE 7.3 Installation Wizard

- **Change Privileged Mode Access Passwords**
- **Customize Network Settings**
- **Customize Datae/Time**
- **Check TKE Crypto Adapter Code Level**
- **Initialize TKE Crypto adapter**
- **Enable Smart Card Readers**
- **Load User Roles and Profiles**
- **Check IBM Supplied Roles**
- **Change IBM Supplied Passphrase Profiles**
- **Add New Access Control Points to User Roles**
- **Load IBM Supplied DEFAULT Role**
- **Save User Roles and Profiles**
- **Load Function Control Vector**
- **Enroll TKE Crypto Adapter in a Zone**
- **Add Migration Zones**
- **Add Key Part Holder Certificates**



TKE 7.3 Full Function EP11 Migration Wizard

- **Extension of CCA Migration Wizard**
- **Collect config data from one EP11 Host Crypto Module and apply to another EP11 Host Crypto**



Increase TKE Session Key Strength

- The ***session key*** on the TKE refers to the encryption key used to protect key parts exchanged between
  - **Smart card ↔ TKE local crypto adapter**
  - **Smart card ↔ Smart Card**
- TKE 7.2 or less, session key is Triple DES key
- TKE 7.3, session key is AES 256-bit

Audit Driven Enhancements

- **Unload Authority Signature Key**
- **Close Host**
- **Domain Group Management - Domain Access Control Points**
- **Domain Group Management - Only Allow Domain in Group Once**
- **User Defined CCA and EP11 Domain Control Lists**
- **Allow Set Master Key from TKE**
- **Limit Ability to Manage Host Entries**
- **Increase TKE Session Key Strength**

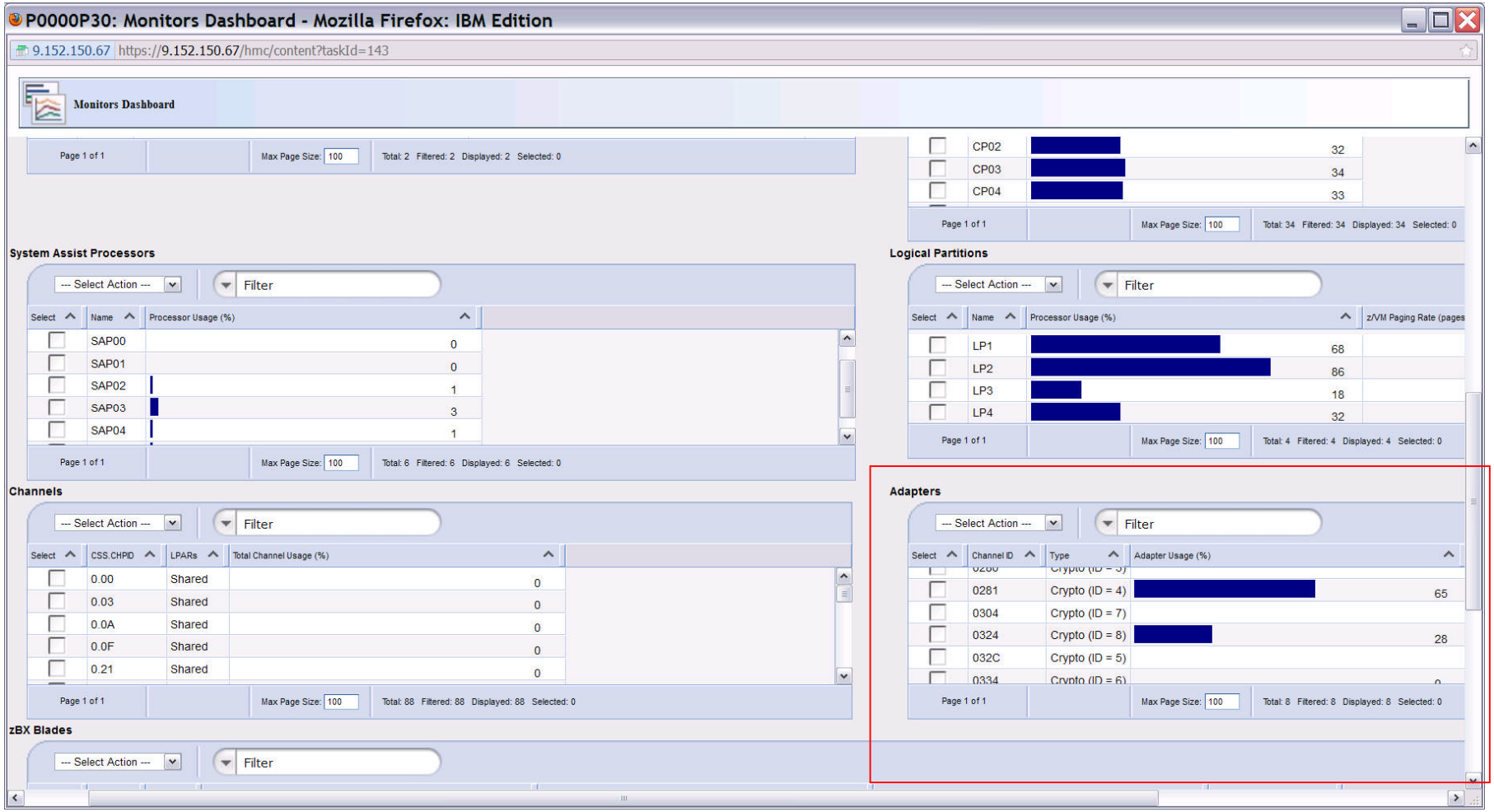
A Couple of Other Things

- **SPE for Encryption Facility for z/OS**
- **Monitor Dashboard**
- **Flash Express**
- **Time Source STP**

IBM Encryption Facility for z/OS (5655-P97) – OA40664

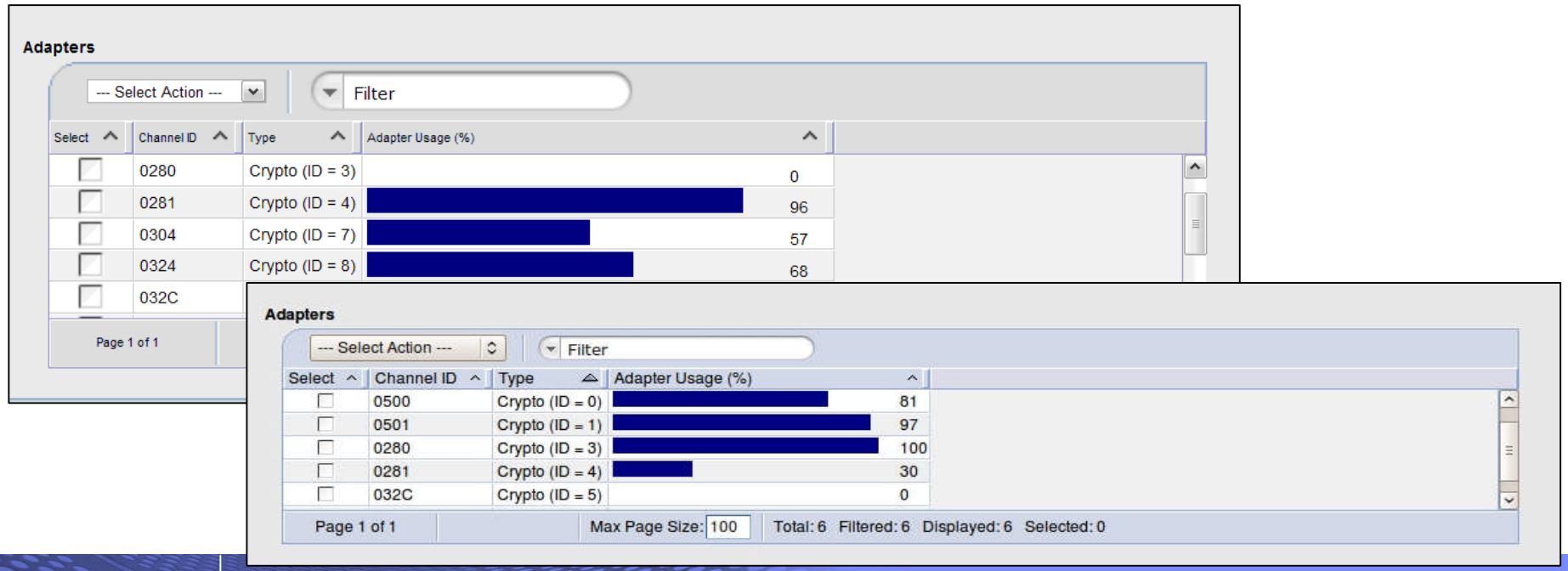
- **RFC 4880 Support in the IBM Encryption Facility**
  - Speculative Key ID Support
  - Multiple recipients with Symmetrically Encrypted Integrity Protected Data Packet
  - Support for notation Data Sub-packets containing raw binary data
- **Batch Key Generation and Batch Public Key Export**

Monitor Dashboard Support for Crypto



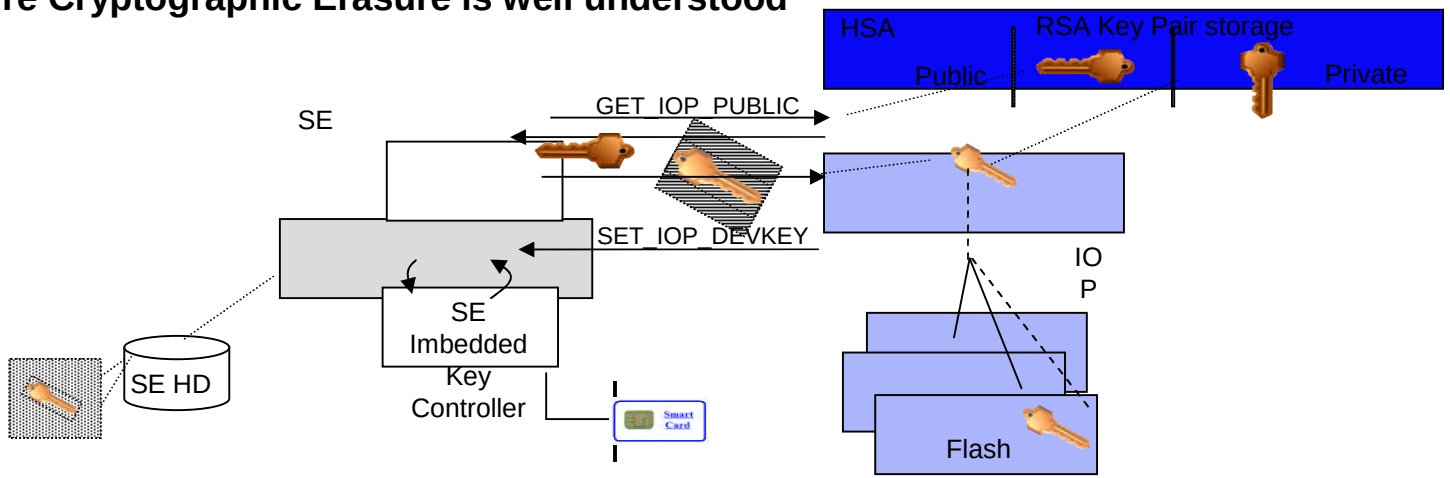
Monitor Dashboard support for crypto

- **Monitors Dashboard on the HMC and SE was enhanced with a new Adapters table for System zEC12/zBC12**
- **Will provide information about Utilization rate per Crypto Processor**
  - System wide utilization (not LPAR specific)
  - Shown per Crypto #
- **Source: collected Crypto performance measurement data (as used by RMF)**



Security of Data on Flash Express

- **System z internal flash can be used for paging, dumping and …**
  - It can contain all data, including audited personally identifiable data
- **Client data on flash is protected by strong encryption**
  - Done using hardware encryption at the device, like IBM's Disk and Tape encryption
- **Key management is provided based on a Smart Card in each Support Element**
- **End of life Audit is based on access to the Smart Card, not access to Flash Memory**
- **Secure Cryptographic Erasure is well understood**



HMC – STP (Server Time Protocol) Broadband Security

- **Network Time Protocol (NTP) Authentication – Added to the HMC's NTP communication with external NTP time servers**
  - Symmetric key authentication – described in RFC-1305 (made available in NTP Version 3)
  - Autokey (using public key cryptography) – described in RFC-5906 (made available in NTP Version 4)

References

- **SA22-7520 ICSF Systems Programmer's Guide**
- **SA22-7521 ICSF Administration Guide**
- **SA22-7522 ICSF Application Programmer's Guide**
- **SA23-2211 TKE Workstation User's Guide**
- **Announcement Letter 112-155 zEC12**
- **Announcement Letter 113-119 zEC12 GA2**
- **Announcement Letter 113-121 zBC12**
- **Announcement Letter 213-292 z/OS 2.1**

More Good Stuff

- **How to videos**
  - http://www.youtube.com/user/IBMTKE
- **TechDocs**
  - www.ibm.com/support/techdocs (and search on Crypto)

Questions

Trademarks

The following are trademarks of the International Business Machines Corporation in the United States, other countries, or both.

Not all common law marks used by IBM are listed on this page. Failure of a mark to appear does not mean that IBM does not use the mark nor does it mean that the product is not actively marketed or is not significant within its relevant market.

Those trademarks followed by ® are registered trademarks of IBM in the United States; all others are trademarks or common law marks of IBM in the United States.

For a complete list of IBM Trademarks, see www.ibm.com/legal/copytrade.shtml:

*BladeCenter®, DB2®, e business(logo)®, DataPower®, ESCON, eServer, FICON, IBM®, IBM (logo)®, MVS, OS/390®, POWER6®, POWER6+, POWER7®, Power Architecture®, S/390®, System p®, System p5, System x®, System z®, System z9®, System z10®, WebSphere®, X-Architecture®, zEnterprise, z9®, z10, z/Architecture®, z/OS®, z/VM®, z/VSE®, zSeries®

The following are trademarks or registered trademarks of other companies.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.
Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.
Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. 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, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
UNIX is a registered trademark of The Open Group in the United States and other countries.
Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.
IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency, which is now part of the Office of Government Commerce.

* 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.